Of course, terrorists didn't need the CIA to tell them that the U.S. government monitors their communications. Telegram is only one in a string of messaging systems ISIS has employed to protect its communications, U.S. officials told The Daily Beast. And some apps that have marketed their privacy-enhancing features, such as Snapchat and Secret have either disclosed their users' supposedly-private information, or have been shown to be vulnerable to hacking. In other words, they're not-so-secret after all.

But Telegram is ISIS' new "it" app—until they find another.

Founded in 2013, Telegram is the brainchild of a pair of Russian brothers, Pavel and Nikolai Durov. Pavel, the 31-year old founder of Russia's biggest social network, VKontakte, or VK, is a vocal critic of Vladimir Putin's government and provides the financial backing. Nikolai is the technical brains behind the outfit.

Not surprisingly, Telegram doesn't market its product to terrorists. But being a force against government surveillance is built into the company's philosophy.

"The No. 1 reason for me to support and help launch Telegram was to build a means of communication that can't be accessed by the Russian security agencies," Durov told TechCrunch last year in an interview.

The company says that Telegram has no connections to the Russian government. In fact, its headquarters are in Berlin.

Durov may have been trying to frustrate the Russians, who are waging their own war against Islamist militants. But he's also piqued the Americans. And, it turns out, the Iranians, who this week arrested administrators of more than 20 Telegram groups, accusing of them of spreading "immoral" content, Reuters reported. Smartphone messaging apps are popular among Iranian youth, who compose the majority of the country's population, and Iranian hardliners have been cracking down on potential subversion as the country opens up more to the West with the lifting of economic sanctions.

Telegram may be a tool for pro-democracy activists. But its anti-surveillance capabilities won't win it any points in the CIA's eye.

In his remarks Monday, Brennan was forceful in his assertion that technologies and policies set up in part to counter government overreach were making his agency's job harder.

"In the past several years, because of a number of unauthorized disclosures and a lot of handwringing over the government's role in the effort to try to uncover these terrorists, there have been some policy and legal and other actions that are taken that make our ability collectively internationally to find these terrorists much more challenging," Brennan said.

He didn't mention any names, but one in particular hung unspoken in the air: Edward Snowden.

Brennan seemed to give voice publicly to what dozens of his colleagues have argued privately, that a chain of events starting with the Snowden leaks in 2013 has worked their efforts to stop terrorist attacks. Following the disclosures, some European governments moved to enact stricter data protection rules seen as a bulwark against American surveillance. And the European Court of Justice recently invalidated an agreement that allows the free-flow of

personal information from European countries to the U.S., based on allegations of surveillance found in press article based on Snowden's leaks.

"I do hope that this is going to be a wake-up call, particularly in areas of Europe where I think there has been a misrepresentation of what the intelligence security services are doing by some quarters that are designed to undercut those capabilities," Brennan said.

Paris attack suspects: what do we know about them?, The Guardian

The Guardian
2015 11 17

French authorities have said seven attackers died while carrying out Friday night's terror attacks, while one other believed to be "directly involved" in the bloodshed is on the run. Belgian authorities have arrested seven other men in connection with the attacks.

Four have been officially named – three of the dead attackers, and the wanted man – but details have emerged about others suspected of involvement. Among them are three brothers: one dead, one arrested and one on the run.

The alleged mastermind

French officials have named Abdelhamid Abaaoud, a 27-year-old Belgian linked to a Brussels-based terror cell, as the alleged mastermind of the Paris attacks. He remains at large and is believed to be in Syria.

Abaaoud was also linked by French officials to the thwarted attacks on a Paris-bound high-speed train in August and a foiled plot to attack a church in Paris in April. The French newspaper Libération also linked Abaaoud to Sid Ahmed Ghlam, a French student charged with murder, attempted murder and terror offences.

It is alleged that documents found at Ghlam's home and results from a search of his computer and telephone suggested that he was in contact with a French speaker in Syria who had ordered him to carry out an attack on a church.

Abaaoud has been described as the alleged ringleader of a Belgian terror cell , which the authorities tried to destroy in January, days after the Charlie Hebdo attacks in Paris. The counter-terror raids led to the arrests of 13 jihadis in Belgium – however, Abaaoud remained at large.

In July, Abaaoud was sentenced in absentia to 20 years in prison for recruiting Islamic State fighters to Syria. He was among 32 people charged in Belgium with running one of Belgium's largest jihadist recruitment networks, although many of the defendants – including Abaaoud – were tried in absentia and remain at large.

Abaaoud was also accused of kidnapping after his younger brother Younes travelled to Syria in January 2014 at the age of 13 and earned the media nickname of "the youngest jihadist in the world." Their father Omar Abaaoud, having heard no news from his two sons, filed a police complaint against the older son, AFP reported in May.

He is known to have spent time fighting alongside Islamic State in Syria, arriving in the wartorn country in January this year. He was known to security forces after appearing in an Isis video at the wheel of a car transporting mutilated bodies to a mass grave.

VTM, a Flemish-language channel, reported that Abaaoud made calls from Greece to the brother of one of two heavily armed suspects killed in Verviers during the counter-terrorism raids in January.

In an interview with the Isis magazine Dabiq in February, Abaaoud boasted that he had been able to plot attacks against the west under the nose of Belgian intelligence agencies.

Abaaoud, also known as Abu Umar al-Baljiki, said he and two fellow jihadis wanted to "terrorise the crusaders waging war against the Muslims".

Posing for photographs holding an Isis flag and the Qur'an, the bearded militant said he and two fellow fighters travelled to Belgium to wage jihad in the country.

Abaaoud revealed that he was stopped during the journey by "an officer" after a picture of him fighting for Isis was published in Belgian media. He added, however, that the officer "let me go, as he did not see the resemblance". It is not clear when or where this police intervention is said to have taken place.

Asked by the magazine why he became a suspect, Abaaoud said: "The intelligence knew me from before as I had been previously imprisoned by them. After the raid on the safe house, they figured out that I had been with the brothers and that we had been planning operations together. So they gathered intelligence agents from all over the world – from Europe and America – in order to detain me.

"They arrested Muslims in Greece, Spain, France, and Belgium in order to apprehend me... All those arrested were not even connected to our plans! May Allah release all Muslims from the prisons of these crusaders."

He boasted that he had been able to plan terror attacks against westerners while living in Belgium and being wanted by intelligence agencies. Some time later, he travelled to Syria.

"I was able to leave... despite being chased by so many intelligence agencies," he told the magazine. "All this proves that a Muslim should not fear the bloated image of the crusader intelligence.

"My name and picture were all over the news yet I was able to stay in their homeland, plan operations against them, and leave safely when doing so became necessary. I ask Allah to accept the fruitful deeds of the shuhada' who terrorised the crusaders of America, France, Canada, Australia, Germany, and Belgium."

The Bataclan attackers

1. Omar Ismaïl Mostefai was the first attacker named by French authorities. The 29-year-old is of Algerian heritage and grew up in Courcouronnes, just south of Paris; he had a criminal record for petty offences. He was identified by prints taken from a severed finger found in the Bataclan concert hall, where he detonated his explosives belt.

French intelligence took note of Mostefai when he began spending time at a mosque with radical links in 2010, but they lost track of him in 2013, when he may have travelled to Syria, the Washington Post reported. Turkish authorities said he entered the country in 2013 and there is no record of him leaving. His brother said they had not spoken for years, but he is still being questioned by police along with six others, including Mostefai's father and sister-in-law.

Turkish authorities said they notified France twice about Mostefai – in December 2014 and June this year – after French officials requested information on his whereabouts on 10 October last year. Officials in Ankara said they never heard back from their French counterparts on the matter until after the Paris attacks, when they received another information request about Mostefai.

In 2010, Mostefai had been the subject of a police "S" file for radicalisation, but the state prosecutor said he had never been implicated in membership of a terrorist organisation. Police are reported to be investigating whether Mostefai travelled to Syria from 2013–2014. The local paper, Le Journal du Centre, reported that Mostefai attended a mosque in Lucé, a town that borders Chartres, and may have followed a radical Belgium-based Islamist who visited the mosque.

2. Samy Amimour , a 28-year-old Frenchman, was named on Monday as the other suicide bomber at the Bataclan. Born on 15 October 1987 in Paris, from the north-eastern suburb of Drancy, Amimour reportedly worked as a bus driver in Paris until 2012. Also that year, he was allegedly charged in a terrorism investigation and placed under judicial supervision. However, he dropped off the radar and was the subject of an international arrest warrant. Amimour's father, Mohamed, 67, went to Syria last year to try bring his son home – but was unsuccesful. Mohamed told Le Monde in December 2014 that he had an "extremely cold reunion" with his son in Syria in June last year and was unable to convince him to return. Samy had been injured and was on crutches during the brief reunion, Mohamed said: "Samy was with another guy who never left us alone. It was an extremely cold reunion and he did not take me to his house, did not tell me how he's been injured [or] if he had fought." Three of his family and friends were arrested in pre-dawn counter-terrorism raids on Monday.

The Stade de France attackers

3. Another attacker who lived in Belgium was named by the Washington Post as Bilal Hadfi, although he has not yet been officially identified by French prosecutors. The 20-year-old is thought to have fought for Islamic State in Syria, the paper said, but did not give his nationality. Belgian reports suggest Hadfi was from Neder-over-Heembeek, in north Brussels, and became quickly radicalised last year. He is said to have gone to Syria in spring this year, according to Belgian newspaper Het Laatste Nieuws .

4. Another attacker who detonated his explosive vest outside the Stade de France stadium was carrying a Syrian passport in the name of Ahmad Almohammad , aged 25, from Idlib. A statement from the prosecutor's office said the passport "remains to be verified, but that the fingerprints matched those of someone who entered Europe through the Greek island of Leros in October. The Serbian newspaper Blic said he crossed into the country on 7 October, having arrived four days earlier in Leros. The paper also reported that French security officials had asked their Serbian counterparts for help as the man had been registered in the southern Serbian town of Preševo. A Greek newspaper, Protothema, said he was travelling with a second man, Mohammed Almuhamed , and published pictures purporting to show their travel documents. As ever, such details are hard to verify. It cannot be ruled out that the men were

travelling under false documents – the Guardian has previously reported on the burgeoning trade in fake and stolen passports.

Suspect on the run

5. Salah Abdeslam went on the run after the attacks. He is the subject of an international police hunt after the Police Nationale issued a wanted notice for the 26-year-old on Sunday. Abdeslam is thought to have rented the black Volkswagen Polo used by the group that attacked the Bataclan concert hall, the Associated Press reported. He was born and lived in Belgium, although French police have described him as a French national. In the hours after the attacks, French police stopped Abdeslam and two other men close to the border with Belgium, but allowed them to go on their way because their names were not at that stage on any wanted list.

Boulevard Voltaire attacker

6. Brahim Abdeslam , the brother of the fugitive attacker Salah Abdeslam, was identified by prosecutors as the man who rented a Seat vehicle used in the attacks. He carried out the suicide attack at the Comptoir Voltaire cafe. Brahim, 31, was a French national based in Belgium.

Others

Belgian authorities on Monday released five out of the seven suspects who were arrested at the weekend after the Paris attacks, including the brother of one of the suicide bombers, prosecutors said. Mohamed Abdeslam – whose brother Ibrahim took part in the attacks and whose other brother Salah is being hunted by police – was freed "without being charged", a spokesman for the prosecutor's office told AFP.

Several people were also detained in anti-terrorist raids in Toulouse, Grenoble, Jeumont and Bobigny overnight on Sunday, but it is unclear whether any of these are directly connected to the Paris attacks. The Toulouse arrests are not said to be directly linked, but were carried out under the national state of emergency declared by President François Hollande after the Friday night attacks.

ISIS Is Using Everything From Encryption To PlayStations To Avoid Being Spied On, BuzzFeed News

BuzzFeed News
Sheera Frenkel
2015 11 16

New York - In the week leading up to the attack on Paris, which ISIS has claimed responsibility for, at least four different intelligence agencies warned French officials about a possible attack on "Western targets."
"We know of three agencies who passed on these warnings — we were one of them," said an Israeli diplomat, who acknowledged the intelligence they passed on did not include specific targets for an attack or a date. Jordanian officials told BuzzFeed News they had also sent

France a warning, less than a week ago, while Iraqi and Turkish officials have said that they passed on more specific intelligence to French authorities.

"It is fair to say that France was warned," said the Israeli diplomat, who spoke on condition of anonymity because he was not authorized to speak to the press. "But it is also safe to say France had been warned almost weekly for six months. That was what the chatter was telling us."

That chatter is the focus of intelligence agencies this week, as they try to figure out what they missed in the months leading up to ISIS's plan for a complex attack in Paris which left 129 people dead and over 350 wounded. **Western intelligence agencies say it is clear there was an intelligence failure, but what is less clear is how to monitor a group like ISIS, which has become increasingly savvy about its online communications**, encrypting messages and using a variety of platforms ranging from Tor — the browser helps mask location by bouncing it around a free, worldwide network — to the PlayStation gaming network, on which 110 million users regularly communicate, allowing militants to easily hide in plain sight.

Speaking from the G20 summit in Antalya, Turkey, President Obama said that the intelligence on hand before the Paris attacks was not specific enough to "allow for law enforcement or military actions to disrupt it."

"The concerns about potential ISIL attacks in the West have been there for over a year now. And they come through periodically. There were no specific mentions of this particular attack that would give us a sense of something that we need — that we could provide French authorities, for example, or act on ourselves," said Obama.

"ISIL, overall, has a very high level of awareness of operational security," said a U.S. intelligence official who spoke to BuzzFeed News from Jordan, using the acronym for ISIS preferred by the United States. He could not be quoted on the record as he was not authorized to speak to the press. "We've seen militant groups before where maybe the highest echelon are encrypting everything, and only using secure networks. ISIL, at least from mid-2014 onwards, when they declared themselves a caliphate, has used every tool at their disposal to mask communications from the bottom up," he said.

ISIS is hardly the first militant group to consider encryption technology: In papers captured during the U.S. raid on Osama bin Laden's compound a letter was found addressed to bin Laden from an individual identified as "brother Azmarai" which read, "We should be careful not to send big secrets by email. We should assume that the enemy can see these emails and [we should] only send through email information that can bring no harm if the enemy reads it. Computer science is not our science and we are not the ones who invented it."

Those tools range from the most basic — using encrypted messaging platforms such as WhatsApp and Kik — to the more advanced use of gaming platforms to share messages between ISIS leadership in Iraq and Syria and cells awaiting orders in the West. U.S., Israeli, and Jordanian officials who spoke to BuzzFeed News over the weekend said they were aware of the methods and admitted that even though they had the ability to spy on some of that technology, it was like "looking for a needle in a haystack."

The U.S. intelligence officer told BuzzFeed News that ISIS had shown a surprising flexibility to switch between platforms, recently adopting the privacy-centric Telegram app to set up challenges and deliver messages to over 10,000 followers. Telegram co-founder Pavel Durov recently told TechCrunch that the app is seeing 12 billion messages sent out daily via the platform. In his interview with Techcrunch, Durov seemed aware that his app had become popular among militant groups, including al-Qaeda and ISIS.

"I think that privacy, ultimately, and our right for privacy is more important than our fear of bad things happening like terrorism," Durov said, adding that if it wasn't his app, ISIS would find alternative platform for communicating. On Monday, Russian authorities considered a request to close access to the Telegram site.

Durov did not answer repeated requests from BuzzFeed News for comment.
One of those alternatives was highlighted on November 11, when Belgium's federal home affairs minister, Jan Jambon, said that a PlayStation 4 (PS4) console could be used by ISIS to communicate with their operatives abroad.
"PlayStation 4 is even more difficult to keep track of than WhatsApp," said Jambon, referencing to the secure messaging platform.
It remains unclear, however, how ISIS would have used PS4s, though options range from the relatively direct methods of sending messages to players or voice-chatting, to more elaborate methods cooked up by those who play games regularly. Players, for instance, can use their weapons during a game to send a spray of bullets onto a wall, spelling out whole sentences to each other.
In addition to using sophisticated methods to mask its communications, ISIS makes sure the message is often a code, pre-arranged and known only to the operatives involved.
"Today, intelligence agencies have the ability to intercept specific encrypted messages and decrypt them, given time and reason to do so," said the U.S. intelligence officer. "But if they do this, if they intercept the message and the message reads only one word, 'tomorrow' or even, 'the weather is good,' how does that help us? We might be warned that something is happening but we don't know where or when."
Even as intelligence agencies increase efforts to monitor the myriad platforms on which ISIS is communicating, ISIS can quickly shift and switch tactics. Jordanian and U.S. officials say the most critical intelligence they are lacking is the information gathered by human sources (HUMINT), rather than information gathered by intercepting signals (SIGINT) to monitor emails and phone calls.
"If you imagine the regular flow of SIGINT communication as an ocean where you are trying to find, and swim with, a certain school of fish, deciphering encrypted communication is like trying to find a specific fish in the ocean," said the Israeli diplomat, who has previously worked closely with his country's intelligence services. "It can be done, but you need to know exactly what you are looking for."

Alleged mastermind mocked Western security agencies after earlier terror plot, Globe and Mail

Tu Thanh Ha
17 November 2015
The Globe and Mail

No media-shy man, the alleged mastermind behind the Paris attacks gave an interview this year to a jihadi magazine in which he bragged about outwitting European law enforcement.

Abdelhamid Abaaoud also tipped his hat to those who had attacked Canada and other Western countries. "I ask Allah to accept the fruitful deeds of the shuhada [martyrs] who terrorized the crusaders of America, France, Canada, Australia, Germany and Belgium," he said at the end of the interview.

His remarks appeared in the February issue of Dabiq, the glossy propaganda magazine of the group calling itself the Islamic State (IS). That interview and a gruesome video in which he can be seen in IS-controlled Syria at the wheel of a pickup truck, smiling as his vehicle dragged a pile of bodies behind him, are now in the spotlight again.

As police in France and Belgium carried out a series of raids on Monday, attention turned to the connection of the suspects to IS, which has claimed responsibility for the attacks that killed at least 129 people in Paris on Friday.

According to French media, investigators believe that the 27year-old Mr. Abaaoud is a key figure in the plot, citing his ties to Salah Abdeslam, another Belgian national wanted by police as a suspect in the Nov. 13 attacks.

Both men have been in custody for their joint involvements in armed robberies in Belgium in 2010 and 2011, BFMTV and Le Monde reported.

Of the two, Mr. Abaaoud has the higher profile. He had already made the news for travelling to Syria to join the Islamic State, luring his teenaged brother to enlist and heading back to Belgium for a failed terror plot.

Mr. Abaaoud, one of six children of a Moroccan family, grew up in Molenbeek, the Brussels suburb that has a reputation as a nexus of Islamist activity and has been linked to four recent terrorist plots.

While a teen, he attended one of Brussels's fancier schools, the Catholic Collège Saint-Pierre, in the district of Uccle, the Belgian newspaper La Capitale reported, adding that he was remembered as “an intelligent boy who wasn't very motivated by his classes."

Mr. Abaaoud's father, Omar, runs a clothing store and has repudiated Abdelhamid, saying he has dishonoured his family by joining the Islamic State and getting involved in a terror plot against Belgium.

Abdelhamid Abaaoud appeared in a video obtained last year by two journalists working for Paris Match.

By Mr. Abaaoud's own account, a fellow jihadi had lost his camera, which “a murtadd" (apostate) later sold to journalists.

The gory video shows a cheerful Mr. Abaaoud driving a truck, towing behind him about half a dozen stiffened bodies. Wearing an Afghan pakol hat and with a GoPro camera strapped to his chest, Mr. Abaaoud jokes and tells the cameraman, “Before, we towed Jet Skis, quads, motorcycles, big trailers full of luggage and gifts for vacation. … Now we tow the apostates and the nonbelievers. You can film now, brother, film my new trailer."

Mr. Abaaoud was in the news again after a police raid last January in the Belgian city of Verviers near the German border, where officers killed two suspected terrorists.

In his interview with Dabiq, he said he and the two men who were killed had gone to Belgium “to terrorize the crusaders waging war against the Muslims."

Because of the video, “my picture [was] all over the media, but alhamdulillah [praise be to God], the kuffar [non-believers] were blinded by Allah," he said.

He said he was even stopped by an officer who failed to notice his resemblance to the face on the video.

Mr. Abaaoud said he was able to make his way back to IS-held territory after the shootout in Verviers.

“Allah blinded their vision and I was able to leave and come to Sham [the Levant] despite being chased after by so many intelligence agencies," he said.

In words that now carry more weight after the Paris attack, he ridiculed the efforts of European counterterrorism agencies.

“A Muslim should not fear the bloated image of the crusader intelligence," he said. “My name and picture were all over the news, yet I was able to stay in their homeland, plan operations against them and leave safely when doing so became necessary."

Column—Fake passports stoke concerns, National Post

Matthew Fisher
National Post
17 November 2015

'Everyone in the world is afraid of Syrians right now," says Mohammad Mohammed. "But that does not mean we are all terrorists."

The former clothing wholesaler, who fled his home in Edlib when extremist factions took over, was among those gathered outside Beirut's UN High Commission for Refugees Monday.

But like a million-plus other Syrians registered as refugees in Lebanon, he knows his chances could be worse since the Paris attacks last weekend.

One of the terrorists allegedly came to Europe as a Syrian refugee. Now, questions about screening procedures are being raised in many countries, including Canada, which is set to take 25,000 Syrian refugees in the next six weeks. Some groups are even calling for a cold stop to bringing Syrians across their borders.

The refugees on the street here say they understand the challenge facing anyone assessing who really is a refugee and who isn't, especially given that Lebanon and other countries in what is a notoriously tough neighbourhood are awash with dubious Syrian documents.

"Every one of us has heard about fake passports and ID cards," says Mohammed. "It is a business. Some Lebanese are buying them."

Khaled Ghazawi, who was pouring small cups of thick, sour coffee at $1 a shot, says he's seen what he believes are "fake" passports in the hands of people from seemingly everywhere - Morocco, Egypt.

The 45-year-old husband and father of six, a former grocery store manager from the brutally contested town of Daraa, says the worst are those he believes "help people get such papers."

If they are right, says Jihan Ismail, a Lebanese shop clerk, it compounds the challenge of figuring out "who is peaceful and who is a terrorist."

"It is not easy to identify terrorists," he says.

Omar Saifeddin, a fruit and vegetable salesman also from Edlib, raises his hand during the street-side discussion.

"You can see that not every finger is the same," he says. "It is like that with people, too. There are good Syrians and bad Syrians. The problem is that only God knows for sure who is good and bad."

Pouring more coffee for the growing crowd, Ghazawi says he understands the latest terror attacks claimed by ISIL "will, of course, have an effect on how foreign governments view us."

He believes the solution for countries willing to accept Syrian refugees is "really good clearances so you know who the people are that you are accepting. Remember there are many other ways for Daesh (the Arabic acronym for the terrorists) to reach where they want to go other than claiming to be refugees."

The men also insist taking in current Syrian refugees from Lebanon is a safe prospect: Lebanon ordered the UNHCR to stop registering Syrian refugees about a year ago, and "terrorists won't want to wait around for years to see if they can go somewhere," said one.

Mohammed adds he thinks the fear many countries have of refugees is misplaced.

"Canada's problem is not with Syrian refugees," he says. "There were French citizens involved in this too, so why aren't Canadians afraid of them? It is that Daesh is already in many centres overseas - they boast that they are in Canada, too, and I am sure that they are right."

Meanwhile, Radia Zammar, who had brought her fouryear-old granddaughter with her to the UNHCR compound, hadn't heard about the terror attacks in Beirut or Paris.

"I am anuneducated woman," she said. "I have only come here today to beg for help for my daughter who requires kidney dialysis. I am afraid that she is going to die. My son-in-law Ahmed Hajar disappeared last year in Syria and we believe he is dead.

" S " comme " sans résultats ", Sud Ouest

ANALYSE La plupart des terroristes qui sont passés à l'acte ces dernières années faisaient l'objet d'une fiche " S ".
Sud Ouest
Toutes éditions
mardi 17 novembre 2015, p. Périgueux-C1_6

DOMINIQUE RICHARD

Ce n'est pas une surprise : plusieurs des auteurs des attentats de Paris étaient connus des organes de renseignement, voire de la justice. Comme précédemment Mohamed Merah, Mehdi Nemmouche, Amedy Coulibaly ou Yassin Salhi, ces tueurs qui, de Toulouse au Musée juif de Bruxelles, de l'Hyper Cacher de Paris à Saint-Quentin-Fallavier, en Isère, ont semé la terreur.

Tous faisaient l'objet de la fameuse fiche " S ", la balise policière qui signale les individus susceptibles de menacer la sécurité de l'État. En France, la base de données relative aux personnes suspectées de radicalisation comporterait près de 10 000 noms.

Souvent critiqué, le système d'information européen Schengen a permis de l'étoffer du fait de la mutualisation des informations entre services. Bien que résident espagnol, le Marocain Ayoub el-Khazzani, l'agresseur du train Thalys, avait été signalé au printemps lorsqu'il avait pris de Berlin l'avion pour Istanbul.

Cible idéale

Cette fiche " S ", qui n'est pas systématiquement consultée lors des vérifications d'identité, n'a rien d'une botte secrète. En aucun cas, elle ne peut déboucher sur une arrestation ou une mesure coercitive. Pour ne pas éveiller l'attention, les forces de l'ordre sont d'ailleurs priées de rester discrètes lors des contrôles. Priorité est donnée au recueil d'informations sur les allées et venues des suspects potentiels.

En pratique, la collecte, même quand elle n'est pas freinée par des zizanies entre services, survient souvent avec un temps de retard. Au regard de l'importance de la population à surveiller, de son nomadisme et de l'afflux de candidats au djihad, les 3 500 agents de la Direction générale de la sécurité intérieure (DGSI) sont débordés.

" J'ai la conviction que les jours les plus sombres sont devant nous ", avertissait le 30 septembre dernier le juge antiterroriste Marc Trévidic au moment où, au terme des 10 ans autorisés, il était contraint de quitter ses fonctions (lire en page 5). Du fait de sa position géographique, des facilités d'entrée sur son territoire de djihadistes d'origine européenne, de sa politique étrangère, qui en fait l'allié du " grand Satan " américain, et de la fascination qu'exerce ce mouvement barbare sur une frange de la jeunesse issue de l'immigration, la France constitue presque la cible idéale.

Paradoxalement, elle n'a jamais été si désarmée, ses dispositifs policiers et judiciaires ne s'étant pas adaptés à la montée des périls. Ce que reconnaissent, entre les lignes, François Hollande et Manuels Valls en laissant entendre que le pire peut se reproduire à tout moment.

Les juges de côté

En décrétant l'état d'urgence sur tout le territoire et en invitant hier le Parlement à voter une loi qui prolongera ce dispositif de trois mois, du jamais-vu depuis la guerre d'Algérie, le gouvernement contourne la justice. Les préfets auront désormais la possibilité de " taper dans le fichier S " et d'ordonner des perquisitions et des assignations à résidence.

De quoi malmener l'État de droit. Mais peut-on critiquer cette mesure alors que, selon les mots mêmes du juge Trévidic, Daesh, le monstre que la France et les États occidentaux ont laissé se développer, peut à tout moment déclencher un 11 Septembre sur le territoire national ? Les premiers résultats des opérations engagées hier matin dans 19 départements ne sont pas anodins. Plus de 100 personnes présumées dangereuses sont désormais sous surveillance, des armes de guerre ont été saisies dans le Rhône, illustrant une fois de plus la connexion entre le banditisme et l'islamisme radical.

Espionnage légal

Imperceptiblement, la notion de " dangerosité supposée ", qui a émergé à l'époque du quinquennat de Nicolas Sarkozy, continue à se glisser dans les textes. L'emploi des outils d'espionnage survient désormais légalement avant toute saisine du juge. Les pouvoirs de la DGSI ont été considérablement renforcés lors du vote de la dernière loi sur le renseignement.

En annonçant hier des recrutements massifs aussi bien dans la justice que dans les services d'enquête, François Hollande s'est bien gardé de dire si la crise actuelle allait définitivement déplacer le curseur au détriment des juges, garants des libertés individuelles, mais aussi de l'efficacité des enquêtes.

Si le cas de Mohamed Merah, initialement signalé à sa hiérarchie par un policier toulousain, avait été transmis au parquet, sept personnes auraient peut-être eu la vie sauve.

Remarks for CIA Director John O. Brennan as Prepared for Delivery at the Center for Strategic & International Studies Global Security Forum 2015, CIA Press Office

November 16, 2015

Thank you very much, John, for those kind words and thank you for inviting me to speak this morning at CSIS's Global Security Forum. I had the pleasure of speaking at CSIS when I was at the White House serving as Assistant to the President for Homeland Security and Counterterrorism, and it is a privilege to come back to share some thoughts with you on some of the major global challenges our country faces today.

I also want to express publicly my deep appreciation to John Hamre, who has led CSIS for nearly 16 years and who is certainly one of the leading lights in the field of national security. After a distinguished government career, John has continued to make important contributions to our national security, and I think I speak for all of us in thanking him for adding such wisdom and value to the public conversation on global issues. [Applaud]

In many respects, CSIS shares the mission of our Intelligence Community: to help policymakers identify, understand, and—hopefully—successfully address the myriad national security issues that our Nation faces in a dynamic and very dangerous world.

A very dangerous world, indeed.

My opening remarks this morning are different from those I reviewed and finalized in the early afternoon of last Friday. They are different because our sensibilities and our souls have been jarred once again by the horrific and wanton violence perpetrated upon the innocent in the streets, cafes, and concert halls of the beautiful city of Paris. Our hearts ache for the scores killed and injured in those savage attacks, and our thoughts and prayers are with them and their families. Likewise, our condolences and our prayers go out to those killed in the crash of the Russian airliner a little over two weeks ago in the Sinai, Egypt.

And while we await confirmation of culpability for these tragedies, they each bear the hallmarks of terrorism carried out by the so-called Islamic State of Iraq and the Levant, or ISIL, an organization of murderous sociopaths that carries out its criminal and morally depraved actions under bogus religious pretense. With its roots in al-Qa'ida in Iraq, and empowered by a large influx of foreign adherents, ISIL over the past several years has swallowed up large swaths of

territory in Iraq and Syria, brutally killing thousands upon thousands of men, women, and children along the way. Not content to limiting its killing fields to Iraqi and Syrian lands and to setting up local franchises in other countries of the Middle East, South Asia, and Africa, ISIL has developed an external operations agenda that it is now implementing with lethal effect.

I am sure that we will talk more about ISIL in the question and answer session, but let me note that the grave threat posed by the phenomenon of ISIL makes it absolutely imperative that the international community urgently commit to achieving an even greater and unprecedented level of cooperation, collaboration, information sharing, and joint action—in intelligence, law enforcement, military, and diplomatic channels. The ISIL threat demands it.

At CIA, we work closely with foreign intelligence security services around the globe to advance our shared counterterrorism goals. Over the course of many years, we have forged broad and deep partnerships with our closest allies in Europe such as Great Britain, France, and many, many others. These strategic relationships have been instrumental in helping to knit together a transnational architecture that allows counterterrorism officials and experts to work closely together across sovereign borders to disrupt terrorist plans and activities. And while many terrorist operations have been thwarted as a result of strong transnational teamwork, tragically, not all terrorist plans are uncovered in time.

These strategic counterterrorism relationships need to stretch far beyond the traditional trans-Atlantic environment and alliances, which is why we are working closely with so many services in different parts of the world.

For instance, we are working very closely with our Egyptian partners, who are working tirelessly to prevent ISIL terrorists from launching attacks that are aimed at derailing Egypt's political reform initiatives and economic development objectives. I reiterated our commitment to strengthening our counterterrorism partnership with Cairo in a call to my Egyptian counterpart this past weekend.

And while Washington and Moscow have significant policy differences on how best to bring the bloodshed in Syria to a close, I have had several conversations with one of my Russian counterparts over the past several weeks about ways to strengthen U.S.-Russian counterterrorism cooperation, specifically on the ISIL threat.

These relationships are an essential adjunct to diplomacy and military operations. By working with our foreign partners, we enhance global security by helping them tackle challenges that threaten us all. And we benefit from a wider net of collection and from the insights of local services, all of which enhance the intelligence we provide to policymakers.

The fact is, good intelligence—timely, accurate, and insightful—is the cornerstone of almost every aspect of national security policy today, from military action to diplomacy to international law enforcement.

With good intelligence, our policymakers can better understand the risks, challenges, and opportunities attendant to key national security issues, which is ever-more important given the unprecedentedly complex and overlapping array of major challenges to US and global security that we face today.

The impression one might get from the daily headlines is that the world has become more unstable. And indeed, the historical record supports that judgment.

In the past three years, there have been more outbreaks of instability than at any time since the collapse of the Soviet Union, matching the rate we saw during decolonization in the 1960s. This has not just been a period of protests and government change, but of violent insurgency and, in particular, of breakdowns in many states' ability to govern.

Ongoing conflicts in Syria, Iraq, Ukraine, Yemen, Libya, and parts of Africa are clear examples. The human toll is reflected in the UN's recent announcement that the number of refugees and internally displaced persons in the world is the highest it has been since World War II. And of course, all this localized strife gives rise to the persistent threat of international terrorism.

When CIA analysts look for deeper causes of this rising instability, they find nationalistic, sectarian, and technological factors that are eroding the structure of the international system. They also see socioeconomic trends, the impact of climate change, and other elements that are cause for concern. Let me touch upon a couple of them.

First, the ideas, institutions, and states that have undergirded the post-Cold War system are under significant stress. It is easy to think of this as a phenomenon confined to the developing world, and that is certainly where we see states that have actually failed, and borders that no longer carry any practical effect, such as the border between Syria and Iraq. But there is considerable stress on governments in even the world's most stable regions.

In Europe, for instance, the migration crisis, sluggish economic growth, and a host of other factors have given rise to heightened nationalism, secession movements, and the increasing popularity of political parties on both the far-right and far-left. Even ideas that were the pillars of the Continent's postwar prosperity—such as economic integration and democracy itself—are being questioned in some quarters.

Across the globe, in both authoritarian and democratic societies, governments are finding it increasingly difficult to meet the demands—realistic or not—of their skeptical and restive populaces. The so-called Arab Spring revolutions were not fought for democracy per se as much as they were fought for relief from regimes that had failed to meet basic standards of governance and civil society.

And as we have seen, when people become disillusioned with the powers that be, social media enable them to more quickly and easily form associations that defy the status quo. And in part, that is why the global landscape has been changing at a faster, more disruptive pace.

How nations respond to these challenges, adapt to them, and evolve will be one of the great plot lines of this century.

When I meet with my foreign counterparts—from both friendly and not-so-friendly governments—I sense a very real apprehension about instability and its various manifestations: terrorism, humanitarian crises, proliferation, and so on. Interestingly, I hear these concerns even from officials representing governments whose policies are quite arguably contributing to the problem.

In Europe, anxiety has risen in states along Russia's periphery after Moscow demonstrated its willingness to use military and paramilitary forces in Ukraine. And in the South China Sea, tensions persist as China unilaterally pursues its territorial claims, including actions that rival claimants perceive as violating their sovereignty.

At the same time, the principle of democratic governance is under siege. For the ninth consecutive year, Freedom House in 2014 reported more declines than gains in the quality of democracy worldwide. Worsening ethno-sectarian and socioeconomic strains are eroding democracy, as is the rise of a more sophisticated form of authoritarianism that forgoes brute force and heavy-handed propaganda in favor of media manipulation, ubiquitous surveillance, criminalization of dissent, and controlled elections.

Second, the resumption of strong, sustained growth in the wake of the 2008 financial crash and Eurozone crisis has been elusive for some of the world's largest economies. Even China's economy, with its seemingly endless potential for growth, is slowing.

In many developing societies, growing pessimism about the prospects for economic advancement is fueling instability. Regions with burgeoning youth populations, such as the Arab world, have been unable to achieve the growth needed to reduce high unemployment rates. Perceptions of growing inequality have resulted in more assertive street politics and populism. At the same time, slower growth has left these nations with fewer resources to devote to economic, humanitarian, and peacekeeping assistance to address these challenges.

Mankind's relationship with the natural world is aggravating these problems and is a potential source of crisis itself. Last year was the warmest on record, and this year is on track to be even warmer.

Extreme weather, along with public policies affecting food and water supplies, can worsen or create humanitarian crises. Of most immediate concern, sharply reduced crop yields in multiple places simultaneously could trigger a shock in food prices with devastating effect, especially in already fragile regions such as Africa, the Middle East, and South Asia. Compromised access to food and water greatly increases the prospect for famine and deadly epidemics.

And finally, the rapid advance of information technology has given rise to an entirely new and wide-open domain for human interaction and progress: the cyber realm.

As an intelligence officer, much of my job involves dealing with the unintended consequences of the cyber revolution. For as much as it brings the world together, it also serves the purposes of those who wish us harm.

Of greatest concern, the cyber realm gives small groups and even individuals the potential to inflict damage on a scale previously restricted to nation-states. And while states are largely rational actors subject to deterrence, the same does not apply to terrorists and criminals.

Both government and private networks are under constant attack. The Department of Homeland Security reports that more than 640,000 cyber-related incidents affected federal agencies in fiscal year 2014. The massive and prolonged hacking of employee records held by the Office of Personnel Management underscores the intensity of assaults on government IT systems. And I am all too familiar with the ease with which miscreant hackers can use social engineering techniques to perpetrate criminal intrusions into personal email accounts and information technology and communication systems.

Unfortunately, there is every reason to expect cyber intrusions to increase in quantity, cunning, and impact. For one thing, the economics of cyber attacks are skewed to favor the attacker.

"Exploits," or malicious software tools, are easily acquired. In fact, their prices are falling dramatically in some criminal markets, not because of declining demand but because of an increasingly competitive marketplace. These exploits can be reused on multiple targets, and the likelihood of detection and punishment remains low.

And while the vast majority of cyber attacks target money, proprietary information, and privacy itself, we need to realize that the range of potential targets is much greater. We simply cannot discount the very real possibility of attacks against vital infrastructure—utilities, transportation, and other essential underpinnings of modern civilization.

The world has changed dramatically since I first raised my hand and swore an oath of allegiance to the United States Government as a 24-year old newly minted CIA officer eager to make a difference in August of 1980. I remember vividly taking a seat at my first desk on the sixth floor of our Langley Headquarters, putting my fingers not on the keyboard of a computer but on the keys of an electric typewriter, which was quite high tech at the time.

Thirty-five years later, our lives as well as our fingers are inextricably linked to the cyber realm—the new digital frontier, where most human interactions, transactions, and communications take place. And while that digital environment holds tremendous potential and opportunity for the further advancement of humanity, our increasing dependence on it brings obvious risks and challenges.

To deal with those risks and challenges, reactive strategies are insufficient. There has to be systematic learning, informed by constant information sharing, so that one organization's detection becomes another's prevention.

In other words, countering cyber threats is very much a team effort. And a crucial point to bear in mind is that about 85 percent of the Worldwide Web's critical infrastructure is held by the private sector. This is a privately owned and operated environment in which the rules remain uncertain at best.

A number of federal efforts in recent years have promoted the sharing of cyber threat information between the private sector and government. DHS and FBI, for example, have programs to share cyber threat information with a broad community of industry stakeholders.

We should be sharing a lot more information than we are as a nation, but programmatic, technical, and legal challenges—as well as concerns about privacy and the role of government—have hampered progress. Congress over the past few years has tried, so far without success, to pass laws addressing the need for comprehensive cyber policy, especially on information sharing.

The fact is, 20th century laws cannot effectively deal with 21st century threats.

Within the past few weeks, the Senate passed the Cybersecurity Information Sharing Act, or CISA, which is roughly similar to two bills passed in the House. We may see a conferenced bill by early next year, which would be an important step forward.

And as our country deals with this issue—and, specifically, the security and privacy concerns that revolve around information sharing—it is important to note that security and privacy are not mutually exclusive. The benefits of improved information sharing can be achieved in a manner that protects privacy and civil liberties.

My hope is that America—ideally, along with our allies—can eventually adopt a comprehensive legal and operational approach to this threat without being forced to by a catastrophic cyber attack, in the same way that 9/11 forced our country to integrate its national security assets in a more rational and effective way against terrorism.

Shortly after I returned to the Agency some two-and-a-half years ago, I started to consider what we could do to ensure that CIA is well-prepared for both the opportunities and challenges of the future. The digital world stood out as an area that required special attention.

When I asked a group of our senior officers last fall to ponder the Agency's future and come back with a strategic plan, they agreed that we had to do a much better job of embracing and leveraging the digital revolution. Consequently, one of the pillars of the modernization program we launched last March was the addition of a fifth Directorate as part of the biggest change to CIA's structure in five decades: the Directorate of Digital Innovation.

This new Directorate is at the center of the Agency's effort to hasten the adoption of digital solutions into every aspect of our work. It is responsible for accelerating the integration of our digital and cyber capabilities across all our mission areas—espionage, all-source analysis, open source intelligence, and covert action.

Multiple elements of the Agency in the past have responded to the challenges of the digital era. But if we are to excel in the wired world, we must place our activities and operations in the digital domain at the very center of all our endeavors.

Our new digital directorate was launched last month, and we expect it to contribute enormously to every facet of our global mission. Alongside our partners across the Intelligence Community, we at CIA will be more capable and effective in safeguarding our country from the full range of threats we face beyond our borders.

Let me conclude by saying what I always say to each new class of Agency officers to whom I administer the oath of office every month in our Headquarters lobby. I have the absolutely best job in the world, because I work each day with some of the most dedicated, talented, courageous, and patriotic individuals this country has to offer. And, in light of the nature and scope of the national security challenges I just highlighted, the need for the contributions of these individuals has never been greater.

Thank you, and I'll be happy to take your questions.

Attaques terroristes à Paris/ Paris Terrorist Attacks

(A Communications Branch product/un produit de la Direction des communications)

Saturday, November 21 2015
le samedi 21 novembre 2015
09:00 / 9 h00

Highlights/Faits saillants

- The fact that most of **the Paris attackers identified so far were European-born radicals has once again shined the spotlight on the growing problem in the West of homegrown extremism.** There is no reliable profile for many of the candidates being recruited by extremist Islamic groups, **Phil Gurski, a former intelligence analyst with CSIS,** told *CBC News*. "Throughout **my career at CSIS** and looking at a lot of these things, we simply found that there were no useful elements in terms of profiles, whether it was age or ethnicity or employment status or education or psychological or criminal background," Gurski said.
- Une **fiche de synthèse des services de renseignements belges** concernant le parcours **d'Abdelhamid Abaaoud**, que *Le Monde* a pu consulter,reprend point par point, de façon chronologique, jusqu'en février 2015, **l'itinéraire connu du djihadiste**
- An **elite unit of anti-terrorism "hacktivists"** is helping the **British security services** with intelligence operations against Isis, The *UK Times* has learnt. Since the **Paris attacks**, members have infiltrated online Isis accounts run by individuals who had prior knowledge of the shootings.
- In a *Globe and Mail* report, **General Petr Pavel, chairman of the North Atlantic Treaty Organization's military committee** says the **Paris attacks are a "game changer" for security** in the West as the ascendant Islamic State moves beyond its selfproclaimed caliphate in Iraq and Syria to wage al-Qaeda-style attacks on distant targets.
- *France 24* souligne que **François Hollande a vivement remercié le roi Mohamed VI** en visite à Paris, vendredi 20 novembre, **pour le rôle crucial des services de renseignement marocains** dans l'enquête sur les attaques à Paris.
- **French officials are particularly frustrated with their European Union partners over what they see as insufficient cooperation in intelligence**, security and defense, the *Wall Street Journal* reports. "Everyone must understand that it's urgent for Europe to recover, to organize itself, and to defend itself against the terrorist menace," French Interior **Minister Bernard Cazeneuve** said this week.

Service Mentions/Mentions du Service

Paris attacks show how hard it is to profile ISIS recruits, CBC News

Sheena Goodyear
CBC News
2015 11 21

The fact that most of the Paris attackers identified so far were European-born radicals has once again shined the spotlight on the growing problem in the West of homegrown extremism.

Authorities have identified four Frenchmen and two Belgians as suspects in the shootings and suicide bombings that killed 129 people on Friday. That puts them among ISIS's legion of foreign fighters, which some have estimated to be as many as 200,000.

A seventh suspect's body was found near a Syrian passport, but its authenticity has come under scrutiny after Serbian police arrested a man with an almost identical copy, the Guardian newspaper reported.

The European backgrounds of the perpetrators puts France and the West in the difficult position of trying to understand why their own citizens would sacrifice their lives to murder their neighbours on behalf of an extremist organization in another part of the world ? a question radicalization analysts say is almost impossible to answer.

There is no reliable profile for many of the candidates being recruited by extremist Islamic groups, Phil Gurski, a former intelligence analyst with the Canadian Security Intelligence Service, told CBC News.

"Throughout my career at CSIS and looking at a lot of these things, we simply found that there were no useful elements in terms of profiles, whether it was age or ethnicity or employment status or education or psychological or criminal background," Gurski said.

Abdelhamid Abaaoud, the suspected mastermind of the Paris attacks, killed in a police assault, was a lifelong Muslim and the child of Moroccan immigrants.

By contrast, Damian Clairmont, the Calgary man who died fighting with ISIS in Syria last year, was a white Muslim convert with an Acadian ancestry.

Even gender is not a guaranteed common factor, as there have been multiple reports of Canadian women joining ISIS.

"We've had people ? poor, rich, married, unmarried, mental illness, converts, not-converts ? and so there's nothing really there in terms of profile," says Amarnath Amarasingam, a post-doctoral fellow who researches terrorism and radicalization at Halifax's Dalhousie University.

"What all of them do tend to have in common … is youth, [with a] thrust towards meaning and purpose and significance. A lot of these youth don't feel like they fit into the broader society, they don't feel like they belong."

Giving ISIS what they want

The fact that ISIS preys on those who feel isolated and excluded should be a wake-up call for Western nations to build more inclusive societies, says Rima Berns-McGown, a University of Toronto history professor who researches how government policy affects youth radicalization.

She's concerned that certain state responses to the Paris attacks, like closing doors to Syrian refugees, play into ISIS's hands.

"The reason ISIS does these things, launches these attacks and so on, is because it actually wants to create an environment in which the West appears to be hostile to people who are not of the West. It wants to create a sort of civilizational war," she said.

"It wants to create anger and resentment. It wants to create Islamophobia. It wants to create racism. Because if it does that, it makes the lives of individual Muslims more uncomfortable, and it wants to say, 'You cannot be at home in the West. You need to come and be at home in the only place that will respect you.'"

'Utopian' vision

For his part, Amarasingam said ISIS is unique among Islamic extremists organizations in selling this "utopian" vision of a caliphate, or Islamic state, where people can find a sense of belonging.

"It's a state where they believe that Islamic law is being practiced in its purest and fullest form, and therefore all Muslims around the world have an obligation to make migration to that state," he said.

"The fact that the vast majority of Muslims around the world disagree that this is the authentic Islamic state doesn't seem to bother them too much." But many of the youth it is able to recruit "are drawn to that nation-building, utopian vision that they're portraying themselves to be."

The warning signs

When people start to buy into this propaganda, they exhibit certain behaviours.

In his book The Threat From Within: Recognizing al-Qaeda-Inspired Radicalization and Terrorism in the West, he outlines 12 indicators of radicalization, including:

- Expressing vocal opposition to Western values.

- Spending lengthy amounts of time on violent jihadist websites.

- Exhibiting hatred towards non-Muslims, moderate Muslims or Shia Muslims.

- Isolating themselves from people who disagree with them.

He cautions that while all homegrown radicals exhibit some or all of these behaviours, not everyone who shows these warning signs crosses the line into violence and criminality.

People with friends or family members who fit this profile shouldn't necessarily make accusations or call 911, he said. Instead, just talk to them and find out what's going on.

"These are warning signs. In the same way that if you think someone is engaged in gang activity or illegal substances or whatever, you don't just kind of sit back and say 'Oh that's interesting.' You take action."

Liberals' refugee plan still unsettled, Globe and Mail

By DANIEL LEBLANC, STEVEN CHASE
21 November 2015
The Globe and Mail

Debate continues over whether to conduct screening on foreign soil to avoid later legal hurdles, which could have effect on timeline

The Liberals are still debating whether to extend the Dec. 31 deadline to bring 25,000 Syrian refugees to Canada in order to allow all health and security screening to be conducted on foreign soil, sources said.

The greatest concern at this point is that if some refugees land in the country as unscreened temporary residents, the government would face a series of legal hurdles before it could expel any of them for failing required tests, the sources said.

The Trudeau government is in the final stages of preparing its resettlement plan, which, in the recent election campaign, the Liberals promised to conclude by the end of the year. The final details will be unveiled on Tuesday, after a meeting of Prime Minister Justin Trudeau's full cabinet.

A key issue still under debate is whether to allow some of the refugees to land in Canada as temporary residents and undergo further screening here, or to conduct all screening abroad and welcome all of the asylum seekers in the country as permanent residents, sources said.

The first option would accelerate the process; the second one could push back the arrival of a portion of the refugees into January, a source said.

Given the ongoing conflict in Syria, the government wants to avoid a situation in which it would have “stateless citizens" on its soil. In that context, some federal officials are pushing for the government to do the entire screening abroad, in countries such as Lebanon and Jordan.

“You don't want people who are in the country who are legally ambiguous and you have nowhere to send them," a federal official said, adding that the internal debate “could change the timeline" for the arrival of the refugees.

Immigration lawyer Gordon Maynard said the issue for the government is that providing temporary residency status to refugees would speed up the process, but it would be hard to subsequently send them back to their “country of nationality."

Concerns about the security risks posed by Syrian refugees began spreading among provincial and municipal governments after last Friday's terror attacks in Paris. **The Trudeau government is striving to convince Canadians that the refugees are a minimal risk, insisting that the RCMP and CSIS have endorsed the proposed screening as robust and strong.**

Asked about polls suggesting Canadians are sharply divided on bringing in so many Syrian refugees so quickly, Canada's new Defence Minister, Harjit Sajjan, offered a passionate rejoinder.

Mr. Sajjan said welcoming 25,000 Syrians in a matter of weeks is not just “a humanitarian project" but also a rebuke of the Islamic State, which seeks to convince Syrian Muslims and others that the West is their enemy.

“This sends a great message to ISIS," he said, using one of the acronyms for the Islamic State, “that you might have created this environment for us but we will not let you take advantage of this."

Sources said there are still a “number of moving parts" as federal officials work with other levels of government to finalize plans to welcome and house the refugees across the country – as many as half at military bases – and help them integrate into Canadian society.

Speaking at the Canada202 conference in Ottawa, Ontario Premier Kathleen Wynne said she is convinced that adequate security measures are in place.

"What we can't give into is allowing security to mask racism," she said. "That's the danger."

Canada

Paris attacks a 'game changer' for NATO, general says, Globe and Mail

By STEVEN CHASE
21 November 2015
The Globe and Mail

One of NATO's senior officials says the Nov. 13 Paris attacks are a "game changer" for security in the West as the ascendant Islamic State moves beyond its selfproclaimed caliphate in Iraq and Syria to wage al-Qaeda-style attacks on distant targets.

General Petr Pavel, chairman of the North Atlantic Treaty Organization's military committee, said all Western countries are at risk of not just IS-inspired attacks but also terrorism planned and executed directly by the Islamic State, also known as ISIL and ISIS.

"Anyone who is not following the values of ISIL should be afraid."

Recent examples include IS-organized attacks in Beirut, Turkey and Paris, where 130 people were killed and hundreds wounded by gunmen and bombers, as well as the downing of a Russian aircraft carrying 224 people over the Sinai Peninsula in October.

"It is apparent that the Islamic State has reached the limits of geographical expansion and now they are even losing some, so they [will] probably expand into our domain and one of them may be even hitting us on our own ground," Gen. Pavel said in an interview.

"We are most probably at the beginning of a new phase of ISIL activities that will affect us in our own countries and we will have to take appropriate measures," said the general, who was attending the Halifax International Security Forum, an annual gathering of security and defence experts sponsored by the Canadian government.

Gen. Pavel argued that what happened in Paris does not constitute grounds for France to invoke Article 5 of the NATO treaty, which would oblige collective action by all members of the military alliance. The United States invoked this article for the first time in NATO's history after the Sept. 11, 2001, terrorist attacks, but France has not chosen to follow suit.

"It is difficult to imagine a terrorist attack in France as a military aggression against France," the general said. "It's not a military attack."

However, he said NATO needs to share intelligence better and continue to support local forces in Iraq and Syria to fight the Islamic State.

French President François Hollande has called for a grand military coalition of the United States, France and Russia to "eradicate" the Islamic State.

This would force Washington and Moscow to set aside their estrangement over Russia's 2014 annexation of Ukraine's Crimean Peninsula and its ongoing backing for rebels fighting Kiev in eastern Ukraine.

Gen. Pavel said that while the West may have to “pragmatically co-ordinate" with Moscow to fight the Islamic State, he warned against losing focus on Russia's ongoing occupation of Crimea and the fragile ceasefire in eastern Ukraine.

“That would be a mistake on our side," he said, warning that this would play into Moscow's hands. “That would be exactly … one of the objectives of President Putin – to take attention out of Ukraine and move it elsewhere [and] now in this case to Syria."

“We shouldn't let Ukraine disappear from the radar and stay focused on the fact there were breaches to the international security system made by Russia that are not forgiven and not forgotten."

He said there have been increasing breaches of the Minsk ceasefire between Kiev's soldiers and the Russian-backed rebels in recent days and heavy weaponry has not been removed from the immediate region, as required.

Canada has nearly 70 special forces soldiers in Iraq advising Kurdish fighters in their battle against the Islamic State and CF-18 warplanes are currently bombing IS targets in Iraq and Syria. The new Liberal government is planning to withdraw the jets and expand training efforts in Iraq, possibly including government forces.

About 200 Canadian troops are currently deployed to Ukraine to train Kiev's forces to better fight the Russian-backed rebels.

Other/Autres

Le niveau d'alerte passe à 4, Agence Belga

Agence Belga
2015 11 21
"Un risque d'attentat par des individus avec armes et explosifs à plusieurs endroits de la capitale"

Le niveau d'alerte terroriste a été relevé samedi à 4, soit le niveau le plus élevé qui qualifie la menace de "sérieuse et imminente", pour toute la Région bruxelloise, indique le Centre de crise du SPF Intérieur à la suite d'une nouvelle évaluation de l'OCAM.

Selon le Premier ministre, Charles Michel, ce rélèvement du niveau d'alerte serait lié à un risque d'attentat par des individus avec armes et explosifs, peut-être à plusieurs endroits de la capitale.

Quatre axes de mesures

Le Premier ministre Charles Michel a annoncé l'entrée en vigueur de mesures immédiatement opérationnelles en quatre axes pour répondre au niveau maximal de menace terroriste à Bruxelles et au niveau trois dans le reste du pays, à l'issue d'une réunion du Conseil national de sécurité samedi matin. Le nombre de grands évènements sera diminué, "pour des raisons de sécurité et de capacité", a indiqué le Premier ministre, "car cela permet de libérer des capacités qui peuvent être mobilisées pour sécuriser tout le territoire". Les organisateurs d'évènements peuvent se mettre en contact avec le centre crise pour recevoir des informations complémentaires.

Les transports publics feront l'objet d'une vigilance accrue, principalement dans le métro. La circulation de ce dernier à Bruxelles reste stoppée jusque dimanche après-midi au moins. La capacité de déploiement de la police et de l'armée est renforcée sur tout le territoire, mais surtout à Bruxelles.

Enfin, une ligne téléphonique - 1771 - est ouverte pour permettre de s'adresser au centre de crise, recevoir des informations et des conseils. Pour ne pas surcharger cette ligne, il est recommandé de consulter en priorité le site internet www.centredecrise.be.

Le relèvement du niveau d'alerte terroriste au niveau quatre a été décidé durant la nuit sur base de l'évaluation de l'Organe de coordination pour l'analyse de la menace (OCAM), pour la région bruxelloise et Vilvorde, mais reste au niveau trois pour le reste du pays. "Cela résulte d'informations relativement précises d'un risque d'attentat tel que déroulé à Paris" a déclaré le Premier ministre, la menace portant sur une hypothèse d'un ou plusieurs individus avec des armes et explosifs à même de frapper à plusieurs endroits en même temps, a-t-il précisé lors d'une conférence de presse.

Les cibles potentielles, selon les informations dont les autorités disposent, sont les centres commerciaux, les rues commerçantes, les transports publics, et les évènements rassemblant beaucoup de monde, a indiqué Charles Michel.

Les mesures annoncées peuvent "à tout moment être modifiées", a précisé le Premier ministre. Le Conseil national de sécurité se réunira à nouveau dimanche dans l'après-midi. Une nouvelle évaluation de la menace par l'OCAM sera formulée à ce moment-là également.

Le Premier ministre a indiqué que les enquêtes en France et en Belgique sur les attentats de Paris se poursuivaient et qu'il n'était "pas question de faire le moindre commentaire pour des raisons de sécurité évidente". "Nous recommandons à la population de respecter l'ensemble des consignes de sécurité et de se tenir informée en utilisant les voies de communication officielles", a déclaré le Premier ministre.

Le gouvernement belge appelle la population à faire preuve de prudence et de vigilance, mais aussi de ne pas glisser dans la panique, a insisté Charles Michel.

"La situation est suivie de manière permanente"

Le Centre de crise n'était pas en mesure de préciser combien de temps le niveau 4 restera en application dans la Région bruxelloise. "La situation est suivie de manière permanente. Elle peut dès lors être réévaluée à tout moment si de nouveaux éléments nous parvenaient", a expliqué Peter Mertens, porte-parole du Centre de crise.

Lundi en fin de soirée, le Centre de crise avait annoncé le relèvement du niveau d'alerte terroriste à 3 pour l'ensemble du territoire. Il avait alors rappelé que Salah Abdeslam, suspecté d'avoir participé à l'organisation et à l'exécution des attentats perpétrés à Paris le 13 novembre, était toujours recherché. Celui-ci est encore en fuite actuellement. Le gouvernement communiquera au sujet du relèvement de la menace samedi matin.

Pour déterminer un niveau, l'Ocam se base sur les informations transmises notamment par la Sûreté de l'Etat, le Service général du renseignement et de la sécurité (SGRS), les polices locales et fédérale, les douanes et l'Office des étrangers. Placé sous l'autorité des ministres de la Justice et de l'Intérieur, cet organe est composé d'experts détachés des services dont il utilise les informations et d'analystes propres. Il est chargé d'évaluer périodiquement et ponctuellement le degré de menace terroriste en Belgique.

La deuxième fois de l'histoire du pays

C'est seulement la deuxième fois que le niveau d'alerte terroriste atteint l'échellon le plus elevé sur le territoire belge. La première fois était survenue lors des fêtes de fin d'année 2007-2008 après l'interpellation de 14 personnes qui planifiaient de permettre à Nizar Trabelsi de s'évader.

La section terrorisme de la police fédérale et le parquet fédéral craignaient alors des actes à caractère terroriste et avaient pris des mesures de sécurité exceptionnelles. Le niveau de la menace avait été à maintenu à 4 entre le 21 décembre 2007 et le 3 janvier 2008. Le traditionnel feu d'artifice du Nouvel an dans le centre de Bruxelles avait été annulé à la suite cette situation.

Nizar Trabelsi avait été condamné en juin 2004 à 10 ans de prison pour la préparation d'un attentat contre la base militaire de Kleine-Brogel.

Le Conseil national de sécurité se réunit samedi matin après que le niveau d'alerte a été relevé à quatre, soit le maximum, pour Bruxelles durant la nuit. "Nous avons suffisament d'éléments pour estimer que la menace est précise et imminente", a affirmé à son arrivée le ministre des Affaires étrangères Didier Reynders. Le Premier ministre Charles Michel, avec les vice-premiers ministres chargés de de l'Intérieur, Jan Jambon, des Affaires étrangères, Didier Reynders, de la Justice, Koen Geens, et de l'Economie, Kris Peeters, sont arrivés au 16 rue de la loi à Bruxelles vers 9h00, pour se concerter avec les autorité chargées de la sécurité. "La menace est suffisante pour passer au niveau d'alerte quatre, nous devons maintenant prendre des mesures", a déclaré à son arrivée le ministre de l'Intérieur, Jan Jambon.

Le niveau 3 maintenu ailleurs

Le niveau 3, soit une menace "possible et vraisemblable", reste en vigueur pour le reste du pays. L'analyse de l'Organe de coordination pour l'analyse de la menace (OCAM) démontre en effet "une menace sérieuse et imminente nécessitant la prise de mesures de sécurité spécifiques ainsi que des recommandations particulières à la population", précise le Centre de crise, qui qualifie la situation de "très grave" dans la Région bruxelloise.

Belgian capital under serious terrorism threat, with at least 1 Paris attacks suspect at large, Associated Press

Nov 21, 2015 7:36
THE ASSOCIATED PRESS

BRUSSELS _ **Heavily armed police and soldiers patrolled key intersections and subways were closed in Belgium's capital Saturday as the government warned of a threat of Paris-style attacks. At least one suspect from the deadly Paris attacks is at large, and was last seen crossing into Belgium.**

Prime Minister Charles Michel said the decision to raise the threat alert to the highest level was taken ``based on quite precise information about the risk of an attack like the one that happened in Paris ... where several individuals with arms and explosives launch actions, perhaps even in several places at the same time."

The Belgian Federal Prosecutor's office said Saturday that several weapons were discovered during the search of the home of one of three people arrested in connection with the Paris attacks, but said no explosives were found.

And in Turkey, officials detained 26-year-old Ahmad Dahmani, a Belgian national of Moroccan origin, who was believed to have been in contact with the Paris attackers.

Authorities across Europe, the Mideast and in Washington are trying to determine how a network of primarily French and Belgian attackers with links to Islamic extremists in Syria plotted and carried out the deadliest violence in France in decades _ and how many may still be on the run.

A new potential link emerged Saturday in Turkey, where authorities said they detained a 26-year-old Belgian suspected of connections to Islamic extremists _ and possibly to the Paris attacks.

Belgium's national Crisis Center had raised its terrorism alert for the Brussels region to Level 4, which indicates a ``serious and immediate threat.'' Belgium's special security Cabinet held an emergency meeting Saturday morning.

Brussels was the home of Abdelhamid Abaaoud, the suspected organizer of the Nov. 13 Paris attacks, and Belgium has filed charges of ``participation in terrorist attacks and participation in the activities of a terrorist organization'' against three suspects relating to the Paris attacks.

At least one Paris attacker, Salah Abdeslam, crossed into Belgium the morning after the attacks. A Paris police official and the Paris prosecutor's office said Saturday they had no firm information on Abdeslam's whereabouts, including whether he was in the Brussels area.

Heavily armed police and soldiers were patrolled Saturday morning at key intersections of the Belgian capital, a city of more than 1 million that is home to the headquarters of the European Union, the NATO alliance and offices of many multinational corporations.

Residents were recommended to avoid gatherings, train stations, airports and commercial districts. Service was halted on the Brussels Metro, as well as on streetcar lines that run underground.

The prime minister, speaking at a news conference after the emergency government meeting, said, ``We urge the public not to give in to panic, to stay calm. We have taken the measures that are necessary.''

He said that the government's crisis cell will meet again on Sunday afternoon to reassess the threat.

Dahmani was detained in the Turkish coastal city of Antalya along with two other suspected Islamic State militants. A senior Turkish government official said Dahmani was believed to have been in contact with the Paris attackers, though the official did not say when. Dahmani had arrived in Turkey Nov. 14 from Amsterdam, and the three were preparing to cross into Syria, the official said.

The official cannot be named because of Turkish government rules that bar officials from speaking to reporters without prior authorization.

Government officials in Belgium and France would not immediately comment on Dahmani's arrest.

A Paris police official said Saturday that he had no information about Dahmani or his possible visit to the attack sites. The Paris prosecutor's office said it had no information to communicate about Dahmani.

Concerns about Europe's porous borders prompted interior and justice ministers meeting in Brussels on Friday to promise tightened controls to make it easier to track the movements of jihadis with European passports travelling to and from warzones in Syria.

Paris prosecutors said Friday that they had determined through fingerprint checks that two of the seven attackers who died in the bloodshed Nov. 13 had entered Europe through Greece, an entry point for many of the hundreds of thousands of migrants seeking asylum in Europe.

The five other attackers who died had links to France and Belgium. One of the seven dead has not been identified, while a manhunt is underway for one suspect who escaped, 26-year-old Abdeslam. French police stopped Abdeslam the morning after Friday's attacks at the Belgian border but then let him go. His brother Brahim blew himself up in the Paris attacks.

The suspected ringleader, Abdelhamid Abaaoud, was killed in a raid Wednesday on an apartment in the Paris suburb of Saint-Denis.

Marking a week since the carnage, some Parisians lit candles and paid tribute Friday night to the victims with silent reflection. Others decided that enjoying themselves was the best way to defy the extremists. They sang and danced on Place de la Republique, in the heart of a trendy neighbourhood where scores of people were killed.

France's Parliament has extended a state of emergency for three months, expanding police powers to carry out arrests and searches and allowing authorities to forbid the movement of persons and vehicles at specific times and places.

French President Francois Hollande is also meeting with British Prime Minister David Cameron on Monday morning in Paris to discuss co-operation in the fight against the Islamic State group

in Syria and Iraq, Cameron's office said. Hollande will travel to Washington and Moscow later in the week to push for a stronger international coalition against IS.

L'enquête avance sur le commando de Saint-Denis, Le Monde

Trois personnes sont mortes lors de l'assaut. Le passeport de la cousine d'Abaaoud a été retrouvé sur place
Le Monde
2015 11 21

L'invité surprise des attentats du 13 novembre à Paris et Saint-Denis, Abdelhamid Abaaoud, a bien été abattu mercredi matin par les policiers du RAID, lors de l'assaut de l'appartement où plusieurs terroristes avaient trouvé refuge dans le centre de Saint-Denis, a révélé, jeudi 19 novembre le procureur de la République à Paris, François Molins. Il restait, vendredi matin, au moins un fugitif : Salah Abdeslam, 26 ans, Français résident à Bruxelles, reparti vers la Belgique samedi matin après les attaques.

Invité surprise, car si le rôle d'Abdelhamid Abaaoud, un Belge de 28 ans parti rejoindre l'Etat islamique (EI) début 2013, comme probable commanditaire des attentats du 13 novembre, est apparu assez rapidement aux enquêteurs, sa présence à Paris, et sa participation directe aux attaques, interroge sur la capacité des services de renseignement français et européens à suivre le mouvement des djihadistes de l'EI. Y compris les plus signalés d'entre eux.

Les enquêteurs s'interrogent aussi sur le parcours qui a permis à au moins deux autres auteurs des attaques de revenir de Syrie : Samy Amimour et Ismaël Omar Mostefaï, deux assaillants du Bataclan. Par ailleurs, l'identité réelle du kamikaze du Stade de France auprès duquel un passeport syrien a été découvert reste à établir.

« Nous ne savons pas » comment Abaaoud est entré en France, a reconnu le premier ministre, -Manuel Valls, jeudi. « Ce n'est que le 16 novembre, postérieurement aux attentats de Paris, qu'un service de renseignement d'un pays hors d'Europe nous a signalé avoir eu connaissance de sa présence en Grèce » , a précisé le ministre de l'intérieur, Bernard Cazeneuve, dans une déclaration à la presse.

Succès de police judiciaire, échec du renseignement? L'annonce de l'identification d'Abdelhamid Abaaoud parmi les corps retrouvés dans l'appartement rue du Corbillon, à Saint-Denis, où a eu lieu l'assaut, a provoqué un véritable soulagement parmi les enquêteurs. C'est la directrice centrale de la police judiciaire, Mireille Ballestrazzi, qui l'a annoncé personnellement au ministre de l'intérieur, Bernard Cazeneuve. Le corps du djihadiste était criblé de balles, sa tête méconnaissable et le buste en partie dévasté par le souffle d'une explosion.

L'enquête de la section antiterroriste de la police judiciaire parisienne, de la sous-direction antiterroriste de la direction centrale de la police judiciaire (SDAT) et de la direction générale de la sécurité intérieure (DGSI) avance à grand pas depuis les attaques de vendredi, qui ont fait 129 morts et plusieurs centaines de blessés lors d'attaques kamikazes et de fusillades simultanées au Stade de France, au Bataclan et dans l'est parisien.

Les tribulations d'Abdelhamid Abaaoud dans la capitale française et sa proche banlieue entre vendredi et mercredi se précisent. Une caméra de vidéosurveillance de la RATP l'a filmé sur la ligne 9 vendredi 13 novembre, à 22 h 14, entrant à la station Croix-de-Chavaux, à Montreuil

(Seine-Saint-Denis). Des images tendant à corroborer l'idée que celui qui se faisait appeler Abou Omar était dans la Seat convoyant le commando qui a tiré sur les terrasses de café du 10e et du 11e arrondissement. La voiture avait été retrouvée dans la nuit de samedi à dimanche, rue Edouard-Vaillant, à Montreuil. Des éléments de téléphonie en cours d'exploitations pourraient venir confirmer cette hypothèse.

Services marocains

Selon une source proche de l'enquête, c'est la géolocalisation du téléphone d'Hasna Ait Boulahcen, 26 ans, la cousine d'Abaaoud, qui a permis de confirmer le premier renseignement obtenu lundi après-midi selon lequel elle se trouvait à Saint-Denis avec son cousin. Un témoin est ensuite venu confirmer cette hypothèse. A la veille de la visite du roi du Maroc en France, plusieurs médias ont assuré que ce sont les services marocains qui avaient mis la police française sur la piste de l'appartement de Saint-Denis. Des informations démenties de sources judiciaires et policières françaises, qui tout au plus expliquent que les services du royaume chérifien ont transmis a posteriori des précisions sur les personnes interpellées dans l'appartement.

C'est bien un renseignement de police judiciaire, l'exploitation de la téléphonie et des réquisitions bancaires qui ont mis les enquêteurs sur la piste de Saint-Denis. Toutefois, il n'est pas exclu que la Direction générale de la sécurité extérieure (DGSE) a pu bénéficier de renseignements transmis par des services de renseignements étrangers qu'elle aurait ensuite fournis aux enquêteurs français.

L'assaut, d'une grande violence, a entraîné une certaine confusion concernant l'identification des occupants de l'immeuble. Alors que les services de la police scientifique progressaient péniblement dans l'appartement ravagé par la confrontation entre les policiers et les terroristes, l'incertitude demeurait sur le nombre exact de personnes tuées pendant l'assaut du Raid ainsi que sur le ou la kamikaze qui a déclenché une ceinture d'explosif au moment de l'affrontement.

Selon les informations du Monde, un corps de femme a été retrouvé dans les décombres ainsi qu'un sac à main contenant un passeport au nom d'Hasna Ait Boulahcen. Mais la tête retrouvée par la police scientifique correspond finalement à celle d'un homme. Aucune arme n'a pour l'instant été retrouvée dans l'appartement.

Le procureur de la République de Paris, François Molins, a affirmé mercredi soir que tout laissait à penser « qu'au regard de leur armement, de leur organisation structurée et de leur détermination, ce commando pouvait passer à l'acte . Mais aucun projet précis n'a pu être mis en évidence à ce stade.

Huit personnes étaient toujours en garde à vue à Levallois, dans les locaux de la SDAT, vendredi matin. Parmi elles, Jawad B., qui s'était spontanément présenté comme le logeur du dernier commando à Saint-Denis devant les caméras de BFM TV, assurant toutefois qu'il ignorait tout de ses hôtes. Parmi les autres, des Marocains et des Egyptiens en situation irrégulière qui pourraient n'avoir rien à voir avec les attentats mais qui squattaient vraisemblablement dans l'immeuble.

Des doutes subsistent sur le rôle précis de Salah Abdeslam, qui pourrait être l'un des passagers de la Seat noire utilisée lors des fusillades de terrasses de restaurants et cafés du 10e et 11e arrondissement, mais qui pourrait également avoir conduit la Clio noire qui a déposé

les trois kamikazes du Stade de France. Vendredi matin, l'identité de trois des assaillants morts durant les attentats restait inconnue : deux du Stade de France, et un au Bataclan.

Le rôle opérationnel d'Abaaoud se précise, Le Monde

Le Monde
France, lundi 23 novembre 2015, p. 13
Laurent Borredon, Simon Piel, et élise Vincent

Ses empreintes ont été retrouvées sur une kalachnikov laissée dans l'une des voitures du commando

Une semaine après les attentats qui ont frappé Paris, l'enquête menée par la section antiterroriste de la police judiciaire parisienne, de la sous-direction antiterroriste de la direction centrale de la police judiciaire (SDAT) et de la direction générale de la sécurité intérieure (DGSI) précise peu à peu les rôles tenus par les membres du commandos.

La place tenue par Abdelhamid Abaaoud, tué mercredi à Saint-Denis (Seine-Saint-Denis) lors de l'assaut du RAID, est au coeur des investigations en cours. Sa présence aux côtés de Brahim Abdeslam qui s'est fait exploser devant le Comptoir Voltaire et d'un homme encore non identifié dans la Seat Leon retrouvée à Montreuil (Seine-Saint-Denis) dans la nuit de samedi à dimanche est désormais établie. Il s'agit de l'équipe qui a mitraillé les terrasses des cafés du 10e et du 11e arrondissement.

Vendredi 20 novembre au soir, une source judiciaire indiquait que les empreintes du djihadiste franco-belge avaient été identifiées sur une kalachnikov retrouvée dans la voiture. Les policiers étudient l'hypothèse qu'Abdelhamid Abaaoud ait été au volant de la Seat dans la soirée du 13 novembre. Des éléments de géolocalisation téléphonique permettent de penser que la Seat a en tout cas continué à tourner dans le 11e après les fusillades pendant une quinzaine de minutes avant de se rendre à Montreuil. Des images filmées par une caméra de surveillance de la RATP attestent de la présence d'Abdelhamid Abaaoud au métro Croix de Chavaux à 22 h 14.

Son itinéraire ensuite est encore flou. Pendant le week-end, il semble errer sans point de chute; cherche à se procurer des couvertures ainsi que deux costumes pour des raisons encore inconnues. C'est ensuite parce que les appuis logistiques manquent qu'il fait appel à sa cousine Hasna Aït Boulahcen.

Selon l'AFP, celle-ci serait venu le récupérer mardi dans un entrepôt à Aubervilliers (Seine-Saint-Denis) après lui avoir trouvé le logement de la rue du Corbillon à Saint-Denis. Alors qu'il avait initialement été présenté comme l'unique commanditaire des attentats, le rôle opérationnel qu'il a joué à Paris et l'enregistrement diffusé par l'Etat islamique où Fabien Clain lit le communiqué tendent à s'interroger sur le véritable commanditaire des attaques. Le procureur de la République a d'ailleurs insisté sur ce point lors de sa conférence de presse tenue mercredi soir.

Samedi matin, les gardes à vue de sept des huits personnes interpellées à Saint-Denis après l'assaut du RAID avaient été levées. Cinq d'entre elles seraient des étrangers en situation irrégulière, sans lien avec les attentats, qui squattaient vraisemblablement l'immeuble de la rue du Corbillon. Seul Jawad B., qui s'était présenté comme le logeur du commando, devant les caméras de télévison, était toujours en garde à vue. Par ailleurs, à ce stade de l'enquête, l'identification du troisième assaillant du Bataclan était toujours en cours.

Le parcours de Salah Abdeslam dont le portrait avait été diffusé par la police française s'affine lui aussi. C'est lui qui aurait conduit le commando du Stade de France au volant d'une Clio retrouvée dans le 18e. Selon le Nouvel Observateur , son téléphone aurait été ensuite localisé un peu plus tard dans le secteur Montrouge-Châtillon avant d'être exfiltré par deux amis venus de Belgique aujourd'hui inculpés pour leur appui logistique.

Toujours selon le Nouvel Observateur , les deux hommes auraient retrouvé Salah, porteur d'une ceinture d'explosif, dans un état de " choc " . Une version qui expliquerait pourquoi l'Etat islamique a mentionné une attaque dans le 18e arrondissement de Paris dans son communiqué de revendication alors qu'aucune n'attaque n'a finalement eu lieu. Selon Me Xavier Carrette, l'avocat belge d'un des deux hommes, ces derniers auraient simplement admis que Salah était " un peu stressé " quand ils l'ont récupéré.

La confirmation qu'un deuxième kamikaze du Stade de France soit passé par la route des migrants conforte la crainte des autorités née après la découverte, dès samedi, d'un passeport syrien près d'un des djihadistes. " Nous ne sommes pas à l'abri d'un scénario où presque tous les auteurs des attentats soient passés par là ", explique une source proche de l'enquête.

Outre les deux kamikazes du Stade de France, des questions se posent notamment sur le parcours qui a permis à au moins quatre autres auteurs des attaques de revenir de Syrie : Samy Amimour et Ismaël Omar Mostefaï, deux assaillants du Bataclan. De même que sur les allers et retours entre la Syrie et l'Europe d'Abdelhamid Abaaoud, probablement le djihadiste francophone le plus connuainsi que le parcours de Salah Abdeslam avant son arrivée en France.

Depuis plusieurs mois, le ministère de l'intérieur avait été alerté par des policiers présents en Grèce de la faiblesse, voir de l'absence de filtrage sérieux à l'arrivée sur les îles de la mer Egée.

Une telle utilisation coordonnée de la route des migrants, sous des fausses identités et/ou avec de faux passeports, serait inédite. " A cette échelle, c'est une capacité que l'on découvre " , explique une source Place Beauvau. Les centre de " tri " des migrants, baptisés " hot spots " sont bien en train d'être installés aux frontières extérieures de l'Europe, notamment en Grèce ou en Italie, mais dans la pratique, leur fonctionnement serait surtout formel et surtout adaptés à l'identification des personnes vulnérables ayant besoin de protection.

Jusqu'ici, l'écrasante majorité des djihadistes français étaient revenus en Europe sous leur propre identité. Depuis le loupé qui avait vu trois hommes, dont un ami d'enfance de Mohamed Merah, échapper à la direction générale de la sécurité intérieure (DGSI) à leur retour en France, en septembre 2014, ils sont récupérés par la direction de la coopération internationale (DCI) du ministère de l'intérieur - qui a la responsabilité des attachés de sécurité intérieure placés dans les ambassades de France. Plus de 150 personnes auraient pris le chemin du retour à visage découvert depuis un an.

Enfin, l'irruption d'Hasna Ait Boulahcen, 26 ans, par le biais d'un témoignage spontané à la police, pose une nouvelle fois la question de la surveillance des milieux djihadistes par les services de renseignement. Alors qu'Abdelhamid Abaaoud était une cible privilégiée de la DGSI en raison de son rôle supposé dans plusieurs projets d'attentats en France, sa cousine, récemment radicalisée, avait-elle été repérée par la DGSI, ou a-t-elle échappé aux radars du service?

Les investigations judiciaires ne permettront pas forcément de répondre à cette question - ce n'est pas leur rôle - mais elle intrigue les enquêteurs. En tous cas, plusieurs sources confirment que, jusqu'au bout, tous les services de renseignement et de police judiciaire impliqués dans le dossier ont été persuadés que l'homme était toujours en Syrie, incrédules devant la possibilité que ce cadre de l'EI ait pu voyager aussi discrètement en Europe.

Analysis: In Terror Fight, French Feel Increasingly Isolated, Wall Street Journal

By Yaroslav Trofimov
21 November 2015
The Wall Street Journal

PARIS -- The world seems awash in sympathy with France's tragedy, from candlelight vigils to stadiums illuminated in tricolor. But, when it comes to action against Islamic State, there is growing fear in Paris that France may be in this fight dangerously alone.

French officials are particularly frustrated with their European Union partners over what they see as insufficient cooperation in intelligence, security and defense. "Everyone must understand that it's urgent for Europe to recover, to organize itself, and to defend itself against the terrorist menace," French Interior Minister Bernard Cazeneuve said this week.

In one way, the U.S. has responded much more quickly than France's European partners after the Nov. 13 attacks, boosting intelligence sharing with Paris. But Washington hasn't signaled that a more determined military effort against Islamic State lies ahead. President Barack Obama reiterated this week that the current U.S. approach of limited military engagement is working, and ruled out the use of ground troops.

French officials and politicians worry that the U.S. is underestimating the threat Islamic State poses to the international community.

"The goal of the attacks in Paris was to destroy our values, the values shared by the U.S. and France. And without a doubt we need for the American people to understand that this is also their war," said Frederic Lefebvre, a member of the defense committee in the French National Assembly and a former minister.

In September 2001, America's allies -- such as France -- instantly offered their help under the North Atlantic Treaty Organization's Article 5, which provides for collective defense.

Paris, which described the Nov. 13 shooting and bombing spree that killed 130 people as "an act of war," hasn't asked for NATO assistance, invoking instead the mutual-defense obligations of the European Union. The response has been lukewarm, at best. Even France's request to loosen fiscal rules so it could beef up its army and police to protect the country against Islamic State has been met with noncommittal statements from Brussels, so far.

"We are on our own, and we are counting our friends," said Francois Heisbourg, an adviser at the Fondation pour la Recherche Strategique think tank and a former senior French diplomat.

No other European country has joined France in airstrikes against Islamic State in Syria so far, though British Prime Minister David Cameron has called for a Parliament vote to authorize such an operation. In Iraq, too, no additional European countries entered the air campaign that is being conducted by France, the United Kingdom, Belgium, Denmark and the Netherlands as part of the American-led coalition against Islamic State.

Paris has asked for something simpler: help in its campaign against Islamist radicals in Mali and other West African nations. That would allow the French to free up elite troops to concentrate on Islamic State. But on that front, too, only Ireland has offered to send a "small" number of troops so far.

"Many countries avoid military action because they don't want to run the risk of becoming targets themselves, and because it is costly," said Mr. Lefebvre, the lawmaker.

Even though France asked, following the January Charlie Hebdo attacks, for the sharing of information on air travel bookings, the European Parliament scuttled the decision over privacy concerns. Mr. Cazeneuve this week noted that no European nation tipped off Paris on the movements of Abdelhamid Abaaoud, the architect of the Paris attacks, across the continent from Syria. There is also a persistent sense in Paris government offices that France can't count on the U.S., either.

Now, it is France rather than the U.S. that is paying the costs of Washington's regional "disengagement without taking into account the consequences," said Gilles Dorronsoro, a professor of political science at Sorbonne University in Paris.

"There are almost no refugees in America, and, for now, no terror attacks," Mr. Dorronsoro said. "The stakes, or at least the perceived stakes, for the U.S. are not the same."

Anti-terrorism 'ghosts' wage war from a computer, UK Times

James Dean
21 November 2015
The Times

An elite unit of anti-terrorism "hacktivists" is helping the British security services with intelligence operations against Isis, The Times has learnt.

Ghost Security Group, which counts former military computer experts among its members, is credited with providing intelligence that foiled a terrorist attack against British tourists in Tunisia this year.

Since the Paris attacks, members have infiltrated online Isis accounts run by individuals who had prior knowledge of the shootings. The group also believes that it has uncovered chatter stored on an encrypted messaging service that shows Isis members plotting the attacks.

Ghost Security Group (GSG) passes intelligence leads to MI5 and other security organisations across the world through the American authorities.

The group, which formed in January after the Charlie Hebdo massacre, comprises 14 anonymous individuals with backgrounds in the military and in private computer security

companies. The group focuses on intelligence gathering but it also launches digital attacks against Isis.

The group's executive director, who goes by the name DigitaShadow, told The Times: "You guys have a lot of jihadists over there. We try to identify these people, then alert the [US] authorities, so that they can alert MI5."

GSG investigates online accounts that it suspects are owned by influential members of Isis. One line of inquiry involves accounts on the Telegram encrypted messaging system, which has become the favoured messaging and broadcast service of several jihadist organisations. "We have data that the planning for Paris was conducted through Telegram," DigitaShadow said.

Members of Ghost Security Group create "infiltrator accounts" — online profiles where they pose as jihadist sympathisers or potential recruits — to develop trust with Isis insiders. Their infiltration operations are backed by translators and analysts to make their fake profiles as credible as possible. Once trust is gained, they are able to glean intelligence from the terrorists and make contact with others higher up the chain.

GSG tries to identify online accounts that are being used to lure would-be jihadists. The group focuses its attention on social media, messaging and other accounts where Isis operatives have already made progress with recruiting vulnerable individuals.

The group also provides intelligence to the authorities about the hacking capabilities of Isis, the targets of Isis hackers and the identities of the Isis hackers themselves.

DigitaShadow said that the group had removed 149 websites, 6,000 propaganda videos and 111,000 social media accounts linked to Isis since January. The group does not remove any sites that have intelligence value, Digita-Shadow said.

The group uses Michael Smith, the chief operating officer at Kronos Security, a US counterterrorism consultancy, as a conduit to pass information to the American security services. Mr Smith, who has advised the US Congress on terrorism matters, said that the group was focusing its efforts on intelligence about possible follow-up attacks to the Paris shootings.

Mr Smith said that intelligence gathered by GSG had helped to foil a terrorist plot to attack British and Jewish tourists at Houmt Souk in Djerba, Tunisia, in July.

"Ghost Security Group is the most effective and best of the very small cast of groups I'm engaging with," he said. "It's small but there are individuals who possess the knowledge and skills that are capable of producing quality information that can be passed to intelligence services.

"The authorities in the UK are aware of the value of GSG. I know that the officials here who I liaise with have spoken with officials from the UK about Ghost Security Group. They have expressed more and more interest in their work."

However, Mr Smith suggested that the attack campaign announced by Anonymous this week could upset some intelligence work being done online.

"If they [intelligence agents and Ghost Security Group members] are undercover posing as Isis agents, Anonymous is going to end up ruining someone's investigation."

He added that the security and intelligence agencies "really do have a strong handle on the social media landscape. But Isis is so prolific that there's a need to have more eyes on the system."

EU to Step Up Checks on Citizens Entering Bloc in Security Push, Wall Street Journal

Luxembourg says 'Europe has to act now' after Paris attacks
By Valentina Pop and Laurence Norman
1393 words
20 November 2015
The Wall Street Journal Online

BRUSSELS—The European Union has ordered stepped-up checks on its own citizens when they enter the bloc, a move aimed at stemming the terror threat from foreign fighters in the wake of last Friday's Paris attacks.

The decision comes after it emerged that the organizer of the Paris attacks, Abdelhamid Abaaoud, a Belgian citizen, had traveled unhindered from Syria back to Paris in time for last Friday's killing spree.

"The strengthening of controls at our external borders is indispensable for the protection of EU citizens," French Interior Minister Bernard Cazeneuve said, after meeting with EU justice and interior ministers in Brussels on Friday.

Under current rules, non-EU citizens are supposed to be checked against police data when they enter the bloc to see whether they are wanted by authorities or could be carrying a fake passport.

EU nationals are sometimes checked against police data if they display suspicious behavior or if there is reason to believe they pose a terror threat. However, such checks are sporadic.

Governments agreed to implement the measure immediately. Meanwhile, the European Commission, the bloc's executive, will start working on rule changes so that the systematic checks become permanent.

"I am happy about this, checks have to be made systematically and against all relevant databases to flag up the movement of jihadists," said Mr. Cazeneuve.

The new measures come as the bloc struggles to cope with the effects of the Paris attacks, the biggest act of terrorism in the bloc in years.

Central to the problem is the EU's 26-member Schengen border-free zone. Weak controls on Schengen's external borders, combined with the absence of checks once a person enters the bloc, have hugely complicated Europe's efforts to stop terror threats.

Ministers also pushed again Friday for new rules to be passed rapidly allowing airline passenger data to be shared.

The European Parliament has blocked the legislation for years over privacy concerns and has sought to water down how long the data would be retained and who would be registered.

France insisted again Friday that the proposed system—the so-called Passenger Name Record—should include intra-EU flights and that data should be kept for at least a year. The European Parliament wanted to restrict the data being kept longer than one month and to exclude intra-EU flights.

Luxembourg's Deputy Prime Minister Etienne Schneider said Friday the bloc wants an agreement on the new rules in early December and that they should be implemented “as soon as possible."

German Interior Minister Thomas de Maizière said that air travelers' records were needed because foreign fighters in Syria move back and forth when planning attacks on Europe.

“Almost every week a traveler [by air] is arrested in Germany. But there is also information we aren't getting, and then there are security gaps," Mr. de Maizière said, on his way into the meeting.

Ministers committed to better track and stop illegal firearms from being traded. The commission this week proposed tighter rules for the sale of decommissioned weapons after evidence emerged they have been used in other terror attacks in Paris this year.

The officials also pledged Friday to step up intelligence sharing. The head of the EU's police agency, Europol, said Thursday that half of the names on the organization's foreign fighters list come from just five of the EU's 28 member states.

The EU's counterterrorism coordinator, Gilles de Kerchove, said that intelligence agencies, not only police, need to include data on potential terrorists in the EU-wide databases. “This is the issue we had with Nemmouche, he was in the system but not explicitly linked to terrorism," he said, in reference to the French national, Mehdi Nemmouche, who shot four people at the Jewish museum in Brussels last year.

Mr. de Kerchove also spoke of “institutional schizophrenia" in the EU, where data gathered by the bloc's border agency Frontex on incoming migrants cannot be shared with Europol. Ministers on Friday said the two should be linked up and start exchanging data as of Jan. 1.

With Europe floundering to respond to the terrorist threat, some European officials have floated more radical options. European migration Commissioner Dimitris Avramopoulos said Friday he believed the bloc should explore an EU-wide intelligence agency, an idea quickly shot down by the German interior minister.

Meanwhile, Austria's Interior Minister, Johanna Mikl-Leitner, refused to discard some preliminary ideas, floated in the Netherlands, of restricting the Schengen free border-free zone to a small group of western European countries in an emergency.

“For now this is just a thought experiment that doesn't have highest priority. But in a situation as difficult as the one that we are experiencing at the moment, we must not prohibit the experts from thinking. Because we all know that things cannot continue as they are," she said.

Despite the decisions Friday, there is skepticism as to how quickly the EU can tighten security on its external borders.

Ministers are aiming for a March deadline to provide border authorities with the ability to run database checks against incoming people. However, in the case of Greece alone, that requires providing thousands of computers and staff at 220 border crossings, said one senior EU diplomat.

Greece has come under heavy pressure from its EU partners to improve its screening of the hundreds of thousands of migrants who have arrived there from Turkey over the past year.

One of the Paris suicide bombers, carrying what seems to have been a fake Syrian passport, was registered entering Greece in October. Mr. Abaaoud also traveled through Greece.

On Friday, Nikos Toskas, the Greek minister for public order and citizen protection, defended his country's record of securing Europe's external border.

“The big flows of refugees are continuously coming but they are checked, screened and identified according to European rules."

Meanwhile Hungarian Prime Minister Viktor Orban said Friday that European Union member states should renegotiate the bloc's founding treaty to reinforce a sense of strength and unity, or they will face the radicalization of the continent.

The Hungarian leader also lashed out at the open-door policy for migrants and criticized Europe's plan, supported by Brussels and Berlin, to resettle migrants in EU countries. Such plans provide a means to spread terrorism in Europe, Mr. Orban said.

“Migration increases the terrorism threat, increases crime and puts our cultural identity in danger. That's why it must be stopped," the prime minister said. “Support for off-mainstream, radical, extremist political forces is on the rise…which is not in the interest of any one of us."

Mr. Orban said the Schengen system “must be corrected by all means" in light of what he sees as the current inconsistency, which see countries such as Greece fail to protect their external borders from illegal immigration while others, like Hungary, do their utmost to guard their frontiers.

“Hungary doesn't really like to belong to a treaty that some adhere to while others don't. This system is impossible to maintain," Mr. Orban said in an interview on state radio Friday.

“Several things happened over the past six to seven years that underpin the claim that we must rethink some basic issues regarding European politics."

Suspected ISIL scout in Paris attacks arrested in Turkey's Antalya, Dogan News Agency

2015 11 21
Dogan News Agency

Antalya, Turkey—**Turkish police have detained a Belgian man of Moroccan origin on suspicion that he scouted out the target sites for Islamic State of Iraq and the Levant (ISIL) in attacks that killed 132 people in Paris on Nov. 10.**

The suspect, and two others detained for possible links to him, were arrested by a court on Nov. 21.

Ahmet Dahmani, 26, was detained at a luxury hotel in the Mediterranean coastal city of Antalya.

Two other men, 29-year-old Ahmet Tahir and 23-year-old MMohammed Verd -both Syrian citizens- were also detained on a nearby highway on suspicion that they had been sent by ISIL in Syria to ensure Dahmani's safe passage across the border and were planning to meet him. The suspects had fake passports in their possession, the police said.

Counter-terrorism police first became aware of Dahmani when he arrived on a flight to Antalya and tracked him to the hotel in the Manavgat district of the city.

Separately, Turkey deported a group of Moroccans detained at Istanbul's main airport this week over suspected links to ISIL.

The eight, who said they had arrived at Atatürk Airport on Nov. 17 night from Casablanca for a holiday, were detained by border police and questioned by profiling experts who flagged them as suspected militants, a government official told Reuters.

Ce que les Belges savaient d'Abaaoud, Le Monde

France, samedi 21 novembre 2015, p. 2
Elise Vincent
Le Monde

Les services de renseignement le croyaient en Syrie, il était en réalité en France. Abdelhamid Abaaoud, soupçonné d'être le commanditaire des attentats du 13 novembre à Paris, est mort le corps criblé de balles, mercredi 18 novembre, dans l'appartement de Saint-Denis (Seine-Saint-Denis) pris d'assaut par la police.

Les enquêteurs vont s'attacher à retracer le parcours du djihadiste de l'Etat islamique. Et tenter de comprendre les failles qui ont permis le retour en Europe, incognito, de ce jeune Belge d'origine marocaine, visé par un mandat d'arrêt international et soupçonné, selon le ministre de l'intérieur, Bernard Cazeneuve, d'être à l'origine de quatre des six attentats déjoués sur le sol français depuis le printemps.

Une fiche de synthèse des services de renseignements belges concernant le parcours d'Abdelhamid Abaaoud, que Le Monde a pu consulter, donne de premiers éléments de réponse. Ce document, daté du mois d'avril, reprend point par point, de façon chronologique, jusqu'en février 2015, l'itinéraire connu du djihadiste. Un parcours à l'évidence composé de nombreux trous, que les services belges ne cherchent pas à cacher.

Extrêmement précise, cette fiche d'une vingtaine de pages retrace notamment tous les numéros de téléphone connus du djihadiste. Le dernier date de mai 2013, et il est turc. Elle retrace également l'évolution de ses kunya (« pseudonymes ») : Abou Omar en mai, Abou Omar Soussi en juillet 2014, puis Abou Omar Al-Baljiki, à partir de février 2015. Son adresse email quasi certaine a aussi été identifiée.

D'après cette fiche, l'intérêt des services de renseignement belges pour le jeune homme commence suite à une note déclassifiée de la sûreté de l'Etat en date de février 2013. Celle-ci concerne le départ simultané vers la Syrie de sept jeunes gens. Rapidement, les enquêteurs vont découvrir une page Facebook où ils communiquent, intitulée la katiba al-muhajireen (« la brigade des immigrés »). Et très vite, ils vont mettre au jour la toile de leurs amitiés.

En parallèle, les enquêteurs vont commencer à faire des recherches sur l'histoire et l'entourage d'Abdelhamid Abaaoud. Le jeune homme est né à Anderlecht, dans l'agglomération de Bruxelles, le 8 avril 1987, il est l'aîné d'une famille nombreuse de six enfants. Il a la double nationalité belge et marocaine. Avant son premier départ pour la Syrie, début 2013, il était célibataire et vivait seul.

Le jeune homme a commencé à connaître des ennuis judiciaires à partir de 2002 et a multiplié les séjours en prison entre 2006 et 2012, « mais jamais pour plus de trois mois » , précise la note. Dans la famille, Abaaoud, Abdelhamid n'est pas le seul à avoir des démêlés avec la justice : son frère Yassine est connu pour des petits faits de délinquance. D'après son père, un petit commerçant auditionné en février 2014, la radicalisation d'Abdelhamid Abaaoud a démarré très vite après sa sortie, en septembre 2012, de l'établissement pénitentiaire de Forest. Il se met à porter la barbe. Arrête de fréquenter ses amis du quartier. Interrogé à la même époque, son frère Yassine pense qu'il a effectué un court séjour en Egypte avant de se rendre en Syrie.

Chapitrée par grandes dates clé, la fiche des services belges s'arrête ensuite sur la période de mars 2013. Abdelhamid Abaaoud est cette fois repéré par hasard, lors d'écoutes téléphoniques, sur le téléphone turc d'un interlocuteur situé à la frontière turco-syrienne. Abaaoud souhaite alors que ce jeune homme fasse l'intermédiaire avec son frère Yassine, resté en Belgique, et l'incite à lui envoyer de l'argent pour lui et pour « Allah » .

Sans explication, la fiche des services belges bascule immédiatement au mois de septembre 2013 : Abdelhamid Abaaoud est alors considéré comme en étant de retour en Belgique. « On sait très peu de choses sur [ses] faits et gestes jusqu'à ce qu'il revienne sur le territoire belge » , concède la fiche. « De source policière, il a été aperçu à la fin du mois de septembre en train de se promener dans Molenbeek-Saint-Jean [une banlieue de Bruxelles] . » Il était accompagné d'un homme qui est parti ensuite combattre en Syrie.

Younes, 13 ans

Le 20 janvier 2014, nouveau saut de puce temporel : le djihadiste est cette fois contrôlé à l'aéroport de Cologne, en Allemagne, direction Istanbul. « Il est resté très discret et ne réapparaît sur notre radar » qu'à ce moment-là, assume aussi la fiche de synthèse belge. Il est identifié en compagnie de son petit frère mineur Younes, âgé seulement de 13 ans, et d'un autre jeune homme d'origine malienne, qui mourra plus tard en Syrie. Abdelhamid Abaaoud a en fait soustrait Younes à l'attention de ses parents à la sortie de l'école. Rien ne les empêchera de s'envoler. L'adolescent sera alors surnommé « le plus jeune djihadiste de Syrie » par les médias belges.

A partir de février 2014, Abdelhamid Abaaoud est définitivement considéré par les services de renseignements comme un « moujahid de l'Etat islamique . Les services s'appuient particulièrement sur la vidéo de lui, diffusée sur le site de BFM-TV, où il apparaît tout sourire, au volant d'un pick-up traînant plusieurs cadavres de « mécréants », selon ses mots.

C'est vers le mois de juin 2014 que le père d'Abdelhamid Abaaoud situe ensuite le dernier contact téléphonique avec son fils. Ce jour-là, Omar Abaaoud tente d'obtenir de parler avec le plus jeune des frères, Younes. Il ne l'a plus eu au téléphone depuis deux mois et s'inquiète. Mais il n'aura plus jamais de nouvelles. Omar Abaaoud pense alors que les deux frères n'étaient plus ensemble en Syrie à ce moment-là.

Selon la fiche de synthèse, ce n'est qu'en août 2014 que des mandats d'arrêts belges et internationaux vont être émis formellement contre Abdelhamid Abaaoud.

Le feuilleton s'arrête finalement en février 2015, quand les services belges tombent sur l'interview du djihadiste au magazine de l'Etat islamique Dabiq. Sur l'une des photos de l'article, les enquêteurs reconnaissent deux jeunes gens soupçonnés de prévoir un attentat sur le sol belge. Deux hommes tués à Verviers lors d'une intervention des forces de l'ordre belges contre une « cellule terroriste opérationnelle », en janvier, quelques jours après les tueries de Charlie Hebdo et de l'Hyper Cacher. Dans cet entretien à Dabiq, Abdelhamid Abaaoud affirme qu'il se trouvait en Belgique le jour du démantèlement de la cellule de Verviers. Et qu'il avait pu regagner la Syrie sans se faire repérer.

Les deux mois qui courent avant la publication de la fiche de synthèse, en avril, ne sont pas documentés. Reste à écrire le film des sept mois suivants, jusqu'aux attentats de Paris.

Après l'assaut de Saint-Denis, la traque se poursuit, Le Figaro

Cornevin, Christophe
Le Figaro
samedi 21 novembre 2015, p. 7
Salah Abdeslam, ultime rescapé présumé des commandos de tueurs, est l'objectif prioritaire. Pas moins de 2 000 policiers sont mobilisés.

LA PLUS grande traque jamais menée par la police française pour percer les arcanes des commandos qui ont frappé de manière coordonnée le coeur de Paris et Saint-Denis ne se relâche pas d'un iota. Près de 2 000 limiers du renseignement et de la police judiciaire poursuivent leur course contre-la-montre pour identifier, localiser et neutraliser le reste de l'hydre djihadiste ayant semé la mort au nom de l'État islamique. Au dernier stade des investigations, neuf islamistes sont soupçonnés d'avoir participé directement aux fusillades et actions suicides qui se sont soldées par un bilan toujours provisoire de 130 morts. Selon une source judiciaire jointe par Le Figaro, les enquêteurs affichaient vendredi la plus grande prudence sur l'éventuelle implication des cinq personnes extraites de l'appartement « conspiratif » de Saint-Denis après l'assaut du Raid. En effet, si les vérifications se confirment, il s'agirait de trois Marocains et deux Égyptiens, tous clandestins qui squattaient sur place sans subodorer un seul instant partager le toit d'islamistes. La garde à vue des trois autres suspects se poursuit. Outre une jeune femme habitant elle aussi sur place, les policiers interrogent deux « logeurs » soutenant avoir mis les lieux à disposition d'un « ami qui avaient deux copains belges » .

Depuis une semaine, les limiers recomposent avec méthode un terrifiant puzzle dont ils ignorent le nombre de pièces. Après avoir exploré dans de périlleuses conditions les décombres de l'immeuble dévasté et en passe de s'écrouler à Saint-Denis, ils ont établi jeudi avec certitude, grâce à des comparaisons d'empreintes digitales, que le cadavre de femme est bien celui d'Hasna Aitboulahcen. Un passeport portant ce nom a en outre été retrouvé à ses côtés. Âgée de 26 ans, née dans les Hauts-de-Seine, elle est présentée comme la cousine du commanditaire présumé des attaques, Adbelhamid Abaaoud éliminé lui aussi mercredi matin

par les policiers d'élite. C'est notamment la géolocalisation et la mise sur écoute de son téléphone mobile qui aurait **permis aux services de renseignement** de recentrer leur recherches sur l'appartement « conspiratif » où était retranchée la cellule terroriste. Mercredi, le procureur de la République, François Molins, a révélé que « la présence d'Abaaoud sur le territoire français » émanait d'un « témoignage obtenu lundi, recoupé par de nombreuses vérifications téléphonique et bancaires » . « Il a été recueilli dans le seul et unique cadre des investigations de police judiciaire » , a confié une source au coeur du dossier. L'origine du « service de renseignement d'un pays hors d'Europe » qui a, comme l'a précisé Bernard Cazeneuve, « signalé avoir eu connaissance de sa présence en Grèce » , reste entouré d'un épais mystère. Même si le nom de la Turquie a été évoqué, sans confirmation.

Tour à tour dépeinte comme « parfois excentrique » , « extravertie » , « garçon manqué » voire « instable » par son proche entourage, Hasna Aitboulahcen avait rompu les amarres familiales dès l'âge de quinze ans avant de se radicaliser de manière brutale. Troquant le chapeau de paille qu'elle portait volontiers contre un niqab noir, elle avait posté le 11 juin dernier une photo sur son compte Facebook avec ce commentaire : « Jver biento aller en syrie inchallah biento depart pour la turkie » (sic).

À la faveur des investigations, les enquêteurs, qui savent que le troisième corps retrouvé dans l'appartement de Saint-Denis est celui d'une kamikaze non identifiée, ont désormais acquis la présomption qu'Abaaoud serait le neuvième membre des commandos de vendredi. Cette figure tutélaire du djihadisme européen, que les services antiterroristes croyaient en Syrie il y a une semaine encore, a en effet été filmé par une caméra de vidéosurveillance de la RATP à Montreuil-sous-Bois (Seine-Saint-Denis) alors qu'il entrait dans la station de métro Croix de Chavaux, à 22 heures 14, le soir des attentats. Un rapprochement a été fait avec la Seat Leon noire, retrouvée à proximité dans la nuit de samedi à dimanche, avec trois kalachnikov à son bord et utilisée lors du raid qui a décimé les terrasses de cafés de l'est parisien. C'est de cette voiture immatriculée en Belgique que Brahim Salah est sorti pour se faire sauter devant le Comptoir Voltaire, dans le XIe arrondissement. Et c'est à son volant que se trouvait a priori son frère Salah, toujours en cavale. Plus que jamais, cet « objectif prioritaire » est au coeur d'une chasse à l'homme menée sans relâche à travers toute l'Europe. Exfiltré de toute urgence à sa demande vers la Belgique au lendemain des attentats de Paris dans une Golf noire contrôlée à Cambrai et interceptée à Molenbeek d'où sa famille est originaire, le Français de 29 ans, natif de Bruxelles, est la cible de coups de filets répétés dans le royaume. Vendredi, sept des neuf individus interpellés la veille dans la capitale belge lors d'une vague de perquisitions ont été remis en liberté après interrogatoire. La garde à vue des deux autres a été prolongée de 24 heures. L'un est interrogé dans le cadre de l'enquête ouverte au début de l'année par la justice belge après le départ en Syrie de Bilal Hadfi, un des trois kamikazes confondus par ses empreintes papillaires prélevées près du McDonald's du Stade de France, où il s'est fait exploser.

Déterminé à mettre un nom sur chacun des supposés commanditaires ou inspirateurs qui ont planifié et orchestré les tueries, les services de renseignement tournaient à plein régime pour localiser Jean-Michel Clain et son frère Fabien, vétéran du djihadisme dont la voix a été authentifiée dans l'enregistrement de la vidéo de revendication de l'État islamique. Car la relève d'Abaaoud, dont la mort n'a pas encore été exploitée par l'appareil de propagande terroriste, ne saurait tarder. Aiguillonnés par l'idée de frapper à nouveau Paris, nul doute que ses prétendants réfléchissent à une réplique d'ampleur.

Depuis une semaine, les limiers recomposent avec méthode un terrifiant puzzle.

Attacks Push European Union to Consider Limits on Passport-Free Travel, New York Times

By STEVEN ERLANGER; James Kanter contributed reporting from Brussels, and Alison Smale from Berlin.
21 November 2015
The New York Times

PARIS -- If Europe's system of passport-free travel was not under enough pressure after a summer of chaotic migration, then last week's attacks in Paris have fortified doubts over how much longer that freedom of movement -- one of the most cherished accomplishments of the European Union -- can survive.

The Nov. 13 massacres in Paris were carried out almost entirely by European passport holders who slipped in and out of Syria without being identified or checked. In addition, the discovery of a Syrian passport apparently held by one of the Paris assailants has renewed fears that terrorists have infiltrated the migrant wave.

With the focus now on bolstering security, European Union interior and justice ministers met in an emergency session on Friday and vowed to complete French proposals for tighter controls by the end of the year.

For the first time, the ministers agreed finally to establish a system to share the passport data of air travelers within the open border area under what is known as the Schengen Agreement.

Given the double chaos of migratory flows and cross-border terrorists, many countries -- including France, Germany, Austria, Belgium, the Netherlands, Hungary, Slovenia, the Czech Republic, Slovakia and Sweden -- have already established temporary border controls.

The concern is that they will make those temporary controls, which are allowed under Schengen, effectively permanent, destroying the agreement.

On Thursday night, adding to the confusion, most nations along Europe's migrant corridor abruptly shut their borders to those not coming from war-torn countries such as Syria, Afghanistan or Iraq, leaving thousands stranded at Balkan border crossings.

Manuel Valls, the French prime minister, said on Thursday: "If Europe doesn't shoulder its responsibilities, then it's the whole Schengen system that's put into question."

The open-border arrangement, established 20 years ago, covers 22 European Union countries and four other nations. But the system can work only if its external borders are policed and protected, and it is obvious to all that Europe has failed to do so.

Arnaud Danjean, a member of the European Parliament and a former security official and diplomat from France, put it bluntly: "If by the end of the year necessary measures to reinforce external border controls and to check passports of Schengen citizens are not implemented, I think Schengen is dead."

Otherwise, he said, "many countries will come back in January and say we need another system, and until we have one, we will adopt permanent border controls."

French proposals for tighter controls were first made after Islamist radicals attacked the satirical newspaper Charlie Hebdo and a kosher supermarket in January.

But they were stalled by inaction and by concerns over data privacy in the European Parliament, raised particularly by Germany and the newer members from Central and Eastern Europe, which have been largely untouched by terrorism.

On Friday, however, the ministers gave their backing to measures demanded by France this week that included tightening external borders by extending checks to more people who can usually enter, and move freely within, the Schengen area.

Strengthening controls at external borders is "indispensable for the protection of European citizens," Bernard Cazeneuve, the French interior minister, said at a news conference.

Overhauling the Schengen rules would mean "systematic and obligatory checks to be carried out at all our external borders and on all people entering the Schengen area, including those who benefit from the freedom of movement," he said.

Mr. Cazeneuve has expressed fury that France found out that the ringleader of the Paris attacks, Abdelhamid Abaaoud, had slipped undetected back into Europe only from intelligence provided by a non-European country, believed to be Morocco.

Under the proposals, if a Schengen passport holder travels to a third country, whether Turkey, Syria or the United States, upon re-entering the Schengen area the passport should not just be examined but checked against criminal and security databases.

The ministers also agreed to establish a single European gun registration file. Mr. Danjean said he hoped that the gun control laws could be unified eventually in the European Union, pointing out that Belgian laws are much less restrictive than French ones.

While the difficulties with Schengen are largely technical and administrative, the politics around the subject have become nasty, feeding Europe's far-right parties, especially France's National Front and Sweden's Democrats.

Marine Le Pen, the leader of the National Front, said that "the absence of national borders is criminal madness." Striking a familiar but trenchant theme, she said: "The French elites have given themselves over to this surreal myth of a country without borders. Open your eyes, now!"

Euroskeptics and the far right, "those trying to benefit from the situation, are trying to redefine the entire Schengen debate in a way that makes Schengen look like the culprit here," said Jan Techau, director of Carnegie Europe, a Brussels-based research institution.

And the Islamic State "used a very vulnerable time for their attacks, knowing full well that the refugee crisis is like a force multiplier of their attacks," Mr. Techau added. However unfair, he said, "it's very hard to separate them now."

"The victim is Europe," said Alain Frachon, a columnist for Le Monde. The Paris attacks coming alongside the migrant crisis "are one more bullet in the corpse of Schengen," he said.

"But of course Schengen was never really applied," he said. "Freedom of internal travel required European border controls," under an agency called Frontex, "but no one wanted to put any money into Frontex."

In general, Mr. Frachon said, "the first reflex of any police, border and customs agency is to keep national control."

To defend Europe's external borders efficiently, he said, one needs a supranational, European agency that works. "But that is exactly the opposite of what public opinion is asking for now, and it's a terrible contradiction," he added.

For the European Union, this is a defining moment, said François d'Alançon, an analyst at the newspaper La Croix. "This is not only about Islamic State, but about the refugee crisis, the euro, freedom of movement and the integration of Muslims all over Europe," he said.

"We have all these people claiming that we should shut the national borders," he said, "but we know that all the answers are really European ones. For intelligence sharing, for refugees, you need more Europe, with unified asylum policies and security policies."

For many people, Mr. D'Alançon said, "we all thought the European idea, the European project was the only ideal left." But now, he said, "it's all gone, it's just a big fog."

Informer, c'est aussi démentir les rumeurs, Le Monde

Agenda, samedi 21 novembre 2015, p. 15
Le Monde

Théâtre de manifestations de solidarité, les réseaux sociaux sont également, en ces temps troublés, l'outil de propagation de « l'intox »

La France vit, agit, souffre et pleure aussi sur Internet et sur les réseaux sociaux. Et la tragédie du 13 novembre l'a, s'il le fallait encore, prouvé. La France qui sort le vendredi soir, celle des 18-40 ans, c'est celle des utilisateurs de Twitter, Facebook ou WhatsApp. Et c'est vers ces médias qu'elle se tourne, même, voire surtout, en cas d'urgence.

C'est par ces canaux que passeront, vendredi, les premières informations, celles des milliers de témoins qui tweetent ou postent pour dire les coups de feu, les victimes, la panique. C'est sur les réseaux sociaux qu'on verra, au coeur de l'horreur du vendredi soir, le meilleur : des mobilisations spontanées, comme le hashtag #porteouverte sur Twitter, sur lequel des habitants du 11e arrondissement proposent un abri à ceux qui courent dans les rues; ou les dizaines d'initiatives, ensuite, pour retrouver les disparus de cette soirée tragique.

Mais c'est aussi par les réseaux sociaux que viendra, sinon le pire, du moins le reflet de la panique du pays, sous forme de rumeurs, d'intox, relayées souvent de bonne foi, parfois avec de mauvaises intentions, et de « course au buzz », à la notoriété, à tout prix.

Il y a les paniques qui s'amplifient, comme celle de dimanche, après les rassemblements, place de la République, qui se sont soldées par des mouvements de foule, à la suite de quelques pétards, bruits de voiture ou ampoules éclatées. Les réseaux sociaux, cette fois, ont joué un rôle de caisse de résonance de la panique des uns, qui s'est transmise aux autres, dans un contexte d'angoisse collective qui l'explique aisément.

Recherche du « buzz »

Sur le site du Monde , nous avons ouvert dès vendredi un suivi en direct, jour et nuit, des événements, dans lequel nos lecteurs pouvaient nous poser des questions. Nous avons aussi beaucoup publié sur les réseaux, essentiellement pour démentir des rumeurs et des bruits qui se diffusent d'autant plus vite dans ce contexte de peur.

L'effroi, la sidération, l'angoisse, on pouvait les lire dans les questions de nos internautes, ou par le biais de messages directs sur Facebook, reçus dans une proportion inédite. « On parle de coups de feu à [Montélimar, Marseille, Bordeaux...] , pouvez-vous confirmer? » Des dizaines, sinon des centaines de questions de ce genre nous ont été posées cette semaine, par des internautes sincèrement inquiets après avoir entendu telle ou telle rumeur. Nous avons tâché d'y répondre au mieux.

Ces fausses informations provenaient généralement d'échanges, notamment via des SMS qui ont circulé massivement, partout en France, toute la semaine. Emanant d'un « ami qui connaît quelqu'un à la DCRI » ou dans quelque haute sphère, ils préviennent d'un péril imminent à tel ou tel endroit. Nos lecteurs nous en ont envoyé une bonne demi-douzaine, à Toulouse, Marseille, etc. Tous faux, évidemment, mais tous emblématiques d'un pays apeuré, inquiet.

Evidemment, au-delà de la peur, la malveillance existe. Sur les réseaux sociaux, quelques irresponsables, mauvais plaisantins ou militants de telle ou telle cause, ont diffusé mensonges, rumeurs et propagande, avec parfois un certain succès. Ce sont, par exemple, des photos de militants du Hamas se réjouissant d'un cessez-le-feu en 2012, en les faisant passer pour une célébration des attentats à Paris vendredi, ou cet adolescent en mal de notoriété qui inventera samedi des perquisitions à Strasbourg, où il ne s'est rien passé, simplement pour voir combien de partages il va obtenir.

La recherche du « buzz », c'est aussi ce qui poussera certains à créer des comptes supposés aider des familles à retrouver leurs disparus, mais qui diffuseront parfois de fausses photos, ou des clichés de personnes décédées, avec un message nauséabond : « Un RT [un partage] = un soutien », dans l'idée d'obtenir un maximum d'influence, puis de changer le nom et l'objet du compte. Il y a enfin ces petites histoires, moins essentielles, mais significatives : cette citation par exemple, certes fort belle, attribuée à un éditorial du New York Times et très largement diffusée, y compris par des personnalités diverses, qui était en fait... un commentaire sur le site du journal américain.

Le souci de la source s'est ici effacé devant le besoin de partager, de commémorer, de communier. On en recensera plusieurs, de ce même type, histoires erronées ou déformées, mais partagées en toute bonne foi par des dizaines de milliers d'internautes.

Aider à faire le tri

Face à ces mensonges, il nous a semblé important de ne pas négliger les réseaux sociaux. Inlassablement, durant toute la semaine, nous avons donc chassé ces canulars, pour mettre en garde les utilisateurs. Nous avons aussi taché de donner quelques « bonnes pratiques » pour éviter de se faire piéger. Ce qui n'a évidemment pas suffi à empêcher les rumeurs, bonnes ou mauvaises, de circuler, mais a pu aider une partie des internautes à faire le tri.

Quelles leçons tirer de cet épisode? Sans doute que, si les réseaux sociaux transforment chacun d'entre nous en média, au sens de transmetteur de l'information, la responsabilité que cela peut impliquer n'est pas évidente pour tout le monde. Les réseaux virtuels ont des conséquences réelles. Et la presse aussi doit en tenir compte : on ne peut plus faire le pari de « ne pas nourrir le troll », d'ignorer la rumeur : nous ne sommes qu'un canal parmi des millions d'autres. Et notre rôle doit être aussi de certifier la fiabilité de l'information et de combattre la rumeur.

Paris attacks: Indonesia calls for more intelligence sharing, Financial Times

Ben Bland
Financial Times
2015 11 21

Kuala Lumpur—**Indonesia, the world's most populous Muslim-majority country, has called on nations to step up intelligence sharing following last week's terrorist attack in Paris.**

Speaking on the sidelines of a regional summit in Kuala Lumpur this weekend, Retno Marsudi, Indonesia's foreign minister, told the FT countries were not doing enough to share information about the global threat from militants linked to Isis.
On Sunday, US President Barack Obama will meet 17 Asia-Pacific leaders at the East Asia Summit to discuss a range of regional security issues including terrorism, migration and the South China Sea disputes.

"The [terrorist] threat is not only to Europe but to every country," said Ms Marsudi. "That is why during the meeting, Indonesia will make a call again on the importance of having co-operation on intelligence information."

She said some countries were not sharing as much intelligence as Indonesia would like and that Indonesia was willing to become more open in order to support the global effort against the Isis threat.

"It's a must for every country because this is not a one-country issue, it's a global issue."

The Paris attacks exposed gaps in intelligence sharing even within the EU, where there is significant pooling of sovereignty and links between security services are well developed.

Intelligence co-operation is even harder in Southeast Asia and other parts of the developing world, where governments are less co-ordinated and the principle of non-interference in other nations' domestic affairs is considered sacrosanct.

One diplomat gave the example of Turkey, which has been deporting foreigners suspected of trying to join Isis without explaining to the relevant governments what level of threat the individuals posed: misguided youths or terrorist masterminds.

Southeast Asia is increasingly concerned about the threat from jihadi fighters returning from Syria and Iraq with military training, funding and the ideological determination to carry out mass-scale terrorist attacks.

Indonesia's elite antiterrorism police unit — Detachment 88 — has neutralised much of the threat from the Islamist terrorists who executed a wave of deadly bombings in the early 2000s.

But terrorism analysts and government officials in Southeast Asia fear that the conflict in Syria could become a breeding ground for a new generation of militants, as has happened in Europe.

The Indonesian government believes about 400-500 of its citizens are fighting in Syria, a number that Ms Marsudi said was relatively small given that nearly 90 per cent of the country's 255m people are Muslims.

Najib Razak, the prime minister of Malaysia, another Muslim-majority country, told other Southeast Asian leaders on Saturday that they must do more to combat extremism.

But he said that the problem "requires new solutions" and cautioned against calls for renewed military action in the Middle East.

"Understandably, many will want to fight the so-called Islamic State out of the lands they have stolen from millions of Syrians and Iraqis," he said. "But a military solution alone will not be enough to defeat those who see peace, and want to cause war; those who see order and civilisation and wish for nothing but mayhem and death."

The war in the Middle East: Fighting near and far, The Economist

21 November 2015
The Economist

Islamic State may be lashing out abroad because it has been weakened nearer home; but it will still be hard to take down

"ENDURING and expanding": Islamic State's alliterative motto leaves out its burning desire to eradicate everything else, but otherwise sums up its ambitions pretty well. If IS has, in recent times, seemed more concerned with the enduring bit, its history shows that it has never long lost sight of expanding in any way possible: by capturing territory, by spawning offshoots far and wide, by inspiring new recruits, and by spreading fear. As a state with puny resources and no real friends, it needs to be a moving target.

It is not clear to what extent recent strikes by IS beyond the boundaries of the territory it has carved out of Syria and Iraq mark a change of course. Its various affiliates--some 36 groups around the world have declared allegiance to IS's secretive caliph, Abu Bakr al-Baghdadi--have been mounting terrorist attacks for some time (see chart). A recent survey by the New York Times estimated that these offshoots have killed perhaps 1,000 civilians since January via mosque bombings in Yemen, attacks on tourists in Tunisia and suicide-bombs in Ankara and Beirut (the figure excludes the murderous rampages of Boko Haram in Nigeria). The group has also encouraged "lone-wolf" acts by like-minded would-be terrorists. But the death toll over the past few weeks seems to take things to a new level.

It may be a coincidence that plots to murder hundreds in Paris, blow up an aircraft over Sinai and kill indiscriminately on the streets in Beirut all came to fruition so close together. They may have been long planned; similar attempts earlier may have been thwarted. But it may also be a considered response to challenges that IS faces closer to home.

Pentagon sources say that coalition air strikes killed 20,000 IS fighters in the 14 months after their onset in August 2014. That sounds over-optimistic. But it is certain that a number of commanders have been among the dead. The intense fighting at Kobane, a Kurdish enclave in northern Syria to which IS laid siege last September, eventually being driven back by heavy air strikes in December, is thought to have cost it 2,000 men. An IS defector told Michael Weiss, an American journalist, that the losses were at least twice that, and that tightening of the Turkish border had made it harder for IS to replace fallen fighters. He said it was partly in response to this that IS turned to attacks on the "far enemy". Single, dramatic attacks are an immense force-multiplier in propaganda terms.

Losses on the scale of Kobane are doubtless a blow but not, alas, a fatal one. Estimates of the group's military manpower range from about 30,000 (America's Central Intelligence Agency) to about 100,000 (Hisham al-Hashimi, an Iraqi security expert). Mr Hashimi reckons about 20% are foreign-born, a similar figure to that given in UN papers.

Factor into these figures the fact that IS fighters seem a lot more effective than those who oppose them. When the Iraqi city of Tikrit was recaptured last April, it took 30,000 soldiers from the Iraqi army and associated Shia militias to overcome 1,000 IS fighters. When IS took the Iraqi city of Ramadi, its forces were outnumbered ten to one by the defenders.

A willingness to use kamikaze tactics is definitely part of what gives IS forces an edge; but they are also innovative, well-drilled and better led than many of those they face. In April IS used a drone to record its troops taking an oil refinery and distributed the footage on the internet. A former American Green Beret, quoted by McClatchy, a news service, said the attackers showed "quiet tactical confidence: correct movement, intervals, fire discipline".

Fighting well is not enough

Despite these impressive fighters, IS has recently been losing ground, largely because its adversaries have air power. Kurdish forces captured Sinjar in Iraq, along with adjacent territory in Syria, and IS forces are being pushed back elsewhere in Iraq, too. With help from Russian aircraft and Iranian-backed militias, Syrian government forces recently relieved an airbase near Aleppo to which IS had long laid siege. Following the deaths of 224 Russians in the Metrojet airliner bombing of October 31st, Russia may now be targeting IS in preference to other enemies of President Bashar Assad's regime.

Yet IS endures. Indeed its territory remains one of the safer parts of Syria: aid officials in Turkey say that in September and October as many as 70,000 civilians fled to Islamic State from the province of Homs. Coalition bombing in the caliphate is much less indiscriminate than that of the Russian and Syrian air forces elsewhere. What is more, food is cheaper and there is justice of a sort. There is also a functioning economy, largely thanks to an estimated 20,000-30,000 barrels of oil pumped daily from captured fields in eastern Syria and northern Iraq.

Its dependence on oil revenues--they provide around $50m a month, according to investigative reporting by the Financial Times--is just one way in which IS looks more like an old-fashioned Arab dictatorship than a new Islamic Utopia. It doles out alms to the poor in exchange for total obedience. It promotes a cult of personality around Mr Baghdadi. It churns out turgid propaganda about repaired bridges and newly opened schools. Like all the region's successful autocracies, it has created multiple and mutually suspicious security services, the better to stave off coups.

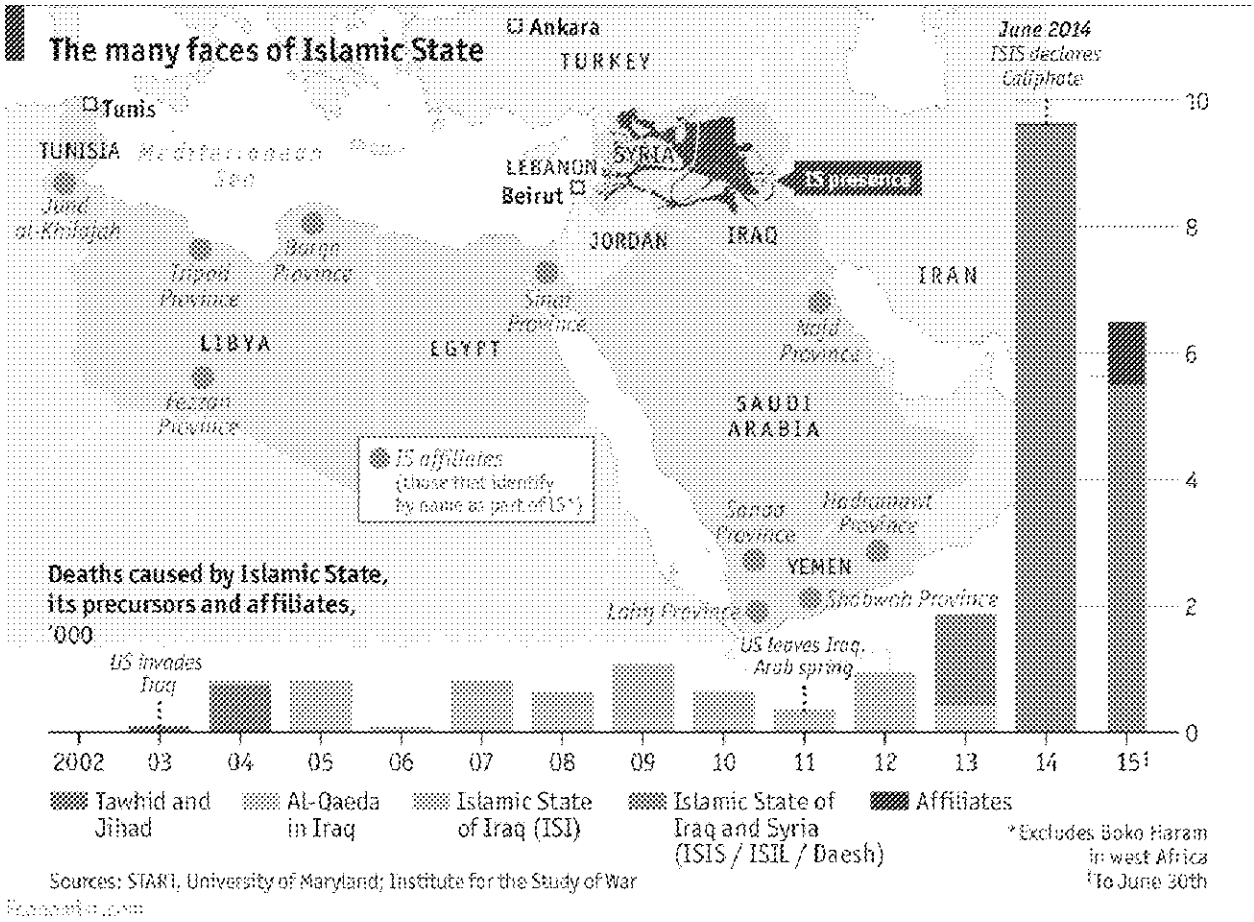
In the wake of the Paris attacks, military action aimed at denying IS its territorial base seem likely. The firepower available to IS's enemies dwarfs all that it can muster. In an interview with the BBC, the security chief of Iraq's Kurdish region reckoned that, given the necessary will, the job could be done in months or even weeks. France has already ramped up its aerial attacks and Russia, now fielding heavy bombers, says it will double the number of daily sorties. American aircraft are attacking new targets in the group's oil infrastructure. Recent strikes, preceded by warnings for civilians to escape, have destroyed hundreds of tanker trucks. America has also boosted supplies to Kurdish and other Syrian rebel forces on the IS frontlines.

The area IS controls seems likely to shrink under such pressure. But the capture of large cities like Raqqa and Mosul will require a far bigger effort on the ground. And as Sinjar and Kobane have shown, the cost will be high: both those towns now lie in ruins. The challenge is not just the diplomatic and military one of mustering, motivating, co-ordinating and deploying sufficient forces, huge though that is. It is also humanitarian: such action is likely to displace still more desperate refugees, and leave them little to return to.

The Western powers and Russia are not keen to send troops. They are even less keen to be left holding ravaged and probably hostile territory. Iraq's forces are overstretched and deeply distrusted by many of the Sunnis they would liberate; many prefer the rule of IS to that of Shia militias. Syria's forces are exhausted, overstretched and loyal to a regime responsible for war crimes. Local powers such as Iran, Turkey, the Kurds and Saudi Arabia have a range of conflicting agendas; eliminating IS is at the top of none of them.

There is progress to be made that does not need boots on the streets of Raqqa. Better police work can help; it is already producing results in Turkey, which has rounded up several cells in recent weeks. Improved planning and communication between anti-IS forces in the field would help, too. Trust, lamentably absent today, must be built.

Breaking up the would-be caliphate militarily would destroy the aura of invincibility which constitutes a large part of its attraction. But successor groups, and even more, IS's ideology, will endure for as long as the poisonous swamp it inhabits persists. A partial list of its ingredients includes a hyped-up sense of Sunni victimhood, indoctrination by xenophobic Wahhabists, the dismal anomie and yearning for heroism of some young urban Muslims in Europe and elsewhere, and the rage generated by brutal and repressive regimes such as Syria's. It has pooled and festered across the band of collapsed and failing states that stretches from Algeria to Pakistan. It will take more than a hot sun, or heavy firepower, to make it evaporate.



Le rôle déterminant du Maroc dans la localisation d'Abaaoud, France 24

France 24
2015 11 20

À l'occasion de la visite du roi Mohamed VI à Paris, vendredi, François Hollande a remercié le Maroc pour "l'assistance efficace" qu'il a apporté à la France en l'aidant à repérer la présence, sur son territoire, d'Abdelhamid Abaaoud.

François Hollande a vivement remercié le roi Mohamed VI en visite à Paris, vendredi 20 novembre, pour le rôle crucial des services de renseignement marocains dans l'enquête sur les attaques à Paris.

C'est en effet Rabat qui a permis aux services antiterroristes parisiens de se mettre sur la piste d'Abaaoud sur le territoire français et contribué à déclencher l'opération à Saint-Denis. C'est aussi le royaume chérifien qui aurait orienté les enquêteurs français sur la piste belge.

Le renseignement marocain appelé à l'aide

Dès mercredi matin, le site marocain Le360.ma, l'affirmait : "Ce sont les services de renseignement marocains qui ont réussi à localiser les terroristes retranchés dans un

appartement de Saint-Denis". Le site précisait : "Au lendemain des attentats qui avaient ensanglanté la capitale française, et sur demande des autorités françaises et belges, des officiers des renseignements marocains s'étaient rendus à Paris et Bruxelles pour aider dans les investigations en cours. Et déjà cette collaboration donne ses fruits avec l'opération menée ce (mercredi) matin."

Le mois dernier en effet, les services marocains ont arrêté un jeune frère du djihadiste, Yassine Abaaoud, alors que l'avion à bord duquel il se trouvait venait d'atterrir à Agadir, a indiqué vendredi une source marocaine à Reuters. Dès qu'elle a été informée de la présence d'Abdelhamid Abaaoud en France, la Direction générale de la sécurité intérieure (DGSI) a suivi les écoutes d'Hasna Ait Boulahcen, présentée comme sa cousine, explique-t-on de source policière.

La jeune femme d'origine marocaine de 26 ans, qui a été tuée mercredi avec Abaaoud lors de l'assaut des forces de l'ordre, était déjà surveillée par la police judiciaire (PJ) de Seine-Saint-Denis, pour trafic de stupéfiants. "Dès que l'information est tombée via le Maroc, la PJ de Seine-Saint-Denis a transmis à la DGSI ses informations, les correspondants d'Hasna Ait Boulahcen, les bornes téléphoniques, ses points de chute", explique la source policière.

"Surveillance physique"

Les écoutes ont permis d'entendre une conversation dans laquelle Hasna Ait Boulahcen faisait état de la présence d'Abaaoud, un Belge d'origine marocaine de 28 ans, selon une autre source policière. "Il y a eu ensuite une surveillance physique qui a permis de déterminer que la jeune femme et le djihadiste se sont présentés dans l'immeuble de la rue Corbillon à Saint-Denis mardi en début de soirée", explique-t-elle.

La Sous-direction anti-terroriste (SDAT) ayant l'assurance que la "cible" se trouvait dans l'immeuble, décision a été prise de donner l'assaut mercredi au petit matin, d'autant que le groupe était soupçonné de préparer une nouvelle attaque jeudi.

Les autorités françaises ont aussi indiqué cette semaine avoir bénéficié d'une information de la Turquie pour localiser Abdelhamid Abaaoud, le situant en Grèce.

After Paris attack, safety vs. liberties, New York Times

Rattled countries tilt toward bolder security, starting rights debate
By STEVEN ERLANGER and KIMIKO DE FREYTAS-TAMURA
21 November 2015
New York Times

Shocked by the carnage of the Paris attacks, France and Belgium moved aggressively to strengthen the hand of their security forces, pushing Europe more deeply into a debate that has raged in the United States since Sept. 11, 2001: how to balance counterterrorism efforts and civil liberties.

With their populations stunned and nervous, and political pressure growing on the right, the French and Belgian governments made it clear on Thursday that, for now, they would put protecting their citizens ahead of other considerations.

With time, the United States has moved to ease some elements of the U.S.A. Patriot Act, passed in the aftermath of the Sept. 11 attacks. It has also strengthened oversight of intelligence agencies and of mass domestic surveillance in the wake of the revelations by Edward J. Snowden, the former contractor for the National Security Agency who leaked documents about surveillance.

But European nations battered by terrorism are moving in the other direction. Those nations include France, which has suffered multiple attacks this year; Belgium, where many of the Paris attackers lived or grew up; and Britain, which has thwarted a number of plots in recent years. Each is updating and strengthening government power while debating further controls over passport-free travel within Europe.

Since the Nov. 13 attacks on Paris, France has aggressively used emergency powers, for example, to round up potential terrorism suspects across the country in an effort to disrupt any further plots.

Finding the right balance between individual rights and antiterrorism measures has grown more complex in the 14 years since the United States was struck by Al Qaeda, in part because of the pervasiveness of digital technology and the ensuing questions about personal privacy. But in the days after the Paris attacks, there has been relatively little reflection about the trade-offs as the nations most affected — France and Belgium — rushed to put new security measures in place and alter their legal and constitutional structures to give government more flexibility in dealing with threats.

As Prime Minister Manuel Valls of France warned darkly on Thursday of the possibility of chemical and biological attacks, France's National Assembly voted, 551 to 6 with one abstention, to extend for three months a national state of emergency imposed after the attacks in Paris by the Islamic State, which killed 129 people and wounded 352.

"The state of emergency, it's true, justifies certain temporary restrictions on liberties," Mr. Valls said. "But resorting to this, it's to give us every chance to fully restore these liberties."

In Belgium, Prime Minister Charles Michel said he would rush through legal changes to make it easier to capture, try and punish terrorism suspects operating there. He also said he would seek constitutional changes to extend the length of time suspects can be held by the police without the filing of charges to 72 hours, from 24.

His plan calls for the imprisonment of jihadists returning to Belgium from overseas, and would require anyone deemed a threat to wear an ankle bracelet. The plan would also ban the anonymous sale of telephone SIM cards that allow terrorists to hide their identities; would remove restrictions on what times of day the police are permitted to conduct raids on terrorism suspects; and would allow the authorities to arrest or expel religious figures "who preach hatred."

Mr. Michel also wants to require all passengers traveling on high-speed trains as well as airplanes to register their identities before departure.

Jan Techau, the director of Carnegie Europe, a research organization based in Brussels, said he saw the reactions as natural. "The home front is the field of political activity now — it will all be about homeland security," he said. "There is a sense that the authorities are no longer in control, and it's a clear attempt by authorities to regain some trust."

But advocates for civil liberties warned against governments going too far, and suggested that European nations had to be particularly careful that the measures they were taking were not aimed at one class of citizens: Muslims.

Officials at Human Rights Watch in Belgium cautioned on Thursday that the authorities should ensure such measures did not lead to indiscriminate roundups or unnecessary restrictions on freedom of speech, movement and religion.

"Like every nation, Belgium has a responsibility to protect its people from attacks, but it should not trample basic rights in the process," said Letta Tayler, a senior terrorism and counterterrorism researcher at Human Rights Watch. "Whenever a country is attacked or threatened, there is a danger that governments will overreact in an effort to make people secure."

The French emergency bill, which the French Senate was expected to approve on Friday, extends the powers of a 1955 emergency law to allow the dissolution of radical groups running mosques and other places of prayer; the blocking of websites and social media that glorify or incite terrorism; and the use, in certain cases, of electronic tagging for those placed under house arrest.

It is the first time since the 1955 law was passed that a national state of emergency has been declared. France is already being patrolled by heavily armed soldiers, and now police officers who are off duty will be allowed to carry firearms and use them if they wear an armband identifying themselves as police.

On Wednesday, the French authorities said they had carried out over 414 raids across the country, arrested 64 people and placed 118 under house arrest.

Under the emergency, the authorities are permitted to conduct raids and make arrests without first obtaining a warrant. But as soon as someone is arrested or property is seized, the regular legal system kicks in. Suspects in terrorism cases are already allowed to be held without charge for up to six days.

In the United States, even in the immediate aftermath of Sept. 11, raids on that scale would have created a storm of criticism, but the French, only 10 months after Islamist radicals attacked the newspaper Charlie Hebdo and a kosher supermarket, have generally accepted the crackdown as necessary.

President François Hollande has also called for enshrining the state of emergency law in France's Constitution, making it easier to declare such a state for longer periods of time without resorting to the more drastic options currently available in the Constitution.

Mr. Hollande also wants to make it easier to expel foreigners deemed to be a security threat; to revoke the French nationality of dual citizens, even those born in France, if they are convicted of terrorism-related offenses; and to close radical mosques.

France had already moved last summer to strengthen and modernize laws governing electronic surveillance after the attacks in January. Laws passed by large majorities gave broad legal authority for the state to snoop on citizens.

In Belgium, the call for broad new powers came after the government was stung by criticism that it had failed to act aggressively enough to identify and stop plots being planned on its soil. Mr. Michel also vowed a crackdown on Molenbeek, the Brussels district that has bred so many jihadists and harbored others.

As in France, many Belgians said that while the measures were drastic, they were prepared to give up some of their personal freedoms in return for security.

Belgium has been so shaken by the Paris attacks that there is a broad agreement that something needs to be done, said Steven Blockmans, an analyst at the Center for European Policy Studies based in Brussels. There is a consensus about the need to strengthen law enforcement, intelligence agencies and local governments, he said.

Mr. Michel's moves are a partial vindication for the right-wing New Flemish Alliance, which has been calling for these measures for years, Mr. Blockmans said. The interior minister, Jan Jambon, who is a member of the party, recently said that Molenbeek needed to be "flushed out."

Belgium has looser gun control laws than France but stricter controls on surveillance, which the new measures would loosen. For example, the authorities can intercept telephone conversations only if there is a strong suspicion that the targets are terrorists, said Jelle Van Buuren, a lecturer in counterterrorism at Leiden University. The surveillance cannot be extended to people who may be accomplices, he said.

Bart Tommelein, Belgium's federal secretary in charge of privacy, said that the restrictions on privacy would only apply to terrorism suspects.

"If we are talking about suspected terrorists and people who have committed such crimes, then privacy doesn't exist," he said. "So for people who go to Syria, or return from Syria, that border can be crossed, they lose that right," but others will not.

It was not the government's intention to "put everyone in a database, but to target and put people suspected of engaging in terrorist activity in a database," he said, and he insisted, "We won't place security above freedom."

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
October 6, 2015 / le 6 octobre 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Appuis discrets malgré de bonnes finances
L'aéroport de Québec ne réclame plus de subvention pour la construction d'un centre de prédédouanement américain, en plus de promettre des retombées économiques appréciables. Le président et chef de la direction, Gaëtan Gagné, se demande donc pourquoi les appuis sont si difficiles à aller chercher en pleine campagne électorale. Dans son bureau avec vue sur les pistes, M. Gagné explique au Soleil les avantages d'un tel équipement. Les passagers, qui franchissent les douanes américaines au départ plutôt qu'à l'arrivée ou en escale, épargnent surtout du temps. Une fois aux États-Unis, ils peuvent récupérer rapidement leurs bagages ou prendre une correspondance sans autre embêtement. Les voyageurs devraient aussi avoir accès à de nouvelles liaisons, plaide le président d'Aéroport de Québec inc., la société privée qui gère l'aéroport international Jean-Lesage. Les transporteurs pourront en effet se rendre directement dans des aéroports sans poste de dédouanement puisque leurs passagers auront déjà reçu l'autorisation d'entrer aux États-Unis. Fini le détour par New York ou un autre grand aéroport seulement pour passer les douanes... Québec pensait que c'était acquis puisque son nom figurait sur la courte liste des aéroports où ajouter des «points de précontrôle», selon le jargon utilisé dans un accord entre le Canada et les États-Unis datant de 1995 et renouvelé en 2001. Or, une nouvelle version signée en mars dernier par le conservateur **Steven Blaney, ministre de la Sécurité publique** et député de Lévis, ne fait plus référence aux villes à desservir en priorité. Il faut dire que seules Québec et London (Ontario) n'ont toujours pas l'équipement tant désiré. Pour Gaëtan Gagné, cette omission est inquiétante. «Québec se retrouve pénalisée parce qu'on n'a pas suivi l'ancien protocole. [...] C'est comme si on avait décidé de fermer le marché du prédédouanement, ça n'a pas de sens», expose-t-il. Le gestionnaire poursuit en disant qu'«il faut que les politiciens décident que ça va

marcher». Il y va du développement de la région de Québec, selon lui. Le gouvernement du Québec l'a compris et a nommé vendredi dernier l'ex-ambassadeur Raymond Chrétien afin qu'il convainque les Américains - et les Canadiens - de la pertinence de la candidature de Québec. Le maire Régis Labeaume rame dans le même sens. Il a inclus le centre de prédédouanement dans ses priorités pour la campagne électorale fédérale. Jusqu'à maintenant, le Bloc québécois et le Nouveau Parti démocratique (NPD) ont appuyé l'initiative. Le Parti libéral et le Parti conservateur se font tirer l'oreille. M. Gagné en est à se demander s'il ne faudrait pas demander une subvention. «C'est un peu moins glamour pour les politiciens, peut-être, de dire qu'il n'y a pas d'argent qui va avec ça. Mais l'autorisation, ça nous suffit.» Au bureau du **ministre de la Sécurité publique**, on souligne que ***l'entente a été déposée à la Chambre des communes et doit encore être étudiée avant d'être ratifiée. Pour les nouveaux points de précontrôle, toutes les villes canadiennes seraient toutefois sur le même pied d'égalité. «Ce n'est pas un signal ou un non-signal»,*** nous a-t-on fait valoir. Le Soleil, 10/Front

«Je n'en espérais pas tant»
Lorsqu'on lui fait remarquer qu'il a connu une ascension fulgurante dans le gouvernement Harper, **Steven Blaney** secoue la tête. «Je ne pense pas que le mot fulgurant est approprié», corrige-t-il, admettant tout de même être surpris par sa trajectoire en politique. «Je n'en espérais pas tant.» Le candidat conservateur dans Bellechasse-Les Etchemins-Lévis a connu une année occupée qui a confirmé son ascension, de simple député au poste névralgique de **ministre de la Sécurité publique**. Avant le déclenchement hâtif des élections, c'est lui qui a été chargé d'articuler la réponse du gouvernement Harper aux attentats d'Ottawa et de Saint-Jean-sur-Richelieu. Les élections du 19 octobre surviendront d'ailleurs presque un an jour pour jour après la fusillade dans le Parlement fédéral. Le projet de loi C-51 a placé **Steven Blaney** sous le feu des projecteurs comme jamais auparavant. Aux Communes, devant la presse, il a martelé sans broncher le message conservateur, allant jusqu'à invoquer l'Holocauste pour justifier qu'on étende les pouvoirs des agences de surveillance. Finalement, cette question délicate pour le gouvernement conservateur est pratiquement absente des débats de la campagne fédérale. D'ailleurs, le Parti libéral a appuyé le projet de loi. ***«Ç'a été le plus grand défi de ma vie»*, relate Steven Blaney** en revenant sur la dernière année. La Presse, A5

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

***Belleisle rebounds after being hammered by rain**
Belleisle schools have reopened for those who can actually get to class. Anglophone School District South Supt. Zoe Watson says for those who cannot get to school, they have an excuse that won't be questioned. Both Belleisle Elementary School and Belleisle Regional High School were closed Oct. 1 and 2 after a rainstorm hammered the region, wiping out millions of dollars in infrastructure. Bridges and roads were destroyed making several in the region inaccessible. But as the community encompassing Belleisle, Springfield and Hatfield Point pulls together, there is a lot to be said about its resilience, says Aaron Law of Kars. "Great co-operation, compassion and camaraderie amongst friends and neighbours" is seeing the tight-knit community through, he said. Telegraph-Journal, B3

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Exiled spy kids battle to reclaim their citizenship
It's the stuff of a gripping spy thriller - international intrigue, stolen identities, even a mail-order diaper business. But for two brothers who were stripped of their Canadian citizenship when their parents were unmasked as Russian spies, none of that is important. The only thing that matters to them is the return of what they see as their birthright: their citizenship. Former Toronto residents Alexander Vavilov, 21, and his older brother, Timothy, 25, are in the midst of a legal battle to get their citizenship back, arguing they shouldn't be penalized for the sins of their parents. "It is not fair to punish us for something we have nothing to do with. We have done nothing wrong," Alexander Vavilov told the Star in an exclusive interview from an undisclosed city in Europe, where he is studying for an undergraduate degree (...) Alexander and Timothy have never been in trouble with the law, though it's a different story for their parents - Andrey Bezrukov and Elena Vavilova - who acquired their new personas by stealing the

identities of two dead Canadians, Donald Heathfield and Tracey Ann Foley. Ottawa would not even have been aware of the identity theft if FBI agents had not arrested them in 2010 for espionage in the United States, where the family lived for 11 years before they were booted out and deported to Moscow in a spy swap. Toronto Star, A1

Toronto 18 boss loses parole appeal
A leader of the Toronto 18 terrorist group has lost his appeal of a parole board decision that concluded he wasn't yet ready to be released from prison. The board's decision was fair and reasonable, the appeals panel ruled in the case of Fahim Ahmad, who organized a paramilitary training camp north of Toronto and plotted to attack the Parliament buildings and behead MPs in 2006. The decision was "based on relevant, reliable and persuasive information," the appeal division wrote in a five-page decision that cited the "gravity" of Ahmad's offences and "lack of a release plan," among other factors. Ahmad was the leader of one of two factions of the al-Qaidainspired Toronto 18. The leader of the second faction, Zakaria Amara, last month became the first Canadian terrorist to lose his citizenship under a controversial new law. At least five other Toronto 18 members have been notified they may also lose their citizenship under the law, which applies to dual nationals convicted of terrorism offences. Ahmad's lawyer said last week his client was not among those who had received such a notice. National Post, A6

Privacy breach possible in loss of citizenship
Federal officials are investigating an apparent privacy breach involving an imprisoned terrorist who was stripped of his citizenship. Zakaria Amara's receipt of a government letter informing him he no longer held Canadian citizenship was promptly reported in the media late last month and soon after confirmed by a Conservative cabinet minister in the middle of a closely fought election campaign. The issue quickly reignited campaign trail debate about new provisions that allow the government to revoke a terrorist's Canadian citizenship as long as the person has nationality elsewhere. However, Citizenship and Immigration Canada is refusing to release a copy of the letter to Amara "due to privacy considerations," said department spokesman Rémi Larivière. As for the public disclosure of the revocation, Larivière said the department "takes privacy matters seriously and has procedures in place to protect personal information." "Within the department, we will be looking into the matter according to normal procedures." Canadian Press (Times Colonist, B6; *Whitehorse Daily Star)

The 1970 October crisis: Questions still remain
The majestic home at 1297 Redpath Crescent in Montreal looks much like it did 45 years ago, its arched wooden door a gateway to the tony Golden Square Mile, once a bastion of Montreal's English speaking elite. Nestled at the foot of Mount Royal and located on a cul-de-sac, the classic stone manor remains a landmark of the October Crisis of 1970, a turbulent chapter in the history of Quebec and Canada that still stirs political passions and jars our collective memory nearly a half-century later. Then, more so than now, Quebec's place in Canada was unsettled. But the events of October 1970, which culminated in two highprofile kidnappings and the grisly murder of provincial cabinet minister Pierre Laporte by Front de libération du Québec (FLQ) terrorists shocked Quebecers of all political leanings at the time, and contributed to the loss of support for violent means to attain the political goal of Quebec independence (…) Forty-five years later, we are still left with unanswered questions about who actually killed Laporte and the role of Hamer, the lone anglophone who participated in the Cross kidnapping but was never brought to justice until his identity emerged publicly almost a decade later. (He was arrested in 1980, and sentenced the next year to 12 months in jail after pleading guilty for his role in the kidnapping.) But given the lay of Quebec politics, we may never find out the truth. "As long as there is an independent, federalist divide in Quebec, as long as Quebec politics is structured around this, you're not going to have an honest reckoning of what happened," Bélanger said. Montreal Gazette, A4

*** Programme - Violence conjugale et malbouffe au menu des libéraux: Les modifications à la loi antiterroriste C-51 sont enfin connues**
Le Parti libéral a divulgué sa plateforme électorale complète lundi, levant ainsi le voile sur les quelques éléments du programme de Justin Trudeau qui n'étaient pas encore connus. La lutte contre les gras trans et la malbouffe est au menu, tout comme le renversement du fardeau de la preuve pour la remise en liberté des récidivistes en matière de violence conjugale. Les changements envisagés à la loi antiterroriste sont aussi enfin connus (…) La plateforme explique aussi comment le Parti libéral

modifierait la loi antiterroriste C-51, pour l'appui de laquelle il a été vertement critiqué. Ainsi, pas question d'abolir les nouveaux super-pouvoirs de " perturbation " accordés aux espions canadiens. Les libéraux s'engagent seulement à garantir que tous les mandats obtenus par les agents du Service canadien du renseignement de sécurité (SCRS) soient conformes à la Charte canadienne des droits et libertés. On se rappellera que le C-51 a accordé au SCRS le pouvoir d'enfreindre la loi dans ses " perturbations " moyennant l'obtention de l'aval d'un juge. Le Devoir, A2

* **The big hole in Harper's policy on terror**
An opinion piece states "Stephen Harper and the Conservative government continually argue that terrorist organizations in the Middle East, notably ISIS, are a threat to Canadians at home. Their belief in this is so strong that they are willing to spend millions of dollars and risk the lives of Canadian military by participating in bombing and training missions in Iraq and Syria. Assuming this is true, apart from the moral issue of depriving people of their citizenship, how does he justify supporting terrorist organizations by providing new recruits?" Hamilton Spectator, A14

* **'Deport them'**
An open letter to the National Post states, "(…) I applaud the government's efforts to strip the citizenship of convicted terrorists. We should widen the scope of this law to include heinous crimes such as rape and murder. Canadians have the right to fulfil their ambitions in a peaceful and secure environment. Their lives should not be threatened by criminals who lurk in the shadows. Convicted criminals should be deported to their country of origin so that the lives of Canadians are not jeopardized by their menacing presence on Canadian soil. Revoking someone's citizenship only applies to dual citizens who have violated their oath to this country by committing a crime against the well-being of the population. Since there is no death penalty in Canada, the only way to get rid of these criminals is to deport them." National Post, A9

* **Dog-whistle politics**
An open letter to the National Post states "Calgary Mayor Naheed Nenshi doesn't like the dog whistles in the federal election campaign. Who is whistling and who are the dogs? (…) Dog whistles cannot be heard by ordinary people, as their ultrasonic waves are too high frequency for the human ear to detect. Dogs can hear them though, and so the dog whistle signals the dogs in a way that other people cannot hear. So, to take the example that greatly exercised Mayor Nenshi - whose rhetorical style blanches from anything so discreet as a lowly whistle when a bullhorn may be at hand - the prime minister is blowing his dog whistle on refugees. Prime Minister Stephen Harper says that refugee resettlement must respect the requirements of national security. That's the part ordinary people can hear. But there is another part that only the dogs can hear - namely that we have to be careful about these refugees because they are Arab and Muslim. The "dogs" are those animated by sundry bigotries; they don't like Arabs and Muslims." National Post, A9

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Norcal group grows its airport relationship
Calgary has become an important international hub specializing in receiving, transferring, storing and distributing air, rail and highway cargo. The Calgary Airport Authority continues to offer land lease development opportunities at both Calgary International Airport and Springbank Airport. More than 320 hectares of land are under lease and long-term plans envision future development that will add another 80 to 120 hectares to the city's industrial land base... Norcal managing broker Kevin Deeks says Norcal Centre, designed by Form 3 Designs, is located close to the Canada Border Services Agency and private jet hangers making it an ideal building for customs brokers, freight forwarders, a business centre and other airport related companies. Postmedia Network (Calgary Herarld, C2)

«Bon pour le Québec», dit Daoust
Certains producteurs agricoles québécois subiront les conséquences d'un nouvel accord commercial, mais son impact sera globalement positif pour l'économie québécoise, a déclaré lundi le ministre de

l'Économie, Jacques Daoust. M. Daoust a affirmé que les industries québécoises dans le secteur de l'aéronautique, du bois, des pâtes et papier ainsi que des métaux profiteront de la disparition progressive de droits de douane grâce au Partenariat transpacifique (PTP)... Le ministre a évoqué un resserrement des contrôles douaniers sur les substituts du lait, une interdiction formelle aux importations de lait produit avec des hormones de croissance, ainsi qu'une compensation adéquate des dommages subis à cause du PTP. Presse Canadienne (Le Quotidien, 21/Front); Le Soleil, 25/Front

Autres réactions au PTP

L'Union des producteurs agricoles (UPA) dénonce l'entente qui touche de plein fouet les producteurs laitiers, d'oeufs et de volailles. «Il est déplorable que les productions sous gestion de l'offre représentant 43% des revenus agricoles québécois fassent les frais de l'accession du Canada au Partenariat transpacifique (PTP)», souligne par voie de communiqué le président, Marcel Groleau. Ce dernier réclame maintenant la mise en place de mesures concrètes pour assurer un contrôle rigoureux des frontières et le respect intégral des normes de composition fromagère. «C'est la seule manière d'assurer une gestion de l'offre efficace et fonctionnelle pour l'avenir. L'UPA s'attend à ce que le gouvernement fédéral prenne sans délai les mesures qui s'imposent», ajoute M. Groleau. Le Quotidien, 7/Front

Qui sont les gagnants au Québec?

Le Canada et 11 pays se sont entendus sur le Partenariat transpacifique (PTP). Pour le Québec, l'intérêt de ce traité de libre-échange est notamment d'ouvrir les frontières du Japon, un pays développé de 127 millions de personnes qui maintient des tarifs élevés sur les produits agricoles et les biens manufacturés. En contrepartie, Québec subira la concurrence de pays dont la main-d'oeuvre est bon marché, comme le Viêtnam. Qui seront les gagnants et les perdants? Avec le PTP, le Canada reste sur le même pied que les Américains en ce qui a trait à l'accès au marché du Japon. «La réaction dans l'industrie est unanime», dit Jacques Létourneau, président de Canada Porc international. Le tarif de 4,3 % sera progressivement éliminé. Le Québec rattrapera ainsi deux pays du PTP, le Mexique et le Chili, qui profitaient d'un traitement préférentiel. De grands exportateurs porcins, le Brésil et le Danemark, deviennent désavantagés, puisqu'ils ne sont pas signataires du Partenariat. Le Canada a exporté 2,3 milliards $ en 2014 vers les marchés du PTP, dont 41 % à destination du Japon. Le Québec est le deuxième producteur de porc au pays. Le bois et les produits forestiers sont frappés de taux pouvant atteindre 10 % au Japon, 31 % au Viêtnam, voire 40 % en Malaisie. Les exportations canadiennes de bois et de produits forestiers atteignent 20,4 milliards par an. Le Québec produit 32 % des pâtes et papiers au Canada et arrive derrière la Colombie-Britannique pour le bois. Le Canada exporte pour 22 milliards $, «et ce chiffre est appelé à augmenter grâce à la nouvelle entente», s'est réjoui l'Association des produits forestiers du Canada (APFC) dans un communiqué. La Presse (Le Soleil, 24,25/Front); La Presse Canadienne (Le Soleil, 23/Front, La Presse, Le Devoir)

Twelve countries reach tentative Trans-Pacific trade deal

Twelve nations, including Canada, have reached a tentative deal on a massive Pacific Rim trading bloc billed as the largest-ever deal of its kind, with implications for hundreds of millions of people, hundreds of products and industries, and for long-term relationships between countries on four continents. After five days of marathon, aroundthe-clock negotiations, a deal was announced Monday to create the Trans-Pacific Partnership -- which would start by covering 40 per cent of the world's economy, with participants predicting it would become the building block for future trade deals. "Today is a historic day, it is a great day for Canada, it is a great day for Canadians," Prime Minister Stephen Harper beamed during a news conference Monday in Ottawa. "With this agreement, the largest economic partnership in the history of the world, Canadian exporters will gain nearly tariff-free access to almost 800 million customers in the Asia-Pacific region... including - crucially for us - Japan."... There's a major discrepancy between Canada and the U.S. on tariff-elimination for cheaper Asian parts - - with a five-times-faster phase-out north of the border, five years compared with the U.S.'s 25 years. In addition, both countries will see a 17.5-per-cent drop in the amount of regional content required in cars to avoid a tariff, compared with NAFTA. Canadian Press (Red Deer Advocate, A1, Times Colonist, B1/Front); Postmedia News (Ottawa Citizen, A1/Front); Postmedia News (National Post, A1, Chronicle Herald, Times Colonist , Calgary Herald)

Deal may signal 'slow erosion' of dairy supply management system

Canada is opening the taps to dairy from foreign competitors as part of the Trans-Pacific Partnership deal and though the new imports may just seem like a trickle right now, some say the leak could mean the beginning of the end for supply management. Details of the TPP released Monday include allotting 3.25 per cent of annual production to foreign dairy products entering Canada, to be phased in over the next five years with an increase in exports from the 11 other TPP countries that will annually displace about 250 million litres of Canadian milk. "There seems to be this slow erosion of our supply management principals, which is really based on one premise: producing what we need domestically, and that's it," said Sylvain Charlebois, a professor at the University of Guelph's Food Institute. "This gives dairy farmers the opportunity to shift their model in order to compete in the global market place, which is something they've never had to do before." The current supply management system controls levels of milk production by tying it to Canadian consumer demand and limiting foreign competition through high tariffs. Postmedia News (StarPhoenix, D1/Front; Montreal Gazette, Calgary Herald, Charlottetown Guardian); Globe and Mail, A1/FRONT; Montreal Gazette, A15

*** Will Canadians walk through the door to the Pacific?**
Canada's signature on Monday's sweeping trade deal will open a door for companies to expand deeper into the Asia-Pacific region - but it remains to be seen how many will actually walk through it. With the world's largest economy right next door, Canada's business community has had good reason to remain focused on the fish-in-a-barrel opportunities offered by the United States market. So, will Canada's participation in the Trans-Pacific Partnership - a 12-country pact billed as covering 40 per cent of the global economy - encourage Canadian companies to finally step out of their North American comfort zone? "It's so easy for Canadian firms to just walk across the border," said Ian Lee, an economics professor at Carleton University's Sprott School of Business in Ottawa. Toronto Star (Record, C1)

Bridge fixed on building new truck plaza
An ongoing project to upgrade the Ambassador Bridge includes the construction of a controversial on-site truck inspection plaza, the company revealed in a written statement Monday. The city has for years blocked the proposed plaza at the foot of the bridge on Windsor's west side because it requires closing streets in the area - including a section of Huron Church Road - and could have a significant impact on the surrounding neighbourhood. "They don't have permission," said Windsor Mayor Drew Dilkens. "We've had no discussion whatsoever with the Ambassador Bridge with respect to adding a commercial inspection plaza to their current facility." Should it be built, the plaza would be located west of Huron Church Road. "There are a lot of approvals required before they could ever move forward with that type of work," Dilkens said. "I'm not aware they have approvals from any of the various bodies required before they can move forward." Secondary truck inspection by the Canada Border Services Agency is currently done two kilometres south of the bridge at a large site off Malden Road. Postmedia (Windsor Star, A1/FRONT)

*** B.C. wife, husband 'stuck' after IRA-related refugee claim turned down**
A former British soldier married to a disabled Canadian woman may be forced to leave their Victoria home for the United Kingdom after a series of missteps and a snarl of red tape. John Collins, 62, first made an application for refugee status when he entered Canada, based on alleged harassment in the U.K. by a member of the Irish Republican Army. The application was denied and he's been ordered to leave by the Immigration and Refugee Board... Citizenship and Immigration Canada, the Immigration and Refugee Board and Canada Border Services Agency declined to comment on the case, citing privacy concerns. CTVNews (CityNews)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

CHASE THE ACE

Cameron MacQuarrie has one piece of advice for communities planning a Chase the Ace fundraiser: be prepared. The vice-president of Branch 132 of the Royal Canadian Legion and chairman of its Chase the Ace committee in Inverness, said Monday that anyone considering such an undertaking should begin by developing contacts with other community groups that may be needed to help. "You need to gather your community leaders from other organizations and prepare with them in the event that it gets as big as it could possibly get," said MacQuarrie. "You need to look at what resources you have available in terms of other spaces, more volunteers, RCMP and EHS." By the 48th week of Inverness's Chase the Ace, thousands of people poured into the small community, pushing the jackpot up to $1.7 million for Saturday's draw. Donelda MacAskill of Englishtown got the jackpot by winning the draw and then selecting the ace from the three cards remaining in the deck. All previous draw winners had failed to flip the ace. Chronicle Herald, A1

Celebrity dance off to support Julietta's Place
A Red Deer celebrity dance event that raises money for charity has chosen its benefactor and announced the eight celebrity dancers. Women's Outreach Julietta's Place will be the partner charity for the 2016 Sheraton Celebrity Dance off, which will take place April 16. Co-chair of the event, Christine Moore, said the celebrity dancers include David Brant, Dusty Daines, Bonnee Gregg, veterinarian Pat Higgins, coach Ken King, RCMP Const. Charlotte Rockwell, Hermes Salas and Tammy Schlamp. Julietta's Place provides housing to women who are fleeing domestic abuse. The popular event has raised over $1 million over the past four years. It brings together professional dancers, community leaders, business and many volunteers. Tickets for the 2016 event go on sale Jan. 19. Red Deer Advocate, C1

Airdrie shooting suspect surrenders to police
A second suspect in the shooting of a man outside a fitness centre in a Calgary bedroom community last week has turned himself in. RCMP had issued a warrant for the man on Friday. Mathew Van Schiak of no fixed address faces one count of aggravated assault and three weaponsrelated charges. The 21-year-old is to appear in Airdrie provincial court later this week. Also charged with aggravated assault is Michael Sharman. The 35-year-old, who is from Calgary, was arrested during a traffic stop on Friday. The 39-year-old victim was shot three times but is expected to recover fully. Canadian Press (Edmonton Journal, A7, Calgary Herald, A11)

Man charged for turning a jar into a bomb
RCMP in southern Alberta have charged a man with making a homemade bomb. Mounties say a resident in Airdrie found a suspicious looking jar last Friday among some belongings left behind in a rental property. The person had moved several of the items when the jar was spotted in an ammunition container. Officers evacuated several homes in the neighbourhood and safely destroyed the device. Kristopher Goyman, 24, of Airdrie has been charged with making an explosive device with intent to endanger life or cause serious property damage. He is to appear in Airdrie provincial court Oct. 22. Canadian Press (Edmonton Journal, A2; Red Deer Advocate); Postmedia News (Calgary Herald, A11)

Escaped Bowden inmate captured by RCMP
A man who escaped Bowden Institution on Sunday morning was apprehended by Innisfail RCMP later the same day. Kenton Matthew Boyle, 29, had been unlawfully at large since 11: 45 a.m. after staff members discovered he was missing during a count. CSC said it immediately contacted the Innisfail RCMP detachment, and a warrant for his arrest was issued. Innisfail RCMP arrested him at about 7 p.m. Boyle is currently serving a sentence in the minimum security facility of four years, six months for armed robbery, disguise with intent, possession of property obtained by crime and operate motor vehicle - flight. CSC is conducting an investigation into the circumstances surrounding the incident. Red Deer Advocate, C1

*** Province investigating contract controversy**
The Alberta government is considering new accountability rules for municipal governments following a police investigation into a secretive $1.4-million contract awarded to the former mayor of Lloydminster. Last week, Lloydminster Mayor Rob Saunders revealed that the City of Lloydminster was "actively participating" in an RCMP investigation into a July 22, 2013, contract between the city and AHHA

Moments Inc., a consulting firm operated by former Lloydminster mayor Jeff Mulligan, that was signed on the same day Mulligan announced his resignation. "The RCMP review was forwarded to the Alberta Crown Prosecutors' Office and they have determined that there is no evidence to support any criminal charge against the City of Lloydminster or AHHA Moments Inc. in this matter and that this file is now closed," said Saunders in a prepared statement. Saunders refused to take questions from reporters on the issue. The city, which straddles the Alberta-Saskatchewan border, fought to keep details of the agreement under wraps but the contract was released last month by the Office of the Saskatchewan Information and Privacy Commissioner. The contract was worth an estimated $1.4 million over three years for consulting work but was severed by the city after three months and $178,000 in payments to AHHA Moments Inc. The contract was never publicly tendered and was signed by city officials the same day Mulligan announced his resignation but was still sitting as mayor. A spokesperson for Municipal Affairs Minister Deron Bilous said the NDP government "takes the concerns of the residents of Lloydminster seriously." "Under the Municipal Government Act (MGA), municipalities are first and foremost accountable to their residents," said spokesperson Shannon Greer. "We are aware of the situation and under the ongoing MGA review are examining whether additional tools to enhance municipal accountability are required." Edmonton Sun, 7

*** Former Windsor Mountie spent life helping others**

Bernie Campbell could be an imposing figure in his RCMP dress uniform. He had a long and distinguished career in law enforcement that stretched over three decades but at home with his boys, he was ready for all manner of hijinks. "Much to my mom's chagrin, he was one of the boys," said Bernie's oldest son Ian. "She didn't have three boys, she had four." Campbell died last Friday from complications of a genetic malady known as arteriovenous malformation. He was 64... Campbell proudly played the bagpipes in the Windsor Police Band, although he often joked he was positioned in the middle of the pack so no one could hear him. He spent 17 years in drug enforcement with the Windsor RCMP detachment. He retired with the rank of corporal after 33 years. "He was quite a character but he was an even better friend," said Rick Bohus, who worked with him on the force. "One of Bernie's greatest features was his caring attitude toward others on the job or in civilian life." Bohus, who is flying in for the funeral service from his retirement home in Moncton, N.B., recalled the story of a young RCMP officer who feared losing his career after being injured in the line of duty. With Campbell's help, the young man avoided a medical discharge, went on to a full career and rose to the rank of inspector. For his work in labour relations, Campbell won the Queen's Golden Jubilee medal and the Queen's Diamond Jubilee medal. He also received the RCMP's Good Conduct and Long Service medal. Postmedia News (Windsor Star, A2)

*** Mountie hurt, trial ordered**

Two men accused of severely injuring an RCMP officer near Kamloops have been ordered to stand trial. Jerry Lamar and Leon Leclerc were charged with one count each of attempting to wound, maim or disfigure Const. Paul Koester in Pritchard on July 5, 2014. A trial date is expected to be set on Nov. 9. Koester shot and killed Ian Bush, 22, during a 2005 altercation at the RCMP detachment in Houston. An investigation cleared him. Canadian Press (Times Colonist, A8)

*** When paranoia trumps evidence**

A column states "Re: The warming comfort of a familiar paranoia, Oct. 5. Columnist Shannon Gormley offers hard facts, logic and statistics to demonstrate that fundamentalist and terrorist Muslims are no more a threat than fundamentalist or terrorist Christians to Canada's security and values. However, paranoia trumps evidence more often than not - especially if used by a politician to cement support. Prime Minister Stephen Harper seems to be doing all that he can to provide warming comfort to Canadians who feel threatened by the niqab. In appealing court decisions and in promising new laws if his appeals do not succeed, he is making sure that Canadians know that he really cares about their feelings and values. Last week he offered even more comfort. There will be an RCMP tip line for Canadians to report barbaric cultural practices. Some of us were under the impression that we had a responsibility to report barbaric practices to the police. Now, we are to tip off the RCMP if culture is involved. Paranoia will always be with us. It does not need encouragement from Harper." Postmedia News (Ottawa Citizen, C3)

*** 'Barbaric' hotline no solution to serious issues of family abuse**

Sonia Bitar is no stranger to the issue of domestic violence in immigrant communities. The former citizenship court judge is executive director of Edmonton's Changing Together, a centre for immigrant women and their children. For years, Bitar has worked to empower women, helping them to understand their legal rights, flee abusive family situations, and integrate into the Canadian community. Many of the women and girls she works with are the very ones the federal Conservative Party says it's trying to help with its promised new "barbaric cultural practices" tip line. For Bitar, an immigrant from Lebanon, the party's campaign pledge provokes a sharp reaction. "Oh my God. Are we still using these kinds of words?" she says. "Are we now saying there are two different kinds of Canadians? I'm very disappointed." It isn't just the inflammatory language that bothers Bitar. She knows the oppressive domestic and cultural situations that women who are new to Canada can face. In her experience, the best way to assist women at risk is to build trust, and to reach out to them in their own languages. Many, she says, don't know their rights in Canada. Others don't trust the police. Others feel too economically or socially dependent on their husbands or families to break away. It can take time and patience to help them. Postmedia News (Edmonton Journal, A3)

*** Tip line? Surely they jest**

A colum states "Immigration Minister Chris Alexander has announced that, if re-elected, the Conservative government will create an RCMP tip line people can phone to report their neighbour's barbaric cultural practices. Some people, unused to the Harper government's wry sense of humour, have taken the announcement seriously. Immediately tipping off that it was an early April Fool's joke, however, was that it was delivered by Alexander, who is best known for his award-winning imitation of Fraser Crane's brother, Niles. This announcement, a bravura performance, exceeds even Alexander's stunning role in the recent Syrian refugee crisis. Were his announcement serious, my fingers would be at the ready to dial in such barbaric practices as circumcision, the drinking of blood and eating of flesh (even in symbolic form), and the yearly celebrations of murder by crucifixion. But since it was made in jest, perforce to bring some levity to this overly long election campaign - a newly introduced form of barbarism - I propose in similar vein the following list of barbaric cultural practices. To start, the cultural practice of displaying "butt crack." While it may be necessary to grant religious accommodation to plumbers, there is no excuse for anyone else. Women's shoes. 'Nuff said." Winnipeg Free Press, A9

*** Prisoner escapes from hospital, steals car**

A prisoner known for fleeing from police custody managed to run from corrections officers at Victoria General Hospital, steal a car and crash it into a motorcycle before escaping Sunday, according to police. Police were hunting Monday for Tyler Desmond Fong, 31. West Shore RCMP Const. Alex Berube said Fong is not considered armed or dangerous. "Although he has a history of fleeing from police, we have no information to suggest he has a violent past which jeopardizes public safety." The convict, being held at Vancouver Island Regional Correctional Centre, escaped shortly before 8 p.m. Sunday from the custody of provincial correctional officers while at Victoria General Hospital for medical treatment, police said. He smashed his way out of the emergency department. Police did not alert the media until after they got a warrant for his arrest Monday morning and were legally able to release the prisoner's name and photograph, Berube said. Justice Minister Suzanne Anton said B.C. Corrections takes public safety "very seriously" and such escapes are rare. "They are doing a review of this to find out what happened ... it's very unusual," Anton said. The Justice Ministry said privacy rules prevent it from releasing details of the medical treatment the prisoner was obtaining. The ministry said B.C. Corrections cannot disclose specifics of how inmates are managed while escorted outside of correctional centres, for security reasons. Every escort is determined on a case-by-case basis and security protocols are put in place based on risk level, the ministry said. A "critical-incident review" of the escape must be completed within 40 working days. Times Colonist, A3

***Surrey Six accused admits to drug, gun crimes**

A man accused of playing a role in the 2007 Surrey Six slayings has pleaded guilty to several drug trafficking and firearms charges. Sophon Sek entered the plea to seven counts in Surrey Provincial Court on Oct. 1. He'll be back before the judge on Nov. 3 to fix a date for his sentencing. Last spring, Surrey RCMP announced that Sek, 36, was facing 20 charges related to allegations he had trafficked drugs for months despite being on bail for manslaughter in connection with the Oct. 19, 2007 murder of six in a

Surrey highrise. Twelve others were also charged after a 21-month-long investigation that led to four search warrants being executed in September 2014. Postmedia News (Vancouver Sun, A9)

***The barbaric cultural practice of election pronouncements**
There's a low-frequency thrumming in the background of this election campaign – the political equivalent of the tension track used in movies to provoke anxiety and foreboding. If this election was indeed a movie, we would probably now be watching monochrome images of bewildered Canadians clutching their children while some sinister, shifting shape takes form in the near distance – foreign eyes staring malevolently from beneath slit veils or religious zealots mutilating their helpless daughters and forcing them into marital servitude. I can think of no better narration than Rod Serling's dire intonation at the beginning of each *Twilight Zone* episode: "It is the middle ground between light and shadow, between science and superstition, and it lies between the pit of man's fears and the summit of his knowledge." Instead of economic issues and the timeless election slogan of jobs, jobs, jobs, the drumbeat today seems to be Muslims, Muslims, Muslims. It's not quite that explicit, of course. Using that sort of language wouldn't be "politically correct," to borrow a Conservative attack phrase. Rather, the language is more suggestive. Just last week, we were reminded by the immigration minister, standing beside the minister responsible for the status of women, that Canada now has something called the Zero Tolerance for Barbaric Cultural Practices Act, and that if re-elected, the government would establish an RCMP task force, and a "tip line" for Canadians who wish to call the Mounties to denounce someone, a neighbour, it was suggested, for engaging in a barbaric cultural practice. CBC News

***Taloyoak's Netsilik School vandalized over the weekend**
School officials in Taloyoak, Nunavut, are picking up the pieces after their school was vandalized on Sunday. Principal Gina Pizzo says vandals entered Netsilik School and destroyed materials and equipment. She says she is grateful that some residents called police. "[It's] really nice when people do come forward to stop that kind of activity when they see it happening, or help clean up afterwards," she says. "We do really appreciate all the people pitched in to help us clean up the mess. Hopefully we won't see any more of this activity going on anytime soon." Pizzo says some material cannot be salvaged and replacements will have to be flown into the community. She says RCMP are investigating. CBC News

***Editorial: Missing and Murdered Vigil Needs to be Met With a Real Response From Canada**
An editorial "Sunday marked the 10th anniversary of the March and Vigil for Missing and Murdered Indigenous Women, and the Canadian government has still not addressed this problem with a nationwide, federal inquiry. With ever-rising numbers, it's a problem that is always at the forefront every October 4. The annual event is an important reminder, but it's an issue that falls on the wayside throughout the course of the year. The Canadian government ignores it as well as a majority of its population. For the last 10 years, marches have been happening all over the country for a federal inquiry into the deaths of more than 1,200 indigenous women. So far the demands have been met with an almost deafening silence. While promises have been made to have police investigations it does not address the severity of the issue. We live in world where we talk about appropriate responses to crimes daily, but when crimes actually need a significant response, there's almost none. According to the most recent RCMP report on the issue, there has been a 9 per cent decrease in unsolved cases—from 225 to 204. It's a start, but it's still not good enough. There are still at least 204 indigenous women whose stories are yet to be concluded, and we will not forget them." The Link

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Devries back in custody
A B.C. serial fraudster has turned himself in after being wanted on a Canada-wide warrant. Last week, police said they were actively looking for Wesley John Devries, 45, after he allegedly breached conditions of his release. Devries had been released from prison over the summer after pleading guilty in 2013 to 13 counts of fraud and theft. Many of his victims were women he met through dating websites. He had most recently been living in the Victoria area, said Victoria police spokesman Bowen Osoko. The Province, A10

* **'There is no appreciable gaps in his criminal behaviour'**
The federal Crown is seeking dangerous offender status for Mark Lange, a 40-year-old Yukon man with 42 convictions, including six for violent crimes. The status could put Lange in jail indefinitely. Alongside Dean Boucher, Lange was convicted of manslaughter in the death of a Carcross hotel owner in 2004. Both were originally found guilty of second-degree murder. However, the Yukon Court of Appeal overturned the sentence in 2011 citing contradictory instructions the presiding judge told the jury. On Friday, Crown prosecutor Noel Sinclair noted the crimes Lange had committed fit two of the requirements for the status: a pattern of persistent aggressive behaviour, and a failure to restrain his behaviour and a likelihood of causing death or injury to other persons. In the case of an indeterminate sentence, it must be shown a lesser sentence would not protect the public adequately.Sinclair pointed to Lange's lengthy criminal record. Whitehorse Daily Star, 2/Front

* **Ex-investment adviser gets 3û years**
Schriver pleaded guilty to 'cold, calculated scheme' involving 22 people, over $1m
A former Halifax investment adviser has been sentenced to 3û years in prison for defrauding investors of more than $1 million. Bruce Patrick Schriver pleaded guilty in June to one charge of fraud over $5,000, involving 22 victims who lost a combined $1,054,986 over a six-year period. "The wake of this fraud will be long felt and long suffered by his many victims," Crown attorney Mark Heerema said Monday at Schriver's sentencing in Halifax provincial court. "The number of victims also speaks to the amount of time that Mr. Schriver had to consider carefully what he was doing. This case is far from a momentary lapse of judgment or an impulsive decision. "It was a cold, calculated scheme that was occurring." The Chronicle-Herald, A7

* **UN CRIMINEL DE CARRIÈRE**
Robert Simpson est né en septembre 1962 dans la région d'Ottawa, où il a grandi. Il vient d'une famille nombreuse. Il est très proche de son jeune frère, Timothy, avec lequel il est devenu témoin repenti dans cette affaire. « J'ai toujours protégé mon frère, y compris de notre mère lorsqu'elle le battait », a-t-il témoigné. Robert Simpson est un criminel de carrière et un tueur de sang-froid. Il avait 17 ans lorsqu'il a été envoyé au pénitencier pour la première fois. Il y a passé plus de 35 ans de sa vie jusqu'à maintenant. La Presse+

* **Confessions d'un tueur de sang-froid**
Un procès pour meurtre qui s'est ouvert il y a quelques semaines à Montréal s'est transformé hier en véritable incursion dans le monde sordide et impitoyable des tueurs de sang-froid. Les sept femmes et cinq hommes chargés de déterminer le sort de l'accusé, Leslie Greenwood, un résidant de la Nouvelle-Écosse de 45 ans, ont commencé à entendre le témoignage de Robert Simpson, un criminel notoire devenu témoin repenti. Simpson, 53 ans, a déjà admis avoir commis les deux meurtres pour lesquels Greenwood est aussi accusé. Il a été condamné à la prison à vie, sans possibilité d'obtenir sa libération conditionnelle avant 25 ans. Les deux victimes, Kirk Murray et Antonio Onesi, ont été tuées le soir du 24 janvier 2010 dans le stationnement d'un restaurant McDonald's du quartier Notre-Dame-de-Grâce. Le Quotidien, 16; Le Journal de Montréal

* **Les élections font jaser... jusqu'en prison**
Lorsque Rick Sauvé rend visite à des prisonniers ces jours-ci, ils ont un nouveau sujet de conversation : les élections fédérales. Ils le bombardent de questions, lui demandant ce que disent les sondages ou qui, selon lui, a le plus de chances de gagner. «Ça leur permet de parler d'autre chose, affirme M. Sauvé. Parce que chaque jour est comme le jour de la marmotte, chaque jour se ressemble. Alors, quand un scrutin survient, ça attire leur attention.» Les détenus de toutes les prisons provinciales et fédérales pourront voter vendredi, soit 10 jours avant les élections, à des bureaux de vote spécialement installés dans les établissements carcéraux. La Presse Canadienne (Le Soleil, 8; Le Devoir)

* **25-year stance on son's innocence impoverishes ex-Saanich parents**
After 25 years, David and Elouise Lord still believe their only son, Derik, is innocent of a notorious double murder that gripped B.C. in 1990. It's an enduring faith that has led them here, to a rundown house on Yale Road in Chilliwack that the insurance company won't touch. The yard is overgrown, the shoddy stairs near collapse. Inside, the small rooms are full of clutter, including several large cabinets stuffed with

papers and documents relating to Derik's case... The violent murders rank among B.C.'s most chilling and infuriating, in great part because Derik Lord continues to believe he was wrongfully convicted, despite a confession from Muir and a stack of compelling evidence. In 1992, Lord was sentenced to life in prison with no eligibility for parole for 10 years. It's where he has remained ever since. His claims of innocence have positioned him at odds with his two co-accused and bankrupted his fiercely loyal parents, who estimate they've spent $800,000 in legal bills over the years. His campaign has also ensured a regular flow of headlines over the past 10 years during which he's been eligible for parole - the latest hearing another unsuccessful, and emotionally charged, event this past March. By contrast, Muir, who at the time of the killings was a cherub-faced 16 year old, admitted his guilt and was granted full parole in 2003. He's lived a quiet life ever since. Huenemann, meanwhile, who was sentenced in 1991 to life in prison, became eligible for full parole this year. By his request, a parole hearing scheduled for this month was postponed until 2016, the Parole Board of Canada said. According to a newspaper report from 2003, he has also admitted to his role in the murders, after years of denial. It's believed he's in Quebec. Times Colonist, A2

* **Cellulaires, drogue, armes et porno saisis en prison**
Les agents correctionnels de la prison de Bordeaux viennent de faire un grand ménage dans l'aile abritant les hells Angels et les gangs de rue, saisissant des téléphones cellulaires, des pics artisanaux, de la drogue et du matériel pornographique contenu dans des ordinateurs. La rafle menée jeudi dernier aurait permis d'identifier une demi-douzaine de membres et d'associés des Hells Angels parmi les détenus fautifs, a appris Le Journal. Arrêtés lors de plusieurs opérations policières menées ces dernières années, ces motards sont détenus de façon provisoire dans la prison centenaire de Montréal en attendant l'issue des procédures judiciaires intentées contre eux. Certains de ces accusés bénéficient exceptionnellement d'une permission de la cour pour avoir accès à un ordinateur portable en détention afin de pouvoir préparer leur défense. Le Journal de Montréal, 6

* **New trial begins**
A new trial has begun for a man previously convicted of beating his lover to death. Michael Pearce was found guilty of manslaughter in the 2007 bludgeoning death of 36-year-old Stuart Mark and sentenced in 2012 to seven years in prison. At trial, prosecutors alleged Pearce flew into a rage after learning Mark was HIV-positive and beat him with a golf club at Mark's Alfred Avenue home. Last year, the Manitoba Court of Appeal ordered a new trial in the case, ruling jurors were not adequately cautioned about the phenomenon of false confessions. Winnipeg Sun, 4

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Suspects versus sex crime survivors
A Halifax taxi driver accused of sexually assaulting a passenger is allowed back on the job. A bartender charged with aggravated sexual assault can keep mixing drinks at a downtown bar. A university student charged with sexual assault after a frosh week incident continues attending classes on campus - until a second victim comes forward. The three cases pit the competing need to protect public safety and the survivors of sexual assault against one of the most sacred legal tenets: The presumption of innocence. "It's a difficult balance," Dalhousie University law professor Wayne MacKay said. "On one hand, you have the rights of the larger society and victims within that society to have a safe environment. On the other hand, you have to protect the important rights of the accused, including presumed innocence and the right to a fair trial." In each case, however, respecting the rights of the accused appears to be held in higher regard than the potential risk to public safety and women's sense of security. Yet MacKay, the Yogis &Keddy Chair in Human Rights Law, said there is an increasing shift toward survivors' rights. "It's a bit of a newer focus and one that has generated some political and policy heat. The current government has taken more of a stand in protecting victims." The Conservatives' proposed victims' bill of rights, for example, has generated support but has also faced criticism from more traditional legal academics, MacKay said. The Chronicle-Herald, A1

*** Chief defends crime comments**
Linking rising city crime rates to the tumbling price of oil and resulting job losses is just a general observation, says Acting Chief Brian Simpson, defending comments from Edmonton's top cop. Simpson made the point Monday after Wood Buffalo Mayor Melissa Blake slammed comments made last week by Edmonton police Chief Rod Knecht as "derogatory" towards oil field workers from northern Alberta. Knecht said displaced workers from Fort McMurray and Cold Lake gravitate to Edmonton after job losses and he pointed to low oil prices as a reason for Edmonton's sharp increase in property and violent crime. Edmonton police saw a 12% increase in violence and an 18% increase in property crime this year over last. "When oil is up we're busy, and when oil is down we're really busy," said Knecht. Calgary Sun, 20

*** Sisters in spirit 'Come together for a peaceful vigil and prayer ceremony'**
"I'll bet you and I would be treated very differently if we walked into a grocery store," says Josie Nepinak. "I might be followed around. I'd likely not receive the same courtesy as you would." Nepinak and I are women in the middle age of life, both well dressed and both educated with rewarding careers. It's the colour of our skin, she says, that changes everything. "I still hear, 'I hate you Indians,' sometimes at a bus stop." It's one other, even bigger difference between us that stands out when we make our acquaintance Monday morning on the steps of Calgary's City Hall. "I had an aunt back in 1978 who was murdered and her killer has never been found," she says matter-of-factly of tragedy hitting so close to home. "And I have a cousin who in 2012 was murdered by serial killer Sean Lamb in Winnipeg." As the executive director of Calgary's Awo Taan Healing Lodge Society, the only aboriginal women's shelter in Alberta, Nepinak has spent the past 25 years promoting health and wellness for First Nations women and their families. Once a year, though, her sole focus is on the more than 1,200 murdered and missing aboriginal women in Canada over the past three decades. Calgary Herald, A6

*** Police department tries to clarify link between rising crime, oil price**
Edmonton's police force tried to clarify Monday comments its chief made last week that out-of-work oilpatch workers could be to blame for the city's recent rise in crime. On the weekend, the Edmonton Police Service released tables and charts that it said shows monthly crime statistics in Edmonton climbing over the past 12 months as oil prices dropped to record lows. On Monday, deputy chief Brian Simpson spoke to reporters on the steps of police headquarters. "It's not linked to oil prices," he said. "It's linked to the change in the economy that we experience in Alberta. This has been an Alberta experience for a long time." Red Deer Advocate, A5

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

Long-awaited inquest into young aboriginal deaths starts
A long-awaited inquest into the deaths of seven aboriginal youths who moved from their remote reserves in northern Ontario to go to high school in Thunder Bay, Ont., opened Monday following a sunrise ceremony. In an opening statement to the jury, presiding coroner Dr. David Eden warned of a difficult road ahead. "We are starting on a long pathway," Eden said. "During that time as we go through this pathway, there will be differences. It's our job to manage those differences with wisdom, not with anger." The inquest, expected to last until next spring and hear from about 200 witnesses - some will testify more than once - is probing the deaths of Jethro Anderson, 15, Curran Strang, 18, Robyn Harper, 19, Paul Panacheese, 21, Reggie Bushie, 15, Kyle Morrisseau, 17 and Jordan Wabasse, also 15. All died between 2000 and 2011 while, as Eden put it, trying to advance their lives and the well-being of their communities through education. Canadian Press (Red Deer Advocate, A6; Kingston Whig Standard, Waterloo Region Record, Hamilton Spectator); Toronto Star; * Postmedia Network (Vancouver Sun, B2, StarPhoenix, C8, Calgary Herald, B2, Ottawa Citizen, C1/Front, Leader-Post, B5, Edmonton Journal, N3, Gazette, A11)

INTERNATIONAL

*** Snowden seeks return to U.S**

Edward Snowden says he has offered to return to the United States and go to jail for leaking details of National Security Agency programs to intercept electronic communications data on a vast scale. The former NSA contractor flew to Moscow two years ago after revealing information about the previously secret eavesdropping powers, and faces U.S. charges that could land him in prison for up to 30 years. Snowden told the BBC that he'd "volunteered to go to prison with the government many times," but had not received a formal plea-deal offer. Earlier this year, former U.S. Attorney General Eric Holder said a plea deal with Snowden was a possibility. Associated Press (Times Colonist, B7; Toronto Sun, Winnipeg Sun, Edmonton Sun, Waterloo Region Record, Globe and Mail, Times and Transcript)

***Ship sinks near Bahamas**

The captain of the 790-foot El Faro planned to bypass hurricane Joaquin, but some kind of mechanical failure left the U.S. container ship with 33 people aboard helplessly - and tragically - adrift in the path of the powerful storm, the vessel's owners say. On Monday, four days after the ship vanished, the U.S. Coast Guard concluded it sank near the Bahamas in about 15,000 feet of water. One unidentified body in a survival suit was spotted, and the search went on for any trace of the other crew members. The ship, carrying cars and other products, had 28 crew members from the U.S. and five from Poland. Associated Press (Times Colonist, B7)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 10, 2015 / le 10 novembre 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

*** Politics This Morning: Ad hoc Cabinet committee on refugees meets today**
The Liberal government's announcement that it created an ad hoc committee on refugees to bring 25,000 Syrian refugees to Canada by the end of this year is "short on details" and doesn't show a concrete plan to deliver on the campaign commitment, says the NDP."We are glad that the government remains committed to resettling 25,000 Syrian refugees by year's end. We support this goal. But today's announcement was short on details and we believe Canadians were looking for a concrete plan for getting vulnerable refugees out of harm's way, not hearing about new Cabinet subcommittees," NDP MP Jenny Kwan told The Hill Times in a statement. "This is the new government's first test on delivering the change they promised to Canadians-we hope that the next announcement, on how they will achieve this goal, is coming very soon."The committee, which will hold its first meeting today, is chaired by Health Minister Jane Philpott and has eight other members. They include: Canadian Heritage Minister Mélanie Joly who will be the vice-chair, **Public Safety and Emergency Preparedness Minister Ralph Goodale,** Foreign Affairs Minister Stéphane Dion, Immigration, Refugees and Citizenship Minister John McCallum, Treasury Board President Scott Brison, International Development and La Francophonie Minister Marie-Claude Bibeau, Defence Minister Harjit Sajjan and Democratic Institutions Minister Maryam Monsef.HillTimes

Des réfugiés pourraient loger dans des bases militaire
Des réfugiés pourraient être accueillis dans des bases militaires canadiennes, a confirmé hier le nouveau ministre de l'Immigration, John McCallum. Le Parti libéral du Canada a promis en campagne électorale d'accueillir 25 000 nouveaux réfugiés d'ici la fin de cette année. M. McCallum a annoncé la création d'un sous-comité d'une demi-douzaine de ministres qui auront le mandat de coordonner cette tâche. La ministre de la Santé Jane Philpott présidera ce comité, qui inclura aussi la ministre du Patrimoine Mélanie Joly, **le ministre de la Sécurité publique Ralph Goodale** et la ministre des Institutions démocratiques Maryam Monsef, elle-même admise au Canada en tant que réfugiée provenant de l'Afghanistan. Le ministre de la Défense, celui des Affaires étrangères et celle du Développement international seront aussi impliqués. LaPresse

Bibeau nommée au comité special
Quelques jours après avoir été nommée ministre, la nouvelle députée de Compton-Stanstead, Marie-Claude Bibeau, voit son nom associé à un dossier chaud du nouveau gouvernement de Justin Trudeau. Le ministre de l'Immigration, des Réfugiés et de la Citoyenneté, John McCallum, a annoncé la création d'un comité spécial chargé d'aider à faire venir 25 000 réfugiés syriens au Canada. La ministre du Développement international et de la Francophonie fait partie du groupe. Ottawa n'est pas encore en mesure de préciser quand les premiers réfugiés syriens fouleront le sol canadien, mais ce comité spécial a été mis sur pied pour préparer le terrain. M. McCallum reconnaît que le temps presse pour le gouvernement fédéral, qui a promis d'accueillir 25 000 réfugiés syriens au Canada d'ici la fin de l'année, mais il dit ne pas vouloir rater son coup. En conférence de presse dans le foyer des Communes, lundi, il a annoncé la création d'un comité composé de neuf ministres qui aura le mandat de donner suite à cet engagement. Le comité sera présidé par la ministre de la Santé, Jane Philpott, qui sera notamment épaulée par son collègue aux Affaires étrangères, Stéphane Dion, **à la Sécurité publique, Ralph Goodale**, ainsi que la ministre du Patrimoine canadien, Mélanie Joly. La Presse Canadienne (LeDevoir, LaTribune); LaPresse; LeDevoir

Military aircraft, bases may be tapped for refugees
The federal government is considering using ships and commercial and military aircraft to transport 25,000 Syrian refugees to Canada by the end of December. At a news conference Monday, Citizenship and Immigration Minister John McCallum also said the Liberal government might lodge the refugees at military bases upon their arrival. The emphasis is being put on two factors: security screening and the health of the refugees. To that end, the government has established an ad hoc cabinet committee to ensure the Liberals make good on their election pledge. The nine-member committee, which will hold its first meeting Tuesday, is chaired by Health Minister Jane Philpott, who has previously worked with refugees in Africa. Others include: McCallum; Foreign Affairs Minister Stéphane Dion; **Public Safety Minister Ralph Goodale**; Defence Minister Harjit Sajjan; Treasury Board President Scott Brison; Canadian Heritage Minister Mélanie Joly; International Development Minister Marie-Claude Bibeau; and Democratic Institutions Minister Maryam Monsef, herself a refugee originally from Afghanistan. The government also appointed a senior bureaucrat to provide greater focus. Malcolm Brown, the deputy minister for International Development, becomes special adviser to the Clerk of the Privy Council Office on the "Syrian Refugee Initiative." He is a former executive vice-president of the Canada Border Services Agency with experience in several departments. Postmedia News (Leader-Post, B8, Vancouver Sun, StarPhoenix, Ottawa Citizen, Calgary Herald)

25,000 refugees are coming, one way or another
They might come by military transport, on chartered flights or warships; from Jordan, Turkey or Lebanon; to army bases or the homes of generous Canadians. When it comes to fulfilling the government's commitment of bringing 25,000 Syrian refugees to Canada over the next eight weeks, "all options are on the table," said John McCallum, Canada's new Minister of Immigration, Refugees and Citizenship, during his first news conference since taking over the cabinet post from Chris Alexander. "Whatever works, whatever is cost effective, whatever will get them here safely and quickly. So yes, we're looking at the possibility of commercial airlines. We're looking at the possibility of the air force. We're looking at the possibility of ships. All of these things are being considered as we speak, and all will be used to the extent that they are needed to get the job done." It will be up to a new Ad Hoc Committee on Refugees, chaired

by Health Minister Jane Philpott, to figure out how. (...)She will be joined by seven other high-profile ministers, including veteran politicians **Ralph Goodale** (**public safety minister**) and Foreign Affairs Minister Stéphane Dion, as well as the Minister of Democratic Institutions Maryam Monsef - whose own life in **Canada** began as a refugee from Afghanistan - and Defense Minister Harjit Singh Sajjan. Gazette

Réfugiés syriens
Le gouvernement fédéral n'est pas encore en mesure de préciser la date à laquelle les premiers réfugiés syriens attendus d'ici la fin de l'année fouleront le sol canadien, mais il a mis sur pied un comité spécial afin de préparer le terrain. Le ministre de l'Immigration, des Réfugiés et de la Citoyenneté, John McCallum, reconnaît que le temps presse pour le gouvernement, qui a promis d'accueillir 25 000 réfugiés syriens au Canada d'ici le 31 décembre. Mais Ottawa ne doit surtout pas rater son coup. «Oui, on veut le faire vite, mais en même temps, on veut le faire d'une façon correcte en termes de considérations de sécurité et de santé», a plaidé le ministre McCallum en conférence de presse au parlement, lundi. Pour atteindre l'ambitieux objectif que s'est fixé le chef libéral Justin Trudeau pendant la campagne électorale, un comité spécial composé de neuf ministres a été créé. Une première réunion de ce comité interministériel doit avoir lieu dès mardi. (...) Le ministre a également signalé que le gouvernement avait l'intention de rétablir dans son intégralité le Programme fédéral de santé intérimaire (PFSI), qui offre une protection en matière de soins de santé limitée et temporaire aux réfugiés et aux demandeurs d'asile. Le comité dont la formation a été annoncée lundi sera présidé par la ministre de la Santé, Jane Philpott. La coprésidence a été confiée à la ministre du Patrimoine canadien, Mélanie Joly. Elles seront notamment épaulées par leurs collègues aux Affaires étrangères, Stéphane Dion, **à la Sécurité publique, Ralph Goodale,** au Développement international, Marie-Claude Bibeau, ainsi que par la ministre des Institutions démocratiques, Maryam Monsef, une réfugiée afghane. La Presse Canadienne (Acadie Nouvelle, 16, Voix de l'Est, Soleil, Voix de lEst)

* **Un comité spécial créé pour accueillir 25 000 réfugiés syriens**
Le gouvernement Trudeau mobilise plusieurs ministres pour lui permettre d'atteindre son objectif d'accueillir 25 000 réfugiés syriens avant la fin de l'année. Le ministre de l'Immigration, des Réfugiés et de la Citoyenneté, John McCallum, a annoncé hier la création d'un comité spécial composé de neuf membres du cabinet qui se réuniront à compter d'aujourd'hui pour mettre l'épaule à la roue.
Si l'objectif d'accueillir 25 000 réfugiés en moins de deux mois tient toujours la route, M. McCallum a insisté pour dire que cet engagement électoral de Justin Trudeau devait se réaliser sans compromettre pour autant la santé et la sécurité. (...) Le comité ministériel sera présidé par Jane Philpott à la Santé, secondée par Mélanie Joly, à la tête du portefeuille de Patrimoine canadien. Outre M. McCallum, **les ministres de la Sécurité publique, Ralph Goodale,** des Affaires étrangères, Stéphane Dion, du Conseil du Trésor, Scott Brison, du Développement international, Marie-Claude Bibeau, de la Défense nationale, Harjit Singh Sajjan, et des Institutions démocratiques, Maryam Monsef, elle-même une réfugiée afghane, font partie du comité. JournaldeQuebec

* **Trudeau's Cabinet: The essential breakdown of roles and priorities**
Prime Minister Justin Trudeau unveiled his Cabinet last week, with 30 members in addition to himself, 15 men and 15 women. In the process, several changes were made to the machinery of government, giving some departments new titles and transferring responsibilities for some agencies. **Public Safety and Emergency Preparedness Minister Ralph Goodale** (Regina-Wascana, Sask.)The File**: Mr. Goodale's** most high-profile responsibility will be reforming the anti-terrorism law, Bill C-51, introduced by the last government. He is also next in line to take over Prime Minister Justin Trudeau's duties if needed. The Public Safety and Emergency Preparedness deputy minister is François Guimont, and the department has a $1.2-billion budget for 2015-16, according to the Main Estimates.Cabinet Committees: Chair of Canada in the World and Public Security; vice-chair of the subcommittee on Canada-United States Relations. Member of Agenda and Results; Intelligence and Emergency Management; and Open and Transparent Government.Background: **Mr. Goodale** was first elected as an MP in 1974, at the age of 24. He was then the Saskatchewan Liberal leader before coming back to the Hill in 1993. He's held several high-profile Cabinet positions. Hilltimes

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

***Le déversement est autorisé**
La Ville de Montréal ira «rapidement» de l'avant avec le déversement de 8 milliards de litres d'eaux usées dans le fleuve Saint-Laurent tout en respectant les conditions ordonnées par la nouvelle ministre de l'Environnement, a annoncé hier le maire Denis Coderre. Selon toute vraisemblance, le rejet aura lieu cette semaine. La date sera annoncée ce matin. «C'est réglé, il va y avoir déversement», a déclaré hier soir M. Coderre lors d'un point de presse à l'hôtel de ville. Une heure auparavant, en conférence téléphonique depuis Paris, la nouvelle ministre de l'Environnement Catherine McKenna a déclaré que le déversement pourrait se faire «dès ce matin», si la Ville acceptait quatre conditions. Elle demande notamment à la Ville d'effectuer une surveillance visuelle des panaches de l'effluent, de mettre sur pied un plan d'urgence pour gérer les rejets imprévus des industries durant la période de travaux et de fournir jusqu'en juin 2016 à Environnement Canada des données qui mesurent la qualité de l'eau du fleuve. La Presse, A2/FRONT (Le Quotidien, La Nouvelliste, Le Soleil); Globe and Mail, A4

*** Encore beaucoup de travail à faire**
Même si on vient d'annoncer à Lac-Mégantic que la décontamination est terminée, plus de 27 mois après la tragédie ferroviaire de juillet 2013, il ne faudrait pas croire que le travail du ministère du Développement durable, de l'Environnement et de la Lutte aux changements climatiques (DDELCC) est fini pour autant. Selon Paul Benoît, gestionnaire responsable des activités de nature environnementale associées à la réhabilitation du centre-ville de Lac-Mégantic, un plan de décontamination et une nouvelle planification adoptée au début de 2015 vaudraient sûrement qu'on rende public un certain rapport à saveur de bilan avec certaines statistiques sur l'ampleur des travaux réalisés. «Plusieurs étapes sont terminées, mais le rapport n'est pas encore disponible, cela devrait venir à la fin de 2015 ou au début de 2016. Tous les sols du centre-ville contaminés par le déversement causé par la MMA ont été excavés et remplacés par des sols propres, venant de l'extérieur. Cette opération s'est terminée en octobre», décrit Paul Benoît. La Tribune, 23

*** Crews work to clear tracks after 2 train derailments, oil and chemical spills in Wisconsin**
Crews worked Monday to clear freight cars from rail tracks and contain spilled crude oil and chemicals after two trains derailed in Wisconsin about 200 miles apart over the weekend. More than a dozen cars of a Canadian Pacific Railway train loaded with crude oil jumped the tracks in Watertown on Sunday afternoon, puncturing one car that spilled hundreds of gallons of its load and caused the evacuation of a neighbourhood in the small southern Wisconsin city. Residents who evacuated dozens of homes were still being kept away Monday as 12 derailed cars were moved to a temporary track. Thirteen of the train's 110 cars derailed, and 109 of them were carrying crude oil, officials said. Crews were dismantling and removing the car that was punctured, Canadian Pacific spokesman Andrew Cummings said, adding that it spilled no more than 1,000 gallons. The railroad said the leaking car was sealed, the oil contained and siphoned off, and that none of the product reached any waterways. Associated Press (Cape Breton Post)

*** Divers continue to investigate sunken barge**
Lake Erie divers surveying the sunken wreck of the barge Argo last week were sent to hospital after a sudden leak released an unknown substance. U.S. Coast Guard spokesman Thomas McKenzie said the divers were sent to hospital as a precaution but all have been released. "They were fine and they've already left the hospital," McKenzie said. Crews were conducting a "survey" of the vessel - what McKenzie described as a rinse offof the barge - when "a rivet popped or a pinhole leak opened up and they realized there was some discharge." The leak was sealed before the divers surfaced. Crews were preparing to dive again Monday to get a sample of the solvent-like material, thought to be the petroleum distillate benzol. The Argo was carrying 4,800 barrels of crude oil when it sank during a storm in 1937 in U.S. waters approximately 12 miles northeast of Sandusky, Ohio. It now sits 44 feet below the surface with silt and bottom sand building up around its sides. Windsor Star, A6

***'Two very lucky backcountry travellers' after avalanche near Rogers Pass**
Two people had a near-miss in a big avalanche near Rogers Pass on the weekend, kicking off this year's season in earnest. Around 2:35 p.m. Sunday, officials with Parks Canada said they received a report of a Size 3 avalanche - enough to bury a car, damage a truck, destroy a house or break trees - on the upper

part of Bruins Ridge. "It was a good-sized avalanche," said Percy Woods, a visitor safety technician with Glacier National Park. "We have two very lucky backcountry travellers." It's one of the first avalanches of the season where people got caught. A second one happened Saturday in Kootenay National Park, where five climbers on Mount Stanley were caught and carried 60 metres downslope. They were able to extricate themselves and walk away unharmed, according to Parks Mountain Safety in a Facebook post. The avalanches have prompted a reminder from officials to be prepared when heading into the backcountry. Calgary Herald

* **Families should have 72 hours of supplies on hand in case of an emergency**
This time of year, I always think about being prepared for an unexpected emergency situation in my home. In the Maritimes, we are lucky that we are naturally immune to some of the terrifying weather systems that occur in other parts of the world. There are, however, certain situations that we should be ready for at any given time. When I think about recent events that have given me cause to check my emergency preparedness kit, I think about autumn hurricanes, severe winter snow storms and a 15-minute evacuation order. You can't possibly be prepared for every scenario, but you can put together a very helpful kit for you and your family if you were trapped in your home without services for 72 hours or hear the knock on the door from EMO or the police ordering you to leave your home in 15 minutes. Chronicle-Herald

NATIONAL SECURITY / SÉCURITÉ NATIONALE

RCMP to honour Hill terror heroes
The RCMP will give awards to 20 Mounties and former House of Commons security officers in recognition of their bravery when a gunman stormed Parliament Hill last year. The national police force will make the presentations during a private Nov. 23 ceremony at RCMP headquarters. The RCMP said the awards are intended to recognize the online post. 1.866.977.2737 "bravery, dedication and quick thinking" of those who were directly involved in the events of Oct. 22, 2014. On that day, Michael Zehaf Bibeau fatally shot honour guard Cpl. Nathan Cirillo at the National War Memorial before rushing into Parliament's Hall of Honour, where he was killed in a flurry of bullets. Former House of Commons sergeant-at-arms Kevin Vickers, now Canada's ambassador to Ireland, was lauded for his role in subduing Zehaf Bibeau, but there has been no formal recognition of others. The RCMP was responsible for the grounds of the parliamentary precinct during the attack, while House of Commons and Senate security forces had jurisdiction inside the Parliament nuildings. A now-merged parliamentary protective service manages dayto-day security on Parliament Hill, a direct consequence of Oct. 22 intended to avoid confusion. Times Colonist, A8 (Kingston Whig-Standard, London Free Press, Chronicle Herald); * Postmedia News (Ottawa Citizen, A8); * Agence QMI (Journal de Montréal, 18)

* **Whistleblower to deliver address for Queen's**
A man some people consider a hero and others believe is a criminal is to present the opening address at a Queen's University conference later this week. Edward Snowden, 32, the former Central Intelligence Agency employee and United States government contractor who leaked thousands of classified documents that revealed the extent of global surveillance programs operated by the U S. and its English-speaking allies, is to present the opening keynote speech at the Queen's International Affairs Association's Model United Nations Invitational on Thursday. (...) Bill C-51, the Anti-terrorism Act 2015, broadened the authority of Canada's surveillance and law enforcement agencies by giving them more power to thwart suspected terrorist plots - not just gather information about them. Kingston Whig-Standard, A3

* **It's your military, Mr. Sajjan. What do you want it to do?**
Just a week into his government, Prime Minster Trudeau has made some bold moves. His fresh, balanced cabinet and his stated intent to bring collaboration back to the business of government policy-making is being welcomed with enthusiasm by a lot of Canadians. Every one of these new cabinet ministers faces a massive workload - none more than the new minister of Defence, Harjit Sajjan.(...) Key governmental departments, including DFATD, Public Safety Canada and DND, should collaborate quickly to help the government formulate a defence White Paper outlining a new national security

strategy. Once that's done, Mr. Sajjan and his team can start the work of drafting a national military strategy that would allow civilian and military leaders within DND to plan and execute their operational and institutional responsibilities more efficiently and effectively. iPolitics; Canadian Press (National Post, A5, Star Phoenix, Calgary Herald)

Brandon boy, 16, faces terrorism-related charge
A 16-year-old boy in Brandon, Man., faces a terrorism charge for allegedly using social media to express support for the Islamic militant group ISIS. The teen has also been charged with one count of possessing child pornography. He appeared in court in Brandon on Monday, but the case was adjourned until Thursday because he had not secured legal counsel, said Manitoba's chief federal prosecutor Ian Mahon. The boy, who cannot be named under the Youth Criminal Justice Act, remains in custody. Mahon said he expects a bail application to be heard on Thursday. Not much is known about the boy. Brandon residents told CBC News he grew up in the western Manitoba city and is attending high school there. Mahon said items have been seized from the teen's home, including a computer that is closely being looked at. The matter remains under investigation. Another Manitoban, Aaron Driver, was arrested in Winnipeg in June after he openly supported ISIS on Twitter. Although Driver is not accused of any crime, the RCMP is seeking to have his current bail conditions extended for a longer term, based on the suspicion that he might help or engage in terrorist activities. He appeared in court last week to fight the Mounties' attempts to limit his freedoms. Mahon, who is also the federal prosecutor in that case, had said the restrictions are "not punitive" but reasonable for public safety. CBC News (2015-11-09)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

* **Tim Hortons loses bid to turf rights complaint**
A Canadian coffee giant and franchisee have lost their bid to toss out a human-rights complaint lodged by Mexican workers in northeastern British Columbia. Edxon Chein, Eric Dessens, Rodolfo Lara and Ruben Ramirez were all hired under the Temporary Foreign Worker Program to work in a Tim Hortons franchise in Dawson Creek in 2012. The workers filed a complaint with the B.C. Human Rights Tribunal against Tim Hortons Inc., TDL Group Corp., a subsidiary that oversees restaurant operations, and franchise operator Tony Van Den Bosch. They allege they had to endure inferior working conditions, racist and derogatory comments and sub-standard living conditions owned by the franchise operator. A lawyer for Tim Hortons argued before the tribunal that the company wasn't connected to the issues raised in the complaint and that Van Den Bosch operates as independent contractor. The tribunal didn't make a final decision, but ruled against the application to dismiss the case, ordered it to go to a hearing and urged the parties to seek mediation. Canadian Press (Times Colonist, A6)

***Bakery owner could face jail for weapon stash**
Crown prosecution argued for as much as two years behind bars while defence counsel contended a conditional sentence order is appropriate during a hearing Monday for a Prince George man who was at the centre of a massive haul of guns and bullets from his home slightly more than two years ago. Much of the hearing, held in Prince George provincial court, was spent itemizing the weapons RCMP seized from his Prospect Point home and matching them to each of the six charges Karl Heinz Haus, 55, pleaded guilty to from the September 2013 incident. It began when Canada Border Services Agency officers intercepted two packages that originated in Germany and destined for Haus's home address. They contained components used to convert an M-16 assault rifle into a fully automatic weapon. The information was passed onto the RCMP federal serious and organized crime unit and after the parts were determined to be prohibited, investigators secured a search warrant for the home. Prince George Citizen (2015-11-09)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

***Europe declaws Iran's 'rocket kitten' hackers**

European authorities have taken action to take down a cyber espionage campaign believed to be linked to Iran's powerful Revolutionary Guard, the first operation of its kind since Tehran signed a nuclear treaty, researchers say. The hacker group - dubbed "Rocket Kitten" by security experts who have been hunting the hacker group since early 2014 - has mounted cyberattacks on high-profile political and military figures globally since that time, according to researchers from several cyber security firms who have monitored its activities. The action could hamper Tehran's efforts to gather sensitive intelligence from rivals including Saudi Arabia, Israel, Turkey, the United States. Reuters (Toronto Sun, A46; Edmonton Sun, Calgary Sun, Winnipeg Sun)

***Parsing the risks in cyber insurance**

When an insurance company sells protection against a house fire or car accident, it leans on decades of data from past experience to price policies. For every 1,000 houses you insure you have a rough idea how many will burn. That basic yet key ingredient is all but missing in the growing business of cyber insurance, in which business is booming as the list of hacking incidents from Target to Ashley Madison grows. Add to the mix the ever-changing nature of hacks and different levels of security sophistication among companies, and the challenges mount alongside the opportunities. "There are many unknowns," said Nick Galletto, cyber risk services leader for the Americas at Deloitte. Hacks such as the one that hit adultery website Ashley Madison can give an idea of the cost of the fallout of such an event. But that doesn't come close to providing the depth of data insurers use to create and measure the underwriting standards when they sell protection against house fires, break-ins and car accidents. Financial Post, FP3

LAW ENFORCEMENT / APPLICATION DE LA LOI

Dieppe Mountie gets major Interpol post

A New Brunswick Mountie and former commanding officer of the Codiac Regional RCMP has been elected Interpol's vice-president for the Americas. Todd Shean, who was born and raised in Dieppe,is currently an assistant commissioner and officer in charge of the RCMP's Federal Policing Special Services. This new position will be part of his regular duties with the RCMP. He was elected to Interpol's 13-member executive committee during the 84th Interpol General Assembly, which took place last week in Kigali, Rwanda. He is now one of three vice-presidents of the organization. Created in 1923, Interpol is the world's largest international police organization, with 190 member countries. In 1949, Canada became a member of Interpol and the RCMP was delegated the responsibility for administering and operating Canada's National Central Bureau, known as Interpol Ottawa. The bureau works with other countries through international criminal databases, the exchange of timely and accurate information and the coordination of international requests for assistance. Reached in Berlin, where he was attending the G7 summit on Monday, Shean said he plans to improve policing partnerships to advance Interpol's operational priorities. "We know that crime and all that goes with it is increasingly international," he said, emphasizing that it is more important than ever for law enforcement agencies to cooperate, corroborate and share information and best practices. Shean's 29-year career in law enforcement has included operational and leadership positions in tackling organized crime and financial crime, as well as in criminal intelligence and international policing. From 2005 to 2008, he led the Codiac Regional RCMP. At Codiac, he established a street crime unit, dedicated traffic section and other specialist officers in areas such as domestic violence. During that time, Metro Moncton had one of the lowest crime rates in the country. In 2008, Codiac had the best "clearance rate" among police forces in Canada for resolving serious crimes. Leading one of the largest RCMP detachments in the country, policing a bilingual city that is a microcosm of Canada, and providing services to three different municipalities were all good training, Shean said. "Codiac brings a number of different challenges. It really helps you prepare for other challenges." Shean has also held posts in British Columbia and Florenceville. Since leaving Codiac, he has gone back and forth between Ottawa and Fredericton. His base will continue to be in Ottawa, but he maintains a home in Dieppe. "I'm a Maritimer. All my ties are there. I'll be back." Times & Transcript, A1

'Our country benefits to this day'

Sgt. Gil Boone proudly participates in local Remembrance Day ceremonies each year with other members of the Cape Breton Regional Police Service. He is among 22 members of the Cape Breton Regional Police Service who have participated in 24 peacekeeping missions in places like Kosovo, Sierra

Leone, Jordan and Afghanistan. Each Nov. 11, he is reminded of his own time overseas, but says his service hardly compares to what others have gone through... He said it reminded him of the quality of life back in Canada and the veterans who fought in wars to make sure that was possible. "The men and women that went over and fought for us, they did so much for us, and our country benefits from it to this day. People just don't seem to realize that." That's why he marches each year in a Remembrance Day parade. This year, he'll take part in commemorations on the Northside. The RCMP manages the deployment of Canadian police on peacekeeping missions, including planning and evaluating, selecting and training personnel and providing support throughout deployment. Cape Breton Post, A3/Front

Remembrance Day ceremonies planned throughout region
Communities across southeastern New Brunswick will join Canadians across the country in pausing to remember those who have served the nation in uniform and those who made the ultimate sacrifice doing so. Here's a look at some of the main Remembrance Day ceremonies around our region. Moncton: Thousands will gather at the Moncton Coliseum for the largest ceremony in our region, organized by the Royal Canadian Legion Branch Number 6. The ceremony runs from 10:30 a.m. to noon, with a special Lest We Forget display open after the ceremony in the adjacent Agrena complex. As well, the Sunny Brae Legion will host a parade that will leave the legion, 164 Broadway St., at 10:40 a.m. and end at the cenotaph on Massey Avenue. If it rains, the ceremony moves to the Knights of Columbus Hall on Broadway. There is also the annual informal ceremony at the Victoria Park cenotaph - including veterans and anyone who has served as a police officer, firefighter or in the military - that will be held at 11 a.m. Dieppe: The City of Dieppe, in collaboration with the Dieppe Military Veterans Association, will be holding a ceremony on Wednesday, November 11, at École Anna-Malenfant to commemorate Remembrance Day. The parade, made up of veterans, cadets and members of the RCMP, will form up around 10:30 a.m. and will make its way indoors for the ceremony. Times & Transcript, A3

*** Troubled veterans lacking necessary support: critics**
It was chilly March day when former master corporal Collin Fitzgerald - one of the country's most highly decorated Afghan war veterans - decided that the way he wanted to go out was in a spray of police bullets. It was, he believed at the time, the only thing he could do to wash away the pain of his crumbling marriage and to erase from his mind the faces of dead Taliban fighters that haunted him each night, every time he closed his eyes. "I was done with life and everything," Fitzgerald told The Canadian Press. "And I cannot truly say to you what that feels like, but is a very hollow, shallow, cold place to be." He tried everything. Nothing worked. "Therapy. The alcohol had run its course, the (prescription) drugs had run their courses; I was done," he said. "You just want the pain to be done. I get it." But the fact he found the strength to go on living for his daughter, and to eventually face justice after holding police at bay for five hours at his home in Iroquois, Ont., south of Ottawa, was just the start of his nightmare. Fitzgerald soon encountered another chilling reality: that Canada's justice system often treats troubled veterans as threats to public safety. After an eight-month investigation, The Canadian Press has found that the federal government allowed key findings in the tragic shooting death of another troubled veteran with severe post traumatic stress disorder to gather dust. The B.C. coroner's office investigated the September 2012 RCMP killing of retired corporal Gregory Matters and made several recommendations to both National Defence and Veterans Affairs, including making mental-health professionals available to police emergency response teams who deal with troubled veterans. Letters obtained by CP, dated from the summer of 2014 and addressed to the coroner, show that both federal departments believe they are doing enough to reach and treat troubled military members. Canadian Press (Record, A3, Spectator, Times & Transcript, Daily Gleaner)

*** RCMP stymied in probe of Parliament Hill shooter's Winchester rifle**
The RCMP believes it has "come to a dead end" in its probe of where Parliament Hill shooter Michael Zehaf Bibeau got his gun one of the most vexing questions about the events of Oct. 22, 2014. The Mounties continue to investigate several threads of what happened that day, including whether Zehaf Bibeau had accomplices, but have not gathered evidence sufficient for criminal charges. A source with direct knowledge of the police investigation provided the update to The Canadian Press on condition of anonymity due to the ongoing sensitivity of the file. On Wednesday, crowds will gather for Remembrance Day ceremonies at the National War Memorial, where Zehaf Bibeau killed honour guard Cpl. Nathan Cirillo, shooting him in the back three times with a .30-30 Winchester rifle. The attacker quickly made his

way up Parliament Hill and into the Centre Block before being gunned down in the Hall of Honour, not far from then-prime minister Stephen Harper and countless MPs. The RCMP will honour 20 Mounties and former House of Commons security officers later this month in recognition of their bravery during the violent episode. Shortly before his attack, the gunman made a video in which he cites retaliation for Canada's military involvement in Afghanistan and Iraq as his motivation. Zehaf Bibeau, 32, plainly speaks of assaulting soldiers to show Canadians "that you're not even safe in your own land, and you gotta be careful." RCMP Commissioner Bob Paulson told a Commons committee in March that the Mounties considered Zehaf Bibeau a terrorist, and that he would have been charged with terrorism offences under the Criminal Code had he lived. Guardian (Prince Albert Daily Herald, Western Star, Telegram, Mississauga News, Brandon Sun); CTV News; Globe and Mail

*** Help sought in shooting probe - Investigative unit seeks witnesses to Friday's events**
The province's team of independent investigators is looking for witnesses as it probes a police shooting that killed a Winnipeg man Friday. Mark DiCesare, 24, died after being shot by officers near Kapyong Barracks following a police chase through River Heights around 1:15 p.m. Friday. DiCesare had been upset over a recent breakup with his girlfriend, a source told the Free Press. Whether DiCesare was armed as he led police on a chase Friday is part of the Independent Investigation Unit of Manitoba's probe, said executive director Zane Tessler... The unit is currently investigating several other cases, including the recent police shooting of 44-year-old Haki Sefa Sept. 20, the case of a stolen RCMP gun being used in a gang-related shooting that injured a teenage girl Oct. 24 and the apparent suicide of a murder suspect who shot himself after police tried to pull him over Nov. 2. Winnipeg Free Press, B1

*** Arbitration gets the boot - Carstairs backs away from option to resolve expense-claim dispute**
A former Manitoba senator has changed her mind about using binding arbitration to resolve her Senate expense-claim issues and will likely now face legal action. Sharon Carstairs, who left the Senate in October 2011, is one of 30 senators who were identified in June by the auditor general as having made what were deemed to be ineligible expense claims. Senators were given the option to repay the amount owing or go to binding arbitration with former Supreme Court Justice Ian Binnie. Those who don't repay and don't go to arbitration will be pursued in court... Former Liberal senators Rose-Marie Losier-Cool and Bill Rompkey and Conservatives Gerry St. Germain and Don Oliver also initially requested binding arbitration but have since rescinded that request. There are seven senators who still owe money from the audit who haven't sought binding arbitration, including former Manitoba Liberal senator Rod Zimmer, whose outstanding amount of $176,014 was the highest total for any of the senators identified in the audit. Zimmer's claims were related to his secondary residence as well as travel the auditor said didn't appear to be for Senate business, contracts without proper documentation, as well as gifts and taxi rides for Zimmer and his spouse in Ottawa for personal activities. All seven are among the nine whose files were referred to the RCMP to see if any criminal laws were broken. None of those senators has been charged. Winnipeg Free Press, A3

*** Un Néo-Brunswickois soupçonné d'agressions sexuelles**
Un homme âgé de 61 ans du Nouveau-Brunswick, Jean-Marie Rodrigue, doit faire face à la justice pour des agressions sexuelles graves qui auraient été commises il y a quelques années au Québec. Les faits qui lui sont reprochés seraient survenus entre 1985 et 1998 en Beauce et en Montérégie. Le Service d'enquêtes régionales de la Sûreté du Québec (SQ), avec la collaboration de la Gendarmerie royale du Canada (GRC), a procédé à l'arrestation du suspect samedi à sa résidence au Nouveau-Brunswick. L'Acadie Nouvelle a contacté la SQ pour savoir à quel endroit avait eu lieu l'arrestation, mais un agent nous a répondu que cette information «n'est pas disponible». Jean-Marie Rodrigue doit comparaître à Saint-Joseph-de-Beauce relativement à ces accusations d'agressions sexuelles. L'enquête de la Sûreté du Québec tend à démontrer qu'il pourrait avoir fait d'autres victimes. Selon la sergente aux communications de la SQ, Ann Mathieu, le suspect connaissait les personnes avec lesquelles il aurait posé ces gestes à caractère sexuel. La Presse Canadienne (Acadie Nouvelle, 7)

Youth worker left alone with violent teen
A 15-year-old Charlottetown youth in the care of the province has been placed on probation for two years after he engaged in the unwanted sexual touching of a female youth worker. The youth, whose identity is protected under the provisions of the Youth Criminal Justice Act, has been ordered by the court to attend

a sexual education program. He must undergo assessment, counselling and treatment for any underlying issue that might have contributed to the commission of this offence. That counselling could include sessions on sexual deviancy and anger management. Provincial Court Judge Nancy Orr ordered the accused to provide a sample of his DNA for the national DNA databank. She also imposed a weapons prohibition. Guardian, A1

*** 'God didn't want me to die'**

A Charlottetown youth who attempted to commit suicide by cop in the parking lot of the Charlottetown Mall was placed on probation Monday for two years on each of four weapons- related offences. The youth, whose identity is protected by the Youth Criminal Justice Act, had entered guilty pleas to possession of brass knuckles, using brass knuckles in a careless manner, using a firearm in a careless manner and possession of a weapon for a purpose dangerous to the public peace. The court was told the accused had drawn police to the rear parking lot of the Charlottetown Mall last Good Friday by placing a call to the authorities to say there was a man in the parking lot with a gun and shots had been fired. Multiple units were dispatched and when police arrived they spotted a figure with a gun, his face covered with a balaclava... Orr ordered the accused to perform 25 hours of community service on each of the four charges. He must also provide a DNA sample for the national DNA databank. Guardian, A3

Drug probe hits jackpot

A Saskatchewan police investigation dubbed Project F-Jackpot has cashed in, with four arrests and 25 charges. "The objective of this investigation was to disrupt the criminal activity and dismantle the group of individuals involved in the distribution of cocaine and crystal methamphetamine in communities in the province of Saskatchewan," said a news release issued Monday. No one was available for an interview to provide further details. The bust was made by the Saskatchewan Combined Forces Special Enforcement Unit (CFSEU), a provincewide integrated policing task force targeting existing and emerging organized criminal groups. Members of the Regina CFSEU have been involved in Project FJackpot for the past two months. The investigation concerned alleged drug trafficking by a group operating "extensively" across the province, according to the release. Saskatoon CFSEU, the Regina Police Service and RCMP units in Saskatchewan's F Division were also involved in the project. It culminated in four arrests on Wednesday. James Edward Lloyd, 36, of Regina is charged with trafficking in cocaine, possession of cocaine, meth and oxycodone for the purpose of trafficking, possession of cannabis under 30 grams, possession of proceeds of crime exceeding $5,000, and six weapons charges. Postmedia News (Leader-Post, A1)

Man critically injured in fight

Three suspects are in custody after a man was critically injured during a confrontation between two groups of people in Surrey City Centre early Monday. RCMP said that at 3:20 a.m. police were called to 108th Avenue and 132nd Street following reports of screams and two groups fighting on the street. Police found one man, in his early 20s and known to police, with a serious gash to his chest. Two men and one woman were arrested and remain in custody while the investigation continues. The victim is listed in critical condition. Postmedia Network (Vancouver Sun, A4)

Moose cull prompts protests

Dennis Day was all ready to protest a Mi'kmaq moose hunt that Parks Canada approved for Monday on North Mountain in Cape Breton Highlands National Park, but there was nothing to protest. Day, a resident of nearby Cape North, set up camp along the Cabot Trail just outside the park on Sunday night, but Mi'kmaq hunters and Parks Canada officials were still putting things in place Monday and were not expected to start hunting until Tuesday at the earliest. "I'm not even going up on the mountain," Day said Monday morning inside his roadside hut, which is equipped with a wood stove inside and a porta-potty next to it. "I'm staying right here." Day said he intends to peacefully protest Parks Canada's plan to cull up to 90 per cent of the moose population in a 20-square-kilometre area on North Mountain... However, Const. Mark Skinner of Nova Scotia RCMP said no complaints had been laid by Monday morning and police were not investigating any threats. Day said he didn't complain to police, because he didn't take an online threat he received seriously. And, he said, he has no intention of disrupting the hunt. "We just want to get our word across," he said. "I can't stress enough that this isn't against the aboriginals. This is against the park." RCMP and Parks Canada enforcement officers spent Monday morning meeting with Day and local citizens to keep things calm. Chronicle Herald, A3

Cops hunt for man
Surrey RCMP are looking for a man who allegedly tried to force his way into the home of a 15-year-old girl. Police say the man approached the teen outside her home in the 13300-block of Sutton Place around 2:15 p.m. Friday. He talked to her, then tried to go into the home uninvited. The two struggled in the doorway and the teen was able to call for help, police said. The man, described as a 25-to 30-year-old South Asian man, about 5-foot-8 with a medium build, fled in an older black car, possibly a Honda Civic. Canadian Press (Province, A8)

*** Charges laid in theft of poppy donations**
A man faces charges after poppy boxes were stolen in **Grande Prairie** gas station. RCMP were called to the business on Sunday. Corey Donald Muise, 23, is charged with theft under $5,000, possession of stolen property and failure to abide by probation orders. Grande Prairie is approximately 460 kilometres northwest of Edmonton. Postmedia Network (Edmonton Journal, A5); Edmonton Sun, A6

Missing man left financial quandary
Harold Backer, who has been missing since Nov. 3, may have left the country as a result of financial mismanagement that has cost his clients a considerable amount of money. The 52-year-old Backer, who is registered as an active mutual fund dealer with Investia Financial in B.C. and Ontario, was listed as missing last week by Victoria police. Some of Backer's clients, who asked to remain anonymous, told the Times Colonist it looks as though they have lost a substantial amount of money due to his actions. It is unknown how many clients are affected. According to Canadian Securities Administrators, the umbrella group that brings together the country's various provincial securities regulators, Backer was an active dealer with Investia but under the terms and conditions of his registration he had agreed "to be closely supervised." The Mutual Fund Dealers Association did not return calls Monday to clarify what that meant. According to a spokesman, the B.C. Securities Commission cannot comment on whether a complaint has been made against a dealer or if an investigation is ongoing... On Monday, Victoria police announced they are working with U.S. law enforcement agencies to find Backer. "Both through our efforts and the fantastic support from our U.S. law enforcement partners, such as the Port Angeles Police Department, we continue to receive tips that we're working with now," said Det. Sgt. Kris Rice in a statement. "Tips are important in a missing persons file like this and sometimes it is the smallest detail that helps." Times Colonist, A1

*** Opposition calls for action on fentanyl**
Alberta's main opposition parties say Premier Rachel Notley's government has responded with indifference as deaths from fentanyl abuse have surged in the province and turned into a public-health crisis. Ms. Notley's New Democrats have defended their response to the fast-acting opioid by pointing to the creation of a committee to review mental health care in the province. However, members of the Wildrose and Progressive Conservative parties say resources need to be allocated immediately to overtaxed health and police services. In the first half of the year, 145 Albertans died from fentanyl... A pill of fentanyl costs about $20 on the streets of Alberta's major cities and is 50 times more potent than heroin. While the drug has been tied to prescription abuse in Eastern Canada, the variant found in the Prairies is believed to be produced by organized crime. What sets fentanyl apart from other opioids is how toxic it is - two milligrams are enough to kill the average person in less than 15 minutes. Globe and Mail, A11

*** Bible Hill RCMP office undergoes renovations**
The RCMP detachment in Bible Hill is getting an expansion and facelift. Work is underway on the project that will expand and upgrade the detachment at 283 Pictou Rd., consolidating in one building all units and offices in the Bible Hill area, an RCMP news release said. “By expanding and upgrading our current detachment facility, the RCMP is making a long-term commitment to policing services in the Bible Hill area and Colchester County in general,” Staff Sgt. John Berry, Colchester District commander, said in the release. “This infrastructure project will also bring all RCMP resources in Bible Hill under one roof, which will enhance service delivery in the long run.” In the first phase of the project, the original building will be expanded by about 1,200 square metres. The original structure will be renovated and upgraded in the

second phase. When it is completed, the detachment will house eight RCMP units, including those now located in the nearby Agritech Park. Chronicle Herald (2015-11-09)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Collectibles thief granted day parole
The mastermind behind the thefts of more than 1,000 rare artifacts from universities, museums and private collections is being released on day parole. John Mark Matthew Tillmann of Fall River is serving an eight-year federal sentence for multiple counts of possession of stolen property, theft under $5,000, possession of a forged document and obstruction of justice. Tillmann was sentenced in 2013 after pleading guilty to the theft of the museum pieces, artifacts and other items in Nova Scotia. The items, which police said were worth hundreds of thousands of dollars, were recovered after police searched his Guildwood Drive home. In a Nov. 5 decision, the Parole Board of Canada granted Tillmann day parole for six months upon a bed becoming available at a community halfway house. He must return to the facility each night. Chronicle-Herald, A4

*** La maison de transition pour un importateur de cocaïne**
Après avoir purgé la moitié d'une peine de huit ans, Angelo Follano, chef d'orchestre d'un complot visant à importer 1300 kg de cocaïne éventé en 2006 durant la rafle antimafia Colisée, a convaincu hier matin les commissaires aux libérations conditionnelles de l'envoyer en maison de transition. Grand sportif, Follano, 42 ans, qui portait d'ailleurs un chandail des Bears de Chicago, de la Ligue nationale de football, a raconté aux commissaires que son implication dans le crime a commencé en raison de ses problèmes de jeu compulsif. La Presse, A8

*** Stéphane "Godasse" Gagné veut sortir de prison**
La file était longue, lundi, dans les couloirs du palais de justice de Montréal. Pendant des heures, les citoyens ont défilé devant le juge Jerry Zigman, certains dans l'optique d'être sélectionnés comme jurés, d'autres dans l'espoir d'être exemptés. Ce mardi, ils devraient être douze à s'installer dans une salle d'audience : ce sera à eux que le motard et célèbre délateur Stéphane Gagné s'adressera dans le but de faire devancer sa date d'admissibilité à la libération conditionnelle. Depuis près de 18 ans, Stéphane " Godasse " Gagné écoule le temps derrière les barreaux. Il s'y trouve parce qu'il a abattu par balles la gardienne de prison Diane Lavigne, une mère de famille choisie au hasard, le soir du 26 juin 1997, tuée pour le métier qu'elle pratiquait. Le Devoir, A4, Journal de Québec (Journal de Montréal), La Presse (La Tribune)

Psychiatric evaluation delays first-degree murder trial
Concerns over the mental state of a man convicted of first-degree murder delayed the start of his second trial for the gangland style killing of Brandon Neil Prevey. Christopher Martin Fleig, 31, was convicted in 2012 of the April 2009 drive-by shooting death of Prevey, 29, in Inglewood in Red Deer. Though Fleig did not actually shoot Prevey, the Crown believed he had orchestrated the killing. The Alberta Court of Appeal ordered a new trial on March 10, 2014, but did not overturn the conviction. Fleig's second trial started Monday in Red Deer Court of Queen's bench before Justice Larry Ackerl of Edmonton. Defence counsel Allan Fay began the trial by requesting an adjournment for a mental fitness evaluation for Fleig. Faye said he had concerns about the mental state of Fleig, citing his bipolar disorder and a recent refusal to take medication while being held at the Red Deer Remand Centre ahead of the trial. Fleig, wearing blue prisoner coveralls, was handcuffed in the prisoner box where he alternated between standing and sitting regularly. Faye told Ackerl he had visited Fleig over the Thanksgiving long weekend at the Edmonton Institution maximum security facility, and said he was lucid. But an attempt to visit Fleig at the prison this past weekend before the start of trial was thwarted by a lockdown. He later learned that Fleig was not taking his medication. (...) Fleig was convicted of first-degree murder and sentenced to life in prison by Justice Kirk Sisson on May 30, 2012. Red Deer Advocate, A1, Canadian Press (Cape Breton Post, The Guardian, The Telegram)

Cop's recorded threats halt robbery trial

A Fredericton police officer's threat toward a suspect was an abuse of process that merited a halt to a robbery and break-in prosecution, a judge ruled Monday. Michael David Johnston, 36, of no fixed address, stood trial Monday on charges of break, enter and assault at a residence at 548 Lincoln Rd. on May 24, and robbing Brittini Sowers of a cellphone and money on June 24. However, after hearing testimony and viewing video evidence Monday, provincial court Judge William McCarroll issued a stay of proceedings in the case. That means the prosecution has been halted and essentially fizzles out. The ruling came as a result of the actions of Sgt. Tim Sowers, father of the complainant, Brittini Sowers, 27. In an unexpected turn in the trial, it was revealed Sgt. Sowers had confronted Johnston at the police station after he was arrested this summer. (…)While the charges against him are now gone, Johnston remains in custody. He was federal parolee at the time of the allegations, and his parole was revoked as a result of them. It remains to be seen if that parole revocation will be lifted or if he'll have to serve the remainder of his previous federal-prison sentence for an unrelated incident. Daily Gleaner, A1

Mother hopes inquest into daughter's death will bring her peace
The mother of a seven-year-old girl killed by her legal guardians appeared shaken Monday as a coroner's inquest listened to the 911 call that led paramedics to her daughter's bruised and battered body in a Toronto apartment in 2008. Emotions broke through Bernice Sampson's otherwise stoic demeanour at least once more as the inquest into Katelynn Sampson's death began more than seven years after the girl's death. On the call, made in the early morning hours of Aug. 3, 2008, Katelynn's guardian, Donna Irving, could be heard sobbing as she told the operator the girl had choked to death on bread. "She's been laying there for half an hour and she's not breathing," she said on the recording. "I was so scared, I didn't know what to do." Irving continued to cry while the operator instructed her to perform CPR, and later mumbled: "I didn't mean to." Irving and Katelynn's other guardian, Warren Johnson, were convicted three years ago of second-degree murder in the girl's death and sentenced to life in prison with no chance of parole for 15 years. The pair beat Katelynn for months until her body went into septic shock. Canadian Press (Cape Breton Post, A9, Whitehorse Daily Star, The Telegram, The Guardian, Times Colonist), Postmedia Network (Toronto Sun, Ottawa Sun, Edmonton Sun, Winnipeg Sun, Toronto Sun, Calgary Sun), Toronto Star, Canadian Press (The Guardian, The Telegram)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

First Nations groups urge caution before government's missing women inquiry
A coalition on missing and murdered indigenous women is urging the new federal Liberal government to be cautious before launching an inquiry into the problem. The group says the failure of British Columbia's own missing-women inquiry led by former attorney general Wally Oppal should be a lesson in what not to do. The coalition, made up of more than two dozen groups and individuals, says B.C.'s investigation neglected to consult the families of the missing women and also fell short of implementing many of the final report's 56 recommendations. The group came together after their organizations were shut out of the B.C. inquiry and it has continued to meet to pursue justice for murdered and missing women. Canadian Press (Whitehorse Daily Star, 8, Red Deer Advocate, Times Colonist, Waterloo Region Record, Hamilton Spectator, London Free Press, The Province, Vancouver Sun, Globe and Mail, Cape Breton Post, The Telegram)

Government to consult on terms for missing, murdered inquiry, says Bennett
Canada's new minister of indigenous and northern affairs says pre-inquiry consultations should be launched within the next two weeks as the Liberal government lays the groundwork for a long-awaited probe on missing and murdered aboriginal women. Carolyn Bennett says the consultation process will involve speaking with the families of victims, provincial and territorial representatives and grassroots organizations. She also says it will be key to establish terms for the inquiry, including its mandate and how many commissioners should conduct the study. In their election platform, the Liberals promised to spend $40 million over two years on the inquiry. Canadian Press (iPolitics)

*** Val-d'Or: les chiffres d'une crise annoncée**

Les récentes révélations de l'émission *Enquête,* de Radio-Canada, sur les abus envers les femmes autochtones par des policiers de la Sûreté du Québec à Val-d'Or, braquent de nouveau les projecteurs sur les conditions de vie difficiles des femmes des Premières Nations. Des chiffres pour comprendre. L'Actualité

Quebec police probe shouldn't be delayed
An editorial states, "The Quebec government has taken some positive steps in the last two weeks in response to disturbing allegations made by several indigenous women in Val-d'Or, who have said they suffered physical or sexual abuse by Sûreté du Québec officers. Last Wednesday, Premier Philippe Couillard met with Quebec aboriginal leaders. he appointed Fannie Lafontaine, a human rights lawyer, as an independent observer of the probe being conducted by Montreal police. The province also pledged $6.1 million so vulnerable women in Val-d'Or can get medical and mental health help. In Val-d'Or, some police will be patrolling alongside social workers to make them more sensitive to the realities of marginalized society. However, those steps go only a small way toward addressing the enduring problems between aboriginals, police and the Quebec government. Lafontaine has said she would not have taken the post if she thought she would not be able to act independently. Let's hope her optimism proves warranted, but a fully independent investigation would have greater credibility with aboriginals, who have little trust in the SQ." Postmedia Network (Kingston Whig-Standard, A4, London Free Press)

Red dresses draw attention
A letter to the editor states, "All across the UPEI campus, there are red dresses hanging from trees. At first glance, they appeared to be nothing more than some form of a prank. However, along with these dresses are signs addressing the issue of the more than 1,200 Aboriginal women who have been murdered or gone missing. This has been a growing issue as Canadian citizens are pressing for the problem to be discussed in Parliament. Prime Minister Justin Trudeau has pledged to explore the different reasons why these women have been murdered or gone missing, and promised to give answers to those who are waiting for them. However, there is so much more to the issue than simply finding out what happened to these women. As Canadians, what can we do to prevent these disappearances from happening? Is there a way for us to save Aboriginal women before it is too late?" The Guardian, A6

Will carding crackdown tie officers' hands?
Community activists are applauding the Ontario government for proposing strict new curbs on carding. Police, to no one's surprise, are not. Some police chiefs and police unions say they are worried the curbs will hamper their ability to interact with the public and control crime. Police, of course, tend to resist any check on their authority. It would be easy to dismiss their complaints as nothing more than reflex. In this case, they deserve a hearing. Police argue that when they conduct street checks - questioning and documenting people they encounter on the beat but are not under arrest - they often learn things that help them prevent or solve crimes. Globe and Mail, A10

Police carding is not over
An opinion piece states, "Last week, the Wynne government announced draft regulations meant to herald in a new era in policing in Ontario. The proposed rules would mean the "end of carding," Queen's Park proclaimed. No longer would people be subject to discriminatory street checks by police. I was immediately suspicious. How can a government regulate a practice it is eliminating? Frustration soon turned to dull, familiar rage as I read the new policies. Carding is not over, and nothing in the draft regulations will prevent the status-quo discriminatory and disproportionate criminalization of black Ontarians. On the face of it, the regulations would prohibit police from stopping and questioning people based on race (with significant exceptions). They also state that being present in a "high crime neighbourhood" cannot be the sole reason for a street check (this doesn't scream progress to me). But let's be honest: these rules are nothing new. There are already laws in existence meant to prevent racist policing. Here's what's in the fine print: police are not to stop people based on their race, unless race is an important identifying factor in the police's search for a particular individual. In other words, carding can still happen to you - if you fit a certain description. Sadly, this is almost always the excuse used to criminalize black people. Also in the fine print: if an officer collects information from an individual in a manner that violates the regulation, there is no consequence to the officer, no recourse for the carded individual and

the identifying information is retained in the police database. In other words, police can continue to card with impunity." Toronto Star, A13

Changing the face of the force

When Ingrid Cataldo arrived in Montreal from Chile 20 years ago, she had her heart set on becoming a police officer. But like many immigrants, she had a hard time convincing her mother that being a cop is a respectable profession. Her mother wanted her to get a university degree; so Cataldo enrolled at Université de Montréal and studied social work and criminology. After receiving her diploma on graduation day, Cataldo hugged her mother and whispered something in her ear. "I told her: 'Now, I'm going to become a police officer.' " Cataldo, 41, has been a Montreal police constable for 13 years, having entered the force through an equal opportunity program at a time when the SPVM was hiring more women. Almost four years ago, the SPVM's human resources department was looking for a new recruiter, someone who could be successful in persuading members of Montreal's growing visible minority community to join their ranks. As a visible minority officer who speaks French, Spanish, Italian and some English, Cataldo felt she was a good candidate. The force agreed and gave her the difficult task of trying to woo other minorities into the police force. For years, Montreal police have talked about wanting to increase the force's diversity, and its top brass hasn't been shy about expressing frustration at not being successful. In 2014, only 317 of the force's 4,601 officers were members of a visible minority - about 6.8 per cent. Another 193 were ethnic minorities and 17 were First Nations. Former police chief Marc Parent acknowledged the department struggles to recruit non-white officers. "For some, it's a trust issue, maybe. For others, it's not a respectable profession for them," he said before his retirement this year. Among officers who work on the beat, about eight per cent are visible minorities. Philippe Pichet, the force's new chief, said that number is not high enough. Montreal Gazette, A1

Don't expect deep moral justice

A proposed class-action settlement for current and former foster children who were victims of child abuse and other crimes could cost Alberta more than $20 million. But the legal firm representing the plaintiffs says most will likely receive just $15,000 to $30,000 in compensation. An Edmonton court Friday will hear arguments about the draft settlement for victims who were in provincial care between 1966 and 2008. The class-action lawsuit was originally brought by Edmonton lawyer Robert Lee in 2004 and certified by the courts, after a long legal battle, in 2009. Since then, the courts have removed Lee from the case and reassigned it to a London, Ont., firm which specializes in class-actions lawsuits. Last week, the province and the firm, McKenzie Lake, finally agreed on a draft settlement. But for hundreds who joined the original lawsuit, the settlement may be a bitter disappointment. The lawsuit was never about holding the child welfare system accountable for physical and sexual abuses. It deals, instead, with a far narrower issue: whether the province, as their guardian, failed to take timely civil action to protect the financial rights of those abused children. The lawsuit claims the province failed to sue those who had victimized the minors and then failed to apply, on behalf of young victims, to the province's own Victims of Crime Compensation Fund. Edmonton Journal, A1

Identity crisis

He's survived being shot, stabbed and beaten with a baseball bat, so James Lathlin has plenty of experience when it comes to getting back on his feet. Lathlin has spent the last 15 years trying to make a better name for himself, but now it's his name that is causing him trouble. Lathlin speaks with children and teens about the perils of gangs and drugs. His work resulted in him being part of an art campaign last March that blanketed downtown, aiming to challenge negative perceptions of Winnipeg's indigenous residents. The campaign featured two photos of Lathlin, the first being a grim-faced portrait that read: "Drug Dealer?" The second was of a smiling Lathlin that read: "A father, son, youth counsellor, motivational speaker, coach, author, rapper and an aspiring stand up comedian." In an unfortunate coincidence, James Robert Victor Lathlin's younger cousin, James Roderick Lathlin, was identified in 2012 by RCMP in Portage la Prairie as one of more than 30 people charged in a major drug trafficking bust, dubbed Project DEMERIT. "Ever since then I've been having problems," Lathlin said. "It has sabotaged my entire life and it sabotaged that whole campaign ... because here was James Roderick Lathlin who was a drug dealer." Winnipeg Sun, A5

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

Province gearing up for new influx of refugees - With 1,000 already arrived, 2,000 more is ambitious goal

Manitoba is flowing money and putting in place the logistics to accept another 2,000 refugees, on top of the 1,000 already arrived, by the end of the year if it can be done, Premier Greg Selinger said Monday. In an interview with the Free Press, Selinger said the $1.2 million the province pledged in September for settlement services for refugees is starting to flow to the organizations so they can ramp up to prepare for an influx of people. "We're working on it, we said let's get this money moving," he said. He said the money needs to flow so organizations can hire people and get the supplies they need to manage. Prime Minister Justin Trudeau promised during the election to bring 25,000 Syrian refugees to Canada by the end of this year. Manitoba committed to taking up to 3,000 this year, which would be about 1,500 more than originally planned. It is a tall order, and some immigration experts think it may even be impossible, but Immigration, Refugees and Citizenship Minister John McCallum said Monday the government will try to make it happen. Winnipeg Free Press, A4

Syrian refugees warned of resettlement scams on social media

Ottawa's plan to usher in 25,000 Syrian refugees may have also opened the door to unscrupulous people seeking to make a profit off the backs of desperate asylum seekers hoping to resettle in Canada. Flyers and online messages have sprung up on social media offering to connect Syrian refugees with sponsorship groups and submit their refugee applications to Canada - for a fee of hundreds and sometimes thousands of dollars. But resettlement groups are warning people to beware, noting that refugee resettlement is about helping people, not about turning a profit. "You don't make money off humanitarian work. That's why refugee resettlement is under the humanitarian stream of Canadian immigration," said Brian Dyck, chair of the Council of the Canadian Refugee Sponsorship Agreement Holders Association. Government-recognized private sponsorship agreement holders say they only work directly with groups or individuals who fundraise to support the refugee they select for resettlement at a fee of no more than $100, as government rules stipulate. One recent posting on the Arabic news page, Canada Today, offered to connect Syrian refugees with private sponsorship groups, referring inquiries to a licensed immigration consultant. It is not illegal for a registered member of the Immigration Consultants of Canada Regulatory Council (ICCRC) to charge for such a service. Toronto Star, A8

Air Canada offers planes to help airlift Syrian refugees by year's end

Plans to resettle 25,000 Syrian refugees by year's end could involve assistance from commercial air carriers, at least one of which has already offered space on its planes to the Liberal government. Air Canada reached out to the new government following the election, offering its services to help ferry people to Canada as they flee the ongoing civil war and other unrest in Syria. Though the airline can't fly directly into Syria itself, it could land planes in Istanbul as well as Beirut an estimated 1 million people in Lebanon have registered with the United Nations as refugees from the conflict. "Air Canada has offered to co-op-erate with the federal government to the fullest extent possible in any operation to transport Syrian refugees," spokesman Peter Fitzpatrick said in an email. "At this point, however, we have only exchanged preliminary information." Commercial aircraft are one of a range of options the government is exploring, Immigration Minister John McCallum said Monday as he announced a new cabinet committee specifically tasked with overseeing the resettlement program promised during the election campaign. Other options include ships and military planes, and the government is also exploring housing refugees in old military bases. Canadian Press (Daily Gleaner, B1, Red Deer Advocate, Ottawa Sun, Times Colonist, Times & Transcript, Telegraph-Journal, Chronicle-Herald)

Au moins 125 familles syriennes à Québec, espère Duclos

«J'ai espoir que la région de Québec puisse contribuer à l'accueil d'une bonne partie des réfugiés syriens», a dit le ministre canadien des Familles, des Enfants et du Développement social en entrevue au Soleil. Sans détour, il a avancé le nombre de «125 familles», soit environ 500 personnes. «C'est peu pour une population de 700 000 habitants. Je pense qu'on peut faire mieux, mais je mettrais ça comme barre minimale. On peut se donner comme objectif collectif ici à Québec de faire cette contribution», a poursuivi M. Duclos. Au-delà du fait d'aider une population en détresse, Québec bénéficiera, dit-il, de l'arrivée de

réfugiés à l'heure où la région a «besoin de nouveaux immigrants et de main-d'oeuvre». Le nombre minimal de 125 familles avancé par M. Duclos est le même que celui évalué par le maire de Québec, Régis Labeaume, et différents organismes comme le Centre multiethnique. Lors d'une conférence de presse en septembre, ils avaient dit vouloir accueillir de 125 à 200 familles, soit de 500 à 800 réfugiés syriens. Récemment, le maire de Québec a toutefois déploré ne «pas avoir eu de nouvelles» du gouvernement provincial alors que sa ville est prête à recevoir ces familles qui fuient la guerre. Lundi, Jean-Yves Duclos a dit que la question des réfugiés syriens a fait l'objet d'une discussion dès la première rencontre du Conseil des ministres la semaine dernière. Le gouvernement Trudeau a encore comme objectif d'accueillir 25 000 réfugiés d'ici la fin de 2015, même si le temps file. «On travaille fort, c'est notre intention d'y arriver», a martelé le nouveau ministre. La Presse (Le Soleil); *QMI Agency (Journal de Québec)

Ils seront 25 000

De Harper à Trudeau, le contraste est saisissant en matière d'accueil des réfugiés. D'un gouvernement qui utilisait la sécurité comme prétexte pour ne pas agir, nous voilà devant un gouvernement déterminé à relever tout un défi: accueillir 25 000 réfugiés au Canada d'ici le 31 décembre.Un scénario à l'étude prévoit l'accueil de 6000 réfugiés syriens par semaine qui seraient hébergés dans des bases militaires comme celles de Valcartier ou de Trenton, selon des informations obtenues par Le Devoir. Une opération d'urgence d'envergure qui s'inspire du plan déployé en 1999 lors de l'arrivée des réfugiés kosovars au Canada. Est-ce réaliste d'accueillir autant de réfugiés en si peu de temps? «Ça dépend du niveau d'urgence qu'on attribue à la chose», me dit Janet Dench, du Conseil canadien pour les réfugiés. Si la volonté politique est là, si l'organisation suit et que les citoyens se montrent solidaires, il est clair que l'on peut accueillir beaucoup plus de gens que le gouvernement précédent ne voulait nous le faire croire. Ce qui compte, ce n'est pas d'atteindre le chiffre magique de 25 000 réfugiés le 31 décembre à minuit. Ce qui compte, c'est d'admettre qu'il y a urgence, de reconnaître que nous avons des responsabilités en matière de protection des réfugiés et d'agir en conséquence. La Presse

***Former CFB Cornwallis site offers to house Syrian refugees**

Beth Earle knows the role Canadian military bases played in helping refugees from Kosovo in 1999 and she believes that can happen again as the federal government prepares to bring in refugees from Syria. "I thought, well, that was 5,000 refugees (in 1999), they're talking about 25,000 in a very short period of time (now) and maybe we can reach out and work once again with the federal government." Earle is the CEO of the Annapolis Basin Conference Centre, located at the site of the former CFB Cornwallis. While the location didn't host anyone from Kosovo back in 1999, there is more than enough space and experience to help this time, she said. Each summer, the site serves as home to 900 people as it hosts the HMCS Acadia Sea Cadet Training Centre. With Prime Minister Justin Trudeau's government planning to bring 25,000 refugees to Canada by the end of the year, Earle decided to reach out to representatives at the National Defence Department and local political representatives to see if they need help in the way of temporary housing. "All of our facilities are inspected regularly and we do have the size of facilities and the infrastructure to help out in that way," she said. Chronicle-Herald

***Liberals look to expedite refugee process**

Immigration Minister John McCallum says a portion of the 25,000 Syrian refugees the Liberals plan to bring here will likely be housed at first on military bases, and he predicts some asylum seekers might arrive under a temporary protection program rather than as permanent residents. The Trudeau Liberal government on Monday announced it is assigning nine cabinet ministers, including Health Minister Jane Philpott and Defence Minister Harjit Sajjan, to expedite the Syrian refugee initiative. The Liberals promised during the federal election campaign to resettle 25,000 Syrians by Jan. 1 - an exceedingly ambitious goal, according to refugee advocates in this country, who say it cannot be done this fast. Refugee experts say some Syrians might arrive with more temporary status for two reasons. In some cases, Ottawa may want to speed up intake of refugees by bringing them here before screening is complete. Others might be content to live here temporarily with a plan to return to their homeland if conditions significantly improve. To expedite the arrival of 25,000, Mr. McCallum could use a ministerial permit to bring in some refugees whose security or health checks were not yet completed - and allow the rest of the scrutiny to take place in Canada. Globe and Mail, A4

***Ottawa refugee health groups prepare to welcome Syrians**
Refugee settlement and community health groups in Ottawa are trying to figure out how to best help the thousands of new refugees expected to arrive in the region in the coming weeks. John McCallum, the minister of immigration, refugees and citizenship, confirmed Monday the federal government plans to bring in 25,000 government-sponsored refugees in the next eight weeks. Assmaa Bilouni spends her days helping refugees navigate Canada's health care system. She's been watching from afar as her home country, Syria, has been torn apart by war, forcing millions of people to flee to neighbouring countries for safety. (...) Bilouni, who is now a Canadian Citizen, recently met with a group of other refugee advocates to talk about how to help the displaced Syrians when they arrive. That group, called Refugee 613, is helping co-ordinate local efforts. (...)For the past few years, Dr. Doug Gruner, a refugee doctor in Ottawa, fought the former federal government's decision to cut interim health care for some refugees and claimants. Now that the Liberals are reversing those cuts and reinstating health care for all refugees, Gruner said he's redirecting his energy into helping the new arrivals. "Now, no longer will the costs of medications and other issues like prosthetics be on the shoulders of our private sponsors, church groups," said Gruner. CBC.ca

***Now comes the tough part for Trudeau**
An opinion piece states, "In all the commentary on political affairs no insight has ever come close to matching that concocted a near half-century ago by British Prime Minister Harold Macmillan. A journalist had asked him what had been the most challenging force he had ever had to deal with. MacMillan's famous reply was, "Events, dear boy, events." To this point, Justin Trudeau has performed with exceptional, indeed quite extraordinary skill. (...) In the election Trudeau promised to bring 25,000 Syrian refugees here by the year's end. That's incomparably better than the equivalent mean-mindedness of the Conservatives. But a Canadian winter is absolutely the worst time to bring in refugees who've lived their entire life in a warm country like Syria." Toronto Star, A13

***Advice for the new immigration minister**
An opinion piece states, "New Minister of Immigration, Refugees and Citizenship John McCallum faces some herculean tasks. He has to deliver on a promise to resettle 25,000 Syrian refugees before the end of the year. In addition, in order to meet a court-imposed demand, he must find ways to provide adequate health care and medications to asylum seekers and refugees.(...) In having the first conversation, Minister McCallum may want to evaluate how Canada has been avoiding its international obligations to refugees. To keep asylum seekers far from our borders, Canada uses devices such as visas, electronic travel authorizations, agreements to outsource decision-making to other states, carrier sanctions on transportation companies, and even billboards in foreign countries advertising that Canada will rapidly deport failed asylum seekers." Ottawa Citizen

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

INTERNATIONAL

*** New defence minister warned of 2006 attack**
Canada's new minister of national defence said he warned NATO command against a fateful 2006 Afghanistan mission that sent Canadian soldiers into an ambush where four were killed, but alliance officials ignored his warning. Harjit Sajjan, who served in Afghanistan before being named to cabinet by Prime Minister Justin Trudeau last week, also criticized coalition forces for not doing enough to "look at

the root cause" of Taliban recruitment in a documentary airing this week. Sajjan, who was deployed three times to Afghanistan, was released from military service on Sunday and is no longer a reservist in the Canadian Armed Forces. Postmedia Network (Edmonton Journal, N5, Gazette, London Free Press, National Post)

*** Forces plane carrying arms to Kurds held for days in Iraq**

Iraqi officials temporarily seized a military aircraft carrying weapons for Canadian special forces in Kurdistan, amid a wave of anti-western conspiracy theories rife in Iraqi politics. The seizure and the reasons for it raise questions for Canada's new Liberal government, which has vowed to do more military training in the country. The Iraqis said they held the Canadian Forces Hercules transport aircraft, carrying supplies into Kurdistan without authorization, for four days. Some Iraqis are concerned that the Kurds, who ultimately want independence for their territory, will use the support and weapons they receive from the U.S.-led coalition to eventually break away. Postmedia Network (Ottawa Citizen, A1/FRONT, Gazette)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Sent to: !DMS - EARLY DRAFT

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 19, 2015 / 19 novembre 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Réfugiés - L'objectif réel d'Ottawa prendra plus de temps
La promesse libérale de faire venir 25 000 réfugiés syriens " parrainés par l'État " ne sera pas remplie avant le 31 décembre : le gouvernement se donne quelques mois de plus pour atteindre cette cible, a appris Le Devoir. Les réfugiés qui arriveront avant la nouvelle année seront entre autres parrainés par des organismes privés. Le gouvernement fédéral a ainsi confirmé mercredi que plusieurs milliers de réfugiés faisant partie de la cohorte des 25 000 attendus avant 2016 sont en fait des déplacés qui seraient venus au Canada peu importe les résultats de l'élection du 19 octobre. " Les demandes de parrainage provenant du secteur privé [généralement des familles qui font affaire avec des organismes] font partie de notre objectif à court terme ", a expliqué Nancy Chan, porte-parole d'Immigration, Réfugiés et Citoyenneté Canada. Impossible de savoir exactement quel sera le ratio de réfugiés parrainés par le privé ou par l'État. Le ministère soutient ne pas " avoir plus de précisions à donner pour l'instant "... Ces détails suggèrent que la pression immédiate mise sur le processus de sélection et de vérification des dossiers de réfugiés sera plus légère de quelques milliers de cas. Le **ministre de la Sécurité publique**, **Ralph Goodale**, a par ailleurs confirmé mercredi que les dossiers de tous les réfugiés seraient épluchés et qu'aucun d'entre eux ne profitera d'une vérification allégée. Les demandeurs d'asile seront rencontrés en entrevue, les données biométriques seront contrôlées, leur passé corroboré dans des bases de données canadienne et internationale. ***" Nous détaillerons les différentes étapes de contrôle quand***

le plan complet sera annoncé. Mais ce sera robuste et nous voulons nous assurer que la qualité de la vérification de sécurité, au final, est au rendez-vous ", a-t-il dit en point de presse. Ce processus de contrôle prend actuellement 12 à 18 mois. Il faudra attendre ladite annonce officielle pour préciser les délais anticipés. ***" Mais ce sera beaucoup, beaucoup plus court*** ", a certifié M. **Goodale**. Le **ministre** avait évoqué la possibilité la semaine dernière qu'une part des vérifications soit menée une fois les réfugiés en sol **canadien**. ***" Notre objectif est d'accomplir la plus grande part du travail avant que les nouveaux arrivants arrivent ",*** a-t-il affirmé mercredi. Quant aux populations ciblées par Ottawa, ce sera les ***" vulnérables, qui [soulèvent] le moins de questions [en matière] de sécurité, et des gens qui ont les meilleures chances d'avoir une intégration réussie "***, a expliqué le ministre. Ottawa demeure globalement avare de détails sur la mécanique de l'opération, à six semaines de l'échéancier qu'il s'est fixé. Mercredi, Cogeco Nouvelles soutenait que la base de Valcartier pourrait accueillir 500 réfugiés dès le 1er décembre. La base de Trenton en recevrait pour sa part 1000. Le **ministre Goodale** a refusé de commenter ces informations. Le Devoir, A1; * La Presse, A7 (La Voix de l'Est)

Processing of Syrians can be 'fast, effective'

A respected authority on immigration and refugees says **Canada** and the United Nations have the operational know-how and security safeguards to safely vet 25,000 Syrians for rapid resettlement. But the question remains: Can the humanitarian resettlement project be pulled off by the Liberal government's looming Dec. 31 deadline without compromising domestic security? (...) Immigration Minister John McCallum has repeatedly said the would-be refugees will be properly screened. "I think his implication has been that if it takes longer, if it goes over the deadline, then it goes over the deadline," Showler said in an interview with the Citizen. "Certainly my understanding from him is that getting the job done properly is the priority."(...) **Public Safety Minister Ralph Goodale** Wednesday tried to reassure **Canadians** the timetable will not compromise safety. ***"There have been very enormous efforts and thorough consultations ... to make sure that that system is strong," Goodale*** said. Michel Coulombe, director of the Canadian Security Intelligence Service, added: "I want Canadians to know that as director of CSIS I am confident that the measures in place are robust and appropriate." Under normal circumstances, Showler explained, Canada's refugee-resettlement process happens in three phases. His comments are based largely on his experience helping Syrian and other refugees in Lebanon last year... Phase three is security screening by Canada-based CSIS, RCMP and Canada Border Services Agency officers. Names, travel documents and sometime a person's biometrics are checked against national and international police and security intelligence databases. **Goodale** and CBSA president Linda Lizotte-MacPherson said Wednesday no refugees will be allowed into Canada until those checks come back clean. Postmedia News (Ottawa Citizen, A1/Front); * Postmedia Network (Vancouver Sun, Windsor Star, StarPhoenix, Calgary Herald, Leader-Post, National Post, Gazette, Edmonton Journal)

RCMP, CSIS say Ottawa's refugee plan is feasible

The heads of Canada's police and spy agencies are backing the Trudeau government's plans to safely screen and bring in 25,000 Syrian refugees by the end of the year. A number of municipal and provincial politicians have called on the government to take longer to conduct security checks on the asylum seekers, but RCMP Commissioner Bob Paulson and CSIS director Michel Coulombe insist the government's plans are feasible. As the pair spoke alongside **Public Safety Minister Ralph Goodale** at a news conference in Ottawa Wednesday, giving assurances that it can be done in that time frame without compromising the country's safety, Ontario's Health Minister told reporters how Canada's most populous province can help meet the commitment. Details so far are vague as to Ottawa's plans, but Eric Hoskins says that Ontario is looking at decommissioned hospitals as potential housing for refugees. He noted, for example, that Toronto's Humber River Hospital has moved from three sites to one... "Yes," he answered in a direct question on the government's ability to meet its deadline. "We will play a role in making the security checks and confirm people's identity. In my view, the system is satisfactory." Added Mr. Coulombe, the director of CSIS: "I am confident that the measures in place are robust and ... appropriate." **Mr. Goodale** said that the first objective of the government's promise to take in 25,000 refugees is humanitarian, in order to ***"rescue people who are in terrible conditions and fleeing from the scourge that is [the Islamic State],"*** However, he added the government would meet its objective ***"without any diminution or reduction in our security work."*** The **Public Safety Minister** said federal officials would conduct database checks and **biometrics** tests to verify the ID of all refugees, in addition

to submitting them to interviews. To do the task quickly, some officials from other agencies are being seconded to the operation, including border guards. Globe and Mail, A1

Canada-Paris link probed
The RCMP is looking into whether the Islamic State in Iraq and the Levant's claim of responsibility for the Paris attacks was made by a Canadian, a spokeswoman for the police force says. Staff Sgt. Julie Gagnon said the RCMP was "following up" on reports the English-language audio recording issued by the terrorist group sounded Canadian. "What I can tell you is that we are aware of the reports and are following up," she told the National Post, responding after she was asked whether the RCMP was investigating whether a Canadian had made the ISIL statement. A **Public Safety Canada spokeswoman**, meanwhile, said, ***"We do not generally discuss operational matters related to national security"*** but that police and security agencies ***"continue to monitor the situation in Paris very closely."*** The morning after the co-ordinated killings that left 129 dead, ISIL released a series of written and audio statements in Arabic, French and English that said "a group of believers from the soldiers of the Caliphate" were responsible. The attacks targeted "the capital of prostitution and obscenity, the lead carrier of the cross in Europe - Paris," the statements said, adding France was singled out because of its role in the international coalition fighting ISIL in Syria and Iraq. The identically worded releases offered no new information about the attacks other than what had already been reported but the familiar accent of the narrator of the English version caught the attention of some Canadians. Dozens of Canadians have joined the conflict in Syria and Iraq, some on the side of ISIL. On Tuesday, former Calgary resident Farah Mohamed Shirdon, 22, who has appeared in previous ISIL videos, was placed on the INTERPOL wanted list. Kingston Whig Standard, B1/Front (National Post); Toronto Star, A8

*** Ottawa ne voit pas de menace imminente**
Malgré les attentats de Paris, le niveau d'alerte au Canada demeure inchangé, a indiqué le gouvernement libéral mercredi, tentant de se faire rassurant. Mais les autorités ont du même souffle reconnu qu'elles ne peuvent pas garantir hors de tout doute qu'aucun des Canadiens partis rejoindre le groupe armé État islamique n'est revenu au pays. " On ne peut pas garantir à 100 % qu'on peut détecter le retour de ceux qui sont là [au Moyen-Orient] ", a consenti le directeur du Service canadien du renseignement de sécurité, Michel Coulombe. L'un des terroristes qui pourraient être impliqués dans les attaques commises à Paris vendredi dernier devait se trouver, selon les informations de la communauté internationale, en Syrie. Or, il appert qu'Abdelhamid Abaaoud aurait été tué dans l'assaut lancé en banlieue parisienne dans la nuit de mardi à mercredi, selon le Washington Post. Se peut-il alors qu'un Canadien comme John Maguire, qu'on croit mort au combat en Syrie, soit discrètement revenu au pays sans que les autorités s'en soient aperçues ? " Il y a toujours une possibilité -- l'utilisation de faux documents par exemple serait une façon d'arriver au Canada. On met en place toutes les mesures avec nos partenaires domestiques et internationaux pour pouvoir détecter le retour. Mais comme toute chose dans la vie, une garantie à 100 %, ça n'existe pas ", a admis M. Coulombe lors d'une conférence pour faire le point sur l'état de la menace terroriste au Canada. Les autorités estimaient, l'an dernier, qu'une centaine de Canadiens sont partis à l'étranger grossir les rangs des organisations terroristes.
Vigilance M. Coulombe et le **ministre de la Sécurité publique**, **Ralph Goodale**, sont cependant catégoriques : le niveau d'alerte n'a pas changé depuis l'attentat d'octobre 2014 au parlement, et les individus impliqués dans les attentats de Paris n'ont aucun lien avec le Canada. Les deux hommes ont néanmoins appelé les Canadiens à demeurer ***" vigilants ".*** Le Devoir, A2; Canadian Press (Red Deer Advocate, A5, Cape Breton Post, Guardian, Telegram); 1 (Times Colonist, A9); Agence QMI (Journal de Québec, 7, Journal de Montréal); La Presse Canadienne (Le Droit, 16, Le Nouvelliste, La Tribune, Acadie Nouvelle); Ottawa Sun, A3

*** Canadians prefer bombs over trainers against ISIL, poll finds**
Canadians broadly approve of both the country's bombing mission against Islamic State and its program of training those who fight the militant group. But if they had to choose between the two policies, more would opt for bombs over trainers, a new poll for Postmedia has found. The study by Mainstreet Research, conducted three days after the deadly terror attacks in Paris, also found Canadians were not sure the country was prepared to deal with a terrorist attack, even as they maintained they don't feel personally threatened (...) Prime Minister Justin Trudeau has vowed to end the bombing campaign on ISIL militants in Iraq and Syria before March 2015. Meanwhile, he will expand the training mission,

although details on how this will be done have not yet been provided. He told reporters this week he wants Canada to be "a strong and positive contributor to the continuing mission against ISIL." Meanwhile, more than four in 10 Canadians said they didn't think Canada was prepared to deal with a terrorist attack should one occur here. Twenty-six per cent felt the country was prepared but fully one-third said they didn't know. Nonetheless, almost twothirds said they are not concerned about a terrorist attack where they personally live or work. This last finding is in accord with the government's own message. On Wednesday, **Public Safety Minister Ralph Goodale** said there's no reason to raise Canada's threat level, even after the Paris attacks. Postmedia News (Ottawa Citizen, A10)

*** Cyberattacks on infrastructure a 'major threat,' says CSIS chief**
The head of Canada's main spy agency says he views the possibility of a cyberattack by ISIS or other extremist groups on the country's "critical infrastructure" as "a major threat." "Cyber is one of our top priorities," Michel Coulombe, director the Canadian Security Intelligence Service (CSIS) told an Ottawa news conference on Wednesday. Coulombe was responding to questions after Britain announced it is nearly doubling funding for cyber counterterrorism amid fears ISIS is looking to target Western infrastructure such as hospitals, airports or power plants by using the internet. He was flanked by RCMP Commissioner Bob Paulson and **Ralph Goodale**, Canada's newly appointed **minister of public safety**. ***"This is an area that I'm beginning to be further briefed on by the department,"*** Goodale told reporters, deferring to his deputy minister and CSIS. CBC News

*** Those calling for a refugee crackdown should tread carefully**
An editorial states "The debate over whether to adjust our refugee policies on the chance that a **terrorist** might use them to enter Canada has had less to do with calculating the actual threat - and more to do with passing judgment on hundreds of thousands of desperate people.Following the traumatic attacks in Paris last week, refugees from Syria - people without homes or food or much money - have suddenly become the key suspects in the effort to thwart future terrorist plots.In Canada, those who have taken this leap of faith include the Conservative Party of Canada, several prominent pundits and one premier. They argue the federal government should slow down on its promise to bring 25,000 refugees from the Middle East by the end of the year.While the situation remains unclear and difficult to judge, people should tread with caution before agreeing with this speedy assessment. Xenophobic fear has accompanied all major refugee migrations; it's a story as old as exodus itself. The Islamic State itself reportedly believes the refugees are apostates who deserve to die. Denying haven to so many refugees amounts to delivering them into the hands of psychopaths.(...) A complete description is unlikely, but most of the information so far available has been coming from media reports - not the government. Before the Paris attacks, **Public Safety Minister Ralph Goodale** said refugee claimants are less of a security threat than the previous Conservative government thought. He owes the public a detailed explanation of what he meant then and whether he still means it now. On Wednesday, he said officials from CBSA have provided invaluable support in refugee processing." iPolitics

ATTACKS IN PARIS / ATTENTATS A PARIS

Alleged plotter remains shadowy figure
Much about Abdelhamid Abaaoud's path to armed Islamic radicalism remains mysterious. In the words of Koen Geens, the Belgian justice minister, he mutated from a student at an upscale Brussels school into "an extremely professional commando," one seemingly able to slip across borders at will, someone who openly mocked the inability of Western law enforcement agencies to catch him. On Wednesday, the fate of the son of an immigrant shopkeeper from Morocco remained unclear. Police raided a suburban Paris apartment where they believed he was hiding. The siege ended with two deaths and seven arrests but no definitive information on Abaaoud, who French authorities have called the mastermind of the violence that killed at least 129 in Paris last week. The wanted jihadi's own father believes prison - where he served time for petty crimes - changed him for the worse. After his son got out, Omar Abaaoud noticed "signs of radicalization," the elder Abaaoud's lawyer, Nathalie Gallant, told RTBF broadcasting Wednesday. If so, that would fit the pattern of a number of jihadis who were radicalized in prison. Associated Press (Chronicle-Herald, A15, Ottawa Sun, Telegraph-Journal, Times & Transcript); * Agence France Presse (Le Nouvelliste, 3, La Tribune)

*** Le cerveau des attaques mort ?**

L'Europe nageait en pleine confusion hier, alors que tous s'interrogeaient à savoir si le présumé «cerveau» derrière les attentats de Paris était bel et bien mort lors de l'assaut de sept heures à Saint-Denis. «Le présumé chef des attentats de Paris (Abdelhamid Abaaoud) a été tué hier lors de l'assaut de la police française, ont affirmé deux hauts responsables des autorités européennes», a écrit le Washington Post hier. Mais aucun autre média ni les autorités françaises n'ont confirmé cette information, ce qui a soulevé plusieurs questionnements dans la population. L'opération a été «extrêmement difficile » en raison de «l'usage de fusils d'assaut, de tirs de sniper et d'une grande offensive d'explosifs», a lancé le procureur de Paris, François Molins. L'opération qui a duré sept heures visait bel et bien le présumé «cerveau» des attentats de vendredi. Au moins deux personnes sont mortes, dont une kamikaze qui «a activé son gilet explosif au début de l'assaut», a précisé la police qui n'a pas confirmé les noms. De plus, huit personnes ont été placées en garde à vue après l'opération, mais ni Abaaoud, ni Salah Abdeslam, l'un des suspects des attaques toujours en fuite, ne figurent parmi elles. Une information qui laisse donc croire qu'Abaaoud serait le deuxième mort. Le Journal de Québec, 5 (Journal de Montréal); * Daily Gleaner, B1 (Telegraph-Journal); Associated Press (Toronto Star); 1 (Ottawa Sun, Calgary Sun, Winnipeg Sun, Toronto Sun); CNN

AIR FRANCE FLIGHT DIVERTED

Passengers aboard Air France Flight 055 didn't learn that a bomb threat was the reason their Paris-bound flight was being diverted to Halifax until after they landed Tuesday night. Genevieve Lapeyre, a pediatric anesthesiologist from Geneva, was flying back to Europe after a meeting in Washington, D.C. She is half-Swiss and half-French, and planned a three-day layover in Paris. The terrorist attacks Friday gave her a strong wish to be in the city. (…) None of the passengers panicked, but they felt something odd was going on, she said. At one point, she wondered if there had been another attack against Paris and the aircraft couldn't go there. After the Boeing 777 touched down at about 10:15 p.m., she soon realized there was something happening regarding her flight. "I saw the firemen and everything, and I said, 'OK, there is something else.'" Lapeyre said the pilot seemed to be trying to control his emotions. "He said, 'Don't worry.' He was too much trying to reassure us." On the tarmac, passengers were told to grab their belongings and get off the plane, which they did quickly. However, they were then housed for about 30 minutes in a bus parked alongside the aircraft, which some considered dangerous, she said. Halifax RCMP spokesman Cpl. Greg Church said 262 passengers and crew got off the jet within 15 minutes of landing, which is when officers began checking for explosives; none were found. The jet was declared explosives-free at 4:28 a.m. Wednesday. The passengers were taken to a secure area to pass through customs. Postmedia Network (Chronicle-Herald, A1, Guardian, Whitehorse Star, Acadie Nouvelle); Postmedia Network (Cape Breton Post, A9)

'Like A War Zone'

2 Dead, 8 in custody after paris police launch a massive early-morning raid against a suspected **terror** cell located in a reinforced apartment When Tagara Traoré, a former revolutionary soldier in his native Burkina Faso, was jolted awake by a boom early Wednesday, his "military reflex" kicked in. "You get up quickly and either hide or try to get out," he said. In socked feet and wearing the sweatpants he was sleeping in, he grabbed his key and ran out the door of his fourthstorey apartment, only to find a battalion of police rushing up the stairs, headlamps glaring. "I started sensing tear gas that was coming up the stairwell. I thought the building was on fire," he said. "The police told me, 'Go down, down, down!' There were so many they had to move aside to let me out." It was 4:20 a.m., and he had been caught in the middle of a massive anti-terror operation that quickly became a protracted gun battle between police and terror suspects. A woman in the targeted apartment in the Paris suburb of Saint-Denis, identified by French media as a native of nearby Clichy, was one of the dead. Initial reports said she killed herself by detonating an explosive vest, but the French prosecutor's office later said the "point needs to be verified by an analysis of the body and human remains." At least one other suspect in the apartment was killed and eight people were taken into custody. Five police officers suffered minor injuries, and a police dog - Diesel, a Belgian shepherd - was killed by the terrorists, according to the national police. Paris prosecutor François Molin said the targeted apartment had a fortified door that withstood initial police attempts to break in and gave the terrorists time to mobilize and return fire. Daily Telegraph (Windsor Star, N1/Front, National Post, StarPhoenix, Gazette); 1 (Vancouver Sun, B1/Front, Leader-Post, National Post, Edmonton Journal, Ottawa Citizen, Whig-Standard, Calgary Herald); Toronto Star, A1; Globe and Mail,

A1; * Agence France Presse (Le Soleil, 22); * Associated Press (Times Colonist, A13, Times & Transcript)

Prochaine station, la guerre
Il devait être 4h20 quand Fares s'est mis à crier. «Maman! Maman! La guerre commence! Il y a des bombes!» Fares a 7 ans. De grands yeux noisette dans lesquels on lit l'effroi. «Il ne sait même pas c'est quoi, la guerre», me dit sa mère Souhila, 38 ans. Souhila, elle, sait. Elle est née en Algérie... J'étais dans l'avion quand l'assaut antiterroriste a été donné à Saint-Denis, dans la banlieue nord de Paris, non loin du Stade de France. Dès que l'avion s'est posé, des cellulaires de passagers ont sonné. «C'est la pagaille à Saint-Denis.» La «pagaille», le mot est faible. C'est Fares qui avait raison. Ça ressemblait plus à une guerre. Rue Corbillon, à l'angle de la rue de la République, au moins deux personnes ont été tuées, dont une femme kamikaze qui a activé sa ceinture d'explosifs. Un commando, lourdement armé, qui semblait prêt à passer à l'acte, a été démantelé. Pendant une heure, les habitants du quartier ont entendu des tirs nourris. Le bruit était si fort que certains ont cru qu'il y avait un bombardement. Il y a eu au moins 5000 munitions tirées par la police. Un immeuble éventré, criblé de balles. Des voisins terrorisés. Comme si on était à Gaza et non en banlieue parisienne. L'assaut a duré sept heures, durant lesquelles le quartier a été bouclé, le métro, fermé, les écoles aussi. Des résidants ont été évacués. Les riverains ont été sommés de ne pas sortir de chez eux. Une fois l'assaut terminé, j'ai pu prendre le métro pour la guerre. La Presse, A4/Front

Mission
Ce sont des spécialistes des assauts risqués, qui montent au front contre les pires terroristes. Le RAID, le commando de la police française qui est intervenu hier à Saint-Denis, est constamment sollicité depuis un an. A Paris, La Presse s'est entretenue avec l'ancien chef des négociateurs de l'unité, Christian Caupenne, pour dresser le portrait d'une équipe devenue mythique. Fondé il y a 30 ans, le RAID (pour Recherche, Assistance, Intervention, Dissuasion) est l'unité d'élite de la police nationale, destinée à intervenir partout en France pour contrer le terrorisme et le «grand banditisme». Elle est notamment intervenue lors de l'attaque du marché Hyper Cacher en janvier et à la salle de spectacle Bataclan, vendredi dernier. Selon le chef de la police nationale, Jean-Marc Falcone, l'assaut à Saint-Denis a été l'un des plus difficiles que ses troupes ont connu. «Les scènes vécues par le RAID sont très dures. Même ces hommes rodés à la violence ont été marqués», a-t-il déclaré hier à ce sujet. La Presse, A5/Front

*** Paris attacks: Extremists may strike next with chemical, biological weapons, French PM says**
With France still reeling from last week's deadly attacks in Paris, Prime Minister Manuel Valls warned Thursday that Islamic extremists might at some point use chemical or biological weapons, and urged lawmakers to extend a national state of emergency by three months. "Terrorism hit France not because of what it is doing in Iraq and Syria ... but for what it is," Valls told the lower house of Parliament. He added, "We know that there could also be a risk of chemical or biological weapons." Valls did not say there was a specific threat involving such weapons. The French Interior Ministry and Paris prosecutor's office, meanwhile, said it still remains unclear whether the suspected mastermind of last week's attacks, in which 129 people were killed and hundreds of others wounded, has been killed or is still at large. Officials said authorities are working on determining whether 27-year-old Belgian Abdelhamid Abaaoud was among those killed in a chaotic and bloody raid on an apartment in the Paris suburb of Saint-Denis on Wednesday. Associated Press (CBC News)

*** Belgium vows crackdown on terrorists, boost security spending**
Belgium's prime minister on Thursday called for changes to the country's constitution to combat extremists, and promised hundreds of millions of euros to boost the security forces. Addressing the federal parliament as security forces were conducting raids around the capital Brussels, Charles Michel pledged to use changes to the constitution to extend preventive detention times for suspects from 24 hours to 72 hours. He also affirmed that Belgium would move forward alone on a system of airline passenger information sharing that European Union nations have been incapable of agreeing in four years. Associated Press (CTV News, Times Colonist)

*** EU to tighten anti-terror laws**

The European Commission, the EU's executive arm, will expand its anti-terrorist legislation early next year to target fighters like those involved in the Paris attacks. The new measures will widen the range of actions punishable under the legislation to include travelling for the purpose of carrying out a terrorist act, facilitating travel or receiving training to carry out an attack. In a direct response to the Paris killings, EU citizens who travel outside the bloc and then return to carry out attacks will be considered as foreign fighters, and those helping their movement will also face prosecution. The bloc 's Migration, Home Affairs and Citizenship Commissioner, Dimitris Avramopoulos, told a news conference Wednesday that the Commission would have proposals ready by the end of November and wants to see them enacted "within the first two months of the next year." Toronto Sun, A56 (Calgary Sun)

*** Killer's passport fueling fear of refugees**

After the bombs and Kalashnikov fire of the Paris attacks, a mere document - a passport - found near the body of an attacker is generating a new wave of dread throughout Europe and beyond. But whether the document ended up there by chance, or was part of an elaborate plot to sow panic, is not clear. Regardless of the answer, the passport has played into the Islamic State group's hands by raising concerns that militants may be marching alongside the thousands of asylum seekers flowing into Europe. That possibility is redefining the debate over immigration in Europe and even the United States, and prompting a backlash against Muslim refugees. The far-right French leader Marine Le Pen called for an immediate end to the flow of migrants into France, while across the Atlantic about half of U.S. governors are taking steps to prevent absorbing Syrian refugees in their states, citing the passport. "This terrorist attack will clearly change Europe's refugee policies and how the arrivals in Europe are treated," said Konrad Pedziwiatr, a sociologist and expert on Islam in Europe at the Krakow University of Economics. "Already the open-door policy (in Germany and Sweden) of welcoming refugees was going to be reformed because the inflow is so significant that countries cannot cope with the numbers," he said. "What the Paris attacks add to this difficult situation is the additional element of fear." A passport bearing the name of Ahmad Al Mohammad, 25, was found near one of the suicide bombers who blew himself up outside the Stade de France football stadium. It indicates that he entered Greece from Turkey on Oct. 3 and later passed through Serbia and Croatia, getting registered in every new country. The passport's authenticity has not been determined, but fingerprints of the attacker match those taken by Greece and Serbia. The other attackers who have been identified so far are all European citizens. The oddness that a passport - an intact one - was found near a man who blew himself up is creating suspicions that it is part of a plan by the Islamic State to create a backlash against the refugees. "I have never heard of terrorists carrying passports with them," Pedziwiatr said. Associated Press (Whig-Standard, B5, Telegraph-Journal, Times & Transcript)

*** ISIS is slowly killing the European experiment**

As neighours and allies declare solidarity with France, few are facing up to the inevitable: the fact that fallout from Friday's terrorist attack in Paris will stall - perhaps even reverse - the political integration of Europe. The discovery that most of the terrorists identified so far were Muslims born in France, using neighbouring Belgium as a base, will add volume to loud demands for an end to the open-border policy among the 28 members of the European Union. Pressure to terminate what is known as the Schengen Area - a pillar of the EU political integration project, along with the now-debased euro and attempts to unify foreign and defence policies - has been building as about a million refugees from the Middle East and North Africa have flooded into Europe (…) While ISIS has taken responsibility for the outrage and was, at the very least, the inspiration for it, the Paris killings were, like almost every other terrorist attack in Canada, the United States and Europe in the last 14 years, a home-grown affair. Neither Canada nor the U.S. is immune to the popular suspicion that the floods of Syrian and Iraqi refugees are an easy route for ISIS to plant terrorists in target countries. The governors of over half the 50 states in the U.S. have said they will not participate in settling Syrian refugees. And the new government of Prime Minister Justin Trudeau is facing growing pressure from both the public and provincial governments - on whom much of the responsibility for resettling refugees will fall - to rethink his campaign pledge to allow 25,000 Syrian migrants into Canada by the end of the year. iPolitics

*** French expats still feel sting an ocean away**

Juliette Elchinger was home in Montreal on Friday evening when her Twitter feed lit up with news of the terrorist assaults in Paris. "I went into a state of shock," the native Parisian said. "I just started to shake and cry." Five days later, the 19-year-old was still struggling to make sense of the violence visited on her cherished city. She stood on Wednesday surrounded by knots of other students and staff at the University of Montreal, some holding hands and wiping tears off stricken faces, for a sombre gathering of commemoration. In the days since the shocking attacks took the lives of 129 people, Ms. Elchinger has attended solidarity marches and commemorations, monitored news from Paris obsessively and joined other members of Montreal's large expatriate French community. Some have connections to the tragedy; Ms. Elchinger's best friend lost a professor, who was slain at the Bataclan theatre along with 88 others who had attended a rock concert there. For the expats, separation from events back home has fed feelings of loss and helplessness, along with a deepened call to their French identity. Globe and Mail, A9

*** Free world solidarity after Paris**

An editorial states, “There aren't a lot of game-changing moments in international affairs, says Peter Van Praagh. But the ISIS terrorist attacks on Paris last weekend, like the 9-11 attacks on New York and Washington in 2001, fall into that rare category. It is, he says, one of those "events that turn things." It has acutely heightened the public sense of "how vulnerable open societies are." But it has also produced, he believes, "a fundamental solidarity and common understanding that something has to be done to address it." "We are all affected now," the security specialist told our editorial board on Wednesday, after arriving in Nova Scotia to chair, for the seventh time, the annual Halifax International Security Forum. The forum will bring 300 delegates from 60 democratic countries to the city this weekend to brainstorm the complex angles of peace and security - military, political, economic, educational and cultural. The group ranges from four-star generals to ministers to aid organizations, journalists and scholars. Their agenda runs the gamut from building new anti-terror alliances to cutting off the financing of terrorism through drug and human trafficking. There was plenty of evidence in Halifax and elsewhere this week to show security issues now touch us all.” Chronicle-Herald, A6

*** Hollande faces the enemy from within**

The streets of Paris are no strangers to mass bloodshed. The City of Light has borne witness to more than its share of extreme violence over the centuries. The worst of it has not been perpetrated by a foreign army. The enemy has most often come from within.From the Wars of Religion, through the Revolution and the Reign of Terror, to the Paris Commune, the French often worked through their differences in the bloodiest ways possible. Since the 1960s, Paris has been a repeated target of terrorists, often French citizens or immigrants, aggrieving in some way France's unresolved colonial past in North Africa or its mandates in the Middle East.The inspiration for the most recent attacks may have come from Iraq or Syria, but their perpetrators came from the Paris suburbs. The January assaults on the satirical magazine Charlie Hebdo and a kosher supermarket were conducted by French-born radicalized Muslims. Most of those involved in Friday's sickening attacks on cafés and a concert hall appear to have had similar backgrounds."We know, and it's cruel to say it, it was French people who killed French people on Friday," President François Hollande said in a speech for the ages. "There are, living on our soil, individuals who move from delinquency to radicalization and then to terrorist criminality." Globe and Mail

*** La vie doit reprendre, dit Hollande**

Dans la foulée de la série d'attentats à Paris, le président français François Hollande a encouragé ses compatriotes à «défier les terroristes» en continuant de vivre normalement, en fréquentant les cafés, les musées, et les stades sans tomber dans la crainte et la xénophobie. Les terroristes prennent la vie des innocents, mais ils veulent aussi suspendre celle des autres, a soutenu le président, mercredi, lors d'un discours télévisé devant les maires de partout au pays. Il estime que les Français ont le «devoir» de poursuivre leurs activités normales. Il a martelé que la vie «devait reprendre pleinement», ajoutant que la sécurité serait resserrée dans les lieux publics. Le président français a assuré que la France resterait un pays «de liberté, de mouvement, de culture» qui ne «pliera pas à la peur». François Hollande s'est engagé à travailler avec ses alliés pour détruire le groupe armé État islamique, qui a revendiqué la responsabilité des attaques dans la capitale française qui ont fait 129 morts et 368 blessés. Dans une allocution prononcée quelques heures après une opération antiterroriste de la police en banlieue de

Paris, le président a réitéré que la France était «en guerre avec les terroristes», mais il a aussi appelé les Français à la retenue. Associated Press (Le Droit, 17)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Coderre veut éviter un autre Lac-Mégantic**
Depuis la tragédie de Lac-Mégantic, la Ville de Montréal se fait beaucoup plus prudente dans l'aménagement de son territoire, a expliqué Denis Coderre, hier, en réaction au reportage sur la récente interdiction de toute construction près des installations de Suncor. En revanche, au gouvernement du Québec, on ne s'émeut guère de la situation. Hier, La Presse faisait état d'un moratoire interdisant toute construction dans un rayon de 435 mètres des trois ballons de butane de Suncor. Même une enseigne de quatre pieds sur six ne peut y être installée. Le Centre de sécurité civile juge cette zone rouge à «risque très élevé» dans l'éventualité d'un accident impliquant les sphères de butane. Une explosion est jugée peu probable, mais elle provoquerait d'énormes dégâts. Or, cette zone rouge est traversée par l'autoroute Métropolitaine et 100 000 automobilistes y circulent chaque jour. La Presse, A16

*** Crise en santé publique - La surveillance de l'état de santé des Méganticois écope**
Bien que les impacts de la tragédie de Lac-Mégantic se fassent toujours sentir dans la population, la Direction de santé publique de l'Estrie a été contrainte de se départir de deux experts qui travaillaient de façon spécifique sur ce dossier. En janvier dernier, la Direction de santé publique de l'Estrie publiait une étude révélant que l'accident ferroviaire survenu à Lac-Mégantic en 2013 faisait encore souffrir la population : 95 % de Méganticois disaient avoir été touchés par la tragédie. On observait plus de dépressions, de troubles anxieux et de problèmes de consommation d'alcool. La directrice de la santé publique, la Dre Mélissa Généreux, s'en inquiétait. Pourtant, quelques semaines plus tard, elle mettait à pied le professionnel affecté à la surveillance de l'état de santé de la population de Lac-Mégantic. Ce dernier a fait les frais d'une vague de compressions imposée à toutes les directions de santé publique régionales au printemps dernier, dont Le Devoir tente de cerner les impacts dans une série diffusée cette semaine. En Estrie, la Direction de santé publique a dû couper 1,21 million sur un budget de 2,5 millions. " Ça représente 40 % de notre budget, ça a été toute une épreuve pour nous, tout un choc à absorber ", soupire Mélissa Généreux en entrevue téléphonique. Avec son équipe, elle a tenté de faire les choix " qui allaient engager le moins de conséquences possible sur la population ". Mais elle devait couper quelque part. " Ce n'est pas parce qu'on s'est dit que les impacts étaient moins importants, mais quand vient le temps de choisir les postes, il y a toutes sortes de considérants, en matière d'ancienneté entre autres. " L'enquête annuelle sur la population de Lac-Mégantic, qui est financée par un autre " petit budget protégé ", sera maintenue. " Ce qui a été plus difficile, c'est que parallèlement à ça, on ne voulait pas surveiller juste une fois par année, on avait donc un agent de programmation, planification et recherche (APPR) -- celui dont on a supprimé le poste --, qui se chargeait de faire des bulletins de surveillance périodiques. C'est lui qui prenait le crayon et qui faisait l'analyse de ces données. " Le Devoir, A1

*** Spend more to prevent dam spills, experts say**
As miners globally review the way they store waste in the wake of another horrific dam spill, the solution may be as simple as it is dramatic: spend a lot more. Images of sludge spewing into towns and rivers could be a thing of the past if mines used different types of storage such as removing water or building on more stable ground. While that can be as much as 10 times costlier for companies already squeezed by slumping prices, the cost is much higher when things go wrong. The cleanup bill for the Nov. 5 spill at the Samarco iron-ore venture in Brazil, owned by BHP Billiton Ltd. and Vale SA, probably will exceed $1 billion US, Deutsche Bank AG said. Then there's lost output and potential lawsuits. "A failure is a lot more expensive than doing it right," said Dirk van Zyl, professor of mining engineering at the University of British Columbia and one of three experts on a panel into a dam spill in Canada last year. Samarco says its dams were deemed safe in a July inspection and that it's too early to determine reasons for the spill. On Monday, BHP chief executive officer Andrew Mackenzie said the company is "carrying out a thorough review of all of our dam facilities of scale." On the same day, Vale said it's open to improvements, even after concluding that its other installations, which use state-of-theart safety practices, were fully compliant. The Samarco breach, which propelled about 50 billion litres of mud into communities below, comes a

year after Imperial Metals Corp.'s Mount Polley mine in Likely, southeast of Prince George, also dumped billions of gallons into lakes and rivers. Bloomberg (Vancouver Sun, D3)

*** Lepreau residents evacuated in simulation**
As an imaginary cloud of radioactive steam was vented from the Point Lepreau nuclear power plant Wednesday, real calls went out to residents within a 20 kilometre radius telling them to get out. By noon about 150 people were gathered in the gym at the G. Forbes Elliot Forbes Athletics Centre at UNBSJ and there was even space set up nearby for pets in a separate centre run by a disaster animal response team from Nova Scotia. It was the final part of a two-day exercise simulating a nuclear emergency at the power plant based on a couple of years of planning. The emergency was centred around an extreme bad weather event damaging the plant, said Meghan Gerrish a spokeswoman for NB Power... In September members of the media were given a tour of the plant to see the four large, mobile, diesel power generators that were added as a second level of backup to make sure there would always be power to control the equipment. The plant already had a backup generating system but the portable generators are a second level. Large water pumps capable of shooting streams of water over the outside of the reactor to cool it were also purchased. At that time Tony Munn, emergency preparedness manager at the plant, said the industry has learned many lessons from the three major nuclear accidents in the past 50 years - Three Mile Island in the United States, Chernobyl in Russia and Fukushima in Japan. Observers from utilities around the world were at the power plant during the exercise, Gerrish said. "There are over 1,000 people involved in this exercise," she said. Telegraph-Journal, B1

*** Body found near site of Tofino whale-watching tragedy - BC Coroners Services says it can't confirm if it's the passenger who was missing, presumed dead**
A body has been recovered close to Vargas Island near Tofino, B.C., says the BC Coroners Service.On Oct. 25, a whale-watching boat capsized in the area, killing five people. Another victim, 27 year-old Australian Raveshan Pillay, was never found, but presumed dead."While I appreciate there is certainly interest with the possibility this may be linked to the missing person from the Leviathan, it is premature to suggest so," said Matthew Brown with the Coroners Service. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Terror travel investigations on the rise
Radicalized Canadians intent on going to far-off combat zones are developing sophisticated cover stories and using "broken travel patterns" to disguise their true motivations, according to an internal RCMP document that reveals public safety officials were, as of one year ago, closely monitoring about 50 foreign fighters abroad and 14 who had returned home. Family and friends are often reluctant to notify police if they suspect someone is planning a trip, the document states. Also, the speed with which a person becomes radicalized to violence and makes travel plans is sometimes so fast, police only become aware of them after they've left the country. "There is no doubt that the number and complexity of terrorist travel investigations has increased," said the briefing document, which was prepared for the RCMP commissioner and obtained by the National Post through an access-to-information request. Though the document was prepared a year ago, many of the challenges of identifying extremist travellers persist, said a Dalhousie University researcher studying Canadian foreign fighters. Amarnath Amarasingam said much of ISIL's advice to people who want to migrate to Syria is to "blend in to Western ways of life," especially right before they leave... The wave of attacks in Paris last Friday that killed 129 people has heightened concerns about the foreign-fighter phenomenon. A new report this week from the think-tank Institute for Economics and Peace said an estimated 25,000 to 30,000 foreign fighters from 100 countries have flowed into Iraq and Syria since 2011 - half from neighbouring countries and a quarter from Europe and Turkey. Public safety officials in Ottawa said Wednesday there was no evidence of any Canadian involvement in the Paris attacks. They were also unaware of any direct threats to Canada related to the attacks. Amarasingam said he believes at least 60 Canadians have gone to fight in Iraq and Syria. One of them, Toronto-born Farah Mohamed Shirdon, who police say has served in combat, recruiting and propaganda roles with ISIL, was added to INTERPOL'S wanted list this week. Neither Bob Paulson, the RCMP commissioner, nor Michel Coulombe, director of the Canadian Security Intelligence Service, would say Wednesday how many high-risk travellers their agencies are tracking. Postmedia News (Vancouver

Sun, B1/Front, National Post, Ottawa Citizen, Windsor Star, Leader-Post, StarPhoenix, Calgary Herald, Gazette, Edmonton Journal, Province)

Ontario accent heard in video?

Investigators are working to confirm a potential Canadian accent heard in an English audio recording released by what is believed to be the Islamic State. The recording was released Saturday and claims responsibility for the terrorist attacks that shook Paris and the rest of the world last weekend. "It is concerning if it is Canadian, but it is speculative at this stage," said RCMP Commissioner Bob Paulson told a news conference Wednesday, adding that the Mounties are working to confirm it. Meanwhile, a dialect expert south of the border said it's very likely the male speaker has a Canadian - specifically an Ontarian - accent. "I mainly listened for vowel variations because that's where most of the variation in English is," said Erik Thomas, a linguistics professor at North Carolina State University. The professor was first asked by CNN to analyze the recording. He took detailed notes on words chosen by the speaker in the recording, such as "explosive" and "hand". "Everything he uttered seemed to match up with forms that predominate in Canada," he said. Certain vowels, such as the short 'o', were among the giveaways suggesting the accent originated in regions of either Canada or northern U.S. states. Winnipeg Sun, A7 (Ottawa Sun, Toronto Sun, Calgary Sun, Toronto Sun)

Hatred burns hot, but not very bright

Among responses to the scattered targeting of Muslims in the wake of the Paris attacks, the most indicative might be the safety preparations under way at a Hindu temple in Hamilton, Ont. Hindus had nothing to do with the killings in Paris. The "brains" behind the terrorist bloodshed appear to have lived in Belgium, not India. The preparations in Hamilton are predicated on the assumption that the sort of people who firebomb mosques and beat up helpless women won't know the difference. In other words, that they're so stupid they direct their hatred at anything that strikes them as vaguely Middle Eastern, even if they're off by an entire culture and a continent or two. There's good reason for their concern. The temple was set aflame in the days following the 9/11 terror attacks in the U.S., by someone who apparently confused it with a nearby mosque. A number of synagogues were also targeted at the time. Hatred may be all-consuming, but it's not very smart. That's already evident from the incidents of the past few days. The only mosque in Peterborough was torched by a person or persons unable to grasp the difference between peaceable people going about their life and the barbaric practices of the terrorists who characterize themselves as the Islamic State. A woman picking up her son at a school in Toronto was kicked, beaten and robbed in mid-afternoon by two men who are so stupid they think a hijab - which she was wearing - must signal support for the sort of brutalities meted out in Syria, most often on Muslims themselves. In Montreal, a man wearing a mask threatened to kill an Arab or a Muslim every week, obviously too dim to realize that plenty of Arabs aren't Muslims. There's a difference between ignorance and stupidity. Ignorance is a lack of knowledge. Stupidity is the determined projection of ignorance. It's likely that the people responsible for the incidents in Toronto, Peterborough and Montreal are both, but while ignorance is likely, stupidity is certain. Postmedia News (National Post, A1/Front)

Man charged after threat to kill Arabs in Quebec

A Montreal man will spend the next few days in jail after being charged in connection with a YouTube video in which someone wearing a Joker mask says one Arab would be murdered in Quebec every week. Jesse Pelletier, 24, was arraigned on Wednesday on charges of uttering threats, possession of a false weapon, public incitement of hatred and hoax regarding terrorist activities. Pelletier, who was arrested early Wednesday morning, will remain behind bars until his bail hearing Monday. The person in the video was wearing a Joker mask and could be seen brandishing what looked like a pistol as he made the threats and spoke about last week's terrorist attacks in Paris that killed 129 people. "It's really time to act," the person said in the three-minute video. Canadian Press (Times Colonist, A8, Calgary Sun, Telegraph-Journal, Times & Transcript, Toronto Sun, Winnipeg Sun, Kingston Whig-Standard, Ottawa Sun, Edmonton Sun, Red Deer Advocate), Presse canadienne (La Tribune, Voix de l'Est, Le Droit, Le Devoir), Montreal Gazette, Toronto Star

***To combat extremism, we must work together**
An opinion piece states "Last week, evil struck. There were vicious attacks in Paris, Beirut and Baghdad. I grieve with the families and friends of the victims and hope the perpetrators are brought to justice. Violent extremism is universally condemned; terror is never the answer and the loss of one innocent life is equal to that of all of humanity. We cannot let such horrific violence achieve its goal of striking fear into our communities and dividing us. It is deeply distressing to many that there has been apparent backlash against Muslim communities, including in Canada. In Peterborough, Ont., a mosque was set on fire last Saturday. Police are investigating the fire as a potential hate crime. This week in Toronto, a hijab-wearing woman was verbally assaulted, punched repeatedly in the stomach and had her hijab ripped off. Canadian Muslims are naturally very concerned. At the same time, Canadian Muslims know these cowardly acts do not represent our society. They are simply the ignorant expressions of criminals (…) Experts point out that there is no single reason why such people travel the path of radicalization. The roots are complex, the solutions not obvious. And combating the problem is made yet harder by the reality that this new brand of brazen terror is a contemporary phenomenon - it did not exist in the 1980s or 1990s. Toronto Star, A25

*** Doctor to assess man caught with knife on Parliament Hill**
A Toronto man arrested for allegedly carrying a hidden weapon at the entrance to the Centre Block of Parliament was remanded in custody Wednesday. Yasin Ali, 56, was detained by the Parliamentary Protective Service on Tuesday after a security screening discovered what police say was a knife. Ali made a brief court appearance Wednesday on a charge of carrying a concealed weapon. Defence lawyer Peter Azzi said his client is due back in court on Friday and will be assessed by a doctor. Neither Azzi nor the RCMP would discuss media reports that described the weapon as a meat cleaver. RCMP Commissioner Bob Paulson applauded the "great job" by the protective service, for which the Mounties have day-to-day responsibility. "The individual was identified behaving oddly, suspiciously. And one of our officers challenged him, saw the knife, took him into custody," Paulson said. "I understand that it is less a concern around socalled national security considerations than it is a mental-health issue." Security on Parliament Hill has been tight since Oct. 22, 2014, when Michael Zehaf Bibeau gunned down a soldier at the nearby National War Memorial and sprinted through the main doors of Centre Block. Moments later, Zehaf Bibeau was fatally shot by security officials outside the Library of Parliament. Canadian Press (Times colonist, A8)

*** Des musulmans sur leurs gardes après des menaces**
Menaces de mort au téléphone, agressions verbales dans la rue, messages haineux sur les réseaux sociaux: des membres de la communauté musulmane de Montréal affirment vivre dans la peur depuis les attentats de Paris. «Depuis ce qui est arrivé à Paris, je ressens une peur chez les musulmans. Je crains que tout cela finisse mal», lance Haroun Bouazzi, de l'Association des musulmans et des Arabes pour la laïcité au Québec (AMAL).«J'ai l'impression que ce n'est qu'une question de temps avant qu'un membre de notre communauté se fasse casser les deux jambes. Il y a trop de haine sur les réseaux sociaux», poursuit-il. Mercredi matin, le téléphone ne dérougissait plus à l'AMAL, plusieurs citoyens s'inquiétant de menaces de mort proférées sur les réseaux sociaux par un homme déguisé en joker, qui a finalement été arrêté par les policiers. «Beaucoup de gens m'ont écrit en panique. C'est étonnant de voir à quel point ils vivent dans la peur», affirme M. Bouazzi. Haroun Bouazzi dit recevoir régulièrement des menaces sur le site de son organisation. Mais il affirme ressentir une «pression supplémentaire» depuis quelques jours. Il n'est pas le seul. Joint mercredi par *Le Journal*, Mehmet Deger, président de la mosquée Dorval, a rapporté avoir reçu un coup de fil menaçant mardi après-midi (…) Cependant, le Centre islamique de l'est de Montréal de l'imam controversé Adil Charkaoui, de même qu'une mosquée du quartier Hochelaga, ont été vandalisés au cours des derniers jours. QMI Agency (Journal de Quebec, Journal de Montréal)

*** 'Loves Me Not' Poem Captures Heartbreaking Reality Of Islamophobia In Canada**
Taunts in public. Comments online. And recently, physical abuse. In the past months, Canada has witnessed far too many attacks against Muslims, particularly women. Earlier this week, a Muslim woman was physically assaulted in front of her children's school and called a "terrorist." In October, a woman wearing a niqab was attacked at a Toronto mall. It's difficult for most of us to imagine the emotional trauma victims of such discrimination endure. But one poem, written by a group of Muslim women in Toronto, captures the heartbreaking reality. "Loves Me Not", a video poem created earlier this year during

a filmmaking workshop hosted by TIFF Special Delivery and advocacy group Outburst, tells the story of a young Muslim girl who wears the hijab. The poem begins with the girl, her hijab constructed with colourful petals. She holds a flower in her hand, but as she suffers from Islamophobia her flower begins to die. "Everywhere she looked, people would stare," the poem states. "They asked, 'Is that something your dad forced you to wear'?" According to Outburst's Facebook page, the poem was inspired by Islamophobia endured by the writers as they attended school in Toronto. The video continues to show the lasting impact of discrimination. "One day she broke down, the comments made her drown." Huffington Post

*** Web et jeux vidéo au service du terrorisme**

Le 10 novembre dernier, soit trois jours avant les attentats de Paris, le ministre de l'Intérieur belge Jan Jambon a laissé entendre que des terroristes utilisaient une console PS4 pour communiquer entre eux, une information qui a refait surface au cours des derniers jours. La réalité: aucune console PS4 n'a été retrouvée lors des nombreuses perquisitions effectuées en France et en Belgique. Ce qui ne veut pas dire que les jeux vidéo ne jouent pas un rôle dans les milieux terroristes. En 2013, grâce à des documents rendus publics par Edward Snowden, le Guardian et le New York Times ont révélé que la NSA et la CIA avaient déjà mené des opérations d'espionnage sur des consoles Xbox. Quelle utilisation les terroristes peuvent-ils faire des jeux vidéo? «Dans les jeux multijoueurs (pensons au jeu Call of Duty, par exemple), on retrouve des plateformes de "chat" afin que les joueurs puissent échanger entre eux, explique Hugo Loiseau, professeur à l'École de politique appliquée de l'Université de Sherbrooke. La Presse, A14

*** Hindu temple gratified by public support**

Young Muslims from the Toronto area would like to help pay for the damage caused at the local Hindu temple that was vandalized this week, but a temple board member said insurance covered the costs and the windows have been repaired. So the group known as Dawahnet, which means "spreading knowledge" in Arabic, will donate $2,299 that was collected in 24 hours on a gofundme website to the temple. Temple board member Vijay Solanki said the temple was overwhelmed with public support with many offering to help with the damage costs. "We gratuitously thanked them for the offer, but it is not appropriate to raise thousands of dollars for something that didn't cost us," he said. The gofundme page was set to raise $10,000 for the Kitchener temple by Dec. 1, but organizer Arshia Lakhani of Mississauga said they closed the site after speaking to the temple (...) Swami Chaitanya Jyoti and two other women were in the building and were frightened by the noise at the back of the building shortly after 11 p.m. No one was hurt in the incident. Hours before the vandals struck, Jyoti was at the Kitchener vigil honouring those who lost their lives in the Paris terrorist attacks. Record, B2

*** Extend vigilance to everyday threats**

An opinion piece states "In the wake of the attacks in Paris, there has been no shortage of security experts in the media talking about how to best keep safe. RCMP Assistant Commissioner Roger Brown, for example, articulated what everyone intuitively knows - there's no real science to spotting a terrorist plot. The best you can hope for is your gut tells you something is wrong. "When you do find yourself in a position where you see or do become aware of something that's not right, the next logical step is to report it to the proper authorities," Mr. Brown said. To his credit, the assistant commissioner hasn't fanned the flames or paranoia. He's done a good job of explaining the scope of the threat in Canada, not exaggerating it. David Charters of the Gregg Centre for the Study of War and Society at the University of New Brunswick has a similar message, calling an attack "a possibility but a relatively remote possibility." "The message 'If you see something, say something' is not a bad idea," Mr. Charters says. This is sound advice. It's true New Brunswick hasn't been the target of a terrorist attack, which isn't to say it's been a terror-free province. Justin Bourque's rampage in Moncton remains fresh in New Brunswickers' memories. And who can forget the seven months Allan Legere was on the loose in 1989. While the threat of a terrorist attack in Fredericton is remote, it's no excuse to be complacent. It's the reason schools practice lockdown drills. It's the reason passing through security at airports has become a much more intimate experience thanks to body scans and random searches." Daily Gleaner, A8

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Douanes à Bagotville: Lebel offre sa collaboration
Au cours d'un entretien avec le journaliste du Quotidien, le député conservateur de Lac-Saint-Jean affirme que le gouvernement Harper était prêt à annoncer, il y a quelques mois, un projet-pilote à travers le Canada, mais que la défaite électorale du 19 octobre avait modifié les plans. Depuis plusieurs années, les compagnies aériennes et les passagers qui se rendent en vacances dans le Sud réclament un service de douanes à l'aéroport de Bagotville. Il faut savoir que le service existe pour les voyages d'affaires de 30 passagers et moins seulement. Présentement, lorsque l'avion quitte le Mexique, Cuba, le Panama ou la République dominicaine, le pilote doit obligatoirement faire un arrêt à Québec. Les touristes doivent débarquer et passer par les douanes. Chaque fois, l'arrêt dure au minimum une heure et oblige les compagnies d'aviation à défrayer des sommes d'argent pour avoir le droit de se poser, en plus des dépenses de carburant que cela implique. (…)Au cours des dernières années, Denis Lebel et des fonctionnaires du gouvernement ont tenté de trouver une solution qui ne serait pas coûteuse pour ce projet. Et l'ancien ministre y était parvenu. Chaque atterrissage à Québec entraîne des coûts assez importants pour les compagnies aériennes. Ils seraient de l'ordre d'environ 10 000$, que les voyageurs paient sur leur billet. «Ce que je propose, c'est que l'on prenne cette somme et qu'on l'investisse dans les équipes de douaniers. Ça ne coûterait rien de plus au gouvernement, mais ça éviterait une escale.» «L'équipe volante des douaniers pourrait être formée des douaniers actuels de l'aéroport et on pourrait ajouter des militaires et des policiers à la retraite pour donner un coup de main. Au départ, ce serait un projet temporaire, soit pour la durée des vols offerts vers les destinations du Sud», analyse Denis Lebel. La Presse

L'ABC des achats de Noël en ligne
plusieurs consommateurs n'aiment pas faire la tournée des centres commerciaux pour faire leurs emplettes des fêtes. de nos jours, il est possible d'éviter cette épreuve annuelle en commandant ses cadeaux en ligne. Selon un récent sondage du Conseil québécois du commerce de détail (CQCD), plus du quart des Québécois (26 %) prévoit acheter un ou des cadeaux sur inter-net cette année. Année après année, ce geste devient toujours plus populaire. En 2010, seulement 11 % des Québécois prévoyaient acheter en ligne pour la période des Fêtes. (…)En théorie, en achetant sur un site américain, vous épargnerez la taxe de vente, car vous êtes résident d'un autre pays. Cela dit, bon nombre d'États américains n'ont tout simplement pas de taxe de vente. L'économie atteint près de 15 %, mais elle prive le Québec de revenus. Par contre, à la frontière, votre paquet pourrait être vérifié par l'Agence des services frontaliers du Canada, qui procède de façon aléatoire. Le cas échéant, on vous facturera des frais de dédouanement et des taxes canadiennes. Ces frais augmenteront le coût de votre achat. Journal de Québec, 42; * Journal de Montréal, 36

U.S. border airports seeing drop in Canadian travelers
The shuffle off to Buffalo to catch a cheap flight on a U.S. airline is losing its shine, thanks to a lower loonie. "We have seen an impact, but it's difficult to quantify the exact number," said Pascal Cohen, senior manager of marketing at the Buffalo Niagara International Airport. That's because no data is collected on citizenship, when passengers arrive to catch their flight. However, airport officials do conduct licence plate surveys at the parking lot at the Buffalo airport. Previously, when the Canadian dollar was at par with the U.S. dollar, as many as 40 per cent of vehicles were Ontario plates. These days, the airport estimates it is about 15 to 20 per cent fewer Ontario plates. Cohen says overall passenger volume at the Buffalo airport is up 1.9 per cent, year over year, which could be attributed to an improving U.S. economy. It's unclear whether Canadian airports will enjoy a bump in traffic as travellers choose to fly from home airports. Pearson airport says passenger traffic on transborder routes are up this year, but can't attribute that to a shift in travel patterns. Toronto Star, S11

*** U.S. to have tariffs against Cape Breton paper**
A series of costly duties will be levied against Canadian mills, including one in Point Tupper, that produce glossy paper following a vote Wednesday affirming the trade action by the U.S. International Trade Commission. The trade body says the vote was part of the final phase of a countervailing duty investigation into Canadian imports of supercalendered paper, which is mainly used for magazines, catalogues, corporate brochures and advertising inserts... Canada's international trade minister Chrystia

Freeland, issued a statement saying an appeal under the North American Free Trade Agreement will determine if the countervailing duties are being applied in accordance with the laws of the United States. Canadian Press (Cape Breton Post. A1, A4); Chronicle Herald, A1

*** SNAPSHOT: Children in immigration detention**
The location of CBSA's three immigration detention centres. CROSSINGS. Chronicling the global refugee and migrant experience 65 Number of days spent in a Canada Border Services Agency immigration holding centre (as of Nov. 13) by one of the two children currently waiting to hear the results of a refugee claim. The other has been there for 18 days. An agency spokesperson said that both children's parents prefer they stay in the centre with their families, rather than be relocated by child-protection services. "If you are a Canadian citizen and you're born in immigration detention or you're a Canadian citizen but your parents are undocumented, get arrested and placed in detention, the parents have a choice to give their children over to Children's Aid Society custody and never see them again or bring them in with them in prison. Adults make the difficult decision to bring their kids into prison ... What does a two-year-old do? Globe and Mail, L4

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Blackmailers target clients of Ashley Madison - Complaints to FTC claim online extortionists active in wake of site's hacking**
Victims of the Ashley Madison hack say they are being blackmailed months after millions of customers had their information leaked online. Complaints filed with the U.S. Federal Trade Commission detail how customers continue to feel the aftermath of the July attack on the Toronto-based adultery website. "A recent hack from the company exposed numerous amounts of private information from me. Now I am being harassed by others who are maliciously using the contents of that information," wrote one person. The hackers, who are still at large, leaked the information online, causing shock waves across the world as millions of alleged Ashley Madison customers had their dirty laundry aired. Toronto Police are still investigating the cyber attack, which they previously linked to online hate crimes, online scams and two unconfirmed reports of suicide. Toronto Star, S12

*** More offers too good to be true - Fraudsters finding new ways to victimize computer users**
An opinion piece states “Raise your hand if this has happened to you: A telephone call from Microsoft (or Windows) telling you your computer needs immediate attention. An email from your bank notifying you that your bank account has been compromised and you need to reset your password. Or, you are visiting a website, to get a recipe or read some news, and you get a screen message that your computer is running slowly so ‘click here’ to repair the problem. Keep your hand raised if you are a senior. Well then, join the club. And it's a growing club because fraudsters can easily get your phone or email address and with mass calls and/or mailings are sure to grab more and more unsuspecting customers. Locating the scammers is almost impossible; many are out of country and most use disposable cellphones that are difficult to trace. Here's a taste of how it all goes down. An elderly friend, let's call him Blake (whom I had previously helped with computer issues) called me to say that Microsoft had phoned him and he had allowed the caller remote access to his computer. The "technician" immediately claimed to find mountains of viruses and offered to clean his computer - for a price. What credit card would he like to use? Blake, rightfully reluctant to give out his card number, hesitated. The caller pressed him further, this time to go to Western Union and send cash. When Blake once again refused, the caller informed him that unless he paid $179 his computer would become inoperable. Blake hung up. When he called me I congratulated him for not responding to an obvious scam, but here's the thing: the scammer had reset his user password and Blake could not get into his computer. Not an easy fix. Other similar examples include opening your computer only to find a detailed welcome screen seemingly from the FBI/RCMP warning you to pay a fine for illegal downloads or else your computer will remain in lockdown. This kind of malware is more easily removed, but how many people - especially seniors - are intimidated and fall for these and similar schemes?” Hamilton Spectator, A15

LAW ENFORCEMENT / APPLICATION DE LA LOI

A night on the town

At 9:50 p.m. Nov. 4, two police trucks responded to a call about a woman threatening to commit suicide. The call came from a family member and was relayed to the detachment over the phone. "The whole town doesn't need to hear that over the scanner," said Const. Yannick Gagnon as he followed a vehicle to where the woman lives. In the end, police decided the woman wasn't an imminent threat to herself and took her to a relative's home. "Just to be on the safe side, we're not going to let her be alone," said Gagnon. "If she didn't have family to go to, we would bring her to the hospital to get her cleared, and if she was imminently suicidal she would be taken to the hospital right away. Better safe than sorry." He said this way if there are more concerns over the course of the night, at least the officers know the situation. Gagnon arrived at the RCMP detachment shortly before 7 p.m. on Nov. 4 to get ready for night shift. It was "superconstable" night, something that happens once every two weeks or so when shifts overlap and nearly all officers work on a given day. It means they can get caught up on paperwork and share important events with the next crew to come on. Gagnon's regular partner, Const. Mackenzie McGuffin, spent the shift preparing for a case going to court the next morning. "It's what ties everything together," he said. "You can respond to a call, but if you don't follow up with the paperwork, there's no chance those charges will go through." Gagnon said he was a few weeks into Depot, where all RCMP members go to be trained, before he realized the job was 90 per cent pencil-pushing and 10 per cent "fun stuff." "I wanted to quit right there," he joked. Inuvik Drum

Man charged over concealed cleaver

A Toronto man who allegedly tried to carry a meat cleaver onto Parliament Hill is to undergo a psychiatric assessment. A lawyer for Yasin Ali asked for the assessment in court Wednesday after the 56-year-old appeared by video from the courthouse cellblock on a charge of carrying a concealed weapon. He will remain in jail until his next appearance on Friday, when he is to appear in court in person. The man had a ticket to visit the Peace Tower, and was in line to go through the visitors' entrance at about 11:30 a.m. on Tuesday when a House of Commons security guard asked him to open his coat. The guard found the man was concealing a large cleaver with an approximately 15-cm-long blade. The man never made it as far as the metal detectors. RCMP Commissioner Bob Paulson told reporters that Ali is known to authorities, but "not in the sort of counter-terrorism context." In fact, Paulson does not believe that the man's actions were politically motivated or an act of terror. Postmedia Network (Windsor Star, N5, Toronto Sun, Ottawa Citizen); ; *La Presse; * Canadian Press, (Times Colonist, A8)

*** La GRC pourrait avoir agi illégalement, dit la juge**

Une juge de la Cour suprême de la Colombie-Britannique a affirmé que la preuve tendait à montrer que la Gendarmerie royale du Canada (GRC) avait agi illégalement durant une opération d'infiltration antiterrorisme de haut profil, et a ordonné à la police de remettre des documents juridiques confidentiels. La juge Catherine Bruce n'a pas encore déterminé si la GRC avait piégé John Nuttall et Amanda Korody pour qu'ils organisent un complot visant à faire exploser le parlement de la Colombie-Britannique en 2013, mais elle a indiqué que les agents pourraient être coupables d'avoir facilité en connaissance de cause un acte terroriste durant leur opération d'infiltration. «Il existe un lien suffisamment étroit entre les actes illégaux commis par la GRC et les faits reprochés aux accusés pour soutenir une allégation d'abus de procédures», a-t-elle écrit. Mme Bruce a ordonné à la police de dévoiler des avis juridiques confidentiels obtenus relativement à l'opération secrète pendant laquelle des agents se faisaient passer pour des combattants djihadistes. «Ces documents fournissent un aperçu fondamental de l'état d'esprit de tous les agents mêlés à l'intervention», a-t-elle mentionné. La confidentialité de la correspondance avec un avocat est habituellement protégée, mais la magistrate a indiqué que les agents de la GRC avaient renoncé à ce droit en dévoilant délibérément une portion de l'information en cour. La juge estime qu'il est pertinent de savoir si les policiers ont suivi les conseils de l'avocat, car cela pourrait montrer une mauvaise foi de leur part. John Nuttall et Amanda Korody ont été reconnus coupables plus tôt cette année sous des accusations de terrorisme pour avoir planifié de perpétrer un attentat sur le site de l'Assemblée législative de la Colombie-Britannique lors des célébrations de la Fête du Canada de 2013, mais leurs avocats ont argué que la GRC les avait piégés et que le complot n'aurait jamais été organisé sans l'aide de la police. La Presse Canadienne (Le Nouvelliste, 14, La Voix de l'Est); CBC News;

Postmedia News (Province, A8, Times Colonist); Postmedia Network (Vancouver Sun, A2, Calgary Sun, Winnipeg Sun, Province, Globe and Mail, S3)

*** Les agences se font rassurantes**
Les grands patrons des agences canadiennes de sécurité et du renseignement ont cherché à se faire rassurants, hier : ils ont bel et bien la capacité de faire les vérifications qui s'imposent afin de protéger les Canadiens contre les menaces potentielles posées par l'accueil rapide de 25 000 réfugiés d'ici la fin de l'année. « Je veux que les Canadiens sachent qu'en tant que directeur du SCRS, je suis sûr que les mesures en vigueur sont robustes et que j'ai pleinement confiance qu'elles seront appropriées », a déclaré Michel Coulombe, directeur du Service canadien du renseignement de sécurité (SCRS). De plus en plus de gens au Canada expriment leur inquiétude devant cet accueil jugé trop rapide et un nombre trop élevé de réfugiés d'ici six semaines. Les chefs du SCRS, de la Gendarmerie royale du Canada (GRC), de l'Agence des services frontaliers du Canada (ASFC) et le ministre fédéral de la Sécurité publique ont livré une rare conférence de presse conjointe pour répondre à ces préoccupations. Ils ont fourni quelques détails sur la situation sécuritaire au pays dans la foulée des attentats de Paris et sur leurs démarches pour assurer la sécurité tout en respectant la promesse électorale du Parti libéral. La Presse Canadienne (Voix de l'Est, La Presse,); La Presse

*** Takes two to tango in Duffy trial**
The Ol' Duff will be strutting today, his mind firmly convinced that, besides his courtroomdrama playing a key role in bringing down the spiteful Harper government, he will soon be walking out of court totally vindicated. This has been Duffy's firm belief from the outset, and he has sent chastising emails to many in the media who presupposed his guilt. (…)In fact, the RCMP exonerated Wright of any wrongdoing and, after he testified about cutting the cheque to Duffy, he skedaddled back to England and his job as managing director in the London office of Onex Corp. There is no jury here. It is trial by judge alone, so it comes down to Ontario Court Judge Charles Vaillancourt to decide if there was a bribe and, if so, then solve the riddle of who bribed who. But armchair jurors are already taking bets on acquittal. The most entertaining portion of the trial, of course, has been defence attorney Donald Bayne's tarring of the Prime Minister's Office, even though who-knew-what and/or who did or did not tell the prime minister about Wright's cheque has nothing to do with Duffy's guilt or innocence. Postmedia Network (Calgary Sun, A15)

*** Winnipegger warns of immigration phone scam - Callers demand payment**
More than 45 years after Winnipeg resident Monina Relano moved to Canada from the Philippines, she got a phone call Tuesday saying there was a problem with her immigration paperwork."I was scared," said Relano. Though she's been a Canadian citizen since 1975, she was taken aback by the authoritative voice on the phone. The man told her she didn't fill out a required immigration form and now had to pay an out-of-court settlement of $2,490 or the RCMP would be at her door.Relano figured out it was an immigration phone scam but worries more recent newcomers without permanent status in Canada might be conned. She wants to warn them before they get the call and end up swindled. Winnipeg Free Press, B6

*** Diverse workers sought by RCMP**
The RCMP is seeking some good men and women to diversify their ranks. With a visible minority presence of 9.7%, the force is seeking to increase that to 20% to better represent the country it serves, say Mounties. The force is holding a Calgary career presentation Nov. 25 at the Duncan Building, 7575 8 St. N.E. at 6 p.m. On offer are 150 different types of policing opportunities. Those applying for a position with the RCMP must be a Canadian citizen, 19 years of age and be fluent in either or both English and French. They must also possess a valid driver's licence and have a high school diploma or an equivalent, be able to meet fitness requirements and be willing to re-locate anywhere in Canada. Postmedia Network (Calgary Sun, A10)

*** New Kids on the cellblock**
A Red Deer crime syndicate has taken a big hit. Police have arrested and charged three alleged members of Bobby and the Kids, a group that deals mostly in the drug trade. One of them is believed to be "Bobby," the leader of the group. The organization has dealings throughout Central Alberta including Sylvan Lake, Blackfalds and Innisfail and has been operating for "some time," say police. The arrests are

believed to be the first made involving the organization. "We have definitely disrupted this group and eliminated the harm they are doing in the community," said Red Deer RCMP Sgt. Eric McKenzie. Police did not give any indication of the size of the group. Last Friday, the Priority Crimes Task Force seized 55 ounces of cocaine, nine ounces of methamphetamine, marijuana, a stolen pistol, drug paraphernalia and $30,600 in cash after executing search warrants at Timothy Drive and Leonard Crescent in Red Deer and Harvest Close in Penhold. Three men between the ages of 22 and 27 were arrested without incident. Postmedia Network (Red Deer Advocate, A1, A2)

* **Quebec police conduct major raids linked to drugs, organized crime**
Quebec provincial police say they are conducting major raids this morning linked to drug trafficking and organized crime in the Montreal area. Sûreté du Québec spokesperson Audrey-Anne Bilodeau says roughly 200 police officers are taking part in the operation. The raids target "different strains of organized crime in link with the control of the territory, the supply and the distribution of drugs in Montreal," Bilodeau said. In all, Bilodeau says they expect to arrest about 40 people this morning. Bilodeau would not give further details on the suspects or what kind of drugs may be involved. She says members of the SQ, Montreal police and the RCMP are collaborating. A news conference is planned for later this morning to give more details on the operation. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Young Shafia seeks appeal
Hamed Shafia, the Montreal man convicted, along with his father and mother, of murdering four family members in what the trial judge called a "heinous" and "despicable" mass honour killing, is poised to present a new claim to Ontario's top court regarding the appeal of his conviction. The youngest Shafia killer maintains that he was not 18 years old at the time of the murders on June 30, 2009, and he has documents newly obtained from Afghanistan, his birthplace, that purport to prove it. Shafia was tried and sentenced as an adult, based on documents that indicated he was born in Kabul on Dec. 30, 1990. Those records established that he was 18-and-ahalf years old at the time of the killings, and therefore subject to adult criminal law. After a 45-day trial, he was convicted of four counts of first-degree murder and sentenced to the mandatory term of 25 years in prison before parole eligibility. If convicted of murder in youth court and sentenced as a youth, he would be eligible for parole much sooner, perhaps in as few as five years, calculated from the date of his arrest in July, 2009, according to Nicholas Bala, a Queen's University law professor and expert on youth criminal law. The legal scholar said it might be the first case in Canada in which a killer sought to prove he was underage after his adult conviction. Postmedia Network (Kingston Whig-Standard, A1, Montreal Gazette, Toronto Sun, Calgary Sun, National Post, Ottawa Citizen)

McDonald's killer loses appeal
The man believed to be the mastermind behind the most notorious killings in Cape Breton history has lost his appeal of the decision to deny him day parole. Derek Anthony Wood was sentenced to life in prison with no eligibility for parole for 25 years after being convicted of a number of charges, including two counts of first-degree murder in the 1992 Sydney River McDonald's killings when he, Darren Muise and Freeman MacNeil robbed the restaurant and killed three workers. A fourth person was left permanently disabled. Wood had filed an appeal with the Parole Board of Canada after it denied his day parole application earlier this year. He had been deemed a medium-to-high risk to reoffend in a violent manner, according to a psychological assessment. Cape Breton Post, A1

'She's never coming back'
Eighteen years later, the daughters of murdered prison guard Diane Lavigne say they're still struggling to cope. Testifying Wednesday at a hearing where former Hells Angels underling Stéphane Gagné is seeking an earlier parole eligibility on the life sentence he is serving for taking part in the murders of two prison guards in 1997, 40-year-old Isabelle Daoust said she still remembers how sunny it was on the Friday morning her uncle knocked on her apartment door and told her "my sympathies, Isabelle. Your mother's been assassinated." Gagné killed Lavigne in June 1997, shooting her from the back of a motorcycle as she drove home from her job at the Montreal Detention Centre. He later became a

collaborating witness against biker boss Maurice (Mom) Boucher and helped convict him. Boucher is now serving a life sentence for the murders of Lavigne and Pierre Rondeau and the attempted murder of Robert Corriveau, all of them guards at provincial detention centres targeted in an effort to intimidate the Quebec justice system. Daoust called the sequence of events in 1997 "surreal. Things like that didn't happen in Quebec. It's like a film that I was watching from above ... too big and unexpected to ever see coming." Montreal Gazette, A3, Le Devoir, Journal de Québec (Journal de Montréal); * La Presse

* **James Leroy Leopold, convicted of killing fiancée, has parole revoked after 5 months**
A Nova Scotia man who killed his fiancée has had his day parole revoked after just five months. James Leroy Leopold was convicted of manslaughter and sentenced to six years in prison after the death of Laura Lee Robertson in 2012. During his trial, the court heard Leopold told police he and Robertson got into a fight and that she died after he hit her in the throat. Following a hearing in May of 2015, Leopold was granted six months of day parole by the Parole Board of Canada. In their decision, the board noted that Leopold is at a high risk of violence towards a partner. Global News (2015-11-18)

* **Parole extended for killer ex-Mountie**
A former Mountie convicted of first-degree murder who has been running an antiques store in Prince George must spend at least a further six months on day parole, according to a recent Parole Board of Canada decision. Patrick Michael Kelly, 65, was convicted in 1983 for throwing his wife off the 17th-floor balcony of their Toronto apartment. Kelly was originally granted day parole in 2003. Since then, his parole has been revoked several times for failing to disclose financial dealings or relationships with women. The former undercover officer was granted full parole in 2010 and opened his store in Prince George. But the board reversed his release in August 2012 after he failed to report two relationships with women. Prince George Citizen (2015-11-18)

Traque contre un couple de voleurs
Un enquêteur qui a traqué pendant des mois un couple de voleurs à la Bonnie et Clyde, qui ont dérobé pour plus de 1 M$ en cambriolant des maisons cossues partout au Québec, sera récompensé aujourd'hui pour son travail acharné. «Je suis tellement content d'avoir résolu ces dossiers. Sinon, ils auraient continué à commettre d'autres crimes. Certaines victimes ont été démolies en se faisant voler des objets de valeur importants à leurs yeux», a dit le sergent-détective de la Sûreté du Québec, Gordon Hunter. (...)Le sergent Hunter sera récompensé aujourd'hui dans le cadre du Gala des Prix policiers du Québec pour son implication dans cette enquête. (...)Jimmy Simard-Patry et Elyanne Miller ont respectivement écopé de cinq ans et demi et de deux ans de prison en juin. Un complice du couple n'a pas encore subi son procès. Journal de Montréal (Journal de Québec)

Province's plan a 'beacon' for justice: minister - Unveils details of restorative strategy
A five-year plan to make restorative justice a mainstream method of dealing with crime in Manitoba will include a community court in the North End, an expansion of current mental-health and drug-court diversion programs and a focus on victims, the provincial government announced Wednesday. Restorative justice is "local, swift, common-sense, tough justice," Justice Minister Gord Mackintosh told a room of restorative-justice advocates at the legislature building Wednesday, proclaiming legislation he hopes will establish Manitoba as a "beacon in North America for restorative justice." The term restorative justice refers to an individualized approach for offenders (who are often youth or first-time offenders) to take responsibility for their actions, usually by reconciling with victims, performing community service and working toward their rehabilitation. It's used mainly to handle less serious crimes and non-indictable offences, but the justice minister said the province is looking at "tacking on" restorative-justice techniques alongside criminal-court sentencing. The province plans to fulfil the new strategy, announced Wednesday to coincide with the implementation of the Manitoba Restorative Justice Act, by increasing its current $1.8-million annual spending on restorative justice, starting with an additional $320,000 next year. Winnipeg Free Press, B5, Winnipeg Sun; * Radio-Canada

* **Credit-card fraud extends sentence**
Credit-card fraud has added to the length of a Fredericton man's prison sentence. Ashley James Charlton, 35, was brought to provincial court in custody recently on a charge of using a stolen credit card between Aug. 5 to 6. The former Canada Street resident pleaded guilty to the offence during an

appearance last month. Judge Mary Jane Richards sentenced Charlton to six months' incarceration and ordered that he pay a $100 victim-fine surcharge. He was also instructed by the court to pay restitution in the order of $3,279. Charlton told court during an earlier appearance that he's serving time in the Springhill Institution in Nova Scotia for breaking into two food vendor kiosks at the Northside Market and stealing hundreds of dollars worth of meat on Aug. 19. Daily Gleaner, A4

*** World's indigenous leaders look to adopt prison practices at Waikeria**
Indigenous leaders from around the world hope to adopt practices from a Waikato prison unit that rehabilitated violent offenders, drug abusers and sex offenders. Daniel Levi Martin is a tribal leader of Tla-o-qui-aht First Nations people, who live on reserves along the Pacific Rim National Park, Canada. "I hope that I can learn the different ways of doing things here [at the prison], techniques I can take back home to my people," he said. Martin was in Hamilton for the week-long indigenous people's conference, Healing Our Spirit Worldwide - The Seventh Gathering, hosted by Te Rau Matatini. "I'm an elder and an advisor to treatment centres. I hope to learn something here." Waikeria Prison's Karaka Unit is an 80-bed therapeutic community for medium and high risk offenders. Since 2010, 245 prisoners have completed treatment programmes at Waikeria Prison's Karaka Unit. Since 2010, 245 prisoners have completed the programme, with 55 per cent of those identifying as Maori. There are three programmes within the unit; the Dependency Treatment Unit (DTU) for those with substance abuse, the Special Treatment Unit Rehabilitation Programme (STURP) for high-risk offenders, and the Adult Sex Offender Treatment Programme. Stuff.co.nz

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Police must communicate to track missing women
Effective communication between police agencies is essential when it comes to investigating vulnerable women who have disappeared, says the man who oversaw British Columbia's Missing Women Commission of Inquiry. Wally Oppal, a former B.C. Court of Appeal justice and provincial attorney general, said there was little communications between the RCMP and the Vancouver police in the 1990s when multiple women went missing in that province. "When vulnerable women go missing police have to get involved and that is what they didn't do in the 90s," Oppal said in an interview. "The result is you have well over 100 women who were murdered." Exchanging information in such cases has to take place, Oppal said. What happened in B.C. was that women were being picked up in the eastside of downtown Vancouver but were being murdered in Port Coquitlam, about 35-40 minutes away, he said. "There were very little communication between the RCMP and the Vancouver police," Oppal said. "We were very critical of the policing that took place and that there was no real liaison between the sex trade workers and the police." Oppal will be at St. Thomas University Thursday night presenting a public lecture on the inquiry. Appointed commissioner in 2010, Oppal held close to 100 days of public hearings and forums in Aboriginal communities in northern B.C. in which the many victims and survivors of the Robert Pickton tragedies testified. The inquiry was called to examine why Vancouver police and the RCMP failed to catch Pickton before he was arrested in February 2002. Daily Gleaner, A3 (Times & Transcript)

*** Does Canada still need a Status of Women minister?**
We've come a long way in Canada on gender equality - far enough for Prime Minister Justin Trudeau to mandate gender parity in his first cabinet. So do we still need a Status of Women ministry? "Yes, we certainly do," said noted feminist and journalist Michele Landsberg, The new mandate letter for Status of Women Minister Patty Hajdu tasks her with trying to eliminate economic and political inequalities that affect women, tackling violence against women and moving forward with a planned inquiry into murdered and missing aboriginal women. Under the Harper government, Landsberg said, women's rights were set back by budget cuts for research and advocacy in the ministry. This loss of funding, she said, meant government couldn't get a complete picture of what was happening in the lives of women. iPolitics, Toronto Star

*** Saskatoon men asked to combat violence against women**
Members of the University of Saskatchewan Students' Union (USSU) have called for an end to violence against indigenous women and children, hoping men will lead the movement for change. "Traditionally as men, our role was to stand as protectors and also to support our women," said Regan Ratt-Misponas, indigenous student representative with the USSU. "Our women were very much regarded as the leaders of First Nations communities and First Nations reserves." On Wednesday, students were introduced to the "Moose Hide Campaign," a grassroots, non-profit that encourages aboriginal and non-aboriginal men to wear pins made of the material. Global News (2015-11-18)

*** Delete Day aims to combat social media cyberbullying**
Countless people can see what you're doing, and a lot of them are mean. That was the message Windsor police and Catholic Central High School tried to drive home Wednesday during Delete Day, an event they hosted to combat cyberbullying. Students spent time with their vice-principal and a police officer to learn how to delete bullying posts from their social media profiles, along with anything they might regret posting themselves. "There are adults and other people whose sole purpose is to troll the Internet and find young people using social media to see if they can acquire their information," said vice-principal Laura Beltran. "When that happens, it can ruin lives and it's very difficult to put lives back together once information is out there. Especially for young people, their reputation, their self-esteem, their self-concept is still growing and maturing and it can be devastating for them at a very early age." Dozens of students showed up for Delete Day, one of a number of events being held as part of Bullying Awareness Week. Grade 12 student Manal Muzamil said it was a good chance to "refresh" social media accounts, delete bad things people have posted and block those responsible for the negativity. Windsor Star, A3

*** Cyberbulling starts young**
Cyberbullying can affect children far younger than widely believed, experts warn. While it starts to become prevalent in students around the Grade 7 level, children can gain access to this world much sooner, said Brad Burns, principal of Highlands School in Edmonton. "I know of students that are in kindergarten who are coming to school with cellphones, because they are a very useful resource for safety and communication at homes," said Burns. "As technology is more prevalent in our lives and more integrated, that age of being in that world keeps moving down to younger and younger children." On Wednesday, as part of Bullying Awareness Week, Burns was one of five panellists speaking at an Alberta government-sponsored webcast on cyberbullying. He said it's up to the parents to inform and discuss with their children about the importance in becoming a "responsible digital citizen." Calgary Sun, A21 (Edmonton Sun)

*** There's value in carding**
An opinion piece states, "In September 2011, a 15-year-old girl was sexually assaulted in a Brampton park. Officers attached to Peel Regional Police's special victims unit had a description, but the perpetrator was long gone. Detectives checked to see whether there had been any PRP17s (street check reports) filed from anywhere nearby. Bingo. Up came a street check on a 37-year-old man - including name, date of birth and description - who was engaged by police at the park months earlier. They had a suspect and a reason for a search warrant which - when executed - led to the arrest of the man for possessing child pornography as well as the sexual assault on the girl. There's one example of the benefits of police community engagement that opponents feel is racial profiling. Under new rules being implemented next year by the provincial government, police will have to tell people encountered - such as the man engaged in the park - that there is no need for them to talk to officers and that they're free to go. It's absurd." Toronto Sun, A10

*** Fassbender saps amalgamation impetus**
It never was about forcing amalgamation on Greater Victoria, and Peter Fassbender knows it. B.C.'s community charter already bars the provincial government from imposing amalgamation on anyone. No, all that people are asking for is a study into whether amalgamation makes sense. (...)Of course, while Victoria and Esquimalt might see this disparity as an excellent reason to share the cost of policing more equitably, the other municipalities see it as a totally awesome reason to leave things as they are. Why would Langford, whose residents pay just $141 apiece for the RCMP, voluntarily eat a cost hike?

Both Victoria Mayor Lisa Helps and Esquimalt Mayor Barb Desjardins recognize this reality. Times Colonist, A3

*** 'Almost one an hour'**
When she refused to give him money to buy beer, one Edmonton man pushed his girlfriend to the ground, pulled her hair and punched her in the face. (...)"This is only a sample of the files received by the Edmonton Police Service this past weekend," Staff Sgt. Sean Armstrong, in charge of the domestic offender crime section, told a downtown crowd Wednesday. "There were 88 cases responded to by EPS members, and sadly this was a quiet week. I can guarantee you there are many more domestic violence occurrences in our city that were not reported to us." These revelations shocked those gathered for the the Alberta Council of Women's Shelters' (ACWS) 11th annual Breakfast with the Guys at the Chateau Lacombe on Wednesday. In 2014, Edmonton police were involved in nearly 8,000 domestic violence complaints. (...)According to government statistics, Alberta has the fifth highest rate of intimate partner violence reported to police and the second highest rate of self-reported intimate partner violence in Canada. Edmonton Sun, A7

*** First Nation contemplates ban on criminals on reserve**
Elders on the Little Pine First Nation are exploring the idea of banishing criminals from the reserve. The idea of kicking known offenders such as drug dealers and abusers offthe reserve was preposed at a recent community meeting aimed at dealing with crime on the First Nation, located north of North Battleford. "The criminal justice system is not working. Look at the statistics," said Jacob Pete, a band member who helped facilitate the meeting. "We have to take ownership of the problems and come up with local solutions." The idea of banishing criminals from a particular community is not unheard of. Saskatchewan's largest First Nation, Lac La Ronge Indian Band, has been banishing drug dealers and others for decades. First Nations like Mistawasis near Prince Albert and Fishing Lake have also banished people for crimes. StarPhoenix, A3 (Leader-Post)

*** Un quartier général de la mafia visé par un attentat**
Un incendie criminel allumé dans un bar de la rue Jean-Talon la nuit dernière pourrait constituer un nouveau chapitre d'une tension grandissante au sein de la mafia montréalaise. *La Presse* a en effet appris de sources de divers milieux que l'établissement visé, le café Empire, serait l'un des quartiers généraux de la Table de direction de la mafia qui dirige les rênes du crime organisé montréalais, en alliance avec d'autres groupes criminels, depuis la mort naturelle du parrain Vito Rizzuto, il y a près de deux ans. Selon nos sources, Vito Rizzuto aurait été vu souvent à cet endroit après sa libération d'un pénitencier américain et son retour à Montréal, en octobre 2012. La Presse (2015-11-18)

*** Front line workers get info on battling sexual exploitation**
If you don't think human trafficking is a concern within Norfolk County, think again. “Because we're rural, we're a very big source destination for sexual exploitation,” explained Christina Bodine, chair of the Sexual Assault Centre of Brant. Bodine and her colleagues played host to a human trafficking seminar for social service employees and concerned residents at the Norfolk Golf and County Club Wednesday. One of the main messages was human trafficking – at one level or another – certainly does take place in Norfolk, Brantford and Six Nations. The trouble is, not many get the message because young women are often being shuttled to places like Niagara Falls or Windsor. “You have to lay charges in the place that the crime happens, so they'll be laid in places like Niagara Falls and Windsor, but they're gals that are from Brant, Haldimand, Norfolk, Six Nations,” Bodine explained. “That's why those stats aren't showing up, but we're a big source area.” That's why gatherings like the one on Wednesday are held. Speakers addressed the warning signs of human trafficking, what its definition is and who is most vulnerable. “It is complicated, so we're just trying to give an overview so people are aware,” Bodine noted. “What we do know is over 90 per cent is domestic, so it's happening within Canada, it's happening within our borders.” While the day-long event was open to all, Bodine and her team targeted a specific group to take part. Simcoe Reformer (2015-11-18)

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

City pulling together for refugees
It was an unprecedented Edmonton conclave. Ninety representatives from more than a dozen social agencies and government departments met Wednesday at the Ramada on Kingsway to plan a joint mission. Their goal? To settle some 1,500 Syrian refugees in Edmonton before year's end. "We're still not sure of the exact number or the exact timing. And that's causing some anxiety for us," says Stephen Carattini, CEO of Catholic Social Services. His agency has the federal contract to settle refugees in Edmonton. "Normally, we settle 400 to 500 refugees a year. Now, we're going to be settling three or four times that many. It's not unfamiliar, what we're being asked to do. But this is happening very, very quickly." The meeting included representatives from the federal departments of Canadian Heritage and Immigration, Refugees and Citizenship. Representatives of the provincial departments of Alberta Jobs, Skills, and Labour, Alberta Health and Alberta Education were there, too. So were Edmonton's school boards, along with Capital Region Housing and Edmonton and Area Child and Family Services. And there was an eclectic and ecumenical range of other agencies, including the Islamic Family and Social Services Agency, the Edmonton Mennonite Centre for Newcomers, Edmonton Immigrant Services Association, ASSIST Community Services, Centre d'accueil et d'etablissement, Changing Together and the Indo-Canadian Women's Association. Postmedia News (Edmonton Journal, A1/Front)

Queens sponsorship effort edges ahead
A group of residents in Queens County has just squeaked past the halfway point in their goal of raising $20,000 to sponsor a family of Syrian refugees. The Queens Refugee Care Team hopes to sponsor a family of six, and has already raised almost $11,000. Chronicle Herald, A8

Premier confident about refugees
Nova Scotia's premier doesn't want to pre-judge whether Ottawa should pull back from a plan to bring 25,000 Syrian refugees into Canada by the end of the year. Stephen McNeil said that Ottawa is responsible for handling any security concerns that arise from its screening process of refugees and his province remained ready to proceed with welcoming newcomers once it's determined how that will happen. McNeil said he expected many of those concerns to be addressed in a federal-provincial meeting next week, in light of the recent terror attacks in Paris and Beirut. "Security coming into the country is the responsibility of the federal government," said McNeil. "So if it (the plan) continues to move forward we are ready to participate as part of the federation." Canadian Press (Cape Breton Post, A9)

Notley says Calgary, Edmonton among five Alberta cities likely to take refugees
Premier Rachel Notley says Calgary and Edmonton are expected to take in the bulk of Syrian refugees coming to Alberta, with the remainder spread out over three other cities - Medicine Hat, Lethbridge, and Red Deer. "We're working to ensure that we're able to provide a seamless and effective settlement process," Notley told reporters Wednesday. "There are five cities where refugees would most likely land. The vast majority of them will be in Calgary and Edmonton. "Obviously the mayors need to be fully on side with it, and I believe that they are and have it well in hand." Notley was flanked by Edmonton Mayor Don Iveson and Calgary's Naheed Nenshi at the legislature following a meeting to discuss a range of issues, including the refugee resettlement. The federal government has said it wants to resettle 25,000 Syrian refugees across Canada by the end of the year. Notley has said she expects Alberta will take between 2,500 and 3,000 of those fleeing the war-torn region. Postmedia News (Calgary Herald)

Goodwill beats bureaucracy
They've been offered an entire convent in Pointe-Claire to house the refugees, a CEGEP in Rosemont with classrooms and showers to use at least over the holidays, rooms and fridges, winter coats and dishes. While politicians wrangle over whether it's possible to bring in 25,000 Syrian refugees over the next six weeks, grassroots organizations and ordinary Quebecers are making it possible. "Since last week our phones and email accounts have been overloaded with offers from Quebec residents wanting to help Syrian refugees with clothes, furniture, appliances," said Paul Clarke, the executive director of Action Réfugiés Montréal. "As public consciousness has ramped up that Syrian refugees are coming, the generosity has been astounding." And the terrorist attacks in Paris did not stop the flow, Clarke added. He has had to ask people to stop bringing in winter coats and boots to the organization's downtown locale

- there was just no room for more. But while every bit helps, especially if Quebec does receive 5,700 refugees over the next 43 days, such a massive endeavour requires some coordination, between all the groups involved, and every level of government. The community groups tasked with helping refugees resettle in Montreal - there are 18 in Montreal alone that offer services in Arabic - have set up a central list of people who want to volunteer their time, housing and miscellaneous goods, including all those winter coats and boots: infoparrainage@tcri.qc.ca And cities, including the 13 in Quebec that could receive some of the refugees, are also mobilizing. Postmedia News (Montreal Gazette, A1/Front)

Valcartier se prépare à l'arrivée de réfugiés
La base militaire de Valcartier est sur un pied d'alerte et se prépare à accueillir des centaines, voire des milliers de réfugiés syriens d'ici la fin de l'année. Le Canada avait déjà évoqué la possibilité que les bases militaires servent de terre d'accueil temporaire aux réfugiés, et l'hypothèse se confirme selon de nombreuses sources. Les 500 premiers réfugiés syriens débarqueraient dans la région de Québec à partir du 1er décembre - une date évoquée par plusieurs - et seraient logés dans diverses installations de la base militaire, notamment au Camp des Cadets. L'Armée vient de lancer un appel d'offres pour l'«hivernisation » d'une dizaine de baraquements. Les travaux, qui prévoient l'installation de chauffage, sont évalués à 1,5 M$ et seront réalisés «dans un très court délai, d'ici le 30 décembre», peut-on lire dans les documents sur le portail MERX. Journal de Québec, 3 (Journal de Montréal, 7); Le Soleil, 5/Front

Les villes veulent être mieux informées
Les maires des 13 villes québécoises qui accueilleront les réfugiés syriens attendus d'ici la fin de 2015 demandent à être mieux informés des plans d'Ottawa et de Québec, les élus ignorant encore combien d'entre eux chaque ville recevra. Une conférence téléphonique d'une quarantaine de minutes a réuni hier midi ces maires afin de faire le point sur le dossier. «Ce qui me frappe, c'est la volonté des villes à accueillir les réfugiés. Chacune a déjà pris des initiatives pour réunir les groupes sur son territoire. Mais il manque deux morceaux du casse-tête: Québec et Ottawa. Les villes sont déjà à pied d'oeuvre, mais elles n'ont pas toute l'information», a indiqué la mairesse de Longueuil, Caroline St-Hilaire. L'Union des municipalités du Québec a mis en place un comité auquel on espère voir Ottawa et Québec se joindre pour coordonner l'arrivée des réfugiés. «Il faut qu'on s'assoie, s'il le faut quotidiennement, pour éviter que chaque maire appelle à gauche et à droite pour avoir de l'information. On veut éviter qu'il y ait des ratés. On a connu de beaux succès d'accueil de réfugiés et il ne faudrait pas manquer le bateau», a ajouté Mme St-Hilaire. La Presse, A10

Rookie MP Tassi says government committed to accommodating refugees
Filomena Tassi is assuring residents that Canada remains committed to accommodating 25,000 Syrian refugees by Jan. 1. "At the same time, we're going to exercise the highest level of vetting and security," said the rookie MP, who represents the riding of Hamilton West-Ancaster-Dundas and will be sworn in as part of Prime Minister Justin Trudeau's government on Dec. 2. Opposition to the Liberal campaign promise has already grown in reaction to reports that at least one of a number of ISIL terrorists who participated in the Paris attacks in last weekend entered France with other Syrian refugees. But with a majority government, Trudeau and his team appear to be moving ahead on the promise. "We are staying on course," Tassi said. Tassi has been to Ottawa and completed her training for first-time members of Parliament. She is now focused on setting up shop in her widespread constituency, searching for an office from which to serve residents from Ancaster to Westdale and the west Mountain. Tassi said there was nothing to officially announce as far as any committees she will be part of, or other specific roles within the government. Hamilton Spectator, A5

Les initiatives citoyennes se multiplient
Le téléphone de la Table de concertation des organismes au service des personnes réfugiées ou immigrantes n'arrête pas de sonner depuis des jours. «Les gens offrent des logements, des vêtements. Des professeurs à la retraite proposent de l'aide aux devoirs, des Syriens veulent faire de la traduction. Tout le monde veut contribuer et faire partie de ce moment historique», dit Sylvain Thibault. Parmi les offres de dons se trouvent aussi des messages de quelques personnes qui ont déjà pris les choses bien en main. Les initiatives citoyennes se multiplient. C'est le cas de Yasmine Abdelfadel qui a décidé lundi soir qu'elle lançait un projet de paniers d'accueil contenant notamment des paquets de couches et des

fournitures scolaires. Une autre dame est en train d'amasser entre 600 et 900 toutous «pour que chaque enfant qui arrive au Québec en ait un.» Pour l'instant, les gens qui veulent faire des dons spécifiquement destinés aux réfugiés syriens peuvent le faire par l'entremise des initiatives citoyennes qui apparaissent sur les réseaux sociaux ou en communiquant avec des groupes comme la Table de concertation des organismes au service des personnes réfugiées ou immigrantes. Toutefois, la plupart des organismes communautaires sont en attente. La Croix-Rouge canadienne a ouvert, il y a quelques mois, un fonds destiné aux réfugiés syriens, mais elle attend des annonces gouvernementales pour lancer des initiatives locales qui serviront les réfugiés à leur arrivée au Canada et au Québec. Carl Boisvert, porte-parole de la Croix-Rouge pour le Québec, conseille aux personnes qui veulent contribuer à l'accueil de réfugiés ici d'attendre que les campagnes spécifiques soient mises en place. La Presse, A10

On n'a pas le temps

Alors là, un gros bravo. Quand on a retrouvé le petit Alan mort noyé sur une grève en Turquie, vous trouviez que le Canada n'en faisait pas assez pour faire émigrer sa famille chez nous. Maintenant que le Canada a décidé d'accueillir 25000 réfugiés syriens d'ici la fin de l'année, vous branlez dans le manche. Vous avez peur. Tout d'un coup qu'un ou deux terroristes se glisseraient dans le lot. J'entends des maires, des députés, des ministres réclamer des délais. Il faut prendre le temps de bien faire les choses, dites-vous. Le temps de bien faire les vérifications de sécurité. Le temps? Pendant qu'on est là à niaiser autour d'un chiffre, des bombes continuent de tomber sur la tête des gens en Syrie et en Irak. Il y a des exactions, des viols, des décapitations, des défenestrations. Et dans le lot des innocentes victimes, il y a d'autres petits Alan. Qu'est-ce qu'il vous faut pour vous convaincre que le temps presse? Des photos d'enfants déchiquetés par les explosions? Avoir du temps devant soi, c'est le luxe d'une société éloignée de la guerre comme la nôtre. Le Droit, 2/Front

Rapid resettlement is possible: expert

An authority on immigration and refugees says Canada and the United Nations have the operational knowhow and security safeguards to vet 25,000 Syrians for rapid resettlement. But the question remains: can the humanitarian resettlement project be pulled off by the Liberal government's Dec. 31 deadline without compromising domestic security? "I hate answering that question at this point," said Peter Showler, former chair of the Immigration and Refugee Board and former director of the Refugee Forum at the University of Ottawa. "(However) it is possible in a relatively short period of time - with no reference one way or the other to the deadline - to do fast, effective processing that includes reliable security screening." Immigration Minister John McCallum has said the refugees would be properly screened. "I think (McCallum's) implication has been that if it takes longer, if it goes over the deadline, then it goes over the deadline," Showler said. "Certainly my understanding from him is that getting the job done properly is the priority." Showler's appraisal came as the Ottawa Citizen learned refugees arrived Tuesday in Montreal. Department of Immigration, Refugees and Citizenship spokesman Remi Lariviere confirmed a planeload of Syrian refugees landed, but did not make clear if the group was part of the 25,000 targeted for resettlement under the Liberals' plan. Postmedia News (Vancouver Sun, A1/Front)

Clock ticking on Canada's refugee plan

The timing of Canada's crash program to bring 25,000 Syrian refugees to Canada by the end of the year keeps sliding, according to two officials familiar with aspects of the planning. The original goal had been to begin the airlift by Thursday of this week, but as no charter aircraft have been booked yet, it would now be at least one more week before flights got underway, one of the officials said. When the flights reach their peak next month, about 1,000 refugees will be arriving in Canada every day. The officials did not want to be identified because diplomats and immigration officers have been told by Ottawa not to speak about the matter, with all requests referred to the government. "Unfortunately I have nothing to say to you at the moment," Immigration Canada spokesman Jean-Bruno Villeneuve said in an email from Ottawa, adding that he was unable to confirm any details about the resettlement program. (...)But the United Nations High Commissioner for Refugees, which registers asylum seekers and is supposed to be working with Canada on its resettlement program, said this week that it remained largely in the dark about Ottawa's plans. While the UNHCR welcomed the Canadian announcement to settle Syrians, "I am afraid I cannot talk about Canada's program," spokeswoman Ariane Rummery said in an email from Geneva "until we know more about the modalities." Whig-Standard, B2

Le temps du changement
Comme il était de mise dans ces circonstances tragiques qui relativisaient tout le reste, la couverture médiatique du dernier conseil général du PLQ a été presque exclusivement centrée sur les réactions aux attentats de Paris et l'accueil des réfugiés syriens. Même s'il est passé largement inaperçu, le premier ministre Couillard n'en avait pas moins un autre message à transmettre aux militants libéraux réunis à Québec. " Le temps du changement est venu, a-t-il dit. Il faut oser faire les choses différemment, oser remettre les choses en question. " Quelques minutes plus tôt, le président de la commission politique du PLQ, Jérôme Turcotte, avait évoqué les conséquences que le vieillissement accéléré de la population aura sur les coûts des services de santé qui, au rythme actuel, accapareront 70 % des dépenses gouvernementales en 2030. Ces propos semblaient rejoindre ceux que le ministre de la Santé, Gaétan Barrette, avait tenus la semaine dernière à propos du panier de services assurés par la Régie de l'assurance-maladie. S'il n'est pas question " à ce moment-ci " d'exclure certains services de la couverture, il a averti que " la situation budgétaire du Québec nous invite à une réflexion au long cours sur ces éléments-là ". Le Devoir, A4

Weil downplays 'anxiety' as polls reveal fears
Quebec's immigration minister was scrambling to reassure skittish Quebecers and mayors Wednesday that the province's decision to welcome Syrian refugees will not come back to haunt them. But two new polls reveal the brutal Paris terror attacks have spooked people. Suddenly, many are hot on the use of military force to put out threats and favour a goslow approach to accepting refugees. "There is a period of anxiety," Kathleen Weil told reporters on her way into a meeting of the Quebec cabinet. "But I think it's important that mayors and political leaders use the right tone, give the right message. "These are some of the most vulnerable people that we want to greet and settle in Quebec." Weil was responding to growing domestic blowback over the terror attacks last Friday in Paris which left 129 people dead and 350 injured - many of them seriously. With no clear plan forthcoming from Ottawa, Canadian premiers and municipalities have been operating in a void with growing questions about how the country will handle the complicated business of feeding, clothing, housing and integrating the 25,000 Syrian refugees Canada wants to welcome by Jan. 1. The province has already identified 13 Quebec cities with sufficient infrastructure and support systems to accept refugees. Quebec's share of the 25,000 is about 6,000. Postmedia News (Montreal Gazette, A4)

PM condemns racism as Syria refugee plan opposed
Prime Minster Justin Trudeau urged Canadians to resist hatred and racism as a poll showed most Canadians were opposed to his plan to bring in 25,000 Syrian refugees by year-end and a flurry of racist incidents were reported around the country. The Liberals, who took power after an election last month, campaigned on a promise to bring in the refugees by Jan 1. Critics say the number is too large and could threaten security following the attacks in Paris. An Angus Reid poll released on Wednesday showed 54 per cent of Canadians opposed the plan, up from 51 per cent before the bloodshed in Paris. But support for the plan also increased, with 42 per cent in favour, up from 39 per cent in October. Most of those who opposed Trudeau's plan did so because of the short timeline, with 53 per cent saying the schedule was too short to ensure all the necessary security checks were completed. Another 10 per cent said 25,000 was too many, and 29 per cent said Canada should not be accepting any Syrian refugees. (...)"Diversity is Canada's strength. These vicious and senseless acts of intolerance have no place in our country and run absolutely contrary to Canadian values of pluralism and acceptance," Trudeau said. Whig-Standard, B1/Front

Les initiatives citoyennes et les dons se multiplient
« Les gens offrent des logements, des vêtements. Des professeurs à la retraite proposent de l'aide aux devoirs, des Syriens veulent faire de la traduction. Tout le monde veut contribuer et faire partie de ce moment historique », dit Sylvain Thibault. À son bureau de la Table de concertation des organismes au service des personnes réfugiées ou immigrantes, le téléphone n'arrête pas de sonner depuis des jours. Sa boîte de courriels déborde. Parmi les offres de dons de toutes sortes se trouvent aussi des messages de quelques personnes qui ont déjà pris les choses bien en main. Les initiatives citoyennes se multiplient. C'est le cas de Yasmine Abdelfadel qui a décidé lundi soir, après en avoir discuté avec ses parents, qu'elle lançait un projet de paniers d'accueil. Le concept rappelle les paniers offerts spontanément à de nouveaux voisins qui arrivent dans le quartier. Mais les tartes bien chaudes et les confitures maison

seront remplacées par des paquets de couches et des fournitures scolaires. « Des choses que les gens ne pensent pas de donner lorsqu'il y a des collectes », précise la jeune femme, encore surprise de la réponse reçue sur la page Facebook de son Opération paniers de bienvenue. Une réponse telle qu'elle est entrée en contact avec la Table de concertation pour avoir de l'aide logistique. Ce qu'elle aura. « Nous allons faire des paniers personnalisés, selon la famille à laquelle ils seront destinés. » La Presse, 5

Autre dissonance libérale

Pour une deuxième journée d'affilée, le premier ministre Philippe Couillard et son ministre Pierre Moreau ont joué des notes discordantes sur la capacité du Québec à accueillir des réfugiés syriens d'ici la fin de l'année. Le chef de l'État québécois estime que le Québec parviendra «fort probablement» à accueillir sur son sol 3650 d'entre eux avant la fin de l'année, comme il s'y était engagé. Son ministre de la Sécurité est incapable de garantir plus de 2400 réfugiés syriens sélectionnés - et non pas accueillis - au 18 décembre. «Non, on est sur la même longueur d'onde, a assuré M. Couillard en fin d'après-midi. On vient d'en parler, lui et moi, avec tous les collègues. On est très confiants d'atteindre la cible du premier contingent.» (...) Des 1200 personnes prévues à l'origine, le gouvernement Couillard rehaussait son seuil à 3650. C'était avant que l'engagement du nouveau premier ministre canadien Justin Trudeau porte à quelque 5700 le nombre de réfugiés syriens à recevoir au Québec. «Sur le premier contingent [celui de 3650 réfugiés], on n'a aucun doute parce qu'on a les moyens financiers, les mécanismes, a affirmé le premier ministre Couillard. La question qui reste à éclaircir, c'est la mise en place du plan fédéral plus large.» Pourtant, un peu plus tôt, son ministre Pierre Moreau a été incapable d'assurer que Québec parviendrait à sélectionner - et non accueillir - les 3650 personnes prévues avant 2016. Un processus d'habilitation sécuritaire effectué par Ottawa suit l'étape de la sélection par le Québec. La Presse (Le Soleil, 6,7/Front; La Tribune, A7, 23, La Tribune, A7; Le Nouvelliste, 15) * Le Quotidien, 26,27 ; Le Droit, 16) ; * Agence QMI (Journal de Québec, 4 ; Journal de Montréal, 2)

D'ex-hôpitaux ontariens pour héberger des réfugiés?

Le gouvernement ontarien songe à utiliser des hôpitaux récemment désaffectés afin d'héberger temporairement les réfugiés syriens qui doivent affluer d'ici la fin de l'année dans cette province. Le gouvernement fédéral de Justin Trudeau a promis que le Canada accueillerait 25000 réfugiés d'ici le 1er janvier 2016, et l'Ontario s'est engagée à en accueillir 10000 d'ici la fin de 2016. Le ministre provincial de la Santé, Eric Hoskins, a indiqué mercredi que son gouvernement ignorait toujours le nombre de réfugiés qu'Ottawa lui demanderait d'accueillir d'ici la fin de l'année, mais il a assuré que l'Ontario était prête à faire sa «juste part» dans cette vaste opération. L'Ontario pourrait par ailleurs accueillir et soutenir certains réfugiés sur une base temporaire, avant qu'ils ne déménagent dans d'autres provinces ou territoires, a-t-il prévenu. Le Droit, 16; * Canadian Press (Cape Breton Post, A11; The Telegram, D3; Charlottetown Guardian, A7; London Free Press, A3); * Ottawa Sun, A9

La crainte de la passoire

Un article d'opinion déclare, « Ce n'est guère surprenant: 59 % des Québécois ont peur que des terroristes se faufilent parmi les réfugiés qu'on s'apprête à accueillir, parce qu'ils doutent que les autorités soient capables d'effectuer les contrôles nécessaires pour les débusquer. C'est ce que révélait, hier, un sondage Léger mené pour le compte de TVA Nouvelles. Un sondage, on n'en sera pas étonnés non plus, qui indique que trois Québécois sur quatre craignent que des attentats aient lieu au pays. Dans la foulée du drame parisien et de ses rebondissements, de même que de l'intense médiatisation qui a cours, redouter la menace terroriste, surtout après les événements de l'an passé à Saint-Jean et à Ottawa, est un réflexe qui se comprend. On ne peut pas rester insensibles à l'horreur, à la haine. Il est normal de ressentir de l'insécurité face à des actes aussi insensés, aussi méprisables. Encore faut-il gérer ce réflexe avec sang-froid et ne pas céder à la panique ou à la xénophobie. Il faut se rappeler que les auteurs des attaques de l'an dernier chez nous étaient des Canadiens, pas des immigrants. Gardons aussi à l'esprit que la menace terroriste se propage davantage par Internet que par les frontières. Enfin, considérons qu'il y a bien plus d'actes criminels commis par des bandits et des chauffards ivres que par des terroristes. Cela dit, le Canada doit bien sûr mener une lutte impitoyable au terrorisme... » Le Nouvelliste, 18

Canadians leery of Trudeau's refugee plan
A little more than half of Canadians disapprove of the federal government's plan to bring in 25,000 Syrian refugees by the end of next month, a new poll suggests. And if they had to choose, Canadians surveyed by Mainstreet Research for Postmedia appear to be more in favour of bombing terrorists than training other armies howto fight. "The training mission has wider support. Either way, most Canadians believe Canada should be taking a role in the fight against ISIS. Only 8% of Canadians would support no action at all," said Quito Maggi, president of Mainstreet. Conducted Monday, the firm polled a total of 2,718 people. It suggests public opinion is polarized over what to do on the world stage when it comes to bombs and refugees. "Our earlier polling showed strong support for bringing refugees to Canada, but after the attacks in Paris, security is now a higher concern," Maggi said. QMI Agency (Ottawa Sun, A10; Toronto Sun)

* **13 000 réfugiés pour trois mois**
Les Forces armées canadiennes affirment pouvoir fournir de l'hébergement à un maximum de 13 000 réfugiés syriens à travers le Canada pendant une période n'excédant pas trois mois. Si l'objectif de 25 000 avant la fin de l'année est maintenu, cela signifie que les premiers arrivés ne feront que passer par les bases militaires pour ensuite être relogés ailleurs. Le Soleil, 4, 5/Front ; Postmedia News (Winnipeg Sun, A6; Ottawa Sun, A8; Toronto Sun, A4; Calgary Sun, A8)

* **Hamilton readies for influx, but many questions remain**
A broad range of Hamilton groups, agencies, churches, officials and individuals say they have been working for weeks to build plans for what could be a significant number of Syrian refugees landing in this city in the very near future. The trouble is, they don't know how many are coming, or which sponsorship and resettlement programs the refugees will be funnelled through. Hamilton Spectator, A1

* **Canadian business groups tout refugee job opportunities**
Businesses that have a hard time recruiting Canadians say they are reaching out to the federal government and the provinces to see if they can match up with the incoming wave of refugees. Lobby groups for Canadian employers are intrigued by the 25,000 refugees Prime Minister Justin Trudeau expects to bring in by the end of the year. "This has been ramping up since a year ago," said Ron Davidson, director of government relations for the Canadian Meat Council, which lobbies on behalf of meat packing plants. Embassy

* **Un élan de générosité de la population**
L'arrivée massive à Québec de 800 réfugiés syriens prévue en décembre semble provoquer un élan de générosité dans la population. Le Centre multiethnique note une hausse importante du nombre de personnes intéressées à leur venir en aide. Une bonne nouvelle pour l'organisme, qui aura grandement besoin de ressources supplémentaires. Le Soleil, 8/Front

* **Où vont les réfugiés syriens?**
L'un des terroristes à l'origine des attentats de Paris a été retrouvé avec un passeport syrien. On ne sait pas encore si le passeport est authentique ou s'il appartenait vraiment à l'homme qui s'est fait exploser au Stade de France. Mais la nouvelle a fait grand bruit, provoquant des mouvements partout dans le monde afin de fermer les portes aux réfugiés syriens. Voici quelques chiffres pour faire le point sur la crise humanitaire de l'heure. Depuis 2011, l'Agence des Nations unies pour les réfugiés (UNHCR) a dénombré plus de 4,2 millions de personnes qui ont fui la guerre en Syrie. La très grande majorité a trouvé refuge dans des pays limitrophes. Plus du quart d'entre eux ont moins de 18 ans. L'Europe a accueilli à ce jour près de 510 000 réfugiés, dont plus de 150 000 en Allemagne. De son côté, le Canada propose de recevoir d'ici la fin de l'année 25 000 nouveaux réfugiés qui s'ajouteraient aux quelque 3000 déjà au pays. Voici une douzaine de pays ou de régions qui ont accueilli des réfugiés syriens jusqu'à présent. La Presse, A11

* **Accueillir des réfugiés est un devoir**
Comment les réfugiés syriens traverseront-ils l'océan vers le Canada? Quels sont les risques que des terroristes s'infiltrent parmi eux? Beaucoup de Québécois ont des appréhensions face à leur venue. Alors est-ce risqué pour eux de venir ici? Pourquoi les médias ne parlent-ils pas des réfugiés innombrables de

l'Afrique? Des questions comme celles-là, les élèves de cinquième secondaire de l'école Les Pionniers de Trois-Rivières en avaient plusieurs pour Béatrice Vaugrante. Le Nouvelliste, 5

*** Region prepares for 1,150 Syrian refugees**
Planning is underway to prepare for upward of 1,150 Syrian refugees who are soon expected to start arriving in Waterloo Region. Immigration Partnership is hosting a half-day preparedness planning session on Friday that will gather together service providers to be ready for the influx of refugees. The Record, B2

*** Canada should look to the U.S**
Six weeks to go until the new year and by the time we usher in 2016, the Liberal government is determined that 25,000 Syrian refugees will be in Canada. "There was an election. There was a commitment. And we'll deliver on our commitment," Foreign Affairs Minister Stephane Dion told reporters Wednesday at the annual summit of Pacific Rim leaders here. The Liberals may be determined to deliver on that commitment but there is growing unease in Canada that the arbitrary deadline of Jan. 1 may lead authorities to cut corners and open potential security concerns. Prime Minister Justin Trudeau himself says that won't happen but, so far, has yet to provide details on Canada's security arrangements. Trudeau will meet U.S. President Barack Obama on Thursday and, because of our long, shared, undefended border, one would assume Obama wil I want more than platitudes, he'll want some of those details. Postmedia News (Toronto Sun, A22; Calgary Sun, A35; Edmonton Sun, A50)

*** Blue Rodeoto Canada**
The Liberal government's plan to welcome 25,000 Syrian refugees into Canada shouldn't be deterred by recent terror attacks, said Blue Rodeo bandmates Jim Cuddy and Greg Keelor. Cuddy and Keelor, who were among 12 officers and 33 members welcomed into the Order of Canada Wednesday, continued their streak of political pillow talk to discuss some of the major issues facing Canadians under a new Liberal government. Ottawa Sun, A14

*** Ils ne l'ont pas, le temps**
Un article d'opinion déclare, « Alors là, un gros bravo. Quand on a retrouvé le petit Aylan mort noyé sur une grève en Turquie, vous trouviez que le Canada n'en faisait pas assez pour faire émigrer sa famille chez nous. Maintenant que le Canada a décidé d'accueillir 25 000 réfugiés syriens d'ici la fin de l'année, vous branlez dans le manche. Vous avez peur. Tout d'un coup qu'un ou deux terroristes se glisseraient dans le lot... » Le Droit, 21

*** PM has no clear plan**
An opinion piece states, "To be clear: I absolutely believe this country should take Syrian refugees. We have so far been sheltered from the humanitarian crisis that has engulfed Europe, as hundreds of thousands of migrants have fled the turmoil in Syria. What troubles me is the haphazard manner in which the federal government is going about it and the way it's turned into a political football..." Postmedia News (Ottawa Sun, A9; Toronto Sun, A5)

*** Here, the Pope would be suspect**
An opinion piece states, "Back in September, Pope Francis commented on the ongoing refugee crisis in the Mideast in an interview with a Portuguese radio station. He warned of the danger of Islamic State terrorists "infiltrating" European countries amid the huge flow of refugees streaming out of war-torn Syria and Libya. He also cautioned that host countries taking in refugees "cannot be simplistic" about integrating them into their societies, because of their own high unemployment rates. In Canada these days, such reasonable observations, are enough to get one accused of bigotry, hating refugees and fear-mongering by the liberal and Liberal elite..." Postmedia News (Ottawa Sun, A19; Toronto Sun, A15; Calgary Sun, A15; Edmonton Sun, A15)

*** Provinces need more of a role helping refugees**
An opinion piece states, "Most of Canada's premiers are outdoing each other with generous offers to accept Syrian refugees by the thousands during the next six weeks, but their promises are all but meaningless. Premier Kathleen Wynne re-stated her promise-2,500 refugees by the end of this year and

10,000 by the end of 2016-again Tuesday. "It's our responsibility to be open to the world," she said in Toronto..." Postmedia News (London Free Press, A6; Whig-Standard, A4)

*** The refugee discussion is just beginning**
A comment by Jeffrey Simpson reads "The commitment to bring 25,000 Syrian refugees to Canada before Dec. 31, made by the Liberals in the heat of an election campaign, should be seen not as the end but as the beginning of a multiyear commitment to bring tens and tens of thousands more refugees to Canada over many years. Quite apart from whether the government can meet its artificial and politically driven timetable for the 25,000, the larger question is whether the government and the Canadian people are willing, ready and able to handle much bigger numbers in the years ahead. No one has thought about this, let alone prepared for it. Circumstances, however, will force reflection. This 25,000 contingent, and the many who will follow if the government sticks to its policies, is not like, say, previous groups of refugees from Vietnam, Uganda or Kosovo. These groups were much smaller in number, displaced by one event at a given place. By contrast, there were three-day periods throughout the summer and fall when more refugees/migrants were landing on the Greek island of Lesbos than Canada proposes to admit in two months. Today's refugees/migrants are part of a mass movement of millions of people fleeing military conflict, entrenched poverty and government breakdowns across an arc of states in the Middle East and Africa. Climate change is already widening desertification, which causes people to leave drought in search of food." Globe and Mail, A19

*** Our history will win over our fear, anger**
An opinion piece states, "Canadians mostly have opened their doors and their hearts to refugees, displaced persons and immigrants since the 19th century, but it would be a mistake to believe it always was easy and that it happened without some of the fear and political grandstanding now surrounding the Syrian refugee crisis. Yet the common denominator for newcomers to Canada has always been the same, the promise of opportunity, tolerance, freedom and safety. In this, the vast majority of Syrians seeking refuge in Canada are no different from the millions of immigrants who came before them..." Postmedia News (Whig-Standard, A4; London Free Press, A6)

*** Trudeau focused on 'sunny ways'**
A letter to the editor states, "With no foreign policy credentials or experience, Justin Trudeau, in the aftermath of the Paris massacre, is Mark Twain's The Innocents Abroad, peddling his "sunny ways" election message of feel-good infrastructure deficit investment and economic inclusiveness to a G20 audience that is single-mindedly focused on dealing with the global threat of international terrorism. There is Trudeau, valiantly offering the world his prescription for saving an endangered middle class while an endangered world is grappling with how to save itself. But, of course, in Trudeau's world, Canada has nothing to fear from ISIS because of its much-vaunted multicultural diversity and inclusiveness, and soon to become the new home of some 25,000 Syrian refugees to be rushed into the country by year's end with electoral refugee "politics" trumping sustainable and responsible refugee "policies." As to fighting ISIS - glory be! Liberal "soft power" days are here again!" Windsor Star, A7

*** We must be vigilant in accepting refugees**
An opinion piece states, "The world has changed dramatically for Canada's new prime minister. Justin Trudeau needs to acknowledge the gravity of the situation imposed by the Paris terrorist bombings and enhance Canada's military commitment to fighting ISIS, rather than emasculating it. He should ensure no Syrian refugees, let alone 25,000, set foot on Canadian soil without a careful and comprehensive security screening process in place..." Winnipeg Sun, A13

*** Why Canada Can Safely Meet Its Refugee Commitments**
An opinion piece by an immigration lawyer states, "The attacks in Paris last week set off a world-wide flood of empathy and solidarity. Canadians attended vigils, lit monuments in the tricolour and mourned the loss of life and normalcy in the City of Love. However, grief quickly turned into anger, inciting the inevitable search for a scapegoat. Shocking instances of violence against mosques and Muslims have been reported around the world, including a fire at a mosque in Peterborough, Ontario. Xenophobic acts are not an uncommon public reaction; a spike in attacks on Muslims following terrorist attacks has been well studied and documented. In Canada, despite the objective lack of connection, politicians began

sounding off "security concerns" related to incoming Syrian refugees. Saskatchewan's Premier Brad Wall called for a delay in resettling Syrian refugees. Premier Christy Clark of British Columbia stated the obvious: that the government needs to ensure that security checks are done on every refugee. These statements demonstrate a clear lack of understanding by government officials of Canada's process for resettled refugees. Contrary to the influx of migrants crossing into Europe over the past months, Canada is resettling *pre-screened* refugees who have been approved for permanent residency by a Canadian visa officer abroad. The process is thorough and involves international and national law enforcement agencies." The Tyee (2015-11-18)

Lettre - Main-d'oeuvre et réfugiés
Une lettre à l'éditeur déclare, « A la suite de la proposition d'accepter 100 000 réfugiés syriens par année au Canada, il était particulièrement ahurissant d'entendre la présidente de la Fédération canadienne des entreprises indépendantes (FCEI), Martine Hébert, affirmer : " N'importe quelle politique permettant la venue de plus de travailleurs, dont les entreprises ont tant besoin, est une bonne politique. " Mme Hébert reprenait ainsi une rengaine répétée mille fois par les organisations patronales selon laquelle plus d'immigration est toujours souhaitable en raison d'une supposée pénurie de main-d'oeuvre... » Le Devoir, A8

Refugee backlash will strengthen
An opinion piece states, "Because this is Canada, the backlash begins in the most polite of fashions. But make no mistake, a backlash against Justin Trudeau's plan to bring 25,000 Syrian refugees to this country is taking root and seems certain to build. Although the Liberal pledge should be applauded, the new government has helped fuel this backlash by its stubborn determination to meet an arbitrary deadline forged in the hothouse of election campaign politics..." Charlottetown Guardian, A9, The Record, A11)

Vetting questioned
An editorial states, "Re: Don't let Paris attacks alter refugee plan: profs (SP, Nov. 16). So University of Saskatchewan counter-terrorism expert Colleen Bell thinks that turning our backs on 25,000 Syrian refugees would be "a tragedy" because "Canada is a huge country." This is the kind of academic-think that passes for expertise these days. Bell and her fellow academic Martin Gaal are reported as saying that both the UN and Canada "conduct detailed screening" of refugees. You can buy into that Liberal myth if you like. I'm more convinced by U.S. Congressman Peter King, a member of the House Homeland Security Committee, who says "there is no reliable vetting system" for these refugees. "We don't know who these people are because there are no data bases to work from." Saskatonians appear to harbour an admirable skepticism on the issue. For example, of those who responded to a (pre-Paris) CFQC-TV survey that asked if they support Prime Minister Trudeau's plan to import 25,000 Syrian refugees before year-end, 83 per cent replied No. Many media commentators and Canadians alike are cynical about Trudeau's claims that the refugees will be screened rigorously. I will be looking to see exactly which "robust" vetting methods his functionaries employ. But I won't be holding my breath that we'll be given many details." Postmedia News (StarPhoenix, A8)

Logistics, not background checks, are the problem
A letter to the editor states, "White House spokesman Josh Ernest said Wednesday the 10,000 Syrian migrants destined for the U.S, will be subject to background check vetting that can "last up to 24 months" before they are approved, or rejected, as immigrants. Fortunately for the 25,000 Syrian migrants heading for Canada, our security checking is apparently so overwhelmingly comprehensive that the 25,000 will be vetted and accepted into the Canadian family by New Year's Day. Of course, after New Year's, when one or two, or 20 migrants turn out to be Islamic State of Iraq the Levant recruits and sneak into the U.S. to inflict mayhem there, watch out for the wall construction to begin across the 49th parallel and the total loss of U.S. confidence in Canada as a reliable neighbour and ally." Postmedia News (National Post, A11)

Keeping the door open
An editorial states, "The terror attacks in Paris have provoked a maelstrom of emotions and calls to action. It's crucial that governments and individuals refrain from responding in ways that do more harm than good. Reports that one of the attackers had entered Europe as a Syrian migrant have heightened

Canadians' fears. That's because Canada has committed to welcoming 25,000 Syrian refugees by year's end. There had been warnings that ISIS might slip terrorists into the flow of Syrians seeking refuge in the West, and that one case is being cited as confirmation. However, that threat does not justify closing the door to the vast majority of legitimate refugees; it's a reminder of the need for effective security screening. Canada's new government has reiterated its promise to take in 25,000 Syrians by Dec. 31, and for this it should be commended. The renewed commitment underlines a message that is worth repeating : Asylum seekers should not be conflated with terrorists; they are fleeing terror." Postmedia News (Vancouver Sun, B6)

Syrian refugees now scapegoats
An editorial states, "The tragic events in Paris have resulted in an unfortunate over-reaction. There are the expected demands for justice and calls for revenge. But the alarm bells are now sounding that Syrian refugees are guilty until proven innocent. When politicians, statesmen and decision-makers are caught up in this hysteria, it is very disappointing. This irrational conclusion is threatening the refugee resettlement program involving thousands of innocent Syrian refugees involving many nations, including Canada. The attacks in Paris were carried out by French and Belgian citizens. Likely, they were radicalized by terrorist elements or inspired by real or perceived attacks or discrimination against Islam and Muslims. The murders carried out by fanatics have somehow resulted in blame being placed on innocent refugees..." Charlottetown Guardian, A8

Whose side are we on?
An opinion piece states, "There are all sorts of fascinating and necessary questions that remain unanswered about exactly why, whether or when Prime Minister Justin Trudeau should or will withdraw Canada's CF-18s from the U.S.-led coalition arrayed against the Islamic State of Iraq and the Levant (ISIL). There are at least as many troubling questions about whether it is wise or even remotely possible for Canada's new Liberal government to fulfil Trudeau's campaign promise to resettle 25,000 Syrian refugees in this country before Christmas. (...) But if Trudeau's Canada is to be something truly new and different, then in this most horrific of global calamities, Canada should be the voice for Syria's voiceless. That's whose side we should be on." Postmedia News (Ottawa Citizen, C7; National Post)

Let Watson stay
A letter to the editor states, ""... Canada should be a refuge from militarism." PM Pierre Elliot Trudeau, 1970 Among the policies of the past 10 years that the new government seeks to reverse, one is urgent and could be made with the stroke of a pen. Against the will of Parliament, who voted twice to let American war resisters stay, Harper's government issued a deportation order against Rodney Watson, who then went into sanctuary for six years in First United Church, Vancouver. Canadian Immigration Officers waited outside to deport Watson to the U.S., to spend up to two years in prison. What a different era we are in compared to the Vietnam War. In 1967, myself an officer in the U.S. Military Medical Corps, and my wife Bonnie, later an Officer of the Order of Canada, were processed at midnight at Dorval Airport, receiving Landed Immigrant status in 20 minutes. Prime Minister Justin Trudeau has expressed empathy for the plight of refugees from the Iraq War. Urge him and Citizenship, Immigration and Refugee Minister John McCallum, to rapidly end this travesty of justice." Postmedia News (Vancouver Sun, B7)

PUBLIC SERVICE / FONCTION PUBLIQUE

Open public data necessary for functioning democracy
An opinion piece states, "There may be a new era coming in our federal access-to-information laws, and that would be a good thing, However, it's one thing to promise access in a campaign and another to follow through when in government. We'll have to wait and see. Information laws exist to protect our collective right to access public records. Every citizen and permanent resident in Canada has the right to request information from federal, provincial/territorial and municipal governments. All orders of government are subject to the protocols set out in the Access to Information Act (ATIA) at the federal level and Freedom of Information (FOI) legislation at the provincial/territorial and municipal levels. These legal instruments allow individuals to request records, policy documents and correspondence that show how government agencies operate. ATI/FOI files are different than the open-source material found on government

websites, in the rhetorical speeches of politicians, and in the sanitized information packages of public relations experts. ATI/FOI files illustrate how power operates in democratic societies and can expose the often-secretive dealings between state entities and political players. There have been a number of instances where Canadians have become aware of an issue of public interest because of information uncovered using access-to-information laws." Winnipeg Free Press, A9

OTHER / AUTRE

*** Clarity from Liberals needed to calm tensions, says Ambrose**
The new interim Conservative leader is promising to change the party's tone, but Rona Ambrose was not as willing Wednesday to say she would abandon the practice of using cultural wedge issues as a political tactic. Ambrose was asked about a recent tweet in which MP Candice Bergen said she was embarrassed and sickened by Prime Minister Justin Trudeau's approach to the fight in the Middle East and his promise to resettle 25,000 refugees. The Liberals intend to withdraw Canada's jets from the ongoing bombing campaign against the Islamic State of Iraq and the Levant, also known as ISIL or ISIS, but will keep soldiers in the region to train anti-ISIL fighters. Ambrose chalked up Bergen's tweet to heightened passions in the wake of Friday's attacks by ISIL militants in Paris, which killed 129 people and left hundreds more injured. "After what happened last week, there is going to be some emotion and some passion and I'm going to chalk that one up to some emotion and passion," Ambrose said. Similar passions were conjured up during the election campaign in response to the Conservative emphasis on issues like the niqab ban and a tip line to report so-called "barbaric cultural practices," Ambrose acknowledged. Both were considered to be wedge issues exploited by the Conservatives to mobilize votes. Ambrose said she was not part of the decision to promise a tip line, nor did she support it.
But when asked whether her party would drop the wedge politics strategy, Ambrose didn't answer.
Canadian Press (Telegraph-Journal, A8); * Toronto Star

*** Whose side are we on?**
An editorial states "There are all sorts of questions that remain unanswered about Prime Minister Justin Trudeau's decision to withdraw Canada's CF-18s from the U.S.-led coalition fighting against the Islamic State of Iraq and the Levant (ISIL). There are at least as many troubling questions about whether it is wise, or even remotely possible, for Canada's new Liberal government to fulfil Trudeau's campaign promise to resettle 25,000 Syrian refugees in this country before Christmas. But there is a far more important unanswered question that deserves at least some passing attention in all this: just whose side are we on, anyway? For five full years, Stephen Harper's Conservatives chose to go along to get along with U.S. President Barack Obama's half-baked responses to the hideously violent Baathist reaction to the Arab Spring that has now metastasized into the world-devouring catastrophe with its jihadist epicentre in the Syrian hellhole of Raqqa (...) Of course there are other questions. Up to 1,000 Syrian refugees a day are expected to begin arriving next week in the first convoy of a half dozen widebody jumbo jets shuttling Syrian refugees from Jordan, Lebanon and Turkey to Canada. About all that, here's just one of the questions that remains unanswered: what exactly are we going to do with all these people?"
Postmedia News (National Post, A10)

*** Slain volunteer fighter to be honoured**
He was a volunteer fighter in a war in which Canada has no regular troops on the ground.
The group he fought with has murky ties to a group Canada officially lists as a terrorist organization.
John Gallagher, 32, who grew up in Southwestern Ontario and died fighting alongside Kurdish forces against the Islamic State in Iraq and the Levant (ISIL) in Syria, will get a hero's welcome home Friday when his body is returned from the Middle East. His death - and the Highway of Heroes-style salute planned for him - opens a new chapter in Canada's military story, one highlighting the shifting nature of allegiances and the tricky job of honouring those who serve. "He used to be in the military," said Casper Koevoets of the Royal Canadian Legion's Victory branch in London. "He was fighting the right fight that he believed in. I think he deserves a hero's welcome home," Gallagher was killed Nov. 4 in Syria by an ISIL "suicide attack" on Kurdish fighters with the People's Protection Units (YPG), a group that actively recruits English-speaking fighters. Its members include citizens of Canada, the United States and Britain.

Postmedia Network (Vancouver Sun, B2, London Free Press, National Post, Edmonton Journal, Whig-Standard)

*** Climate change the worst threat this century, Dion tells APEC summit**
Foreign Affairs Minister Stephane Dion says climate change is the "worst threat we are facing this century," and warned that emissions-reduction targets don't go far enough. It's a marked departure from the stance of the previous federal government, which had alternated between whether ISIL or Russia was the greatest threat to Canada and the world. The question of how to deal with climate change took centre stage at the Asia-Pacific Economic Co-operation summit Wednesday, which has brought together leaders from 21 countries on both sides of the Pacific. The Syrian refugee crisis and Trans-Pacific Partnership trade deal were also discussed. U.S. President Barack Obama said the Asia-Pacific region is particularly vulnerable to flooding and land loss associated with climate change. Ottawa Citizen (Vancouver Province, A24; Star-Phoenix; Leader-Post; National Post; Montreal Gazette)

INTERNATIONAL

False hope, no mercy for fleeing migrants
For more than two months this spring, Abul Taher did not know where his son had gone. Then his phone rang. "Your son is in the middle of the sea. Give us money," the voice on the other side said. "If you don't give the money, we will kill your son and throw him into the sea." In the background, he could hear screams from his son as captors beat him. Then his son, Muhammad Selim, was allowed to speak. "Please, give them money. Please, save my life," he said. (…)The unfolding of what Amnesty International called a "humanitarian crisis at sea" started long before Syrian refugees began leaving for Europe, and threatens to continue for years. A regional crackdown has won a pause in the number taking to the water this fall. But the grinding poverty and persecution that have driven the trade remain unchanged. "I fully expect that the trafficking will resume. I was in the camps a month ago and lots of people said, 'We don't care about the risk, we're just going to go,' " said David Scott Mathieson, a senior researcher with Human Rights Watch The long southeastern peninsula of Bangladesh slices alongside Myanmar, its 125 kilometres of sand forming one of Earth's longest beaches. It's one of the few places in Bangladesh that attract tourists. It's also home to one of Asia's most vulnerable populations, where poor farmers live alongside drug traffickers, corrupt police and a persistent dream that across the water, there is something better. Globe and Mail, A12

***L'EI lance un nouveau numéro de son magazine**
«Juste terreur» ou «juste la terreur». C'est par ce double sens arrogant - Just Terror, en anglais - que le groupe armé État islamique a coiffé la une du plus récent numéro de son magazine de propagande Dabiq, consacré en partie aux attentats de Paris. Lancé hier sur les réseaux sociaux, le numéro contient quelques images des attentats. Provenant d'agences de presse, elles ont été retouchées avant leur publication dans le magazine. La photo de la une, par exemple, montre des secouristes venant en aide à un blessé. Une femme, qui apparaissait à droite dans la photo originale de l'Agence France-Presse, a été carrément effacée de l'image avec un logiciel de retouche. Les chaussures d'une des femmes victimes de l'attentat, en bas à gauche, ont aussi été floutées. Selon nos vérifications, Dabiq n'a jamais publié de photo montrant une femme, même voilée, dans l'un ou l'autre des onze numéros précédents du magazine voué à la promotion du djihadisme. Une bombe dans une canette Dabiq a aussi publié une image de ce qui serait la bombe artisanale utilisée par l'EI pour abattre l'avion de Metrojet qui s'est écrasé dans le désert du Sinaï, en Égypte. Le dispositif aurait été dissimulé dans une simple canette de boisson gazeuse. «On ne voit que trois éléments: la canette, une charge explosive et un commutateur. Il n'y a pas de minuterie ou de dispositif de déclenchement à distance. Ça laisse croire, si l'image est véridique, qu'ils ont utilisé un kamikaze pour commettre l'attentat», note le Canadien Yannick Veilleux-Lepage, spécialiste de la propagande terroriste à l'Université St. Andrews, en Écosse. La Presse, A14

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PS.PSPMediaCentre/CentredesmediasPSP.SP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 19, 2015 / 19 novembre 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Réfugiés - L'objectif réel d'Ottawa prendra plus de temps
La promesse libérale de faire venir 25 000 réfugiés syriens " parrainés par l'État " ne sera pas remplie avant le 31 décembre : le gouvernement se donne quelques mois de plus pour atteindre cette cible, a appris Le Devoir. Les réfugiés qui arriveront avant la nouvelle année seront entre autres parrainés par des organismes privés. Le gouvernement fédéral a ainsi confirmé mercredi que plusieurs milliers de réfugiés faisant partie de la cohorte des 25 000 attendus avant 2016 sont en fait des déplacés qui seraient venus au Canada peu importe les résultats de l'élection du 19 octobre. " Les demandes de parrainage provenant du secteur privé [généralement des familles qui font affaire avec des organismes] font partie de notre objectif à court terme ", a expliqué Nancy Chan, porte-parole d'Immigration, Réfugiés et Citoyenneté Canada. Impossible de savoir exactement quel sera le ratio de réfugiés parrainés par le privé ou par l'État. Le ministère soutient ne pas " avoir plus de précisions à donner pour l'instant "... Ces détails suggèrent que la pression immédiate mise sur le processus de sélection et de vérification des dossiers de réfugiés sera plus légère de quelques milliers de cas. Le **ministre de la Sécurité publique**, **Ralph Goodale**, a par ailleurs confirmé mercredi que les dossiers de tous les réfugiés seraient épluchés et qu'aucun d'entre eux ne profitera d'une vérification allégée. Les demandeurs d'asile seront rencontrés en entrevue, les données biométriques seront contrôlées, leur passé corroboré dans des bases de données canadienne et internationale. ***" Nous détaillerons les différentes étapes de contrôle quand***

le plan complet sera annoncé. Mais ce sera robuste et nous voulons nous assurer que la qualité de la vérification de sécurité, au final, est au rendez-vous ", a-t-il dit en point de presse. Ce processus de contrôle prend actuellement 12 à 18 mois. Il faudra attendre ladite annonce officielle pour préciser les délais anticipés. ***" Mais ce sera beaucoup, beaucoup plus court*** ", a certifié M. **Goodale**. Le **ministre** avait évoqué la possibilité la semaine dernière qu'une part des vérifications soit menée une fois les réfugiés en sol **canadien**. ***" Notre objectif est d'accomplir la plus grande part du travail avant que les nouveaux arrivants arrivent ",*** a-t-il affirmé mercredi. Quant aux populations ciblées par Ottawa, ce sera les ***" vulnérables, qui [soulèvent] le moins de questions [en matière] de sécurité, et des gens qui ont les meilleures chances d'avoir une intégration réussie "***, a expliqué le ministre. Ottawa demeure globalement avare de détails sur la mécanique de l'opération, à six semaines de l'échéancier qu'il s'est fixé. Mercredi, Cogeco Nouvelles soutenait que la base de Valcartier pourrait accueillir 500 réfugiés dès le 1er décembre. La base de Trenton en recevrait pour sa part 1000. Le **ministre Goodale** a refusé de commenter ces informations. Le Devoir, A1; * La Presse, A7 (La Voix de l'Est)

Processing of Syrians can be 'fast, effective'

A respected authority on immigration and refugees says **Canada** and the United Nations have the operational know-how and security safeguards to safely vet 25,000 Syrians for rapid resettlement. But the question remains: Can the humanitarian resettlement project be pulled off by the Liberal government's looming Dec. 31 deadline without compromising domestic security? (...) Immigration Minister John McCallum has repeatedly said the would-be refugees will be properly screened. "I think his implication has been that if it takes longer, if it goes over the deadline, then it goes over the deadline," Showler said in an interview with the Citizen. "Certainly my understanding from him is that getting the job done properly is the priority."(...) **Public Safety Minister Ralph Goodale** Wednesday tried to reassure **Canadians** the timetable will not compromise safety. ***"There have been very enormous efforts and thorough consultations ... to make sure that that system is strong," Goodale*** said. Michel Coulombe, director of the Canadian Security Intelligence Service, added: "I want Canadians to know that as director of CSIS I am confident that the measures in place are robust and appropriate." Under normal circumstances, Showler explained, Canada's refugee-resettlement process happens in three phases. His comments are based largely on his experience helping Syrian and other refugees in Lebanon last year... Phase three is security screening by Canada-based CSIS, RCMP and Canada Border Services Agency officers. Names, travel documents and sometime a person's biometrics are checked against national and international police and security intelligence databases. **Goodale** and CBSA president Linda Lizotte-MacPherson said Wednesday no refugees will be allowed into Canada until those checks come back clean. Postmedia News (Ottawa Citizen, A1/Front); * Postmedia Network (Vancouver Sun, Windsor Star, StarPhoenix, Calgary Herald, Leader-Post, National Post, Gazette, Edmonton Journal)

RCMP, CSIS say Ottawa's refugee plan is feasible

The heads of Canada's police and spy agencies are backing the Trudeau government's plans to safely screen and bring in 25,000 Syrian refugees by the end of the year. A number of municipal and provincial politicians have called on the government to take longer to conduct security checks on the asylum seekers, but RCMP Commissioner Bob Paulson and CSIS director Michel Coulombe insist the government's plans are feasible. As the pair spoke alongside **Public Safety Minister Ralph Goodale** at a news conference in Ottawa Wednesday, giving assurances that it can be done in that time frame without compromising the country's safety, Ontario's Health Minister told reporters how Canada's most populous province can help meet the commitment. Details so far are vague as to Ottawa's plans, but Eric Hoskins says that Ontario is looking at decommissioned hospitals as potential housing for refugees. He noted, for example, that Toronto's Humber River Hospital has moved from three sites to one... "Yes," he answered in a direct question on the government's ability to meet its deadline. "We will play a role in making the security checks and confirm people's identity. In my view, the system is satisfactory." Added Mr. Coulombe, the director of CSIS: "I am confident that the measures in place are robust and ... appropriate." **Mr. Goodale** said that the first objective of the government's promise to take in 25,000 refugees is humanitarian, in order to ***"rescue people who are in terrible conditions and fleeing from the scourge that is [the Islamic State],"*** However, he added the government would meet its objective ***"without any diminution or reduction in our security work."*** The **Public Safety Minister** said federal officials would conduct database checks and **biometrics** tests to verify the ID of all refugees, in addition

to submitting them to interviews. To do the task quickly, some officials from other agencies are being seconded to the operation, including border guards. Globe and Mail, A1

Canada-Paris link probed
The RCMP is looking into whether the Islamic State in Iraq and the Levant's claim of responsibility for the Paris attacks was made by a Canadian, a spokeswoman for the police force says. Staff Sgt. Julie Gagnon said the RCMP was "following up" on reports the English-language audio recording issued by the terrorist group sounded Canadian. "What I can tell you is that we are aware of the reports and are following up," she told the National Post, responding after she was asked whether the RCMP was investigating whether a Canadian had made the ISIL statement. A **Public Safety Canada spokeswoman**, meanwhile, said, ***"We do not generally discuss operational matters related to national security"*** but that police and security agencies ***"continue to monitor the situation in Paris very closely."*** The morning after the co-ordinated killings that left 129 dead, ISIL released a series of written and audio statements in Arabic, French and English that said "a group of believers from the soldiers of the Caliphate" were responsible. The attacks targeted "the capital of prostitution and obscenity, the lead carrier of the cross in Europe - Paris," the statements said, adding France was singled out because of its role in the international coalition fighting ISIL in Syria and Iraq. The identically worded releases offered no new information about the attacks other than what had already been reported but the familiar accent of the narrator of the English version caught the attention of some Canadians. Dozens of Canadians have joined the conflict in Syria and Iraq, some on the side of ISIL. On Tuesday, former Calgary resident Farah Mohamed Shirdon, 22, who has appeared in previous ISIL videos, was placed on the INTERPOL wanted list. Kingston Whig Standard, B1/Front (National Post); Toronto Star, A8

*** Ottawa ne voit pas de menace imminente**
Malgré les attentats de Paris, le niveau d'alerte au Canada demeure inchangé, a indiqué le gouvernement libéral mercredi, tentant de se faire rassurant. Mais les autorités ont du même souffle reconnu qu'elles ne peuvent pas garantir hors de tout doute qu'aucun des Canadiens partis rejoindre le groupe armé État islamique n'est revenu au pays. " On ne peut pas garantir à 100 % qu'on peut détecter le retour de ceux qui sont là [au Moyen-Orient] ", a consenti le directeur du Service canadien du renseignement de sécurité, Michel Coulombe. L'un des terroristes qui pourraient être impliqués dans les attaques commises à Paris vendredi dernier devait se trouver, selon les informations de la communauté internationale, en Syrie. Or, il appert qu'Abdelhamid Abaaoud aurait été tué dans l'assaut lancé en banlieue parisienne dans la nuit de mardi à mercredi, selon le Washington Post. Se peut-il alors qu'un Canadien comme John Maguire, qu'on croit mort au combat en Syrie, soit discrètement revenu au pays sans que les autorités s'en soient aperçues ? " Il y a toujours une possibilité -- l'utilisation de faux documents par exemple serait une façon d'arriver au Canada. On met en place toutes les mesures avec nos partenaires domestiques et internationaux pour pouvoir détecter le retour. Mais comme toute chose dans la vie, une garantie à 100 %, ça n'existe pas ", a admis M. Coulombe lors d'une conférence pour faire le point sur l'état de la menace terroriste au Canada. Les autorités estimaient, l'an dernier, qu'une centaine de Canadiens sont partis à l'étranger grossir les rangs des organisations terroristes.
Vigilance M. Coulombe et le **ministre de la Sécurité publique**, **Ralph Goodale**, sont cependant catégoriques : le niveau d'alerte n'a pas changé depuis l'attentat d'octobre 2014 au parlement, et les individus impliqués dans les attentats de Paris n'ont aucun lien avec le Canada. Les deux hommes ont néanmoins appelé les Canadiens à demeurer ***" vigilants ".*** Le Devoir, A2; Canadian Press (Red Deer Advocate, A5, Cape Breton Post, Guardian, Telegram); 1 (Times Colonist, A9); Agence QMI (Journal de Québec, 7, Journal de Montréal); La Presse Canadienne (Le Droit, 16, Le Nouvelliste, La Tribune, Acadie Nouvelle); Ottawa Sun, A3

*** Canadians prefer bombs over trainers against ISIL, poll finds**
Canadians broadly approve of both the country's bombing mission against Islamic State and its program of training those who fight the militant group. But if they had to choose between the two policies, more would opt for bombs over trainers, a new poll for Postmedia has found. The study by Mainstreet Research, conducted three days after the deadly terror attacks in Paris, also found Canadians were not sure the country was prepared to deal with a terrorist attack, even as they maintained they don't feel personally threatened (...) Prime Minister Justin Trudeau has vowed to end the bombing campaign on ISIL militants in Iraq and Syria before March 2015. Meanwhile, he will expand the training mission,

although details on how this will be done have not yet been provided. He told reporters this week he wants Canada to be "a strong and positive contributor to the continuing mission against ISIL." Meanwhile, more than four in 10 Canadians said they didn't think Canada was prepared to deal with a terrorist attack should one occur here. Twenty-six per cent felt the country was prepared but fully one-third said they didn't know. Nonetheless, almost twothirds said they are not concerned about a terrorist attack where they personally live or work. This last finding is in accord with the government's own message. On Wednesday, **Public Safety Minister Ralph Goodale** said there's no reason to raise Canada's threat level, even after the Paris attacks. Postmedia News (Ottawa Citizen, A10)

*** Cyberattacks on infrastructure a 'major threat,' says CSIS chief**
The head of Canada's main spy agency says he views the possibility of a cyberattack by ISIS or other extremist groups on the country's "critical infrastructure" as "a major threat." "Cyber is one of our top priorities," Michel Coulombe, director the Canadian Security Intelligence Service (CSIS) told an Ottawa news conference on Wednesday. Coulombe was responding to questions after Britain announced it is nearly doubling funding for cyber counterterrorism amid fears ISIS is looking to target Western infrastructure such as hospitals, airports or power plants by using the internet. He was flanked by RCMP Commissioner Bob Paulson and **Ralph Goodale**, Canada's newly appointed **minister of public safety**. ***"This is an area that I'm beginning to be further briefed on by the department,"*** Goodale told reporters, deferring to his deputy minister and CSIS. CBC News

*** Those calling for a refugee crackdown should tread carefully**
An editorial states "The debate over whether to adjust our refugee policies on the chance that a **terrorist** might use them to enter Canada has had less to do with calculating the actual threat - and more to do with passing judgment on hundreds of thousands of desperate people.Following the traumatic attacks in Paris last week, refugees from Syria - people without homes or food or much money - have suddenly become the key suspects in the effort to thwart future terrorist plots.In Canada, those who have taken this leap of faith include the Conservative Party of Canada, several prominent pundits and one premier. They argue the federal government should slow down on its promise to bring 25,000 refugees from the Middle East by the end of the year.While the situation remains unclear and difficult to judge, people should tread with caution before agreeing with this speedy assessment. Xenophobic fear has accompanied all major refugee migrations; it's a story as old as exodus itself. The Islamic State itself reportedly believes the refugees are apostates who deserve to die. Denying haven to so many refugees amounts to delivering them into the hands of psychopaths.(...) A complete description is unlikely, but most of the information so far available has been coming from media reports - not the government. Before the Paris attacks, **Public Safety Minister Ralph Goodale** said refugee claimants are less of a security threat than the previous Conservative government thought. He owes the public a detailed explanation of what he meant then and whether he still means it now. On Wednesday, he said officials from CBSA have provided invaluable support in refugee processing." iPolitics

ATTACKS IN PARIS / ATTENTATS A PARIS

Alleged plotter remains shadowy figure
Much about Abdelhamid Abaaoud's path to armed Islamic radicalism remains mysterious. In the words of Koen Geens, the Belgian justice minister, he mutated from a student at an upscale Brussels school into "an extremely professional commando," one seemingly able to slip across borders at will, someone who openly mocked the inability of Western law enforcement agencies to catch him. On Wednesday, the fate of the son of an immigrant shopkeeper from Morocco remained unclear. Police raided a suburban Paris apartment where they believed he was hiding. The siege ended with two deaths and seven arrests but no definitive information on Abaaoud, who French authorities have called the mastermind of the violence that killed at least 129 in Paris last week. The wanted jihadi's own father believes prison - where he served time for petty crimes - changed him for the worse. After his son got out, Omar Abaaoud noticed "signs of radicalization," the elder Abaaoud's lawyer, Nathalie Gallant, told RTBF broadcasting Wednesday. If so, that would fit the pattern of a number of jihadis who were radicalized in prison. Associated Press (Chronicle-Herald, A15, Ottawa Sun, Telegraph-Journal, Times & Transcript); * Agence France Presse (Le Nouvelliste, 3, La Tribune)

*** Le cerveau des attaques mort ?**

L'Europe nageait en pleine confusion hier, alors que tous s'interrogeaient à savoir si le présumé «cerveau» derrière les attentats de Paris était bel et bien mort lors de l'assaut de sept heures à Saint-Denis. «Le présumé chef des attentats de Paris (Abdelhamid Abaaoud) a été tué hier lors de l'assaut de la police française, ont affirmé deux hauts responsables des autorités européennes», a écrit le Washington Post hier. Mais aucun autre média ni les autorités françaises n'ont confirmé cette information, ce qui a soulevé plusieurs questionnements dans la population. L'opération a été «extrêmement difficile » en raison de «l'usage de fusils d'assaut, de tirs de sniper et d'une grande offensive d'explosifs», a lancé le procureur de Paris, François Molins. L'opération qui a duré sept heures visait bel et bien le présumé «cerveau» des attentats de vendredi. Au moins deux personnes sont mortes, dont une kamikaze qui «a activé son gilet explosif au début de l'assaut», a précisé la police qui n'a pas confirmé les noms. De plus, huit personnes ont été placées en garde à vue après l'opération, mais ni Abaaoud, ni Salah Abdeslam, l'un des suspects des attaques toujours en fuite, ne figurent parmi elles. Une information qui laisse donc croire qu'Abaaoud serait le deuxième mort. Le Journal de Québec, 5 (Journal de Montréal); * Daily Gleaner, B1 (Telegraph-Journal); Associated Press (Toronto Star); 1 (Ottawa Sun, Calgary Sun, Winnipeg Sun, Toronto Sun); CNN

AIR FRANCE FLIGHT DIVERTED

Passengers aboard Air France Flight 055 didn't learn that a bomb threat was the reason their Paris-bound flight was being diverted to Halifax until after they landed Tuesday night. Genevieve Lapeyre, a pediatric anesthesiologist from Geneva, was flying back to Europe after a meeting in Washington, D.C. She is half-Swiss and half-French, and planned a three-day layover in Paris. The terrorist attacks Friday gave her a strong wish to be in the city. (…) None of the passengers panicked, but they felt something odd was going on, she said. At one point, she wondered if there had been another attack against Paris and the aircraft couldn't go there. After the Boeing 777 touched down at about 10:15 p.m., she soon realized there was something happening regarding her flight. "I saw the firemen and everything, and I said, 'OK, there is something else.'" Lapeyre said the pilot seemed to be trying to control his emotions. "He said, 'Don't worry.' He was too much trying to reassure us." On the tarmac, passengers were told to grab their belongings and get off the plane, which they did quickly. However, they were then housed for about 30 minutes in a bus parked alongside the aircraft, which some considered dangerous, she said. Halifax RCMP spokesman Cpl. Greg Church said 262 passengers and crew got off the jet within 15 minutes of landing, which is when officers began checking for explosives; none were found. The jet was declared explosives-free at 4:28 a.m. Wednesday. The passengers were taken to a secure area to pass through customs. Postmedia Network (Chronicle-Herald, A1, Guardian, Whitehorse Star, Acadie Nouvelle); Postmedia Network (Cape Breton Post, A9)

'Like A War Zone'

2 Dead, 8 in custody after paris police launch a massive early-morning raid against a suspected **terror** cell located in a reinforced apartment When Tagara Traoré, a former revolutionary soldier in his native Burkina Faso, was jolted awake by a boom early Wednesday, his "military reflex" kicked in. "You get up quickly and either hide or try to get out," he said. In socked feet and wearing the sweatpants he was sleeping in, he grabbed his key and ran out the door of his fourthstorey apartment, only to find a battalion of police rushing up the stairs, headlamps glaring. "I started sensing tear gas that was coming up the stairwell. I thought the building was on fire," he said. "The police told me, 'Go down, down, down!' There were so many they had to move aside to let me out." It was 4:20 a.m., and he had been caught in the middle of a massive anti-terror operation that quickly became a protracted gun battle between police and terror suspects. A woman in the targeted apartment in the Paris suburb of Saint-Denis, identified by French media as a native of nearby Clichy, was one of the dead. Initial reports said she killed herself by detonating an explosive vest, but the French prosecutor's office later said the "point needs to be verified by an analysis of the body and human remains." At least one other suspect in the apartment was killed and eight people were taken into custody. Five police officers suffered minor injuries, and a police dog - Diesel, a Belgian shepherd - was killed by the terrorists, according to the national police. Paris prosecutor François Molin said the targeted apartment had a fortified door that withstood initial police attempts to break in and gave the terrorists time to mobilize and return fire. Daily Telegraph (Windsor Star, N1/Front, National Post, StarPhoenix, Gazette); 1 (Vancouver Sun, B1/Front, Leader-Post, National Post, Edmonton Journal, Ottawa Citizen, Whig-Standard, Calgary Herald); Toronto Star, A1; Globe and Mail,

A1; * Agence France Presse (Le Soleil, 22); * Associated Press (Times Colonist, A13, Times & Transcript)

Prochaine station, la guerre
Il devait être 4h20 quand Fares s'est mis à crier. «Maman! Maman! La guerre commence! Il y a des bombes!» Fares a 7 ans. De grands yeux noisette dans lesquels on lit l'effroi. «Il ne sait même pas c'est quoi, la guerre», me dit sa mère Souhila, 38 ans. Souhila, elle, sait. Elle est née en Algérie... J'étais dans l'avion quand l'assaut antiterroriste a été donné à Saint-Denis, dans la banlieue nord de Paris, non loin du Stade de France. Dès que l'avion s'est posé, des cellulaires de passagers ont sonné. «C'est la pagaille à Saint-Denis.» La «pagaille», le mot est faible. C'est Fares qui avait raison. Ça ressemblait plus à une guerre. Rue Corbillon, à l'angle de la rue de la République, au moins deux personnes ont été tuées, dont une femme kamikaze qui a activé sa ceinture d'explosifs. Un commando, lourdement armé, qui semblait prêt à passer à l'acte, a été démantelé. Pendant une heure, les habitants du quartier ont entendu des tirs nourris. Le bruit était si fort que certains ont cru qu'il y avait un bombardement. Il y a eu au moins 5000 munitions tirées par la police. Un immeuble éventré, criblé de balles. Des voisins terrorisés. Comme si on était à Gaza et non en banlieue parisienne. L'assaut a duré sept heures, durant lesquelles le quartier a été bouclé, le métro, fermé, les écoles aussi. Des résidants ont été évacués. Les riverains ont été sommés de ne pas sortir de chez eux. Une fois l'assaut terminé, j'ai pu prendre le métro pour la guerre. La Presse, A4/Front

Mission
Ce sont des spécialistes des assauts risqués, qui montent au front contre les pires terroristes. Le RAID, le commando de la police française qui est intervenu hier à Saint-Denis, est constamment sollicité depuis un an. A Paris, La Presse s'est entretenue avec l'ancien chef des négociateurs de l'unité, Christian Caupenne, pour dresser le portrait d'une équipe devenue mythique. Fondé il y a 30 ans, le RAID (pour Recherche, Assistance, Intervention, Dissuasion) est l'unité d'élite de la police nationale, destinée à intervenir partout en France pour contrer le terrorisme et le «grand banditisme». Elle est notamment intervenue lors de l'attaque du marché Hyper Cacher en janvier et à la salle de spectacle Bataclan, vendredi dernier. Selon le chef de la police nationale, Jean-Marc Falcone, l'assaut à Saint-Denis a été l'un des plus difficiles que ses troupes ont connu. «Les scènes vécues par le RAID sont très dures. Même ces hommes rodés à la violence ont été marqués», a-t-il déclaré hier à ce sujet. La Presse, A5/Front

*** Paris attacks: Extremists may strike next with chemical, biological weapons, French PM says**
With France still reeling from last week's deadly attacks in Paris, Prime Minister Manuel Valls warned Thursday that Islamic extremists might at some point use chemical or biological weapons, and urged lawmakers to extend a national state of emergency by three months. "Terrorism hit France not because of what it is doing in Iraq and Syria ... but for what it is," Valls told the lower house of Parliament. He added, "We know that there could also be a risk of chemical or biological weapons." Valls did not say there was a specific threat involving such weapons. The French Interior Ministry and Paris prosecutor's office, meanwhile, said it still remains unclear whether the suspected mastermind of last week's attacks, in which 129 people were killed and hundreds of others wounded, has been killed or is still at large. Officials said authorities are working on determining whether 27-year-old Belgian Abdelhamid Abaaoud was among those killed in a chaotic and bloody raid on an apartment in the Paris suburb of Saint-Denis on Wednesday. Associated Press (CBC News)

*** Belgium vows crackdown on terrorists, boost security spending**
Belgium's prime minister on Thursday called for changes to the country's constitution to combat extremists, and promised hundreds of millions of euros to boost the security forces. Addressing the federal parliament as security forces were conducting raids around the capital Brussels, Charles Michel pledged to use changes to the constitution to extend preventive detention times for suspects from 24 hours to 72 hours. He also affirmed that Belgium would move forward alone on a system of airline passenger information sharing that European Union nations have been incapable of agreeing in four years. Associated Press (CTV News, Times Colonist)

*** EU to tighten anti-terror laws**

The European Commission, the EU's executive arm, will expand its anti-terrorist legislation early next year to target fighters like those involved in the Paris attacks. The new measures will widen the range of actions punishable under the legislation to include travelling for the purpose of carrying out a terrorist act, facilitating travel or receiving training to carry out an attack. In a direct response to the Paris killings, EU citizens who travel outside the bloc and then return to carry out attacks will be considered as foreign fighters, and those helping their movement will also face prosecution. The bloc 's Migration, Home Affairs and Citizenship Commissioner, Dimitris Avramopoulos, told a news conference Wednesday that the Commission would have proposals ready by the end of November and wants to see them enacted "within the first two months of the next year." Toronto Sun, A56 (Calgary Sun)

*** Killer's passport fueling fear of refugees**

After the bombs and Kalashnikov fire of the Paris attacks, a mere document - a passport - found near the body of an attacker is generating a new wave of dread throughout Europe and beyond. But whether the document ended up there by chance, or was part of an elaborate plot to sow panic, is not clear. Regardless of the answer, the passport has played into the Islamic State group's hands by raising concerns that militants may be marching alongside the thousands of asylum seekers flowing into Europe. That possibility is redefining the debate over immigration in Europe and even the United States, and prompting a backlash against Muslim refugees. The far-right French leader Marine Le Pen called for an immediate end to the flow of migrants into France, while across the Atlantic about half of U.S. governors are taking steps to prevent absorbing Syrian refugees in their states, citing the passport. "This terrorist attack will clearly change Europe's refugee policies and how the arrivals in Europe are treated," said Konrad Pedziwiatr, a sociologist and expert on Islam in Europe at the Krakow University of Economics. "Already the open-door policy (in Germany and Sweden) of welcoming refugees was going to be reformed because the inflow is so significant that countries cannot cope with the numbers," he said. "What the Paris attacks add to this difficult situation is the additional element of fear." A passport bearing the name of Ahmad Al Mohammad, 25, was found near one of the suicide bombers who blew himself up outside the Stade de France football stadium. It indicates that he entered Greece from Turkey on Oct. 3 and later passed through Serbia and Croatia, getting registered in every new country. The passport's authenticity has not been determined, but fingerprints of the attacker match those taken by Greece and Serbia. The other attackers who have been identified so far are all European citizens. The oddness that a passport - an intact one - was found near a man who blew himself up is creating suspicions that it is part of a plan by the Islamic State to create a backlash against the refugees. "I have never heard of terrorists carrying passports with them," Pedziwiatr said. Associated Press (Whig-Standard, B5, Telegraph-Journal, Times & Transcript)

*** ISIS is slowly killing the European experiment**

As neighours and allies declare solidarity with France, few are facing up to the inevitable: the fact that fallout from Friday's terrorist attack in Paris will stall - perhaps even reverse - the political integration of Europe. The discovery that most of the terrorists identified so far were Muslims born in France, using neighbouring Belgium as a base, will add volume to loud demands for an end to the open-border policy among the 28 members of the European Union. Pressure to terminate what is known as the Schengen Area - a pillar of the EU political integration project, along with the now-debased euro and attempts to unify foreign and defence policies - has been building as about a million refugees from the Middle East and North Africa have flooded into Europe (…) While ISIS has taken responsibility for the outrage and was, at the very least, the inspiration for it, the Paris killings were, like almost every other terrorist attack in Canada, the United States and Europe in the last 14 years, a home-grown affair. Neither Canada nor the U.S. is immune to the popular suspicion that the floods of Syrian and Iraqi refugees are an easy route for ISIS to plant terrorists in target countries. The governors of over half the 50 states in the U.S. have said they will not participate in settling Syrian refugees. And the new government of Prime Minister Justin Trudeau is facing growing pressure from both the public and provincial governments - on whom much of the responsibility for resettling refugees will fall - to rethink his campaign pledge to allow 25,000 Syrian migrants into Canada by the end of the year. iPolitics

*** French expats still feel sting an ocean away**

Juliette Elchinger was home in Montreal on Friday evening when her Twitter feed lit up with news of the terrorist assaults in Paris. "I went into a state of shock," the native Parisian said. "I just started to shake and cry." Five days later, the 19-year-old was still struggling to make sense of the violence visited on her cherished city. She stood on Wednesday surrounded by knots of other students and staff at the University of Montreal, some holding hands and wiping tears off stricken faces, for a sombre gathering of commemoration. In the days since the shocking attacks took the lives of 129 people, Ms. Elchinger has attended solidarity marches and commemorations, monitored news from Paris obsessively and joined other members of Montreal's large expatriate French community. Some have connections to the tragedy; Ms. Elchinger's best friend lost a professor, who was slain at the Bataclan theatre along with 88 others who had attended a rock concert there. For the expats, separation from events back home has fed feelings of loss and helplessness, along with a deepened call to their French identity. Globe and Mail, A9

*** Free world solidarity after Paris**

An editorial states, “There aren't a lot of game-changing moments in international affairs, says Peter Van Praagh. But the ISIS terrorist attacks on Paris last weekend, like the 9-11 attacks on New York and Washington in 2001, fall into that rare category. It is, he says, one of those "events that turn things." It has acutely heightened the public sense of "how vulnerable open societies are." But it has also produced, he believes, "a fundamental solidarity and common understanding that something has to be done to address it." "We are all affected now," the security specialist told our editorial board on Wednesday, after arriving in Nova Scotia to chair, for the seventh time, the annual Halifax International Security Forum. The forum will bring 300 delegates from 60 democratic countries to the city this weekend to brainstorm the complex angles of peace and security - military, political, economic, educational and cultural. The group ranges from four-star generals to ministers to aid organizations, journalists and scholars. Their agenda runs the gamut from building new anti-terror alliances to cutting off the financing of terrorism through drug and human trafficking. There was plenty of evidence in Halifax and elsewhere this week to show security issues now touch us all.” Chronicle-Herald, A6

*** Hollande faces the enemy from within**

The streets of Paris are no strangers to mass bloodshed. The City of Light has borne witness to more than its share of extreme violence over the centuries. The worst of it has not been perpetrated by a foreign army. The enemy has most often come from within.From the Wars of Religion, through the Revolution and the Reign of Terror, to the Paris Commune, the French often worked through their differences in the bloodiest ways possible. Since the 1960s, Paris has been a repeated target of terrorists, often French citizens or immigrants, aggrieving in some way France's unresolved colonial past in North Africa or its mandates in the Middle East.The inspiration for the most recent attacks may have come from Iraq or Syria, but their perpetrators came from the Paris suburbs. The January assaults on the satirical magazine Charlie Hebdo and a kosher supermarket were conducted by French-born radicalized Muslims. Most of those involved in Friday's sickening attacks on cafés and a concert hall appear to have had similar backgrounds."We know, and it's cruel to say it, it was French people who killed French people on Friday," President François Hollande said in a speech for the ages. "There are, living on our soil, individuals who move from delinquency to radicalization and then to terrorist criminality." Globe and Mail

*** La vie doit reprendre, dit Hollande**

Dans la foulée de la série d'attentats à Paris, le président français François Hollande a encouragé ses compatriotes à «défier les terroristes» en continuant de vivre normalement, en fréquentant les cafés, les musées, et les stades sans tomber dans la crainte et la xénophobie. Les terroristes prennent la vie des innocents, mais ils veulent aussi suspendre celle des autres, a soutenu le président, mercredi, lors d'un discours télévisé devant les maires de partout au pays. Il estime que les Français ont le «devoir» de poursuivre leurs activités normales. Il a martelé que la vie «devait reprendre pleinement», ajoutant que la sécurité serait resserrée dans les lieux publics. Le président français a assuré que la France resterait un pays «de liberté, de mouvement, de culture» qui ne «pliera pas à la peur». François Hollande s'est engagé à travailler avec ses alliés pour détruire le groupe armé État islamique, qui a revendiqué la responsabilité des attaques dans la capitale française qui ont fait 129 morts et 368 blessés. Dans une allocution prononcée quelques heures après une opération antiterroriste de la police en banlieue de

Paris, le président a réitéré que la France était «en guerre avec les terroristes», mais il a aussi appelé les Français à la retenue. Associated Press (Le Droit, 17)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Coderre veut éviter un autre Lac-Mégantic**
Depuis la tragédie de Lac-Mégantic, la Ville de Montréal se fait beaucoup plus prudente dans l'aménagement de son territoire, a expliqué Denis Coderre, hier, en réaction au reportage sur la récente interdiction de toute construction près des installations de Suncor. En revanche, au gouvernement du Québec, on ne s'émeut guère de la situation. Hier, La Presse faisait état d'un moratoire interdisant toute construction dans un rayon de 435 mètres des trois ballons de butane de Suncor. Même une enseigne de quatre pieds sur six ne peut y être installée. Le Centre de sécurité civile juge cette zone rouge à «risque très élevé» dans l'éventualité d'un accident impliquant les sphères de butane. Une explosion est jugée peu probable, mais elle provoquerait d'énormes dégâts. Or, cette zone rouge est traversée par l'autoroute Métropolitaine et 100 000 automobilistes y circulent chaque jour. La Presse, A16

*** Crise en santé publique - La surveillance de l'état de santé des Méganticois écope**
Bien que les impacts de la tragédie de Lac-Mégantic se fassent toujours sentir dans la population, la Direction de santé publique de l'Estrie a été contrainte de se départir de deux experts qui travaillaient de façon spécifique sur ce dossier. En janvier dernier, la Direction de santé publique de l'Estrie publiait une étude révélant que l'accident ferroviaire survenu à Lac-Mégantic en 2013 faisait encore souffrir la population : 95 % de Méganticois disaient avoir été touchés par la tragédie. On observait plus de dépressions, de troubles anxieux et de problèmes de consommation d'alcool. La directrice de la santé publique, la Dre Mélissa Généreux, s'en inquiétait. Pourtant, quelques semaines plus tard, elle mettait à pied le professionnel affecté à la surveillance de l'état de santé de la population de Lac-Mégantic. Ce dernier a fait les frais d'une vague de compressions imposée à toutes les directions de santé publique régionales au printemps dernier, dont Le Devoir tente de cerner les impacts dans une série diffusée cette semaine. En Estrie, la Direction de santé publique a dû couper 1,21 million sur un budget de 2,5 millions. " Ça représente 40 % de notre budget, ça a été toute une épreuve pour nous, tout un choc à absorber ", soupire Mélissa Généreux en entrevue téléphonique. Avec son équipe, elle a tenté de faire les choix " qui allaient engager le moins de conséquences possible sur la population ". Mais elle devait couper quelque part. " Ce n'est pas parce qu'on s'est dit que les impacts étaient moins importants, mais quand vient le temps de choisir les postes, il y a toutes sortes de considérants, en matière d'ancienneté entre autres. " L'enquête annuelle sur la population de Lac-Mégantic, qui est financée par un autre " petit budget protégé ", sera maintenue. " Ce qui a été plus difficile, c'est que parallèlement à ça, on ne voulait pas surveiller juste une fois par année, on avait donc un agent de programmation, planification et recherche (APPR) -- celui dont on a supprimé le poste --, qui se chargeait de faire des bulletins de surveillance périodiques. C'est lui qui prenait le crayon et qui faisait l'analyse de ces données. " Le Devoir, A1

*** Spend more to prevent dam spills, experts say**
As miners globally review the way they store waste in the wake of another horrific dam spill, the solution may be as simple as it is dramatic: spend a lot more. Images of sludge spewing into towns and rivers could be a thing of the past if mines used different types of storage such as removing water or building on more stable ground. While that can be as much as 10 times costlier for companies already squeezed by slumping prices, the cost is much higher when things go wrong. The cleanup bill for the Nov. 5 spill at the Samarco iron-ore venture in Brazil, owned by BHP Billiton Ltd. and Vale SA, probably will exceed $1 billion US, Deutsche Bank AG said. Then there's lost output and potential lawsuits. "A failure is a lot more expensive than doing it right," said Dirk van Zyl, professor of mining engineering at the University of British Columbia and one of three experts on a panel into a dam spill in Canada last year. Samarco says its dams were deemed safe in a July inspection and that it's too early to determine reasons for the spill. On Monday, BHP chief executive officer Andrew Mackenzie said the company is "carrying out a thorough review of all of our dam facilities of scale." On the same day, Vale said it's open to improvements, even after concluding that its other installations, which use state-of-theart safety practices, were fully compliant. The Samarco breach, which propelled about 50 billion litres of mud into communities below, comes a

year after Imperial Metals Corp.'s Mount Polley mine in Likely, southeast of Prince George, also dumped billions of gallons into lakes and rivers. Bloomberg (Vancouver Sun, D3)

*** Lepreau residents evacuated in simulation**
As an imaginary cloud of radioactive steam was vented from the Point Lepreau nuclear power plant Wednesday, real calls went out to residents within a 20 kilometre radius telling them to get out. By noon about 150 people were gathered in the gym at the G. Forbes Elliot Forbes Athletics Centre at UNBSJ and there was even space set up nearby for pets in a separate centre run by a disaster animal response team from Nova Scotia. It was the final part of a two-day exercise simulating a nuclear emergency at the power plant based on a couple of years of planning. The emergency was centred around an extreme bad weather event damaging the plant, said Meghan Gerrish a spokeswoman for NB Power... In September members of the media were given a tour of the plant to see the four large, mobile, diesel power generators that were added as a second level of backup to make sure there would always be power to control the equipment. The plant already had a backup generating system but the portable generators are a second level. Large water pumps capable of shooting streams of water over the outside of the reactor to cool it were also purchased. At that time Tony Munn, emergency preparedness manager at the plant, said the industry has learned many lessons from the three major nuclear accidents in the past 50 years - Three Mile Island in the United States, Chernobyl in Russia and Fukushima in Japan. Observers from utilities around the world were at the power plant during the exercise, Gerrish said. "There are over 1,000 people involved in this exercise," she said. Telegraph-Journal, B1

*** Body found near site of Tofino whale-watching tragedy - BC Coroners Services says it can't confirm if it's the passenger who was missing, presumed dead**
A body has been recovered close to Vargas Island near Tofino, B.C., says the BC Coroners Service.On Oct. 25, a whale-watching boat capsized in the area, killing five people. Another victim, 27 year-old Australian Raveshan Pillay, was never found, but presumed dead."While I appreciate there is certainly interest with the possibility this may be linked to the missing person from the Leviathan, it is premature to suggest so," said Matthew Brown with the Coroners Service. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Terror travel investigations on the rise
Radicalized Canadians intent on going to far-off combat zones are developing sophisticated cover stories and using "broken travel patterns" to disguise their true motivations, according to an internal RCMP document that reveals public safety officials were, as of one year ago, closely monitoring about 50 foreign fighters abroad and 14 who had returned home. Family and friends are often reluctant to notify police if they suspect someone is planning a trip, the document states. Also, the speed with which a person becomes radicalized to violence and makes travel plans is sometimes so fast, police only become aware of them after they've left the country. "There is no doubt that the number and complexity of terrorist travel investigations has increased," said the briefing document, which was prepared for the RCMP commissioner and obtained by the National Post through an access-to-information request. Though the document was prepared a year ago, many of the challenges of identifying extremist travellers persist, said a Dalhousie University researcher studying Canadian foreign fighters. Amarnath Amarasingam said much of ISIL's advice to people who want to migrate to Syria is to "blend in to Western ways of life," especially right before they leave... The wave of attacks in Paris last Friday that killed 129 people has heightened concerns about the foreign-fighter phenomenon. A new report this week from the think-tank Institute for Economics and Peace said an estimated 25,000 to 30,000 foreign fighters from 100 countries have flowed into Iraq and Syria since 2011 - half from neighbouring countries and a quarter from Europe and Turkey. Public safety officials in Ottawa said Wednesday there was no evidence of any Canadian involvement in the Paris attacks. They were also unaware of any direct threats to Canada related to the attacks. Amarasingam said he believes at least 60 Canadians have gone to fight in Iraq and Syria. One of them, Toronto-born Farah Mohamed Shirdon, who police say has served in combat, recruiting and propaganda roles with ISIL, was added to INTERPOL'S wanted list this week. Neither Bob Paulson, the RCMP commissioner, nor Michel Coulombe, director of the Canadian Security Intelligence Service, would say Wednesday how many high-risk travellers their agencies are tracking. Postmedia News (Vancouver

Sun, B1/Front, National Post, Ottawa Citizen, Windsor Star, Leader-Post, StarPhoenix, Calgary Herald, Gazette, Edmonton Journal, Province)

Ontario accent heard in video?
Investigators are working to confirm a potential Canadian accent heard in an English audio recording released by what is believed to be the Islamic State. The recording was released Saturday and claims responsibility for the terrorist attacks that shook Paris and the rest of the world last weekend. "It is concerning if it is Canadian, but it is speculative at this stage," said RCMP Commissioner Bob Paulson told a news conference Wednesday, adding that the Mounties are working to confirm it. Meanwhile, a dialect expert south of the border said it's very likely the male speaker has a Canadian - specifically an Ontarian - accent. "I mainly listened for vowel variations because that's where most of the variation in English is," said Erik Thomas, a linguistics professor at North Carolina State University. The professor was first asked by CNN to analyze the recording. He took detailed notes on words chosen by the speaker in the recording, such as "explosive" and "hand". "Everything he uttered seemed to match up with forms that predominate in Canada," he said. Certain vowels, such as the short 'o', were among the giveaways suggesting the accent originated in regions of either Canada or northern U.S. states. Winnipeg Sun, A7 (Ottawa Sun, Toronto Sun, Calgary Sun, Toronto Sun)

Hatred burns hot, but not very bright
Among responses to the scattered targeting of Muslims in the wake of the Paris attacks, the most indicative might be the safety preparations under way at a Hindu temple in Hamilton, Ont. Hindus had nothing to do with the killings in Paris. The "brains" behind the terrorist bloodshed appear to have lived in Belgium, not India. The preparations in Hamilton are predicated on the assumption that the sort of people who firebomb mosques and beat up helpless women won't know the difference. In other words, that they're so stupid they direct their hatred at anything that strikes them as vaguely Middle Eastern, even if they're off by an entire culture and a continent or two. There's good reason for their concern. The temple was set aflame in the days following the 9/11 terror attacks in the U.S., by someone who apparently confused it with a nearby mosque. A number of synagogues were also targeted at the time. Hatred may be all-consuming, but it's not very smart. That's already evident from the incidents of the past few days. The only mosque in Peterborough was torched by a person or persons unable to grasp the difference between peaceable people going about their life and the barbaric practices of the terrorists who characterize themselves as the Islamic State. A woman picking up her son at a school in Toronto was kicked, beaten and robbed in mid-afternoon by two men who are so stupid they think a hijab - which she was wearing - must signal support for the sort of brutalities meted out in Syria, most often on Muslims themselves. In Montreal, a man wearing a mask threatened to kill an Arab or a Muslim every week, obviously too dim to realize that plenty of Arabs aren't Muslims. There's a difference between ignorance and stupidity. Ignorance is a lack of knowledge. Stupidity is the determined projection of ignorance. It's likely that the people responsible for the incidents in Toronto, Peterborough and Montreal are both, but while ignorance is likely, stupidity is certain. Postmedia News (National Post, A1/Front)

Man charged after threat to kill Arabs in Quebec
A Montreal man will spend the next few days in jail after being charged in connection with a YouTube video in which someone wearing a Joker mask says one Arab would be murdered in Quebec every week. Jesse Pelletier, 24, was arraigned on Wednesday on charges of uttering threats, possession of a false weapon, public incitement of hatred and hoax regarding terrorist activities. Pelletier, who was arrested early Wednesday morning, will remain behind bars until his bail hearing Monday. The person in the video was wearing a Joker mask and could be seen brandishing what looked like a pistol as he made the threats and spoke about last week's terrorist attacks in Paris that killed 129 people. "It's really time to act," the person said in the three-minute video. Canadian Press (Times Colonist, A8, Calgary Sun, Telegraph-Journal, Times & Transcript, Toronto Sun, Winnipeg Sun, Kingston Whig-Standard, Ottawa Sun, Edmonton Sun, Red Deer Advocate), Presse canadienne (La Tribune, Voix de l'Est, Le Droit, Le Devoir), Montreal Gazette, Toronto Star

***To combat extremism, we must work together**
An opinion piece states "Last week, evil struck. There were vicious attacks in Paris, Beirut and Baghdad. I grieve with the families and friends of the victims and hope the perpetrators are brought to justice. Violent extremism is universally condemned; terror is never the answer and the loss of one innocent life is equal to that of all of humanity. We cannot let such horrific violence achieve its goal of striking fear into our communities and dividing us. It is deeply distressing to many that there has been apparent backlash against Muslim communities, including in Canada. In Peterborough, Ont., a mosque was set on fire last Saturday. Police are investigating the fire as a potential hate crime. This week in Toronto, a hijab-wearing woman was verbally assaulted, punched repeatedly in the stomach and had her hijab ripped off. Canadian Muslims are naturally very concerned. At the same time, Canadian Muslims know these cowardly acts do not represent our society. They are simply the ignorant expressions of criminals (…) Experts point out that there is no single reason why such people travel the path of radicalization. The roots are complex, the solutions not obvious. And combating the problem is made yet harder by the reality that this new brand of brazen terror is a contemporary phenomenon - it did not exist in the 1980s or 1990s. Toronto Star, A25

*** Doctor to assess man caught with knife on Parliament Hill**
A Toronto man arrested for allegedly carrying a hidden weapon at the entrance to the Centre Block of Parliament was remanded in custody Wednesday. Yasin Ali, 56, was detained by the Parliamentary Protective Service on Tuesday after a security screening discovered what police say was a knife. Ali made a brief court appearance Wednesday on a charge of carrying a concealed weapon. Defence lawyer Peter Azzi said his client is due back in court on Friday and will be assessed by a doctor. Neither Azzi nor the RCMP would discuss media reports that described the weapon as a meat cleaver. RCMP Commissioner Bob Paulson applauded the "great job" by the protective service, for which the Mounties have day-to-day responsibility. "The individual was identified behaving oddly, suspiciously. And one of our officers challenged him, saw the knife, took him into custody," Paulson said. "I understand that it is less a concern around socalled national security considerations than it is a mental-health issue." Security on Parliament Hill has been tight since Oct. 22, 2014, when Michael Zehaf Bibeau gunned down a soldier at the nearby National War Memorial and sprinted through the main doors of Centre Block. Moments later, Zehaf Bibeau was fatally shot by security officials outside the Library of Parliament. Canadian Press (Times colonist, A8)

*** Des musulmans sur leurs gardes après des menaces**
Menaces de mort au téléphone, agressions verbales dans la rue, messages haineux sur les réseaux sociaux: des membres de la communauté musulmane de Montréal affirment vivre dans la peur depuis les attentats de Paris. «Depuis ce qui est arrivé à Paris, je ressens une peur chez les musulmans. Je crains que tout cela finisse mal», lance Haroun Bouazzi, de l'Association des musulmans et des Arabes pour la laïcité au Québec (AMAL).«J'ai l'impression que ce n'est qu'une question de temps avant qu'un membre de notre communauté se fasse casser les deux jambes. Il y a trop de haine sur les réseaux sociaux», poursuit-il. Mercredi matin, le téléphone ne dérougissait plus à l'AMAL, plusieurs citoyens s'inquiétant de menaces de mort proférées sur les réseaux sociaux par un homme déguisé en joker, qui a finalement été arrêté par les policiers. «Beaucoup de gens m'ont écrit en panique. C'est étonnant de voir à quel point ils vivent dans la peur», affirme M. Bouazzi. Haroun Bouazzi dit recevoir régulièrement des menaces sur le site de son organisation. Mais il affirme ressentir une «pression supplémentaire» depuis quelques jours. Il n'est pas le seul. Joint mercredi par *Le Journal*, Mehmet Deger, président de la mosquée Dorval, a rapporté avoir reçu un coup de fil menaçant mardi après-midi (…) Cependant, le Centre islamique de l'est de Montréal de l'imam controversé Adil Charkaoui, de même qu'une mosquée du quartier Hochelaga, ont été vandalisés au cours des derniers jours. QMI Agency (Journal de Quebec, Journal de Montréal)

*** 'Loves Me Not' Poem Captures Heartbreaking Reality Of Islamophobia In Canada**
Taunts in public. Comments online. And recently, physical abuse. In the past months, Canada has witnessed far too many attacks against Muslims, particularly women. Earlier this week, a Muslim woman was physically assaulted in front of her children's school and called a "terrorist." In October, a woman wearing a niqab was attacked at a Toronto mall. It's difficult for most of us to imagine the emotional trauma victims of such discrimination endure. But one poem, written by a group of Muslim women in Toronto, captures the heartbreaking reality. "Loves Me Not", a video poem created earlier this year during

a filmmaking workshop hosted by TIFF Special Delivery and advocacy group Outburst, tells the story of a young Muslim girl who wears the hijab. The poem begins with the girl, her hijab constructed with colourful petals. She holds a flower in her hand, but as she suffers from Islamophobia her flower begins to die. "Everywhere she looked, people would stare," the poem states. "They asked, 'Is that something your dad forced you to wear'?" According to Outburst's Facebook page, the poem was inspired by Islamophobia endured by the writers as they attended school in Toronto. The video continues to show the lasting impact of discrimination. "One day she broke down, the comments made her drown." Huffington Post

*** Web et jeux vidéo au service du terrorisme**

Le 10 novembre dernier, soit trois jours avant les attentats de Paris, le ministre de l'Intérieur belge Jan Jambon a laissé entendre que des terroristes utilisaient une console PS4 pour communiquer entre eux, une information qui a refait surface au cours des derniers jours. La réalité: aucune console PS4 n'a été retrouvée lors des nombreuses perquisitions effectuées en France et en Belgique. Ce qui ne veut pas dire que les jeux vidéo ne jouent pas un rôle dans les milieux terroristes. En 2013, grâce à des documents rendus publics par Edward Snowden, le Guardian et le New York Times ont révélé que la NSA et la CIA avaient déjà mené des opérations d'espionnage sur des consoles Xbox. Quelle utilisation les terroristes peuvent-ils faire des jeux vidéo? «Dans les jeux multijoueurs (pensons au jeu Call of Duty, par exemple), on retrouve des plateformes de "chat" afin que les joueurs puissent échanger entre eux, explique Hugo Loiseau, professeur à l'École de politique appliquée de l'Université de Sherbrooke. La Presse, A14

*** Hindu temple gratified by public support**

Young Muslims from the Toronto area would like to help pay for the damage caused at the local Hindu temple that was vandalized this week, but a temple board member said insurance covered the costs and the windows have been repaired. So the group known as Dawahnet, which means "spreading knowledge" in Arabic, will donate $2,299 that was collected in 24 hours on a gofundme website to the temple. Temple board member Vijay Solanki said the temple was overwhelmed with public support with many offering to help with the damage costs. "We gratuitously thanked them for the offer, but it is not appropriate to raise thousands of dollars for something that didn't cost us," he said. The gofundme page was set to raise $10,000 for the Kitchener temple by Dec. 1, but organizer Arshia Lakhani of Mississauga said they closed the site after speaking to the temple (...) Swami Chaitanya Jyoti and two other women were in the building and were frightened by the noise at the back of the building shortly after 11 p.m. No one was hurt in the incident. Hours before the vandals struck, Jyoti was at the Kitchener vigil honouring those who lost their lives in the Paris terrorist attacks. Record, B2

*** Extend vigilance to everyday threats**

An opinion piece states "In the wake of the attacks in Paris, there has been no shortage of security experts in the media talking about how to best keep safe. RCMP Assistant Commissioner Roger Brown, for example, articulated what everyone intuitively knows - there's no real science to spotting a terrorist plot. The best you can hope for is your gut tells you something is wrong. "When you do find yourself in a position where you see or do become aware of something that's not right, the next logical step is to report it to the proper authorities," Mr. Brown said. To his credit, the assistant commissioner hasn't fanned the flames or paranoia. He's done a good job of explaining the scope of the threat in Canada, not exaggerating it. David Charters of the Gregg Centre for the Study of War and Society at the University of New Brunswick has a similar message, calling an attack "a possibility but a relatively remote possibility." "The message 'If you see something, say something' is not a bad idea," Mr. Charters says. This is sound advice. It's true New Brunswick hasn't been the target of a terrorist attack, which isn't to say it's been a terror-free province. Justin Bourque's rampage in Moncton remains fresh in New Brunswickers' memories. And who can forget the seven months Allan Legere was on the loose in 1989. While the threat of a terrorist attack in Fredericton is remote, it's no excuse to be complacent. It's the reason schools practice lockdown drills. It's the reason passing through security at airports has become a much more intimate experience thanks to body scans and random searches." Daily Gleaner, A8

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Douanes à Bagotville: Lebel offre sa collaboration
Au cours d'un entretien avec le journaliste du Quotidien, le député conservateur de Lac-Saint-Jean affirme que le gouvernement Harper était prêt à annoncer, il y a quelques mois, un projet-pilote à travers le Canada, mais que la défaite électorale du 19 octobre avait modifié les plans. Depuis plusieurs années, les compagnies aériennes et les passagers qui se rendent en vacances dans le Sud réclament un service de douanes à l'aéroport de Bagotville. Il faut savoir que le service existe pour les voyages d'affaires de 30 passagers et moins seulement. Présentement, lorsque l'avion quitte le Mexique, Cuba, le Panama ou la République dominicaine, le pilote doit obligatoirement faire un arrêt à Québec. Les touristes doivent débarquer et passer par les douanes. Chaque fois, l'arrêt dure au minimum une heure et oblige les compagnies d'aviation à défrayer des sommes d'argent pour avoir le droit de se poser, en plus des dépenses de carburant que cela implique. (...)Au cours des dernières années, Denis Lebel et des fonctionnaires du gouvernement ont tenté de trouver une solution qui ne serait pas coûteuse pour ce projet. Et l'ancien ministre y était parvenu. Chaque atterrissage à Québec entraîne des coûts assez importants pour les compagnies aériennes. Ils seraient de l'ordre d'environ 10 000$, que les voyageurs paient sur leur billet. «Ce que je propose, c'est que l'on prenne cette somme et qu'on l'investisse dans les équipes de douaniers. Ça ne coûterait rien de plus au gouvernement, mais ça éviterait une escale.» «L'équipe volante des douaniers pourrait être formée des douaniers actuels de l'aéroport et on pourrait ajouter des militaires et des policiers à la retraite pour donner un coup de main. Au départ, ce serait un projet temporaire, soit pour la durée des vols offerts vers les destinations du Sud», analyse Denis Lebel. La Presse

L'ABC des achats de Noël en ligne
plusieurs consommateurs n'aiment pas faire la tournée des centres commerciaux pour faire leurs emplettes des fêtes. de nos jours, il est possible d'éviter cette épreuve annuelle en commandant ses cadeaux en ligne. Selon un récent sondage du Conseil québécois du commerce de détail (CQCD), plus du quart des Québécois (26 %) prévoit acheter un ou des cadeaux sur inter-net cette année. Année après année, ce geste devient toujours plus populaire. En 2010, seulement 11 % des Québécois prévoyaient acheter en ligne pour la période des Fêtes. (...)En théorie, en achetant sur un site américain, vous épargnerez la taxe de vente, car vous êtes résident d'un autre pays. Cela dit, bon nombre d'États américains n'ont tout simplement pas de taxe de vente. L'économie atteint près de 15 %, mais elle prive le Québec de revenus. Par contre, à la frontière, votre paquet pourrait être vérifié par l'Agence des services frontaliers du Canada, qui procède de façon aléatoire. Le cas échéant, on vous facturera des frais de dédouanement et des taxes canadiennes. Ces frais augmenteront le coût de votre achat. Journal de Québec, 42; * Journal de Montréal, 36

U.S. border airports seeing drop in Canadian travelers
The shuffle off to Buffalo to catch a cheap flight on a U.S. airline is losing its shine, thanks to a lower loonie. "We have seen an impact, but it's difficult to quantify the exact number," said Pascal Cohen, senior manager of marketing at the Buffalo Niagara International Airport. That's because no data is collected on citizenship, when passengers arrive to catch their flight. However, airport officials do conduct licence plate surveys at the parking lot at the Buffalo airport. Previously, when the Canadian dollar was at par with the U.S. dollar, as many as 40 per cent of vehicles were Ontario plates. These days, the airport estimates it is about 15 to 20 per cent fewer Ontario plates. Cohen says overall passenger volume at the Buffalo airport is up 1.9 per cent, year over year, which could be attributed to an improving U.S. economy. It's unclear whether Canadian airports will enjoy a bump in traffic as travellers choose to fly from home airports. Pearson airport says passenger traffic on transborder routes are up this year, but can't attribute that to a shift in travel patterns. Toronto Star, S11

*** U.S. to have tariffs against Cape Breton paper**
A series of costly duties will be levied against Canadian mills, including one in Point Tupper, that produce glossy paper following a vote Wednesday affirming the trade action by the U.S. International Trade Commission. The trade body says the vote was part of the final phase of a countervailing duty investigation into Canadian imports of supercalendered paper, which is mainly used for magazines, catalogues, corporate brochures and advertising inserts... Canada's international trade minister Chrystia

Freeland, issued a statement saying an appeal under the North American Free Trade Agreement will determine if the countervailing duties are being applied in accordance with the laws of the United States. Canadian Press (Cape Breton Post. A1, A4); Chronicle Herald, A1

*** SNAPSHOT: Children in immigration detention**
The location of CBSA's three immigration detention centres. CROSSINGS. Chronicling the global refugee and migrant experience 65 Number of days spent in a Canada Border Services Agency immigration holding centre (as of Nov. 13) by one of the two children currently waiting to hear the results of a refugee claim. The other has been there for 18 days. An agency spokesperson said that both children's parents prefer they stay in the centre with their families, rather than be relocated by child-protection services. "If you are a Canadian citizen and you're born in immigration detention or you're a Canadian citizen but your parents are undocumented, get arrested and placed in detention, the parents have a choice to give their children over to Children's Aid Society custody and never see them again or bring them in with them in prison. Adults make the difficult decision to bring their kids into prison ... What does a two-year-old do? Globe and Mail, L4

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Blackmailers target clients of Ashley Madison - Complaints to FTC claim online extortionists active in wake of site's hacking**
Victims of the Ashley Madison hack say they are being blackmailed months after millions of customers had their information leaked online. Complaints filed with the U.S. Federal Trade Commission detail how customers continue to feel the aftermath of the July attack on the Toronto-based adultery website. "A recent hack from the company exposed numerous amounts of private information from me. Now I am being harassed by others who are maliciously using the contents of that information," wrote one person. The hackers, who are still at large, leaked the information online, causing shock waves across the world as millions of alleged Ashley Madison customers had their dirty laundry aired. Toronto Police are still investigating the cyber attack, which they previously linked to online hate crimes, online scams and two unconfirmed reports of suicide. Toronto Star, S12

*** More offers too good to be true - Fraudsters finding new ways to victimize computer users**
An opinion piece states “Raise your hand if this has happened to you: A telephone call from Microsoft (or Windows) telling you your computer needs immediate attention. An email from your bank notifying you that your bank account has been compromised and you need to reset your password. Or, you are visiting a website, to get a recipe or read some news, and you get a screen message that your computer is running slowly so ‘click here’ to repair the problem. Keep your hand raised if you are a senior. Well then, join the club. And it's a growing club because fraudsters can easily get your phone or email address and with mass calls and/or mailings are sure to grab more and more unsuspecting customers. Locating the scammers is almost impossible; many are out of country and most use disposable cellphones that are difficult to trace. Here's a taste of how it all goes down. An elderly friend, let's call him Blake (whom I had previously helped with computer issues) called me to say that Microsoft had phoned him and he had allowed the caller remote access to his computer. The "technician" immediately claimed to find mountains of viruses and offered to clean his computer - for a price. What credit card would he like to use? Blake, rightfully reluctant to give out his card number, hesitated. The caller pressed him further, this time to go to Western Union and send cash. When Blake once again refused, the caller informed him that unless he paid $179 his computer would become inoperable. Blake hung up. When he called me I congratulated him for not responding to an obvious scam, but here's the thing: the scammer had reset his user password and Blake could not get into his computer. Not an easy fix. Other similar examples include opening your computer only to find a detailed welcome screen seemingly from the FBI/RCMP warning you to pay a fine for illegal downloads or else your computer will remain in lockdown. This kind of malware is more easily removed, but how many people - especially seniors - are intimidated and fall for these and similar schemes?” Hamilton Spectator, A15

LAW ENFORCEMENT / APPLICATION DE LA LOI

A night on the town

At 9:50 p.m. Nov. 4, two police trucks responded to a call about a woman threatening to commit suicide. The call came from a family member and was relayed to the detachment over the phone. "The whole town doesn't need to hear that over the scanner," said Const. Yannick Gagnon as he followed a vehicle to where the woman lives. In the end, police decided the woman wasn't an imminent threat to herself and took her to a relative's home. "Just to be on the safe side, we're not going to let her be alone," said Gagnon. "If she didn't have family to go to, we would bring her to the hospital to get her cleared, and if she was imminently suicidal she would be taken to the hospital right away. Better safe than sorry." He said this way if there are more concerns over the course of the night, at least the officers know the situation. Gagnon arrived at the RCMP detachment shortly before 7 p.m. on Nov. 4 to get ready for night shift. It was "superconstable" night, something that happens once every two weeks or so when shifts overlap and nearly all officers work on a given day. It means they can get caught up on paperwork and share important events with the next crew to come on. Gagnon's regular partner, Const. Mackenzie McGuffin, spent the shift preparing for a case going to court the next morning. "It's what ties everything together," he said. "You can respond to a call, but if you don't follow up with the paperwork, there's no chance those charges will go through." Gagnon said he was a few weeks into Depot, where all RCMP members go to be trained, before he realized the job was 90 per cent pencil-pushing and 10 per cent "fun stuff." "I wanted to quit right there," he joked. Inuvik Drum

Man charged over concealed cleaver

A Toronto man who allegedly tried to carry a meat cleaver onto Parliament Hill is to undergo a psychiatric assessment. A lawyer for Yasin Ali asked for the assessment in court Wednesday after the 56-year-old appeared by video from the courthouse cellblock on a charge of carrying a concealed weapon. He will remain in jail until his next appearance on Friday, when he is to appear in court in person. The man had a ticket to visit the Peace Tower, and was in line to go through the visitors' entrance at about 11:30 a.m. on Tuesday when a House of Commons security guard asked him to open his coat. The guard found the man was concealing a large cleaver with an approximately 15-cm-long blade. The man never made it as far as the metal detectors. RCMP Commissioner Bob Paulson told reporters that Ali is known to authorities, but "not in the sort of counter-terrorism context." In fact, Paulson does not believe that the man's actions were politically motivated or an act of terror. Postmedia Network (Windsor Star, N5, Toronto Sun, Ottawa Citizen); ; *La Presse; * Canadian Press, (Times Colonist, A8)

*** La GRC pourrait avoir agi illégalement, dit la juge**

Une juge de la Cour suprême de la Colombie-Britannique a affirmé que la preuve tendait à montrer que la Gendarmerie royale du Canada (GRC) avait agi illégalement durant une opération d'infiltration antiterrorisme de haut profil, et a ordonné à la police de remettre des documents juridiques confidentiels. La juge Catherine Bruce n'a pas encore déterminé si la GRC avait piégé John Nuttall et Amanda Korody pour qu'ils organisent un complot visant à faire exploser le parlement de la Colombie-Britannique en 2013, mais elle a indiqué que les agents pourraient être coupables d'avoir facilité en connaissance de cause un acte terroriste durant leur opération d'infiltration. «Il existe un lien suffisamment étroit entre les actes illégaux commis par la GRC et les faits reprochés aux accusés pour soutenir une allégation d'abus de procédures», a-t-elle écrit. Mme Bruce a ordonné à la police de dévoiler des avis juridiques confidentiels obtenus relativement à l'opération secrète pendant laquelle des agents se faisaient passer pour des combattants djihadistes. «Ces documents fournissent un aperçu fondamental de l'état d'esprit de tous les agents mêlés à l'intervention», a-t-elle mentionné. La confidentialité de la correspondance avec un avocat est habituellement protégée, mais la magistrate a indiqué que les agents de la GRC avaient renoncé à ce droit en dévoilant délibérément une portion de l'information en cour. La juge estime qu'il est pertinent de savoir si les policiers ont suivi les conseils de l'avocat, car cela pourrait montrer une mauvaise foi de leur part. John Nuttall et Amanda Korody ont été reconnus coupables plus tôt cette année sous des accusations de terrorisme pour avoir planifié de perpétrer un attentat sur le site de l'Assemblée législative de la Colombie-Britannique lors des célébrations de la Fête du Canada de 2013, mais leurs avocats ont argué que la GRC les avait piégés et que le complot n'aurait jamais été organisé sans l'aide de la police. La Presse Canadienne (Le Nouvelliste, 14, La Voix de l'Est); CBC News;

Postmedia News (Province, A8, Times Colonist); Postmedia Network (Vancouver Sun, A2, Calgary Sun, Winnipeg Sun, Province, Globe and Mail, S3)

*** Les agences se font rassurantes**
Les grands patrons des agences canadiennes de sécurité et du renseignement ont cherché à se faire rassurants, hier : ils ont bel et bien la capacité de faire les vérifications qui s'imposent afin de protéger les Canadiens contre les menaces potentielles posées par l'accueil rapide de 25 000 réfugiés d'ici la fin de l'année. « Je veux que les Canadiens sachent qu'en tant que directeur du SCRS, je suis sûr que les mesures en vigueur sont robustes et que j'ai pleinement confiance qu'elles seront appropriées », a déclaré Michel Coulombe, directeur du Service canadien du renseignement de sécurité (SCRS). De plus en plus de gens au Canada expriment leur inquiétude devant cet accueil jugé trop rapide et un nombre trop élevé de réfugiés d'ici six semaines. Les chefs du SCRS, de la Gendarmerie royale du Canada (GRC), de l'Agence des services frontaliers du Canada (ASFC) et le ministre fédéral de la Sécurité publique ont livré une rare conférence de presse conjointe pour répondre à ces préoccupations. Ils ont fourni quelques détails sur la situation sécuritaire au pays dans la foulée des attentats de Paris et sur leurs démarches pour assurer la sécurité tout en respectant la promesse électorale du Parti libéral. La Presse Canadienne (Voix de l'Est, La Presse,); La Presse

*** Takes two to tango in Duffy trial**
The Ol' Duff will be strutting today, his mind firmly convinced that, besides his courtroomdrama playing a key role in bringing down the spiteful Harper government, he will soon be walking out of court totally vindicated. This has been Duffy's firm belief from the outset, and he has sent chastising emails to many in the media who presupposed his guilt. (…)In fact, the RCMP exonerated Wright of any wrongdoing and, after he testified about cutting the cheque to Duffy, he skedaddled back to England and his job as managing director in the London office of Onex Corp. There is no jury here. It is trial by judge alone, so it comes down to Ontario Court Judge Charles Vaillancourt to decide if there was a bribe and, if so, then solve the riddle of who bribed who. But armchair jurors are already taking bets on acquittal. The most entertaining portion of the trial, of course, has been defence attorney Donald Bayne's tarring of the Prime Minister's Office, even though who-knew-what and/or who did or did not tell the prime minister about Wright's cheque has nothing to do with Duffy's guilt or innocence. Postmedia Network (Calgary Sun, A15)

*** Winnipegger warns of immigration phone scam - Callers demand payment**
More than 45 years after Winnipeg resident Monina Relano moved to Canada from the Philippines, she got a phone call Tuesday saying there was a problem with her immigration paperwork."I was scared," said Relano. Though she's been a Canadian citizen since 1975, she was taken aback by the authoritative voice on the phone. The man told her she didn't fill out a required immigration form and now had to pay an out-of-court settlement of $2,490 or the RCMP would be at her door.Relano figured out it was an immigration phone scam but worries more recent newcomers without permanent status in Canada might be conned. She wants to warn them before they get the call and end up swindled. Winnipeg Free Press, B6

*** Diverse workers sought by RCMP**
The RCMP is seeking some good men and women to diversify their ranks. With a visible minority presence of 9.7%, the force is seeking to increase that to 20% to better represent the country it serves, say Mounties. The force is holding a Calgary career presentation Nov. 25 at the Duncan Building, 7575 8 St. N.E. at 6 p.m. On offer are 150 different types of policing opportunities. Those applying for a position with the RCMP must be a Canadian citizen, 19 years of age and be fluent in either or both English and French. They must also possess a valid driver's licence and have a high school diploma or an equivalent, be able to meet fitness requirements and be willing to re-locate anywhere in Canada. Postmedia Network (Calgary Sun, A10)

*** New Kids on the cellblock**
A Red Deer crime syndicate has taken a big hit. Police have arrested and charged three alleged members of Bobby and the Kids, a group that deals mostly in the drug trade. One of them is believed to be "Bobby," the leader of the group. The organization has dealings throughout Central Alberta including Sylvan Lake, Blackfalds and Innisfail and has been operating for "some time," say police. The arrests are

believed to be the first made involving the organization. "We have definitely disrupted this group and eliminated the harm they are doing in the community," said Red Deer RCMP Sgt. Eric McKenzie. Police did not give any indication of the size of the group. Last Friday, the Priority Crimes Task Force seized 55 ounces of cocaine, nine ounces of methamphetamine, marijuana, a stolen pistol, drug paraphernalia and $30,600 in cash after executing search warrants at Timothy Drive and Leonard Crescent in Red Deer and Harvest Close in Penhold. Three men between the ages of 22 and 27 were arrested without incident. Postmedia Network (Red Deer Advocate, A1, A2)

* **Quebec police conduct major raids linked to drugs, organized crime**
Quebec provincial police say they are conducting major raids this morning linked to drug trafficking and organized crime in the Montreal area. Sûreté du Québec spokesperson Audrey-Anne Bilodeau says roughly 200 police officers are taking part in the operation. The raids target "different strains of organized crime in link with the control of the territory, the supply and the distribution of drugs in Montreal," Bilodeau said. In all, Bilodeau says they expect to arrest about 40 people this morning. Bilodeau would not give further details on the suspects or what kind of drugs may be involved. She says members of the SQ, Montreal police and the RCMP are collaborating. A news conference is planned for later this morning to give more details on the operation. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Young Shafia seeks appeal
Hamed Shafia, the Montreal man convicted, along with his father and mother, of murdering four family members in what the trial judge called a "heinous" and "despicable" mass honour killing, is poised to present a new claim to Ontario's top court regarding the appeal of his conviction. The youngest Shafia killer maintains that he was not 18 years old at the time of the murders on June 30, 2009, and he has documents newly obtained from Afghanistan, his birthplace, that purport to prove it. Shafia was tried and sentenced as an adult, based on documents that indicated he was born in Kabul on Dec. 30, 1990. Those records established that he was 18-and-ahalf years old at the time of the killings, and therefore subject to adult criminal law. After a 45-day trial, he was convicted of four counts of first-degree murder and sentenced to the mandatory term of 25 years in prison before parole eligibility. If convicted of murder in youth court and sentenced as a youth, he would be eligible for parole much sooner, perhaps in as few as five years, calculated from the date of his arrest in July, 2009, according to Nicholas Bala, a Queen's University law professor and expert on youth criminal law. The legal scholar said it might be the first case in Canada in which a killer sought to prove he was underage after his adult conviction. Postmedia Network (Kingston Whig-Standard, A1, Montreal Gazette, Toronto Sun, Calgary Sun, National Post, Ottawa Citizen)

McDonald's killer loses appeal
The man believed to be the mastermind behind the most notorious killings in Cape Breton history has lost his appeal of the decision to deny him day parole. Derek Anthony Wood was sentenced to life in prison with no eligibility for parole for 25 years after being convicted of a number of charges, including two counts of first-degree murder in the 1992 Sydney River McDonald's killings when he, Darren Muise and Freeman MacNeil robbed the restaurant and killed three workers. A fourth person was left permanently disabled. Wood had filed an appeal with the Parole Board of Canada after it denied his day parole application earlier this year. He had been deemed a medium-to-high risk to reoffend in a violent manner, according to a psychological assessment. Cape Breton Post, A1

'She's never coming back'
Eighteen years later, the daughters of murdered prison guard Diane Lavigne say they're still struggling to cope. Testifying Wednesday at a hearing where former Hells Angels underling Stéphane Gagné is seeking an earlier parole eligibility on the life sentence he is serving for taking part in the murders of two prison guards in 1997, 40-year-old Isabelle Daoust said she still remembers how sunny it was on the Friday morning her uncle knocked on her apartment door and told her "my sympathies, Isabelle. Your mother's been assassinated." Gagné killed Lavigne in June 1997, shooting her from the back of a motorcycle as she drove home from her job at the Montreal Detention Centre. He later became a

collaborating witness against biker boss Maurice (Mom) Boucher and helped convict him. Boucher is now serving a life sentence for the murders of Lavigne and Pierre Rondeau and the attempted murder of Robert Corriveau, all of them guards at provincial detention centres targeted in an effort to intimidate the Quebec justice system. Daoust called the sequence of events in 1997 "surreal. Things like that didn't happen in Quebec. It's like a film that I was watching from above ... too big and unexpected to ever see coming." Montreal Gazette, A3, Le Devoir, Journal de Québec (Journal de Montréal); * La Presse

* **James Leroy Leopold, convicted of killing fiancée, has parole revoked after 5 months**
A Nova Scotia man who killed his fiancée has had his day parole revoked after just five months. James Leroy Leopold was convicted of manslaughter and sentenced to six years in prison after the death of Laura Lee Robertson in 2012. During his trial, the court heard Leopold told police he and Robertson got into a fight and that she died after he hit her in the throat. Following a hearing in May of 2015, Leopold was granted six months of day parole by the Parole Board of Canada. In their decision, the board noted that Leopold is at a high risk of violence towards a partner. Global News (2015-11-18)

* **Parole extended for killer ex-Mountie**
A former Mountie convicted of first-degree murder who has been running an antiques store in Prince George must spend at least a further six months on day parole, according to a recent Parole Board of Canada decision. Patrick Michael Kelly, 65, was convicted in 1983 for throwing his wife off the 17th-floor balcony of their Toronto apartment. Kelly was originally granted day parole in 2003. Since then, his parole has been revoked several times for failing to disclose financial dealings or relationships with women. The former undercover officer was granted full parole in 2010 and opened his store in Prince George. But the board reversed his release in August 2012 after he failed to report two relationships with women. Prince George Citizen (2015-11-18)

Traque contre un couple de voleurs
Un enquêteur qui a traqué pendant des mois un couple de voleurs à la Bonnie et Clyde, qui ont dérobé pour plus de 1 M$ en cambriolant des maisons cossues partout au Québec, sera récompensé aujourd'hui pour son travail acharné. «Je suis tellement content d'avoir résolu ces dossiers. Sinon, ils auraient continué à commettre d'autres crimes. Certaines victimes ont été démolies en se faisant voler des objets de valeur importants à leurs yeux», a dit le sergent-détective de la Sûreté du Québec, Gordon Hunter. (...)Le sergent Hunter sera récompensé aujourd'hui dans le cadre du Gala des Prix policiers du Québec pour son implication dans cette enquête. (...)Jimmy Simard-Patry et Elyanne Miller ont respectivement écopé de cinq ans et demi et de deux ans de prison en juin. Un complice du couple n'a pas encore subi son procès. Journal de Montréal (Journal de Québec)

Province's plan a 'beacon' for justice: minister - Unveils details of restorative strategy
A five-year plan to make restorative justice a mainstream method of dealing with crime in Manitoba will include a community court in the North End, an expansion of current mental-health and drug-court diversion programs and a focus on victims, the provincial government announced Wednesday. Restorative justice is "local, swift, common-sense, tough justice," Justice Minister Gord Mackintosh told a room of restorative-justice advocates at the legislature building Wednesday, proclaiming legislation he hopes will establish Manitoba as a "beacon in North America for restorative justice." The term restorative justice refers to an individualized approach for offenders (who are often youth or first-time offenders) to take responsibility for their actions, usually by reconciling with victims, performing community service and working toward their rehabilitation. It's used mainly to handle less serious crimes and non-indictable offences, but the justice minister said the province is looking at "tacking on" restorative-justice techniques alongside criminal-court sentencing. The province plans to fulfil the new strategy, announced Wednesday to coincide with the implementation of the Manitoba Restorative Justice Act, by increasing its current $1.8-million annual spending on restorative justice, starting with an additional $320,000 next year. Winnipeg Free Press, B5, Winnipeg Sun; * Radio-Canada

* **Credit-card fraud extends sentence**
Credit-card fraud has added to the length of a Fredericton man's prison sentence. Ashley James Charlton, 35, was brought to provincial court in custody recently on a charge of using a stolen credit card between Aug. 5 to 6. The former Canada Street resident pleaded guilty to the offence during an

appearance last month. Judge Mary Jane Richards sentenced Charlton to six months' incarceration and ordered that he pay a $100 victim-fine surcharge. He was also instructed by the court to pay restitution in the order of $3,279. Charlton told court during an earlier appearance that he's serving time in the Springhill Institution in Nova Scotia for breaking into two food vendor kiosks at the Northside Market and stealing hundreds of dollars worth of meat on Aug. 19. Daily Gleaner, A4

*** World's indigenous leaders look to adopt prison practices at Waikeria**
Indigenous leaders from around the world hope to adopt practices from a Waikato prison unit that rehabilitated violent offenders, drug abusers and sex offenders. Daniel Levi Martin is a tribal leader of Tla-o-qui-aht First Nations people, who live on reserves along the Pacific Rim National Park, Canada. "I hope that I can learn the different ways of doing things here [at the prison], techniques I can take back home to my people," he said. Martin was in Hamilton for the week-long indigenous people's conference, Healing Our Spirit Worldwide - The Seventh Gathering, hosted by Te Rau Matatini. "I'm an elder and an advisor to treatment centres. I hope to learn something here." Waikeria Prison's Karaka Unit is an 80-bed therapeutic community for medium and high risk offenders. Since 2010, 245 prisoners have completed treatment programmes at Waikeria Prison's Karaka Unit. Since 2010, 245 prisoners have completed the programme, with 55 per cent of those identifying as Maori. There are three programmes within the unit; the Dependency Treatment Unit (DTU) for those with substance abuse, the Special Treatment Unit Rehabilitation Programme (STURP) for high-risk offenders, and the Adult Sex Offender Treatment Programme. Stuff.co.nz

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Police must communicate to track missing women
Effective communication between police agencies is essential when it comes to investigating vulnerable women who have disappeared, says the man who oversaw British Columbia's Missing Women Commission of Inquiry. Wally Oppal, a former B.C. Court of Appeal justice and provincial attorney general, said there was little communications between the RCMP and the Vancouver police in the 1990s when multiple women went missing in that province. "When vulnerable women go missing police have to get involved and that is what they didn't do in the 90s," Oppal said in an interview. "The result is you have well over 100 women who were murdered." Exchanging information in such cases has to take place, Oppal said. What happened in B.C. was that women were being picked up in the eastside of downtown Vancouver but were being murdered in Port Coquitlam, about 35-40 minutes away, he said. "There were very little communication between the RCMP and the Vancouver police," Oppal said. "We were very critical of the policing that took place and that there was no real liaison between the sex trade workers and the police." Oppal will be at St. Thomas University Thursday night presenting a public lecture on the inquiry. Appointed commissioner in 2010, Oppal held close to 100 days of public hearings and forums in Aboriginal communities in northern B.C. in which the many victims and survivors of the Robert Pickton tragedies testified. The inquiry was called to examine why Vancouver police and the RCMP failed to catch Pickton before he was arrested in February 2002. Daily Gleaner, A3 (Times & Transcript)

*** Does Canada still need a Status of Women minister?**
We've come a long way in Canada on gender equality - far enough for Prime Minister Justin Trudeau to mandate gender parity in his first cabinet. So do we still need a Status of Women ministry? "Yes, we certainly do," said noted feminist and journalist Michele Landsberg, The new mandate letter for Status of Women Minister Patty Hajdu tasks her with trying to eliminate economic and political inequalities that affect women, tackling violence against women and moving forward with a planned inquiry into murdered and missing aboriginal women. Under the Harper government, Landsberg said, women's rights were set back by budget cuts for research and advocacy in the ministry. This loss of funding, she said, meant government couldn't get a complete picture of what was happening in the lives of women. iPolitics, Toronto Star

*** Saskatoon men asked to combat violence against women**
Members of the University of Saskatchewan Students' Union (USSU) have called for an end to violence against indigenous women and children, hoping men will lead the movement for change. "Traditionally as men, our role was to stand as protectors and also to support our women," said Regan Ratt-Misponas, indigenous student representative with the USSU. "Our women were very much regarded as the leaders of First Nations communities and First Nations reserves." On Wednesday, students were introduced to the "Moose Hide Campaign," a grassroots, non-profit that encourages aboriginal and non-aboriginal men to wear pins made of the material. Global News (2015-11-18)

*** Delete Day aims to combat social media cyberbullying**
Countless people can see what you're doing, and a lot of them are mean. That was the message Windsor police and Catholic Central High School tried to drive home Wednesday during Delete Day, an event they hosted to combat cyberbullying. Students spent time with their vice-principal and a police officer to learn how to delete bullying posts from their social media profiles, along with anything they might regret posting themselves. "There are adults and other people whose sole purpose is to troll the Internet and find young people using social media to see if they can acquire their information," said vice-principal Laura Beltran. "When that happens, it can ruin lives and it's very difficult to put lives back together once information is out there. Especially for young people, their reputation, their self-esteem, their self-concept is still growing and maturing and it can be devastating for them at a very early age." Dozens of students showed up for Delete Day, one of a number of events being held as part of Bullying Awareness Week. Grade 12 student Manal Muzamil said it was a good chance to "refresh" social media accounts, delete bad things people have posted and block those responsible for the negativity. Windsor Star, A3

*** Cyberbulling starts young**
Cyberbullying can affect children far younger than widely believed, experts warn. While it starts to become prevalent in students around the Grade 7 level, children can gain access to this world much sooner, said Brad Burns, principal of Highlands School in Edmonton. "I know of students that are in kindergarten who are coming to school with cellphones, because they are a very useful resource for safety and communication at homes," said Burns. "As technology is more prevalent in our lives and more integrated, that age of being in that world keeps moving down to younger and younger children." On Wednesday, as part of Bullying Awareness Week, Burns was one of five panellists speaking at an Alberta government-sponsored webcast on cyberbullying. He said it's up to the parents to inform and discuss with their children about the importance in becoming a "responsible digital citizen." Calgary Sun, A21 (Edmonton Sun)

*** There's value in carding**
An opinion piece states, "In September 2011, a 15-year-old girl was sexually assaulted in a Brampton park. Officers attached to Peel Regional Police's special victims unit had a description, but the perpetrator was long gone. Detectives checked to see whether there had been any PRP17s (street check reports) filed from anywhere nearby. Bingo. Up came a street check on a 37-year-old man - including name, date of birth and description - who was engaged by police at the park months earlier. They had a suspect and a reason for a search warrant which - when executed - led to the arrest of the man for possessing child pornography as well as the sexual assault on the girl. There's one example of the benefits of police community engagement that opponents feel is racial profiling. Under new rules being implemented next year by the provincial government, police will have to tell people encountered - such as the man engaged in the park - that there is no need for them to talk to officers and that they're free to go. It's absurd." Toronto Sun, A10

*** Fassbender saps amalgamation impetus**
It never was about forcing amalgamation on Greater Victoria, and Peter Fassbender knows it. B.C.'s community charter already bars the provincial government from imposing amalgamation on anyone. No, all that people are asking for is a study into whether amalgamation makes sense. (...)Of course, while Victoria and Esquimalt might see this disparity as an excellent reason to share the cost of policing more equitably, the other municipalities see it as a totally awesome reason to leave things as they are. Why would Langford, whose residents pay just $141 apiece for the RCMP, voluntarily eat a cost hike?

Both Victoria Mayor Lisa Helps and Esquimalt Mayor Barb Desjardins recognize this reality. Times Colonist, A3

*** 'Almost one an hour'**
When she refused to give him money to buy beer, one Edmonton man pushed his girlfriend to the ground, pulled her hair and punched her in the face. (...)"This is only a sample of the files received by the Edmonton Police Service this past weekend," Staff Sgt. Sean Armstrong, in charge of the domestic offender crime section, told a downtown crowd Wednesday. "There were 88 cases responded to by EPS members, and sadly this was a quiet week. I can guarantee you there are many more domestic violence occurrences in our city that were not reported to us." These revelations shocked those gathered for the the Alberta Council of Women's Shelters' (ACWS) 11th annual Breakfast with the Guys at the Chateau Lacombe on Wednesday. In 2014, Edmonton police were involved in nearly 8,000 domestic violence complaints. (...)According to government statistics, Alberta has the fifth highest rate of intimate partner violence reported to police and the second highest rate of self-reported intimate partner violence in Canada. Edmonton Sun, A7

*** First Nation contemplates ban on criminals on reserve**
Elders on the Little Pine First Nation are exploring the idea of banishing criminals from the reserve. The idea of kicking known offenders such as drug dealers and abusers offthe reserve was preposed at a recent community meeting aimed at dealing with crime on the First Nation, located north of North Battleford. "The criminal justice system is not working. Look at the statistics," said Jacob Pete, a band member who helped facilitate the meeting. "We have to take ownership of the problems and come up with local solutions." The idea of banishing criminals from a particular community is not unheard of. Saskatchewan's largest First Nation, Lac La Ronge Indian Band, has been banishing drug dealers and others for decades. First Nations like Mistawasis near Prince Albert and Fishing Lake have also banished people for crimes. StarPhoenix, A3 (Leader-Post)

*** Un quartier général de la mafia visé par un attentat**
Un incendie criminel allumé dans un bar de la rue Jean-Talon la nuit dernière pourrait constituer un nouveau chapitre d'une tension grandissante au sein de la mafia montréalaise. *La Presse* a en effet appris de sources de divers milieux que l'établissement visé, le café Empire, serait l'un des quartiers généraux de la Table de direction de la mafia qui dirige les rênes du crime organisé montréalais, en alliance avec d'autres groupes criminels, depuis la mort naturelle du parrain Vito Rizzuto, il y a près de deux ans. Selon nos sources, Vito Rizzuto aurait été vu souvent à cet endroit après sa libération d'un pénitencier américain et son retour à Montréal, en octobre 2012. La Presse (2015-11-18)

*** Front line workers get info on battling sexual exploitation**
If you don't think human trafficking is a concern within Norfolk County, think again. “Because we're rural, we're a very big source destination for sexual exploitation,” explained Christina Bodine, chair of the Sexual Assault Centre of Brant. Bodine and her colleagues played host to a human trafficking seminar for social service employees and concerned residents at the Norfolk Golf and County Club Wednesday. One of the main messages was human trafficking – at one level or another – certainly does take place in Norfolk, Brantford and Six Nations. The trouble is, not many get the message because young women are often being shuttled to places like Niagara Falls or Windsor. “You have to lay charges in the place that the crime happens, so they'll be laid in places like Niagara Falls and Windsor, but they're gals that are from Brant, Haldimand, Norfolk, Six Nations,” Bodine explained. “That's why those stats aren't showing up, but we're a big source area.” That's why gatherings like the one on Wednesday are held. Speakers addressed the warning signs of human trafficking, what its definition is and who is most vulnerable. “It is complicated, so we're just trying to give an overview so people are aware,” Bodine noted. “What we do know is over 90 per cent is domestic, so it's happening within Canada, it's happening within our borders.” While the day-long event was open to all, Bodine and her team targeted a specific group to take part. Simcoe Reformer (2015-11-18)

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

City pulling together for refugees
It was an unprecedented Edmonton conclave. Ninety representatives from more than a dozen social agencies and government departments met Wednesday at the Ramada on Kingsway to plan a joint mission. Their goal? To settle some 1,500 Syrian refugees in Edmonton before year's end. "We're still not sure of the exact number or the exact timing. And that's causing some anxiety for us," says Stephen Carattini, CEO of Catholic Social Services. His agency has the federal contract to settle refugees in Edmonton. "Normally, we settle 400 to 500 refugees a year. Now, we're going to be settling three or four times that many. It's not unfamiliar, what we're being asked to do. But this is happening very, very quickly." The meeting included representatives from the federal departments of Canadian Heritage and Immigration, Refugees and Citizenship. Representatives of the provincial departments of Alberta Jobs, Skills, and Labour, Alberta Health and Alberta Education were there, too. So were Edmonton's school boards, along with Capital Region Housing and Edmonton and Area Child and Family Services. And there was an eclectic and ecumenical range of other agencies, including the Islamic Family and Social Services Agency, the Edmonton Mennonite Centre for Newcomers, Edmonton Immigrant Services Association, ASSIST Community Services, Centre d'accueil et d'etablissement, Changing Together and the Indo-Canadian Women's Association. Postmedia News (Edmonton Journal, A1/Front)

Queens sponsorship effort edges ahead
A group of residents in Queens County has just squeaked past the halfway point in their goal of raising $20,000 to sponsor a family of Syrian refugees. The Queens Refugee Care Team hopes to sponsor a family of six, and has already raised almost $11,000. Chronicle Herald, A8

Premier confident about refugees
Nova Scotia's premier doesn't want to pre-judge whether Ottawa should pull back from a plan to bring 25,000 Syrian refugees into Canada by the end of the year. Stephen McNeil said that Ottawa is responsible for handling any security concerns that arise from its screening process of refugees and his province remained ready to proceed with welcoming newcomers once it's determined how that will happen. McNeil said he expected many of those concerns to be addressed in a federal-provincial meeting next week, in light of the recent terror attacks in Paris and Beirut. "Security coming into the country is the responsibility of the federal government," said McNeil. "So if it (the plan) continues to move forward we are ready to participate as part of the federation." Canadian Press (Cape Breton Post, A9)

Notley says Calgary, Edmonton among five Alberta cities likely to take refugees
Premier Rachel Notley says Calgary and Edmonton are expected to take in the bulk of Syrian refugees coming to Alberta, with the remainder spread out over three other cities - Medicine Hat, Lethbridge, and Red Deer. "We're working to ensure that we're able to provide a seamless and effective settlement process," Notley told reporters Wednesday. "There are five cities where refugees would most likely land. The vast majority of them will be in Calgary and Edmonton. "Obviously the mayors need to be fully on side with it, and I believe that they are and have it well in hand." Notley was flanked by Edmonton Mayor Don Iveson and Calgary's Naheed Nenshi at the legislature following a meeting to discuss a range of issues, including the refugee resettlement. The federal government has said it wants to resettle 25,000 Syrian refugees across Canada by the end of the year. Notley has said she expects Alberta will take between 2,500 and 3,000 of those fleeing the war-torn region. Postmedia News (Calgary Herald)

Goodwill beats bureaucracy
They've been offered an entire convent in Pointe-Claire to house the refugees, a CEGEP in Rosemont with classrooms and showers to use at least over the holidays, rooms and fridges, winter coats and dishes. While politicians wrangle over whether it's possible to bring in 25,000 Syrian refugees over the next six weeks, grassroots organizations and ordinary Quebecers are making it possible. "Since last week our phones and email accounts have been overloaded with offers from Quebec residents wanting to help Syrian refugees with clothes, furniture, appliances," said Paul Clarke, the executive director of Action Réfugiés Montréal. "As public consciousness has ramped up that Syrian refugees are coming, the generosity has been astounding." And the terrorist attacks in Paris did not stop the flow, Clarke added. He has had to ask people to stop bringing in winter coats and boots to the organization's downtown locale

- there was just no room for more. But while every bit helps, especially if Quebec does receive 5,700 refugees over the next 43 days, such a massive endeavour requires some coordination, between all the groups involved, and every level of government. The community groups tasked with helping refugees resettle in Montreal - there are 18 in Montreal alone that offer services in Arabic - have set up a central list of people who want to volunteer their time, housing and miscellaneous goods, including all those winter coats and boots: infoparrainage@tcri.qc.ca And cities, including the 13 in Quebec that could receive some of the refugees, are also mobilizing. Postmedia News (Montreal Gazette, A1/Front)

Valcartier se prépare à l'arrivée de réfugiés
La base militaire de Valcartier est sur un pied d'alerte et se prépare à accueillir des centaines, voire des milliers de réfugiés syriens d'ici la fin de l'année. Le Canada avait déjà évoqué la possibilité que les bases militaires servent de terre d'accueil temporaire aux réfugiés, et l'hypothèse se confirme selon de nombreuses sources. Les 500 premiers réfugiés syriens débarqueraient dans la région de Québec à partir du 1er décembre - une date évoquée par plusieurs - et seraient logés dans diverses installations de la base militaire, notamment au Camp des Cadets. L'Armée vient de lancer un appel d'offres pour l'«hivernisation » d'une dizaine de baraquements. Les travaux, qui prévoient l'installation de chauffage, sont évalués à 1,5 M$ et seront réalisés «dans un très court délai, d'ici le 30 décembre», peut-on lire dans les documents sur le portail MERX. Journal de Québec, 3 (Journal de Montréal, 7); Le Soleil, 5/Front

Les villes veulent être mieux informées
Les maires des 13 villes québécoises qui accueilleront les réfugiés syriens attendus d'ici la fin de 2015 demandent à être mieux informés des plans d'Ottawa et de Québec, les élus ignorant encore combien d'entre eux chaque ville recevra. Une conférence téléphonique d'une quarantaine de minutes a réuni hier midi ces maires afin de faire le point sur le dossier. «Ce qui me frappe, c'est la volonté des villes à accueillir les réfugiés. Chacune a déjà pris des initiatives pour réunir les groupes sur son territoire. Mais il manque deux morceaux du casse-tête: Québec et Ottawa. Les villes sont déjà à pied d'oeuvre, mais elles n'ont pas toute l'information», a indiqué la mairesse de Longueuil, Caroline St-Hilaire. L'Union des municipalités du Québec a mis en place un comité auquel on espère voir Ottawa et Québec se joindre pour coordonner l'arrivée des réfugiés. «Il faut qu'on s'assoie, s'il le faut quotidiennement, pour éviter que chaque maire appelle à gauche et à droite pour avoir de l'information. On veut éviter qu'il y ait des ratés. On a connu de beaux succès d'accueil de réfugiés et il ne faudrait pas manquer le bateau», a ajouté Mme St-Hilaire. La Presse, A10

Rookie MP Tassi says government committed to accommodating refugees
Filomena Tassi is assuring residents that Canada remains committed to accommodating 25,000 Syrian refugees by Jan. 1. "At the same time, we're going to exercise the highest level of vetting and security," said the rookie MP, who represents the riding of Hamilton West-Ancaster-Dundas and will be sworn in as part of Prime Minister Justin Trudeau's government on Dec. 2. Opposition to the Liberal campaign promise has already grown in reaction to reports that at least one of a number of ISIL terrorists who participated in the Paris attacks in last weekend entered France with other Syrian refugees. But with a majority government, Trudeau and his team appear to be moving ahead on the promise. "We are staying on course," Tassi said. Tassi has been to Ottawa and completed her training for first-time members of Parliament. She is now focused on setting up shop in her widespread constituency, searching for an office from which to serve residents from Ancaster to Westdale and the west Mountain. Tassi said there was nothing to officially announce as far as any committees she will be part of, or other specific roles within the government. Hamilton Spectator, A5

Les initiatives citoyennes se multiplient
Le téléphone de la Table de concertation des organismes au service des personnes réfugiées ou immigrantes n'arrête pas de sonner depuis des jours. «Les gens offrent des logements, des vêtements. Des professeurs à la retraite proposent de l'aide aux devoirs, des Syriens veulent faire de la traduction. Tout le monde veut contribuer et faire partie de ce moment historique», dit Sylvain Thibault. Parmi les offres de dons se trouvent aussi des messages de quelques personnes qui ont déjà pris les choses bien en main. Les initiatives citoyennes se multiplient. C'est le cas de Yasmine Abdelfadel qui a décidé lundi soir qu'elle lançait un projet de paniers d'accueil contenant notamment des paquets de couches et des

fournitures scolaires. Une autre dame est en train d'amasser entre 600 et 900 toutous «pour que chaque enfant qui arrive au Québec en ait un.» Pour l'instant, les gens qui veulent faire des dons spécifiquement destinés aux réfugiés syriens peuvent le faire par l'entremise des initiatives citoyennes qui apparaissent sur les réseaux sociaux ou en communiquant avec des groupes comme la Table de concertation des organismes au service des personnes réfugiées ou immigrantes. Toutefois, la plupart des organismes communautaires sont en attente. La Croix-Rouge canadienne a ouvert, il y a quelques mois, un fonds destiné aux réfugiés syriens, mais elle attend des annonces gouvernementales pour lancer des initiatives locales qui serviront les réfugiés à leur arrivée au Canada et au Québec. Carl Boisvert, porte-parole de la Croix-Rouge pour le Québec, conseille aux personnes qui veulent contribuer à l'accueil de réfugiés ici d'attendre que les campagnes spécifiques soient mises en place. La Presse, A10

On n'a pas le temps

Alors là, un gros bravo. Quand on a retrouvé le petit Alan mort noyé sur une grève en Turquie, vous trouviez que le Canada n'en faisait pas assez pour faire émigrer sa famille chez nous. Maintenant que le Canada a décidé d'accueillir 25000 réfugiés syriens d'ici la fin de l'année, vous branlez dans le manche. Vous avez peur. Tout d'un coup qu'un ou deux terroristes se glisseraient dans le lot. J'entends des maires, des députés, des ministres réclamer des délais. Il faut prendre le temps de bien faire les choses, dites-vous. Le temps de bien faire les vérifications de sécurité. Le temps? Pendant qu'on est là à niaiser autour d'un chiffre, des bombes continuent de tomber sur la tête des gens en Syrie et en Irak. Il y a des exactions, des viols, des décapitations, des défenestrations. Et dans le lot des innocentes victimes, il y a d'autres petits Alan. Qu'est-ce qu'il vous faut pour vous convaincre que le temps presse? Des photos d'enfants déchiquetés par les explosions? Avoir du temps devant soi, c'est le luxe d'une société éloignée de la guerre comme la nôtre. Le Droit, 2/Front

Rapid resettlement is possible: expert

An authority on immigration and refugees says Canada and the United Nations have the operational knowhow and security safeguards to vet 25,000 Syrians for rapid resettlement. But the question remains: can the humanitarian resettlement project be pulled off by the Liberal government's Dec. 31 deadline without compromising domestic security? "I hate answering that question at this point," said Peter Showler, former chair of the Immigration and Refugee Board and former director of the Refugee Forum at the University of Ottawa. "(However) it is possible in a relatively short period of time - with no reference one way or the other to the deadline - to do fast, effective processing that includes reliable security screening." Immigration Minister John McCallum has said the refugees would be properly screened. "I think (McCallum's) implication has been that if it takes longer, if it goes over the deadline, then it goes over the deadline," Showler said. "Certainly my understanding from him is that getting the job done properly is the priority." Showler's appraisal came as the Ottawa Citizen learned refugees arrived Tuesday in Montreal. Department of Immigration, Refugees and Citizenship spokesman Remi Lariviere confirmed a planeload of Syrian refugees landed, but did not make clear if the group was part of the 25,000 targeted for resettlement under the Liberals' plan. Postmedia News (Vancouver Sun, A1/Front)

Clock ticking on Canada's refugee plan

The timing of Canada's crash program to bring 25,000 Syrian refugees to Canada by the end of the year keeps sliding, according to two officials familiar with aspects of the planning. The original goal had been to begin the airlift by Thursday of this week, but as no charter aircraft have been booked yet, it would now be at least one more week before flights got underway, one of the officials said. When the flights reach their peak next month, about 1,000 refugees will be arriving in Canada every day. The officials did not want to be identified because diplomats and immigration officers have been told by Ottawa not to speak about the matter, with all requests referred to the government. "Unfortunately I have nothing to say to you at the moment," Immigration Canada spokesman Jean-Bruno Villeneuve said in an email from Ottawa, adding that he was unable to confirm any details about the resettlement program. (...)But the United Nations High Commissioner for Refugees, which registers asylum seekers and is supposed to be working with Canada on its resettlement program, said this week that it remained largely in the dark about Ottawa's plans. While the UNHCR welcomed the Canadian announcement to settle Syrians, "I am afraid I cannot talk about Canada's program," spokeswoman Ariane Rummery said in an email from Geneva "until we know more about the modalities." Whig-Standard, B2

Le temps du changement
Comme il était de mise dans ces circonstances tragiques qui relativisaient tout le reste, la couverture médiatique du dernier conseil général du PLQ a été presque exclusivement centrée sur les réactions aux attentats de Paris et l'accueil des réfugiés syriens. Même s'il est passé largement inaperçu, le premier ministre Couillard n'en avait pas moins un autre message à transmettre aux militants libéraux réunis à Québec. " Le temps du changement est venu, a-t-il dit. Il faut oser faire les choses différemment, oser remettre les choses en question. " Quelques minutes plus tôt, le président de la commission politique du PLQ, Jérôme Turcotte, avait évoqué les conséquences que le vieillissement accéléré de la population aura sur les coûts des services de santé qui, au rythme actuel, accapareront 70 % des dépenses gouvernementales en 2030. Ces propos semblaient rejoindre ceux que le ministre de la Santé, Gaétan Barrette, avait tenus la semaine dernière à propos du panier de services assurés par la Régie de l'assurance-maladie. S'il n'est pas question " à ce moment-ci " d'exclure certains services de la couverture, il a averti que " la situation budgétaire du Québec nous invite à une réflexion au long cours sur ces éléments-là ". Le Devoir, A4

Weil downplays 'anxiety' as polls reveal fears
Quebec's immigration minister was scrambling to reassure skittish Quebecers and mayors Wednesday that the province's decision to welcome Syrian refugees will not come back to haunt them. But two new polls reveal the brutal Paris terror attacks have spooked people. Suddenly, many are hot on the use of military force to put out threats and favour a goslow approach to accepting refugees. "There is a period of anxiety," Kathleen Weil told reporters on her way into a meeting of the Quebec cabinet. "But I think it's important that mayors and political leaders use the right tone, give the right message. "These are some of the most vulnerable people that we want to greet and settle in Quebec." Weil was responding to growing domestic blowback over the terror attacks last Friday in Paris which left 129 people dead and 350 injured - many of them seriously. With no clear plan forthcoming from Ottawa, Canadian premiers and municipalities have been operating in a void with growing questions about how the country will handle the complicated business of feeding, clothing, housing and integrating the 25,000 Syrian refugees Canada wants to welcome by Jan. 1. The province has already identified 13 Quebec cities with sufficient infrastructure and support systems to accept refugees. Quebec's share of the 25,000 is about 6,000. Postmedia News (Montreal Gazette, A4)

PM condemns racism as Syria refugee plan opposed
Prime Minster Justin Trudeau urged Canadians to resist hatred and racism as a poll showed most Canadians were opposed to his plan to bring in 25,000 Syrian refugees by year-end and a flurry of racist incidents were reported around the country. The Liberals, who took power after an election last month, campaigned on a promise to bring in the refugees by Jan 1. Critics say the number is too large and could threaten security following the attacks in Paris. An Angus Reid poll released on Wednesday showed 54 per cent of Canadians opposed the plan, up from 51 per cent before the bloodshed in Paris. But support for the plan also increased, with 42 per cent in favour, up from 39 per cent in October. Most of those who opposed Trudeau's plan did so because of the short timeline, with 53 per cent saying the schedule was too short to ensure all the necessary security checks were completed. Another 10 per cent said 25,000 was too many, and 29 per cent said Canada should not be accepting any Syrian refugees. (...)"Diversity is Canada's strength. These vicious and senseless acts of intolerance have no place in our country and run absolutely contrary to Canadian values of pluralism and acceptance," Trudeau said. Whig-Standard, B1/Front

Les initiatives citoyennes et les dons se multiplient
« Les gens offrent des logements, des vêtements. Des professeurs à la retraite proposent de l'aide aux devoirs, des Syriens veulent faire de la traduction. Tout le monde veut contribuer et faire partie de ce moment historique », dit Sylvain Thibault. À son bureau de la Table de concertation des organismes au service des personnes réfugiées ou immigrantes, le téléphone n'arrête pas de sonner depuis des jours. Sa boîte de courriels déborde. Parmi les offres de dons de toutes sortes se trouvent aussi des messages de quelques personnes qui ont déjà pris les choses bien en main. Les initiatives citoyennes se multiplient. C'est le cas de Yasmine Abdelfadel qui a décidé lundi soir, après en avoir discuté avec ses parents, qu'elle lançait un projet de paniers d'accueil. Le concept rappelle les paniers offerts spontanément à de nouveaux voisins qui arrivent dans le quartier. Mais les tartes bien chaudes et les confitures maison

seront remplacées par des paquets de couches et des fournitures scolaires. « Des choses que les gens ne pensent pas de donner lorsqu'il y a des collectes », précise la jeune femme, encore surprise de la réponse reçue sur la page Facebook de son Opération paniers de bienvenue. Une réponse telle qu'elle est entrée en contact avec la Table de concertation pour avoir de l'aide logistique. Ce qu'elle aura. « Nous allons faire des paniers personnalisés, selon la famille à laquelle ils seront destinés. » La Presse, 5

Autre dissonance libérale

Pour une deuxième journée d'affilée, le premier ministre Philippe Couillard et son ministre Pierre Moreau ont joué des notes discordantes sur la capacité du Québec à accueillir des réfugiés syriens d'ici la fin de l'année. Le chef de l'État québécois estime que le Québec parviendra «fort probablement» à accueillir sur son sol 3650 d'entre eux avant la fin de l'année, comme il s'y était engagé. Son ministre de la Sécurité est incapable de garantir plus de 2400 réfugiés syriens sélectionnés - et non pas accueillis - au 18 décembre. «Non, on est sur la même longueur d'onde, a assuré M. Couillard en fin d'après-midi. On vient d'en parler, lui et moi, avec tous les collègues. On est très confiants d'atteindre la cible du premier contingent.» (...) Des 1200 personnes prévues à l'origine, le gouvernement Couillard rehaussait son seuil à 3650. C'était avant que l'engagement du nouveau premier ministre canadien Justin Trudeau porte à quelque 5700 le nombre de réfugiés syriens à recevoir au Québec. «Sur le premier contingent [celui de 3650 réfugiés], on n'a aucun doute parce qu'on a les moyens financiers, les mécanismes, a affirmé le premier ministre Couillard. La question qui reste à éclaircir, c'est la mise en place du plan fédéral plus large.» Pourtant, un peu plus tôt, son ministre Pierre Moreau a été incapable d'assurer que Québec parviendrait à sélectionner - et non accueillir - les 3650 personnes prévues avant 2016. Un processus d'habilitation sécuritaire effectué par Ottawa suit l'étape de la sélection par le Québec. La Presse (Le Soleil, 6,7/Front; La Tribune, A7, 23, La Tribune, A7; Le Nouvelliste, 15) * Le Quotidien, 26,27 ; Le Droit, 16) ; * Agence QMI (Journal de Québec, 4 ; Journal de Montréal, 2)

D'ex-hôpitaux ontariens pour héberger des réfugiés?

Le gouvernement ontarien songe à utiliser des hôpitaux récemment désaffectés afin d'héberger temporairement les réfugiés syriens qui doivent affluer d'ici la fin de l'année dans cette province. Le gouvernement fédéral de Justin Trudeau a promis que le Canada accueillerait 25000 réfugiés d'ici le 1er janvier 2016, et l'Ontario s'est engagée à en accueillir 10000 d'ici la fin de 2016. Le ministre provincial de la Santé, Eric Hoskins, a indiqué mercredi que son gouvernement ignorait toujours le nombre de réfugiés qu'Ottawa lui demanderait d'accueillir d'ici la fin de l'année, mais il a assuré que l'Ontario était prête à faire sa «juste part» dans cette vaste opération. L'Ontario pourrait par ailleurs accueillir et soutenir certains réfugiés sur une base temporaire, avant qu'ils ne déménagent dans d'autres provinces ou territoires, a-t-il prévenu. Le Droit, 16; * Canadian Press (Cape Breton Post, A11; The Telegram, D3; Charlottetown Guardian, A7; London Free Press, A3); * Ottawa Sun, A9

La crainte de la passoire

Un article d'opinion déclare, « Ce n'est guère surprenant: 59 % des Québécois ont peur que des terroristes se faufilent parmi les réfugiés qu'on s'apprête à accueillir, parce qu'ils doutent que les autorités soient capables d'effectuer les contrôles nécessaires pour les débusquer. C'est ce que révélait, hier, un sondage Léger mené pour le compte de TVA Nouvelles. Un sondage, on n'en sera pas étonnés non plus, qui indique que trois Québécois sur quatre craignent que des attentats aient lieu au pays. Dans la foulée du drame parisien et de ses rebondissements, de même que de l'intense médiatisation qui a cours, redouter la menace terroriste, surtout après les événements de l'an passé à Saint-Jean et à Ottawa, est un réflexe qui se comprend. On ne peut pas rester insensibles à l'horreur, à la haine. Il est normal de ressentir de l'insécurité face à des actes aussi insensés, aussi méprisables. Encore faut-il gérer ce réflexe avec sang-froid et ne pas céder à la panique ou à la xénophobie. Il faut se rappeler que les auteurs des attaques de l'an dernier chez nous étaient des Canadiens, pas des immigrants. Gardons aussi à l'esprit que la menace terroriste se propage davantage par Internet que par les frontières. Enfin, considérons qu'il y a bien plus d'actes criminels commis par des bandits et des chauffards ivres que par des terroristes. Cela dit, le Canada doit bien sûr mener une lutte impitoyable au terrorisme... » Le Nouvelliste, 18

Canadians leery of Trudeau's refugee plan
A little more than half of Canadians disapprove of the federal government's plan to bring in 25,000 Syrian refugees by the end of next month, a new poll suggests. And if they had to choose, Canadians surveyed by Mainstreet Research for Postmedia appear to be more in favour of bombing terrorists than training other armies howto fight. "The training mission has wider support. Either way, most Canadians believe Canada should be taking a role in the fight against ISIS. Only 8% of Canadians would support no action at all," said Quito Maggi, president of Mainstreet. Conducted Monday, the firm polled a total of 2,718 people. It suggests public opinion is polarized over what to do on the world stage when it comes to bombs and refugees. "Our earlier polling showed strong support for bringing refugees to Canada, but after the attacks in Paris, security is now a higher concern," Maggi said. QMI Agency (Ottawa Sun, A10; Toronto Sun)

* **13 000 réfugiés pour trois mois**
Les Forces armées canadiennes affirment pouvoir fournir de l'hébergement à un maximum de 13 000 réfugiés syriens à travers le Canada pendant une période n'excédant pas trois mois. Si l'objectif de 25 000 avant la fin de l'année est maintenu, cela signifie que les premiers arrivés ne feront que passer par les bases militaires pour ensuite être relogés ailleurs. Le Soleil, 4, 5/Front ; Postmedia News (Winnipeg Sun, A6; Ottawa Sun, A8; Toronto Sun, A4; Calgary Sun, A8)

* **Hamilton readies for influx, but many questions remain**
A broad range of Hamilton groups, agencies, churches, officials and individuals say they have been working for weeks to build plans for what could be a significant number of Syrian refugees landing in this city in the very near future. The trouble is, they don't know how many are coming, or which sponsorship and resettlement programs the refugees will be funnelled through. Hamilton Spectator, A1

* **Canadian business groups tout refugee job opportunities**
Businesses that have a hard time recruiting Canadians say they are reaching out to the federal government and the provinces to see if they can match up with the incoming wave of refugees. Lobby groups for Canadian employers are intrigued by the 25,000 refugees Prime Minister Justin Trudeau expects to bring in by the end of the year. "This has been ramping up since a year ago," said Ron Davidson, director of government relations for the Canadian Meat Council, which lobbies on behalf of meat packing plants. Embassy

* **Un élan de générosité de la population**
L'arrivée massive à Québec de 800 réfugiés syriens prévue en décembre semble provoquer un élan de générosité dans la population. Le Centre multiethnique note une hausse importante du nombre de personnes intéressées à leur venir en aide. Une bonne nouvelle pour l'organisme, qui aura grandement besoin de ressources supplémentaires. Le Soleil, 8/Front

* **Où vont les réfugiés syriens?**
L'un des terroristes à l'origine des attentats de Paris a été retrouvé avec un passeport syrien. On ne sait pas encore si le passeport est authentique ou s'il appartenait vraiment à l'homme qui s'est fait exploser au Stade de France. Mais la nouvelle a fait grand bruit, provoquant des mouvements partout dans le monde afin de fermer les portes aux réfugiés syriens. Voici quelques chiffres pour faire le point sur la crise humanitaire de l'heure. Depuis 2011, l'Agence des Nations unies pour les réfugiés (UNHCR) a dénombré plus de 4,2 millions de personnes qui ont fui la guerre en Syrie. La très grande majorité a trouvé refuge dans des pays limitrophes. Plus du quart d'entre eux ont moins de 18 ans. L'Europe a accueilli à ce jour près de 510 000 réfugiés, dont plus de 150 000 en Allemagne. De son côté, le Canada propose de recevoir d'ici la fin de l'année 25 000 nouveaux réfugiés qui s'ajouteraient aux quelque 3000 déjà au pays. Voici une douzaine de pays ou de régions qui ont accueilli des réfugiés syriens jusqu'à présent. La Presse, A11

* **Accueillir des réfugiés est un devoir**
Comment les réfugiés syriens traverseront-ils l'océan vers le Canada? Quels sont les risques que des terroristes s'infiltrent parmi eux? Beaucoup de Québécois ont des appréhensions face à leur venue. Alors est-ce risqué pour eux de venir ici? Pourquoi les médias ne parlent-ils pas des réfugiés innombrables de

l'Afrique? Des questions comme celles-là, les élèves de cinquième secondaire de l'école Les Pionniers de Trois-Rivières en avaient plusieurs pour Béatrice Vaugrante. Le Nouvelliste, 5

*** Region prepares for 1,150 Syrian refugees**
Planning is underway to prepare for upward of 1,150 Syrian refugees who are soon expected to start arriving in Waterloo Region. Immigration Partnership is hosting a half-day preparedness planning session on Friday that will gather together service providers to be ready for the influx of refugees. The Record, B2

*** Canada should look to the U.S**
Six weeks to go until the new year and by the time we usher in 2016, the Liberal government is determined that 25,000 Syrian refugees will be in Canada. "There was an election. There was a commitment. And we'll deliver on our commitment," Foreign Affairs Minister Stephane Dion told reporters Wednesday at the annual summit of Pacific Rim leaders here. The Liberals may be determined to deliver on that commitment but there is growing unease in Canada that the arbitrary deadline of Jan. 1 may lead authorities to cut corners and open potential security concerns. Prime Minister Justin Trudeau himself says that won't happen but, so far, has yet to provide details on Canada's security arrangements. Trudeau will meet U.S. President Barack Obama on Thursday and, because of our long, shared, undefended border, one would assume Obama wil I want more than platitudes, he'll want some of those details. Postmedia News (Toronto Sun, A22; Calgary Sun, A35; Edmonton Sun, A50)

*** Blue Rodeoto Canada**
The Liberal government's plan to welcome 25,000 Syrian refugees into Canada shouldn't be deterred by recent terror attacks, said Blue Rodeo bandmates Jim Cuddy and Greg Keelor. Cuddy and Keelor, who were among 12 officers and 33 members welcomed into the Order of Canada Wednesday, continued their streak of political pillow talk to discuss some of the major issues facing Canadians under a new Liberal government. Ottawa Sun, A14

*** Ils ne l'ont pas, le temps**
Un article d'opinion déclare, « Alors là, un gros bravo. Quand on a retrouvé le petit Aylan mort noyé sur une grève en Turquie, vous trouviez que le Canada n'en faisait pas assez pour faire émigrer sa famille chez nous. Maintenant que le Canada a décidé d'accueillir 25 000 réfugiés syriens d'ici la fin de l'année, vous branlez dans le manche. Vous avez peur. Tout d'un coup qu'un ou deux terroristes se glisseraient dans le lot... » Le Droit, 21

*** PM has no clear plan**
An opinion piece states, "To be clear: I absolutely believe this country should take Syrian refugees. We have so far been sheltered from the humanitarian crisis that has engulfed Europe, as hundreds of thousands of migrants have fled the turmoil in Syria. What troubles me is the haphazard manner in which the federal government is going about it and the way it's turned into a political football..." Postmedia News (Ottawa Sun, A9; Toronto Sun, A5)

*** Here, the Pope would be suspect**
An opinion piece states, "Back in September, Pope Francis commented on the ongoing refugee crisis in the Mideast in an interview with a Portuguese radio station. He warned of the danger of Islamic State terrorists "infiltrating" European countries amid the huge flow of refugees streaming out of war-torn Syria and Libya. He also cautioned that host countries taking in refugees "cannot be simplistic" about integrating them into their societies, because of their own high unemployment rates. In Canada these days, such reasonable observations, are enough to get one accused of bigotry, hating refugees and fear-mongering by the liberal and Liberal elite..." Postmedia News (Ottawa Sun, A19; Toronto Sun, A15; Calgary Sun, A15; Edmonton Sun, A15)

*** Provinces need more of a role helping refugees**
An opinion piece states, "Most of Canada's premiers are outdoing each other with generous offers to accept Syrian refugees by the thousands during the next six weeks, but their promises are all but meaningless. Premier Kathleen Wynne re-stated her promise-2,500 refugees by the end of this year and

10,000 by the end of 2016-again Tuesday. "It's our responsibility to be open to the world," she said in Toronto..." Postmedia News (London Free Press, A6; Whig-Standard, A4)

*** The refugee discussion is just beginning**
A comment by Jeffrey Simpson reads "The commitment to bring 25,000 Syrian refugees to Canada before Dec. 31, made by the Liberals in the heat of an election campaign, should be seen not as the end but as the beginning of a multiyear commitment to bring tens and tens of thousands more refugees to Canada over many years. Quite apart from whether the government can meet its artificial and politically driven timetable for the 25,000, the larger question is whether the government and the Canadian people are willing, ready and able to handle much bigger numbers in the years ahead. No one has thought about this, let alone prepared for it. Circumstances, however, will force reflection. This 25,000 contingent, and the many who will follow if the government sticks to its policies, is not like, say, previous groups of refugees from Vietnam, Uganda or Kosovo. These groups were much smaller in number, displaced by one event at a given place. By contrast, there were three-day periods throughout the summer and fall when more refugees/migrants were landing on the Greek island of Lesbos than Canada proposes to admit in two months. Today's refugees/migrants are part of a mass movement of millions of people fleeing military conflict, entrenched poverty and government breakdowns across an arc of states in the Middle East and Africa. Climate change is already widening desertification, which causes people to leave drought in search of food." Globe and Mail, A19

*** Our history will win over our fear, anger**
An opinion piece states, "Canadians mostly have opened their doors and their hearts to refugees, displaced persons and immigrants since the 19th century, but it would be a mistake to believe it always was easy and that it happened without some of the fear and political grandstanding now surrounding the Syrian refugee crisis. Yet the common denominator for newcomers to Canada has always been the same, the promise of opportunity, tolerance, freedom and safety. In this, the vast majority of Syrians seeking refuge in Canada are no different from the millions of immigrants who came before them..." Postmedia News (Whig-Standard, A4; London Free Press, A6)

*** Trudeau focused on 'sunny ways'**
A letter to the editor states, "With no foreign policy credentials or experience, Justin Trudeau, in the aftermath of the Paris massacre, is Mark Twain's The Innocents Abroad, peddling his "sunny ways" election message of feel-good infrastructure deficit investment and economic inclusiveness to a G20 audience that is single-mindedly focused on dealing with the global threat of international terrorism. There is Trudeau, valiantly offering the world his prescription for saving an endangered middle class while an endangered world is grappling with how to save itself. But, of course, in Trudeau's world, Canada has nothing to fear from ISIS because of its much-vaunted multicultural diversity and inclusiveness, and soon to become the new home of some 25,000 Syrian refugees to be rushed into the country by year's end with electoral refugee "politics" trumping sustainable and responsible refugee "policies." As to fighting ISIS - glory be! Liberal "soft power" days are here again!" Windsor Star, A7

*** We must be vigilant in accepting refugees**
An opinion piece states, "The world has changed dramatically for Canada's new prime minister. Justin Trudeau needs to acknowledge the gravity of the situation imposed by the Paris terrorist bombings and enhance Canada's military commitment to fighting ISIS, rather than emasculating it. He should ensure no Syrian refugees, let alone 25,000, set foot on Canadian soil without a careful and comprehensive security screening process in place..." Winnipeg Sun, A13

*** Why Canada Can Safely Meet Its Refugee Commitments**
An opinion piece by an immigration lawyer states, "The attacks in Paris last week set off a world-wide flood of empathy and solidarity. Canadians attended vigils, lit monuments in the tricolour and mourned the loss of life and normalcy in the City of Love. However, grief quickly turned into anger, inciting the inevitable search for a scapegoat. Shocking instances of violence against mosques and Muslims have been reported around the world, including a fire at a mosque in Peterborough, Ontario. Xenophobic acts are not an uncommon public reaction; a spike in attacks on Muslims following terrorist attacks has been well studied and documented. In Canada, despite the objective lack of connection, politicians began

sounding off "security concerns" related to incoming Syrian refugees. Saskatchewan's Premier Brad Wall called for a delay in resettling Syrian refugees. Premier Christy Clark of British Columbia stated the obvious: that the government needs to ensure that security checks are done on every refugee. These statements demonstrate a clear lack of understanding by government officials of Canada's process for resettled refugees. Contrary to the influx of migrants crossing into Europe over the past months, Canada is resettling *pre-screened* refugees who have been approved for permanent residency by a Canadian visa officer abroad. The process is thorough and involves international and national law enforcement agencies." The Tyee (2015-11-18)

Lettre - Main-d'oeuvre et réfugiés
Une lettre à l'éditeur déclare, « A la suite de la proposition d'accepter 100 000 réfugiés syriens par année au Canada, il était particulièrement ahurissant d'entendre la présidente de la Fédération canadienne des entreprises indépendantes (FCEI), Martine Hébert, affirmer : " N'importe quelle politique permettant la venue de plus de travailleurs, dont les entreprises ont tant besoin, est une bonne politique. " Mme Hébert reprenait ainsi une rengaine répétée mille fois par les organisations patronales selon laquelle plus d'immigration est toujours souhaitable en raison d'une supposée pénurie de main-d'oeuvre... » Le Devoir, A8

Refugee backlash will strengthen
An opinion piece states, "Because this is Canada, the backlash begins in the most polite of fashions. But make no mistake, a backlash against Justin Trudeau's plan to bring 25,000 Syrian refugees to this country is taking root and seems certain to build. Although the Liberal pledge should be applauded, the new government has helped fuel this backlash by its stubborn determination to meet an arbitrary deadline forged in the hothouse of election campaign politics..." Charlottetown Guardian, A9, The Record, A11)

Vetting questioned
An editorial states, "Re: Don't let Paris attacks alter refugee plan: profs (SP, Nov. 16). So University of Saskatchewan counter-terrorism expert Colleen Bell thinks that turning our backs on 25,000 Syrian refugees would be "a tragedy" because "Canada is a huge country." This is the kind of academic-think that passes for expertise these days. Bell and her fellow academic Martin Gaal are reported as saying that both the UN and Canada "conduct detailed screening" of refugees. You can buy into that Liberal myth if you like. I'm more convinced by U.S. Congressman Peter King, a member of the House Homeland Security Committee, who says "there is no reliable vetting system" for these refugees. "We don't know who these people are because there are no data bases to work from." Saskatonians appear to harbour an admirable skepticism on the issue. For example, of those who responded to a (pre-Paris) CFQC-TV survey that asked if they support Prime Minister Trudeau's plan to import 25,000 Syrian refugees before year-end, 83 per cent replied No. Many media commentators and Canadians alike are cynical about Trudeau's claims that the refugees will be screened rigorously. I will be looking to see exactly which "robust" vetting methods his functionaries employ. But I won't be holding my breath that we'll be given many details." Postmedia News (StarPhoenix, A8)

Logistics, not background checks, are the problem
A letter to the editor states, "White House spokesman Josh Ernest said Wednesday the 10,000 Syrian migrants destined for the U.S, will be subject to background check vetting that can "last up to 24 months" before they are approved, or rejected, as immigrants. Fortunately for the 25,000 Syrian migrants heading for Canada, our security checking is apparently so overwhelmingly comprehensive that the 25,000 will be vetted and accepted into the Canadian family by New Year's Day. Of course, after New Year's, when one or two, or 20 migrants turn out to be Islamic State of Iraq the Levant recruits and sneak into the U.S. to inflict mayhem there, watch out for the wall construction to begin across the 49th parallel and the total loss of U.S. confidence in Canada as a reliable neighbour and ally." Postmedia News (National Post, A11)

Keeping the door open
An editorial states, "The terror attacks in Paris have provoked a maelstrom of emotions and calls to action. It's crucial that governments and individuals refrain from responding in ways that do more harm than good. Reports that one of the attackers had entered Europe as a Syrian migrant have heightened

Canadians' fears. That's because Canada has committed to welcoming 25,000 Syrian refugees by year's end. There had been warnings that ISIS might slip terrorists into the flow of Syrians seeking refuge in the West, and that one case is being cited as confirmation. However, that threat does not justify closing the door to the vast majority of legitimate refugees; it's a reminder of the need for effective security screening. Canada's new government has reiterated its promise to take in 25,000 Syrians by Dec. 31, and for this it should be commended. The renewed commitment underlines a message that is worth repeating : Asylum seekers should not be conflated with terrorists; they are fleeing terror." Postmedia News (Vancouver Sun, B6)

Syrian refugees now scapegoats
An editorial states, "The tragic events in Paris have resulted in an unfortunate over-reaction. There are the expected demands for justice and calls for revenge. But the alarm bells are now sounding that Syrian refugees are guilty until proven innocent. When politicians, statesmen and decision-makers are caught up in this hysteria, it is very disappointing. This irrational conclusion is threatening the refugee resettlement program involving thousands of innocent Syrian refugees involving many nations, including Canada. The attacks in Paris were carried out by French and Belgian citizens. Likely, they were radicalized by terrorist elements or inspired by real or perceived attacks or discrimination against Islam and Muslims. The murders carried out by fanatics have somehow resulted in blame being placed on innocent refugees..." Charlottetown Guardian, A8

Whose side are we on?
An opinion piece states, "There are all sorts of fascinating and necessary questions that remain unanswered about exactly why, whether or when Prime Minister Justin Trudeau should or will withdraw Canada's CF-18s from the U.S.-led coalition arrayed against the Islamic State of Iraq and the Levant (ISIL). There are at least as many troubling questions about whether it is wise or even remotely possible for Canada's new Liberal government to fulfil Trudeau's campaign promise to resettle 25,000 Syrian refugees in this country before Christmas. (...) But if Trudeau's Canada is to be something truly new and different, then in this most horrific of global calamities, Canada should be the voice for Syria's voiceless. That's whose side we should be on." Postmedia News (Ottawa Citizen, C7; National Post)

Let Watson stay
A letter to the editor states, ""... Canada should be a refuge from militarism." PM Pierre Elliot Trudeau, 1970 Among the policies of the past 10 years that the new government seeks to reverse, one is urgent and could be made with the stroke of a pen. Against the will of Parliament, who voted twice to let American war resisters stay, Harper's government issued a deportation order against Rodney Watson, who then went into sanctuary for six years in First United Church, Vancouver. Canadian Immigration Officers waited outside to deport Watson to the U.S., to spend up to two years in prison. What a different era we are in compared to the Vietnam War. In 1967, myself an officer in the U.S. Military Medical Corps, and my wife Bonnie, later an Officer of the Order of Canada, were processed at midnight at Dorval Airport, receiving Landed Immigrant status in 20 minutes. Prime Minister Justin Trudeau has expressed empathy for the plight of refugees from the Iraq War. Urge him and Citizenship, Immigration and Refugee Minister John McCallum, to rapidly end this travesty of justice." Postmedia News (Vancouver Sun, B7)

PUBLIC SERVICE / FONCTION PUBLIQUE

Open public data necessary for functioning democracy
An opinion piece states, "There may be a new era coming in our federal access-to-information laws, and that would be a good thing, However, it's one thing to promise access in a campaign and another to follow through when in government. We'll have to wait and see. Information laws exist to protect our collective right to access public records. Every citizen and permanent resident in Canada has the right to request information from federal, provincial/territorial and municipal governments. All orders of government are subject to the protocols set out in the Access to Information Act (ATIA) at the federal level and Freedom of Information (FOI) legislation at the provincial/territorial and municipal levels. These legal instruments allow individuals to request records, policy documents and correspondence that show how government agencies operate. ATI/FOI files are different than the open-source material found on government

websites, in the rhetorical speeches of politicians, and in the sanitized information packages of public relations experts. ATI/FOI files illustrate how power operates in democratic societies and can expose the often-secretive dealings between state entities and political players. There have been a number of instances where Canadians have become aware of an issue of public interest because of information uncovered using access-to-information laws." Winnipeg Free Press, A9

OTHER / AUTRE

*** Clarity from Liberals needed to calm tensions, says Ambrose**

The new interim Conservative leader is promising to change the party's tone, but Rona Ambrose was not as willing Wednesday to say she would abandon the practice of using cultural wedge issues as a political tactic. Ambrose was asked about a recent tweet in which MP Candice Bergen said she was embarrassed and sickened by Prime Minister Justin Trudeau's approach to the fight in the Middle East and his promise to resettle 25,000 refugees. The Liberals intend to withdraw Canada's jets from the ongoing bombing campaign against the Islamic State of Iraq and the Levant, also known as ISIL or ISIS, but will keep soldiers in the region to train anti-ISIL fighters. Ambrose chalked up Bergen's tweet to heightened passions in the wake of Friday's attacks by ISIL militants in Paris, which killed 129 people and left hundreds more injured. "After what happened last week, there is going to be some emotion and some passion and I'm going to chalk that one up to some emotion and passion," Ambrose said. Similar passions were conjured up during the election campaign in response to the Conservative emphasis on issues like the niqab ban and a tip line to report so-called "barbaric cultural practices," Ambrose acknowledged. Both were considered to be wedge issues exploited by the Conservatives to mobilize votes. Ambrose said she was not part of the decision to promise a tip line, nor did she support it. But when asked whether her party would drop the wedge politics strategy, Ambrose didn't answer. Canadian Press (Telegraph-Journal, A8); * Toronto Star

*** Whose side are we on?**

An editorial states "There are all sorts of questions that remain unanswered about Prime Minister Justin Trudeau's decision to withdraw Canada's CF-18s from the U.S.-led coalition fighting against the Islamic State of Iraq and the Levant (ISIL). There are at least as many troubling questions about whether it is wise, or even remotely possible, for Canada's new Liberal government to fulfil Trudeau's campaign promise to resettle 25,000 Syrian refugees in this country before Christmas. But there is a far more important unanswered question that deserves at least some passing attention in all this: just whose side are we on, anyway? For five full years, Stephen Harper's Conservatives chose to go along to get along with U.S. President Barack Obama's half-baked responses to the hideously violent Baathist reaction to the Arab Spring that has now metastasized into the world-devouring catastrophe with its jihadist epicentre in the Syrian hellhole of Raqqa (...) Of course there are other questions. Up to 1,000 Syrian refugees a day are expected to begin arriving next week in the first convoy of a half dozen widebody jumbo jets shuttling Syrian refugees from Jordan, Lebanon and Turkey to Canada. About all that, here's just one of the questions that remains unanswered: what exactly are we going to do with all these people?" Postmedia News (National Post, A10)

*** Slain volunteer fighter to be honoured**

He was a volunteer fighter in a war in which Canada has no regular troops on the ground.
The group he fought with has murky ties to a group Canada officially lists as a terrorist organization.
John Gallagher, 32, who grew up in Southwestern Ontario and died fighting alongside Kurdish forces against the Islamic State in Iraq and the Levant (ISIL) in Syria, will get a hero's welcome home Friday when his body is returned from the Middle East. His death - and the Highway of Heroes-style salute planned for him - opens a new chapter in Canada's military story, one highlighting the shifting nature of allegiances and the tricky job of honouring those who serve. "He used to be in the military," said Casper Koevoets of the Royal Canadian Legion's Victory branch in London. "He was fighting the right fight that he believed in. I think he deserves a hero's welcome home," Gallagher was killed Nov. 4 in Syria by an ISIL "suicide attack" on Kurdish fighters with the People's Protection Units (YPG), a group that actively recruits English-speaking fighters. Its members include citizens of Canada, the United States and Britain.

Postmedia Network (Vancouver Sun, B2, London Free Press, National Post, Edmonton Journal, Whig-Standard)

*** Climate change the worst threat this century, Dion tells APEC summit**
Foreign Affairs Minister Stephane Dion says climate change is the "worst threat we are facing this century," and warned that emissions-reduction targets don't go far enough. It's a marked departure from the stance of the previous federal government, which had alternated between whether ISIL or Russia was the greatest threat to Canada and the world. The question of how to deal with climate change took centre stage at the Asia-Pacific Economic Co-operation summit Wednesday, which has brought together leaders from 21 countries on both sides of the Pacific. The Syrian refugee crisis and Trans-Pacific Partnership trade deal were also discussed. U.S. President Barack Obama said the Asia-Pacific region is particularly vulnerable to flooding and land loss associated with climate change. Ottawa Citizen (Vancouver Province, A24; Star-Phoenix; Leader-Post; National Post; Montreal Gazette)

INTERNATIONAL

False hope, no mercy for fleeing migrants
For more than two months this spring, Abul Taher did not know where his son had gone. Then his phone rang. "Your son is in the middle of the sea. Give us money," the voice on the other side said. "If you don't give the money, we will kill your son and throw him into the sea." In the background, he could hear screams from his son as captors beat him. Then his son, Muhammad Selim, was allowed to speak. "Please, give them money. Please, save my life," he said. (…)The unfolding of what Amnesty International called a "humanitarian crisis at sea" started long before Syrian refugees began leaving for Europe, and threatens to continue for years. A regional crackdown has won a pause in the number taking to the water this fall. But the grinding poverty and persecution that have driven the trade remain unchanged. "I fully expect that the trafficking will resume. I was in the camps a month ago and lots of people said, 'We don't care about the risk, we're just going to go,' " said David Scott Mathieson, a senior researcher with Human Rights Watch The long southeastern peninsula of Bangladesh slices alongside Myanmar, its 125 kilometres of sand forming one of Earth's longest beaches. It's one of the few places in Bangladesh that attract tourists. It's also home to one of Asia's most vulnerable populations, where poor farmers live alongside drug traffickers, corrupt police and a persistent dream that across the water, there is something better. Globe and Mail, A12

***L'EI lance un nouveau numéro de son magazine**
«Juste terreur» ou «juste la terreur». C'est par ce double sens arrogant - Just Terror, en anglais - que le groupe armé État islamique a coiffé la une du plus récent numéro de son magazine de propagande Dabiq, consacré en partie aux attentats de Paris. Lancé hier sur les réseaux sociaux, le numéro contient quelques images des attentats. Provenant d'agences de presse, elles ont été retouchées avant leur publication dans le magazine. La photo de la une, par exemple, montre des secouristes venant en aide à un blessé. Une femme, qui apparaissait à droite dans la photo originale de l'Agence France-Presse, a été carrément effacée de l'image avec un logiciel de retouche. Les chaussures d'une des femmes victimes de l'attentat, en bas à gauche, ont aussi été floutées. Selon nos vérifications, Dabiq n'a jamais publié de photo montrant une femme, même voilée, dans l'un ou l'autre des onze numéros précédents du magazine voué à la promotion du djihadisme. Une bombe dans une canette Dabiq a aussi publié une image de ce qui serait la bombe artisanale utilisée par l'EI pour abattre l'avion de Metrojet qui s'est écrasé dans le désert du Sinaï, en Égypte. Le dispositif aurait été dissimulé dans une simple canette de boisson gazeuse. «On ne voit que trois éléments: la canette, une charge explosive et un commutateur. Il n'y a pas de minuterie ou de dispositif de déclenchement à distance. Ça laisse croire, si l'image est véridique, qu'ils ont utilisé un kamikaze pour commettre l'attentat», note le Canadien Yannick Veilleux-Lepage, spécialiste de la propagande terroriste à l'Université St. Andrews, en Écosse. La Presse, A14

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PS.PSPMediaCentre/CentredesmediasPSP.SP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
December 1, 2015 / 1 décembre 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** University, Intact team up on climate research site**
The University of Waterloo and Intact Financial Corp. have created a new research centre that will look for new ways to reduce weather-related property damage linked to climate change. Intact will initially provide $4.25 million for a program focused on how to protect Canadian communities from severe precipitation, such as unusually heavy rains and ice storms. Another program will identify how various Canadian industrial sectors are vulnerable to extreme weather. The new Intact Centre on Climate Adaptation will be based in the university's environment faculty. The centre will monitor applied research from around the world and conduct its own research. The ICCA will also launch a national Home Adaptation Audit Program (HAAP) to assess the vulnerability of homes to flood damage, and make specific recommendations to help homeowners avoid costly damage from extreme weather. Canadian Press (Chronicle-Herald, B4); Toronto Star

* **CP to fight $409-million Lac-Mégantic lawsuit**
Canadian Pacific Railway Ltd. says it will fight a $409-million lawsuit the province of Quebec has launched over the 2013 LacMégantic oil train explosion that killed 47 people. The lawsuit filed in Quebec Superior Court alleges CP was negligent in handing over the tank cars to Montreal, Maine and Atlantic Railway, the now-defunct company that was in possession of the 74-car train left unattended before it rolled into LacMégantic and wiped out much of the town's core. The lawsuit also accuses CP of failing to take steps to prevent the disaster. "CP intends to fully defend itself in court," a company spokesman said on Monday. CP hauled the oil train from its origin in North Dakota to Montreal, where it handed over the cars to MM&A. The train was destined for Irving Oil's refinery in Saint John. In October, CP dropped its objections to a $446-million compensation fund for victims, allowing the settlements to begin flowing. Of about 24 settling parties, CP was the sole company refusing to pay into the fund, a stance that leaves it open to possible future damage claims. Globe and Mail, B5

* **Belledune - forte opposition québécoise au projet de port pétrolier**
Le projet de construction d'un terminal pétrolier au port de Belledune par l'entreprise Chaleur Terminals continue de susciter la mobilisation de citoyens et de groupes écologistes du Québec opposés au transport de pétrole par train pour l'exportation. Jeudi, les partis de l'opposition à l'Assemblée nationale du Québec ont uni leurs voix à celle des opposants du projet qui prévoit l'acheminement par train au Nouveau Brunswick de pétrole issu des sables bitumineux de l'Alberta… En entrevue à l'Acadie Nouvelle, la députée Manon Massé a indiqué que sa formation politique exige elle aussi la tenue d'audiences et d'un examen par le Bureau d'audiences publiques sur l'environnement, l'organisme québécois voué à l'information et à la consultation publiques sur des projets susceptibles d'avoir un impact majeur sur l'environnement. Celle-ci se dit sensible aux critiques venants de plusieurs néo-brunswickois qui craignent de voir l'opposition à de tels projets mener à l'abandon d'initiatives qui seraient créatrices d'emplois pour diverses communautés du Nouveau-Brunswick. «Loin de nous l'idée de dire qu'il faut pénaliser les petites communautés. La question qui se pose, c'est comment pouvoir sortir de cette économie qui est basée sur la filière pétrolifère», explique Manon Massé. La députée montréalaise estime qu'à l'image de la tragédie de Lac-Mégantic, les populations locales subissent et absorbent les risques du transport de produits pétroliers. «L'Industrie pétrolifère est financée à coup de milliards de dollars, cet argent devrait plutôt être investi dans la création d'autres types d'emplois, comme dans la fonction publique et dans les industries de la forêt et des énergies renouvelables», estime Manon Massé. L'Acadie Nouvelle, 8

* **Incertitude**
Une pièce d'opinion dit « « Alors que Chemin de fer Central Maine & Québec (CMQ) pourrait techniquement transporter du pétrole brut à compter du 1er janvier, l'incertitude de la Coalition des citoyens et organismes engagés pour la sécurité ferroviaire est bien légitime et commande davantage d'écoute de la part des autorités. Le président du CMQ, John E. Giles, soutient que sa compagnie n'a encore aucun contrat pour le transport de pétrole brut et rappelle son engagement d'aller rencontrer les citoyens et les dirigeants municipaux si la situation change. Mais la levée même symbolique de l'embargo volontaire sur le transport de pétrole brut n'en constitue pas moins une épée de Damoclès. Depuis juin 2014, M. Giles a fait de la sécurité ferroviaire son leitmotiv, affirmant que sa compagnie a investi 22 millions$ pour améliorer la voie ferrée et les infrastructures après des années de négligence de l'ancien propriétaire, Montréal, Maine & Atlantic. Il a aussi démontré une volonté de rassurer les citoyens à la suite la tragédie de juillet 2013, alors qu'un convoi de 72 wagons-citernes remplis de pétrole avait déraillé en plein centre-ville. Toutefois, malgré le verdict de Transports Canada selon lequel les voies sont sécuritaires, les observations effectuées par des citoyens et le consultant Jacques Vandersleyen ont démontré des problèmes de rails usés, de traverses pourries, de même qu'un ponceau en mauvais état. » La Tribune, 14

NATIONAL SECURITY / SÉCURITÉ NATIONALE

* **Trudeau's Parliamentary Secretaries To Be Charged With Policy Files**
Prime Minister Justin Trudeau will appoint his parliamentary secretaries in the next day or two, The Huffington Post Canada has learned. Parliamentary secretaries resemble junior cabinet ministers, but

they traditionally don't attend cabinet meetings and they have no managerial responsibilities over departments. They mostly answer questions on behalf of their minister when he or she is not in the House. This time, however, some parliamentary secretaries will be charged with actual policy files... Another Liberal source cautioned that there might be several familiar names left off the list of appointees this week. The PMO is hoping that some who are left off the list will be elected committee chairs, including the chair of the soon-to-be struck national security committee — the oversight body the Liberals promised as a response to the concerns over increased sharing of information by security agencies in Bill C-51. Huffington Post (2015-11-30)

*** Can we please stop blaming terrorism on civil libertarians?**
An opinion piece by Andrew Mitrovica states "White. Male. Academic. Check off those three boxes and you've got a good chance of being anointed a "national security expert" by the mainstream media ... no questions asked. You'll be contacted by reporters for instant comment on the terrorist attack *du jour*, based on information that you've likely gleaned from reading newspapers and watching TV - just like everybody else. But you've got a PhD, so that's all that really matters. One frequent rider on the national security pundit carousel is Christian Leuprecht, a professor at the Royal Military College, Queen's University and a 'senior fellow' at the Macdonald-Laurier Institute. Last week, Leuprecht penned a column for the *Globe and Mail* that was rife with inaccuracies, offered a vacuous defence of Bill C-51 and made the breathtakingly absurd suggestion that "self-righteous" critics of the "surveillance state" (presumably including journalists like yours truly) have prevented the forces of order from "leveling the playing field with the bad guys" responsible for the Paris atrocities.. Readers may recall that in a March column I dissected the equally laughable remarks Leuprecht made before the Senate's Public Safety and National Security Committee considering Bill C-51. Caught in one act of ill-formed hyperbole, Leuprecht has chosen to double-down. He starts his latest rant in the *Globe* by chastising unnamed "critics" for pointing out that many of the terrorists who murdered hundreds of innocents all over Paris were hardly in deep cover - that, as the *Wall Street Journal* has so meticulously reported, the killers made their deadly preparations in "plain sight" of somnolent French and other European intelligence services... Leuprecht then compounds this bit of lunacy by suggesting Canadian cops and spies are reluctant to share such information because of ... Canadian torture survivor Maher Arar. "Since the Maher Arar case," Leuprecht writes, "Canadian agencies are loath to share intelligence with other departments, let alone countries." iPolitics

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Deportation order hard to grasp
At first glance it seems a contradiction, one many Londoners find difficult to understand. As Canada lays out the welcome mat for 25,000 Syrian refugees fleeing catastrophic conditions in their home country, the government shut the door last week on a Colombian family who say they fear they will be killed when they return to theirs. (...)"It's clear in the law, but I can understand why people in the community don't understand it. It's quite complex," London immigration consultant Mia Loebach said Monday. "The basic answer to that is anyone, before they come to Canada, needs a permanent resident visa to come in." "The (Syrian refugees) have been processed by the United Nations.They will land as permanent residents," Loebach said. In contrast, when people ask for refugee status after arriving in the country - as Johanna Santos, Edgar Regalado and their two children did in April 2013- they are immediately given what's called a "conditional removal order," Loebach said. "And that moves pretty quickly once the refugee claim is refused," she said. The plight of the Santos-Regalado family has triggered an outpouring of support in the northwest London community where the children attend St. Paul elementary school and the parents have put down roots. They said they had been targeted by the Revolutionary Armed Forces of Colombia (FARC) for years, had moved cities to avoid persecution and fled the country after a FARC member shot at Regalado. But in a decision later upheld by a federal court, a refugee board denied their claim for status here, saying they had not done enough to get help in Colombia. The family has received an order to leave the country on Wednesday. London Free Press, A1/Front

Woman arrested at St. Stephen border
A 28-year-old woman was sent to jail on Saturday after being taken into custody by Canadian customs officials. Police were called to St. Stephen on Saturday at 7 p.m. after the woman was identified as being wanted for an outstanding committal warrant, said Sgt. Lori Magee of the Saint John Police Force. Such warrants typically are issued for unpaid fines. Telegraph-Journal, B4

Low dollar gives tourism a temporary lift
Tourism to Canada rebounded in 2015, thanks to the low Canadian dollar, but the travel industry can't count on a favourable exchange rate to prop it up indefinitely. The sector has to make some significant changes if it is going to regain its spot among the top 10 destinations in the world, according to the latest annual report from the Travel Industry Association of Canada. That means boosting marketing efforts, trimming airport taxes and fees for incoming travellers and making sure there are enough employees to work in the sector. The report notes that Canada was in eighth place among the world's top destinations - measured by international visits - in 2000, but it has fallen well out of the top 10 since then. By 2014, Canada was in 17th place, behind countries such as Saudi Arabia, Greece, Thailand and Austria. (…) Another key issue for the tourism sector is a labour shortage, especially in Western Canada. Loosening the Temporary Foreign Worker Program to allow a seasonal stream of employees would be one short-term fix, TIAC suggests. Globe and Mail, B3

La lutte aux gangs de rue s'intensifie
Le chef de la police d'Ottawa, Charles Bordeleau, a présenté son budget préliminaire pour 2016, à la Commission des services policiers, lundi soir. Quelques heures plus tôt, le numéro un de la police municipale a confirmé au Droit que son unité des gangs de rue et des armes à feu était débordée. C'est pourquoi douze agents viendront en aide - temporaire - à la dizaine déjà en place dans cette escouade. (…) Du même souffle, le chef de police a mis en relief une surabondance des armes à feu provenant des États-Unis qui débordent à Ottawa. De plus en plus d'armes de poing achetées au pays de l'Oncle Sam traversent la frontière canadienne, et servent à des criminels plus ou moins avertis dans la capitale fédérale. Le Droit, 5/Front

Deporting this family seems wrong
An opinion piece states, "Regarding the article Colombian clan loses bid to stay in Canada (Nov. 28). Would someone please explain to me why this family of four (who apparently has assimilated into Canadian culture with support fromfamily, community, school and a job) is being deported. Meanwhile we are prepared to offer thousands of refugees free passage, lodging and everything else supplied to come to Canada, London included. Are we being humane only to Syrians and disregarding anyone else? I don't understand the rational behind this decision." London Free Press, A5

Jury duty can be taxing in more ways than one
A letter to the editor asks, "Q "I read recently that Canada and the U.S. are exchanging border information to keep closer tabs on how long people are staying in the two countries. The insinuation is that if you spend more than 182 days outside Quebec, you could lose your health benefits in Quebec. Is this true?" A It has been rumoured for a while that border monitoring is being stepped up, which could mean a nasty surprise for Quebecers who don't check - or don't care - how long they stay in the U.S. or anywhere else. To be covered by the provincial health card, residents are supposed to be present here more than half the year. You cannot be absent more than 182 days in a calendar year. (Departure and return days don't count against you in the calculation, and neither does any absence of 21 days or less). "Any person who does not respect this condition is not covered by the provincial health system for that year or any other where they're absent for 183 days or more," a spokesman for the Régie de L'Assurance Maladie du Québec said. "The Régie will ask to be reimbursed for any health services received during that period."" Postmedia News (Montreal Gazette, B1/Front)

Time for action on new terminal
An opinion piece states, "Victoria Mayor Lisa Helps is part of a 13-member delegation in Ottawa this week trying to drum up federal funding for a new Belleville Street ferry terminal. This is no junket. After decades of talks, task forces, reports and hand-wringing, replacement of the dismal terminal on the south side of Victoria's Inner Harbour is long overdue. Visitors coming to downtown Victoria by sea are treated to a

magnificent view that, besides natural features, includes the B.C. Parliament Buildings, the Empress Hotel and other heritage buildings. Much work over the years has gone into turning a bleak industrial site into an attractive, welcoming harbour. But the welcome mat for ferry passengers is tattered and grubby. The terminal is a hodge-podge of temporary industrial trailers, hardly a fitting portal to a beautiful harbour and a beautiful region. (...)Travellers arriving in Greater Victoria by air are greeted suitably. In 2011, Victoria International Airport, which receives federal funding for improvements, was rated among the top 10 most-loved airports in the world, and has consistently won awards for customer service. While the Belleville Street terminal does not handle as many travellers as the airport, it, too, is an important portal. The federal government should do its part to ensure travellers by sea are welcomed in comfortable and attractive surroundings, not in temporary buildings more suitable for an oil camp than a port of entry to Canada." Times Colonist, A10

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Kids' tech maker VTech hacked, 5 million at risk**

Kid's technology maker VTech says the personal information of about 5 million of its customers and their children may have been stolen by hackers. The Hong Kong-based company disclosed the breach of a customer database late last week, but didn't say until Monday how many people could be affected. The news comes just as the holiday shopping season is kicking into gear and kids' smartwatches and tablets made by companies such as VTech are expected to be high on children's wish lists. VTech's Kidizoom Smartwatch is predicted to be a top seller this holiday season, while its InnoTab tablets have been popular in the past. Compromised information in the VTech breach includes the names, birthdates and genders of child users. It also includes adult user information including names, email addresses, passwords, secret questions and answers for password retrieval, IP addresses, mailing addresses and download histories. The affected database doesn't contain any credit card numbers, or personally identification information such as Social Security or driver's licence numbers, VTech said. Customers from the U.S., Canada and 15 other countries are affected. The hacking serves as a reminder to parents to be careful about what kinds of information about their children they enter into on Internetconnected devices. While devices like kid-friendly smartwatches and tablets may block a child's access to the bulk of the Internet, they're still a potential target for hackers. The breach took place Nov. 14 and was discovered 10 days later. It involved customer data stored on the Learning Lodge app store database. Customers use Learning Lodge to download apps, games, e-books and other content to VTech products. Associated Press (Times-Colonist, B3); Telegraph-Journal; Reuters (National Post)

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Vader Trial 'Crisis'**

Court hears how lack of disclosed evidence led to stayed charges. The Crown is denying it is an abuse of process to put Travis Vader on trial for killing two vanished St. Albert seniors after charges against him were earlier stayed. And court heard Monday during a hearing into the case that the "disclosure crisis" that led to the first-degree murder charges being stayed was the fault of the RCMP. Edmonton Chief Crown prosecutor Michelle Doyle testified at the Court of Queen's Bench hearing that she was "stunned" to learn of the "staggering" amount of evidence in the case which had not been disclosed by police. "I couldn't believe it," said Doyle. "I was very upset and very angry and that was communicated quite clearly." In the month before Vader's April 28, by2014, trial for the alleged killing of Lyle McCann, 78, and his 77-year-old wife Marie, was set to start, a team of 20 Mounties was tasked to figure out the situation, but it quickly became apparent the evidence would not be disclosed in time. "At this point I had lost all confidence in the status of disclosure," said Doyle, adding she knew then that she could not proceed with the upcoming trial. Postmedia Network (Edmonton Sun, A10); CBC (2015-12-01); CBC News; Edmonton Journal (2015-11-30)

Man charged with murder in death of Cutknife

A 19-year-man has been charged with second degree murder of a Samson Cree Nation woman. Maskwacis RCMP found the body of Kirsten Cutknife on the Samson Cree town site residence on

Saturday morning. Joshua Crier, 19, was also charged with assault with a weapon involving another women. She did not receive life-threatening injuries. All three people are known to one another. All three people are known to one another. Crier is in police custody and will make a first appearance in relation to the charges in Wetaskiwin Provincial Court on Dec.17. An autopsy has been tentatively scheduled for Wednesday at the Office of the Medical Examiner in Edmonton. Postmedia Network (Red Deer Advocate, A5)

Mother of five one of three found dead in rural home

Friends and family have identified a woman who recently started a new job at a fast-food restaurant as one of three people killed in a rural Alberta home. Mounties say the bodies of a man, a woman and a teenage girl - all with "obvious trauma" - were found in a house near Edson on Sunday. Sylvia Standing said Monday that her goddaughter Roxanne Ruth Berube was 36, had five children and was a good mother. There were also media reports identifying the male victim as Dan Miller. Insp. Gibson Glavin said the deaths were not a murder-suicide. "I will be clear that there was someone out there, or some people, who did this and we have not arrested them yet," he said. RCMP major crimes investigators and other Mounties were speaking with people in the area west of Edmonton looking for leads and clues, he said. Police found the bodies after responding to a call from someone outside the home. Glavin said police don't believe anyone else is at risk, but urged people to be careful. "We do urge the public to be cautious, to be aware of people or circumstances that cause them to believe that they have some knowledge or some connection with this homicide investigation," he said. Postmedia Network (Red Deer Advocate, A1,A2, Times Colonist, London Free Press Edmonton Journal, Edmonton Sun, Toronto Sun, Vancouver Sun, Calgary Sun, Calgary Herald Times & Transcript); National Post, Presse canadienne (La Voix de l'Est, 4)

*** School response to undisclosed threat was 'precautionary'**

Two messages sent to parents of students at Bernice MacNaughton High School concerning a threat at the school were a matter of caution, said the superintendent of the Anglophone East School District Monday afternoon. Gregg Ingersoll said in an emailed statement that the principal of the high school in west Moncton received information late last week that caused her to initiate a security protocol that resulted in two messages being sent to parents over the weekend disclosing that a threat had been made. The school district has an established assessment tool for determining the significance of any threat connected to a school. Ingersoll said in this case, "the result was that the situation posed a low level of concern, however the school asked the RCMP to get involved as a precautionary measure. The school had a smooth start up this morning and officials at the school are working with the RCMP in the ongoing investigation." The district's assessment tool defines a "Low Level of Concern" as instances when "risk to target(s), student, staff and school safety is vague and/or indirect." The involvement of the RCMP is typically reserved for high levels of concern when a threat is imminent or immediate, but that was not the case in this instance. Postmedia Network (Times & Transcript, A3)

*** Tories hand over Atcon computer servers to RCMP**

Progressive Conservatives have handed over Atcon's back-up computer servers to the RCMP after revealing on Monday that the party purchased them at a bankruptcy auction in 2013. The Miramichi company's bankruptcy cost taxpayers close to $70 million. The Progressive Conservatives have long said questions remain over the former Liberal government's dealings with the failed Miramichi company. Interim Tory Leader Bruce Fitch says there's now "enough new information" on the servers to prove a new audit is required, something the Liberal government hasn't committed to doing. Liberal cabinet Minister Donald Arseneault labelled the move a "pretty pathetic" attempt to divert attention away from issues of the current day by an opposition without any new ideas. Arseneault also questions whether there's anything to the servers - beyond a political stunt. In a 61-page report earlier this year, Auditor General Kim MacPherson found that Atcon received a total of $77 million from the defunct Department of Economic Development, with nearly $70 million of that amount in default. She noted that her office hadn't done a forensic audit on the money trail, but would be willing to do one if the Legislative Assembly asked her to do it and provided the resources to make it happen. The Progressive Conservatives contend it didn't seek to analyze the servers it quietly purchased now more than two years ago - even through a general election - because it was waiting on what the auditor general found. Fitch said on Monday that the current Liberal government's stance to not move forward on a larger audit then led the party to hand

the servers over to police. It first paid about $1,800 to have the servers analyzed by an IT firm to recover some of the documents. Postmedia Network (Times & Transcript, A10, Daily Gleaner, Telegraph-Journal)

*** Youth pleads guilty to being an accessory to robbery**

A Moncton teen has admitted to being an accessory to robbery and will be sentenced on Dec. 14. The female offender appeared in Moncton youth court Monday morning with her lawyer Helene Beaulieu. She can't be named because she was 17, a youth, when the offence was committed. She pleaded guilty to being "a party" to robbing Bharat Kumar Gadher of electronic items while wounding him with a knife. The Crown withdrew charges of aggravated assault and robbing money from him while armed with a knife. She also pleaded guilty to two breaches of undertaking in June and July. The offence occurred just before 4 a.m. on May 3. The RCMP were called to the parking lot of the Sports Rock Bar on Paul Street where a man was suffering from stab wounds. Police said he drove himself there and his vehicle ran into the back of a cab. Postmedia Network (Times & Transcript, A3)

Murder scene was 'pretty horrific,' officer tells jury

Even for a seasoned Hamilton police forensic investigator, the Lou Malone murder scene was horrific. "There is a male deceased lying on the west sidewalk with a large pool of blood at his head. The top part of his head appeared to have been shot off," Det. Const. Doug Moon told a jury of the murder scene he witnessed on Kenilworth Avenue North in the early morning hours of Nov. 9, 2013. "Are you able to characterize the scene?" prosecutor Craig Fraser asked the officer. "It was a bloody mess. Pretty horrific. It was ugly," Moon replied. Brothers John and Mike Josipovic, aged 52 and 49 respectively, have pleaded not guilty to first-degree murder in the slaying of Malone, 49. Malone, a former biker, had been shot point blank in the back of the head after being chased by two men in a pickup truck. Moon testified Monday that birdshot pellets from the shotgun blast that killed the ex-Hells Angel biker broke storefront windows on the west side of Kenilworth, south of Hope Street. The seven-man, five-woman jury learned earlier that Malone was initially grazed in the neck in front a home at 35 Robins Ave. Moon presented evidence that showed how close that blast had been. Postmedia Network (Hamilton Spectator, A8)

*** Murder charges should be stayed, lawyer say**

Murder charges against Travis Vader in the case of a slain St. Albert couple should be stayed because the prosecution gave itself an unfair advantage by delaying the case for two years, according to his lawyer. In turn, the prosecution has blamed the delay on an Alberta RCMP "fiasco" that put Vader's right to a fair trial in jeopardy with late disclosure of evidence. The RCMP's disclosure problems were massive and egregious, according to the prosecution, and left no option but to stay the charges in one of the province's most-watched trials. Michelle Doyle, the original prosecutor in the case, said she believed disclosure of evidence was complete before the RCMP sent thousands of new documents in the weeks before Vader's 2014 trial was set to begin. (...) Vader's previously scheduled trial was derailed on March 29, 2014, when prosecutors stayed the murder charges because of the RCMP's lack of disclosure. Later that year, they lifted the stay and Vader faced the murder charges once more. Postmedia Network (Edmonton Journal, A7)

Cocaine, weapons found in home near school

Drugs and a firearm were seized Sunday from a Sidney home directly across the street from Sidney Elementary School. Sidney/North Saanich RCMP executed a search warrant at the home and found cocaine that was packaged - seen as an indication that it was prepared for distribution - as well as a rifle with prohibited ammunition capacity and a set of brass knuckles with a Taser built in. Police arrested a 17-year-old girl, a 23-year-old woman and two men, ages 19 and 21. The females were released without charge, but the men are facing charges that include possession of a controlled substance for the purpose of trafficking and unlawful possession of a firearm. They have been released and are awaiting court appearances. Sidney/North Saanich Cpl. Erin Fraser said it's disturbing to have to carry out a bust like this one near a school. "Definitely not ideal, especially given there was a weapon found," she said. "There was no direct threat to the kids, no links that we could establish with the kids, but just the fact that it's right there certainly is concerning to us." Postmedia Network (Times Colonist, A4)

Property crimes spike
Police are cracking down on organized crime and making headway when it comes to safer youth and safe roads, according to the Red Deer RCMP's annual policing report. But the year-to-end results show a significant spike in total property crimes from Jan. 1 to Sept. 30 over the last five years. In 2015 there were 10,034 total property crimes compared to 9,506 in 2014 and 7,342 in 2011. RCMP Insp. Gerald Grobmeier said this may be attributed to the growth in Red Deer's population, the downturn in the economy or that people are reporting more crimes. It's probably a combination of everything," he said. Criminal code offences, such as disturbing the peace and offensive weapons, have stayed relatively the same with 16,313 in 2015 compared to 16,241 in 2014 and 14,297 in 2011. Total persons crimes were down to 2,117 in 2015 compared to 2,336 in 2014 and 2,567 in 2011. This includes crimes such as robberies, sexual assault and utter threats. Grobmeier said the downward trend is common throughout the country. He said it could be a combination of better education, better programs and more calls to the police. Postmedia Network (Red Deer Advocate, A1, A2)

*** Stemming the violence - Legislation would make it easier for victims to obtain protection orders**
An editorial states, "The Selinger government has introduced legislation to make it easier for victims of domestic violence to obtain protection orders and to require the subjects of such orders to surrender firearms they may possess.The measures come in the wake of two high-profile deaths in the province this fall. Manitoba has the second-highest rate of spousal homicide in Canada, next to Saskatchewan, Attorney General Gord Mackintosh said Monday in announcing several administrative and proposed legislative changes. "We have to do better," he said. "We have to end this terror." Mackintosh said amendments he introduced in the legislature to the Domestic Violence and Stalking Act will set a less onerous standard for obtaining protection orders. (…) Over the last two years, more than 1,200 protection orders have been granted in Manitoba, but another 1,700 have been dismissed." Canadian Press (Winnipeg Free Press, A3)

*** Real protection**
In the wake of two recent deaths linked to domestic violence, the provincial government hopes to soon offer victims the strongest protection in Canada. To do so, it must first eliminate barriers that are relatively unique to Manitoba. Over the past two years, 1,200 protection orders were granted in the province, while 1,700 - 59% - were dismissed because of a high threshold for victims to qualify, said Justice Minister Gord Mackintosh. And when protection applications came in, courts also weren't required to follow up on reports the suspected abuser had a gun or check into his or her criminal record. "We have to open wider the doors of justice, particularly for those women living in fear," said Mackintosh. Mackintosh announced new legislation Monday that aims to make protection orders easier to get. Those with orders against them would also face automatic criminal checks and be banned from keeping guns. The new bill follows two deaths that raised questions about Manitoba's current system. Selena Rose Keeper was denied a protection order before her ex-boyfriend was charged with killing her in October. And Camille Runke was allegedly shot to death by her ex-husband while she had a protection order against him. "This is for Selena and Camille and too many other women who deserve long lives and a life in peace," Mackintosh said. Postmedia Network (Winnipeg Sun, A5)

*** Solicitor general vows to help ALERT cope with shortfall**
Alberta's solicitor general has vowed to protect Alberta Law Enforcement Response Teams (ALERT) from layoffs stemming from a $3-million drop in funding anticipated next year, but future changes to the agency are being considered. On Monday, Kathleen Ganley dismissed fears that 70 ALERT members could be laid offnext year as a result of a reduction in federal grant funding. "We don't believe that will be the case," Ganley told reporters at the legislature. "We're committed as a fundamental principle to ensuring that no layoffs occur and that the functions of this organization continue going forward." The province received a $42.4-million grant from Ottawa in 2008-09 as part of the federal government's initiative to recruit new police officers. Funds were allocated to ALERT in increments until the grant was depleted. "During this fiscal year they are adequately funded and they can continue to maintain their operations," she said. "Going forward we have, with the support of both ALERT and the Association of Chiefs of Police, performed an audit on ALERT and we will be determining in the coming days how best to perform that function." She noted ALERT is made up of a series of specialized teams. The 280-member agency brings together six teams from across Alberta to deal with fugitives, grow ops, child pornography, cybercrime

and other large cases. ALERT chair Shami Sandhu said last December that a cut of one-quarter of the agency's officers would jeopardize the work it does and leave it on a "shoestring" budget. Ganley said earlier this month during her ministry's budget estimates that the province recently had an outside audit conducted into the operations of the 10-yearold integrated unit of municipal police, RCMP and provincial sheriffs "to see how well that was working for everyone." Postmedia Network (Calgary Herald, A6, Edmonton Journal)

*** Father of 2 shouldn't have been killed by Thompson RCMP, family says**
The family of a Thompson man shot to death by RCMP says he never should have been killed over a case of drinking and driving. Steven Campbell, 39, was shot and killed by an RCMP officer on Nov 21 after a short police chase ended in an officer shooting into the vehicle he was driving. "Steven had his demons, and Steven was no saint, but I just wanted to tell his story because he made mistakes, and he didn't deserve this," said Shannon Heck, Campbell's sister. According to RCMP, Campbell had been driving erratically when officers tried to pull him over. CBC (2015-12-01); Thompson Citizen (2015-11-30)

Downloading costs
In a classic case of downloading from Ottawa and Victoria, municipalities are being asked to pay more for DNA crime analysis. It's baffling that this isn't included in the current RCMP contract. Policing is the biggest of big-ticket items in municipal councils' budgets and they're growing impatient with ever-ballooning costs. This will likely spur a closer look into whether we could be saving money or getting better service by jettisoning the RCMP in favour of a local or regional police force. Housing is a provincial responsibility, yet cities and districts are regularly allowing denser condo developments in exchange for the inclusion of non-profit or market rental housing - both things the province and the feds have largely pulled out of over the last 30 years. That siphons off money that could otherwise be invested in areas that are within municipal jurisdiction, such as updating old rec centres or paying for local infrastructure. Postmedia Network (Times Colonist, A10)

*** Saisie par la GRC de cigarettes électroniques contenant de la marijuana**
Les policiers ont récemment saisi dans un véhicule intercepté au Nouveau-Brunswick une grande quantité de marijuana, de l'hydromorphone et des cigarettes électroniques contenant de la marijuana. Le conducteur, Stéphane Fournier, un homme âgé de 39 ans de la région d'Ottawa, a été arrêté lors de cette opération qui s'est produite en octobre, près de Havelock, mais qui n'a été rapportée que cette semaine par la GRC. Les cigarettes électroniques saisies contenaient de l'huile de cannabis et du tétrahydrocannabinol (THC), la composante psychoactive de la marijuana. C'était la première fois que la GRC au N.-B. interceptait un produit de la marijuana sous cette forme. Les cigarettes électroniques contenant de la marijuana peuvent être consommées discrètement, car elles ne dégagent aucune odeur et ressemblent à une cigarette électronique typique. En Cour provinciale à Moncton, Stéphane Fournier a été accusé de trois chefs d'accusation de possession d'une substance réglementée dans le but d'en faire le trafic et de trois chefs d'accusation de trafic d'une substance réglementée. Il a été libéré sous certaines conditions et comparaîtra de nouveau en cour à une date ultérieure. Presse canadienne (Acadie Nouvelle, 2)

*** Legalizing pot shouldn't be another promise to go up in smoke**
Prohibition has not served us well, let's hope Trudeau follows through. After Prime Minister Justin Trudeau's recent climb down on his refugee commitment, it might be fair to wonder how many other of his election promises might be compromised. For example, is it a certainty that marijuana will be legalized? It was one of Trudeau's first promises as Liberal leader, and his mandate letters to the relevant ministers spell out the need to create a federal-provincial process "that will lead to the legalization and regulation of marijuana." Mind you, "creating a process" makes it sound like the government is less than 100 per cent committed. If there's any kind of significant pushback on this issue, will they get cold feet? The public, at least, seems to be onside with the concept (…) Calgary police chief Rick Hanson, however, took a much different view on such matters, and was never shy about expressing his opinion on what laws we needed or did not need. So where does our current chief stand? Back in October, newly minted police Chief Roger Chaffin seemed to take a hands-off approach. He expressed his hope that law enforcement would at least be consulted, and said in the meantime, they would "continue our education, enforcement and

public outreach activities in regards to marijuana and other illicit drugs." Postmedia Network (Calgary Herald, B4)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Assante settlement greenlighted
A $10-million settlement has been approved in the class-action lawsuit involving a former Red Deer investor incarcerated for first-degree murder. Justice John Rooke, associate chief of the Alberta Court of Queen's bench, approved the settlement between a class of 804 claimants against Assante Capital Management, Assante Wealth Management, and Brian and Christine Malley. It was approved on Monday in Red Deer Court of Queen's bench. The Malley's ran the Assante Capital and Wealth Management office in Red Deer. Former clients launched the suit claiming invest mismanagement. (...)Brian Andrew Malley, 58, of Innisfail was convicted of first degree murder on Feb. 24 in Red Deer Court of Queen's bench. Victoria Shachtay, 23, of Innisfail was killed on Nov. 25, 2011. The quadriplegic single mother died when she opened a gift left on her doorstep. The gift disguised a pipe-bomb, which detonated. Malley was sentenced to life without parole for 25 years. He is currently appealing the decision and sentence. Red Deer Advocate, A2

*** Son sort repose sur la crédibilité des délateurs**
La crédibilité des frères Robert et Timothy Simpson, délateurs qualifiés de «sociopathes» par la défense, pèsera lourd dans le sort d'un de leurs présumés complices d'un double meurtre à Montréal. C'est ce qu'ont convenu les procureurs des deux parties au procès de Leslie Greenwood, qui tire à sa fin après deux mois et demi d'audition. Le garagiste est accusé d'avoir participé aux meurtres du trafiquant Kirk Murray et de son chauffeur, Antonio Onesi, dans le stationnement d'un McDonald's du quartier Notre-Dame-de-Grâce, le 24 janvier 2010. Les victimes ont été abattues par Robert Simpson, aidé de son frère cadet, sous l'ordre du Hells Jeffrey Lynds. (...)Robert Simpson est incarcéré pour sept meurtres, dont quatre perpétrés dans des pénitenciers et qu'il a décrits en détail au procès. Journal de Montréal, 18

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Speeding up justice for victims
In her more than 25 years working as a prosecutor, Kelly Winchester has never found that it gets easier to look at the bloody and bruised photographic evidence of intimate partner violence, or to hear the heartbreak of abuse. Yet she remains dedicated to prosecuting sexual assault and domestic violence cases. The images, the stories, as difficult as they may be, steel her determination. And she has plenty of work to do. Winchester estimates about a quarter of the files that come across her desk entail some type of domestic violence. This is in keeping with data from Statistics Canada that intimate partner violence comprises a quarter of violent crimes in New Brunswick. More than drugs, robbery, motor vehicle theft and even drunk driving, it's intimate partner violence that consumes Winchester's time. Winchester works out of the Crown's Saint John office. In a province that has the highest rate of police-reported intimate partner violence east of Manitoba, the Port City is the crime's epicentre. The city regularly ranks as one of the most dangerous for couples in the country. According to data obtained exclusively from Statistics Canada by the Telegraph-Journal, in 2014 Saint John Police reported more than one incident of domestic violence a day. One out of every five victims reported by police in the province was located in Saint John. Telegraph-Journal, A1 (Daily Gleaner, Times & Transcript)

*** Real protection**
In the wake of two recent deaths linked to domestic violence, the provincial government hopes to soon offer victims the strongest protection in Canada. To do so, it must first eliminate barriers that are relatively unique to Manitoba. Over the past two years, 1,200 protection orders were granted in the province, while 1,700 - 59% - were dismissed because of a high threshold for victims to qualify, said Justice Minister Gord Mackintosh. And when protection applications came in, courts also weren't required to follow up on reports the suspected abuser had a gun or check into his or her criminal record. "We have to open wider

the doors of justice, particularly for those women living in fear," said Mackintosh. Mackintosh announced new legislation Monday that aims to make protection orders easier to get. Those with orders against them would also face automatic criminal checks and be banned from keeping guns. Winnipeg Sun

* **First phase of inquiry into missing, murdered indigenous women expected this week**
The federal government is expected to release the details of the first phase of a national inquiry into missing and murdered indigenous women this weekend, CTV News has learned. Ottawa plans to make the announcement, which is expected to begin with the consultation of the victims' families, on or before the National Day of Remembrance and Action on Violence Against Women on Dec. 6. "As we promised, we will listen to the families first, who have good experience with this and good instincts, and then we will engage with the other partners in the aboriginal organizations, provinces and territories, (and) experts," said Indigenous and Northern Affairs Minister Carolyn Bennett. A full inquiry is expected to be launched in the spring of 2016. CTV News

* **'Gender inclusive' inquiry for indigenous men not for everyone**
A recent petition calling for a "gender inclusive" inquiry into missing and murdered aboriginal people in Canada is not sitting well with everyone. Adam Jones, an associate professor with the University of British Columbia, started the petition a few weeks ago, saying men and boys account for more than 70 per cent of total aboriginal homicide victims in Canada and should not be ignored in a national inquiry. Canada's minister of Indigenous Affairs, Carolyn Bennett, has previously said she hasn't ruled out the possibility of including men and boys in the national inquiry. CBC News

'Karina was stolen from our family'
Carol Wolfe never forgot the last words her daughter said before she disappeared five years ago. "The last memory I have is Karina saying, 'I love you mom and I will be home later,' " she said through a sign language interpreter Monday at the Saskatoon police station. Karina never came home. Last month, the man who is charged with killing Karina Wolfe led police to the area northwest of the city where they discovered her remains. (…)People said Carol Wolfe was tireless in her search for her daughter. "She never gave up," Darlene Okemaysim-Sicotte said, standing a few feet away from the spot where police recovered Karina's body. (…)Meanwhile, supporters are working hard to help Karina's family. Okemaysim-Sicotte said her grassroots organization, Women Walking Together, has been working with Wolfe's family since she disappeared. She said the fact that Constant volunteered information that led to the body's discovery and his subsequent arrest shows that awareness about missing and murdered aboriginal women is working. Postmedia News (StarPhoenix, A1, Edmonton Journal, Ottawa Citizen, National Post)

Man pleads guilty to Winnipeg assaults
A 21-year-old man has pleaded guilty to last year's attack on a Winnipeg teen, admitting his role in the nearly fatal assault that turned the young woman into a voice for Canada's missing and murdered indigenous women. In provincial court in the Manitoba capital on Monday, Justin Hudson, a member of the Poplar River First Nation, pleaded guilty to two counts of aggravated sexual assault in relation to the Nov. 8, 2014, attack on the young woman and a separate assault hours later on a second indigenous woman. He had been charged with attempted murder, aggravated sexual assault and sexual assault with a weapon. The young woman's name is protected by a publication ban ordered by the court on Monday, as is the second victim's. (…)The young woman, now 17, is today an advocate for a national inquiry into Canada's missing and murdered indigenous women - a probe the Liberal government has said it will launch by the summer. Her case also provoked a conversation about identifying victims of sexual assault. Globe and Mail, A3, Winnipeg Free Press, Canadian Press (Times Colonist), CBC News

Quilt stitches families together - Honouring slain, missing women
A quilt made by family members of Canada's missing and murdered indigenous women is to be unveiled Friday at the Winnipeg Art Gallery. The project, which involved 200 relatives from every province, is believed to be the first time families have come together to work on an art installation of this kind. The 200 family members made the patches in Winnipeg in September when the province hosted a national event to bring families from across Canada together. "There are a lot of projects to honour missing and murdered indigenous women and girls, but this one is about the families. It's the families who are creating

something, making something for their loved one," said Nahanni Fontaine, Manitoba's special adviser on aboriginal women's issues. Fontaine spearheaded the project, modelling it on a quilt created in Manitoba for missing and murdered indigenous women and girls. That quilt, with 35 patches, was unveiled at the art gallery in 2014. With 95 patches, the new quilt is three times the size of the Manitoba one, which Fontaine takes to meetings around the country. Winnipeg Free Press

*** Sunday vigil to mark 26th anniversary of Montreal Massacre**
In honour of the National Day of Remembrance and Action on Violence Against Women, the Comox Valley Transition Society and Honouring Our Sisters will host a vigil on Sunday, Dec. 6 at 2 p.m. on the plaza in front of the Comox Valley Art Gallery, 580 Duncan Ave., Courtenay. Dec. 6 will be the 26th anniversary of the Montreal Massacre, where 14 young women were gunned down simply because they were women who were studying to become engineers. Over the last 40 years, approximately 1,200 indigenous women have gone missing or have been murdered in Canada. Every six days, a woman is murdered by a current or former partner. Comox Valley Record (2015-11-30)

Police shuffle aims to deal with shootings, gangs
Ottawa's police chief has reassigned as many as 12 officers to his force's guns and gangs unit in response to the growing number of shooting incidents in the city. The deployment comes in advance of a meeting this week with Mayor Jim Watson, Chief Charles Bordeleau and police board chair Eli El-Chantiry to discuss what could become a record year for gunfire. Most of the 42 shooting incidents in Ottawa so far this year appear connected to gangs and have ranged from reports of shots being fired to young men showing up at hospitals with bullet wounds. The total compares with 49 incidents in all of 2014. El-Chantiry said the additional officers will come from other departments within the force. Ottawa Citizen, A2

Le SPVM mène une offensive contre les gangs de rue
L'opération policière qui a mené à une dizaine d'arrestations samedi à Montréal et sur la Rive-Sud s'inscrit dans une offensive plus globale contre les gangs de rue lancée par le Service de police de la Ville de Montréal (SPVM) à la fin de l'été, a appris *La Presse*. Cette offensive, baptisée « Projet Accalmie », doit se poursuivre au moins jusqu'à la fin de l'année et avait comme premier objectif de mettre fin à une vague d'événements violents qui ont secoué les gangs de rue depuis le printemps dernier. Une dizaine de meurtres, de tentatives de meurtre, d'agressions et d'autres événements se sont produits durant cette vague qui a culminé avec l'assassinat de Donald César, survenu à Montréal-Nord au début du mois de septembre. César était le demi-frère de Chénier Dupuy, défunt chef des Rouges tué durant l'été 2012, et des policiers avaient ensuite dit à *La Presse* craindre une escalade de la violence. Un inspecteur du SPVM avait toutefois assuré qu'il n'y avait pas de guerre entre les gangs de rue et que plusieurs mobiles différents pouvaient expliquer les événements violents. La Presse

*** Nunavik beer, wine sales foster lower crime rates: police**
Police in Puvirnituq say there has been a major drop in the number of calls they've had to handle since the Nunavik community's co-op store began selling beer and wine in October. The Povungnituk Co-operative Association began offering beer and wine sales from its local store in October, the second co-op in the region to do so since the Fort Chimo Co-operative Association in Kuujjuaq re-launched its own sales in 2013. "It's been a month, and for us, we've seen a huge decrease in the number of calls we've received," said Kativik Regional Police Force captain Jean François Morin, who serves as interim deputy chief of operations in Puvirnituq. "There's been a huge decrease in the number of files we've had." Morin said it's not just law enforcement that's noticed the difference, but the community's health and social services workers too. (…)It's less clear how beer and wine sales have impacted on crime in Kuujjuaq; last year, the KRPF has said crime rates in Nunavik's largest community have remained roughly the same. But the KRPF says there has been a recent and overall drop in violent crime across Nunavik, and that this decrease is related to a bump in alcohol seizures over the past year. Nunatsiaq Online (2015-11-30)

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

Dilkens in Ottawa to hear federal plan for Syrian refugees in Windsor
Windsor Mayor Drew Dilkens could find out Tuesday in Ottawa how many hundreds of Syrian refugees his city will be expected to welcome over the next 90 days. "That's what all of us mayors are hoping to hear," said Dilkens, who is being joined by municipal leaders from across Canada at a morning meeting at Rideau Hall with Gov. Gen. David Johnston and federal and provincial ministers. The mayors are in the capital to hear the Liberal government's how-to plan on mobilizing Canadians and co-ordinating agencies to receive 25,000 refugees from war-torn Syria over the next three months. Initially advised that Windsor could expect up to 1,000 refugees - triple its normal annual immigrant intake - Dilkens said he was reassured by both the federal and provincial ministers responsible for immigration that the actual number could be anywhere between 200 and 400. He said he told both that Windsor has a relatively high residential vacancy rate of four per cent but also has Canada's highest unemployment ate. "Everybody wants them to be successful, and part of being successful is being able to find employment," said Dilkens. Postmedia News (Windsor Star, A1/Front)

* **First 'new wave' of Syrian refugees arrive in Canada from Lebanon**
Ibrahim Tonbari struggled off Air Canada Flight 8867 in Windsor, Ont., Monday with his wife, Zaineb, and four children under the age of seven. He shuddered in the cold, but told CBC News in Windsor that the first thing he thought of was a better future for his children. (...)Sunday, they piled into one taxi and make the three-hour drive to Beirut's Hariri airport. None of them has ever flown on a plane, let alone a 28-hour journey with four kids and two layovers. "I didn't sleep last night", says Zaineb wanely. The Canadian government has contracted the International Organization of Migration to handle logistics and country exits. The official arrives and starts calling out names for the 32 refugees who are on the flight that night. Each gets a blue bag, stenciled IOM, and inside is the coveted document , a copy of Canadian "permanent resident status" — one each for Ibrahim, his wife and four kids. CBC News

Refugee hotline set up
Manitobans looking for ways to help Syrian refugees coming to the province can now go to an information hotline. The line has been set up by the provincial government, the Manitoba Emergency Measures Organization and the Canadian Red Cross. It will provide information to anyone looking to make a donation or who wants to volunteer with resettlement efforts. Manitoba is expecting between 1,500 and 2,000 people who have fled Syria. Winnipeg Sun, A12

* **Advice for Syrian refugees**
Over the next month, thousands of Syrian refugees will land in Quebec, in a foreign land, at the beginning of winter, where few speak Arabic and still fewer have a full understanding of the kind of upheaval they have experienced - first in Syria, then as they waited in limbo in Jordan, Turkey or Lebanon. Some Montrealers do know what it's like, however - because they went through it themselves not so long ago. We asked a few of them what advice they had for those following in their footsteps. (...)Originally from Idlib in northwestern Syria, Feras, 41, fled to Lebanon in 2014 after his house was destroyed in fighting between the Assad government and rebel groups, and he started receiving threats from both sides. He arrived in Montreal June 23. Hariri's advice to newcomers? "You have to give it time. "You have to breathe," Hariri says. It's not easy to sit around and wait - for language classes, for an apartment, for a job, Hariri says. "Syrians want to be Canadian just like everyone else and get the new job right away and the new car. But it doesn't work that way. You have to be patient." Learn the language - French or English, preferably both. Postmedia News (Montreal Gazette, A1/Front)

* **Privately sponsored refugees fare better in the short term, research says**
It was nearly 20 years ago that Drenka Debro set foot in B.C., she, her husband and their young son fleeing the Bosnian war that had left an estimated 100,000 people dead. Given a choice between Australia, the United States and Canada, they chose Canada - partly because of Ms. Debro's childhood memory of a beloved pair of winter boots that were called "Canadian boots" and partly because they understood Canada was a peaceful country. Beyond that, they knew little. When they learned they were to be privately sponsored by St. Peter's Church in Campbell River, B.C., they had to look up the city on a map. (...)Privately sponsored refugees are most often brought over by Sponsorship Agreement Holders

(SAH) such as a humanitarian group or a church. The St. Peter's Church, which sponsored the Debro family, is part of the Anglican Diocese of B.C., which is a SAH. Refugees can also be sponsored by a constituent group - a group of five or more Canadian citizens or permanent residents, or a community sponsor. Privately sponsored refugees often have family links in the country of resettlement. In a 2012 survey, the department's research and evaluation branch found privately sponsored refugees economically outperform government sponsored ones, at least initially. Globe and Mail, S1

Phone calls about Canada offer hope to refugee family

Mohammad Mnaahe, only a year old and not yet walking, crawls across the beige carpets in his family's rented apartment about 30 kilometres from the Jordanian border with Syria. As his brother Tamim sleeps on a yellow and red mattress on the floor and another brother, Saif, is tucked in next to his father, Mohammad plays with a laminated plastic certificate, oblivious to the value it holds for his family. His parents, however, keep a close eye on it. To them, it represents their best hope of getting out of Jordan and to Canada - proof from the United Nations of their official status as refugees of the Syrian war.(…) When word begin to spread through Syrian refugees in this town that Canada was going to be taking in many thousands - and quickly –Mohammed's father, Mjdi, said something told him he might be among them. And then, two weeks ago, the call came. Would they be interested in moving to Canada, the UN asked him, possibly as early as the end of the year? He said yes, and last week, was among 900 people called to the UN's office building in Amman to have his file reviewed for possible submission to the Canadian government program. He was there eight hours, he said - case number 698. After two 15-minute interviews, was told to await another call. That one came, too. So on Dec. 10, his entire family will go to the new Canadian processing centre at a Jordanian military exhibition facility to fill out more paperwork, have their fingerprints and other biometric information taken, be interviewed by Canadian officials, and get a medical check or an appointment for a future one. Once all that's done, they'll wait again. Canadian Press (Times Colonist, B7, Red Deer Advocate, Times & Transcript)

Family beats odds to make first cut in bid to escape grim Zaatari camp

Ahmad Lakash was already a famous man in Zaatari. His falafel restaurant is the first thing you see when you enter the sprawling refugee camp. It sits right at the top of the dusty market road that residents refer to deadpan as the "Champs Élysées."Now Mr. Lakash is envied for another reason. His family of six are the only ones among Zaatari's 79,120 residents known to have received a text message from the United Nations High Commissioner for Refugees inviting them for an interview that could put them on track for resettlement to Canada. The family, who arrived in Jordan in early 2012 after fleeing the fighting in Syria, have no idea why they made the list while their neighbours in Zaatari didn't."Maybe we'll be making falafels in Canada," the 48-year-old says with a grin, leading a tour of the family's modest home in refuge - two sparsely furnished caravans connected by a tarp that creates a chilly sitting area between them. "We won't need to take anything with us from here. We'd be ready to leave within a week." While Immigration Minister John McCallum, Defence Minister Harjit Sajjan and Health Minister Jane Philpott made a show of visiting Zaatari during a whistlestop visit to Jordan on Sunday, the UN refugee agency says that none of the several hundred names it has forwarded thus far to the Canadian government are Zaatari residents. (Mr. Lakash has only been invited for a preliminary interview with the UNHCR.
If approved by the refugee agency, the family will be given an appointment with Canadian officials who have arrived in Jordan to do additional health and security screening before refugees are invited to Canada.) Globe and Mail, A1

Complications in Turkey slow arrival of Syrians to Canada

The operation to resettle as many as 5,000 Syrian refugees from Turkey to Canada is being slowed by the additional "complexities" of the situation in that country, Canada's ambassador to Ankara said in an interview. The situation in Turkey is different from both Jordan and Lebanon, the other countries from which Canada is accepting Syrian refugees, because the Turkish government and not the UN High Commissioner for Refugees registers and keeps track of refugees in the country. The sheer size of Turkey - as well as concerns about security in the southern regions where most of the Syrian refugees are registered - create additional complications. (…) John Holmes, Canada's ambassador to Ankara, told The Globe and Mail that the Turkish government last week submitted a list of 5,000 names that Turkey was suggesting for resettlement to Canada. The Canadian embassy will now hand the list to the International Organization for Migration, which will try to establish whether those 5,000 still reside at the

addresses where they're registered by Turkish authorities, and whether those families are indeed willing to move to Canada.(...) "Our normal points of operation, Istanbul and Ankara, are not really viable," Mr. Holmes said. Among the additional challenges, he said, would be finding hospitals that are up to Health Canada standards - so that health checks can be carried out on refugees - as well as airports capable of handling the large planes the Canadian government will likely have to charter for the operation. Globe and Mail, A1

Feds to waive travel costs

Syrian refugees' arrival in Canada will be made slightly easier as the federal government waives repayment of any costs they incur getting over here. Currently, the government provides loans of up to $10,000 for government-assisted refugees to make their way to Canada. It's a sticking point activists have been fighting for years. But last week, the government announced it will waive that repayment, along with costs refugees typically have to pay for medical exams and other fees. "Given the extreme and unprecedented hardships faced by this community, Canada is upholding its humanitarian tradition by offering help and protection to those most in need," Theodora Jean, a communications rep for Immigration, Refugees and Citizenship Canada, explained in an e-mail. Postmedia Network (Toronto Sun, A5, Calgary Sun, Winnipeg Sun, Ottawa Sun, Edmonton Sun)

Ottawa urged to double Syrian refugee intake

As Canada braces for the arrival of 25,000 Syrian refugees, the man who served as immigration minister during the Vietnamese boat people crisis says Ottawa should be doing much more. Ron Atkey believes the 25,000 Syrians Ottawa is promising to resettle initially is a "noble objective" but he wants Canada to up the ante. "If Canada can do another 25,000 - that would make a significant contribution in line with Canada's contribution with the Vietnamese boat people in 1979 to 1980. It will demonstrate to the Americans that they have to do more. We'll shame them into it, similarly the Australians," says Atkey, who was immigration minister in the Joe Clark government in 1979 when 50,000 Vietnamese refugees were granted asylum in Canada. By the end of 1980, that number had risen to 60,000. "For us to take a dramatic position on the world stage is important. We won a medal from the United Nations High Commission for Human Rights. We gained a lot of prestige as a humanitarian country. I think that's consistent with Canadian tradition." Atkey, who is also a lawyer, professor and national security expert, is chair of Humanity Wins, a group of prominent Canadians who came together earlier this year to advocate for re-settlement of Syrian refugees to Canada. Toronto Star, A6

* **Ottawa urged to sprinkle refugee flow across country**

Mayors and provincial officials are putting pressure on the federal government to ensure that Syrian refugees initially settle all over the country instead of congregating in Canada's biggest cities. Details of Ottawa's plans to bring in 25,000 refugees by the end of February remain incomplete, including when the Syrians will start arriving in Canada and where they will be settled. However, there are growing concerns that a large majority of the government-sponsored refugees will be drawn to cities such as Montreal and Toronto, where thousands of privately sponsored refugees are heading in coming weeks to join large, existing communities of Syrian Canadians. Officials in the Atlantic provinces, including Halifax Mayor Mike Savage, argue that having refugees more uniformly distributed could provide a great opportunity for the region to deal with its demographic challenges. "It ties in with the needs of Nova Scotia for immigrants to come to the province, so we think there can be not only a humanitarian and compassionate side to this, but also be very good for our economy," Mr. Savage said . "All provinces and cities will likely be saying, 'We think we can play a role here and we want to have a chance to do so.' " Manitoba Premier Greg Selinger added that his province would like to welcome up to 8 per cent of the Syrian asylum seekers - about twice Manitoba's proportion of the overall Canadian population. "We know that Manitobans want to do their part in welcoming these innocent victims of war [and helping them] find a better life," he said. Globe and Mail, A1

Refugee aid groups overwhelmed

A groundswell of public generosity for Syrian refugees has left some local non-profit organizations overwhelmed by the response of Montrealers. Action Réfugiés Montréal (ARM), a non-profit organization dedicated to helping refugees and asylum seekers, has been inundated with phone calls and emails since it put out a call through social media for winter coats and boots. "We were looking for 30 or 40 coats," said

Paul Clarke, executive director of ARM. "We put out a call in early November, then it got shared on Facebook 60 times. It was oversubscribed very, very quickly," said Clarke, who has already collected more than 50 coats, some with new retail stickers still attached. And the donations keep on coming. "I went to speak at a church yesterday and there were about 30 bags of what we need, plus more, and we have very limited space ourselves," said Clarke. He dropped offthe extra clothing at the Syrian Canadian Council, but wonders whether the local refugee aid effort could benefit from better coordination by civic authorities. Postmedia News (Montreal Gazette, A3); * Radio-Canada

Rideau Hall forum may be a 'call to action'
Because things are so urgent, most of the Syrian refugees coming to Canada are being brought in directly by the federal government, rather than through private sponsors. These government-assisted refugees, as they're called, are at greater risk of failing or of falling through cracks. How can you help? A forum at Rideau Hall Tuesday hopes to tell you. Governor-General David Johnston, who convened the forum, believes the Syrian refugee crisis is simply the latest in a long line of events that challenge Canada's willingness to welcome the world. (...)Participants include federal Immigration Minister John McCallum, who returned Monday from a fact-finding mission in Jordan, provincial immigration ministers, mayors from Halifax to Victoria, leaders of non-profits that work with refugees and of other charitable organizations, representatives of the Canadian Armed Forces, aboriginal leaders, faith and interfaith leaders, and representatives of the private sector, among others. The purpose of the gathering, which is open to the media and will be televised, is for everyone to tell everyone what everyone is doing, to swap ideas and tips, and to make sure that this extraordinarily complex and multifaceted operation will come off with as few hitches as possible. Globe and Mail, A9; * CBC News;* Hill Times

Sea of red tape faces refugees looking to Canada
Consider the to-do list of a Syrian refugee who hopes to come to Canada. This isn't someone who floated on a leaky boat across the open sea last month. This is someone who has been under observation for several years in a refugee camp in Lebanon, Jordan or Turkey. He or she has registered with the United Nations, then submitted to a multiple-step, protracted interview about their life history. Next, undergone a medical exam, then provided biometric data, including fingerprints. If they pass all this and are deemed "most vulnerable," the UN grants refugee status. The most vulnerable category accounts for less than one per cent of the world's refugees. ISIS would probably get better odds if it wanted to sneak a terrorist into Canada like a guy with a plane ticket and a Belgian passport. Next, the UN selects the resettlement country. If Canada is picked, our immigration officials conduct multiple interviews and background checks overseas, including fingerprint checks. The refugee's information is crosschecked with terrorist and criminal databases. The final check is in Canada, at the airport immigration counter. Chronicle-Herald, A4

All roads lead to Toronto
Almost 80% of the privately sponsored Syrian refugees coming to Ontario will start out in Toronto. Numbers released by the federal government over the weekend detail the destinations for 4,584 refugees who are being sponsored by organizations or groups of Canadians. Ottawa's numbers don't include the 3,650 refugees the government of Quebec says it will take in by the end of the year. Ontario, meanwhile, can expect 3,318 privately sponsored Syrian refugees - 33 have arrived since Nov. 4 and 3,285 are still being processed by the government. Of those refugees coming to Ontario, 2,602 will be coming to Toronto. According to the federal government, 1,326 will come to central Toronto, 1,079 are destined for Willowdale, 156 are headed to Scarborough, 23 will go to North York, and 18 are expected to head to Etobicoke. Councillor Joe Mihevc said Toronto can "absolutely" handle the refugees. "For a city of almost three million people, my back of envelope (calculation) that's 0.01% which is not a tough number for us to absorb," Mihevc said. Dr. David McKeown, the city's chief medical officer of health, added Toronto Public Health is preparing to help with the refugees coming to Toronto. Toronto Sun, A5

* **Ontario ready to take 4,000 refugees this year**
Ontario is prepared to take roughly 4,000 of the 10,000 Syrian refugees set to arrive in Canada by the end of the year and may not need as many resources to accommodate them as previously thought, says the province's health minister. Since Ontario accounts for about 40 per cent of the country's population, it is prepared to take in that proportion of refugees, Eric Hoskins said Monday. "It will depend on the flow of refugees coming from those various countries," he said. "I think it's a better approach to understand that

we will be receiving our share. We know what that will be roughly and we're prepared within a margin on either side of that to accommodate them." Hoskins has said Ontario was looking at using recently decommissioned hospitals to house refugees on an interim basis, but now they may not be needed. "We have sites identified. Some of those sites have taken the extra step of ensuring they are prepared to accommodate the refugees, but we'll see if that type of facility is in fact required," he said. "It will depend partly on the numbers that arrive. We were thinking maybe 1,000 a day. Now the federal government is thinking somewhat fewer than that and it's over a longer period of time." Ottawa has said military bases are an option for interim housing. The federal government pushed back the timeline for settling 25,000 people from the end of this year to the end of February, so Hoskins said Ontario may not need to dedicate as many resources. Canadian Press (Waterloo Region Record, A3, Toronto Sun, Calgary Sun, Ottawa Sun, Hamilton Spectator, Times & Transcript)

Ready to serve

Some have been jailed and tortured; others, sexually assaulted while their children were forced to watch. Some fled their homes and homeland years ago and-their hope rising and falling with the passage of time - have waited in refugee camps for the world to take notice. It's not just shelter these 100 Syrian refugee families coming to London will need, but support in dealing with a range of traumas inconceivable to most Canadians. And though large teams of volunteers are working out logistics of winter coats and English-language classes for when families arrive in coming months, some area professionals are working to meet needs of the psyche and soul for people who have been dislocated and relocated. At right is a look at how London professionals are preparing to help and how regular Londoners can help: "There's a lot for (refugees) to deal with," said LloyWylie, an assistant professor in the master's of public health program atWestern University. "In the past five years in London alone, people are saying there's a higher level of trauma (among refugees) than they've ever seen." Wylie is helping lead a team that includes mental-health professionals from London Health Sciences Centre, London Inter-Community Health Centre and the Cross-Cultural Learner Centre to help refugees and immigrants. London Free Press, A3

*** Refugees coming to province expect to work hard, says Syrian immigrant**

In his six years in Moncton, Elian Elias has invested more than a million dollars in the community creating businesses, buying a home and commercial buildings and employing many Canadians. He's contributing to his adopted community in small ways too, providing free pizzas each month to a local group that's been feeding the homeless, an interesting counterpoint to the voices these days arguing Canada should take better care of its poor and homeless people before welcoming Syrian refugees. Elias is not a refugee, because he had the good fortune to come to Canada from Syria in 2009 as an immigrant before there was any sign of significant trouble in his homeland. That's all changed now, of course, as Syrians find themselves trapped in the madness of civil war and the Islamic State. He's currently struggling to get his brother and brother's family out of Syria before more violence comes to their region near the Lebanese border. Elias owns the Freddie's Pizza in Riverview and Mama's Pizza in downtown Moncton. If he can get his brother here, he will employ him and house his family until they get their foothold, just as New Brunswickers are planning to do for the 1,500 Syrian refugees expected here in the next few months. Elias is sure of one thing: the Syrian refugees who come to Moncton and the rest of the province won't need as much help as some might imagine. "The Syrians are hard workers. The Syrians who already live in Canada? You will find they almost all own their own businesses. They come here for a better life and they expect to work hard. They have that plan before they leave their country." Times & Transcript, A1

300 to 600 refugees expected to resettle in city

Fredericton is now expected to receive 300 to 600 Syrian refugees, but there is still no word on when they will arrive. The capital is also getting ready to have translated into Arabic some key documents such as Fredericton's newcomers guide and its recreation guide to help the refugees adjust. David Seabrook, Fredericton's assistant director of growth and community services, released the refugee number to the capital's council-in-committee meeting Monday night. A city task force on Syrian refugees that involves all the local agencies involved was established last week and will meet for the first time on Thursday, said Seabrook. The lead organization in the refugee settlement effort is the Multicultural Association of Fredericton, he said. (...) Mayor Brad Woodside said he and other councillors are getting calls from people who want to help. He asked where they should direct those calls. Seabrook said councillors should direct those calls to the Multicultural Association of Fredericton. He also warned that volunteers

who want to work with refugees will have to undergo a police check. Fredericton Police Chief Leanne Fitch confirmed that requirement. Daily Gleaner, A1

Universities offer their support to Syrian refugees arriving in Fredericton
St. Thomas University is planning to offer full scholarships to Syrian refugees making their way to Fredericton. A team of professors and university staff members are discussing the possibility of providing tuition and covering residence and food costs. Jeffrey Carleton, communications director with St. Thomas University, says the scholarship is still in its early stages but there could be a range of up to four scholarships. "The idea came from a number of people at the same time," he said. "There's still lots of details to be worked out but there will always be a thousand details." Carleton says international scholarships range up to $13,000 per student. Telegraph-Journal, A3

Yukoners are ready to welcome refugees
There's still some unpacking to do, but the beds are made, dishes are stacked in the cupboards and towels are in the closet as Yukoners get ready to welcome a family of 10. Raquel De Queiroz, who heads up Yukon Cares, said this morning her group spent much of the weekend getting a four-bedroom house ready. It did so with numerous donations from the community for the family of Syrian refugees it's sponsoring to come to Canada. The group has been fundraising since September to sponsor the family. While the fundraising and collecting of household donations has been underway, the paperwork and formal process has also progressed, with the family recently having had their visa interview with federal authorities. Following that, Yukon Cares was asked to submit its paperwork to the federal government for the sponsorship. "That was done and submitted on Friday," De Queiroz said. The family must now go through medical and security clearance before they can be approved to come to Canada, she added. Whitehorse Daily Star, 2/Front

Les premiers vols nolisés pour bientôt
Le ministre de l'Immigration, des Réfugiés et de la Citoyenneté espère voir les premiers avions nolisés transportant des réfugiés syriens se poser au Canada la semaine prochaine. John McCallum n'a pas voulu avancer de date précise, disant souhaiter que le premier de ces vols nolisés arrive «aussitôt que possible», soit «possiblement» dans une semaine. Le gouvernement prévoit que le premier appareil à se poser en serait un des forces aériennes du Canada, et les suivants des vols commerciaux, a spécifié M. McCallum. On prévoit attendre «d'avoir la capacité d'avoir plusieurs vols et pas seulement un» avant de fixer une première date d'arrivée, a-t-il exposé en conférence téléphonique, lundi. Presse canadienne (Voix de l'Est, 14, Le Soleil, Le Nouvelliste, Acadie Novelle, La Tribune)

What is a privately sponsored refugee?
Groups or organizations can agree to privately sponsor refugees. The federal government's plan to bring 25,000 Syrian refugees to Canada by next year relies heavily on processing thousands of privately-sponsored refugees. Around 4,511 files of privately-sponsored refugees are being processed for Canadian cities outside Quebec. Postmedia has reported the province of Quebec has more than 3,000 privately-sponsored refugee applications. According to Citizenship and Immigration Canada, sponsoring groups must agree to provide refugees with care, lodging, settlement assistance and support for approximately the first year in Canada or until the refugee becomes self-sufficient. The group has to demonstrate they have the funds to cover rent, utilities, food and dayto-day living costs. Once the sponsored refugees arrive, the sponsors are expected to help them become accustomed to Canada including assisting with the search for employment. Ottawa Sun, A10

*** Lawyers bridge gap between Canada's goodwill and caution**
Many Canadians rushed to find a way to do something to help Syrian refugees in the days after photos were published showing little Alan Kurdi's lifeless body on a Turkish beach. It's who we are, and why Canadians bear the national stereotype of being nice. Do-gooders, even. Phone calls, emails and texts ping-ponged among friends, including my own. Maybe we can sponsor a family. How hard could it be?(...) For now, let's just focus on G5s - those nice people unaffiliated with a faith group or other sponsorship agreement holder. G5s "must agree to give emotional and financial support to the refugee(s) for the full sponsorship period - usually one year," according to the government's website. But what does that mean? Then, the G5 need to provide a settlement plan and prove the group can afford the

sponsorship. Before potential G5 members even get to the application, they are urged to go to the refugee sponsorship training program website. The application makes the longform census seem like a walk in the park, a superficial glance at people's private lives. Among the documents that must be filed by at least three of the five members of the group are: the most recent T4; the most recent notice of assessment from Revenue Canada; proof from your employer confirming financial details or a letter from an accountant if you are self-employed; proof of any other income. (...)So, a group of powerful and well-connected lawyers has stepped in to bridge that gap. It began as a conversation between Jennifer Bond, a professor at the University of Ottawa's law school and faculty director of its Refugee Hub, and Jacqueline Swaisland, a Harvard-trained, Toronto lawyer who teaches a course in immigrant and refugee law at the university. They decided to expand the Refugee Hub's existing sponsorship support program by training 15 students to advise groups in the Ottawa area about the process, the liabilities and legal responsibilities. Other lawyers expressed interest and were trained as well at a fivehour workshop in October. The next night, at a forum hosted by Ottawa Mayor Jim Watson, they held a pop-up clinic for wannabe sponsors. More than 450 people showed up and close to 60 lawyers helped them. Postmedia News (Vancouver Sun, A4)

'Like a dream come true'

A Kosovo refugee who arrived at Canadian Forces Base Kingston in the spring of 1999 has some advice for potential Syrian refugees should they arrive next month and move into barracks at the base, as he had over 15 years ago. "My first thing is you came to this country, you must love and respect this country because this country is your best opportunity. It's like a dream come true for everybody," said Avni Lushaku, now 37, on Monday from Mississauga, where he now lives with his wife, Shqipe, and one-month-old son Artin. (...)He was able to learn English by volunteering at the base's Salvation Army tent for donated clothes. His mother encouraged him to volunteer and learn English at the same time as an inbetween person the volunteers and refugees. During his time in Kingston, he toured around the city and took lots of photos. He added that many volunteers took his family offthe base for home-cooked meals. "They were our families, they were our uncles, like our aunts, because we had nobody here," Lushaku said. His family's stay was short at CFB Kingston, only a month, before being shipped offto Valcartier, Que., where he had to learn French, but by the end of September when the Canadian refugee camps started to wind down, he and his family came back to Kingston to settle. Kingston Whig-Standard, A1/Front

Accueil de réfugiés syriens

Le Centre d'accueil multiculturel et des nouveaux arrivants de Saint-Jean (CAMNASJ) tiendra une séance d'information sur l'arrivée de réfugiés syriens dans la région, le mercredi 2 décembre, à 9 h 30, au bureau du CAMNASJ, situé au 165 rue Union. Le Centre vous informera du besoin de bénévoles lors de l'arrivée des réfugiés syriens au cours des prochaines semaines et des prochains mois. Le Centre expliquera également ce qu'il prévoit mettre en place afin d'accueillir, d'orienter et de soutenir les familles qui arriveront à Saint-Jean. Veuillez confirmer votre présence auprès de Sandrine Selway, agente d'accueil et d'établissement, au 642-7265 ou par courriel (sandrine.selway@sjmnrc.ca). Acadie Nouvelle, 25

*** Laurentian students eager to help refugees**

Yvonne Udowa found the weather in Sudbury to be frigid, but the people full of warmth. An international student at Laurentian University who hails from Nigeria, she said the Nickel City was as friendly as any she has visited. "Everybody here is helpful," said Udowa, a fourth-year liberal science student at LU. "Everybody here is so open and ready to help, so it was easier for me to get into the community when I came. It's so easy to get around here, the transportation system is great – the weather, not so great, but other than that, everything else is good. There are so many activities, so many multicultural associations here that I could attend or join when I came, and it helped me get used to the society quickly. It wasn't hard at all." She hopes that when a pair of refugees from Syria arrive next year to study at Laurentian, they find folks just as welcoming. Udowa is a member of the World University Service Canada local committee at Laurentian, which plans to sponsor two young Syrian refugees who will study at the university beginning next year as part of the WUSC Student Refugee Program. (...)WUSC is now working in refugee camps in Jordan and Lebanon, in co-operation with the United Nations High Commissioner for Refugees, to interview and document appropriate candidates for sponsorship. Sudbury Star (2015-11-30)

*** One great heart, united**

An opinion piece states, "It's a truism that bears repeating: We all came from somewhere else. Canadians remember this to their credit as they prepare to welcome 25,000 Syrian refugees this year and early next. Of these, New Brunswick is on tap to resettle about 1,500 in Moncton, Saint John and Fredericton. In fact, all regions of this country are old hands at this form of humanitarian aid. According to one federal government web site, "Our compassion and fairness are a source of great pride for Canadians. These values are at the core of our domestic refugee protection system and our Resettlement Assistance Program. Both programs have long been praised by the United Nations Refugee Agency (UNHCR)." The system works this way: "Refugees selected for resettlement to Canada have often fled their homes because of unimaginable hardships and have, in many cases, been forced to live in refugee camps for many years. When they arrive in Canada, they basically pick up the pieces of their lives and start over again. "As a member of the international community, Canada helps find solutions to prolonged and emerging refugee situations and helps emerging democracies try to solve many of the problems that create refugee populations. To do this, Canada works closely with the UNHCR." Crucially, "Under our legislation, all resettlement cases must be carefully screened to ensure that there are no issues related to security, criminality or health. Citizenship and Immigration Canada (CIC) works with its security partners such as the Canada Border Services Agency to complete this work as quickly as possible." Times & Transcript, A9

Welcome to Canada

A letter to the editor states, "It's not common sense that's been missing from the discussion about screening Syrian refugees, it's a surprising inability to connect a few dots. The first dot is that the terror attacks carried out in IS's name in the West were done by homegrown supporters, not Syrian refugees. Why would IS bother smuggling someone out as a refugee when it has wannabe terrorists here? The second dot is that IS in Syria is primarily made up of, not Syrians, but Sunni Muslims from Iraq and a few thousand hotheads from Europe and elsewhere. The third dot is that there are more than three million Syrians seeking refuge.Connect these dots and the unsurprising conclusion is that there is a 99.9 per cent chance terrorists are not hiding among those who want to come here.Single men included. Tight screening won't better the odds." Globe and Mail, A10

Letters to the Editor

A letter to the editor states, "Are refugees aware of difficulties here? Our federal government wants to bring 25,000 Syrian refugees to Canada. I am in complete agreement because these people are leaving everything they own behind as they run for their lives. Any civilized country could do no less. But do we hide the total truth about Canada from these people who are so desperately in need of hope? Things like a lack of jobs, a lack of decent housing, poverty and isolation among so many of our indigenous peoples, poverty among children and seniors, food banks everywhere struggling to meet the needs of an ever growing number of clients, and social assistance programs that are based on the wealth of the individual provinces (for example, a person can get a lot more on social assistance in Alberta than in a province like New Brunswick)?" Telegraph-Journal, A6

Une politique discriminatoire

Un article d'opinion déclare, « L'accueil des réfugiés syriens se double d'une politique discriminatoire inacceptable: les hommes seuls seront exclus, sauf s'ils sont gais (on se demande comment ces derniers réussiront à en faire la preuve, mais c'est une autre question). On peut certes établir des priorités dans une politique d'accueil. Ainsi, il serait normal qu'en sélectionnant les réfugiés parrainés par le gouvernement, on privilégie les chrétiens et les yézidis, qui sont les premières cibles du groupe État islamique (EI). Les chrétiens sont la minorité la plus persécutée dans l'ensemble du Proche-Orient. Quant aux yézidis, adeptes d'une ancienne religion répandue chez les Kurdes, les hommes capturés sont assassinés sur-le-champ et leurs femmes, réduites à l'esclavage. Le gouvernement a manifestement voulu, en écartant les hommes seuls, rassurer les citoyens qui craignent que des terroristes ne s'infiltrent parmi les réfugiés. Mais l'exclusion des hétérosexuels masculins, outre qu'elle est injuste, constitue une protection parfaitement illusoire. Ce que cette décision laisse entendre, c'est que tout homme musulman est un terroriste potentiel, et que les hétérosexuels portent en eux un facteur supplémentaire de violence. Pourtant, les gais, comme n'importe quels autres humains, ont produit leur lot de déviants. » La Presse, A11

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Grits firm up line between politics, PS**
Prime Minister Justin Trudeau is introducing the first code of conduct on political staffworking for cabinet ministers, aimed at drawing a "line in the sand" between politics and public service neutrality for ministerial aides. The code is part of the Open and Accountable Government guide, released last week, on roles, responsibilities and standard of conduct Trudeau expects from his cabinet. The guide is an updated version of one that the Privy Council Office prepared for former prime minister Stephen Harper in 2011. The line between politics and the public service has been blurring for decades, with experts calling for a code to govern the behaviour of ministerial staffers - the "political warriors" or "kids in short pants" who roam Ottawa's corridors of power with little accountability. The code says ministerial aides can't meddle in the work of the public service, can't give public servants orders, and that ministers are responsible for their staff's actions. The guide also changes the rules on the personal and partisan use of social media. Ministers' staff, who are hired under the Public Service Employment Act, are exempt from the hiring rules for public servants. Their job is to provide political advice to ministers; bureaucrats offer nonpartisan advice. Karl Salgo, formerly of the Privy Council Office and now executive director of public governance at the Institute on Governance, said the guide doesn't break new ground, but is the first attempt to pull together the rules - written and unwritten - in a single code that will be enforced as a condition of employment. Postmedia News (Ottawa Citizen, A1)

Clinton emails
A U.S. official expressed amazement at how deeply detested Canada's Conservative government was by some employees of the Foreign Affairs Department. That impression was described in a note sent three years ago to Hillary Clinton, who was then the secretary of state and whose emails are now being publicly released. It was contained in a message where a U.S. official described how his colleagues across the border pleaded for his help lobbying the Canadian government not to cut a program for Haiti. The U.S. special co-ordinator for Haiti said Canadians were worried about budget cuts that would have slashed down an operation from 11 employees to four, for a country that was ostensibly a major Canadian foreign policy priority. "I was a little astonished at how openly the career folks at the foreign and assistance ministries disliked their new political masters and wanted us to convince them not to cut Haiti," said Tom Adams, in a May 2012 email forwarded to Clinton and released Monday... The latest released batch includes another interesting exchange about Canada. There was delight in Clinton's office over news that Omar Khadr was being released from the detention facility at Guantanamo Bay and repatriated to a prison in his home country. The newly released emails show the then-secretary of state's response to news that the young man was being transferred to Canada: "Thank you for all you did to get this resolved." She was writing to the State Department's legal adviser -- who was ecstatic at the 2012 development. "So glad we got this done," said the adviser, Harold Koh. "After spending the last 10 years on GTMO, at least this young man finally has another chance." Canada's then-Conservative government was far less enthusiastic about approving Khadr's return, which was delayed amid sniping between Canada and the U.S. In his written decision allowing the transfer, then-public safety minister Vic Toews expressed five points of concern about bringing home a young man he described as a known al-Qaida supporter and convicted terrorist. Canadian Press (Calgary Sun, Edmonton Sun, Toronto Sun, Ottawa Sun, Winnipeg Sun, Guardian, Telegram, Hamilton Spectator, Times Colonist, Ottawa Citizen); * Presse canadienne (L'actualité)

OTHER / AUTRE

Climate talks hailed as 'an act of defiance' against terror
Pushing for a powerful climate deal, President Barack Obama called the global talks opening Monday outside Paris an "act of defiance" against terrorism that proves the world stands undeterred by Islamic State-linked attacks in Europe and beyond. Obama used his speech to more than 150 world leaders at the UN's 21st Conference of the Parties (COP21) summit to salute Paris and its people for "insisting this crucial conference go on" just two weeks after attacks that killed 130 in the French capital. He said leaders had converged to show resolve to fight terrorism and uphold their values at the same time. "What

greater rejection of those who would tear down our world than marshalling our best efforts to save it?" Obama said. Obama's remarks came at the start of two weeks of make-or-break negotiations to finalize a sweeping global agreement to cut carbon emissions and hopefully stave off the worst effects of climate change. He exhorted leaders to fight the enemy of cynicism: "the notion we can't do anything" about the warming of the planet. Prime Minister Justin Trudeau's address dovetailed perfectly with these sentiments. In his opening comments on Monday, he told delegates that Canada "will take on a new leadership role internationally." "Canada is back, my friends," Trudeau declared. "We're here to help." Associated Press (Toronto Star, A1, Telegraph-Journal, Times & Transcript); Canadian Press (Record, A1, Whig-Standard, Red Deer Advocate, Telegram, Guardian, Chronicle-Herald, Cape Breton Post, Hamilton Spectator, Times Colonist, Daily Gleaner); Globe and Mail, A4; Postmedia News (National Post, FP7); * Associated Press (Acadie Nouvelle, 22)

NATO eager to size up Grits as ISIL threat emerges in Libya

Stephane Dion hasn't even arrived yet in Brussels, but a lineup is already forming to meet Canada's new foreign affairs minister. Canadian staffat NATO headquarters are fielding requests from alliance members keen to size up the Liberal government's new point man on the evolving confrontation with Russia and the growing influence of the Islamic State of Iraq and the Levant in Libya. Dion will join foreign ministers from the other 28 member countries on Tuesday and Wednesday, several of whom are eager to take stock of Justin Trudeau's plan to end the bombing campaign against extremists in Iraq and Syria, instead refocusing the military effort on training local forces. While NATO is not formally involved in the 62-country, U.S.-led coalition against ISIL, its members see Canada's planned actions as important.
One of Dion's most important tasks will be to reassure allies the country remains stalwart, especially in light of the terror attacks in Paris and the security lockdown in Brussels. Canadian Press (Whig-Standard, B1/Front, Guardian, Waterloo Record, Spectator); * Ottawa Sun, A9; * La Presse Canadienne (La Tribune, 33, Le Droit)

*** U.S. targets 2016 to end ISIL airstrikes**

A top U.S. general involved in the bombing war against ISIL says he hoping the campaign will be wrapped up by the end of next year. Canada is expected to withdraw its six CF-18 fighter jets from the coalition campaign before March. Lt.-Gen. Charles Brown Jr., who is in charge of the U.S. air force Central Command, said ISIL hasn't been able to mount any major ground offensives during the past several months. "By the time we get to the end of 2016, I hope to be pretty well done with Daesh," Brown told the Air Force Times newspaper, using an Arabic term for ISIL. "That's probably aspirational, but I think we are putting pressure on Daesh. We have not seen from Daesh any major offensive in the past couple of months. Most of the stuff we see is more harassing attacks. So they don't have the staying power that they're going to need to survive what we're putting on them." It's not the first time a U.S. military leader has talked optimistically about ISIL's waning military capabilities. Canadian and U.S. senior officers said this year the extremist group was on the verge of defeat, only to have ISIL forces go on the offensive. Prime Minister Justin Trudeau has said he is sticking to his election promise to remove the CF-18s. Postmedia News (Edmonton Journal, N6, Ottawa Citizen)

*** Conflict investigation involving former Alberta premier to be reviewed**

The Alberta government is launching an outside review of an investigation two years ago into conflict-of-interest allegations involving former premier Alison Redford. The 2013 investigation looked into how a Calgary law firm with close ties to Redford was awarded the contract to represent Alberta in a lawsuit against tobacco companies. One of the partners in the law firm was Redford's former husband, who remained a strong Conservative supporter. Neil Wilkinson, the ethics commissioner at the time, cleared Redford of any conflict in awarding the multibillion-dollar contract while she was justice minister. The NDP government says concerns have emerged that Wilkinson might not have had all the relevant information needed for his investigation. The review is to be handled by retired Supreme Court justice Frank Iacobucci. "These allegations are serious. We believe that the best path forward to ensure an objective review is to have that review performed externally," Alberta Justice Minister Kathleen Ganley said in a statement. "Our government is committed to transparency and accountability, which is why we're taking action." Canadian Press (Times Colonist, A8, Calgary Sun); Postmedia News (Calgary Herald, A3, Edmonton Journal); Edmonton Sun, A7

*** From observation to activism, one Canadian man's experience of Syria**
When Cody Bergerud left Saltspring Island for northern Syria, he didn't tell anyone where he was going. "It just made things easier," he says. No fights with family. No awkward conversations with the authorities, at least until he came back. Unlike other Canadians who have travelled to the region, Mr. Bergerud wasn't driven by the thought of taking up arms for or against the terrorist group the Islamic State. His is not that kind of story. The University of Victoria political philosophy student was in northern Syria to witness what he calls a social revolution. Amid the country's years-long civil war, the Kurdish population in the north has gained a level of autonomy. A website for the Lions of Rojava, which is aligned with the Kurdish People's Protection Units (YPG), describes its society's three principles as direct democracy, gender equity and sustainability - all of which it pursues while within firing range of the Islamic State. Mr. Bergerud, 26, went to Rojava to observe. He arrived in Syria in March, slipping into the country through the northeast after a 2 1/2-week stint as a volunteer at a Turkish refugee camp. While at the camp, Mr. Bergerud says he primarily helped on the construction side. He also took time to play with some of the children. Getting into Syria, he says, was fairly simple. "I made friends, and they were able to connect me with people who got me across the border," he said. "They pick out a good spot and you kind of just run over the border. The whole process takes three to five minutes." Mr. Bergerud met five or six Canadians while he was in Rojava. The youngest was 24, while the oldest was 67. He never met John Gallagher, a Canadian who was killed in Syria earlier this month while fighting with the YPG against the Islamic State. Globe and Mail

INTERNATIONAL

*** Key suspect in Paris attacks may have eluded dragnet, fled to Syria**
Paris attacks suspect Salah Abdeslam may have fled to Syria, according to reports quoting French intelligence services. A major manhunt is under way for the Belgian-born French national who has been on the run since the Nov. 13 attacks, which killed 130 people. But investigators are now working under the assumption the 26-year-old has slipped the net and is now in Syria, a source close to the investigation and a counter-terrorism source told CNN. The Islamic State of Iraq and Levant, which controls a large swathe of territory across Syria and Iraq, has claimed responsibility for the attacks. French police have issued an international arrest warrant and a wanted poster for Abdeslam, describing him as highly dangerous. He rented the VW Polo and Renault Clio cars used in the attacks. Investigators say he went to Belgium from France the day after the attacks in a VW Golf, despite being stopped by French police along the way in routine road checks before his name was circulated as a suspect. His brother Brahim died in the attacks. Postmedia News (National Post, A12)

*** La NSA ne stocke plus les données des appels**
C'est une victoire pour Edward Snowden, qui avait révélé l'ampleur des pouvoirs de surveillance de la toute puissante agence de renseignement américaine NSA: depuis dimanche, l'agence ne stocke plus les données liées aux appels téléphoniques des Américains. La révélation en juin 2013 par Edward Snowden que les métadonnées (horaires, durée, numéros appelés) des appels étaient conservées dans les gigantesques ordinateurs de la NSA avait provoqué la stupeur et l'indignation chez beaucoup d'Américains. En juin dernier, le Congrès avait adopté une loi mettant fin à cette collecte et introduisant un nouveau système qui permet à l'agence de renseignement de continuer à accéder si nécessaire aux données des appels des Américains, avec un contrôle juridique renforcé. Si elle ne dispose plus elle-même des données, la NSA peut toutefois les exiger auprès des compagnies téléphoniques. La NSA pourra toujours avoir accès aux données concernant les appels téléphoniques d'un suspect et les correspondants de ce suspect. Mais ces recherches seront moins «efficaces» et «prendront plus de temps», affirme Stewart Baker, avocat spécialiste des problèmes de cybersécurité et surveillance électronique. AFP (Le Soleil, 21; Le Devoir)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PS.PSPMediaCentre/CentredesmediasPSP.SP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
January 20, 2016 / le 20 janvier 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Goodale calls refugee integration crucial
Public Safety Minister Ralph Goodale says it's vital that resettled Syrian refugees are successfully integrated into Canadian towns and cities, not just from a social and cultural perspective, but from a public safety perspective. ***"It's extremely important that they settle well and successfully and we and the settlement agencies and the provinces and the cities need to work at that to make sure that it is successful. If we, being Canada, are going to maintain our very successful efforts so far at pluralism, at diversity and inclusion ...then we've got to be among the best in the world at counter-radicalization. "Because if we fail to detect the causes or the signs, or we don't have the capacity to intervene at the right point and then don't make the intervention successful, then those values of openness and the plural nature of the country will be in jeopardy,"*** he said***. "And that's the very essence of Canada, so we've got to do outreach and counter-radicalization very well."*** Three months into his job in charge of Canada's national security agencies, which have been intimately involved in the resettlement project, **Goodale** says one of the priorities set out in his ministerial mandate letter was to boost efforts to counter violent extremism. At this time, he will say only that ***"a lot more attention"*** must be paid to outreach efforts, and the question of increasing funding for such programs and research into what leads people to become radicalized will be answered ***"a ways down the road."*** (...) **Goodale** stressed the importance of outreach, and research efforts ***"to identify what contributes to radicalization, how the process works."*** He said a national cross-cultural roundtable is a useful forum for different faith leaders, police agencies and social service agencies to work together.

But he said there is a definite need for more such groups on a local level. There are some scattered across Canada, often led by local Muslim leaders, he said. But it's a "***massive project***," he admitted. Toronto Star, A10 (Cambridge Times)

Tory policy up for review

The Trudeau Liberals will review controversial directives enacted by the Harper government that allow for the sharing of information even when it might lead to torture, says the **public safety minister**. The ***"troubling set of issues"*** raised by the foreign information-sharing policy ***"will be raised in the course of our consultations"*** on the overall national security direction of the new government, **Ralph Goodale** said in a recent interview with The Canadian Press. The news follows pressure from human-rights and privacy advocates to conduct a wide-ranging examination of security policies introduced by the Conservatives, booted from office in the October election. The federal policy on foreign information-sharing has been roundly criticized for effectively condoning the torture of people in overseas prisons, contrary to international law and Canada's United Nations commitments. A four-page 2010 framework document, released under the Access to Information Act, says when there is a "substantial risk" that sending information to, or soliciting information from, a foreign agency would result in torture - and it is unclear whether the risk can be managed through assurances or other means - the matter should be referred to the responsible deputy minister or agency head. In deciding what to do, the agency head will consider factors including the threat to Canada's national security and the nature and imminence of the threat; the status of Canada's relationship with - and the human rights record of - the foreign agency; and the rationale for believing that sharing the information would lead to torture. Canadian Press (Waterloo Record, A7, Whig-Standard, Toronto Star, Ottawa Citizen)

* **Dozens of families with no-fly list stories contact Ontario boy's mother**

It turns out the little Ontario boy who's been having trouble boarding airplanes is far from alone. The whirlwind of publicity about six-year-old Syed Adam Ahmed's difficulty at the airport has prompted dozens of other families with similar stories to contact Khadija Cajee, the boy's mother. Twenty-one of them agreed to be mentioned in a letter that Cajee has sent to federal cabinet ministers involved in the high-profile issue. **Public Safety Minister Ralph Goodal**e promised to investigate after Adam's father, Sulemaan Ahmed, tweeted a photo from Toronto's international airport that appeared to show the boy's name with a "DHP" or "deemed high profile" label and instructions on how to proceed before allowing the youngster to check in. They were trying to board an Air Canada flight Dec. 31 to Boston to see the NHL Winter Classic. Tales of other children with the same sorts of travel challenges soon emerged. And now Adam's mother has become an unofficial liaison with the Liberal government on behalf of many families.. After Adam's case hit the headlines, **Goodale** said his officials had reminded airlines they don't need to vet children against Canada's no-fly list. His department is also exploring possible changes to the Secure Air Travel Regulations that would help identify those who have similar or the same names as people on the no-fly list, but are not the intended targets. In addition, **Goodale** indicated the no-fly regime - officially known as the Passenger Protect Program - would be examined during broad public consultations on Canada's overall security framework. In a statement at the time, Adam's parents welcomed **Goodale's** announcement, saying he "addressed several key points that we asked for."... However, it's difficult to understand exactly why he and the other young travelers have been stopped at the airport, in part due to the quiet use of U.S. air-security lists in Canada. Other countries are at liberty to develop their own rules for their own purposes, **Goodale** said in a recent interview with The Canadian Press.***"But it can have a spillover effect that is very difficult to manage. We'll obviously look at that in the process of the consultation that we're going to undertake with the airlines and with the general public. It's just critically important to get this balance right."*** Canadian Press (CTV News, Guardian, Cape Breton Post, Telegram)

Canada is increasing its intelligence efforts

An opinion piece by Wesley Wark states "There was nothing said on the campaign trail, nothing promised in the election platform, nothing laid down in the ministers' mandate letters made public after the Trudeau government came into office. But as the Liberals struggle to define a revamped military mission in Iraq and Syria and come under pressure to respond to a recent spate of terrorist attacks that took Canadian lives in Indonesia and in Burkina Faso, the government is increasingly turning to a hidden dimension of Canadian statecraft for some answers. Intelligence, or in the popular parlance, spying, is increasingly on

the lips of Canadian ministers... Dion could have a look inside his own department to see whether he is satisfied about the resourcing of the little-known "Global Security Reporting program" and whether Global Affairs Canada has the analytical skills that are needed. **Ralph Goodale, the public safety minister**, could consider the question of whether one key intelligence agency in his portfolio, the Canadian Security Intelligence Service, can really perform well as a hybrid domestic and foreign intelligence agency." Postmedia News (Ottawa Citizen, C3)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** New HQ for flood forecasters**
Manitoba's flood forecasters have ditched their cramped headquarters in a west Winnipeg industrial park for roomier digs - equipped with $170,000 in new equipment - on Broadway. No longer confined to cubicles and a small boardroom, they will now judge the seriousness of impending floods in a "war room" adorned with computer monitors that provide real-time information on weather, accumulated precipitation, snowpack levels and other critical information. Improved technology and an expanded workspace for flood forecasters were among a host of recommendations resulting from the 2011 Flood Review Task Force report, issued in 2013. Winnipeg Free Press, A5; CBC.ca

*** New report adds billions to cost of oil spill offsouthern coast**
Environmental and risk assessments for projects that would increase tanker traffic in southwestern B.C. fail to consider billions of dollars in potential social, economic and environmental impacts, according to a new report on the region by the Raincoast Conservation Foundation. The environmental assessments required by senior governments are much too narrow and fail to consider the broader impacts of marine traffic on the ecological health of the region, which includes the Strait of Georgia, Juan de Fuca Strait and Puget Sound, argue the authors of the 108-page report Our Threatened Coast. The Salish Sea's 7,000 kilometres of intricate coastline support ecosystem services from tourism and recreation to flood protection, climate regulation and fish habitat worth tens of billions of dollars, according to studies cited by the authors. Vancouver Sun, A5; Times Colonist

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Questions swirl about our role
Defence Minister Harjit Sajjan has been touting the potential for Canada's military to help gather intelligence in Iraq in the battle against Islamic extremists. But with no recent history of meaningful involvement in Iraq or Syria, a scarcity of Arabic speakers, and a lack of intelligence-gathering equipment such as drones, how much of a contribution can Canada's military make? In late December, Sajjan told journalists that the Liberal government is considering contributing an intelligence capability to the war against the Islamic State, including helping improve the abilities of Iraqi security forces to target extremists. He suggested the Canadian Forces have technology to play this role but didn't specify whether that would be equipment on the ground or in the air. In other interviews, the minister has stated Canada's intelligence capabilities are second to none and the government was looking at how to increase that in the Iraq war... The federal government's electronic spy agency, the Communications Security Establishment, could play more of a role, but it is already monitoring phone calls and emails of Islamic extremists. The Canadian military doesn't have any long-range drones, such as those used by the U.S. and Britain to gather intelligence or target and kill ISIL leaders. Postmedia News (Ottawa Citizen, A6, London Free Press, Whig-Standard, Vancouver Sun)

Terror charge dropped but Quebec woman denied passport
Nearly two years after a court stayed charges against Mouna Diab, who had been accused of smuggling arms parts to the terror group Hezbollah, the government is still balking at granting her a passport. The National Post has learned that Diab, 30, filed a motion with the Federal Court last month, claiming Ottawa is infringing her Charter rights by refusing to act on a passport application she made in June 2014. The passport application came after the Crown abruptly dropped charges against Diab, who was arrested at

Montreal's Trudeau airport in 2011. A native of Lebanon, Diab immigrated to Canada in 1993 as a seven-year-old and gained Canadian citizenship two years later. When she was charged with committing a crime for the benefit of a terrorist group, the Royal Canadian Mounted Police issued a news release alleging she was "acting under the direction of a contact person in Lebanon who is associated with Hezbollah." She faced a second charge of violating a United Nations arms embargo of Lebanon. But on April 17, 2014, a federal prosecutor requested a stay of proceedings, declaring in a brief statement that "there was no longer a reasonable prospect of conviction." Her passport had been revoked following her arrest. When she applied for a new one she was told her request required "a second level of examination" and would not be processed within the standard time. Her lawyer, Richard Prihoda, said she was interviewed for 90 minutes by two Passport Canada agents in October 2014 and was told a decision was imminent. Whig-Standard, B1/Front (National Post)

*** We can't go backwards on terrorism**

If charity begins at home, so does national security - specifi cally at the House of Commons. Prime Minister Justin Trudeau is advised to remember this in the upcoming weeks, as Parliament resumes sitting and he has to decide whether the security measures of the previous Conservative government are too strong, too weak or just right. You know Trudeau has never discovered a security or defence scenario he considers too weak. He hypocritically voted for the Tory Anti-Terrorism Bill (C-51) while in Opposition because if there is anything Trudeau understands it is optics. With terrorist attacks, including a recent assault on Parliament Hill by an ISILinspired, lone-wolf fanatic named Michael Zehaf Bibeau, in everyone's mind, Trudeau reasoned (or at least received the correct advice) that he had better not appear too soft on terrorism with an election around the corner. Incredibly, the nattering Trudeau national media supporters now applaud Justin's "strategic" (read: cynical) decision to side with Stephen Harper. More incredibly, in the wake of outrageous terrorist attacks across Europe, and with the recent RCMP revelation that lone gunman Bibeau would have had a tough time pleading not guilty by reason of insanity in a court of law, Trudeau is prepared to pounce on the anti-terrorism act, suffi-ciently neutering its efficacy to the point of rendering it null and void. Ottawa Sun, A6

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Lawyer lands discharge for angler caught with pot at border

A New Jersey man avoided a criminal record on Tuesday for entering Canada with 14 grams of marijuana in his vehicle last year. However, Matthew Simonelli has likely earned himself trouble crossing the border, Judge Henrik Tonning noted in Saint John provincial court. The judge accepted the arguments from defence counsel Charles Bryant to grant the 30-year-old, Toms River, N.J., native an absolute discharge for possession of marijuana at St. Stephen on Sept. 9. (…) Federal Crown prosecutor Peter Thorn related in court that Simonelli and his wife crossed the border at St. Stephen and declared two expensive bamboo fishing rods. The Canada Border Services Agency officer discovered that one Ryan Mockler tried to bring these same rods into the country earlier but he was deemed inadmissible to Canada, Thorn said. Border agents searched Simonelli's vehicle and found the marijuana plus $600 U.S. in a black shoulder bag, the prosecutor said. The agents investigated further and found messages on Simonelli's cellphone "that made a reference to other drugs and pills being contained in a container or cooler," Thorn said. The border guards searched the vehicle but found nothing, Thorn said. The agents issued a civil penalty of $250 and turned the matter over to the RCMP. Telegraph-Journal, B2

Charges won't affect citizenship bid, says lawyer

The lawyer of a stateless man who has again been charged with drug crimes says the new charges will not affect Deepan Budlakoti's efforts to be declared a Canadian citizen. Yavar Hameed said he is waiting to hear back on his application to the Supreme Court of Canada for review of a Federal Court of Appeal decision "relating to the factual and legal question of whether or not (Budlakoti) is a Canadian citizen." The Citizen reported Monday that Budlakoti was charged Dec. 18 with possessing drugs for the purpose of trafficking and possessing property obtained by crime. He was arrested at his Gatineau apartment by the Gatineau police anti-gang squad in a raid that turned up nearly $10,000 worth of cocaine, a semi-automatic handgun and ammunition. "These charges have no bearing on that application," Hameed said in a statement to the Citizen. "In terms of removal prospects under immigration law, the new charges do

not make him a citizen of India or any other country, so his removal is still unenforceable in law." (…)Budlakoti learned of his unusual citizenship status in 2010 when he was sentenced to three years in prison for weapons and drug trafficking. Officials said the serious nature of those convictions necessitated deportation, but Indian authorities refused to take him. Ottawa Citizen, A4

And the red tape award goes to ...
We have a winner. Stewardship Ontario, Halifax Regional Municipality and Canada Border Services have each received a Paperweight Award from the Canadian Federation of Independent Business (CFIB). The CFIB's annual list, provided exclusively to the Toronto Sun, gives top "honours" a municipal, a provincial and a federal agency that creates the most red tape for small business owners. CFIB vice-president Satinder Chera said he hopes the recognition helps spur change. (…) The federal award goes to Canada Border Services Agency for its website. With no warning, the CFIB says the federal agency dropped a section on its website which included call centre numbers for small business owners. No timeline has been given for its replacement. Toronto Sun, A12 (Edmonton Sun, Winnipeg Sun)

Des impacts pour la région
Les besoins des Canadiens en produits laitiers ont augmenté de 18 % en 2015. La vente de crème et de beurre a connu une hausse marquée, mais celle du lait ne cesse de diminuer depuis quelques années. Et même si le Saguenay-Lac-Saint-Jean a connu une bonne année au niveau de la production, la baisse mondiale du prix du lait a eu des conséquences sur les agriculteurs. (…)« Nous voulions dresser un portrait de la situation et discuter des perspectives pour l'année 2016 avec les producteurs de la région. Évidemment, nous parlons des ventes, des quotas, mais aussi des différents accords et du contrôle des frontières. Mais je dois dire que depuis l'élection fédérale de l'automne dernier, nos producteurs ont une bonne compréhension du Partenariat transpacifique et de la gestion de l'offre, qui sont devenus des enjeux électoraux. En 2016, notre regard sera surtout tourné vers l'accord entre le Canada et l'Europe et vers le contrôle des frontières. Le Partenariat transpacifique nous fera moins mal que l'accord Canada-Europe, qui n'a toujours pas été conclu. On peut dire que ce sera encore une fois une année très politique », a indiqué Daniel Côté, le président régional des Producteurs du lait. Le Quotidien, 16 (La Presse)

Lametti on CETA: 'We'll get this deal to work'
Canada's new government is keeping an "open mind" when it comes to the controversial investor-state arbitration clauses in its proposed Comprehensive Economic and Trade Agreement with the European Union, says David Lametti, the Liberal parliamentary secretary for Trade Minister Chrystia Freeland. (…) Heading off another dispute with the United States over softwood lumber is another priority for the government, as is exploring free trade with China and pursuing Canada's stalled free trade talks with India, said Mr. Lametti. "A trade agreement with China, could it be reached, would be a good thing" if it was "done right," he said, adding the government has already begun to explore the possibility of trade talks with China in "very concrete ways." (…)The government's consultation process for the Trans-Pacific Partnership is another priority, said Mr. Lametti. Ms. Freeland has already spoken with at least 80 groups and individuals about the deal, and other ministers have also discussed the deal with stakeholders, including Finance Minister Bill Morneau and Agriculture Minister Lawrence MacAulay, he said. Mr. Lametti downplayed the importance of the signing ceremony for the deal, expected to take place Feb. 4 in New Zealand. The government still has not decided whether it will sign or ratify the agreement, he said. Whether or not to ratify the TPP is the key decision, he said, adding, "signing really isn't all that important." The TPP and CETA cover many of the same issues, with chapters ranging from competition policy to telecommunications and tariffs. The government is taking a more cautious approach to the TPP primarily because the Liberal politicians now in power have not had as much time to examine the deal, the text for which was only revealed to them during this summer's election campaign. Embassy

* **Canada – New Electronic Travel Authorisation effective 15 March 2016**
On 15 March 2016 the Canadian government will enforce the new Electronic Travel Authorisation (eTA) program. The eTA process went into effect in August 2015 but will not be mandatory until 15 March. The eTA is an online registration system that travellers access online. eTAs are valid for five years, or until the expiration date of a passport, whichever comes first. The eTA requirement applies to travelers who do not need a visa to enter Canada and who are planning to arrive by air. Visa exempt countries include the UK,

Japan, Australia, Korea, countries in the European Union and more. The eTA requirement does not apply to citizens of the US and it is not required if a person is entering at a land or sea port of entry. Nationals of certain visa-required countries (Brazil, Bulgaria, Mexico or Romania) who hold a current US non-immigrant visa, or who have held a Canadian visa in the past ten years, will be allowed to enter Canada with an eTA instead of a visa. This special visa exemption may not, however, be in place by 15 March 2016. Relocate Magazine

Stabbed in the back

Stabbed in the back, resident Patrick Mullin concluded bluntly. Yes, you were, Olde Sandwich Towne. By the very people you elected to represent you. The stately and historic John L. Forster Secondary School, once a hub on Windsor's vulnerable west side, now belongs to Matty Moroun, block-busting, neighbourhood-destroying owner of the Ambassador Bridge. It's not like the public school board didn't know the bridge company wanted - needed - this property. "There was an awareness the bridge company would be a potential buyer," board spokesman Scott Scantlebury admitted to the Windsor Star's Dave Battagello. The company has been hovering, waiting to snatch it, for more than a decade. The school's playing field off Felix Avenue is next to the site of a proposed new truck inspection plaza that the company needs for its planned twin span. (…) It's not like the trustees didn't know the bridge company. Everyone in Windsor knows the bridge company. It's the company that bought more than 100 houses on Indian Road, Edison Street, Bloomfield Road and elsewhere, boarded them up and left them to rot, creating a swath of blight, the scene of fires and rodents, that scars the west side. All for a new span that it doesn't have permission to build. Windsor Star, A2

*** Plaza upgrades approved for Lewiston-Queenston Bridge**

The plaza on the U.S. side of the Lewiston-Queenston Bridge is scheduled for a $50 million modernization project. U.S. Sen. Charles E. Schumer, D-N.Y., announced Tuesday afternoon that U.S. Customs and Border Protection and the U.S. General Services Administration have signed off on funding for the effort. (…) "The Lewiston-Queenston Bridge is a critical artery to cross-border commerce and is the lifeblood of Western New York's regional economy – but the U.S. plaza has needed a major upgrade for years. CBP and GSA have heeded our call and finally approved this $50 million expansion to the plaza is great news for Buffalo and Western New York," Schumer said. (…) Niagara Falls Bridge Commission Chairwoman Kathleen Neville praised Schumer's efforts. "The funding of the Lewiston Plaza project is an important regional trade and transportation priority that will have immense economic benefits for both Western New York and Southern Ontario," she said. Lockport Union-Sun & Journal; Glens Falls Post-Star

*** SI eyes Canada's labour mobility opportunities**

FOREIGN Affairs Minister Milner Tozaka has confirmed Solomon Islands Government's interest to engage in Labour Mobility opportunities with Canada. And to further strengthen relationship between Government and people of both countries, the Mr Tozaka said that plans are underway for the Solomon Islands Prime Minister, Manasseh Sogavare to make a historical visit to Canada and hold discussions on a number of important bilateral issues including labour mobility arrangements, clean energy and to also seek export opportunities for the people of Solomon Islands. These commitments were expressed by Minister Tozaka during his meeting in Honiara last week with the visiting Chairman of Canadian International Training & Education (CITREC) and Solomon Islands Honorary Consul General Mr. Ashwant Dwivedi. (…) "Canada has significant job opportunity which Solomon Islanders can be engaged into as temporary foreign workers. There is no doubt Hon. Minister that almost 80 per cent of Solomon Islands youth population is unemployed and this is an opportunity which can with proper training and education help see Solomon Islands nationals being employed by a Canadian employer," Chairman Dwivedi said. Soloman Star

*** Deadly Montrose hit-and-run suspect arrested at US-Canada border**

A man accused in a deadly hit-and-run accident in Montrose earlier this month is now behind bars in North Dakota. Matthew Alan Putterman is charged with failure to stop and render aid. He was arrested by border agents while trying to cross into Canada. Police say Putterman is responsible for the January 8 death of 23-year-old Michael Alexander Hill. Hill was struck and killed by a red-light runner as he tried to

cross Westheimer at an intersection near Taft. The driver sped off. Officials say Canadian border patrol officials noticed the damage to his vehicle and found text messages between him and his sister talking about the accident and ways to fix his damaged car. KTRK-TV (2016-01-19)

Population issues symposium topic
An editorial states, "Islanders are encouraged to attend a public symposium Thursday that will discuss Amish settlers to P.E.I. and the Temporary Foreign Worker Program. (...) Population change has always been at the core of the development of small islands - and it is no different on P.E.I. Every day the public media deliver news about some aspect of population: youth outmigration, rural depopulation, an aging workforce, temporary foreign workers, refugees, wealthy immigrant investors. The symposium will provide an opportunity for the public to hear about and contribute to the debate on several of the salient population issues that are crucial to the future of P.E.I." Guardian, A6

Weighing our privacy against security
A letter to the editor states, "Re: Thousands flagged for scrutiny by Canada's air screening system, Jan. 15. With a spike in terrorism over the past 15 years, governments around the world have moved to enhance border security. At first it was seen in more flight security and stricter travel laws but with advances in computer technologies security agencies have turned their attention toward spying on their own citizens. Agencies like the NSA have inserted themselves into the homes of almost every U.S. family, and even share data with other countries. In light of revelations into just how widespread government surveillance is, thanks to whistleblowers like Edward Snowden, a global debate has erupted on the ethical implications. Do governments have the right to collect data on their own citizens without their consent? And should personal freedoms like privacy be sacrificed in the name of security?" Toronto Star, A12

CYBER SECURITY / CYBERSÉCURITÉ

*** Beefing up our cyber defences**
An opinion piece states, "With cyber attacks steadily increasing in sophistication, frequency and magnitude, we must ask ourselves whether Canada is ready to meet the challenge these threats pose to our economy, national security and the overall wellbeing of Canadians. Unfortunately, when compared to the United States, the United Kingdom or Germany, Canada is clearly lagging in terms of cyber readiness. This is in part due to a lack of Canada-specific data on the types of cyber attacks affecting the public and private sectors in this country. While the pending mandatory data breach notification provisions under the Personal Information Protection and Electronic Documents Act will likely help in this regard, the notification requirement will be limited to personal information and won't cover cyber attacks involving the theft of intellectual property, trade secrets or other types of critical business information. Within this environment, it's understandable that the public and private sectors have struggled to develop an effective and comprehensive cyber strategy." National Post, A9

*** Take cybersecurity seriously: specialist**
SplashData Inc., one of the leading providers of password management applications, just came out with its list of the worst passwords of the year. Not surprisingly, the worst ones are the easy numeric progressions such as 123456 and the word "password." That sort of careless online presence is keeping cyber-security specialists such as Jay Smith busy. Smith, an information security consultant with Winnipeg-based Online Business Systems, says even if someone's online activity does not include anything that's deemed valuable enough to steal, there is still a responsibility to avoid being used as a patsy or middleman from which nefarious cyberactivity could be launched. Smith gave a presentation Tuesday to the Information and Communications Technology Association of Manitoba. Winnipeg Free Press, N/A

LAW ENFORCEMENT / APPLICATION DE LA LOI

Mounties sent to help authorities in Burkina Faso
RCMP officers have been dispatched to Burkina Faso to help local authorities after more than two dozen people - including six Canadians - were killed in a terrorist attack. A government official, speaking on condition of anonymity, says the Mounties will assist officials with victim identification and paperwork so the bodies of Canadian victims can be returned home. Six Quebecers on a humanitarian mission were killed in Burkina Faso's capital of Ouagadougou last week during an attack carried out by al-Qaida. Four of the dead were from the same family: Yves Carrier, his wife Gladys Chamberland, their adult son Charlelie Carrier and Yves' adult daughter, Maude Carrier. Adam Barratt, a spokesman for Foreign Affairs Minister Stephane Dion, says the department's priority is the families of the victims. He says departmental resources in Ottawa and overseas will be used to help repatriate the victims as fast as possible. Postmedia Network (Chronicle Herald, A9, Red Deer Advocate, Guardian, Edmonton Sun, Calgary Sun, Times Colonist, Winnipeg Sun, Ottawa Sun, Times and Transcript); Journal Montreal, 13; Gazette, A3; Journal Quebec, 7

*** Terror charge dropped but still no passport**
Nearly two years after a court stayed charges against Mouna Diab, who had been accused of smuggling arms parts to the terror group Hezbollah, the government is still balking at granting her a passport. The National Post has learned that Diab, 30, filed a motion with the Federal Court last month, claiming Ottawa is infringing her Charter rights by refusing to act on a passport application she made in June 2014. The passport application came after the Crown abruptly dropped charges against Diab, who was arrested at Montreal's Trudeau airport in 2011. A native of Lebanon, Diab emigrated to Canada in 1993 as a seven-year-old and gained Canadian citizenship two years later. When she was charged with committing a crime for the benefit of a terrorist group, the Royal Canadian Mounted Police issued a news release alleging she was "acting under the direction of a contact person in Lebanon who is associated with Hezbollah." She faced a second charge of violating a United Nations arms embargo of Lebanon. But on April 17, 2014, a federal prosecutor requested a stay of proceedings, declaring in a brief statement that "there was no longer a reasonable prospect of conviction." Her passport had been revoked following her arrest. When she applied for a new one she was told her request required "a second level of examination" and would not be processed within the standard time. Her lawyer, Richard Prihoda, said she was interviewed for 90 minutes by two Passport Canada agents in October 2014 and was told a decision was imminent. "Everybody keeps saying a decision is going to come soon, but here we are almost two years later, and nothing has been done," he said. He would not speculate on why her application is being held up, but described her arrest and the subsequent charges as "a tempest in a teapot." The federal attorney general has declared its intention to oppose Diab's request for a court order requiring the Department of Citizenship and Immigration to act on her application. The department would not comment when asked why Diab's passport application has been delayed. "As the matter is before the court, it would be inappropriate to comment," department spokeswoman Jessica Seguin said. This would not be the first time the government has used its passport powers against people who have come under RCMP scrutiny. The government has had the power to refuse or revoke passports on security grounds since 2004. The section was used to deny a passport to Fateh Kamel, who returned to Canada after serving prison time in France for terrorism-related offences. In 2014, Ali Sbeiti, an Iranian-trained Montreal imam, had his passport revoked and was informed he was a "subject of interest" in an RCMP national security investigation. National Post, A5

Crime Stoppers plays vital role
If you were driving past the Lunenburg County RCMP detachment in Cookville during the late afternoon of Jan. 8 you may have seen two hardened criminals being apprehended by detachment staff. You may also have seen those same criminals, in handcuffs and leg irons with ball and chains hampering their walking, being forced to raise the Crime Stoppers flag on the flag pole in front of the RCMP detachment. January is National Crime Stoppers Month and those two hardened criminals, Fenton Dibbin and Marlene Mercer, are volunteers with Lunenburg County Crime Stoppers. This month, several of the volunteers with the local organization will be at retail locations in the county promoting Crime Stoppers and the work that the organization does to support local police officers in their work. Crime Stoppers is a non-profit

organization that combines the public, media and police in a crime-solving effort. The simple premise of the program is to use the media to ask the public to get involved in assisting the police by identifying suspects involved in criminal activities. It is funded by donations from the public, service groups, organizations and through fund raising initiatives, emanating from the board of directors of local Crime Stoppers chapters. Postmedia Network (Chroncile Herald, S4)

Trial on hold over photo issue
The trial of a man charged with several sex-related and child pornography crimes had to be delayed Tuesday because some of the images in the disclosure package had not been altered to render them non-pornographic. Crown attorney Bob Morrison told Judge Alan Tufts in Kentville provincial court that he received a compact disc of material from the RCMP's technical crime unit Monday but found that some of the images had mistakenly not been altered. Without that, the Crown couldn't provide the disclosure package to the defence without committing the crime of distributing child pornography. The information within the package included images from a phone seized as part of the police investigation. Morrison said after court that only a few of the images were mistakenly not altered. He said there were hundreds of images that police were dealing with in the case. Robin Lee Spidle, 24, is charged with sexual touching of a minor under the age of 16, invitation to sexual touching, sexual assault, possession of child pornography, and communicating with a person under the age of 18 for the purpose of obtaining sexual services.Postmedia Network (Chronicle Herald, A7)

Mounties arrest man after tires slashed on four RCMP cruisers
An RCMP detachment east of Edmonton has been going through a lot of tires. Mounties say they have arrested a man after the tires of four police cruisers were slashed at the Vegreville detachment earlier this month. Jason Larry Kotowich, who is 35, has been charged with three counts of mischief under $5,000, resisting arrest and breaching a probation order. Postmedia Network (Red Deer Advocate, A3)

* **Sexist signs cause stir on social media**
A Prince Edward Island garage manager says he has received a death threat because of a promotional sign branded "sexist and misogynistic" by some angry commenters on social media. "Women are like snowflakes. They can't drive," read the sign outside Mellish Motors in New Annan, P.E.I., a rural community just outside of Summerside, P.E.I. John Mellish, 55, and his wife say they started the business nine years ago and post a new lighthearted message to the board every Sunday. "We've always had something funny or a topic of local conversation on our sign. I've poked fun at myself, my wife, overweight people. We've been brutal to some male people. " Because of social media, this morning at 6:45 a.m., a person phoned and threatened to shoot me. I reported it to the local RCMP because I think that person needs a little bit of help if an issue like this is touching them that bad." Local residents, commenting on Facebook, backed the business for its humorous messages. Some can remember phrases on the board from last February. Toronto Star, A3

* **Ambulance joyride ends in charges against patient**
A 21-year-old woman has been charged with dangerous driving and theft after she allegedly stole an ambulance from the Royal Alexandra Hospital Tuesday and took it on a 40-minute joyride to Duffield. The woman, a patient at the hospital, gained access to a secure ambulance bay on the east side of the central Edmonton hospital and made offwith the vehicle at about 6 a.m., ramming it through a glassand-steel garage door on 102nd Street north of Kingsway Avenue, said Dave Weiss, executive director for emergency medical services in the north zone. The keys were in the ignition, he said. Edmonton police pursued the vehicle, tracking it using its onboard GPS system, west through Edmonton and along Highway 16 into Parkland County. The RCMP managed to stop the ambulance and arrested the woman without incident at about 6:40 a.m. near Range Road 32 and Highway 16 in Duffield. No injuries were reported, police said. Edmonton Journal, A1

* **Charge laid, but cold case remains open**
It took 30 years for a murder charge to be laid in the death of an elderly Interlake man, and RCMP still don't consider the case solved, delaying closure for the family of two men who took polygraph tests in an attempt to prove their innocence. Four months ago, RCMP laid a second-degree murder charge against Lee Norman Pischke, 50, of the RM of Grahamdale, in the death of 80-year-old Michael Kalanza, who

went missing in 1985. Police also arrested a 53-year-old Winnipeg man but let him go without laying criminal charges. At the time, Manitoba RCMP said investigators believed the two were the only ones responsible for Kalanza's death. Police said the 53-year-old Winnipeg man is still not facing charges and the investigation remains open. "We are continuing on vigorously to ensure that all persons involved are held accountable for this murder," an RCMP spokesman said in an emailed statement. "To this end, we would ask that anyone with information regarding the murder of Mike Kalanza call the historical case unit tip line at 204-984-6447 or call Crime Stoppers anonymously at 1-800-222-8477." RCMP couldn't release any other details about the ongoing investigation, which has spanned three decades. The lack of closure doesn't sit well with Pischke's uncle, 67-year-old Dennis Pischke. Winnipeg Free Press, B2

Lawyer lands discharge for angler caught with pot at border
A New Jersey man avoided a criminal record on Tuesday for entering Canada with 14 grams of marijuana in his vehicle last year. However, Matthew Simonelli has likely earned himself trouble crossing the border, Judge Henrik Tonning noted in Saint John provincial court. The judge accepted the arguments from defence counsel Charles Bryant to grant the 30-year-old, Toms River, N.J., native an absolute discharge for possession of marijuana at St. Stephen on Sept. 9. Simonelli did not attend court, but Bryant entered a plea of guilty on his behalf. Federal Crown prosecutor Peter Thorn related in court that Simonelli and his wife crossed the border at St. Stephen and declared two expensive bamboo fishing rods. The Canada Border Services Agency officer discovered that one Ryan Mockler tried to bring these same rods into the country earlier but he was deemed inadmissible to Canada, Thorn said. Border agents searched Simonelli's vehicle and found the marijuana plus $600 U.S. in a black shoulder bag, the prosecutor said. The agents investigated further and found messages on Simonelli's cellphone "that made a reference to other drugs and pills being contained in a container or cooler," Thorn said. The border guards searched the vehicle but found nothing, Thorn said. The agents issued a civil penalty of $250 and turned the matter over to the RCMP. "There was no nefarious intent. There was no smuggling operation," Bryant said. Postmedia Network (Telegraph-Journal, B2)

RCMP defend handling of root beer incident
RCMP officers believed a man was obstructing a liquor offence investigation when he refused to comply with their instructions. Const. Robert Andrew Scott Burchett, 50, and Cpl. Kevin Roger Lee Halwa, 42, both testified Monday as to why they applied the force they did on Levi Desjarlais on the evening of Aug. 20, 2011. Desjarlais has filed a lawsuit against Halwa, Burchett and Cpl. Dean Allan Purcka, 41, for the alleged assault that followed. The three RCMP officers also face assault charges. Desjarlais said he was pepper-sprayed, kneed in the groin and beaten during the altercation. "If you obstruct the police, sometimes bad things happen," said Burchett during his testimony. Burchett and Purcka were in Sylvan Lake that evening on overtime from other detachments. In the summer, the Sylvan Lake RCMP are provided extra money from the town to increase the police presence for the summer rowdiness. Burchett was driving in a dark blue unmarked prisoner van. He saw Desjarlais walking on the sidewalk holding what he believed at the time to be a bottle of beer. Later, Burchett would learn it was in fact root beer. Throughout direct and cross examination, Burchett said he thought Desjarlais held a beer during the incident. Postmedia Network (Red Deer Advocate, A1)

***Saisie de drogue à Shippagan**
Deux femmes de Shippagan, âgées de 47 et 50 ans, ont été arrêtées à la suite de l'exécution d'un mandat de perquisition dans un appartement de Shippagan. Vendredi, vers 19 h, des agents du District du Nord-Est de la GRC, assistés par des membres de la Section de la réduction de la criminalité et de la Section des chiens policiers, ont exécuté un mandat de perquisition à Shippagan. La GRC annonce que les agents ont saisi de la marijuana, de la méthamphétamine, de la cocaïne, des produits du tabac non estampillés, de l'argent ainsi que des instruments pour l'utilisation de drogues illicites. Les femmes ont été libérées, mais devront comparaître en cour provinciale ultérieurement. Acadie Nouvelle, 7

***Driver unaware of fatal strike on senior**
Oceanside RCMP believe they have found the driver involved in a Jan. 13 incident that killed an 80-yearold woman in French Creek. Based on evidence from the scene and witness accounts, police believe a commercial truck driver unknowingly hit the woman with a piece of equipment that was sticking out from the side of the vehicle. The woman was found lying on the side of the road a short distance from her

home. She was taken to Nanaimo Regional General Hospital and then airlifted to Victoria General Hospital, where she died from head trauma. Speed or alcohol do not appear to have been factors. Police said the driver is very upset and is co-operating fully. Postmedia Network (Times Colonist, A4)

*** Wig-wearing robbery suspect arrested**
Police in Surrey said they have arrested a suspect after a man robbed a bank last month wearing an odd disguise. RCMP said they arrested a 39-year-old resident of Surrey after asking for the public's help in identifying the man following a heist near the Guildford Town Centre on Dec. 29. Police said the suspect was wearing a patterned dress, white wool sweater, a long blond curly wig and a pink tuque that partially obscured his face. Postmedia Network (Times Colonist, A2)

*** La GRC appelle à la vigilance dans une affaire de fraudeurs agressifs**
Des fraudeurs sophistiqués et agressifs qui se font passer pour des employés de l'Agence du revenu du Canada visent des Néo-Brunswickois. La GRC dit avoir reçu plus de 100 plaintes au cours du dernier mois. Alors que la saison des impôts approche, la GRC demande aux Néo-Brunswickois d'être sur leurs gardes contre des escrocs qui se font passer pour des employés de l'Agence du revenu du Canada (ARC). Équipés d'outils qui leur permettent d'afficher un numéro de l'ARC ou de la GRC, les fraudeurs demandent à leurs victimes potentielles de rembourser de l'impôt impayé. Avec un accent étranger, ils parlent d'un ton agressif et menacent de se rendre à la maison de leurs victimes si elles ne leur donnent pas immédiatement de l'argent par carte de crédit ou par Western Union. La fraude est répandue à travers le pays. Lundi, la GRC de l'Ontario a publié la transcription d'un échange entre un arnaqueur et sa victime dans laquelle le faux employé de l'ARC menace de faire sauter la maison de son interlocuteur (voir encadré). Acadie Nouvelle

*** Cops packin' major heat**
Toronto Police are getting more lethal and less lethal at the same time. And receiving some praise, as well, for doing so. It turns out there were voids in both availability of stronger firepower and in less deadly alternatives. So on the same day Canada's largest urban police service announced it has started to equip officers with military-style rifles - the C8 carbine - the police force said it would also begin furnishing members with what is called a sock round - in essence a beanbag gun. "(The C8 carbine) is a far more accurate rifle than what they currently have," spokesman Mark Pugash said Tuesday. One of the problems officers face, he said, is that "there are people out there who are wearing body armour ... " While other weapons in the force's arsenal are not able to stop criminals with body armour, the $2,000-$3,000 C8 carbine can. "It's important Toronto Police have these guns available in a timely manner," crime specialist ross McLean, a former Toronto Police officer, said. "The first things officers in san Bernardino called for were 'long guns' when they saw they were badly outgunned by the ar-15 carried by terrorists. RCMP did a long investigation after four of their members were killed without this sort of weapon available. It is a requirement in today's environment." Postmedia Network (Toronto Sun, A19)

*** Police puppy dies after eating rope**
An RCMP plan to document the lives of two German shepherd puppies during their training has ended sadly for one of the canine recruits. The Halifax division announced Tuesday one of the pups - Helo - has died after ingesting rope and rocks. Const. Mark Skinner says the accident occurred as the puppy pursued his natural tendency to chew on objects. (...) During the media launch of the two puppies on Dec. 18, the RCMP officers training them said the dogs live at their homes. Const. Tim Reid, Helo's trainer, had said that every two weeks he and the puppy took part in a six- to eight-hour training day that included a heavy focus on tracking skills. In a few more months, had Helo lived, a fully trained dog handler would have assessed the dog's progress. Reid said Helo was the sixth puppy he'd trained and that only one had graduated to become a police dog. One of the others died of a heart attack, another returned to Innisfail to breed and two others were sold as pets. Reid had said there are about 80 people like himself across the country who are in training to make it into the RCMP dog handler program in central Alberta. An RCMP news release said Reid was saddened by the loss, and noted that condolences can be shared on the force's Facebook page in Nova Scotia and on Twitter using the hashtag RIPHelo. Postmedia Network (Chronicle Herald, A9, Cape Breton Post, London Free Press)

*** Sex assault charge dropped against cabbie**

An Antigonish cab driver has had one of two sexual assault charges against him dropped. William Roger MacLellan was charged in November 2014 for allegedly, on two separate occasions, groping highly intoxicated young women who took his cab home from Piper's Pub to their dorms at St. Francis Xavier University. "I've reviewed the evidence," Crown attorney Darlene Oko told Judge Laurel Halfpenny-MacQuarrie during the third day of MacLellan's trial in Antigonish provincial court. "I do not believe the court could convict him on that charge." The dropped charge stems from an alleged incident during the early-morning hours of Feb. 15, 2014, when an underage St. F.X. student claimed a cab driver had groped her breasts. The woman admitted during her testimony last October that she was drunk to the point of blacking out during the alleged assault and that she never looked at the driver and could only identify him by his voice. Testimony by RCMP officers on Tuesday focused on the remaining sexual assault charge. (...) "My cab driver molested me," the alleged victim told the 911 operator. In the background, a man could be heard telling her that she had fallen and hit her head at the pub. "That's Roger (MacLellan)," RCMP lead investigator Const. Catherine Bezaire told the court. "I know his voice." Bezaire was one of three RCMP officers who testified Tuesday to the events of Oct. 19, from responding to the St. F.X. dorm where the heavily intoxicated victim was surrounded by a growing crowd of concerned passersby, to taking her statement and searching for a dark green van driven by a non-white male. Postmedia Network (Chronicle Herald, A4)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

No parole for Stanley Tippett, convicted of attack on 12-year-old Ontario girl

An Ontario man found guilty of kidnapping and sexually assaulting a 12-year-old girl seven years ago has been denied parole. The Parole Board of Canada says Stanley Tippett remains "an untreated sex offender" who has not addressed his risk to reoffend. Tippett was convicted in 2009 on seven counts - including kidnapping, sexual assault and sexual interference - relating to an August 2008 attack on the girl. (...)He was declared a dangerous offender after being found guilty - a designation which means he can be jailed indefinitely. In a decision issued earlier this month, the parole board denied Tippett day and full parole, saying any form of release to the community would present "undue risk." Canadian Press (Whitehorse Daily Star, 8); ***** Presse canadienne (Acadie nouvelle)

Back before the courts

Dylan Dingwell, who served federal time for the 2011 shooting death of his brother in Charlottetown, is before the courts in Nova Scotia. Dingwell, 27, who now resides in New Minas, N.S., was charged last week with possessing cocaine for the purpose of trafficking. He has consented to be remanded in custody until his next court appearance in April. Dingwell was found guilty of manslaughter for shooting his brother, Kyle Dingwell, on Jan. 17, 2011, and sentenced to five-and-a-half years in prison, minus 17 months for time served. He was granted full parole in February 2014. The Guardian, A3

*** Fate of Nicholas Rasberry's bail in judge's hands**

The Crown no longer has the authority to seek forfeiture of convicted killer Nicholas Rasberry's bail for violating his release conditions, a court was told Tuesday. Lawyers for Rasberry, who posted $60,000 cash for his release, and his grandmother and wife, who put up property, said Justice Jo'Anne Strekaf should rule she no longer can hear the matter. But Crown prosecutor Jonathan Hak said because Rasberry allegedly breached his bail the day before his sentencing occurred, the forfeiture hearing should proceed. "This isn't a case where his bail was discharged when he was sentenced, because there was a violation," Hak told Strekaf. (...)Lawyer Kelsey Sitar, who spoke for the grandmother and wife, said the prosecution should have sought the endorsement to proceed before Rasberry was sentenced to a penitentiary term. (...)Rasberry was sentenced Dec. 11, to seven years for the killing. (...)He has appealed his conviction arguing he should have been acquitted. The prosecution has also appealed, seeking a retrial on the original charge Rasberry faced of second-degree murder. Ottawa Sun (Winnipeg Sun, Calgary Sun, Toronto Sun)

*** La voleuse en Mercedes pourra sortir du pénitencier**

Les autorités ont remis en liberté une voleuse en Mercedes qui a dévalisé plusieurs résidences cossues avec son mari, même si elle a admis qu'elle aurait encore pu commettre des crimes si elle n'avait pas été arrêtée. «Peut-être. C'est l'arrestation qui a tout changé», a dit Elyanne Miller aux commissaires des libérations conditionnelles, hier, au pénitencier de Joliette. François Baron et Michel Lafrenière venaient de lui demander si elle aurait continué ses vols en série, n'eût été la vaste enquête policière qui a permis de lui mettre la main au collet l'an dernier. Auparavant, la jeune femme de 28 ans ne s'était «jamais posé de questions», at- elle répété à de multiples reprises hier. (…)Puisque Mme Miller «ne représente pas un risque indu pour la société », elle pourra reprendre une vie nor-male après trois mois en maison de transition. Journal de Montréal, 11 (Journal de Québec)

*** Nova Scotia music teacher who abused 13-year-old 40 years ago granted parole**

A former music teacher convicted of abusing a 13-year-old boy four decades ago on Nova Scotia's South Shore is being released from prison. Last year, William Albert Perrot pleaded guilty to two counts of indecent assault on a male for incidents dating to the 1970s. He was sentenced to 2½ years in prison. Perrot is originally from Portsmouth, Virginia, but moved to Kingston, N.S., in 1975. He taught music and English at West Kings District High School until he retired in 2009. At a hearing last Thursday, the Parole Board of Canada agreed to release Perrot on day parole, to be followed by full parole. The board said Perrot has caused no issues while in prison and is assessed as a low risk to reoffend. In requesting parole, Perrot told the board he was sexually immature at the time of the offences and thought his relationship with the boy was consensual, according to the board's written decision. He also said he wasn't aware how much damage his crimes caused until he heard the victim's impact statement. CBC News (2016-01-19)

Costly, overcrowded, dehumanizing prisons are doing harm

An opinion piece states, ""It is painful when we see prison systems which are not concerned to care for wounds, to soothe pain, to offer new possibilities," Pope Francis told inmates of the Curran-Fromhold Correctional Facility in Philadelphia last September. The prisoners were among the astounding 2.2 million Americans who are living behind bars. This pain afflicts Canada, too. Listen, for instance, to Kim Pate, executive director of the Canadian Association of Elizabeth Fry Societies. I spent a morning with her at a Cape Breton University workshop a year ago as she poignantly shared research and first-hand cases. I resolved to give this research, these human tragedies, more examination in my own work. The disgusting indignities inflicted on Ashley Smith are not isolated incidents. The New Brunswick teenager, who was living with mental illness, took her own life while being monitored in isolation. It happened in 2007 at an Ontario prison after years of neglect and taunts by so-called "professionals." Some of them coldly looked on as she placed a ligature around her neck. Pate documented case after appalling case of people thrown off by society and processed like numbers through a system, a very expensive system. Why is mainstream society not hearing a lot about the other cases? Excessive solitary confinement has rightly received recent attention, but why are we not having a serious national conversation about correctional reform? The overcrowding of prisons. Lack of effective programs for inmates. No real efforts for restitution, just punishment. Incarceration of non-violent criminals in human warehouses. The tolerance of abuse in prisons. Locking up instead of treating the mentally ill. Exposing youths to all kinds of bad influences in jail. Not enough caring mentors for youthful offenders who have had no positive role models in their lives. Contrary to a bizarre misconception, prisons in Canada are not country clubs." Cape Breton Post, A8

Pedophile jailed four years, declared long-term offender

A Montreal resident has been sentenced to a four-year prison term for possessing child pornography and for luring teenage boys over the Internet. Shawn King, 61, is also required to follow a series of conditions, for a period of 10 years following his prison term, because he was also declared a long-term offender based in part on his previous criminal record. (…)The offences that date back to the 1980s were committed during a period when King, an anglophone, sexually assaulted eight boys between the ages of 11 and 14 while he was involved in minor league sports programs in Shannon, a small town north of Quebec City, between 1969 and 1997. That case shocked the tiny community, and in 1998 King was sentenced to an overall prison term of seven years. While serving that sentence, King admitted to the

Parole Board of Canada there were other victims of his crimes. Two more victims came forward after news of King's arrest for child luring in 2010 became public. Montreal Gazette, A7

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** NL Left Out of Meetings on Missing and Murdered Indigenous Women**
The Government of Canada is holding meetings across the country to talk about murdered and missing indigenous women and girls. The meetings will be held with survivors, family members, and loved ones. But no meetings will be held in Newfoundland and Labrador, PEI or New Brunswick. On its website, the government says it "believes that an inquiry into missing and murdered Indigenous women and girls can only be designed after hearing from those directly affected." The first two meetings were held in December in Ottawa. Meanwhile A federal, provincial and territorial meeting for Justice and **Public Safety** is going ahead in Quebec City for the next two days. Items excepted to be discussed include violence against indigenous women and girls, cyber security and physician-assisted dying. VOCM

*** Nunavik women, families still have time to register for MMIW event**
Two pre-inquiry sessions with the families of missing and murdered Indigenous women and girls are set to be held in Quebec this week, but it's not too late for Inuit women or families in the province to take part. The Saturviit Inuit Women's Association of Nunavik is encouraging Nunavimmiut survivors or families of victims to register for one of two gatherings scheduled between Jan. 20 and Jan. 22 in Montreal and Quebec City. Indigenous and Northern Affairs Canada, the department heading a national inquiry into missing and murdered Indigenous women and girls, has begun hosting pre-inquiry gatherings in different regions across the country. The department, headed by its minister, Carolyn Bennett, has said the government will design the inquiry only after hearing from those directly affected. Only one gathering has been scheduled in the Arctic — Jan. 29 in Iqaluit. But while the Iqaluit session will be an Inuit-specific event, it's easier for Nunavimmiut to travel to southern Quebec, Saturviit's Pascale Laneuville said. Nunatsiaq Online

*** Art installation paying tribute to MMIW stops in Brandon next month**
An indigenous art installation that commemorates the lives of missing and murdered indigenous women will stop in Brandon, Man. next month. Walking With Our Sisters features more than 1,800 vamps, the decorative tops of moccasins, laid out in a design that will take viewers down a winding pathway. The display also commemorates children that died in Canada's residential school system. It's currently on display in North Battleford, Sask. and will open at Brandon University on Feb. 22. CBC News

Crime prevention centre taps social media to respond to growing complaints about crime
Advocates for deterring and reducing crime are on high alert as the economy continues to tank. Their weapon of choice? Information. TerryLee Ropchan, Central Alberta Crime Prevention Centre executive director, said as soon as you hear about the economy and layoffs, immediately the first thing that comes to mind is that there will be repercussions felt throughout the community. "Definitely it is on our radar," said Ropchan. "We try to stay connected with some of the social media so the Facebook pages around stolen vehicles. We are monitoring. We are watching." One of the agency's goals this year is to respond to some of the growing complaints about crimes or happenings in neighbourhoods on social media platforms. She wants people to know they have some place to go. "We have programs, resources and information," said Ropchan. "We want to engage more with the social media crowd. People use social media to vent and find other people who are experiencing the same. But it has not translated to people who want to be part of Citizens on Patrol or join Neighbourhood Watch. Those are the things that we are offering to them so they realize they can make a difference." Crime prevention is more important than ever and is reflected in the work it is doing in the community with its graffiti program, SAFE program, presentations and other programs, she said. Red Deer Advocate, A1

*** Un plus haut taux de crimes haineux à Ottawa**
Le Service de police d'Ottawa (SPO) a déclaré deux fois plus de crimes haineux que la moyenne des autres corps policiers municipaux du pays, selon les plus récentes données fournies par Statistique

Canada. Selon un rapport rendu public en novembre, le SPO a déclaré 64 incidents criminels de ce type en 2013. Il s'agit d'un taux de 6,6 crimes par 100000 habitants, le double du taux canadien, qui est de 3,3. Même les grandes villes cosmopolites comme Montréal et Toronto font meilleure figure, avec des taux de 3,0 et 4,9 respectivement. La police de Gatineau a quant à elle rapporté cinq crimes haineux en 2013. La police d'Ottawa soutient qu'il faut analyser ces données avec précaution. La constable Lila Shibley explique que les forces de l'ordre de la capitale, plus qu'ailleurs, sont très actives sur le terrain. Elle voit d'un bon oeil que les victimes sont nombreuses à porter plainte, car plusieurs décident de se taire. Le Droit, 4

Step up drug fight, health boss urges
London needs a drug strategy fast-by summer-to fight off an onslaught of crystal meth on the heels of the battering the area has taken from abuse of drugs like OxyContin, its top public health official warns. "We should be moving on this more quickly," Dr. Christopher Mackie, medical officer of health and chief executive of the Middlesex London Health Unit, said Tuesday. "It's fair to say we have people being harmed every day. We probably have someone dying of an overdose or an infection or complications due to an infection every week. We have a major issue here." Nothing less than a community-wide approach is needed, said Mackie, who doesn't expect the full-blown plan to be operating by summer but wants to see the first steps taken. He isn't calling anyone out on the lack of progress in London's battle against addiction: He and the health unit took the lead in calling for a community drug strategy after releasing alarming statistics on addiction in 2014. A health survey showed double the rate of overdose deaths in Middlesex County compared to the rest of Ontario, taxing health care and social service agencies, hospitals and police. London Free Press, A1

* **Don't blame violent crime on the mentally ill**
An opinion piece states, “One of my students recently sent me a message wherein he wondered why psychologists appear to be so helpless in predicting mass murders, such as those in San Bernardino, Calif. and in Colorado Springs, Colo. late last year. His question is a common one and the answer most often given by politicians, for example, is that we must improve our mental health outreach programs in order to prevent such tragedies. (…)But while some mass killers may have a psychiatric illness, the vast majority of violent people are not mentally ill and, indeed, most mentally ill individuals are not violent. According to recent statistics, about four per cent of overall violence can be attributed to those with mental illness. Homicides are most often committed by people without mental illness - by family members or people on a first-name basis with their victims. Some homicides are committed during the commission of a lesser crime, such as a robbery, which escalates. Other homicides are perpetrated by individuals who are convinced they will not be caught, and at the bottom are those people with known mental illnesses who commit homicide. Mass killers are almost always young men, isolated, friendless, and filled with smouldering hostility and resentment, people who are in the midst of planning some form of revenge for what they perceive as chronic slights or attacks on their sense of psychological integrity. Complicating the picture, in many cases these young men tend to avoid any contact with mental health professionals, making it more difficult to identify and support them.” Waterloo Region Record, A9

* **Mom wants curfew for teens as a crime-fighting measure**
Agatha Eaglechief says the city needs to enforce a nighttime curfew on all high-school-aged kids to stop gangs of teenagers from roaming late at night. "Their parents are letting them run wild," Eaglechief said from her home in Confederation Park. Eaglechief said she's noticed a spike in gang activity among teenagers in recent years. She said she has spent countless nights out on the streets helping her friends track down their teenage kids. Now it's time for the police to get involved, she said. "There are a lot of innocent children getting involved in the gangs, the thieving and stealing," she said. "We need to put our foot down. The government, the chief of police, everybody. Control these kids." Eaglechief has written a letter to Saskatoon's board of police commissioners and hopes to attend its meeting on Thursday to convince police to take action. Eaglechief isn't alone. Last November, the Town of La Ronge started enforcing an overnight curfew for people under the age of 18. RCMP were told to enforce of the bylaw - which has been on the books since 2005 - after a spate of break-ins, thefts and other vandalism, according to Mayor Thomas Sierzycki. StarPhoenix, A2

*** Charlottetown police rolls out new youth program to replace DARE**
A new program focusing on drug abuse and mental health, developed by Charlottetown police and student services workers, rolls out next week in elementary schools. Healthy Me replaces the Drug Abuse Resistance Education (DARE) program, which taught Grade 6 students about the dangers of drugs, alcohol and tobacco use. DARE has been slowly shutting down since 2014. The new program still covers the topics of drugs and alcohol abuse, but it also adds a mental health component. Also now included in the program is a cyberbullying and social media component. "With DARE, it talked about drugs and how they affect your body, but we never really looked at the wellness component as far as mental health," said Charlottetown police Const. Tim Keizer, who is a school resource officer. Keizer said the new Healthy Me programs asks young participants to ask themselves where they get their values and beliefs from and what are some of the outside influences on their lives. The Guardian

RATS, In gang culture, those who talk to cops are the worst form of life
Former New York mobster Lou Ferrante still remembers the day in 1991 that he heard the shocking news that Salvatore (Sammy the Bull) Gravano had betrayed the Gambino family and was going to testify against John Gotti Sr. "When Sammy the Bull became a rat, none of us believed it. I was the first to say: 'no way'. And a few people said, 'yeah, it's true. It's happening,'" Ferrante recalled in a recent interview. The underworld perception of ratting has percolated through other gangs as well - including B.C. groups like the Red Scorpions and United Nations. The late gangster Bal Buttar once told The Vancouver Sun he was involved in several murders, but would never help police. "I've never in my life been a rat and I'll never be one," Buttar said. (...)Things have changed in B.C. as well in recent years. Police here have convinced many living the gang lifestyle that the best thing they can do is co-operate. Even a killer known only as Person Y, who became a key Crown witness in the Surrey Six murder case, said he finally realized the only way he could break from a 20-year criminal career was to go to the police. "I'll just turn into the biggest rat," he said of his thinking at the time. "I am committing suicide in terms of my name in the game." Staff Sgt. Paul Dadwal, of the Integrated Homicide Investigation Team, has interviewed hundreds of gangsters and associates, persuading many to testify. Often, he said, he has to break through their aversion to "ratting." Underworld bosses and gang leaders perpetuate the myths about co-operating with police, Dadwal said. Vancouver Sun, A1

Black community unfairly targeted in war on drugs
An opinion piece states, "The Supreme Court of Canada will soon decide the fate of the mandatory one-year jail sentence for trafficking certain drugs. The mandatory minimum has come under fire by civil liberty groups for constituting cruel and unusual punishment, arbitrary imprisonment and restricting security of the person contrary to the Canadian Charter of Rights and Freedoms. The case at issue concerns Ryan Joseph Lloyd, a drug addict in his mid-20s, who lived in Vancouver's notorious Downtown Eastside. (...) Seven public interest groups including the African Canadian Legal Clinic, the West Coast Women's Legal Education and Action Fund, and the Union of British Columbia Indian Chiefs, among others, argue that an offender who lives in poverty, has faced systemic barriers and suffers from an addiction disorder should not be automatically subjected to a one-year sentence upon conviction. In fact, before the enactment of the mandatory minimum sentence, judges were free to take social disadvantage into account and prescribe punishments that fit the crime." Toronto Star, A13

*** Province doing little to stop sex slavery: Scott**
Teen girls across Ontario are being forced into sex slavery while the provincial government does little to stop it, says an area MPP. Laurie Scott is the Progressive Conservative MPP for Haliburton-Kawartha Lakes-Brock (which includes Lindsay and Cavan Monaghan Township in Peterborough County). She says about 30,000 girls - average age 14 - are being prostituted in Ontario. It's a huge problem, Scott says, and she'd like the province to do something. Scott belongs to a legislative committee that's trying to stop human trafficking. The committee would like to see Ontario judges, Crowns and police officers get special training to deal with human trafficking cases, for example. Scott said these teens are each making up to $280,000 a year for their pimps, and they're being trafficked in motels all along the Highway 401 corridor. The Peterborough area is not immune to the problem: A 28-year-old Cordova man was charged by police last week in a case of human trafficking involving children. The committee is also pushing for new rules to help victims of sexual abuse, such as new protocols for dealing with abuse on college and university campuses. Scott was in Peterborough with other members of the committee on Tuesday for a

day-long meeting at the Holiday Inn. Committee members were there to collect feedback from local experts on how the province could best help victims. Representatives from places such as Trent University, the Peterborough Haliburton YWCA and the Kawartha Sexual Assault Centre gave presentations. Scott said the committee is touring more cities to conduct the same type of meetings, soon. They're going to London and Toronto next. Scott said she's appalled that Ontario isn't doing more to curb human trafficking. Peterborough Examiner; My Kawartha (2016-01-19)

*** L'intimidation se transporte sur le Web**
Depuis quelques années, on parle de plus en plus d'intimidation à l'école et de ses conséquences parfois désastreuses sur les victimes. Or, l'intimidation peut parfois sortir de la cour d'école et se transporter jusque sur les réseaux sociaux. On parle alors de cyberintimidation. La cyberintimidation se traduit par des propos dégradants ou menaçants tenus publiquement ou en privé, sur les réseaux sociaux, par messagerie instantanée, dans les groupes de discussion, par courriel... Tout comme les gestes et paroles qui atteignent durement les enfants intimidés dans la cour d'école, la cyberintimidation peut affecter lourdement la personne visée. On parle de perte de confiance en soi, d'isolement, d'anxiété, voire de suicide. Le fait que le message puisse être relayé par de nombreuses personnes et devenir viral, en plus de durer dans le temps en raison du support utilisé, ne fait qu'aggraver les conséquences chez la victime. Jeunes et adultes doivent agir lorsqu'ils sont victimes ou témoins de cyberintimidation. La première étape, pour le jeune intimidé, consiste à en informer un adulte de confiance, par exemple ses parents ou un membre du personnel de l'école. On conseille également à la victime de ne pas répondre à l'intimidateur, de retirer celui-ci de ses contacts sur les réseaux sociaux, de bloquer les messages en provenance de cette personne et de conserver les messages reçus. La Revue (2016-01-19)

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

'We are ready'
As some cities take a breather from resettling government-assisted Syrian refugees, others say their doors are open - if the federal government asks and also offers to pay. While the home communities for refugees with private sponsors is dictated by where those sponsors are, refugees whose costs are covered entirely by the federal government are sent to just 36 cities. Not included is Victoria - the lone provincial capital that isn't an official reception centre for government assisted refugees. The only Syrians arriving there as part of the Liberals' Syrian program are those whose costs are split between the government and private sponsors, as well as those coming thanks to private sponsors alone. Victoria Mayor Lisa Helps said she told the federal immigration minister even before the Liberal program was unveiled that her city was interested in taking in Syrians but is still waiting. "We are ready. The church, the school board, the credit union, private donors, private families, we're ready," she said. Canadian Press (Edmonton Sun, A34, Ottawa Sun, Times & Transcript, Daily Gleaner, Times Colonist)

Soldiers prove they're up for any task thrown their way
There were tears, laughter, hugs and enough happiness to spread over this part of the world. It was a scene that could easily have been taken from the cover of a Hallmark greeting card. Early on Jan. 12 approximately 60 infantry soldiers, mostly from The Second Battalion, The Royal Canadian Regiment (2RCR) returned home from deployment in the Middle East - everyone was safe and sound. The unusual part of it all was what the kind of deployment they were coming back from. Usually, when infantry soldiers depart on a mission, they are heading into combat or peacekeeping scenarios. But not this group. They were in Lebanon and Jordan as part of Operation Provision, the federal government's initiative to resettle 25,000 Syrian refugees in Canada by the end of February. They left Canada on Nov. 26 and Nov. 28. An Immigration, Refugees and Citizenship Canada (IRCC) initiative, the ongoing mission sees Forces personnel provide assistance for data entry and biometric screening. (...) Base Gagetown commander Col. Dan MacIsaac said he was "very proud" of the returning soldiers. "It's a fantastic demonstration of the professionalism and agility that we have in the Canadian military and the fact that we are always ready for any missions," he said. Daily Gleaner, A7

Sunny ways won't cure economic woes
An opinion piece states, "Some questions are awkward to ask. Those who raise them risk being accused of hateful intentions. News this week that several Ottawa agencies are calling for a pause in this city's refugee flow has to raise the question of whether we have tried to do too much, too quickly, to meet a target founded in politics and hope, not realism and numbers. More than 11,300 Syrian refugees have arrived in Canada since November, including more than 500 here in the capital. The bulk of the initial wave has been privately sponsored. Local aid agencies say they are already experiencing a service bottleneck, though temporary, for those refugees. What's coming next is a larger, governmentassisted wave. That is also expected to challenge language and other support services. The assistance to Syrians that Canada and, more locally Ottawans, are offering is admirable and heartfelt. It has been good to see. But to bring families into a new life, to have them properly acclimate to our city and country, takes resources and support. Strained services and inadequate supports won't serve Syrian families and newcomers who are desperate not only for a safe haven, but for place where they can prosper and thrive. Let us make sure that we, as a city, get this right." Ottawa Sun, A12

Canada should look after poor, not refugees
A letter to the editor states, "In response to Liz Wall's letter to the editor Jan. 13, about blasting the prime minister on his refugee policies; Ms. Wall, if we people don't speak up against unwise or unfair policies made by government, who will? The prime minister promised to have 25,000 refugees from Syria in Canada by Jan. 1, 2016, and backtracked when it was said it couldn't/shouldn't be done so quickly, especially if security was to be maintained. It has also been reported that not a single applicant who has been screened to come to Canada has been refused refugee status. Canadians were right and the prime minister was wrong." Times & Transcript, A8

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Le fédéral passe à la traduction automatique**
Le fédéral installera un nouvel outil de traduction automatique sur les postes de travail de tous ses fonctionnaires, dès le 1er avril prochain. Mis au point dans le cadre du projet de modernisation du Bureau de la traduction, le nouveau logiciel de traduction est déjà utilisé par un groupe restreint de 200 fonctionnaires dans le cadre d'un projet pilote lancé l'an dernier. Il doit remplacer d'autres outils déjà disponibles sur le marché, dont Google Traduction, afin d'améliorer la compréhension et la traduction de courtes communications internes non officielles. Le projet est toutefois source d'incertitude et d'inquiétude pour les employés du Bureau de la traduction, qui emploie de nombreux traducteurs, interprètes et terminologues. Son arrivée fait craindre une détérioration de la qualité des traductions, alors que les effectifs sont déjà décimés par les compressions imposées ces dernières années sous le gouvernement conservateur. En juin 2015, la présidente de l'Association canadienne des employés professionnels (ACEP), Emmanuelle Tremblay, exprimait l'inquiétude de ses membres face à ce nouvel outil dans une lettre adressée à Donna Achimov, la pdg du Bureau de la traduction. Dans sa missive, la présidente de l'ACEP disait craindre que la «machine à traduction» vienne «souiller» la réputation de l'institution, alors que des traductions de piètre qualité risquent désormais de porter son sceau. Le Droit

*** Heures sombres pour le Bureau de la traduction**
Le Bureau de la traduction du gouvernement fédéral traverse des temps difficiles. Alors que le premier ministre Trudeau s'est engagé à ce que tous les services soient offerts «en parfaite conformité» avec la Loi sur les langues officielles, des sources décrivent le Bureau de la traduction comme un «champ de ruines», miné par des réductions de personnel et l'incertitude crée par le lancement du nouvel outil de traduction automatique. «Le moral des employés est à son plus bas et les conditions de travail deviennent intenables. Certains traducteurs font 80 heures supplémentaires par mois; les traducteurs compétents cherchent désespérément un autre emploi. Les épuisements professionnels se multiplient. Bref, c'est l'hécatombe. Une situation alarmante qui ne semble pas inquiéter le gouvernement Trudeau, qui a bien d'autres chats à fouetter», raconte un traducteur dans une lettre transmise au Droit. La dirigeante du bureau, Donna Achimov, a été nommée par le gouvernement conservateur. Bilingue, elle

se serait entourée d'une équipe de gestionnaires dont le niveau de bilinguisme serait «variable» - l'anglais étant la langue le plus souvent utilisée par la direction, selon nos sources. Le Droit

*** Outdated, understaffed system causes pension delay for reservists**
Senior officials in the Canadian Armed Forces say reservists are waiting too long to receive their first pension cheques because the human resources computers and processes at National Defence are outdated and the department has been understaffed. But they say the system is being streamlined, more administrative personnel have been being hired and the military is moving to faster and more modern technology, which should resolve the problems over the next two years. Globe and Mail, A1

OTHER / AUTRE

Ottawa says it won't grant Canadian citizenship to imprisoned Saudi blogger
The Trudeau government says it won't grant imprisoned Saudi blogger Raif Badawi Canadian citizenship, arguing this would not help the case of a man sentenced to 1,000 lashes and 10 years in jail for blasphemy. Mr. Badawi's spouse and their three children were granted sanctuary in Canada last year and now live in Sherbrooke, Que. Ensaf Haidar, speaking to The Globe and Mail last week, said Canada must do more to help her husband and said "the first thing" it could do now is give Mr. Badawi a Canadian passport. She argued Canadian citizenship would give Ottawa more standing to push for his release. Foreign Affairs Minister Stéphane Dion disagrees. Speaking after a cabinet retreat in southwestern New Brunswick on Tuesday, he said he doesn't believe Canadian citizenship would improve Mr. Badawi's situation. "As a way to release him, it may not be very helpful because Saudi Arabia does not recognize dual citizenship," he said. "We don't think this would be an additional reason for them to consider to release him." Mr. Dion said the government of Quebec has pledged to give Mr. Badawi sanctuary if he is set free. Globe and Mail, A4

Defence minister says anti-ISIL meeting one of many
Canada again finds itself on the outside looking in when it comes to a gathering of countries fighting militants in the Middle East, something the new defence minister is trying to shrug off in the face of opposition criticism. There are meetings all the time to discuss threats around the world, Harjit Sajjan insisted Tuesday, but he stopped short of explaining exactly why Canada isn't invited to this week's meeting in Paris. Counterparts from France, the U.K., Germany, Italy, Australia and the Netherlands will gather Wednesday with U.S. Secretary of Defence Ashton Carter to discuss the ongoing fight against the Islamic State of Iraq and the Levant. Defence sources and at least one defence analyst say there may be more to the fact the Trudeau government was excluded than the domestic political outrage suggests. Officials at NATO and the European Union are seized with ISIL's expanding presence in Libya. U.S. commandos were recently looking for allies among local militias to counter the extremist influence, but met with little success, according to published reports. Canadian Press (Times & Transcript, B4, Times Colonist, Whig-Standard, Toronto Sun, Edmonton Sun, Ottawa Sun, Calgary Sun); La Presse canadienne (Le Droit, 19, Acadie Nouvelle, Le Devoir); * La Presse (Le Quotidien, 18, Le Soleil, La Voix de l'Est); * Journal de Montréal, 30 (Journal de Québec)

*** Ottawa travaille au rapatriement des corps des victimes**
Quatre jours après les attentats terroristes d'Ouagadougou, le gouvernement du Canada ignore toujours quand les corps des six victimes québécoises seront rapatriés. «Nous sommes présentement en discussion avec les familles des victimes pour les détails du rapatriement. Le moment où les corps pourront quitter le pays pour revenir au Canada dépend des autorités du Burkina Faso», a indiqué François Lasalle, porte-parole du ministère des Affaires mondiales, qui ignorait également pourquoi les autorités de ce pays d'Afrique n'avaient pas encore libéré les corps. De son côté, Adam Barratt, porte-parole du ministère des Affaires étrangères, a affirmé à La Presse Canadienne que les ressources du Ministère seraient utilisées pour aider les familles et rapatrier les corps le plus rapidement possible. M. Lasalle a aussi indiqué qu'il y avait des progrès dans l'enquête sur les attentats qui ont coûté la vie à Yves Carrier, sa fille Maude, son fils Charlelie, sa femme Gladys Chamberland ainsi qu'à leurs amis Louis Chabot et Suzanne Bernier. «Tout ce processus est géré par les autorités du Burkina Faso.» Quant à l'identification des corps, M. Lasalle a indiqué que 28 des 30 corps avaient été identifiés. «Il en reste deux

à identifier et nous attendons le communiqué de la procureure à cet effet. Cependant, nous n'avons aucune indication à l'effet que ces personnes pourraient être canadiennes. Toutes les victimes canadiennes ont donc été identifiées.» Quatre des six ou sept terroristes ayant participé aux attentats ont été confirmés comme étant décédés par les autorités locales. Les attentats ont été revendiqués par l'organisation terroriste algérienne Al-Qaïda au Maghreb islamique. Le Soleil (Le Nouvelliste, 20, La Tribune, Le Quotidien, Le Soleil) (2016-01-20); la Presse (2016-01-19)

* **Justin Trudeau to talk up Canada when he takes stage at Davos**
Prime Minister Justin Trudeau makes his debut Wednesday at the annual gathering of the global super elite in this Alpine ski resort that plays host to the World Economic Forum. Mr. Trudeau is expected to be a popular attraction, with meetings scheduled with billionaire investor George Soros and the chief executive officers of Facebook and Microsoft. The annual events draws rich tycoons, the political elite and movie stars such as Leonardo DiCaprio. Mr. Trudeau has already made headlines and attracted buzz around the world. He will deliver a keynote speech to the main forum Wednesday, and is expected to talk up the benefits of investing in Canada and to explain the country has more to offer the world than oil and gas. Globe and Mail

*** How can the Liberals leave others to defend our national security?**
An opinion piece by John Ivison states "Tuesday, October 7, 2014 will go down as a day of ignominy for the Liberal Party of Canada. For crass electoral reasons, the party voted that day against the Conservative motion to send CF-18 fighters to join the coalition arranged against the barbarians of the Islamic State, the militant group who, at the time, were knocking at the gates of Baghdad. Calculating that the war would become unpopular, particularly in Quebec, the Trudeau Liberals locked themselves into a position advocating a "military role of a non-combat nature." That they still haven't found a face-saving way to fix that blunder is now Canada's disgrace. Camille Carrier, the mother of Maude Carrier, who was killed in a terror attack by Islamic fundamentalists in Burkina Faso on Friday, said she is ashamed of Canada. "I have plenty of friends in France who are ashamed of us," she said, as she called for military action against jihadist forces." Postmedia News (National Post, Calgary Herald, Gazette, Leader-Post, Windsor Star, StarPhoenix, Edmonton Journal)

INTERNATIONAL

* **Pakistan attacks: at least 30 dead in terror raid at Bacha Khan University**
A group of militants has stormed a university in north-west Pakistan, killing at least 30 people and leaving dozens injured. The gunmen entered Bacha Khan University in Charsadda, Khyber Pakhtunkhwa province, at about 9.30am (4.30am GMT), apparently using the cover of thick morning fog, and opened fire on students and teachers in classrooms and accommodation blocks. A gun battle ensued between the attackers and Pakistan security forces, with television footage showing soldiers entering the campus as ambulances lined up outside the main gate and anxious parents consoled each other. After several hours the army said four attackers had been killed and that a clearance operation had ended. At midday local time a provincial minister said 30 people had died, though unverified reports from witnesses suggested that number could rise. Naseer, a 23-year-old student, said he counted more than 50 bodies and saw gunmen shooting male and female students "without discrimination". TheGuardian.com

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PS.PSPMediaCentre/CentredesmediasPSP.SP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
January 29, 2016 / le 29 janvier 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Surveillance - Ottawa a laissé filer les informations des Canadiens
Les espions des réseaux électroniques du pays ont non seulement épié des Canadiens, mais ils ont en outre partagé des informations sur ces citoyens avec leurs alliés, a révélé le commissaire chargé de surveiller leurs opérations. L'incident -- " involontaire " -- a été décelé fin 2013... mais n'a été dévoilé au grand jour que deux ans plus tard. Il aura fallu attendre le rapport annuel du commissaire surveillant les activités du Centre de la sécurité des télécommunications (CST) pour apprendre jeudi que l'organisme a transmis certaines métadonnées de Canadiens à ses alliés sans que ces informations soient " adéquatement protégées ". " Aucun nom " n'a été transmis aux partenaires du Canada et les données " en soi ne comportaient pas assez d'information pour mener à l'identification d'un Canadien ", a insisté un fonctionnaire du CST en présentant les conclusions du rapport du commissaire Jean-Pierre Plouffe (...) Le **ministre de la Sécurité publique, Ralph Goodale**, a tenu à rappeler que le gouvernement libéral ***" a entrepris une révision complète du cadre de renseignement et de sécurité*** ". L'objectif : s'assurer que les agences parviennent à protéger les Canadiens, tout en respectant leurs droits et libertés, a-t-il résumé. ***" Et cette révision amènera un lot de changements.*** " Mais les libéraux ont refusé d'indiquer s'ils serraient la vis à l'espionnage de ressortissants canadiens. Le Devoir, A1

CSIS got taxpayer data without warrants
The Canadian Security Intelligence Service repeatedly obtained taxpayer information from the Canada Revenue Agency without presenting a courtapproved warrant for the data. That revelation was among

several concerns raised in the latest annual report of the Security Intelligence Review Committee, which monitors CSIS compliance with law and policy. The report tabled Thursday said the spy service must do more to ensure insiders don't pilfer secret material. It also urged CSIS to inform the Federal Court how it uses metadata - the telltale digital trails that accompany messages and phone calls - collected from cyberspace. The findings came the same day the watchdog over the Communications Security Establishment, Canada's electronic spy agency, found the CSE had improperly shared metadata about Canadians with key foreign allies. The reports prompted the NDP to express concern about erosion of civil liberties. **Public Safety Minister Ralph Goodale** said the federal government is embarking on a comprehensive review of Canada's national security and intelligence framework with the twin aims of effective security and respect for rights. Far from being an isolated incident, there were "multiple instances" of a CSIS regional office getting warrantless access to taxpayer data from the federal revenue agency, the review committee said in its report covering the 2014-15 fiscal year. Questions about the practice were first raised by the Federal Court, prompting CSIS to ask the review committee to look into the matter. Canadian Press (Times Colonist, A8)

Service gathered tax info

The Canadian Security Intelligence Service repeatedly obtained taxpayer information from the Canada Revenue Agency without presenting a court approved warrant for the data. That revelation was among several concerns raised in the latest annual report of the Security Intelligence Review Committee, which monitors CSIS compliance with law and policy. The report tabled Thursday said the spy service must do more to ensure insiders don't pilfer secret material. It also urged CSIS to inform the Federal Court how it uses metadata-the telltale digital trails that accompany messages and phone calls-collected from cyberspace. The findings came the same day the watchdog over the Communications Security Establishment, Canada's electronic spy agency, found the CSE had improperly shared metadata about Canadians with key foreign allies. The reports prompted the NDP to express concern about erosion of civil liberties. **Public Safety Minister Ralph Goodale** stressed the Liberal government was embarking on a comprehensive review of Canada's national security and intelligence framework with the twin aims of effective security and respect for rights. Far from being an isolated incident, there were "multiple instances" of a CSIS regional office getting warrantless access to taxpayer data from the federal revenue agency, the review committee said in its report for 2014-15. Questions about the practice were first raised by the Federal Court, prompting CSIS to ask the review committee to look into the matter. Canadian Press (London Free Press, B3, Toronto Star, iPolitics)

Senators demand role on national security committee

A leading senator is voicing concerns over what role the Senate will play on the Liberals' planned committee of parliamentarians responsible for reviewing the legality and effectiveness of Canada's national security activities. The government wants legislation enacted by June creating an "all-party committee of parliamentarians," to be chaired by Liberal MP David McGuinty. It's an oversight move meant to fulfil a key election promise and set the stage for the Liberals' promised overhaul of the Anti-terrorism Act of 2015, otherwise known as Bill C-51 (...) The committee would be sworn to secrecy, reporting to the prime minister and through him to Parliament. It would have a full-time staff, access to the necessary secret information and be tasked with strategic oversight of every government department and agency that has national security responsibilities. McGuinty, who represents Ottawa South, has declined requests for an interview. **Public Safety Minister Ralph Goodale's** office was no more forthcoming Thursday. ***"The government has committed to create an all-party committee with special access to classified information to review departments and agencies with national security responsibilities,"*** **Scott Bardsley**, **spokesman for Goodale**, said in a statement. ***"The minister's objective is to introduce legislation to do so before the summer. Work is ongoing and we have no further details to announce at this time."*** He wouldn't say if senators will be given seats on the committee. But Wesley Wark, a University of Ottawa security and intelligence expert, said the understanding is that Senate involvement "would be important to assist in the continuity of work of such a committee and to provide for additional expertise." Postmedia News (Ottawa Citizen, A6)

*** Canada Halts Sharing 'Top Secret Data' with Five Eyes**

Canada has stopped sharing secret spy information with a number of countries including the United States. The decision was made after Canada's spy agency discovered that its US counterpart, National

Security Agency, had shared personal details of a number of Canadians. Canada said the Communications Security Establishment failed to hide the metadata of Canadian citizens before sharing it with international partners. Canada is one of the "Five Eyes" intelligence sharing network. The other countries are Australia, New Zealand, the UK and the US (…) CSE said in a report to parliament on Thursday that the unintentional breach had been revealed internally in 2013. According to a CSE official, the blame goes to a software flaw which resulted in exposing personal details of Canadian citizens. According to **Public safety minister Ralph Goodale**, the allies have been ***"very supportive***" as CSE decided to halt information sharing. The Guardian reports that it is illegal to spy on Canadians even though CSE does keep an eye on some while investigating other targets. Australia Network

Teachers across Sask. to mark moment of silence for La Loche
Educators across the province are planning to participate in a show of support in response to the shooting in La Loche last week. While students in Saskatoon's two major school divisions won't be in classes Friday morning, teachers and staff across the city will be observing a moment of silence to honour those killed in the northern Saskatchewan community. The moment of silence at 9 a.m. on Friday was organized by the Federation of Saskatchewan Indian Nations. La Loche, approximately 600 kilometres northwest of Saskatoon, was the scene of multiple shootings on Jan. 22 that left four people dead and seven people wounded.(http://thestarphoenix.com/news/crime/la-loche-struggles-with-why) A 17-year-old boy is accused of shooting and killing Dayne Fontaine, 17, and Drayden Fontaine, 13, in a home in the town before going to the Dene High School in La Loche, allegedly killing 21-year-old Marie Janvier and 35-year-old teacher Adam Wood and wounding seven others. The 17-year-old cannot be named under the Youth Criminal Justice Act. The tragedy has thrust the remote Dene community into the national spotlight and drawn strong support for the community from around the province. Greg Chatlain, director of education with Greater Saskatoon Catholic Schools, said roughly 1,900 teachers and staff across the division will be participating in the moment of silence and conducting a group prayer on Friday. "We have staff and families that are related to and are friends of families in La Loche that have been very impacted by the event," Chatlain said. La Loche Mayor Kevin Janvier, left to right, Saskatchewan Premier Brad Wall, federal **Public Safety Minister Ralph Goodale** and MP Georgina Jolibois lay flowers at a makeshift memorial in La Loche on Jan. 24, 2016. Postmedia News (StarPhoenix) (2016-01-29); * CBC News (2016-01-28)

*** Trudeau to visit La Loche on Friday**
Prime Minister Justin Trudeau will travel to La Loche one week after the school shooting that plunged the northern First Nations community into shock. The Prime Minister's Office announced Thursday morning that Trudeau will travel to the town of about 3,000 people on Friday. The visit had been expected since federal **Public Safety Minister Ralph Goodale** visited La Loche on Sunday and told reporters that Trudeau intended to make the trip. The prime minister has been in Ottawa this week for the first session of Parliament of the new year. Toronto Star (Our Windsor) (2016-01-28)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Le virus Zika est inévitable au Québec, dit Barrette**
Le ministre de la Santé Gaétan Barrette confirme que le virus Zika, qui a notamment infecté trois voyageurs canadiens, est «inévitable» au Québec. À sa sortie du premier nouveau Conseil des ministres, hier, M. Barrette s'est tout de même voulu rassurant, qualifiant le virus Zika de «cousin» du virus du Nil occidental. «On a le virus du Nil au Québec et comme on peut le voir, ce n'est jamais devenu une situation dramatique, a-til expliqué. Le taux de mortalité du virus du Zika est plus faible que celui du Nil, c'est un virus qui est moins agressant. Le vrai enjeu est celui de ses effets sur les femmes enceintes. » Agence QMI (Journal de Québec, 30 ; Journal de Montréal)

*** WHO to decide if Zika is health emergency**
On Thursday, the World Health Organization announced it will hold an emergency meeting on the Zika virus, which is "spreading explosively" and "strongly suspected" of causing a surge in birth defects across Brazil...There are also increasing reports of tourists getting infected and bringing the virus home,

including to Canada, where three cases have been confirmed so far. Two were diagnosed in B.C. and a third in Alberta, with travel histories to either Colombia or El Salvador. All three have since recovered. While Zika's threat to Canadians remains low, the Public Health Agency of Canada is recommending that pregnant women - and women who plan to become pregnant - avoid travel to Zika-affected countries. Canadian Blood Services will also start turning away donors who have visited high-risk countries. The agency already prohibits blood donations from people who have recently travelled to malaria-endemic countries. Toronto Star, A4; Globe and Mail, A3

* **Zika virus 'spreading explosively' through Americas - Canada considered safe as transmitting mosquitoes have not yet arrived**
The mosquito-borne Zika virus is "spreading explosively" in the Americas and will soon be in all but two countries, Canada and Chile, the head of the World Health Organization says. Canada enjoys a "biological barrier" to widespread transmission of the virus, according to Dave Patrick, a physician and epidemiologist at the University of B.C. "The particular mosquitoes that are capable of transmitting the virus are not here," he said. "We've got to keep looking out for them and make sure there isn't a northward migration." Canadian Press (Vancouver Sun, A1/Front)

* **Northern Alberta town on alert after rise in water levels on rivers**
The northern Alberta town of Peace River is on a "green alert" after a rise in river water levels earlier this week. Alberta Environment and Parks Public Affairs officer Jason Penner stresses that right now it's a watch and not a warning. Canadian Press (Daily Star, 12)

* **NOVA SCOTIA**
Nova Scotians are hunkering down for another winter storm that could bring as much as 25 cm of snow to central and northern parts of the province on Friday. Chronicle Herald, A4

* **Tempête : jusquà 40 cm de neige prévus par endroits en Atlantique**
Les résidents de plusieurs régions des provinces de l'Atlantique vont devoir ressortir leur pelle, car d'importantes chutes de neige sont prévues vendredi et samedi. Le sud-est du Nouveau-Brunswick et presque toute l'Île-du-Prince-Édouard devraient recevoir de 15 à 20 cm de neige à compter de vendredi après-midi, selon Environnement Canada. Jusqu'à 40 cm sont prévus sur le comté de King à l'Île-du-Prince-Édouard. Radio-Canada ; Charlottetown Guardian, A2

* **Blacks Harbour residents fed up with power outages**
The village of Blacks Harbour is calling for a special meeting with the president of the NB Power, saying the community is experiencing an unusually high number of power outages this winter. Heather Chase, the village's chief administrative officer, says Mayor Terry James has received so many calls with complaints she wants a face-to-face meeting with the head of the utility. CBC News

* **Residents demand end to sewer backups**
Thompson Avenue residents say that the sewer backs up into their homes whenever a heavy rain and high tide come at the same time. Sherry Currie spoke on behalf of a delegation at Monday night's town council meeting, stating that sewers started backing up on a semi-regular basis since the major flood that hit Charlotte county in December 2010. Telegraph-Journal, B4

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Spy agency broke privacy law by sharing info, watchdog says
Canada's secretive electronic spying agency realized in 2013 it was breaking domestic privacy rules by transferring Canadians' data to allied countries, but the government kept the mistake under wraps for two years. The transfers were discovered by the spy agency, the Communications Security Establishment, at a time when the questionable practices of national security agencies were being revealed by U.S. whistleblower Edward Snowden in 2013. The agency said it quickly informed the defence minister at the time, as well as the watchdog that reviews its operations. Rob Nicholson, who was Conservative defence

minister when the transfers were discovered, could not be reached for comment Thursday (...) But metadata may not be as innocuous as it sounds. The former head of the National Security Agency, CSE's American counterpart, famously pointed out that the U.S. kills people based on metadata. CSE describes metadata as the "context" of Internet and telephone data, not the "content." Toronto Star, A1; Canadian Press (London Free Press, B1/Front, Times Colonist, Times & Transcript, Red Deer Advocate, Chronicle Herald, National Post, Waterloo Record, Ottawa Sun, Toronto Sun, Winnipeg Sun, StarPhoenix, Windsor Star, Gazette, Leader-Post, Calgary Herald, Edmonton Journal, Edmonton Sun, Whig-Standard, calagary Sun, Hamilton Spectator, Daily Gleaner); Globe and Mail, A1; * La Presse canadienne (Le Droit, 32); * La Presse canadienne (Le Nouvelliste, 24); * Journal de Québec, 25 (Journal de Montréal); * Journal de Québec, 25; * Agence France-Presse (Le Devoir)

*** Kurdish allies terrorists under Canuck law?**

The notion that Canadian volunteers fighting with Kurdish forces in northern iraq and Syria could face prosecution under the former Conservative government's tough anti-terror laws has one human rights group calling for stricter supervision of the country's military training mission. A secret "Canadian Eyes Only" analysis of the Kurdish peshmerga, prepared by Transport Canada's intelligence branch, warns there are some factions of the militia group that are designated as terrorist entities under federal law. "Any Canadians claiming to have links to organizations such as the People's Worker Party (PKK) are likely to become the subject of Canada's antiterror legislation," says the report to the department. The assessment comes to light following an amnesty international report last week that accused peshmerga forces of bulldozing, burning and blowing up arab villages in apparent retaliation for supporting islamic State of iraq and the Levant. Canadian special forces are training Kurdish fighters, and the Trudeau government is preparing to significantly increase the size of that commitment. Canadian Press (Ottawa Sun, A9, Toronto Sun, Winnipeg Sun, Calgary Sun, Province, Windsor Star, Leader-Post, Vancouver Sun, Calgary Sun, Ottawa Citizen, Whig-Standard, Edmonton Sun); * Times & Transcript, B3

*** Privacy report reinforces need for overhaul**

To learn that our digital surveillance agency broke privacy laws by revealing information about Canadian citizens to our allies is one thing. To learn that the Conservative government of the day, when apprised of this security breach, withheld the information from Canadians, is quite another. But that is where we are today, after learning of a major invasion of Canadian privacy more than two years after the fact. If our spy agencies, aided and abetted by the government of the day, wanted to fuel suspicion of internal surveillance in this country, they succeeded. If they wanted to ratchet up distrust, they scored. This despite an effort Thursday to get ahead of this story with the first-ever background briefing for journalists from an official with the Canadian Security Establishment (CSE) - only 26 months after a software glitch was discovered that was sending metadata on Canadians to our Five Eyes allies without the proper scrubbing to hide identities. How many Canadians? We don't know. What did the allies do with the information? We are only left with the assurances of Defence Minister Harjit Sajjan that our relationship with those allies, including the U.S. National Security Agency, was "solid" and they wouldn't take advantage of an honest mistake. Toronto Star, A12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Hells Angels turfed from Hamilton haunt

A visiting Hells Angels member from Europe has been detained under a rarely used section of the Immigration Act after a landlord evicted the Hamilton chapter from its clubhouse for non-payment of rent. A bailiff, aided by 10 officers from the Hamilton Police Service and OPP Biker Enforcement Unit (BEU) drilled through the front door of Hells Angels' rented and fortified bunker at the corner of Gage Avenue North and Beach Road Thursday morning. The clubhouse is used by the Hells Angels motorcycle club as well as their puppet club, the Red Devils, according to Det. Staff Sgt. Len Isnor, the OPP officer in charge of the joint-forces BEU. (...) Police were there "to ensure public safety and keep the peace during the proceeding," according to Const. Steve Welton, Hamilton police media officer. He added that the eviction went smoothly and Hamilton police are "not conducting any criminal investigations there." However, the only person inside the clubhouse when the bailiff and police arrived was arrested by the Canada Border Service Agency (CBSA), Isnor said. Lawyer Jaime Stephenson, speaking on behalf of the

club, said the man - whose name was not revealed - would be "returning to Germany on his scheduled flight" Thursday evening. The man was visiting from Europe and is a "prospect member" of the Hells Angels, Isnor said. Under Section 37 of the Immigration and Refugee Act, any foreigner who comes into Canada and is part of a recognized criminal organization can be arrested - even if they do not have a criminal record, he said. Typically, a detention review hearing must take place within 48 hours of someone being taken into custody, said a CBSA spokesperson, who added that specific charges under the act "are not in the public domain" until a hearing takes place. (...) "Usually we don't have foreign (Hells Angels) in Canada," Isnor said, because most of the time, border agents nab organized crime members before they are able to enter the country. But in this case, the man is not yet a full-fledged Hells Angel and so may have slipped past them. Waterloo Region Record, B4 (Hamilton Spectator)

New cargo hub slow to bring in tenants
Progress on a cargo hub at Windsor Airport is behind what was suggested in a 2010 study commissioned by the city, and the one tenant so far is getting a "sweetheart deal" with rental rates, according to a former city councillor. Alan Halberstadt voted for the deal when he was on council, but now says he wouldn't have if he had been given details he recently received through a freedom of information request. The documents include the rental deal FedEx has with the city for being the first tenant in the $16.8-million cargo hub building. (...) The Institute for Border Logistics and Security, a partnership between the City of Windsor and the University of Windsor, will occupy 10,000 square feet. The city will also continue seeking tenants for the facility's remaining 27,000 square feet. "The cargo-hub development at the airport offers huge potential for employment and economic generation to the city of Windsor," Mayor Drew Dilkens said this week. (...) Windsor Airport is its own success story, going from a drain on city taxpayers to last year for the first time providing the city with a $1 million dividend. The same is expected this year. But as successful as Windsor Airport has become, with new airlines and destinations and an increasing number of passengers, it's still not enough for another thing that was supposed to give Windsor an edge with a new cargo hub: U.S. border pre-clearance. Former American ambassador to Canada James Blanchard was even hired to lobby Washington on the idea years ago, though little came of it. Still, Dilkens hopes with a new Canadian government in power, U.S. pre-clearance could one day become a reality. Either way, he sees good things coming. Windsor Airport is flying. And the longwished for cargo hub is about to start, with a global brand in FedEx. Windsor Star, A1/Front

The man without a country
The Supreme Court of Canada doesn't want Deepan Budlakoti either. On Thursday, the country's top court declined to hear the case of Canada's "stateless" man, whom the government has been trying to deport for years. "I'm stateless in the country I was born in - what am I supposed to do?" Budlakoti said in a statement released by his supporters. "I will continue to fight, no matter how many court challenges I have to launch." Budlakoti, 26 , was born in Canada, holds an Ontario birth certificate and was issued a Canadian passport. The government, however, says he is not a citizen and began trying to deport him since he was convicted of drug and firearms trafficking in 2010. (...) Budlakoti's immigration lawyer Yavar Hameed said Budlakoti's final plea to avoid deportation is before the United Nations Human Rights Committee and backed by the Canadian Civil Liberties Association. (...)The courts have said Budlakotih as a number of options open to him, including asking for Canadian citizenship or seeking Indian citizenship - avenues that have been open to him for years, but which he has never explored. India says they have no record of his citizenship and has refused to issue him a travel document. A Canadian citizenship application would likely be marred by his criminal convictions. Ottawa Sun, A3 (2016-01-29); * CBC News (2016-01-28)

*** André-Michel Boyer : Recherché pour meurtre au premier degré et outrage envers un cadavre**
MISE À JOUR: Il s'est livré de lui même cet après-midi aux enquêteurs de la Section des crimes majeurs du Service de police de la Ville de Montréal, moins de 24h après la diffusion de l'avis de recherche dans les médias. L'information a été confirmée à 15h35 par le SPVM. André Michel Boyer rencontre présentement les enquêteurs. (...) Les enquêteurs cherchent à localiser le suspect qui se serait rendu au Costa Rica et en Asie avant de revenir au Canada, le 11 janvier 2016, selon l'Agence des services frontalier du Canada. Un mandat d'arrestation pan–canadien a depuis été émis envers André Michel Boyer pour meurtre au 1er degré et pour outrage envers un cadavre. Zone 911 (2016-01-28)

Border officers seize marijuana
U.S. border officers at the Ambassador Bridge seized 76 pounds of marijuana Wednesday that was hidden in a truckload of auto parts. Customs and Border Protection said a 56-year-old truck driver arrived at Detroit's Fort Street cargo facility with a load of auto parts. After the driver declared the auto parts, an officer decided to put his truck through an X-ray inspection. The X-ray revealed "unusual shapes" in the back of the trailer. Officers broke the seals on the trailer and opened it up. They allegedly found two duffel bags stuffed with 68 bundles of marijuana. Officers seized the weed and turned the driver over to U.S. Homeland Security Investigations. U.S. Customs and Border Protection said the driver was a member of the Free and Secure trusted trader program. "The Free and Secure Trade program affords low-risk drivers to move through customs between the United States and Canada with minimal delay," said John Nowak, acting port director in Detroit. "Violations will result in immediate revocation and, in this case, prosecution to the fullest extent of the law." Windsor Star, A3

* **Windsor's weather, traffic and gas prices for Friday**
There is up to a 30-minute delay for commercial vehicles entering Canada at the Ambassador Bridge. At the Windsor-Detroit Tunnel there is a 10-minute delay for passenger cars. CBC News

* **Canada Confirms It Will Sign TPP Next Week**
Canada will sign the Trans-Pacific Partnership (TPP) agreement next week at a TPP meeting in New Zealand -- but this doesn't mean the deal is ratified. In an open letter regarding the massive, multi-lateral trade deal, Canada's Trade Minister Chrystia Freeland said Canada will attend next week's meeting in order to remain at the table with the other countries, but Freeland says this will not seal the deal, as more consultation and examination is needed. "Many Canadians still have not made up their minds, and many more still have questions," Freeland said in her letter. "That is why our consultations with the provinces, municipal officials, students, labour leaders and members, business representatives, academic experts, and others are just the beginning of the examination needed to fully understand the TPP's impact." (…) Ron Bonnett, president of the Canadian Federation of Agriculture, thinks this move is a good sign. "I think the government has recognized the negotiated deal was a balance," he says. "We can't be outside the deal. If all of a sudden the United States and Australia — the two main players I'd be worried about — have access to the Japanese market in a preferential way to Canadian producers, we'll be shut out of those markets." Steinbach Online

402 overpass damage leads to charges
Charges have been laid in last fall's collision between a tractor-trailer and an overpass that knocked out a stretch of busy highway near the Canada-U.S. border for several days. Two-way traffic on the Indian Road overpass at Highway 402 in Sarnia resumed only after a temporary fix following the Nov. 23 collision. (…)The 402's eastbound lanes reopened Nov. 26 after the damaged section was removed. The southbound side of the overpass is still awaiting repair. Lambton County has spent $100,000 on a temporary fix to allow overpass traffic to move in both directions. London Free Press, A3

Ottawa yet to conduct on-site inspections under new foreign worker program
The federal government has yet to conduct a single on-site inspection of employers under the new International Mobility Program, which was created as part of a heavily promoted overhaul of the Temporary Foreign Worker Program. In response to controversy, the Conservative government moved in 2014 to split the foreign worker program into two, with the creation of a new International Mobility Program aimed at more highly skilled workers. At the time, the government promised the new offshoot program would include "a robust compliance system, featuring inspections of thousands of employers." Those promised inspections were aimed at ensuring foreign workers received the wages they had been promised and that workplaces were free from abuse. Regulations for the new program came into effect on Feb. 21, 2015. However, newly released data show the enforcement activity has fallen short of the high bar Ottawa promised. (…) However, the 2014 decision to split the TFWP into two parts also created the International Mobility Program. Under that section, employers can bring in a foreign worker without having to prove they were unable to hire locally. The International Mobility Program includes workers who come to Canada under free-trade agreements such as the North American Free Trade Agreement. The flow of cross-border labour under the program is expected to increase, should Canada follow through with two proposed free-trade deals. They include the Comprehensive Economic and Trade Agreement with

the European Union and the Trans-Pacific Partnership agreement, involving Canada and 11 other Pacific Rim nations. Globe and Mail, A4

Escalating lumber exports expected to stir U.S. duties
The boost Canadian lumber exports are getting from the falling loonie is certain to bring out protectionist forces in the U.S. lumber lobby, said the CEO of Quebec-based forestry company Tembec. "I think that they're watching the Canadian dollar drop, particularly in lumber, and they're saying, 'This isn't fair,'" CEO James Lopez said Thursday. While groups such as the U.S. Lumber Coalition didn't complain about the Canadian dollar when it was above parity, Lopez suspects they will use the loonie's slump to argue that American producers are now at a competitive disadvantage, particularly since the Canada-U.S. softwood lumber agreement expired in October. (…) In 2006, Canada and the U.S. signed a nine-year agreement that set aside lawsuits and punitive tariffs against imported wood from Canada. It brought temporary peace in a dispute over whether Canadian lumber businesses receive an unfair subsidy through cheap access to public land. (…)The U.S. Lumber Coalition declined to comment on whether currency fluctuations have changed its view of the trade agreement. But it said it is pushing for a renewed softwood lumber agreement before a so-called standstill period, which prevents the U.S. from bringing trade action against Canadian softwood lumber producers, expires this October. (…) Canadian forestry companies are expected to save tens of millions of dollars this year because export tariffs and duties are no longer payable for one year following the expiry of the softwood lumber agreement three months ago. Canadian Press (Times Colonist, B1/Front, Cape Breton Post)

*** Tomas Tales: Canadian Motor Speedway Traffic Plan gets The Thumbs Up from Big Thumbs!**
This was enormous, and a long time in the process! Major stakeholders involved in the Canadian Motor Speedway Traffic Management Plan, or the TMP as we call it for short, have given CMS their support and final input on the implementation of what Executive Director Azhar Mohammad calls an "unprecedented document". And that's exactly what it is. The goal of the meeting in St.Catharines this week at The 4-Points Sheraton Hotel, where they make excellent sandwiches, was to get closer to the end of the Ontario Ministry of Transportation's (MTO) final process to approve the CMS TMP with a final review and consensus by those organizations and bodies who will have a hand in the traffic management process for major CMS events. The list of those in the meeting was very impressive. These are the key decision-makers who will ultimately make sure the fan experience, coming from both sides of the border to CMS is a pleasant and safe one. People like The Ministry of Transportation of The Province of Ontario, The Niagara Region, The Town of Fort Erie, The Niagara International Transportation Technology Coalition, Canada Border Services Agency, Department of Homeland Security, and of course The Ontario Provincial Police, The Niagara Regional Police Service, and Niagara Emergency Medical Services. The meeting was really one of the final steps after years of in-depth painstaking discussions with specific agencies responsible for traffic, transit, emergency services, border crossings and the QEW corridor which will service the facility. Sportsnet (2016-01-28); News Talk 610 CKTB (2016-01-28)

*** CLOSEUP: Banner year for Canadian operators**
Let the good times roll. The lower Canadian dollar is encouraging more Americans to visit and more Canadians to stay at home. At Fallsview Casino in Niagara Falls, business has been "solid since the spring of last year" and they have continued to experience measurable growth in the summer and fall of 2015. "January is following the same trend," said director of communications Greg Medulun. The favourable exchange rate and lower fuel costs, he added, is "definitely encouraging more Americans to visit." (…) Last year, a projected $3 billion was spent by tourists on same day and overnight stays in the peninsula's hot spots for travellers. Even so, the body blows to area tourism have been repeated — from the September 11, 2001 terror attacks, to new U.S. passport requirements and the 2008-09 recession. (…) To that end, a falling loony isn't the only positive sign, she said. Americans avoiding trips across the Canadian border now have less reason to do so, with 35 per cent of them now having a required passport, when only 15 per cent did in 2000. Niagara Falls Review (2016-01-28)

*** Guns finally go silent at Chilliwack's RCMP open-air gun range**
Conspicuous in their absence, volleys of gunfire no longer ring out near the Vedder Bridge as regular weekday Rotary Trail users and University of the Fraser Valley (UFV) staff and students have noticed. It was April 2014 when those behind the RCMP's Pacific Regional Training Centre (PRTC) announced $19

million in federal dollars to build the new indoor firing range to replace the open-air range, long the bane of UFV students and faculty, Vedder Crossing residential neighbours and Rotary Trail users. The new range is to be used to train and re-certify RCMP officers as well as agents with the Canada Border Service Agency (CBSA), and is a 4,000-square-metre building with two 16-lane, 50-metre ranges with advanced sound abatement technology. Chilliwack Times (2016-01-28)

Smart, reliable, experienced - and going nowhere
An opinion piece states, "You probably know someone who can figure anything out but doesn't have a Canadian degree or diploma; someone who is smart, well-organized and always comes through in a crunch, but stuck in an entry-level job; someone who could single-handedly improve the productivity of most workplaces but won't get the chance. There are 884,238 people like that in Canada, according to the Conference Board of Canada. They could earn an additional $13.4 billion to $17 billion if their skills, resourcefulness and experience were recognized, the Ottawa think-tank estimates. "Learning recognition systems need to evolve if Canada is to get the most out of its workforce," says Michael Bloom, vice-president of the Conference Board in a report released this week. Ottawa can do a better job of integrating credential recognition into its immigration selection and settlement process. After the 2013 debacle over temporary foreign workers, then-immigration minister Jason Kenney said he would link immigration to the labour market. But the Conservative government made little headway. Post-secondary institutions can accelerate their expansion into countries that produce large numbers of immigrants to Canada (China, India, the Philippines and Pakistan), offering students credentials that Canadian employers will recognize. They can also develop faster and more transparent procedures for assessing the credentials of graduates trained abroad." Toronto Star, A15

*** Organized crime possibility a concern**
A letter to the editor states, "I was interested in the article, "OPP tobacco team launched" (Chatham Daily News, Jan. 27). Indeed, it might be tempting to be able to buy a carton of cigarettes for less than $20, but lots of people don't realize it's contraband. I knew that smoke shops across First Nation communities in Ontario legally sell tobacco products that are both excise taxed and non-taxed. And, as the news story states, non-taxed tobacco products are illegal to buy, possess or distribute without proper authorization. Apparently, smoke shop operators on reserves are supposed to ask for identification when selling untaxed tobacco products. I wasn't aware of the scope of purchasing contraband tobacco until I read this story. And I certainly wasn't aware this is sometimes linked to organized crime. (…)The Ontario Ministry of Community Safety and Correctional Services has announced steps to snuff out illegal tobacco sales, using the OPP, the RCMP, Canada Border Services and international agencies. Apparently drivers could even be questioned about the possession of tobacco products found during traffic stops caused by a Highway Traffic Act offence. It amazes me – and scares me – that a packet of cigarettes could be providing cash for organized crime." Chatham Daily News (2016-01-28)

CYBER SECURITY / CYBERSÉCURITÉ

*** CBC adopts SecureDrop to allow for anonymous leaks**
CBC News is launching a powerful new tool to help those with important information or sensitive documents contact our journalists using encryption and anonymous online messaging. CBC's SecureDrop is a web-based system that allows whistleblowers to confidentially reach CBC journalists, including those who work in investigative units across Canada and on our leading programs the fifth estate, Go Public and Marketplace. CBC News

*** Ministry broke rules, leading to data breach: Privacy czar**
British Columbia's Education Ministry lost personal information pertaining to 3.4 million students when staff breached security policies and misplaced a hard drive with data stretching back 30 years, an investigation has revealed. Privacy Commissioner Elizabeth Denham said in a report released Thursday that the ministry did not secure a portable hard drive when the information was transferred from computer servers in an effort to save on storage costs. Globe and Mail, A5

*** Privacy concerns raised over webcams**
A young child asleep on a couch in Israel. Mourners huddled together at a small funeral in Brazil. An elderly woman stretching in a fitness centre in Poland. All available for anyone to watch via the unsecured webcams overhead. This isn't "1984," it's the world in 2016. Shodan, a search engine that indexes computers and devices rather than information, now allows users to pull screenshots from nanny cams, security cameras and other connected devices around the world that don't ask for a username or password. Canadian Press (Red Deer Advocate, C5)

*** U.S., British spies hacked Israeli air force: reports citing Snowden**
The United States and Britain have monitored secret sorties and communications by Israel's air force in a hacking operation dating back to 1998, according to documents attributed to leaks by former U.S. spy agency contractor Edward Snowden. Israel voiced disappointment at the disclosures, which were published on Friday in three media outlets and might further strain relations with Washington after years of feuding over strategies on Iran and the Palestinians. Reuters (Yahoo! News)

*** Privacy breach a failure of 'executive leadership'**
An opinion piece states, "For the sake of a $14,000 saving in storage costs, the B.C. Education Ministry embarked on a botched data backup scheme that risked breaching the personal privacy of millions of British Columbians. So said Information and Privacy Commissioner Elizabeth Denham Wednesday upon releasing the findings of an investigation launched last fall when the ministry reported it misplaced a computer hard drive containing data on some 3.4 million school students, their families and some teachers..." Vancouver Sun, B6

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** HIV-positive woman didn't infect man**
A Winnipeg woman convicted of aggravated sexual assault after having sex without disclosing she was HIVpositive may have exposed her victim to the virus but it is almost certain he contracted it from somebody else, a judge has been told. Marjorie Schenkels, 27, was found guilty of aggravated sexual assault following a jury trial last year. On Thursday, Schenkels' doctor told court her viral load is so low it is considered "undetectable." That points to another person being responsible for infecting the victim, defence lawyer Ian Histed told Justice Colleen Suche. "The odds here are extremely unlikely that he got the HIV from Ms. Schenkels," Histed said. "This is a case of exposure, not transmission." Crown attorney Manoja Moorthy said jurors could have convicted Schenkels of attempted aggravated sexual assault if they believed someone else had infected the victim. "We are asking the court to make the inference the jury did find (the victim) contracted HIV from Ms. Schenkels," Moorthy said. Histed is asking Suche to grant Schenkels a suspended sentence while the Crown is recommending a sentence of five years in prison. With medication, HIV is much more manageable than it once was. Still, "it's not the consequences only that we have to look at, but the moral blameworthiness (of the accused)," Moorthy said. In a police interview video played at her trial, Schenkels admitted she should have disclosed her diagnosis to the now 38-year-old victim but said she was "in denial." "I was still pretending I didn't have it and I continued to pretend I didn't have it until a few weeks ago," Schenkels told Gimli RCMP in the May 2012 video. Postmedia Network (Winnipeg Sun, A12)

*** Un influent motard trouvé coupable 23 fois**
Un influent motard de terrebonne dont la tête vient d'être mise à prix par la mafia italienne a subi un cuisant échec, hier, au terme d'une saga judiciaire de presque dix ans.Sergio Piccirilli, un ami de longue date du chef présumé des Hells Angels, Salvatore Cazzetta, a été déclaré coupable de 23 chefs d'accusation par la juge Marie- Suzanne Lauzon. Entre 2005 et 2006, l'homme de 56 ans a trempé dans le trafic de méthamphétamine, de cocaïne et de cannabis, en plus de comploter en vue de l'importation de produits servant à fabriquer des speeds dans un laboratoire clandestin à Laval. Des verdicts de culpabilité pour gangstérisme et possession illégale d'armes prohibées -dont une carabine semi-automatique et des silencieux -ont aussi été rendus contre ce membre fondateur des Devils Ghosts, un clubécole des Hells Angels. Piccirilli comptait parmi les 36 suspects appréhendés par la GRC lors du projet d'enquête Cléopatre, en juin 2006. Journal Montreal, 14

*** Fraud probe evidence raises**

Interviews conducted by B.C. Securities Commission investigators and read into evidence in a securities commission fraud hearing against Ayaz Dhanani reveal a complex real-estate transaction with connections to alleged fraud and organized-crime players. This raises big concerns about Vancouver's property market and the B.C. Real Estate Act. In late December 2014, Vancouver realtor Liang Ming Wei walked into the frenetic dining hall of Floata in Chinatown. With hundreds of diners and waiters racing around with steaming plates of dim sum, the Keefer Street restaurant was perfect for an obscure transfer. Wei had arranged for three million yuan to be deposited in a Chinese bank and transferred to a Richmond currency exchange. Exchange owner Tony Xu called Wei and told the realtor his client's cash had arrived and it was converted to $521,470 Canadian. It was 10 times the legal amount individuals are allowed to transfer from China. And it was 50 times over the $10,000 limit that must be reported under Canada's antimoney-laundering laws. Instead of having Wei come to his Richmond location to pick up the cash, Tony Xu said it was better for the realtor to meet his brother Frank Xu in Vancouver. Wei's client, Zhongyun Zhang, a Chinese transportation professional, had come to Vancouver in August 2014 and set up a Bank of Montreal account with Wei's help (...) In 2011 Cheng was arrested and charged in Calgary with three others in a joint, organized-crime fraud investigation involving the Calgary Police Service and the RCMP Commercial Crime section. Calgary's economic crime unit said the four were part of "a commercial enterprise" of "organized" cells sent from B.C. to Alberta to steal cash advances from casinos and buy high-end clothing and electronics using counterfeit credit cards. Province, A10

*** Police in no rush to probe Ponzi fraud**

Mismatched priorities: Government cracks down when ICBC is defrauded, but victims of investment scams seldom get justice. The RCMP won't go after a man who bilked more than 100 people out of nearly $12 million, a decision that emphasizes the lack of will to tackle whitecollar crime. The Insurance Corp. of B.C. and the government that owns it prosecute anyone suspected of car insurance fraud, but the authorities rarely give commercial fraudsters the same treatment. Consider that a B.C. Securities Commission panel recently concluded Thomas Arthur Williams and his Global Wealth Creation group of companies committed fraud and raised money illegally with the help of commissioned finders. The panel found that between February 2007 and April 2010, Williams masterminded a Ponzi scheme that fraudulently raised about $11.7 million from 123 investors across Canada and in the U.S. "Instead of investing the funds as Williams represented, investor funds were used to make payments to earlier investors, pay commissions to Williams and to pay money to third parties," the panel concluded. Roughly $4.9 million was returned to investors in makebelieve interest payments on their non-existent investments. Most of the $6 million that vanished, the panel said, was sent to entities controlled by or connected to crooks such as Michael Slamaj, sentenced in 2002 in the U.K. to six years in prison for fraud and possession of fake bonds. Williams, of Surrey, personally pocketed at least $440,000 and ignored the hearing. He did not return calls requesting comment. Vancouver Sun, A2

*** Un citoyen du Nord-Ouest coupable d'avoir poignardé son chien**

Un individu accusé d'avoir poignardé et abandonné son chien a reconnu sa culpabilité face aux accusations de cruauté animale déposées contre lui. Il connaîtra sa sentence le 7 mars. Les incidents reprochés à Marc Couturier, de Saint-Joseph, remontent à mai 2014. Il est accusé d'avoir attaché à un arbre et laissé à l'abandon son chien dans un secteur boisé près du chemin Maxim. Le corps de l'animal était perforé à trois endroits lorsqu'il a été retrouvé. Les plaies ont été commises avec un couteau. Ce sont des passants qui ont découvert l'animal mort et qui ont averti les autorités policières. Dès le lendemain, la GRC, assistée de la Société pour la prévention de la cruauté animale, a demandé l'aide du public et a rapidement obtenu des informations sur qui était le propriétaire du chien. L'individu est passé aux aveux durant son interrogatoire. L'homme âgé de 29 ans a inscrit un plaidoyer de culpabilité lors du début de son procès, jeudi. Il connaîtra sa sentence le 7 mars. Lors d'une comparution antérieure en septembre 2014, il avait reconnu sa culpabilité face à ce méfait. Les deux avocats en cause s'étaient entendus qu'une amende de 2000 $ était la peine appropriée. A ce moment, la juge Brigitte Volpé a dit vouloir consulter la jurisprudence au Canada avant de rendre la sentence. Les réactions à l'amende de 2000 $, que plusieurs estimaient inadéquate, ont été sévères dans les médias sociaux. Acadie Nouvelle, 8

*** Meurtre près de Campbellton**
La GRC continue d'enquêter sur le meurtre d'un homme âgé de 77 ans de Dawsonville. Le 9 janvier, un peu avant 12 h 30, des policiers se sont rendus à une résidence du chemin Restigouche River. Le corps d'Emerson Main a été trouvé à l'intérieur de sa demeure. L'autopsie a permis d'établir que le décès de M. Main est un homicide. La GRC refuse par contre de dévoiler les détails de l'autopsie, à savoir la cause du décès ou encore à quand remonte le décès. La rumeur court que l'homme a été abattu par balle, ce que refusent de confirmer les policiers. La GRC souligne que «les enquêteurs ont fait le suivi de plusieurs pistes en lien avec le décès de M. Main et ils poursuivent l'enquête». «Nous avons reçu des renseignements et nous en faisons le suivi, déclare la gendarme Jullie Rogers-Marsh de la GRC. Nous continuons tout de même à demander aux membres du public de communiquer avec la police s'ils pensent avoir des renseignements qui pourraient aider à élucider le meurtre d'Emerson Main». Quiconque a des renseignements est prié de communiquer avec le Déta-chement de Campbellton au 789-6000. Pour conserver l'anonymat, il est aussi possible de communiquer avec Échec au crime. Si vos renseignements mènent à une arrestation, vous pourriez être admissible à une récompense en argent pouvant aller jusqu'à 2000 $. Acadie Nouvelle, 11

*** RCMP seize meth, cocaine**
Three men face drug trafficking charges after RCMP recovered a stash of cocaine and meth from a Red Deer home. Mounties had been working a drug trafficking investigation on Jan. 14, and raided a home eight days later in the community of Clearview Ridge. They found 217 grams of cocaine, almost 49 grams of meth and $2,100 in cash. They also found two men, who were promptly arrested. While authorities were searching the home, a third man stumbled into the raid in progress. When officers searched him they found nearly a quarter pound of cocaine and $33,547 in cash. He too was arrested. Damon Rhys Meidinger, 22, of Red Deer, and Justin Davis Yakimchuk, 23, of Blackfalds, are charged with possession of stolen property over $5,000 and two counts of possession for the purpose of trafficking. Meidinger was released from custody and Yakimchuk was remanded in custody. Postmedia Network (Edmonton Sun, A38, Calgary Herald)

*** Escaped con fails in hijack attempt**
A 16-year-old B.C boy and tha baby he was travelling with were the victims of a "harrowing" carjacking by an escaped Alberta prisoner earlier this week. Police have released more details into the pursuit of 29-year-old Harley John Lay, a prisoner from Peace River Correctional Facility, who was sprung from police custody on Monday near the Peace River hospital by a masked armed man. A third person driving a white minivan acted as a getaway driver. Police say they first received reports of their whereabouts at around 10:30 a.m. Tuesday after Lay, and one other male suspect, confronted an employee at a Husky bulk fuel plant along the Alaska Highway after running out of gas just south of Fort Nelson, B.C. Northern Rockies RCMP Cpl. Dan Moskaluk says the employee recognized Lay and eventually called police, who set up on the highway and attempted to stop the oncoming van. Moskaluk says officers successfully deployed a spike belt but failed to bring the van to a full stop. "At least one front tire was punctured, and running on its rims," said Moskaluk. Postmedia Network (Edmonton Sun, A11, Edmonton Journal)

Pornographie juvénile
Un jeune de Caraquet a été jugé, jeudi, à Tracadie, pour avoir détenu et distribué sur le web des images pornographiques incluant des enfants, en 2013. Son ordinateur portable contenait près de 6500 photos de ce genre. Il encourt deux ans de prison. Jonathan Laplante, 24 ans, affirme qu'il voulait juste se faire des amis sur internet. C'est pourquoi il leur a envoyé, via les réseaux sociaux, des photos et des vidéos de pornographie juvénile qu'il trouvait sur la toile. D'après lui, ces «amis virtuels» - qu'il n'a jamais rencontrés - le lui demandaient. L'argument a été énoncé jeudi, en cour provinciale de Tracadie, dans le cadre du procès. Il est poursuivi pour possession et diffusion d'images et vidéos pornographiques mettant en scène des enfants. Devant le juge Camille Vautour, il a plaidé coupable. L'avocat de la Couronne, Me Pierre Gionet, a suggéré au magistrat de le condamner à deux ans de prison assortis de plusieurs restrictions. La sentence sera prononcée mardi. Les faits remontent à 2013 lorsque la compagnie Twitter, basée aux États-Unis, détecte qu'un de ces utilisateurs distribue à un groupe restreint d'individus, des photos tout aussi indécentes qu'illégales. Elle alerte les autorités américaines qui s'aperçoivent que le compte est alimenté depuis la Péninsule acadienne. Ces dernières transmettent le dossier aux services

concernés. La GRC ouvre une enquête. Rapidement, Jonathan Laplante est identifié. Le compte Twitter est associé à son adresse courriel et à celle de son ordinateur portable. L'Acadie Nouvelle

Bomb threat at Come By Chance refinery

Operations at the North Atantic Oil Refinery in Come By Chance have returned to normal, following a bomb threat Thursday morning. Clarenville RCMP said in a news release, shortly after 11 a.m., the RCMP, in consultation with management at the North Atlantic Oil Refinery, "have determined that the site is safe. Operations are returning to normal." Police investigators were departing the scene. However, the investigation into the origin of the threat is ongoing. North Atlantic spokeswoman Gloria Slade issued a news release Thursday afternoon. "In consultation with the RCMP, this morning we activated our bomb threat procedure and conducted an extensive search of our refinery site. It has been concluded that this is not a creditable threat. The RCMP is continuing their investigation." The facility's first bomb threat came in October 2015. Support services were also called in at that time, including an explosives disposal team and a police service dog trained in explosives detection, with added help from the refinery security team and Come By Chance and Arnold's Cove volunteer fire departments. Nothing was found in that case, with an all clear given by 5 p.m. the same day. Telegram, A9

Crown witness in murder trial found

A Crown witness sought to testify in the second-degree murder trial of a Cape Breton man has been located in British Columbia. Ashley MacDonald is now expected to be returned to Cape Breton to testify in the trial for Thomas Ted Barrett, 40, of Glace Bay who is charged with the murder of 19-year-old Brett Elizabeth McKinnon. McKinnon, of Glace Bay, was first reported missing in 2006 and her skeletal remains were found in a wooded area near a former dump in 2008. MacDonald is a former girlfriend of the accused and was the subject of a witness warrant issued last week by Justice Robin Gogan, who is presiding over the trial with no jury. Officers with the Cape Breton Regional Police travelled to British Columbia last week in a bid to locate MacDonald. The officers were aided in their search by the RCMP. Neither the Crown nor regional police would confirm Thursday that MacDonald was in custody but other sources have confirmed to the Post that she was located and is expected to be returned to Cape Breton. The trial was scheduled to continue this week but was adjourned Monday in order to allow time to locate MacDonald. Cape Breton Post, A2

RCMP hits YouTube in N.B. murder case

The New Brunswick RCMP have produced a YouTube video that includes nine new photos of a fugitive murder suspect who is accomplished at altering her looks. Twenty-year-old Marissa Shephard hasn't been seen since mid December. Shephard is charged with first-degree murder and arson in the death of 18-year-old Baylee Wylie, whose body was found by firefighters Dec. 17 in a burned-out triplex in Moncton. In the video, Insp. Jamie George encourages viewers to share the video, saying people should have a close look at the wildly different images. The pictures are mostly selfies, showing Shephard in a wide range of appearances - from a pouting glamour shot with heavy makeup to less-guarded images that depict a happy schoolgirl. The Mounties say Shephard is considered dangerous due to the violent nature of the crime, but police have yet to release details about the cause of death or a possible motive. She is described as white, 5-foot-5 and weighing about 100 lbs. She has brown eyes, brown hair and has a tattoo with the name Stephen on the back of her neck and a tattoo of a crown on her chest. Postmedia Network (Telegram, B8, Guardian); Acadie Nouvelle, 11

B.C. mom and dad convicted of assault for spanking 14-year-old girl for sexting

A British Columbia mother and father who used a plastic hockey stick and a skipping rope to spank their 14-year-old daughter have been found guilty of assault with a weapon. A provincial court heard the couple from Salmon Arm, B.C., wanted to punish their daughter for sending nude photos to a young man over the Internet and instead of being grounded, the teen chose the spanking. Her father used a mini hockey stick two or three times on his daughter's buttocks over her pyjama pants and when her mother came home, she delivered a similar punishment with a skipping rope. When the girl went to school with lacerations and bruises, her friends told administrators, who called RCMP. Postmedia Network (Red Deer Advocate, A7, Times Colonist, Calgary Sun, Toronto Sun, Province)

*** Police commissioners mum on profiling claims**

The majority of members of the Re- gina Board of Police Commission ers defer to the chairman, Mayor Michael Fougere, when it comes to the issue of racial profiling. Allegations of racial discrimi nation against aboriginals by city police officers have been made by community members over the years, and more recently by Simon Ash-Moccasin. The Regina man was detained by officers in De cember 2014, an action the prov ince's Public Complaints Commis sion (PCC) said was unnecessary, though it did not suggest he was targeted because he is First Nations. Vic Pankratz and Gordon Selinger sit on the five-member committee to represent civilians on the oversight governing body for police officers. Both declined to comment when asked about claims of racial profil ing in the city. "It was a personal decision not to speak," Fougere said on Wednes day. "In any case, they just don't want to comment." Shortly after the board's first meeting of 2016, in which Fougere was acclaimed as chair, Pankratz said the mayor is the spokesman and his views are reflective of the board. "It's a personal choice but (Pan kratz and Selinger) also speak in public session of the commission," said the mayor. "They speak their opinion and they provide account ability in that way." The police commission has not yet publicly discussed racial pro filing. Wednesday's meeting was in stead dedicated to accepting notes of appreciation - social media praise from community members - and once again naming the may or as the board's chairman. Fougere and the board are confi dent the systems in place to moni tor allegations of racial profiling are working. Those systems - most notably the PCC - never have proven true an allegation of racial profiling or racism made against a Regina police officer. "If there are issues of inappropri ate conduct by the police service, issues of alleged racism or activi ties that are difficult, any member of the public can go to the Public Complaints Commission and lodge that complaint," Fougere said. "The commission will investigate and come back. They are indepen dent of the police service and those rulings stand." There have been more than 400 Regina-based complaints to the PCC since 2006. Leader-Post, A6

Bomb threat case delayed

A preliminary hearing into charges laid after a verbal threat was made to blow up Parliament last year has been re-scheduled at the Chatham courthouse. The hearing for David Osterbrook, 50, of Chatham, was set to begin Thursday, but a representative for the defence said the adjournment was needed due to an unforeseen scheduling conflict. Osterbrook was arrested April 10 after an RCMP officer received a phone call from a man ranting about anarchy and making threats to blow up Canada's parliament buildings. Police laid two charges, making a terrorist hoax and uttering a threat. Postmedia Network (London Free Press, A2)

Accusée d'avoir volé plus de 100 000 $ à son employeur

A l'issue d'une longue enquête, des accusations ont été portées contre une femme d'Astle, au Nouveau-Brunswick, en lien avec un vol et une fraude de plus de 100 000 $. Le 23 avril 2013, le Détachement de Blackville de la GRC a reçu une plainte au sujet d'un vol et d'une fraude. Une femme a été arrêtée en janvier 2014, mais aucune accusation n'avait été portée à ce moment. L'enquête s'est poursuivie. Le 7 décembre 2015, des accusation ont été déposées contre Gina MacKay-Munn, 46 ans: un chef d'accusation de vol de plus de 5000 $ et un chef d'accusation de fraude de plus de 5000 $. Les vols se seraient produits sur une période de quatre ans, soit de 2008 à 2012. Alors que Gina MacKay-Munn était employée chez O'Donnell Line and Electric, elle aurait volé et escroqué plus de 100 000 $ à l'entreprise. Gina MacKay-Munn comparaîtra lundi en Cour provinciale à Miramichi, à 13 h 30, pour inscrire son plaidoyer. Acadie Nouvelle, 11

*** B.C. teen and baby became victims of carjacking by escaped Alberta prisoner**

A 16-year-old B.C. boy travelling with a baby were the victims of a "harrowing" carjacking by an escaped Alberta prisoner earlier this week. Police have released more details into the pursuit of 29-year-old Harley John Lay, a prisoner from Peace River Correctional Facility who was sprung from police custody Monday near the Peace River hospital by a masked, armed man. A third person driving a white minivan acted as a getaway driver. Police said they first received reports of the men's whereabouts at about 10:30 a.m. Tuesday after Lay and one other male suspect confronted an employee at a Husky bulk fuel plant along the Alaska Highway after running out of gas just south of Fort Nelson, B.C. Northern Rockies RCMP Cpl. Dan Moskaluk said the employee recognized Lay and eventually called police, who set up on the highway and attempted to stop the van with a spike belt, but the van kept going. Officers caught up to the van at a Highway 97 Subway restaurant, where police arrested a lone female occupant. While making the arrest,

police received calls about a carjacking that occurred minutes earlier at the same Subway. "It was alleged that the two males obtained the vehicle by telling a 16-year-old male to get out of the truck," says Moskaluk. "The young man did have time to retrieve an infant that was in a car seat in the vehicle." The two escaped without injury. Vancouver Sun

*** Mounties describe harrowing recapture of escaped Alberta prisoner**

British Columbia RCMP are describing a "harrowing" attempt to recapture an escaped Alberta prisoner this week, saying at one point the man and an accomplice carjacked a 16-year-old boy and a baby. Cpl. Dan Moskaluk of the Northern Rockies RCMP says in a news release that the chase began Tuesday morning when employees at a Husky bulk fuel plant along Highway 97 reported seeing Harley John Lay, 29. While several Mounties stopped traffic on the highway, others moved in and tried to stop a minivan carrying the prisoner, but it got away.Down the road, they deployed a spike belt which slowed the vehicle as it continued toward Fort Nelson, B.C., with officers following at a safe distance behind with emergency lights and sirens activated. One the minivan hit city limits, the pursuit was stopped but officers later spotted the vehicle and approached it, arresting a female occupant without incident. Then, police received a report of a truck at a fast-food restaurant being carjacked. "It was alleged that the two males obtained the vehicle by telling a 16-year-old male to get out of the truck," says Moskaluk. "The young man did have time to retrieve an infant that was in a car seat in the vehicle." RCMP found the truck in a ditch. Moskaluk says police allege Lay and a second male tried to commandeer another vehicle but traffic would not stop for them. They were arrested without incident. Mounties allege Lay escaped on Monday while he was being escorted to a hospital in Peace River, Alta. Postmedia Network (Guardian)

*** Legalized Marijuana could boost economy**

Call it Prime Minister Justin Trudeau's secret stash. A new report from CIBC World Markets says Canada's federal and provincial governments could reap as much as $5 billion annually in tax revenues from the sale of legal marijuana. CIBC economist Avery Shenfeld crunched the numbers using current estimates of Canadian recreational pot consumption, the revenue experience in U.S. states that have legalized, and other factors - such as prevailing "sin tax" rates on alcohol and tobacco. "The bottom line is that federal (and) provincial governments might reap as much as $5 billion from legalization, but only if all the underground sales are effectively curtailed," writes Shenfeld. "That's on the order of 0.25 per cent of GDP, no barnburner." The Liberal government has promised to legalize, tax and regulate marijuana and has made MP Bill Blair, the former Toronto police chief, the lead on investigating a new regulatory model. Trudeau maintains that legalized pot will not be a cash cow, and that all revenues will be used to address mental health and addictions issues. "It was never about a money-maker, it was always about public health, public safety," the prime minister said in December during a year-end interview. The report uses Colorado sales figures to estimate a Canadian pot market worth about $10 billion annually, then looks at net profit margins from Ontario's government booze monopoly and other associated income and payroll taxes to come up with the revenue total. Shenfeld also suggests that the oft-touted law enforcement savings from pot legalization may not materialize due to ongoing international obligations to stop marijuana exports and the enforcement needed to curb the untaxed black market. Canadian Press (Windsor Star, N6, Province, Calgary Sun, Vancouver Sun)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Crown says managing man's risk 'speculative hope'

Superior Court Justice Gary Tranmer was asked Thursday to sentence repeat sex offender David A. Wilson to an indeterminate term in prison and to leave the question of when, if ever, he's released back into the community in the hands of the Parole Board of Canada. Assistant Crown attorney Megan Williams argued that managing Wilson's risk in the community, even at the end of a lengthy sentence with a fixed release date and a long-term supervision order of up to 10 years, would amount to little more than "speculative hope." (...)It was suggested to the judge by forensic psychologist Looman that Wilson's risk could be controlled in part by requiring him to live in a federal halfway house such as the recently built Henry Traill Community Correctional Centre. Henry Traill, which sits on land attached to Collins Bay Penitentiary fronting Bath Road, currently replaces the contentious Portsmouth Community Correctional Centre, and the psychologist suggested it would provide 24-hour-a-day supervision for Wilson. But

Williams observed that a supervisor of parole officers for Correctional Service Canada testified that Henry Traill doesn't offer that level of security. Lindsay Maahs testified that there are parole officers and parole officer supervisors available during centre's daytime office hours and commissionaires on duty at night, but no correctional service officers. There used to be corrections officers on duty, she told Justice Tranmer, but she said that ended four or five years ago "as part of a debt-reduction action plan." Consequently, Williams said: "Mr. Wilson requires residency with 24-hour supervision that does not exist." Kingston Whig-Standard, A1

Des fraudes... à partir de la prison
Dominique Duhaime devra demeurer six mois de plus derrière les barreaux pour avoir fraudé des personnes âgées pendant qu'il était emprisonné pour un autre dossier. Cet individu de 24 ans a été incarcéré à partir de 2014 de façon préventive pour un dossier de voie de fait causant des lésions corporelles et utilisation d'une arme à feu. Du 20 au 25 novembre 2014, il en a alors profité pour frauder trois personnes âgées et deux commerces de la région. En utilisant le téléphone de la prison de Trois-Rivières grâce à une carte d'appel, il a téléphoné à des aînés en se faisant passer pour leur petit-fils. Une fois qu'il avait réussi à les mettre en confiance, il prétendait avoir besoin d'argent, soit parce qu'il était hospitalisé, soit parce qu'il avait eu un accident d'auto. (...)En effet, Duhaime a écopé il y a quelques semaines d'une peine de cinq ans de prison pour voie de fait causant des lésions. Les six mois de prison pour les fraudes viennent donc s'ajouter à cette première sentence. (...)Notons qu'au pénitencier, ses appels téléphoniques seront contrôlés, car il devra fournir la liste des personnes qu'il peut appeler. Le Nouvelliste, 7

Agression nocture dans NDG : le suspect comparaît
Mathew Roberge, 25 ans, a comparu brièvement à la cour, ses cheveux longs attachés en queue de cheval. La poursuite s'est objectée à sa remise en liberté. Il reviendra en cour le 15 février pour son enquête sur remise en liberté. (...) Matthew Roberge était sorti de prison à la mi-octobre. Il avait écopé d'une peine de quatre ans de prison pour homicide involontaire après avoir asséné un violent coup de poing à un client dérangeant dans un bar de Laval, en 2013. L'homme était tombé, s'était cogné la tête et était décédé après avoir sombré dans le coma. Au moment du prononcé de sa sentence, Roberge avait déjà passé un certain temps en détention préventive, ce qui fait qu'il ne lui restait que 19 mois et demie à purger. Comme le veut procédure, aux deux tiers de cette peine, il a été libéré automatiquement, cet automne. La Presse, * Journal de Montréal (Journal de Québec)

Coupable de leurre informatique
Martin Bourque plaide coupable aux accusations de leurre informatique. Avec ce plaidoyer, il pourrait être déclaré délinquant dangereux au terme du processus judiciaire. L'automne dernier, l'ancien militaire de 37 ans avait déjà déclaré qu'il était pour reconnaître sa culpabilité aux actes qui lui sont reprochés. Après avoir été représentée par Me Gitane Smith et Émelie Ainsley, c'est finalement avec Me Justine Guay-Langevin qu'il a entériné les plaidoyers de culpabilité, jeudi après-midi, devant le juge Jean Hudon, de la Cour du Québec. Il est reconnu coupable de leurre informatique auprès de 16 victimes, de bris de probation, de ne pas s'être inscrit au registre des délinquants sexuels (ce qui a été fait lors de son arrestation le 3 juin), d'avoir eu en sa possession du matériel informatique et d'avoir eu accès à Internet. Sorti du pénitencier en février 2015 (30 mois pour du leurre informatique en 2013), Bourque n'a pas mis de temps à répéter son manège auprès de jeunes filles de moins de 16 ans. Dès le mois d'avril suivant, il tentait de les attirer sous la couverture. Le Quotidien, 4, * Journal de Québec

Kaven Sirois de retour en cour le 18 février
Les plaidoiries visant à déterminer le lieu de garde de Kaven Sirois, ce jeune homme condamné à la prison à vie sans possibilité de libération conditionnelle avant dix ans pour le triple meurtre de la rue Sicard, auront finalement lieu le 18 février. C'est du moins ce qui a été convenu, jeudi matin, entre le juge Bruno Langelier et les avocats Me David Guévin à la défense et Me Hippolite Brin à la Couronne. Rappelons que le 30 octobre dernier, Kaven Sirois a été assujetti à une peine pour adultes après avoir plaidé coupable aux six accusations portées contre lui, soit trois chefs pour meurtre au premier degré et trois autres pour complot pour meurtre. Il pourra demander une libération conditionnelle après 10 ans et non 25 ans puisqu'il était mineur à l'époque. Il reste maintenant à déterminer son lieu de garde. Les

possibilités qui s'offrent au jeune homme sont l'Institut Philippe-Pinel, une prison provinciale ou le pénitencier. Le Nouvelliste

*** Pair in major cocaine bust loses court appeal**
Two men convicted of possession for the purpose of trafficking in connection with the largest cocaine bust in B.C. history will continue to serve lengthy prison sentences. On Thursday, the B.C. Court of Appeal dismissed a bid by Scott Pedersen, a commercial diver and former Port Hardy fisherman, and Mexican fisherman Vincente Serrano-Hernandez to have their convictions overturned. The two men were found guilty in 2011 of transporting 1,001 one-kilogram bricks of cocaine from Panama to Port Hardy aboard the sailing vessel Huntress. In March 2010, Pedersen and Serrano-Hernandez off-loaded $26 million in cocaine into a waiting Zodiac at Shushartie Bay, near the northern tip of Vancouver Island. Justice Jennifer Power sentenced Pedersen and Serrano-Hernandez to 16 years in prison. They have more than nine years left on their sentences. The two appealed on the grounds that they were improperly arrested when they sailed into Port Hardy and that evidence found on board the Huntress during unlawful police searches should have been excluded. Police searched the Huntress four times without a warrant. The appeal court dismissed these grounds of appeal. Times Colonist, A3

*** Il aurait pu empêcher le meurtre qui l'a envoyé en prison**
«On a comploté pour voler et ça a mal fini. Je n'ai pas tué la victime, mais je me sens responsable quand même. J'aurais dû l'empêcher. J'aurais pu.» Maxime Bourdage aimerait bien revenir en arrière. «Il y a 1000 affaires que j'aurais dû voir. Que ce n'est pas normal de voler. Que ce n'est pas normal de partir avec un couteau et un marteau», a dit le jeune homme de 21 ans aux commissaires des libérations conditionnelles hier. Bourdage purge actuellement une peine de cinq ans au pénitencier à sécurité minimum de Sainte-Anne-des- Plaines relativement à des infractions de complot pour meurtre et complicité après les faits. Bien qu'il démontre «une certaine in-conscience inquiétante», le jeune homme a obtenu sa semi-liberté hier, un peu moins de deux ans après sa condamnation, en mars 2014. Journal de Montréal, 22

No parole for pervert
An editorial states, “The plea deal that notorious pedophile Peter Whitmore struck nine years ago with Saskatchewan justice officials to avoid his being designated a dangerous offender will doubtless be a talking point on the inevitable day this deviant applies for parole. If he'd been designated a dangerous offender in 2007, Whitmore would have been given an "indefinite" federal prison sentence - and the stigma of that designation as one of the worst of the worst would have carried additional weight against his ever getting parole. As it was, Whitmore pleaded guilty to a dozen charges, including kidnapping, sexual assault, sexual assault causing bodily harm and uttering death threats against two boys, aged 10 and 14, in 2006. He was given a life sentence, but would be able to apply for parole in 2013 - seven years from the date of his arrest. Thus far, Whitmore hasn't applied - but according to one recent media report, his former lawyer says Whitmore, now 45, wants to be released. Yes, the plea deal was controversial, but even if he'd been designated a dangerous offender, Whitmore also would have been eligible to apply for parole after seven years. In either case, parole isn't automatically granted.” Leader-Post, A8

*** Sex offender living in King Township prompts concern from residents**
Residents of a King Township community are expressing concern following the release of a sex offender deemed at high risk to re-offend and now living at a group home in the area. Keith Constantin, 35, was let out of prison last month after serving time for numerous sexual assaults and attacks, including some against children, which took place in Hamilton. He now lives in a group home run by non-profit organization Christian Horizons."[He] technically served his time but when you say you have urges to rape again and even kill, I'm pretty sure that designates him as a 'dangerous offender,"' said resident Amy Castellano. Castellano is behind a string of community protests and a petition to have Constantin deemed a dangerous offender. That status would allow the courts to impose specific residency conditions, an indeterminate prison sentence or electronic monitoring. Constantin's release has people in the community of Schomberg concerned about their safety and prompted a warning this month by police to students in York Region. It also spurred the creation of a task force on high-risk offenders whose members include a retired OPP officer, a retired corrections officer and two Schomberg residents, among others. CBC News (2016-01-28)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

We need a leaner, more modern police service
An editorial states, "Earlier this month, Deputy Chief of Toronto Police Peter Sloly told Torontonians he wants to "blow up" what he sees as the wasteful and ineffective reactive model of policing. He wants more prevention and greater use of technology to push community safety forward. The resulting emotional and ideological maelstrom - now in its second full week - is all too familiar when it comes to policing reform. And it stands as a harbinger of what may come as the provincial government embarks on what Minister of Community Safety Yasir Naqvi calls "the biggest transformation of policing in 25 years," over the next 18 months. The entire process runs the risk of being overtaken by the type of low-level political and personality contests that have surrounded Sloly's public intervention. (…) Policing costs in Canada are rising much faster than inflation and as fast as health costs - all while most measures of crime are dropping and demands for health services grow. This reality was not suddenly discovered by Sloly. The Drummond Report on controlling Ontario's spending warned of precisely this trend five years ago. In it, prominent public economist Don Drummond proposed evidence-based controls to reduce police spending. The report has since been gathering dust, while the province slips deeper into debt every year. Other careful studies backing Sloly have so far been under-exploited. **Public Safety Canada** has convened two major national conferences on the Economics of Policing and Community Safety in the last five years, leading to reports that emphasize precisely the solutions pushed by Sloly to replace the reactive model. The Harper Conservatives mostly sat on this information - and it's not at all clear that Justin Trudeau's Liberals will have the stomach to grab a fraught and unforgiving file that promises little political reward to reformers trying to move public opinion." Toronto Star

*** Inquiry must be more than political theatre**
An opinion piece states, "When justice ministers from across Canada met recently in Quebec City, Prime Minister Justin Trudeau promised that an inquiry into missing and murdered indigenous women and girls was at the top of the agenda. Federal Justice Minister Jody Wilson-Raybould was particularly interested in the perspective of her B.C. counterpart, Suzanne Anton, given the province's recent experience with a similar probe. That, of course, was the Oppal Commission, headed up by former B.C. attorney-general Wally Oppal, which looked into the disappearance of scores of women, mostly aboriginal, from Vancouver's Downtown Eastside starting in the late-1970s. Many of them were victims of mass murderer Robert Pickton. Mr. Oppal's report led to 63 recommendations, many focused on the behaviour of the Vancouver Police Department. The force was criticized for the lack of concern it demonstrated toward those who had vanished, a disregard many attributed to the dim view the police held of the poor, often drug-addled aboriginal women who called the Downtown Eastside home. Despite Mr. Oppal's best efforts, many in the aboriginal community were not pleased with his commission. Some felt it was not inclusive enough, saying it ignored too many points of view. Others felt the most important thing it accomplished was telling the story of the women themselves - before their lives took a terrible turn. Which brings us to Ms. WilsonRaybould's challenge. What does she do with her inquiry that will ensure it produces something worthwhile, and not just an expensive vehicle for people to vent?" Globe and Mail, A11

*** Bullies, beware**
An editorial states, "Cyber bullies, beware. Canada's courts are prepared to come down hard on people who publish intimate videos or pictures on the Internet without consent. And a good thing it is, in an era of "sexting" and "revenge porn." In the first case of its kind in Canada, Ontario Superior Court Justice David Stinson has just ordered a man to pay $100,000 in damages, plus $41,708 in legal costs and interest, to a former girlfriend for posting a sexually explicit video of her after promising he wouldn't show it to anyone. This sends a forceful and welcome message that abusing a partner's trust can carry a heavy cost. While "publication of an intimate image without consent" has been a crime in Canada since 2014, subject to up to five years in prison, this latest ruling fills a gap by setting a precedent in civil law as well. It establishes the right to sue for breach of confidence "if the matter publicized or the act of publication ... would be highly offensive to a reasonable person and ... is not of legitimate concern to the public." And rightly so, given the damage that can result." Toronto Star, A14, Globe and Mail

*** Nova Scotia woman's cyberbullying video mocked by bullies**

A Dartmouth woman who made an online video to raise awareness about cyberbullying says she has become the target of bullies, with thousands of comments pouring in. Courtney Bolivar, 20, made the video in July 2014. It depicts a young woman who gets a series of degrading text messages, then takes her own life as a result. "I've dealt with [bullying] my whole life and it's something that awareness really needs to be brought to," said Bolivar. "Cyberbullying is such a big thing these days, and it's just so terrible that I ended up getting cyberbullied for making a cyberbullying short film." The irony isn't lost on Bolivar, who noticed a video making fun of her work this week. The attack video shows Bolivar's face and name. After the video was posted by an anonymous user who goes by Leafy, thousands of comments flooded Bolivar's YouTube channel. "It was mocked, just basically making fun of the awareness of it and a lot in the video is said that cyberbullying doesn't exist and people can just close their laptop, turn off their phone," she said. "Now there are thousands and thousands of internet trolls and people just being hateful on all of my videos." CBC News

*** Spousal-violence numbers on decline: report - But local agency has not detected decrease in demand for services**

Family-violence rates in Manitoba are some of the highest in the country, but over the past decade the number of Manitobans reporting spousal violence has steadily declined, a Statistics Canada report has found. Manitoba has the second-highest rate of police-reported family violence among the provinces after Saskatchewan, according to the 2014 data. (The territories still have the highest overall rate of family violence in Canada, more than double the rate of violence in the provinces.) About 3.29 per cent of Manitobans in spousal relationships reported experiencing violence in 2014, down from 7.32 per cent in 2004. Over those 10 years, reports of violence between spouses declined in every province but Prince Edward Island. Rates of self-reported family violence suffered by aboriginal people aren't on the same decline - from 10 per cent in 2009 to nine per cent in 2014 - the report shows, and aboriginal people, particularly indigenous women, remain more likely to face family violence. About 10 per cent of aboriginal women were victimized by their current or former partners, compared with three per cent of non-aboriginal women. Klinic Community Health, which runs a crisis phone line and offers family violence counselling, has not seen a decrease in self-reported family violence, said Rosemarie Gjerek, the organization's director of counselling and community health. (...)Statistics Canada found 41 per cent of those who reported they were victimized by a former partner said the violence happened after the relationship ended. Winnipeg Free Press, B3

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

Le doute plane sur le nombre de parrainage privé de réfugiés syriens

Grâce à des soirées dans des bars, à des sites de financement collectif, à des soupers spaghetti dans des sous-sols d'églises et à des foires d'artisanat, des milliers de Canadiens tentent actuellement de ramasser l'argent nécessaire pour parrainer des réfugiés syriens. Il est toutefois difficile de déterminer combien de demandeurs d'asile syriens parrainés de manière privée le Canada finira par accueillir. Le programme des libéraux vise à amener le total à 25 000 réfugiés syriens au pays d'ici la fin du mois de février - auxquels doivent s'ajouter 25 000 autres d'ici la fin de l'année. Selon le plan initial, environ 10 000 du premier contingent de réfugiés devaient être parrainés par le secteur privé. Mais des renseignements récemment divulgués par le gouvernement indiquent qu'à la mi-décembre, les demandes de parrainage privées étaient insuffisantes. Des données fournies à la Chambre des communes en réponse à une question du Nouveau Parti démocratique (NDP) montrent qu'entre le 1er janvier et le 15 décembre 2015, le gouvernement a reçu des requêtes de parrainage privé pour 8214 personnes. (...)Selon les données, le délai de traitement pour les demandes de parrainage privé était en moyenne de 10 mois l'an dernier. Si les libéraux se disent toujours prêts à accueillir 25 000 réfugiés pris en charge par le gouvernement d'ici la fin de l'année, ils n'ont toutefois pas précisé combien de demandeurs d'asile parrainés par le secteur privé ils comptaient recevoir Au 26 janvier, 14 003 Syriens avaient mis les pieds au Canada depuis le 4 novembre, dont 8004 pris en charge par le gouvernement, 5112 parrainés par le secteur privé et 887 dans le cadre d'un programme mêlant public et privé. Près de 6000 autres Syriens ont reçu l'approbation pour venir s'installer au Canada, mais ne sont pas encore arrivés au pays. Presse canadienne (Acadie Nouvelle, 18); Canadian Press (Times & Transcript, B7)

Base 'on hold' for refugees
Military bases in Canada, including Canadian Forces Base Kingston, likely won't be used to house government-sponsored Syrian refugees, said a Queen's University immigration expert. CFB Kingston had been identified as an interim lodging site for government-sponsored refugees, but Naomi Alboim, an adjunct professor and chair of the policy forum at the School of Policy Studies, said the bases would be used only as a last resort. "Military bases are on hold, as in Kingston's, but in my opinion will likely never be used," Alboim said Thursday at the Community Foundation of KLFA's lunchtime speaker series event.(…) "The easy part is get them screened, getting them over here and transportation," she said. It's more important to get them into the community, she added. Military bases such as CFB Kingston would only be needed if the 36 settlement communities reach their capacity, which has not happened, although officials in Ottawa, Toronto and Vancouver earlier this month asked the federal government for a short pause in the flow of refugees coming to those cities. Whig-Standard, A2

Language barrier hampers refugee resettlement
The scope and pace of settling Syrian refugees in Metro Moncton is straining local resources, with the language barrier proving to be a major obstacle, says the executive director of Moncton's cultural agency. The Multicultural Association of the Greater Moncton Area was under the impression that refugee families settling here would have at least some basic command of English or French, said Jean-Pierre Alexandre on Thursday. "The reality is none of them have," he said, adding that most of MAGMA's volunteer interpreters have day-time jobs so settling the refugees has meant working against "a huge language barrier." This week, the Canadian Red Cross, the City of Moncton and area Rotarians joined forces with MAGMA to bolster the region's resettlement plans. Since Dec. 29, 120 refugees have landed in the city, with 37 more, the largest group yet, arriving Thursday. That's far more than the 70 to 100 annually that MAGMA is used to working with. "We knew the numbers were going to be high," says Moncton Ward 2 Councillor Charles Leger, who represents the city on MAGMA's board. "It's challenging. It's stressful for everyone." Telegraph-Journal, A5 (Times & Transcript, Daily Gleaner)

Struggle to find refuge for Syrian refugees
As the number of Syrian refugees in Ottawa is set to balloon, local officials are scrambling to find housing for them. About 35 governmentsponsored Syrian refugees are expected to start arriving in the city every day in the next month, said Carl Nicholson, executive director of the Catholic Centre for Immigrants. That will more than double the number Ottawa has during February alone. The big challenge now, Nicholson said, is to find enough two-and three-bedroom apartments for the Syrian families, which tend to be large. Out of the 90 families that have already landed, he said, accommodation has been found for 55 of them. Most of the families have four or five members; about 60 per cent of the new arrivals are children. "Clearly, they want to live in places where there are concentrations of people like them, but we can't always do that," said Nicholson. "So sometimes, it takes persuading. They want to live together: It's normal. It's comfort, it's security in a strange place." Ottawa Sun, A6; Ottawa Citizen, A3

*** Canada's refugee resettlement plan gets high marks from ex-UN refugee agency head**
Former United Nations high commissioner for refugees Antonio Guterres has high praise for Canada's resettlement program, ranking it as one of "the two best in the world" alongside Australia's. "Canada has been, during the 10 years I was high commissioner for refugees, a very reliable partner and a strong supporter of our activities worldwide," said Guterres in a phone interview with CBC News on Thursday. (…) Guterres said Canada's most recent contribution comes as the refugee crisis worsens and while anti-refugee sentiment has grown in cities around the world. "The Canadian initiative has been an extremely helpful initiative in trying to reverse this negative tide against foreigners in general, migrants and refugees in particular." "Canadians can be very proud of the society they are building," Guterres said on Thursday. (…) According to the UNHCR, "refugees are identified as in need of resettlement when they are at risk in their country of refuge or have particular needs or vulnerabilities." The list of persons the UN will prioritize for resettlement includes women and children at risk, survivors of torture and violence, refugees with medical needs, among others. Guterres said the UN agency does not pick and choose refugees based on their ethnicity or religion. "We are totally against that," Guterres told CBC News. CBC News (2016-01-28)

Refugees on safe but bumpy road

An editorial states, "It is better to be safe and warm in a Kitchener hotel than huddled in a bombed-out Syrian city where bullets fly and people die. Canadians intuitively know that. The 220 government-sponsored refugees from that war-torn country who recently arrived in this country and are now being housed in Kitchener's Howard Johnson hotel surely know it, too, from hard experience. Many have fled horrors that few Canadians could imagine, and they must be filled with thanks and hope for a chance at a new life here. Yet if many of these people also feel cooped up, frustrated and anxious about their future today, who can blame them? Strangers in a strange land, they awaken each morning to another bleak, grey January day where many will feel in their bones the unfamiliar but unrelenting bite of a Canadian winter. (...)That's how it is in Kitchener. That's how it is in Toronto where nearly 1,000 Syrian refugees are in a limbo-land of the city's hotels. That's how it is in Vancouver and Ottawa, too. And this leads us to ask if the Liberal federal government is doing a good enough job in managing the resettlement of so many people it has sponsored. (...)But the Liberals should learn from this experience because their handling of this file is helping yet also distressing highly vulnerable people. The warehousing of thousands of Syrian refugees is happening when there are plenty of private sponsors who have found homes for the new arrivals. But because the government-sponsored refugees are in a different stream from those who have been privately sponsored, the homes stand empty." Waterloo Region Record, A6

Drop focus on numbers in refugee intake
An editorial states, "Two weeks ago, the government announced it reached its refugee target score: 10,000 Syrian migrants by the middle of January. Yes, the goal had been revised - it was once 25,000 by Dec. 31 - but the Liberals conceded in November it would be nearly impossible to bring that many to Canada in such a short time. Public servants worked around the clock to meet the government's arbitrary deadline of Dec. 31 and managed to reach the 10,000-refugee mark a couple of weeks later. But local agencies have scrambled to find housing in tight markets such as Toronto, Ottawa and Vancouver. The task proved so difficult, some requested a temporary halt on the intake of new arrivals. Thousands of refugees have been put up in hotels at the public's expense - some, such as those in Vancouver, for a month or more - stuck in bureaucratic limbo while they wait to get their kids into school. Some refugees, evidently, have come to regret their decisions to leave the camps." Vancouver Sun, B6

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Trudeau's cozy relationship with unions will end up costing us coin**
Nice work if you can get it. At a campaign rally in Waterloo on September 15, a local union paid 23 members $100 each to stand behind Liberal Leader Justin Trudeau as he made an announcement about investing $750 million in worker training programs. Problem was, the party didn't declare the rent-a-crowd to Elections Canada. The Elections Commissioner has now ruled that the Liberals benefitted from the equivalent of a $2,300 donation, which the party has now paid to the Receiver General. The Liberals claim they were unaware of the payments. But they certainly courted Big Labour's support during the campaign. In "an open letter to Canadian public servants" published September 25, 2015, Trudeau pledged to repeal several bills that unions didn't like. These included changes to sick leave in Bill C-59, and to collective bargaining rights in Bill C-4. The Liberals also pledged to revoke Bill C-377 on union disclosure and C-525 on union certification. Now that they're in power, the Liberals are busily following through on those promises. Employment Minister MaryAnn Mihychuk announced this week that C-377, which required unions to make public all transactions over $5,000 and executive salaries in excess of $100,000, and Bill C-525, which required a secret ballot vote before certifying a workplace in industries governed by the Canada Labour Code, are both on the chopping block. iPolitics (2016-01-28)

*** Le Sénat pourrait bloquer**
Un premier bras de fer pourrait avoir lieu dans l'arène du Sénat sur la question des règles syndicales. Le gouvernement de Justin Trudeau abroge deux lois touchant les syndicats qui avaient été adoptées par les conservateurs. Ces derniers n'ont pas l'intention de se laisser faire et menacent à mots couverts de faire obstruction à l'initiative libérale au Sénat, où ils ont la majorité. Du temps où ils étaient au pouvoir à Ottawa, les troupes de Stephen Harper avaient déposé deux projets de loi qui avaient suscité la grogne dans le milieu syndical. La loi C-377 aurait obligé les syndicats à ouvrir leurs livres comptables, ce qui

aurait donné un avantage indu à l'employeur lors des négociations, selon les syndicats. Elle les aurait notamment forcés à dévoiler toute dépense de plus de 5000$ ainsi que tout salaire de plus de 100000$. Elle a reçu le sceau du Sénat en juin dernier, mais comme son annulation était dans la plateforme libérale, les syndicats avaient déjà eu la permission de ne pas fournir toutes ces informations détaillées sur leurs finances pour 2015. Quant à C-525, elle changeait les méthodes d'accréditation syndicale en imposant un vote secret. La ministre de l'Emploi, MaryAnn Mihychuk, a soutenu en conférence de presse à Ottawa, jeudi, que l'annulation de ces deux lois amènera «de l'équilibre et de l'équité» ainsi qu'un plus grand sens du «respect» dans les relations de travail. La Presse Canadienne (Le Droit, 22)

*** Liberals move to kill two anti-labour bills**
The federal government has taken the first step in repealing two controversial labour bills.
On Thursday, MaryAnn Mihychuk, Minister of Employment, Workforce Development and Labour; and her parliamentary secretary, Cape Breton-Canso MP Rodger Cuzner, announced that the department had filed notice to introduce legislation that will repeal Tory-backed private members bills C-377 and C-525. The legislation is expected to go before the House of Commons next week. Speaking with reporters, Mihychuk said the legislation is a move toward restoring fairness and balance to the labour landscape. "The prosperity of workers, employers and our economy as a whole depends on a sound labour relationship. So we cannot allow these bills to disrupt the vital relationship between employers and employees," she said. Labour unions across Canada welcomed the announcement, with many taking to social media to express their approval. "This proves what we've been saying all along: that these bills were nothing more than an attempt to undermine unions' ability to do important work like protecting jobs, promoting health and safety in the workplace, and advocating on behalf of all Canadian workers," said Canadian Labour Congress president Hassan Yussuff in a press release. Bill C-377 would have forced labour unions to disclose publicly expenditures, including how much they spend on political activities, as well as salaries. It was gutted through a series of amendments by a group of rogue Tory senators during its first go around in 2013, but the amendments died on the notice paper when then Prime Minister Stephen Harper prorogued parliament that summer. The bill was resurrected without the amendments in 2014 and eventually rammed through the Senate in the final days of the 41st Parliament. Chronicle-herald, A3

OTHER / AUTRE

Canadian detained in China on spy charges
China's official news agency says a Canadian who was detained more than a year ago has been indicted on accusations of spying for Canada and stealing Chinese state secrets. Xinhua says Kevin Garratt was indicted by prosecutors in Dandong city, near China's border with North Korea, where the former Vancouver man and his wife ran a popular coffee shop and conducted Christian aid work. Garratt and his wife Julia - who have lived in China for 30 years - were arrested in August 2014. Julia was released on bail in February 2015. The Xinhua report says that during an investigation Chinese authorities found evidence that implicates Garratt in accepting tasks from "Canadian espionage agencies to gather intelligence in China." Their son, Simeon Garratt, who lives in Vancouver, has denied his parents were involved in espionage. The accusations against the couple in August 2014 came about a week after Canada accused a China sponsored hacker of infiltrating Canada's National Research Council, the country's top research and development organization. Xinhua said the Garratt case will be tried at the Dandong Intermediate People's Court. Canadian Press (Ottawa Citizen, C1/Front, Province, Times Colonist, National Post, Daily Gleaner, Times & Transcript); Globe and Mail, A1; * Canadian Press (Vancouver Sun, A8); * London Free Press, B3 (Whig-Standard); * Le Figaro; * CBC News; * ABC News; * Presse canadienne (La Tribune)

Signs of discord after attack a threat to religious harmony
A few days after the **terrorist** attack that killed 30 people here, the people of Ouagadougou were outraged by a foreign report: A French television channel had described one of their neighbourhoods as the "Muslim quarter." Many people felt insulted and shocked. How could there be a "Muslim quarter" in a country where Muslims and Christians are so deeply integrated? How could anyone imply that the two religions were obliged to live separately? They are valid questions, and key to the country's resilience.

Unlike many countries around the world, Burkina Faso has managed the extraordinary achievement of connecting its two main religions in a cultural melting pot. Muslims and Christians coexist within even the same families, and there is widespread tolerance and conviviality between the two faiths. Despite the Jan. 15 terrorist attack, Burkina Faso's leaders are convinced that religious extremism will fail to find a foothold here. Their country could even be a model for others. Yet this achievement might now be under threat. Pressures are intensifying. Islamist radicals have slipped across the frontiers from countries such as Mali, where extremism is growing. Even within Burkina Faso, there have been worrisome signs of religious tension since the terrorist attack. Globe and Mail, A1; Toronto Star, A12

* **Helping Syria's neighbours**

An opinion piece states ''Lloyd Axworthy and Allan Rock states ''Harrowing scenes of starvation from the besieged Syrian town of Madaya this month served as yet another reminder of the horrific plight of those trapped inside Syria. It is hardly a surprise that so many attempt to flee. To date, 4.6 million Syrians - the equivalent of the entire population of British Columbia - have already done so. Canada is playing a commendable role in responding to the greatest refugee crisis since the Second World War. Since Prime Minister Justin Trudeau and the Liberal government came to power, Canada has welcomed more than 10,000 Syrian refugees, a number that will soon climb to the target of 25,000. While Canadians can be proud of the moral leadership we are displaying and the international example we are setting, more must be done for the refugees remaining in Jordan, Lebanon and Turkey. Those millions who will not be lucky enough to be welcomed to Canada (or a handful of other countries resettling refugees) face a difficult choice: continue a bare existence in a camp with few services and almost no hope, or risk a perilous journey to Europe.'' Globe and Mail, A12

INTERNATIONAL

* **Japan puts military on alert for possible North Korean missile test**

Japan has put its military on alert for a possible North Korean ballistic missile launch after indications it is preparing for a test firing, two people with direct knowledge of the order said on Friday. "Increased activity at North Korea's missile site suggests that there may be a launch in the next few weeks," said one of the sources, both of whom declined to be identified because they are not authorized to talk to the media. Indian Express

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PS.PSPMediaCentre/CentredesmediasPSP.SP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
January 30, 2016 / le 30 janvier 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Justin Trudeau se rend à La Loche pour «exprimer la tristesse du pays»
Le premier ministre Justin Trudeau a visité vendredi la petite communauté dénée de La Loche, dans le nord de la Saskatchewan, «pour exprimer personnellement le choc et la tristesse de tout le pays» à la suite des fusillades qui ont fait quatre morts et plusieurs blessés, il y a une semaine. **Le ministre de la Sécurité publique, Ralph Goodale**, est aussi le seul libéral qui a été élu en Saskatchewan lors du dernier scrutin. Dans un communiqué, M. Trudeau indique qu'«il est toujours déchirant et accablant de voir des vies si prometteuses nous être enlevées si prématurément». Presse Canadienne (L'Acadie Nouvelle, 28) ; Toronto Star, A12; Postmedia News (StarPhoenix, N1/Front; Whig-Standard, Montreal Gazette, Ottawa Citizen, Edmonton Journal, Vancouver Sun, Windsor Star, Leader-Post, National Post)

Data breaches renew calls for stricter oversight of spies
Civil-libertarians are responding to new privacy warnings from spy watchdogs by saying that such cases show that a proposed fix to Canada's intelligence system amounts to a half-measure. In separate reports on Thursday, watchdogs for Canada's two spy agencies revealed potentially unlawful breaches of Canadians' data. Such cases raise continued accountability questions for the agencies. "Review" is the preferred bureaucratic term for the work of the Security Intelligence Review Committee, and the Office of the CSE Commissioner (OCSEC), the federal agencies that determine whether Canada's spies are acting lawfully. SIRC and OCSEC look at spying operations of the Canadian Security Intelligence Service and the Communications Security Establishment after the fact, by pulling records and conducting

interviews... **Public Safety Minister Ralph Goodale** has promised wideranging consultations with citizens and stakeholders in coming months regarding how Canada runs its intelligence agencies. **Scott Bardsley, a spokesman for Mr. Goodale**, said on Friday that, although the Liberals did not campaign on reforming review bodies, the government would be open to hearing views. Globe and Mail, A13

Too little oversight on Allstream sale, MPs complain
The recent sale to a U.S. firm of the Allstream division of Manitoba Telecom Services Inc., raised the ire of some critics in Ottawa who think the government didn't look at the deal closely enough before allowing it through. The sale of Allstream to Colorado-based Zayo Group was announced in November 2015, and the sale was completed in mid-January. MTS expects to make $420 million on the sale. Manitoba MP Niki Ashton tried to get the government to provide more details about the review process for the deal, including its benefit to Canada and the national security considerations of having a coast-to-coast national fibre-optic cable network that carries data for the government and private sector in the hands of an American company... "The previous government blocked an earlier attempt based on national security concerns, so why is the Liberal minister refusing to do a review to protect Canadians?" she said. **Public Safety Minister Ralph Goodale**, who has authority over national security issues, brushed off Ashton's question in the House of Commons. ***"Security screening is part of the process,"* he** said. ***"That is in the law, and the government of Canada follows the law."*** Under the Investment Canada Act, if the minister of innovation believes a foreign investment, such as the Allstream-Zayo deal, raises national security concerns, cabinet can order a national security review. Once the companies involved are notified there may be national security issues to look at, and the government has 45 days to decide whether or not to do such a review. It can take up to 200 days to actually complete a national security review. **A spokesman for Goodale** told the Free Press Friday the Investment Canada Act prevents the government from speaking at all about what kind of reviews are completed. Winnipeg Free Press, B7

People in la loche need jobs above all
An opinion piece states, "Now that Prime Minister Justin Trudeau, Premier Brad Wall, **Public Safety Minister Ralph Goodale**, Assembly of First Nations Chief Perry Bellegarde and other dignitaries, along with hordes of media, have visited La Loche following last week's shooting spree that left four dead and seven injured, it is difficult to find something original or insightful to say about the tragedy. Much has been said and written about the lack of recreation facilities, the underfunding of social programs, the chronically high unemployment, the persistent problems of alcohol and drug abuse, the high suicide rate, the gangs, the sad history of colonization, residential schools and 'cultural genocide' of the Dene people. The last thing anyone in that community needs is another so-called "expert from the South" telling them what they need and don't need..." Postmedia News (StarPhoenix, B2; Leader-Post)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Public health officials attempt to ease fears about Zika virus**
As alarm about the Zika virus spreads through the Americas, Canadian public health officials are attempting to calm nerves at home. Chief public health officer Dr. Gregory Taylor said Friday the risk to Canadians is very low, although he acknowledged many questions that remain to be answered about the mosquito-borne virus that is being associated with birth defects in Brazil and elsewhere. Ottawa Citizen, A4

*** Héma-Québec prévoit des mesures d'exclusion**
Le premier cas d'un Québécois infecté par Zika a été révélé hier, alors que héma- Québec a mis en place des mesures d'exclusion pour les donneurs revenant de régions où le virus sévit. «Pour le moment, on invite les gens qui ont séjourné dans des régions autres que le Canada, les États-Unis et l'Europe à attendre 30 jours avant de faire un don de sang», confirme le porte-parole d'Héma-Québec, Laurent-Paul Ménard. Journal de Montréal, 9

*** Electrocuted squirrel latest animal blamed for Nova Scotia power outage**
Nova Scotia's power utility, which has blamed blackouts on everything from crows and seagulls to "salty fog" over the last decade, and Friday an electrocuted squirrel left a swath of suburban Halifax in the dark.

The furry critter scaled a transformer in a substation in the Hammonds Plains area just before 5 p.m. Thursday, Nova Scotia Power said Friday. Spokeswoman Bev Ware said the squirrel became a conduit for the electricity, which subsequently caused roughly 5,400 customers to lose power. Canadian Press (Cape Breton Post, Edmonton Sun, A66;)

*** Winter storm conditions strike much of Newfoundland**
A winter storm hampered much of Newfoundland Saturday, causing power outages and dangerous driving conditions. Todd Bate, meteorologist with the Environment Canada Gander weather office, said there is a blizzard warning in effect for much of central and western Newfoundland, a winter storm warning for Connaigre, Clarenville and the Bonavista Peninsula, a wind warning for the Avalon Peninsula, and a blowing snow advisory for the Northern Peninsula. CBC News

*** Lac-Mégantic: ouverture officielle du Bureau de reconstruction**
C'est samedi après-midi que sera officiellement ouvert le Bureau de reconstruction du centre-ville de Lac-Mégantic. Le gouvernement fédéral a délégué le ministre Marc Garneau pour assister à l'événement. Il doit faire une annonce de financement. Sur le budget total de 2,2 millions de dollars sur trois ans, Ottawa accorde 1,9 million au Bureau. La Presse

*** Hardisty expansion plan on hold**
An ambitious plan to expand an oil-by-rail terminal outside Hardisty, Alta., is being overhauled after the federal government ordered the first-ever environmental review of a rail-based oil-shipping facility... Federal scrutiny of the Alberta terminal would be one of the first public reviews of the growing oil-by-rail industry since the disaster in Lac-Mégantic, Que. Globe and Mail, S3

*** Leur machine de guerre contre des écosystèmes vitaux**
Après avoir qualifié la tragédie de Lac-Mégantic d'illustration du « côté sombre du capitalisme », notre cher maire Labeaume semble tout à coup aveuglé et incapable d'appréhender les risques pour l'eau potable que constitue le pipeline de TransCanada. Une compagnie canadienne qui souhaite tirer des profits de l'exportation d'un des produits pétroliers les plus toxiques de la planète ne pourra jamais faire croire qu'elle place « les gens et la nature avant ses profits ». Le Devoir

*** Security deals forced on RMs: Tories - Say they were bullied into signing contracts**
The Tories and a former reeve accuse provincial officials of misconduct over contracts for security during the 2011 flood. The Conservatives, along with the former reeve of the RM of St. Laurent, said government officials bullied municipal leaders into signing millions of dollars in contracts with Impact Security. Former reeve Earl Zotter, whose municipality is on the southeastern shore of Lake Manitoba, saw his community ravaged by the one-in-300-year flood. As water surrounded the community 80 kilometres northwest of Winnipeg, a security firm was called in to guard properties and watch checkpoints in the community of about 1,400 residents. Zotter and other former members of his council allege the Emergency Measures Organization (EMO) forced them to hire Impact Security. Winnipeg Free Press, A4

*** Coast guard begins annual ice-breaking operations**
U.S. and Canadian Coast Guard crews kicked office-breaking operations Friday in local waterways, 20 days later than last year. Dubbed Operation Coal Shovel, the work involves breaking ice in Southern Lake Huron, Lake St. Clair, the St. Clair/Detroit River system, Lake Erie, Lake Ontario and the St. Lawrence Seaway. Windsor Star, A5

Nova Scotia winter storm leaves thousands without power
Heavy snowfall has left thousands of people without electricity and Nova Scotia power estimates it could take until midnight before crews are able to restore electricity to many homes in the northern part of the province, many of which have been in the dark since Friday evening. About 51,800 customers were without power at 7:30 a.m. Saturday. The outages affect about two dozen communities and range from Yarmouth to Dartmouth, Tatamagouche to Sydney. CBC News; *Chronicle Herald, A6

Colombie-Britannique
Cinq personnes sont mortes dans une avalanche près de McBride, en Colombie-Britannique, a indiqué le bureau du coroner de la province. La porte-parole Barb McLintock a indiqué qu'il y avait eu une avalanche de grande ampleur, vendredi après-midi, dans un secteur où un groupe de personnes faisait de la motoneige. Elle a affirmé que deux coroners avaient été dépêchés de Prince George, et que la Gendarmerie royale du Canada (GRC) enquêtait. Avalanche Canada a soutenu que l'avalanche semblait avoir été déclenchée par une activité humaine, sans donner plus de détails. L'organisme a indiqué que la pluie et la neige au cours des quelques derniers jours ayant été suivies par un refroidissement, vendredi, pourraient avoir causé des pressions dans le manteau neigeux. Avalanche Canada a appelé les gens à la prudence en fin de semaine. Presse Canadienne (Le Devoir, A7; La Tribune, Le Quotidien, Le Droit) ; Canadian Press (Red Deer Advocate, A4; *Times Colonist; *Cape Breton Post, *Winnipeg Sun, *Edmonton Sun, *Calgary Sun, *Ottawa Sun, *Vancouver Sun, *Calgary Herald)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** 24 Sussex woes continue**
Prime Minister Justin Trudeau may be unable to move into 24 Sussex drive during his current four-year term in office, an email released to the Ottawa Citizen under access to information suggests. the email from Stephen Wallace, secretary to gov. gen. David Johnston, was sent to Mark Kristmanson, CEO of the national Capital Commission, on Oct. 27, 2015 - the day after the Prime Minister's office revealed that Trudeau and his family would live at Rideau Cottage "until further notice."... As well, the rCMP "has expressed the desire to implement security enhancements throughout the buildings and grounds," the document says. Postmedia News (Whig-Standard, B3; Ottawa Citizen)

Big Brother's tough week
One of Canada's foremost privacy experts is challenging the government's assessment that the impact of a privacy breach involving the Communications Security Establishment, Canada's electronic spy agency, "was low." "The privacy impact is not low," Anne Covoukian, the executive director of the privacy and big data Institute at Ryerson told The House. "Metadata can be far more revealing than the actual contents of communication," she said. CBC The House

A privacy breach and a country left in the dark
An opinion piece states, “To learn that our digital surveillance agency broke privacy laws by revealing information about Canadian citizens to our allies is one thing. To learn that the Conservative government of the day, when apprised of this security breach, withheld the information from Canadians, is quite another. But that is where we are today, after learning of a major invasion of Canadian privacy more than two years after the fact. If our spy agencies, aided and abetted by the government of the day, wanted to fuel suspicion of internal surveillance in this country, they succeeded. If they wanted to ratchet up distrust, they scored. This despite an effort Thursday to get ahead of this story with the first-ever background briefing for journalists from an official with the Canadian Security Establishment - only 26 months after a software glitch was discovered that was sending metadata on Canadians to our Five Eyes allies without the proper scrubbing to hide identities...” The Record, A11

Data breaches reason to worry
An opinion piece states, “It's bad enough that we have to be constantly on guard against online snoops and scamsters who would use our personal data for nefarious purposes - we shouldn't have to worry what the government does with the information it collects about us. Yet there is plenty of reason for concern. Privacy commissioner Elizabeth Denham has taken the B.C. Ministry of Education to task for losing a hard drive containing personal information on 3.4 million B.C. and Yukon students and teachers. Her report says the ministry ignored its own policies and violated privacy law. The Canadian Security Intelligence Service also broke the rules when it repeatedly obtained taxpayer information from the Canada Revenue Agency without a warrant, which means the CRA was complicit in those violations. Meanwhile, the watchdog over the Communications Security Establishment, Canada's electronic spy agency, has found that CSE has improperly shared metadata with key foreign allies. (Metadata is

information associated with a communication, such as an email address or a telephone number, but not the message itself.)..." Times Colonist, A12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

*** Gun smuggler jailed in U.S**
A former Osoyoos resident who bought guns in Washington state and then smuggled them into B.C. for resale has been sentenced to prison time. Tyler Ryan Cuff, 32, of Oroville, Washington, pleaded guilty to one count of dealing firearms without a licence and was sentenced in U.S. District Court in Spokane to 30 months in custody, followed by three years of supervised release. Times Colonist, A6

*** Moroun files lawsuit against Windsor**
The Ambassador Bridge company has filed yet another lawsuit against the City of Windsor in regards to the dozens of boarded-up homes it owns in the city's west end. Bridge owner Matty Moroun was sued more than two years ago by residents who remain in the Indian Road neighbourhood for creating what they allege is an eyesore and is devaluing their properties. Windsor Star, A3

*** 'My dream became a nightmare'**
Looking back, Omar Figueroa Ramirez figures he had it pretty good: a hotel job in the Mexican resort town of Huatulco on the Pacific coast, leisure time on warm tropical beaches, and the closeness of his family, friends and a girlfriend. He gave it all up for the chance of a better life as a foreign worker on a Langley blueberry farm, of sending money to help support his family and of saving to build his own dream home in Huatulco. Or so he thought. "I was hoping for a good work experience in Canada," the 24-year-old recalls in an interview with The Vancouver Sun. "In Mexico, the Mexican people, we think that Canada is the best place in the world. But everything changed. My dream became a nightmare." With legal help from the West Coast Domestic Workers' Association, Ramirez has lodged an official complaint with the B.C. Employment Standards Branch demanding that his ex-employer, farm owner Randhir Singh Pandher, pay almost $20,000 in outstanding wages, overtime and vacation pay. Vancouver Sun, A14

*** Timing perfect for Canadian travel**
Fuel prices are dropping, the Canadian dollar is dissuading travel to the United States, and the Euro and other currencies seem to be experiencing a rebound of their own. Perhaps this is the year to visit one of the greatest countries in the world. Yours! Having travelled to more than 65 countries and nine Canadian provinces, I can state wholeheartedly what Canada has to offer ranks among the best tourist destinations around the world. From a scenic standpoint there can be little argument. Winnipeg Free Press, G2

*** Canadian lumber sees benefits from economy**
The boost Canadian lumber exports are getting from the falling loonie is certain to bring out protectionist forces in the U.S. lumber lobby, says the CEO of Quebecbased forestry company Tembec. "I think that they're watching the Canadian dollar drop, particularly in lumber, and they're saying, 'This isn't fair,'" CEO James Lopez said. Canadian Press (Montreal Gazette, B1/Front; Vancouver Sun); Globe and Mail. B1

*** Low dollar, food and shopping enticing Americans and others**
From British Columbia to Montreal, the low Canadian dollar is proving a boon to the tourism sector. Dragged down by cheap oil and an international slump in commodity prices, the dollar is trading at around 70 cents US and enticing Americans to travel north of the border. "We're getting more reservations at the last minute from Americans planning trips for the weekend," says Eve Pare, head of the Hotel Association of Greater Montreal. Canadian Press (Montreal Gazette, B1/Front)

Fini le visa imposé aux Mexicains
Le visa imposé aux mexicains par le canada, «fini, terminé, caput», a déclaré hier, non sans une pointe d'ironie, le ministre canadien des affaires étrangères, Stéphane dion, au terme d'une journée de discussions avec ses homologues du mexique, claudia ruiz massieu, et des états-Unis, John Kerry. Les libéraux de Justin Trudeau avaient pris l'engagement d'éliminer cette barrière à l'entrée qu'avait imposée le gouvernement Harper afin de réduire l'arrivée des travailleurs mexicains en terre canadienne. «Nous

comptons tenir notre engagement d'éliminer le visa imposé aux Mexicains. Ça ne pourra pas se faire du jour au lendemain. Le ministre de l'Immigration John McCallum y travaille», a assuré Stéphane Dion. Agence QMI (Journal de Montréal, 14 ; Journal de Québec)

Low loonie good for business in manufacturing, tech sector
Len Ruby knows all too well the fickle nature of the Canadian dollar. Just a few years ago, when the loonie was trading at or above parity with the U.S. greenback, things weren't pleasant for Ruby and others involved in the production of goods for the American market... Manufacturers with markets south of the border are, by and large, seeing the benefits of a low loonie. "There's a lot of good news out there," said Jay Myers, who heads up the industry association Canadian Manufacturers and Exporters. The Record, D12

Special rules apply near U.S. border
An opinion piece states, "The U.S. has inland Border Patrol checkpoints up to 160 kilometres from the border (usually with Mexico rather than Canada). Despite having broken no laws and being far from the actual border, all highway traffic is stopped and everyone inside each vehicle is detained to determine their immigration status. In Ontario, I believe, only the driver must provide identification if stopped by police. Passengers need not identify unless suspected of a crime. Is this correct, or do we lose freedoms near the border here, too? Apparently, special rules do apply near our border with the U.S. Section 154.2(3) of the HTA authorizes police to stop a vehicle in a border-approach lane and demand identification or authorization, as required, from everyone inside. During a non-border area traffic stop, police can demand identification from a vehicle passenger only if he/she is reasonably suspected of a crime. Ajay Woozageer of the Ontario Ministry of Transportation adds: Section 154.2 HTA was enacted in 2006. The Canadian and U.S. border authorities offer pre-border security clearance for registered commercial and passenger vehicles under the "FAST" and "NEXUS" border-crossing programs. It's an offence for unauthorized drivers to use FAST/NEXUS lanes, and all occupants in the vehicle using a border-approach lane must demonstrate that they are eligible by providing police with the appropriate documentation..." Toronto Star, W6

CYBER SECURITY / CYBERSÉCURITÉ

* **Privacy policies breach affected Yukon students**
Privacy policies were breached in the disappearance of a hard drive containing personal information about Yukon and B.C. students, B.C.'s privacy commissioner has found. Elizabeth Denham said Thursday in a 40-page report while the disappearance of the hard drive remains unsolved, it's clear employees of the B.C. Ministry of Education breached privacy policies. Daily Star, 3/Front

* **U.S. and U.K. spied on Israeli drones for years**
U.S and British intelligence cracked the codes of Israeli drones operating in the Middle East and monitored their surveillance feeds for almost 20 years, according to documents leaked by an American whistleblower and published in international media on Friday. Reports by the German magazine Der Spiegel and the investigative website The Intercept said the details emerged from documents leaked by Edward Snowden, the former National Security Agency contractor who leaked millions of documents about U.S. government surveillance in 2013. Associated Press (Whig-Standard, B5; Ottawa Citizen, Vancouver Sun)

* **Webcam search engine raises concerns for connected devices**
A young child asleep on a couch in Israel. Mourners huddled together at a small funeral in Brazil. An elderly woman stretching in a fitness centre in Poland. All available for anyone to watch via the unsecured webcams overhead. This isn't "1984," it's the world in 2016. Shodan, a search engine that indexes computers and devices rather than information, now allows users to pull screenshots from nanny cams, security cameras and other connected devices around the world that don't ask for a username or password. Canadian Press (Vancouver Sun, D3)

*** US declares 22 Clinton emails 'top secret'**
The Obama administration confirmed for the first time Friday that Hillary Clinton's home server contained closely guarded government secrets, censoring 22 emails that contained material requiring one of the highest levels of classification. The revelation comes three days before the Democratic candidate competes in the Iowa presidential caucuses. State Department officials also said the agency's Diplomatic Security and Intelligence and Research bureaus are investigating if any of the information was classified at the time of transmission, going to the heart of Clinton's defence of her email practices. iPolitics

Transit security beefed up in wake of computer threat
B.C. Transit has beefed up online security in the wake of a threat to its computer systems that prompted the agency to take its website offline for two days in early December. The Crown agency hired information technology experts to assess the situation and make recommendations. Times Colonist, A1/Front

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Infant involved in alleged carjacking by desperate escapee**
B.C. RCMP are describing a "harrowing" attempt to recapture an escaped Alberta prisoner this week. They say at one point the man and an accomplice carjacked a 16-year-old boy and a baby. Cpl. Dan Moskaluk of the northern Rockies RCMP says in a news release that the chase began Tuesday morning when employees at a Husky bulk fuel plant along Highway 97 reported seeing Harley John Lay, 29. Canadian Press (Calgary Sun, A7; Edmonton Sun, Ottawa Sun, Toronto Sun, Times Colonist, Times Colonist)

*** Un enseignant parmi les accusés**
Un enseignant, un animateur en bibliothèque, deux moniteurs scouts, un soi-disant éducateur spécialisé: plusieurs des hommes accusés d'avoir fait partie d'un « club » de pédophiles démantelé par la police cette semaine s'étaient positionnés tout près des enfants. Selon la Sûreté du Québec, ils échangeaient sur les meilleures stratégies pour abuser de mineurs, certains discutant d'ailleurs de leur expérience de récidivistes. Voici ce que La Presse a pu réunir comme information sur chaque membre du groupe. La Presse, A6

*** Les scouts auraient aimé être avisés**
Des organisations scoutes du Québec qui ont compté dans leur rang deux présumés pédophiles accusés de pornographie juvénile déplorent l'absence d'avertissement quant à une enquête visant ces individus. «On a été déçu de ne pas être avisé qu'ils étaient suspectés... Je comprends qu'il y ait une enquête en cours, qu'ils n'aient pas encore été accusés, mais dans ces casci, il me semble qu'il n'y a pas de chance à prendre», a laissé tomber Nicolas Rousseau, de l'Association des Aventuriers de Baden- Powell. Journal de Québec, 57

*** RCMP report into Donald Dunphy death complete**
The RCMP's final report into the investigation of the shooting death of Donald Dunphy is complete, and the police force says an independent review is being arranged. "They will review the file for thoroughness, competency and overall accuracy," said a spokeswoman for the RCMP. The Telegram, A9

*** No hiding from the law on Twitter**
Michelle Rempel was alone in a Winnipeg hotel room in the dark depths of winter when a stream of violent threats started filling her Twitter mentions. The message was so vulgar it has since been expunged from the Internet; so dangerous that the Conservative MP from Calgary - then a cabinet minister travelling for work - called the police. "It was really quite frightening and the appropriate route was to take it to the RCMP," Rempel says. "It doesn't matter if somebody is making a threat to someone or proposing violence to someone to their face or in a different medium, it's still unacceptable." Postmedia News (Calgary Herald, A7; Vancouver Sun, National Post)

*** Rexton students under investigation after video of assault posted to social media**
Richibucto RCMP are investigating an assault at a Rexton high school after video footage surfaced on social media last week. Mellisa Gallant said her daughter Josie Gallant, a Grade 10 student, does not want to return to school after she says she was targeted by a group of bullies at Bonar Law Memorial High School. Times & Transcript, A7

*** Accountant faces charges**
A accountant in Canmore is facing new charges related to a multimilliondollar fraud investigation by RCMP in the mountain resort town. James Russell Neilson, 49, was charged last May with three counts of fraud over $5,000, one count of theft over $5,000 and one count of laundering the proceeds of crime. Police said the latest charges against Neilson are related to his involvement with Abaca Solutions. They include fraud over $5,000, uttering a forged document and laundering the proceeds of crime that allegedly occurred between January 2009 and October 2014. Police suspect the accountant defrauded 40 people of $5.5 million. Canadian Press (Times Colonist, B4); Postmedia News (Calgary Herald, A8; Edmonton Sun, A8)

*** RCMP to demolish building**
The RCMP is planning to demolish the old detachment building in Ingonish Beach. The land will be restored as a community space with road access to the beach and electricity to the property. In early December, the new RCMP Ingonish Detachment officially opened, replacing the oldest detachment in Atlantic Canada. Cape Breton Post, A8

*** Man in standoff shoots himself**
The RCMP and its emergency response team evacuated a quiet Campbell River neighbourhood Friday morning after receiving reports of gunfire inside a house. Police surrounded a home on Glen Eagle Drive just after 9 a.m. and negotiators began talking with a man who had barricaded himself inside the home. The situation ended a few hours later, when the man fatally shot himself. Times Colonist, A4

*** Ex-guard's defence challenges drug analysis**
The defence's case in the trial of former correctional officer Michael Gaber became clearer on Thursday as they relentlessly challenged drug analysis evidence. The court heard from Health Canada drug analyst Sarita Jaswal in a very detailed testimony about the drug analysis process and the results of the analysis done on one of the pills Gaber had when he was arrested... Tarnow zeroed in on the RCMP's handling of the pills. On Wednesday, RCMP Const. Daniel Bray testified he didn't clean a table he used to bag the pills seized, and couldn't say for certain he was wearing gloves. "That's not the way we would request police to handle it," Jaswal said. Daily Star, 2/Front

'Armed and dangerous' suspect surrenders to Toronto police in what may be Mafia-linked slaying
Handout Domenico Scopelliti, 51, is being sought on a first-degree murder charge. A man considered "armed and dangerous" surrendered to Toronto police early Saturday, an hour after detectives launched a public manhunt in the slaying of an 87-year-old man, a shooting in the city's west end that seems linked to some of the city's long-established Mafia clans. National Post

*** Police say new groups behind wave of violence**
Months after promising to jail those responsible for a spike in gun violence, police announced the latest arrest Thursday, this time in connection with a December shooting in the northeast neighbourhood of Coral Springs. Investigators said they remain focused on unsolved cases of shootings from last year as they pore over video surveillance and await lab reports, but warned they are dealing with a new cast of criminals behind the latest shootings in 2016. Calgary Herald, A12

*** Police search nets big haul**
Hamilton police seized brass knuckles, a pellet gun and drugs Thursday after searching a Connaught Avenue South home. A release said the gangs and weapons enforcement unit was preparing to search the building around 10 p.m. when police saw a suspect leaving on foot. Hamilton Spectator, A6

*** Police say $4M hire, council says lower**
Politicians said no to London police Friday,making a relatively small impact in the total city budget but sending a big message about their willingness to curb spending on emergency services. In an 11-4 vote, city council carved about $4 million from the department's proposed operating budget of nearly $400 million over the next four years, cutting in half the hiring Chief John Pare had planned for 2016. In the debate, members of the police services board, which oversees the department, suggested council's vote - which scuttles plans to hire five officers and one civilian staffer this year - could be appealed to a provincial body, the Ontario Civilian Police Commission (OCPC). London Free Press, A1/Front

*** Judge finds Hamilton cop guilty of perjury**
A veteran Hamilton police detective who encouraged an informant to plant a gun at a home, so he could obtain a search warrant from a justice of the peace, has been convicted of three criminal charges. Superior Court Justice Catrina Braid convicted the 12-year officer Robert Hansen of one count of perjury and two counts of obstructing justice on Friday. Hamilton Spectator, A1

*** Calls for Transparency to bolster confidence in police**
Eliminating secrecy in Ontario's police accountability process would go a long way toward improving the public's trust, say critics. "There's an old adage: Justice must not only be done, but must be seen to be done," said criminal defence lawyer Daniel Brown. In Ontario, the Crown is required to notify the chief of police when a judge has called out an officer for questionable conduct and testimony, but the government never confirms or denies whether this has actually been done. Toronto Star, GT4

*** New Peel police board chair sets fresh tone**
"It doesn't affect brown people and white people - it affects black males." With that sharp rebuke of a report on police street checks - insisting that it missed the essence of the controversy - the man now heading the oversight of Peel Region police made clear that change is coming. Minutes after Amrik Singh Ahluwalia stood Friday morning and moved to his new seat following his unanimous election as chair of the Peel Police Services Board, he joined other members calling for change within the country's third-largest municipal police force. Toronto Star, GT2

*** Man gunned down Jan. 22 had long criminal history**
Yonatan (JK) Kassa had gang links and convictions for drug trafficking and a violent home invasion when he was shot to death Jan. 22. But friends who have raised over $9,000 for his family online are portraying Kassa, 30, as "an amazing man" with a "beautiful smile and caring personality."... Kassa's run-ins with police date back a decade, according to online court records. He was convicted of drug trafficking in Surrey in 2006, then in Vancouver in 2008. Kassa and two others were caught trying to rob a Maple Ridge marijuana grow-operation in July 2010. He was convicted and got a one-year conditional sentence. He breached that sentence when in August 2011 he and a gangster named Cody Sleigh forced their way into a North Delta house, waving guns and terrifying the people inside. The tenants sneaked out the back, hopped a fence and called for help. Vancouver Sun, A8

*** Eroding police trust could sway trials**
An opinion piece states, "When the lawyer for Const. James Forcillo said this week that he had unsuccessfully applied to get a judge-alone murder trial for his client, it raised an obvious question: Had public trust in police eroded to the point where juries - once believed to always find in favour of cops - would actually convict an officer for a shooting while on the job?..." Toronto Star, GT4

*** Maybe Forcillo should be treated differently**
An opinion piece states, "On Tuesday, the day after Toronto Police Constable James Forcillo was found guilty of attempting to murder 18-year-old Sammy Yatim aboard a streetcar in 2013, his lawyer, Peter Brauti, took to the airwaves on NewsTalk 1010 to explain why his client shouldn't be treated like someone found guilty of attempted murder. The five-year mandatory minimum sentence for attempted murder using a restricted weapon "was never meant to catch police officers who are acting in the line of duty and may have made a mistake in judgment," said Brauti. "That was meant for a completely different class of people." Twitter's outrage-o-meter spiked, and understandably so. ("Class of people"? Does counsel wish to rephrase?)..." National Post, A8

*** Weighing the Forcillo verdict**
An opinion piece states, "The jury made the best of an impossible situation. They knew they couldn't let Const. James Forcillo get away scot-free after killing Sammy Yatim, but they also didn't have the courage to convict a cop of murder. The "cops are tops" mentality persists. The verdict showed the wisdom of Solomon. It was savvy and wise. When announced, the relief on the streets of Toronto was palpable. Not perfect, but some justice was meted out. Yatim should not have died. Cops are not 007s. They don't - or shouldn't - have a licence to kill..." Toronto Star, IN7

*** Paid leave system for police needs to change**
An opinion piece states, "Wouldn't it be nice to collect a paycheque while you're on the golf course or out on the ski slopes? What if you could collect a paycheque to watch Netflix all day, or just to sleep? Does this sound like winning the lottery? No, it's just what you get if you're convicted of attempted murder as a police officer in Ontario. No, it's just what you get if you're convicted of attempted murder as a police officer in Ontario..." The Record, A10

*** Funds cover police pay hikes**
A Letter to the editor states, "Regarding the article Other cities cost London wage win, budget chief says (Jan. 25). Londoners need to rest assured that at least a portion of the gap between what other lead cities (Toronto, Hamilton,Waterloo Region-all north of 2.5 per cent a year) are settling their police budgets at versus London's recent settlement of 0.95 per cent a year is covered off in both contingency and reserve funds in the 2016-2019 budget currently before council..." London Free Press, E3

A FAMILIAR PAIN, A CONSTANT HOPE
Fires at the cemetery burned for days, flames rising from the frozen Saskatchewan ground where far too many of the town's youth are buried. Grieving relatives tended to the blazes, working to warm the soil and make way for graves. La Loche, a northern town set on a lake at the end of a highway, will begin burying its latest victims of tragedy on Saturday, eight days after gunfire rang out at a local residence and at the village's only high school. Globe and Mail, A10

RCMP make drug bust
Three men have been charged after drugs and a large amount of cash and were seized from a Clearview Ridge home in Red Deer last week. Red Deer RCMP began their investigation into a suspected drug trafficking operation one week before executing a search warrant on the home on Cooper Close on the afternoon of Jan. 22. Red Deer Advocate, C2

RCMP looking for armed robbery suspect
Red Deer RCMP are looking for the man who robbed an A & W Restaurant at gunpoint on Sunday evening. Police say a man entered the A & W Restaurant located at 2004 50 Ave. carrying a handgun shortly after 11 p.m. on Jan. 24. He ordered the employees to the ground and demanded cash. Red Deer Advocate, A4

'We knew the guns were coming'
Members of a Prince Albert group have sent a package to Ottawa containing a five-year plan to address the escalation of gun violence in Saskatchewan. Over the last seven weeks, 14 people have been killed or injured by gun violence in Prince Albert and the province's northern communities, including the La Loche shootings that drew national attention. In Prince Albert, 23-year-old Jonathon Lee Cowan dies on Jan. 9; on Dec. 29, a 15-year-old suffered non-life threatening injuries after being shot in the face; and on Dec. 5, a 26-year-old man was shot in the leg. Postmedia News (StarPhoenix; * Leader-Post, A8)

Hells Angels surprised by eviction and say clubhouse rent is paid
A day after being kicked out of their fortified Hamilton clubhouse, the Hells Angels deny they have been negligent in paying rent. A local lawyer representing the local Hamilton chapter say the issue is one between the building owner - the clubhouse's landlord - and the person who holds the mortgage on the property and not at all about the club. CBC News

Another case tossed due to police errors
Another case has been thrown out of court because of police errors. When the case of Kyle Clarke was called Friday in provincial court in St. John's, the Crown indicated it would not be proceeding with the case... Clarke, from Gull Island, had been charged with three counts - accessing child pornography, possessing child pornography and making child pornography available to others. The Telegram, A1

Suspended Ottawa police officers continue to make Sunshine list in 2015
Officers suspended with pay in the Ottawa Police Service cost more than half a million dollars in salaries last year. The oldest suspension dates back to December 2011, which means that officer has been receiving a full salary since then, aside from a brief five-month reinstatement between hearing processes in 2014. CBC News

Police commission suspends Oland investigation
The New Brunswick Police Commission has suspended its probe into how Saint John police handled the Richard Oland murder case. The investigation will resume once the criminal proceedings end, executive director Steve Roberge said in a statement on Friday. Brunswick News (Telegraph-Journal, B1; Daily Gleaner; Times & Transcript)

Change culture by changing recruits
Inside the Toronto Police College this week, more than 75 mental-health activists and members of the policing community witnessed the very latest in annual training that will be offered to all members of the force. Developed in conjunction with mental health rights groups and survivors, the training emphasizes skills and characteristics that advocates and health professionals have long said are must-haves for police: empathy, communication and understanding. Toronto Star, GT1

What's changed since Sammy Yatim died?
Following the death of Sammy Yatim, Toronto police commissioned an independent review of use of force, looking specifically at encounters between officers and people in crisis. Written by retired Supreme Court justice Frank Iacobucci, the report - based on a year of research - makes 84 recommendations to Toronto police, with the aim of eliminating fatal encounters with police... Iacobucci recommended Toronto police consider expanding the use of conducted energy weapons, or Tasers - currently, only front-line supervisors, about 275 officers, have the weapon - and that may happen in the long term. But in the shorter term, Toronto Police Service's less lethal weapon of choice is the so-called "sock round," a shotgun that has been converted to shoot a small bean bag instead of a bullet. The bean bag "bullets" do not penetrate the skin. The guns will be distributed to all divisions throughout the city. Toronto Star, GT4

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Court relaxes travel, curfew restrictions for Omar Khadr**
Omar Khadr is allowed to stay out past his midnight curfew if required by employment or education commitments, Court of Queen's Bench in Edmonton ruled Friday. Khadr, who is living with his lawyer's family in Edmonton, is taking courses to become an emergency medical responder, possibly working in an ambulance. Such a position would require late hours. Federal and provincial lawyers did not oppose the change to his bail conditions, nor did they oppose Khadr's request to make travel easier. Postmedia News (Edmonton Journal, A4; Edmonton Sun)

*** Conditions de libération conditionnelle allégées pour Vincent Lacroix**
Le fraudeur Vincent Lacroix vient d'obtenir un léger assouplissement de ses conditions de libération conditionnelle en raison de sa bonne conduite. L'ex-PDG de Norbourg, condamné à 18 ans de prison pour avoir floué 9200 investisseurs, devra faire huit heures de bénévolat en milieu défavorisé par mois au cours de la prochaine année. Il devait auparavant en faire le double, soit quatre heures par semaine. Dans une décision du 12 janvier obtenue par La Presse, la Commission des libérations conditionnelles du Canada (CLCC) maintient toutes les autres conditions imposées à Vincent Lacroix depuis sa libération conditionnelle totale en février 2014. Il lui est notamment interdit de travailler comme gestionnaire ou dans le domaine de la finance. La Presse, 11

*** Red Deer man jailed for drug possession**
A Red Deer man caught trying to smuggle drugs into prison pleaded guilty to drug possession on Friday. Cameron Glen Monkman, 31, had been in the Red Deer Remand Centre less than a day when guards found drugs in his cell last May. Cocaine, methamphetamines and marijuana were found hidden in socks in his cell... Defence lawyer Greg Gordon said Monkman has struggled with drugs but is trying to change his life behind bars. He has volunteered for a screening unit in Drumheller Institution where prisoners agree to frequent drugs tests to help them stay clean. Red Deer Advocate, A4

*** Life of Ashley Smith inspires art exhibit**
When Toronto artist Gretchen Sankey looks at pictures of Ashley Smith, she doesn't see the Moncton woman who killed herself inside an Ontario penitentiary as a criminal or a convict. Sankey, herself the mother of a teenager with mental health issues, views Smith as someone who was ultimately failed by the system. Times & Transcript, A9

Corrections investigation of Kinew James death at RPC finds medical response too slow
A nurse at the Regional Psychiatric Centre in Saskatoon took too long to call a Code Blue after finding an inmate unresponsive late one January night, three years ago. That's one of the findings of a federal Corrections investigation report into the death of Kinew James, obtained by the CBC... She experienced chest pains while at another federal prison, Grand Valley Institution in Kitchener, Ont.... Code Blue should have been called. "The Board [of Investigation] believed that a Medical Emergency should have been called when James was found to be unresponsive and that having to wait approximately five minutes for another Correctional Officer to arrive on Church Unit to open the cell door delayed the staff response to an emergency situation," the report stated. CBC News (2016-01-29)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Stories of healing**
STR8-Up has been helping young men and women escape the gang life for decades. Started in Saskatchewan's prison system in the mid-1990s, the program aims to show young people a way out of gangs. The stories of how members escaped can be terrifying. So, too, are the stories of how they entered gang life in the first place. Now, a new book compiles those stories with the aim to show others there is hope. STR8 UP: Stories of Courage - A Healing Workbook is an "autobiographical workbook" that features the stories of 29 men and women who share their personal stories of recovery. Many are exgang members and many have spent time in prison. Here's an excerpt from one of those personal stories by STR8-Up member Jorgina Sunn. StarPhoenix, D1/Front

*** 40 more correctional officers to be hired**
The province says it is recruiting another 40 new correctional officers for Ottawa's chronically understaffed jail. The Ministry of Community Safety and Correctional Services said it is in the process of recruiting 180 new correctional officers to staff jails across the province. The latest hires are on top of a class of 144 recruits the province announced it was sending to the Ontario Correctional Services College earlier this month. It brings the total number of new correctional officers expected to be deployed to the Ottawa-Carleton Detention Centre to 73 since 2013. "The hiring of these new correctional officers will help ensure that staffing levels grow beyond normal turnover and retirement and ensure that officers are reflective of the diverse communities they serve," said a ministry statement released Friday. The new recruits are expected to complete an eight-week correctional officer training and assessment program, which includes mental health training, inmate management techniques and a thorough assessment and evaluation, according to the ministry. Ottawa Citizen, A4; Toronto Star, A14

*** Appeal Court shoots down sentence for bullied man**
A one-year sentence given to a Manitoba man who said he fired shots at a home because two people who lived there had bullied him has been overturned by the province's Appeal Court. Bryce McMillan was given the 12-month term after pleading guilty to firing at the home in Carberry, west of Winnipeg, in 2011.

The trial judge ruled the federal government's mandatory four-year minimum sentence for gun crimes violates the Charter of Rights and Freedoms. The Crown appealed the decision and the Manitoba Court of Appeal imposed the federal minimum term. The Record, A3

*** Leoville man pleads guilty**
Christopher Stephen Hogan, 30, recently pleaded guilty to a single count of using a social media website to utter a death threat against someone. The Leoville man was sentenced on to serve 24 months of probation and must pay a $100 victim surcharge. The incident happened on Aug. 5, 2015. Charlottetown Guardian, A6

*** Heart of darkness**
On paper, Colleen Murphy's angry, anguished response to the Robert Pickton pig farm murders is a numbing, almost unbearably upsetting read. In Imago Theatre's production, the action, involving the sustained taunting, torture and slaughter of a bloody but defiantly unbowed indigenous prostitute, has been transformed into a kind of fugue for four voices. There's the Dying Girl herself (so named to leave us in no doubt of her fate) and the damaged, lonesome Killer who tries to make a connection with her in the vilest ways possible. Then, in another timeframe, there's the Sister who spends years in a fruitless search, and the Police Officer whose initial bureaucratic indifference comes to sear his conscience. Montreal Gazette, F10

*** Bootleg fentanyl, heroin suspected in rash of overdoses**
Drug users who think they are buying cocaine or heroin may be also getting bootleg fentanyl, which is being blamed for overdoses across the country. In Waterloo Region, six overdoses were reported in Cambridge and Kitchener from Jan. 23 to Jan. 26. One person died. The Record, B3

Prisoners' complaints
St. John's lawyer and mental-health advocate Mark Gruchy says psychiatric services in the province's prison system may be tantamount to human-rights abuse, and the province's Human Rights Commission says it's willing to look at cases. Under the Newfoundland and Labrador Human Rights Act, the commission is limited to looking at discrimination based on accommodation, employment and services. The Telegram, A3

UPEI student jailed for drunk driving
An international student at UPEI who was caught swerving on the road while driving drunk was sentenced Thursday to a night in jail... Yousuf is an international student at UPEI who was born in Pakistan. Before hearing his sentence, Yousuf told the court the drunk driving incident was the only time he had done something like it. Douglas sentenced Yousuf to one day in jail and ordered him to pay a $1,000 fine along with a $300 victims of crime surcharge. Charlottetown Guardian, A6

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

*** As other cities hit pause button, Windsor's Syrian refugees flow in**
Other Canadian cities are pressing the 'pause' button on the inflow of Syrian refugees, but not Windsor. "We can ask for a slowdown ... but we haven't needed one yet," said Kathleen Thomas, executive director of the Multicultural Council of Windsor and Essex County, which co-ordinates local resettlement efforts for government-assisted refugees. Windsor Star, A2

Réfugiés syriens
L'ancien ministre de l'Immigration Chris Alexander défend l'approche adoptée par son gouvernement pour relocaliser les réfugiés syriens, niant les allégations selon lesquelles les conservateurs avaient sélectionné soigneusement des dossiers en priorisant certaines minorités ethniques et religieuses. Tous les pays travaillant avec le Haut Commissariat des Nations unies pour les réfugiés en lien avec la crise humanitaire en Syrie ont fonctionné selon un processus accepté d'avance qui établissait les critères de sélection pour choisir les réfugiés, a déclaré M. Alexander en entrevue avec La Presse Canadienne.

Presse Canadienne (L'Acadie Nouvelle, 27) ; Canadian Press (Chronicle Herald, A11; Daily Star, Hamilton Spectator, The Record, Montreal Gazette)

PUBLIC SERVICE / FONCTION PUBLIQUE

The whistleblower
Sylvie Therrien considers herself a "bit of a rebel" - someone who doesn't like being told to keep quiet when she disagrees or feels an injustice is being committed. So when she was asked to help the government squeeze EI payouts, she refused to quietly play along... In the meantime, there is the matter of making a living. Therrien is currently before the Public Service Labour Relations and Employment Board pursuing a grievance against Service Canada, seeking financial compensation for her firing and to have it overturned. She's being represented by the Public Service Alliance of Canada, a union for federal workers. "PSAC has always fought to protect the rights of workers who disclose wrongdoing in the public service," says PSAC national president Robyn Benson, who wouldn't comment directly on Therrien's case. Toronto Star, IN1

PS unions want more than just 'review' of bill
The Liberal government and federal unions are locking horns over a piece of Conservative-era labour legislation even before they reach their first round of collective bargaining. Treasury Board president Scott Brison said Friday he is sticking to his plan to review rather than repeal Bill C-4, the contentious Tory legislation that completely changed the ground rules for collective bargaining in the public service... That's not what the unions wanted to hear. This week, union leaders asked the government to immediately repeal the legislation and bring back the rules that previously governed bargaining. The 18 unions signed a solidarity pact more than a year ago over the contentious issue of sick leave and disability management. They have presented a united front in refusing to make any concessions. "We are in strong disagreement with your proposal to revisit Bill C-4 through consultations with 'public sector partners,' " they wrote in a joint letter... The letter comes as the biggest union, the Public Service Alliance of Canada, is poised for its first bargaining session with the Liberals on Monday. Ottawa Citizen, A10

OTHER / AUTRE

La protection consulaire à géométrie variable
Maher Arar a été emprisonné et torturé en Syrie pendant plus d'un an, au début des années 2000. Omar Khadr a atterri à Guantánamo en 2002, à l'âge de 15 ans, pour en sortir une décennie plus tard, marqué à jamais par le traitement inhumain qu'il y a subi. Plus récemment, le journaliste Mohamed Fahmy a croupi pendant plus de 400 jours dans une prison égyptienne, sous des accusations bidon, avant d'être libéré avec une épaule définitivement endommagée en guise de séquelle. La Presse

Dion et Kerry discutent du futur rôle du Canada contre le groupe État islamique
Le secrétaire d'État américain, John Kerry, ne connaît toujours pas la nouvelle stratégie canadienne de lutte contre le groupe armé État islamique (EI), mais il s'attend à ce que la contribution du Canada soit à tout le moins maintenue. Au terme d'une rencontre des trois ministres des Affaires étrangères de l'Amérique du Nord organisée vendredi à Québec, John Kerry a affirmé qu'il demeure convaincu de voir le Canada maintenir une implication " significative " dans la lutte contre le groupe EI, principalement en Irak et en Syrie. Le Devoir, A3 ; Canadian Press (Chronicle Herald, A8; Times Colonist)

Jordan, Lebanon added to plans
Canada's new role in the fight against the Islamic State will involve ensuring Jordan and Lebanon remain stable, Foreign AffairsMinister Stephane Dion said Friday after a meeting with his U.S. and Mexican counterparts. Dion promised that Prime Minister Justin Trudeau will soon announce details of Canada's new deploymentwithin the Americanled coalition. The Liberals promised during the election campaign to end Canada's role in the bombing mission over Iraq and Syria. Canada's role won't focus solely on Iraq,

said Dion, adding "we will see what to do about Syria." Canadian Press (London Free Press, B3; Montreal Gazette, Times & Transcript)

Sajjan: Let's avoid errors of Afghan war
Defence Minister Harjit Sajjan argued Friday in favour of a calm, considered recasting of Canada's combat mission in Iraq. He pointed to past mistakes, saying that in the Afghan war, some wellintentioned development aid wound up fuelling corruption and instability. Canadian Press (Times Colonist, A10; Whig-Standard, London Free Press); Postmedia News (Ottawa Citizen, A10; National Post)

China denies spy charge against Canadian is retribution against Ottawa
The Chinese government has denied claims it has charged a Canadian man with spying as an act of retribution for the arrest and extradition proceedings against a Chinese man wanted by the United States for allegedly stealing fighter-jet documents. Kevin Garratt was indicted this week after investigators "discovered some new evidence" regarding his "accumulation of information in China," foreign ministry spokeswoman Hua Chunying said Friday. Globe and Mail, A3

Man was spying for canada, china says
China's Foreign Ministry said Friday that an investigation has suggested that a Canadian man charged with spying and stealing Chinese state secrets had carried out assignments for Canadian intelligence agencies. The federal government said Thursday it was concerned that Kevin Garratt had been indicted and that it had raised his case with the Chinese government "at high levels." Associated Press (StarPhoenix, N5; Edmonton Journal, Leader-Post, National Post)

MPs demand federal government act on drug worries
Opposition MPs criticized the federal government Friday for distributing a controversial anti-malaria drug to military personnel while using outdated warnings to users. Their statements followed a U.S. expert's assertion to The Vancouver Sun that Canada is failing to inform soldiers they could suffer from serious and permanent health issues by using mefloquine. New Democratic Party defence critic Randall Garrison, the MP for Esquimalt-Saanich-Sooke, said Canada is handling the drug in a "disturbing" manner. Vancouver Sun, A16

Malaria Drug To Blame, Say Experts
Former soldiers from the disbanded Canadian Airborne Regiment are pushing for a ban on the controversial anti-malaria drug mefl oquine that some say plagued the disastrous 1993 Somalia mission. Two events - the 2013 U.S. military ban on mefloquine for Special Forces and new scientific studies showing toxicity from the drug can cause permanent brain damage - should force a review of Canadian policy, says John Dowe, a former airborne soldier. Edmonton Journal, B1

Canada should play leading role - UN official
A former United Nations refugee chief says Canada's new foreign policy makes it perfectly suited to play a major role in bringing peace to a world facing a dramatic shortage of it. Antonio Guterres said Canada is now perceived as an honest broker and can play a leading role in bringing together warring factions to negotiate peace. Chronicle Herald, A12

Déchéance et indignité
Un article d'opinion déclare, « Victoire du Front national (FN), qui a poussé le gouvernement socialiste de la France à adopter une mesure que n'aurait pas dédaignée le régime pétainiste de Vichy. Victoire des terroristes, qui ont réussi à altérer l'âme de la patrie des Lumières...C'est ainsi que l'on pourrait résumer, en exagérant à peine, ce qui se passe actuellement en France. Les parlementaires français s'apprêtent à voter une loi qui inscrira dans la Constitution la possibilité de retirer la citoyenneté française aux personnes condamnées pour «un crime ou un délit qui constitue une atteinte grave à la vie de la nation». Passons sur le flou de la formulation, qui ouvre la porte à n'importe quoi. On comprend bien qu'il s'agit (pour l'instant) de sévir contre le terrorisme... Au Canada, Stephen Harper comptait enlever la citoyenneté canadienne aux auteurs de crimes terroristes qui détiennent une autre nationalité. Ce projet est heureusement tombé avec son gouvernement. Le projet de loi français ne mentionne pas la binationalité,

pour ne pas donner l'impression de faire des binationaux des citoyens de seconde zone, ce qui aurait l'air de déroger au beau principe de l'égalité républicaine. La Presse, A19

Le sain débat
Une lettre à l'éditeur déclare, « La violence comporte plusieurs visages, dont certains sont flous, à première vue. Je pense à cette violence qui est l'absence de mots, comme le disait avec pertinence le poète Gilles Vigneault…En voulant ainsi clouer le bec aux adversaires, là vous dépassez vous-même les bornes. Je pense ici à un lecteur d'opinion qui traite de naïfs et accuse de raisonner follement celles et ceux qui avancent que les causes profondes des avancées du terrorisme islamique dans le monde sont l'impérialisme et le matérialisme occidentaux. Ou qui se dit en désaccord avec celles et ceux qui pensent que le retrait des avions de guerre canadiens d'Irak et de Syrie par le gouvernement protègera mieux les Canadiens contre les attentats terroristes… » Le Quotidien, 13

INTERNATIONAL

*** Deux des mafiosi italiens sont retrouvés dans un bunker**
Deux mafiosi italiens en cavale depuis plus de dix ans ont finalement été épinglés dans un bunker souterrain, dans le sud de la Calabre. Les deux dirigeants de la 'ndrangheta - Giuseppe Crea, 37 ans, et Giuseppe Ferraro, 48 ans - sont considérés comme deux des fugitifs les plus dangereux d'Italie. Crea est passible de 22 ans d'emprisonnement pour association mafieuse et il était en fuite depuis dix ans. Ferraro a été condamné à la prison à vie, notamment pour meurtre, et il échappait aux autorités depuis 18 ans. Associated Press (L'Acadie Nouvelle, 30) ; Associated Press (The Record, A6)

How Magnet Forensics is making a difference
Police captured Boston Marathon bomber Dzhokhar Tsarnaev from his hideout in a boat in a dramatic hail of bullets, but that was just the beginning of their work. Less exciting, but just as important, was the task of combing through at least 30 electronic devices seized in connection with the investigation into Dzhokhar and his brother Tamerlan Tsarnaev, who was killed in a previous shootout following the 2013 bombing that killed three and injured more than 260. Those devices included seven computers, 10 external hard drives and 13 cellphones, containing more than 20,000 pieces of data. National Post, FP5

The battle against Islam's bearded men
In a bid to curb Islamist radicalization, authorities in the Central Asian republic of Tajikistan shaved the beards off nearly 13,000 men in the country. They also shut down about 160 shops selling traditional Islamic garb and supposedly "convinced" more than 1,700 women to stop wearing hijabs, or head coverings. According to Radio Free Europe's Tajik service, the measures were taken in the southwest Khatlon region, which borders Afghanistan. The region's head of police said that 12,818 men with "overly long and unkempt beards" were "brought to order" in 2015. Washington Post (Toronto Star, WD6)

UN Syria envoy to start talks in Geneva without opposition
A UN official said Syrian peace talks will begin in Geneva as planned today, despite an ongoing boycott by the main Syrian opposition group which continues to stay away pending assurances from the UN chief on the implementation of Security Council resolutions related to humanitarian issues. Associated Press (Daily Star, 18)

Theme parks hire more security due to greater fear of terrorism
Walt Disney World and Universal Orlando are hiring additional security employees as theme parks enter what experts say is a new era of stepped-up efforts to shield visitors from possible terrorism and mass shootings. The theme parks would not say how many people they are adding or give details on the security measures they are taking. At Disney, many of the new security personnel will help staff metal detectors. Times & Transcript, F3

Canada steps away from Israel
An opinion piece states, "This week marked the anniversary of the liberation of Auschwitz, one of the largest Nazi death camps of the Second World War. Six million Jews were killed during the Holocaust,

many inside gas chambers at these death camps. On International Holocaust Remembrance Day, January 27th, people around the world commemorate the horror inflicted on the Jews of Europe... Canadian Foreign Affairs Minister Stephane Dion released a statement calling for restraint in the region and suggesting both sides are equally to blame..." Postmedia News (Winnipeg Sun, A9; Edmonton Sun, Calgary Sun, Ottawa Sun)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PS.PSPMediaCentre/CentredesmediasPSP.SP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
February 19, 2016 / le 19 février 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

We're marshalling our snoops
The Communications Security Establishment, Canada's electronic spy service, is set to play a more prominent role in the war against the Islamic State of Iraq and the Levant, The Canadian Press has learned. Multiple sources familiar with the plans, speaking on condition of anonymity owing to the sensitivity of the matter, say the government is deploying a capability that only a "handful of countries" in the world can provide. CSE is part of the so-called "Five Eyes" community, along with the U.S. National Security Agency-the NSA. CSE spokesperson Ryan Foreman acknowledged the agency is helping Canada's military under the umbrella of Operation Impact, Canada's anti-ISIL mission in the Mideast, but refused to elaborate. "While we are proud of our contributions to CAF's missions, CSE is obligated to respect the Security of Information Act, and cannot address specific operational questions," Foreman said. Defence Minister Harjit Sajjan has for weeks been signalling the military will introduce a "more robust" intelligence-gathering regime, one that allies - chastened by withdrawal of six CF-18s -arehappy to see join the fight. Separately, **Public Safety Minister Ralph Goodale** confirmed Thursday that the Canadian Security Intelligence Service also will play a stepped-up role in the fight against the Islamic State, but he also refused to be specific. Canadian Press (London Free Press, B1/Front, Guardian, Red

Deer Advocate, Times Colonist, Record, National Post, Times & Transcript, Whig-Standard, Waterloo Chronicle); Toronto Star, A10; * Siver Times; * Our Windsor

Ottawa drops appeal of Omar Khadr's bail

The federal government has decided against pursuing an appeal of an Alberta court's decision to grant former Guantanamo Bay inmate Omar Khadr bail. The decision came in a joint statement Thursday from **Public Safety Minister Ralph Goodale** and Justice Minister Jody Wilson-Raybould. ***"The government of Canada respects the decision of the Court of Queen's Bench of Alberta, which determined that Mr. Khadr be released on bail in Canada pending his U.S. appeal of his U.S. convictions and sentence,"*** the statement said. ***"Withdrawing this appeal is an important step towards fulfilling the government's commitment to review its litigation strategy."*** The decision caught one of Khadr's lawyers by pleasant surprise. "We're pleased with the government's decision. We think it's the right decision. We never did think there was much merit to this appeal," Nate Whitling said in Toronto. "Now Omar can get on with his reintegration." The Liberal government decision is a sharp break from its Conservative predecessor, which fought hard to keep Khadr behind bars for the duration of his sentence. Canadian Press (Whig-Standard, B1/Front, Times Colonist, Red Deer Advocate, Guardian, Calgary Sun, Vancouver Sun, Winnipeg Sun, Record, National Post, Toronto Star, Winnipeg Free Press, Edmonton Sun, Toronto Sun, Ottawa Sun, Calgary Herald, Edmonton Journal); La Presse canadienne (Le Soleil, 19, Voix de l'Est, La Tribune, Acadie Nouvelle, Le Devoir, Le Droit, Globe and Mail, Times & Transcript, Telegraph-Journal); Journal de Montréal, 22 (Journal de Québec); * MacLean's; * James Town Sun

U.S. no fly list may have tripped up Canadian youngsters

The U.S. no-fly list, not Canada's secret air-security roster, might be what has been ensnaring Canadian youngsters, **Public Safety Minister Ralph Goodale** is telling several families experiencing travel headaches. In a letter to a representative of dozens of families whose children have trouble boarding airplanes, **Goodale** says delays can occur for passengers who have the same name as a person on Canada's list, or "***another security-related list such as the U.S. no-fly list.***" The reply to Khadija Cajee, whose six-year-old son Adam has been repeatedly delayed at the airport, underscores the complex _ and often hidden _ web of security measures intended to keep North American skies safe. **Goodale** promised to investigate after Adam's father, Sulemaan Ahmed, tweeted a photo from Toronto's international airport that appeared to show the boy's name with a "deemed high profile" label and instructions on how to proceed before allowing the youngster to check in. They were trying to board an Air Canada flight Dec. 31 to Boston to see the NHL Winter Classic. Soon after, **Goodale** said ***his officials had reminded airlines they don't need to screen children against Canada's no-fly list, officially known as the Passenger Protect Program.*** Canadian Press (Cape Breton Post, A9, Guardian, Calgary Sun, Times Colonist, Toronto Star, Winnipeg Free Press, Ottawa Sun, StarPhoenix, Leader-Post, Toronto Sun, Gazette, Calgary Herald, Ottawa Citizen, Whig-Standard); * La Presse canadienne (Acadie Nouvelle, 16)

*** Trudeau government targets cyber threats**

With Internet-based child sex-ploitation crimes skyrocketing, the Trudeau government intends to launch a "credible and comprehensive" review this spring of cybersecurity threats in Canada. Officials with **Public Safety Canada** said Thursday ***that while the details of that review are still being hammered out by Public Safety Minister Ralph Goodale***, a review will determine how Canada can best deal with everything from online predators to digital jihadists. Kathy Thompson, assistant deputy minister in charge of the Community Safety and Countering Crime Branch at Public Safety Canada, said that while the crime rate continues to decline across the country, "there are some exceptions. One of those exceptions is child sexual exploitation over the Internet - that is going up exponentially, year over year." Thompson made her remarks at the House of Commons Public Safety and National Security Committee, where MPs are looking for topics their group can zero in on during the current parliamentary session. A cybersecurity review that looks at legal gaps and shortcomings in police resources could form a plan for the way the Trudeau government approaches lawand-order issues. Toronto Sun, A8 (Calgary Sun, Winnipeg Sun, Ottawa Sun, Edmonton Sun)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Canadian lab ready to produce Zika vaccine by end of the year**
First, it was a Canadian creation that became the first real weapon against Ebola. Scientists at the National Microbiology Laboratory (NML) were working on a vaccine before the 2014 pandemic hit. The World Health Organization used vials of the untried medication in clinical trials in Guinea. It quickly proved a "game-changer" that protected everyone who received it. Now, only days after most people learned the word "Zika," the Winnipeg-based researchers may have done it again. The lab's head of special pathogens said last month they could have a vaccine to combat the mosquito-born illness ready by year's end. "This vaccine is easy to produce. It could be cranked to very high levels in a really short time," Dr. Gary Kobinger told Reuters. Postmedia News (National Post, A1; Vancouver Province, Vancouver Sun, London Free Press, StarPhoenix, Ottawa Citizen, Calgary Herald, Leader-Post, Montreal Gazette, Windsor Star, Edmonton Journal)

*** Rigorous testing of Canada's fixed wing search and rescue candidate aircraft to begin soon**
The Canadian military's fixed wing search and rescue project continues to move along. The bids went in Jan. 11 and the bid evaluation is now underway. An extensive testing of the candidate aircraft is soon to begin. "Bid evaluation, which includes aircraft testing, is expected to take about six months," Public Procurement and Services Canada spokeswoman Jessica Kingsbury told Defence Watch. "Testing is expected to begin in March and will take place at bidders' facilities." Kingsbury would not say which aircraft are being tested. "In order to preserve the integrity of the process, the department can provide no further information while the evaluation is underway," she added. Ottawa Citizen

*** Province preparing for upcoming wildfire season**
Even with snow still on the ground, the Ministry of Environment is preparing for wildfire season. After a precedent-setting wildfire season in 2015, government spokesperson Karen Hill said the government will be ready to respond to upcoming wildfires as they occur. "It is difficult to predict what the 2016 wildfire season may bring, as hazards depend on many factors including the timing and speed of the snow melt, temperatures, late winter [and] spring precipitation, and the overall forest fuel conditions," Hill said in an emailed statement. The wildfire season in Saskatchewan's north runs from April 1 to Oct 31. Hill said with the warm winter and below normal snowfall, Wildfire Management is getting ready for the possibility of an early start to the season. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Canada's electronic spies at the centre of beefed up ISIL intelligence effort**
The Communications Security Establishment, Canada's electronic spy service, is set to play a more prominent role in the war against the Islamic State of Iraq and the Levant. Multiple sources familiar with the plans, speaking on condition of anonymity owing to the sensitivity of the matter, tell The Canadian Press that the government is deploying a capability that only a "handful of countries" in the world can provide. A spokesman for the agency acknowledged the spy agency is helping the Canadian Forces under the umbrella of Operation Impact, but would not get into specifics. Defence Minister Harjit Sajjan has for weeks been signalling that the military would introduce a "more robust" intelligence-gathering regime, but has refused to discuss specifics. The capability being deployed is similar to the one CSE and the Canadian military used to combat the Taliban during the war in Afghanistan. Canadian Press (Cape Breton Post, A9)

*** ELLES JOIGNENT L'ÉI POUR FAIRE DES ENFANTS**
Des jeunes femmes canadiennes se sont rendues en Syrie et en Irak pour joindre le groupe État islamique et faire des enfants. Selon le Globe and Mail, au moins trois Canadiennes ont donné naissance au sein de ce groupe terroriste au cours des deux dernières années. Deux autres seraient enceintes. Ces jeunes mères seraient âgées de 19 à 22 ans et sont parties du Québec, de l'Alberta, de la Colombie-Britannique et de l'Ontario, a affirmé Amarnath Amarasingam, chercheur à l'Université de Waterloo. Leur décision serait motivée par leurs valeurs politiques et religieuses et leur but serait de «produire la

prochaine génération de combattants» islamiques, a-t-il indiqué au quotidien anglophone. Les familles de ces Canadiennes, qui se trouvent toujours au pays, seraient prêtes à les aider en leur envoyant des vêtements et des couches. Journal de Montréal, 28 (Journal de Québec)

*** Tensions et intimidation au collège de Maisonneuve**
L'un des protagonistes de cette bagarre fait partie du groupe de dix jeunes Montréalais arrêtés en mai dernier à l'aéroport de Montréal alors qu'ils tentaient d'aller grossir les rangs d'un groupe islamiste en Syrie. Le jeune homme est un élève du cégep. Rappelons que cinq élèves de Maisonneuve ont quitté le Canada en janvier 2015 et ont réussi à se rendre en Syrie et en Irak. Quatre, dont celui dont il est question dans cet article, ont été interceptés en mai. Deux autres sont derrière les barreaux en attendant leur procès pour avoir eu des substances explosives en leur possession. (…) C'est arrivé le 7 décembre. Le Service de police de la Ville de Montréal a confirmé que ses patrouilleurs sont intervenus dans le stationnement de l'établissement après qu'une bataille impliquant plusieurs personnes a éclaté. Le conflit s'est déclaré dans l'établissement entre un groupe de six élèves en administration qui préparaient un examen devant la bibliothèque et une quinzaine d'autres jeunes, qui, selon plusieurs employés et élèves, monopolisent quotidiennement cet espace. Le garçon intercepté par la GRC à l'aéroport en mai faisait partie de ce deuxième groupe. Selon nos informations, ce sont les commentaires sur le bruit ambiant lancés par une jeune femme qui tentait d'étudier qui auraient mis le feu aux poudres. S'en est suivie une série d'insultes et d'injures entre les deux camps. Puis les élèves en sont venus aux coups, selon ce que nous a raconté une personne impliquée dans l'incident qui a demandé l'anonymat, de peur de représailles. La Presse

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Federal Liberals lift deportation order for Syrian youth
The Liberal government has changed course and lifted a deportation order for a 16-yearold Syrian boy who was recently detained under Canada's immigration laws. The controversial case has highlighted the use of detention for foreign national children. It is supposed to be used as a last resort, but many critics have said it should be shelved. Immigration, Refugees and Citizenship Minister John McCallum cancelled the boy's deportation, which was scheduled for Feb. 25, on Thursday and granted him permanent residency, according to the boy's lawyer, Aviva Basman, of the Refugee Law Office in Toronto. The boy is being referred to as "Mohammed" for safety reasons. "We've had some great news. Mohammed's removal was cancelled. The minister has approved him for permanent residence on humanitarian and compassionate grounds," Ms. Basman said in an e-mail to The Globe and Mail. Mohammed was detained in isolation for three weeks in Toronto last month after attempting to claim refugee status at the Canada-U.S. border. The Canada Border Services Agency (CBSA) can hold people, including children, who are a flight risk, pose a threat to public safety or whose identities cannot be confirmed. However, the Immigration and Refugee Protection Act says that "a minor child shall be detained only as a measure of last resort." (…) The CBSA said that while there were no children in detention under Canada's immigration laws as of last Friday, 16 foreign national children have been detained at some point since November at one of the country's three immigration holding centres in Toronto, Vancouver or Laval, Que. Globe and Mail, A4; CBC News (2016-02-18); ; * Vice News (2016-02-18)

Border agents offer lift to school
A few more pieces of the puzzle regarding a Canada Border Service Agency raid at a Charlottetown motel are starting to fall in place. Ping Zhong, listed in the P.E.I. corporate registry as president, secretary and treasurer of the Sherwood Motel, was reluctant to comment, saying she was not on site Wednesday as agents swooped in to begin a day-long investigation at her motel. Zhong told The Guardian the raid was focused on a woman and her teenage son who had been living in one of the units at the motel for the past two years. A witness at the scene on Wednesday said a person was taken into custody as part of the raid. Zhong was told that is not the case. "I spoke to the mother today," Zhong said. "She said all they did was take the boy to school because he was late for the bus. He usually takes the bus every day." Agents arrived at the motel complex at around 8 a.m. Wednesday, according to residents who live full time at the motel. (…) Zhong said the investigation had nothing to do with the motel or with her personally. "I think this is really damaging our business reputation," she said. She said operations returned to normal

Thursday, but media inquires were pouring in. She said if there is anything more to learn about the investigation, it will be up to the Canada Border Services Agency to release those details. That certainly wasn't happening on Thursday. The Guardian requested additional details from the agency but was told there will be no further comment on the case because it is still under investigation. On Wednesday, Chastity McKinnon, regional director of communications for the Atlantic region of the Canada Border Services Agency, confirmed a search warrant had been executed in relation to an ongoing investigation. Guardian, A1, A2/Front (Journal Pioneer)

* **Le Salon bilingue de l'emploi de St. Catharines établit de nouveaux records de participation**
Le Centre d'emploi et de ressources francophones (CERF) du Niagara et Business Education Council, avaient organisé, le mercredi 10 février, un Salon bilingue de l'emploi dans le Niagara. Les deux organismes ont de quoi être fiers du succès de l'édition 2016 du traditionnel carrefour de rencontres entre les chercheurs d'emploi et les employeurs potentiels. Selon Nicole Schaubel, gérante de programme au CERF-Niagara, le Salon bilingue de l'emploi de St. Catharines a battu son propre record en accueillant plus de 600 visiteurs. En effet, en 2015, l'affluence se situait entre 500 et 600 visiteurs. Du côté des exposants, le répertoire des organisateurs indiquait 92 organismes dont 27 Services communautaires et 65 employeurs potentiels. (…) Du côté des employeurs, il fallait se bousculer pour caser tout le monde. Il y avait toutes sortes d'entreprises : des entreprises familiales aux bureaux locaux de multinationales en passant par des petites et moyennes entreprises. De nombreux secteurs d'activités étaient représentés dont l'industrie touristique, l'économie, l'éducation, la construction, la sécurité, la santé, l'industrie alimentaire ainsi que des associations sans but lucratif tel le Foyer Richelieu. Des services publics tels que la Police, les Forces armées et l'Agence des services frontaliers du Canada étaient également présents avec des renseignements utiles pour les chercheurs d'emploi. Selon le sergent Wayne Paulin, recruteur des Forces armées canadiennes, l'armée offre chaque année quelque cinq mille postes divers à des citoyens canadiens dont l'âge varie entre 18 et 75 ans. Le Régional (2016-02-18)

* **A criminal in Germany and Japan, a "refugee" in Montreal**
A federal department is trying to evict him, but a court decided otherwise. Proof that Canada can not filter those who enter the country as it would like to An arm of the federal government tries to deport an Iranian refugee while another arm tries to keep him here, as our Bureau of Investigation found out. Since 2010, the Ministry of Federal Public Security has tried to expel an Iranian refugee admitted to Canada in 2001, after discovering that he had hidden crimes in Japan and Germany. This refuge was denounced to the Canadian government for alledged involvement in drug trafficking and with the Yakuza, the Japanese organized crime members, according to our information. But as incredible as it may seem, the Immigration and Refugee Board refuse to allow the expulsion of this man from Canada. This is about Afshin Norouzi, who now lives in Montreal. Norouzi's case, which is still pending, shows that the security screening of refugees by the government and its agencies leaves much to be desired. (…) Through his attorneys, Norouzi finally admitted some of his misrepresentations in February 2015, including his criminal history and his multiple trips to Iran after his request for asylum. An important admission? No His criminal history in Japan and Germany had been confirmed to the investigators of Border Services, the GRC (RCMP) and Interpol. The Rebel

Dilkens makes a pitch for self-driving car test site
Windsor Mayor Drew Dilkens pitched the city as a potential test site for autonomous vehicles during a two-day visit to the Canadian International Autoshow. "With respect to the people and industry leaders who are here, we are having those conversations and trying to position our community as a potential test site," Dilkens said Friday. Dilkens joined government officials, auto and information technology industry leaders who attended a morning conference on the advent of autonomous vehicles. (…) Windsor, said Dilkens, has attributes that would also make it an attractive test bed for self-driving cars. "We look at our urban and rural environment; we look at our location with respect to being on the border and having those autonomous vehicles one day being able to cross the border and manage that type of setup," he said. "Those are just two examples of how our region is really well positioned to be a test site in the future for autonomous vehicles." Windsor Star, SR4

Market Slip silt affecting pleasure boat options
Pleasure boats may not have much space to dock at Market Slip this summer after the city scratched a $195,000 line from its capital budget that would have been used to dredge silt that has accumulated there. In the next few weeks, the Saint John Waterfront Development Corporation plans to measure the water depth there at low tide to see if they can put in any floating docks for the summer boating season, said Kent MacIntyre, general manager of the corporation. (...)Coun. David Merrithew has suggested that the Port Corporation might do the city a favour and dredge the spot at Market Slip. (...)Merrithew is disappointed that the Port Corporation can't do the dredging for the city. Port lands don't generate property tax because they are owned by the federal government, but the city provides policing and fire services to the port, he said. The port used to have its own police force but it was disbanded by the federal government in the late 1990s and the responsibility was downloaded onto the city, Merrithew said. In 2004 the Fundy Integrated Intelligence Unit was formed covering the Fundy region. It includes members of the Saint John Police Force, the RCMP J-division criminal intelligence, Canadian Border Services Agency, Rothesay Regional Police, Income Tax, Immigration, Canadian Correctional Services, **Public Safety**, N-West a national weapons enforcement support team, and the Hampton RCMP. Telegraph-Journal, B5

* **How to plan infrastructure spending for the greatest good**
As Finance Minister Bill Morneau prepares his first federal budget, there is a consensus among economists that, given the current state of the economy, some short-term stimulus is needed, and that infrastructure spending is the most effective tool. There is also a consensus that the best infrastructure spending is for strategic capital projects that are not necessarily "shovel-ready" today, that require more planning before they can be built, but that will increase Canada's productive capacity for the long term. Mr. Morneau's challenge is to square the circle. He must address a short-term economic imperative, but must also plan to provide the longer-term support needed for large, strategic capital projects. The new government has committed to investing $125-billion in infrastructure over the next 10 years. The minister's fundamental issues to decide are what types of infrastructure, over how long, how to pay for it and the role of politics in the project decisions. When Prime Minister Justin Trudeau and big-city mayors met in Ottawa on Feb. 5, the mayors had ideas about both kinds of projects - relatively small, shovel-ready projects and larger ones that can transform Canadian cities and contribute to greater economic productivity over the medium and longer term. Tens of billions of dollars are required for our cities because of many years of inadequate spending on municipal infrastructure. There is a large infrastructure deficit for deferred maintenance - repair and modernization of water and sewage lines, road repairs, modernization of civic buildings, construction of social housing and (given Canadian winters) the filling of potholes. But the larger-scale strategic infrastructure projects - public transit, green infrastructure, electricity grids, ports, critical highways, border infrastructure, science and technology infrastructure and so on - also require massive investment over the next decade. Globe and Mail, B4

Eye scanning, facial recognition being tested at San Diego border
The U.S. government announced Thursday it is using eye scans and facial recognition technology for the first time to verify the identities of foreigners leaving the United States on foot at a busy San Diego border crossing with Mexico, the latest move to close a longstanding security gap. Border officials in December started collecting the same information on non-citizens walking into the U.S. through the checkpoint connecting Tijuana and San Diego. The checkout system that launched Feb. 11 aims to ensure those who enter the country leave on time and identify those who stay after their visas expire. Up to half of the people in the U.S. illegally are believed to have overstayed their visas. Congress has long demanded biometric screening such as fingerprints, facial images or eye scans from people leaving the country, but the task poses enormous financial and logistical challenges. Privacy advocates worry the data could be misused or fall into the wrong hands. Before now, foreigners who left the country were rarely checked by authorities before walking into Mexico or Canada at ports of entry. Cameras have started photographing the eye and facial features of non-citizens leaving the country through the Otay Mesa port of entry to verify their identities on their documents. Winnipeg Free Press, A16 (Times Colonist, Cape Breton Post, Fox News)

*** Low loonie attracting U.S. tourists to P.E.I. this summer**
There's an Island upside to the low Canadian dollar: tourism operators say they're expecting to have a fantastic summer season. Several hotels are reporting that bookings from south of the border are already up, and they've been getting a lot of calls lately. "We are gradually getting, I'm finding, getting more and more calls trying to book in," said Nancy Leslie, of Canada's Best Value Inn & Suites. "Because last summer was really, people were calling and couldn't get rooms here." CBC News (2016-02-18)

*** Beating Moroun at his own game**
An opinion piece states, "Since Matty Moroun seems intent on destroying the Windsor waterfront both at the foot of Lauzon Road and in the west end adjacent to the Ambassador Bridge, I'd like to suggest a way to beat him at his own game. Since he sees nothing wrong with letting properties crumble and become eyesores, I suggest in like fashion we build the new Gordie Howe Bridge, and then completely cut offall access to the Ambassador Bridge, rerouting all roads so as to completely cut it off. Then, Huron Church Road will simply become what it was always intended to be - a major artery to the riverfront and the university in the west end. Mr. Moroun's eyesore of a bridge will continue to crumble as it will become a useless bridge to nowhere, thereby ending his monopoly while hugely improving profits at the Canadian-owned Gordie Howe Bridge." Windsor Star, A6

*** Canadian workers should build Site C dam**
A letter to the editor states, "We have heard Premier Christy Clark say Site C is going to provide jobs for the people of B.C. Would someone then explain why so many contracts have been awarded to Spanish and Korean companies? Could it be as high as 80? A job posting dated Feb. 9 states that duties include "creating the Monthly Temporary Workers Report" and "assisting in the Temporary Foreign Worker process." With all the unemployment we have in Canada, why are the B.C. Liberals handing out jobs to foreign corporations and temporary foreign workers? Aren't the unemployed in B.C., Alberta and Saskatchewan good enough to work in B.C. on something that will be paid for by B.C. taxpayers? All those "free trade" agreements signed by the previous federal government have provisions in them for foreign corporations to bring in their own workers, if they have contracts in Canada. Many of us will recall how coal miners were brought into B.C. from China, by simply insisting the miners needed to speak Mandarin. Will the workers this time be required to speak Spanish, Korean, Greek or Polish?" Times Colonist, A13

*** Alberta has potential to be agriculture powerhouse**
Alberta has the potential to be an agriculture and energy "super powerhouse," depending largely on its ability to find the right people for the jobs available, says an industry representative based in Calgary. "The potential is there and I don't think anybody denies that. But if you don't have the boots on the ground to do the work, it ain't gonna happen," said beef sector representative Casey Vander Ploeg, in Red Deer on Thursday for the Alberta Cattle Industry Conference. Like others gathered for the conference, Vander Ploeg was excited to hear earlier that day that the federal government has launched a review of the temporary foreign worker program with a view to easing the persistent labour crisis facing farmers and food processors. "The announcement that the Liberal government made in Ottawa, in my opinion, that is a very positive development," said Vander Ploeg, policy research manager for the Calgary-based National Cattle Feeders Association. "Historically, agriculture has been the gateway of immigration into Canada. Alberta can be an energy and agricultural super powerhouse." But the industry needs access to skilled workers who can fill the many highly specialized tasks involved on the farms and in the processing plants. Feedlot operator John Lawton, based in Niton Junction with additional operations in Southern Alberta, said that while finding workers is hard enough for the farms, the crisis is especially troublesome at processing plants. Alberta's two major beef processors, based in High River and Brooks, are unable to run at full capacity because they don't have enough people to fill their shifts. Red Deer Advocate, C3

CYBER SECURITY / CYBERSÉCURITÉ

*** Facebook, Twitter, Google express public support in Apple's fight with feds**
Leading tech companies are rallying behind Apple — some belatedly — in its fight against a court order requiring the company to help investigators break into an iPhone used by one of the San Bernardino

mass shooters. A U.S. magistrate ordered Apple to produce software that would give investigators access to the iPhone at issue. Apple has until next Tuesday to challenge that ruling, setting the stage for a legal clash that could determine whether tech companies or government authorities get the final say on just how secure devices like smartphones can be. Associated Press (CBC News)

*** Has Apple secretly leaked your private data to the government?**
An opinion piece states "Apple CEO Tim Cook's now widely shared "Message to our Customers" is an attempt to make the best PR move in a bad situation. Were Apple to comply with the FBI's request to access information locked on a suspected San Bernardino shooter's phone, it probably wouldn't be the first time that the government has deputized Apple to breach its customers' privacy. According to documents revealed by Edward Snowden in 2013, Apple was one of the participants in the U.S. National Security Agency's PRISM program, giving authorities access to its customers' information including their emails, messages and photos. Apple for its part has denied any such involvement, but given the secretive nature of the United States Foreign Intelligence Surveillance Court (FISA Court), Apple and other technology companies would be prohibited to publicly acknowledge their involvement in such programs. Hence the frustrating Catch-22 — is Apple really a champion of privacy rights? Or is all this bluster just an act to score PR points with their customers, despite the fact that legislative conditions already exist to force Apple to co-operate in secret?" Toronto Star; Toronto Sun

*** Apple likely to invoke free-speech rights in encryption fight**
Apple Inc will likely seek to invoke the United States' protections of free speech as one of its key legal arguments in trying to block an order to help unlock the encrypted iPhone of one of the San Bernardino shooters, lawyers with expertise in the subject said this week. The company on Thursday was granted three additional days by the court to file a response to the order. Apple will now have until Feb. 26 to send a reply, a person familiar with matter told Reuters. The tech giant and the Obama administration are on track for a major collision over computer security and encryption after a federal magistrate judge in Los Angeles handed down an order on Tuesday requiring Apple to provide specific software and technical assistance to investigators. Reuters

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Bullying, nudity alleged at RCMP training school**
The RCMP is scrambling to defuse a public relations bomb over an investigation into bullying, sexual misbehaviour and nudity among employees at the Canadian Police College in Ottawa, according to CBC News. Top brass have ordered new code of conduct investigations and a review of previous inquiries and have suspended two employees with pay after receiving what they say is new information about alleged harassment at the school, CBC reported Thursday. Yet CBC News said it spoke to four complainants - all former employees of the RCMP's explosives training unit at the school - who say the matter is common knowledge within the force. The men say they tried to share accounts of other disturbing behaviour, including unwanted sexual touching, rampant nudity, and bullying at the school in 2014 and 2015, but RCMP investigators didn't want to know. According to the report, one of the officers suspended Wednesday is RCMP Staff Sgt. Bruno Solesme, who was the unit manager. Solesme had already been disciplined for nudity in the workplace, specifically one instance where he was seen lying naked across the desk of a colleague. He was suspended with pay for several months in 2014 before an internal adjudication board formally issued a reprimand and docked him seven days' pay. The other man reportedly suspended this week is a civilian member of the RCMP and a former Canadian Forces Joint Task Force member, Marco Calandrini. He was docked five days' pay for walking naked around the office on a regular basis. Calandrini was docked another 15 days' pay after the force investigated allegations he had inappropriately touched a former colleague. CBC News said that Solesme and Calandrini were not available to respond to the story. The alleged bullying and harassment is at odds with the priority RCMP Commissioner Bob Paulson has put on addressing allegations of sexual harassment inside the force, as well as promised reforms to its disciplinary system. Late last week, one of those former employees wrote to Paulson for an explanation. Paulson passed the file to Deputy Commissioner Peter Henschel, who is responsible for the college. Ottawa Citizen

*** Le présumé meurtrier sortait de prison**

Le présumé meurtrier de Christine MacNeil, cette femme abattue dans une chambre de l'hôtel Four Points de Gatineau, en octobre dernier, venait de sortir du pénitencier lorsque le crime s'est produit. (…) Un agent de la compagnie de sécurité Garda avait appelé la police de Gatineau pour l'avertir qu'un homme tirait dans la rivière des Outaouais en compagnie d'amis. Les forces de l'ordre ont saisi l'arme et accusé l'homme de quatre chefs reliés aux armes à feu. Le P38 a été confisqué. Le 5 mars 2013, Blake Dooley a plaidé coupable à un seul de ces chefs, soit la possession d'une arme à feu à utilisation restreinte, chargée. La Couronne a demandé un arrêt des procédures sur les trois autres chefs. Le tribunal a alors prononcé une interdiction à vie de posséder des armes à feu. L'inspecteur-chef Leduc n'a révélé que peu de détails sur ce qui pouvait bien relier la victime à son tueur allégué. « L'enquête intensive des derniers mois a démontré que la victime était bel et bien ciblée par son meurtrier », a mentionné le policier. Les autorités croient qu'il est possible que d'autres personnes soient arrêtées dans cette affaire. Outre la police d'Ottawa, la Sûreté du Québec et la Gendarmerie royale du Canada ont aussi collaboré avec le SPVG dans cette affaire. Le Droit, 5

*** Norquay man wanted by police on warrants**

More details have emerged about why RCMP are looking for Wayne M. Babiuk of Norquay. On Tuesday, the RCMP announced it was seeking the public's assistance in locating the man because he was wanted on several Criminal Code warrants, but the force would say little else. Earlier that day Kamsack RCMP officers had received a call about a break and enter at a rural residence northwest of Swan Plain. The RCMP said on Thursday that the home and a vehicle were damaged by a baseball bat and threats were made to the homeowners and the police. Two firearms were also taken from the residence. The victims were not harmed but are known to Babiuk. The 41-year-old is charged with one count of the dangerous operation of a motor vehicle, one count of mischief, two counts of uttering death threats, one count of break and entering, one count of possessing a firearm and six counts of breach of an undertaking. A warrant is out for his arrest and RCMP say not to approach him because he is possibly armed and considered dangerous. Postmedia Network, A6

*** Lourdes amendes pour deux Sherbrookoises**

Deux Sherbrookoises devront acquitter de fortes sommes pour avoir participé à du trafic de tabac illégal. Une amende de 172 410 $ est imposée à Karine Baillargeon. Cette condamnation, prononcée par le juge de paix magistrat Sylvie Desmeules, est le résultat d'une opération effectuée par la GRC, le 30 novembre 2010. Les policiers avaient investi la résidence de Baillargeon et y ont saisi 45 400 cigarettes de contrebande. Pour sa part, Danika Baillargeon a aussi 12 mois pour verser 186 500 $ d'amende à la suite d'une condamnation prononcée par la même juge. Le même jour en 2010, les policiers fédéraux avaient effectué une perquisition visant la résidence de Baillargeon. Ils y ont saisi 404 cigarettes de contrebande. Dans les deux cas, la cour a ordonné la confiscation et la destruction du tabac saisi, annonce un communiqué de presse de Revenu Québec. Les deux Sherbrookoises font partie de personnes reconnues coupables d'infractions liées à la contrebande de tabac. Ces huit personnes ont été condamnées à payer des amendes totalisant plus de 1 073 000 $, dans des délais variant de 2 à 24 mois. De plus, l'une d'elles, Charles Patenaude de Saint-Césaire, a été condamnée à purger une peine d'emprisonnement. «, note le ministère. «Ces personnes n'étaient pas inscrites aux fichiers de Revenu Québec et n'étaient titulaires d'aucun des permis exigés par la Loi pour exercer des activités commerciales liées aux produits du tabac», note le ministère. La Tribune, 29

OFFICIERS DANS L'EMBARRAS POUR INCONDUITE SEXUELLE

Une enquête interne de la GRC a été ouverte en lien avec des allégations d'inconduite sexuelle, d'intimidation et de nudité au Collège canadien de police (CCP), à Ottawa, a rapporté la CBC hier. Les faits se seraient déroulés à l'unité de formation aux explosifs du CCP, un service de police national de la GRC. Le sergent Bruno Solesme et Marco Calandrini, un employé civil de la GRC et ancien de l'armée, ont été suspendus. Responsable de l'unité, le sergent aurait déjà été sanctionné dans le passé pour nudité sur son lieu de travail. Il se serait allongé nu sur le bureau d'un collègue. De plus, il aurait intimidé des anciens employés, les menaçant de ne pas renouveler leur contrat. L'autre employé aurait aussi été déjà suspendu parce qu'il se promenait nu dans le bureau régulièrement. Calandrini aurait aussi été suspendu pendant 15 jours parce qu'il était accusé d'avoir touché un ancien collègue. Une loi coûteuse et inutile. Journal de Montreal, A3

*** Police chief hails new PTSD law**
Waterloo Regional Police Chief Bryan Larkin applauds new provincial legislation making it quicker and easier for first responders with post-traumatic stress disorder to access benefits and treatment. "We have normal people doing an abnormal role in society," said Larkin, referring to the danger police officers face each day. The law introduced Thursday would create a presumption that PTSD in first responders is work-related, removing the need for them to prove a causal link to the Workplace Safety and Insurance Board. It would cover police officers, firefighters, paramedics, workers in correctional institutions, dispatchers of police, firefighting and ambulance services, and First Nations emergency response teams. Canadian Press (Waterloo Region Record, B1); Ottawa Citizen

*** Police critical of Apple technology**
The top-notch encryption technology on Apple mobile phones is now routinely hindering criminal investigations, police and prosecutors in New York City said Thursday. They predict the problem could worsen as more criminals figure out how effective the devices are at keeping secrets. Manhattan district attorney Cyrus R. Vance Jr. told a news conference that his cybercrime lab has 175 Apple devices that investigators can't access because of encryption embedded in the company's latest operating systems. "They're warrant-proof," he said. Associated Press (Waterloo Region Record, A6)

Horse owner charged with cruelty
A 65-year-old Fort McMurray man is charged with causing injury to animals after three horses were found dead and 82 others were found distressed on two of his northern Alberta properties. The RCMP's livestock investigations unit and the Alberta Society for the Prevention of Cruelty to Animals visited a property in the Wandering River area Feb. 3 where they found three horse carcasses and 52 horses in poor condition. Two horses and two donkeys were confined to corrals where there was not enough food or water, RCMP said. After visiting the man's second property, they found 20 more horses in distress. Two days later, police visited the properties again with a search warrant and a veterinarian determined all of the horses were in distress. Once police completed their searches, a total of 82 horses and two donkeys were seized and relocated to a facility for examination and treatment, police said. Gary Herbert Sparshu has been arrested and charged with causing injury to animals and breach of a court order. He has been remanded in custody and will appear in provincial court in Boyle on Tuesday. Calgary Sun, A12 (Edmonton Sun, Edmonton Journal); National Post, A6

Spray of bullets wounds man in taxi
A 40-year-old man was treated in hospital for a minor leg injury after a taxi was sprayed with bullets early Thursday in Surrey. Surrey RCMP Staff-Sgt. Blair McColl said the man was hit in the Surrey Metro cab shortly after 5 a.m. in the area of 109th Avenue and 143rd A Street. Numerous 911 calls were received from the area, he said, as well as a call from a man saying he'd been shot in the leg. The taxi driver was unharmed, but one of the windows was blown out as the cab was hit by multiple gunshots. McColl said the victim went to Surrey Memorial Hospital, where he was treated for a graze to his leg. "The bullet didn't penetrate the leg, and he has since been released." Moonyem Mohammad, the general manager of Surrey Metro Taxi, said the driver is in shock, but otherwise doing OK at home. He said the car has been impounded and the driver, who wishes to remain anonymous, will be off work for the next two or three days. "If he needs more time we can arrange that if he wants," Mohammad said. Postmedia Network (Province, A4, Red Deer Advocate, Times Colonist)

*** Le stratagème pyramidal en vogue dans la Péninsule est illégal, selon un expert**
Le stratagème pyramidal qui a pris de l'ampleur dans la Péninsule acadienne ces derniers mois est illégal, selon le conseiller juridique principal de l'autorité réglementaire provinciale. Comme le rapportait l'Acadie Nouvelle plus tôt cette semaine, un réseau pyramidal ciblant les femmes et présenté comme un «groupe d'entraide» ou un «groupe de don» a étendu ses tentacules dans le nord-est du Nouveau-Brunswick ces derniers temps. (…) Des arguments rejetés du revers de la main. D'après ce que l'on peut lire dans des documents de recrutement destiné aux éventuelles recrues et un courriel envoyé récemment aux femmes qui participent déjà au stratagème, les administrateurs (dont on ne connaît pas l'identité) tentent de se faire rassurants. Ils allèguent que leur combine n'est pas illégale parce qu'il s'agit d'un «groupe de dons» et que des chèques cadeaux sont échangés lorsque des recrues se joignent à un groupe de participants. Ils affirment aussi qu'il ne s'agit pas d'une pyramide parce que personne ne

demeure au sommet de la structure et que les participants sont regroupés en «nuages» de 15 personnes. Mais selon Me Brian Maude, il ne faut pas être dupe. «Ici, c'est bien de dire "non, non, non, c'est un cercle de dons, c'est un cercle de cadeaux." Moi, je peux appeler un cheval un chameau sans bosse. C'est toujours un cheval. L'appeler "nuage" au lieu de pyramide, c'est essentiellement changer le descriptif, mais c'est toujours la même chose.» Un autre argument avancé par les promoteurs du stratagème pyramidal actif dans le nord-est de la province est qu'un groupe semblable a collaboré avec la GRC à Calgary pour s'assurer que leurs activités sont blanches comme neige. Me Brian Maude accueille cela avec beaucoup de scepticisme. «Avez-vous déjà entendu parler d'un système d'investissement qui a travaillé avec la police pour assurer sa légalité?» L'Acadie Nouvelle est d'ailleurs en contact avec la GRC pour savoir si cette allégation faite par les administrateurs du réseau pyramidal est véridique. Nous attendons de leurs nouvelles. Il semble cependant peu probable que ce soit le cas. Un réseau pyramidal identique a fait l'objet d'une sérieuse mise en garde de la GRC albertaine en 2008. Acadie Nouvelle, 4/FRONT

*** Targeted shooting in Kamloops sends one man to hospital**
One man has been sent to hospital for surgery, after a shooting in Kamloops on Thursday night. Kamloops RCMP say the shooting happened in a parking lot near the intersection of Versatile Drive and Copperhead Drive. "This was a targeted shooting and not a random event," Staff Sgt. Edward Preto said in a statement. The victim is a 32-year-old man who is well-known to police. CBC News; CFJC

*** Grand Prairie RCMP investigate attempted child luring incident**
RCMP are investigating an incident where two women in a black van allegedly approached a youth in the Grande Prairie area. The incident allegedly occurred on 71 Avenue near 99 Street at about 3:45 p.m. on February 17. Police said a black mini-van pulled into a driveway and a young woman got out of the driver's seat - she allegedly offered the child a ride home. According to RCMP, when the child declined a second female opened the passenger side door and allegedly told her to get in the van. The girl declined a second time and continued walking until she could safely call her mother. CTV News

Une loi coûteuse et inutile
Un article d'opinion déclare "La tuerie de Polytechnique en 1989 et la fusillade au Collège Dawson en 2006 ont soulevé un débat sur les armes à feu entre les pros et les contre qui, dans certains cas, obnubile le simple raisonnement. Soulignons aussi que les événements sanglants aux États-Unis alimentent les arguments des pros qui continuent de penser que notre système d'acquisition des armes à feu est semblable et que n'importe qui au Québec et au Canada peut acheter une arme à feu sans aucun contrôle. Cette hystérie autour des armes à feu permet aux politiciens d'en faire un enjeu électoral auprès d'une partie de population souvent ignorante des règlements actuels de contrôle des armes à feu et qui ne cesse de réclamer une loi sur l'enregistrement des armes. (...) Une fois ce cours terminé, je peux si je le souhaite acquérir une arme à feu selon des conditions déterminées par la loi des armes à feu canadienne. Et voyons maintenant les exigences du permis d'acquisition. D'abord avoir 18 ans. En plus des renseignements réguliers, nom, adresse, etc., vous devez fournir vos antécédents personnels et ceux de votre partenaire conjugal en relation avec le Code criminel canadien au cours des cinq années précédentes à votre demande. Une réponse négative à l'une de ces questions ne vous permettra pas d'acquérir une arme à feu. De plus, vous devez obtenir la signature d'autorisation de votre conjoint ainsi que celle de deux répondants qui vous connaissent depuis au moins trois ans. Vous devez maintenant envoyer votre demande à la Gendarmerie royale du Canada qui doit vérifier la véracité des renseignements fournis et continuer l'enquête avant de vous délivrer le document demandé ce qui prendra au moins six mois. Votre dossier personnel doit donc être vierge. De plus, ce dossier est enregistré et toute personne de loi (policiers ou gendarmes, etc.) peut y avoir accès lorsque nécessaire. La sûreté du Québec n'a donc pas besoin d'un nouveau système pour savoir qu'un individu possède une arme à feu. Ils n'ont qu'à accéder au dossier d'acquisition." Le Soleil, 23

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Dorchester prison staff find $38K drug stash
Dorchester Penitentiary staff made a major discovery earlier this week when a package containing cocaine and other contraband was found at the prison. "It was a substantial amount," says spokesman Daniel Melanson. "It creates a network among inmates for buying and selling and puts everyone at risk." Correctional Service of Canada staff discovered a package around 10 a.m. on Tuesday, near the perimeter of the medium-security unit. The package was seized and found to contain marijuana, hashish, hashish oil, cocaine, tobacco, pills and nicotine patches. The estimated institutional value of the contraband is $38,000. Melanson said the matter is being investigated to determine how the package got there. CSC has a tip line for all federal institutions where any information relating to drug use or trafficking that may threaten the safety and security of visitors, inmates and staff can be reported. Times & Transcript, A6

Fewer inmates in solitary makes the case for legal reforms
An opinion piece states, “There has been a startling development in the solitary confinement of prisoners in our federal system. For many years, penitentiaries consistently held about 800 prisoners in segregation on any given day. However, over the past year, the Correctional Service of Canada has cut the number of segregated prisoners in half. According to data collected by the CSC, and obtained pursuant to an access-to-information request, the number of prisoners held in cells for up to 23 hours a day is now 405. Questions that emerge are why the change took so long to come about and whether we can expect it to last. This change, while positive, reveals a dark truth. The CSC has long asserted that it relies on segregation only when absolutely necessary, such that any reform would threaten prison security. But if the correctional service can take half of its segregated population out of isolation, it seems clear that it could have made this decision earlier. It seems that the change required only greater incentives within the prison service. The only plausible explanation for this development is that the CSC is responding to intense public pressure, litigation and criticism, including by The Globe and Mail. There has been no change in the law that could explain the reduction. The "administrative segregation" provisions in the Corrections and Conditional Release Act have not been significantly amended since their enactment in 1992. Although the law provides that administrative segregation can be used only as a measure of last resort, it has always lacked concrete rules of enforcement. For example, the law does not include a strict limit on the number of days that a prisoner can be isolated. The result is that prison officials have long enjoyed an enormous amount of discretion.” Globe and Mail, A13

«Ce qui s'est passé en cour m'a fait réaliser le côté inhumain de mes gestes»
Kaven Sirois, l'un des deux auteurs du triple meurtre de la rue Sicard à Trois-Rivières, restera à l'Institut Philippe-Pinel jusqu'en 2020 et sera ensuite transféré dans un pénitencier jusqu'à la fin de sa sentence. Comme prévu jeudi, le procureur de la Couronne, Me Hippolite Brin, et les avocats de la défense, Me David Guévin et Me Matthieu Poliquin, ont suggéré de façon commune le lieu de garde à privilégier pour le jeune homme, maintenant âgé de 18 ans. On sait que ce dernier a été condamné à une peine de prison à vie sans possibilité de libération conditionnelle avant 10 ans pour avoir tué de sang froid trois jeunes le 11 février 2014 et comploté pour tuer d'autres personnes. Déjà informé de cette recommandation, le juge Bruno Langelier l'a entérinée sur le banc, précisant du même coup qu'il envisageait déjà cette possibilité très sérieusement. Selon lui, il est essentiel de garder à l'esprit l'importance de la réhabilitation pour cet adolescent devenu un jeune adulte. (…)Par ailleurs, les procédures pour permission d'en appeler de la peine pour adultes imposée à Kaven Sirois vont se poursuivre. C'est que la défense voudrait faire renverser la décision du juge Langelier afin qu'il soit plutôt condamné à une peine spécifique, soit six ans de garde fermée et quatre ans de suivi externe. «Kaven appartiendra au Service correctionnel du Canada pour toute sa vie. Il s'agit d'un poids lourd à porter. Et c'est pourquoi nous allons en appel», a précisé son avocat Me Guévin. Des audiences sont prévues devant la Cour d'appel le 6 mai. Le Nouvelliste, 3, Journal de Montréal (Journal de Québec)

Lawyer concedes client is dangerous offender
The lawyer for 47-year-old David A. Wilson, a Kingston man soon to be sentenced for a break-in and sexual assault here in March 2014, concedes that his client meets the definition of a dangerous offender.

But defence lawyer Dan Scully is asking Superior Court Justice Gary Tranmer not to sentence his client to prison indefinitely. He told the judge "the Crown has met its burden (of proof)" and "it's open to the court to find that Mr. Wilson is a dangerous offender." That said, however, Scully is urging the judge to find that there's a reasonable expectation Wilson's risk can be managed in the community and to sentence him to seven years in prison followed by a 10-year long-term supervision order. Under the Criminal Code of Canada, a dangerous offender designation presumptively calls for indeterminate - or indefinite - sentencing, with release possible only through the Parole Board of Canada, which, if granted, means parole supervision for life. (...)Scully noted his client was granted early release on his 2010 sentence. Scully told Justice Tranmer that Wilson spent the final eight months of his second penitentiary sentence living at the Henry Traill Community Correctional Centre, a halfway house for federal offenders operated under the aegis of Correctional Service Canada, on the property of Collins Bay Penitentiary. He was there, Scully said, because the Parole Board of Canada imposed a residency requirement on his release. But Scully suggested it showed an increased level of confidence in his client. Kingston Whig-Standard, A1

* **Pushing for cows in pen**

It is easy to pick out the short-timers from the lifers on Jeff Peters' beef and pork farm. The 14 black and white Holstein dairy cows stand in sharp contrast to his regular herd of chocolate-brown Limousin beef cattle in the open winter barns. The dairy cows are excons of a sort. Peters is one of eight Ontario farmers who, for more than five years, have looked after the remnants of the dairy herd that once lived on a farm at the Collins Bay prison complex in Kingston. For most of that time, the farmers, hundreds of residents and a few celebrities have been fighting to reopen the farm and send the cows home. Years of weekly protests and fundraisers had led nowhere. But hopes have blossomed with the October defeat of the Conservative government, which closed the farm. Now, the new Liberal MP from the Kingston area is campaigning to bring farming back to the prison. There is a growing feeling among protesters their efforts will finally be rewarded. Farms have formed part of the Collins Bay Institution since it opened in 1930. In 1962, a farm annex, later named the Frontenac Institution. Prisoners swept stalls, and fed the cows and chickens. Many stayed up all night to help birth calves. In the farm's final years, an inmaterun operation provided milk and eggs for all the federal prisons in Ontario and Quebec, and some provincial jails. Why the Conservatives closed it and five other prison farms across Canada in 2010 was never clear. The move followed other steps that seemed intended to eliminate any notion life in prison was soft. The minister responsible for prisons at the time, Vic Toews, called the farm programs ineffective at rehabilitating prisoners. "Less than one per cent learned any skills that were relevant," he said. (...)Meanwhile, the Monday protests continue at the Collins Bay entrance. National Post, A7

* **Murderer waives parole hearing**

A man convicted of murdering two young girls, their parents and grandparents more than three decades ago in B.C. has waived his right to a parole hearing, and it will be 2021 before he can apply again. David Ennis, who has changed his name from David Shearing since the August 1982 murders, was due for a parole hearing in August. A spokeswoman for the Johnson and Bentley families says relatives of the victims are relieved at the cancellation. Vancouver Sun, A2 (Times Colonist, The Province)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Demand outpaces funding on reserves

Frantic calls for backup that go unanswered, cops wearing worn out bulletproof vests and a pay scale that discourages officers from staying on the job. These are some of the obstacles that plague officers serving in Quebec's remote aboriginal police departments, according to six veteran cops interviewed by the Montreal Gazette. Three of the officers did not want their names published for fear it might affect their future job prospects. Calls for improved working conditions come just days after the shooting death of constable Thierry Leroux - a 26-year-old who was killed last Saturday while patrolling in the Lac Simon First Nation, south of Val-d'Or. Meanwhile, a report released Thursday by the province's ombudsman points to failed crime prevention strategies in the Nunavik region (home to the majority of Quebec's Inuit

population). The document tracks a 239-percent increase in cases before Nunavik's court system over the past decade. It links the spike in crime to a lack of accessible substance abuse treatment and other essential government services. And while the workload for aboriginal police forces is only increasing, their resources can't keep up with the demand - according to senior police sources. (...)In contrast, Montreal's police budget increased by 41 per cent between 2005 and 2015. Though it's hardly scientific to compare a small department with the province's largest municipal police force, budget increases are common in non-Aboriginal communities. Montreal Gazette, A1

*** Sex trafficking at crisis point**
Advocates who work with victims of human trafficking are urging the Ontario government to adopt a private member's bill to take immediate action to address what they call a crisis. "Sex trafficking is a growing and significant issue in Ontario," said Cynthia bland, founder of Voice Found, a survivor-led nonprofit that educates people about commercial sexual exploitation. "The average age when most girls are trafficked into prostitution is 14, and many don't even recognize that they've been trafficked until it's too late." Simone bell of Ottawa, a victim of trafficking, said vulnerable young people need non-judgmental help and understanding. "No child or youth is a prostitute. ... it is human trafficking," said bell. PC women's critic Laurie Scott has a private member's bill that would give police the power to enforce protection orders on behalf of victims. Victims' families, police and Children's aid Societies would be able to apply for a minimum three-year protection order. Canadian Press (Toronto Sun, A16, London Free Press, Ottawa Sun, Hamilton Spectator)

*** Our sexual assault confusion**
An opinion piece states, "'I thought to be assaulted you had to be broken and raped," explained the first complainant in the Ghomeshi trial, when asked why she hadn't come forward sooner with her sexual assault allegations. A great number of Canadians appear to harbour this misconception, and others, about our sexual assault laws. According to two Statistics Canada data sets, there were 21,000 incidents of sexual assault reported to police in 2014, while 633,000 Canadians selfidentified as being victims of sexual assault that same year, either reported or unreported. The reason given by 43 per cent of survey respondents for not reporting an assault was that "Police wouldn't have considered the incident important enough." There may be other reasons why some of these self-identified victims chose not to report. But if we accept these figures as being broadly accurate, they are astonishing. To put them in context, in 2014, roughly 360,000 criminal cases were resolved in Canada's courts. If all 633,000 self-identified victims were to report, the number of sexual assault cases would outnumber all other criminal cases two to one. The high incident and low reporting rates may suggest that many Canadians - both women and men - are ignorant about what constitutes sexual assault in Canada, when to report it, and what level of communication is warranted to ensure sexual relations are consensual." National Post

*** Dites-le en rose : dites non à l'intimidation**
Jusqu'au 24 février, les visiteurs du Carrefour de l'Estrie sont invités à écrire une promesse de gentillesse pour appuyer le mouvement de lutte contre l'intimidation sur un Post-it, qui sera ensuite apposé au mur DITES-LE EN ROSE dans le coin restos du centre commercial. Le mercredi 24 février, les gens sont également invités à porter un chandail rose pour afficher l'importance qu'ils accordent à la sensibilisation et à la prévention face à l'intimidation.L'initiative #24février chandail rose est entre autres appuyée par le Service de police de Sherbrooke (SPS), le Carrefour de l'Estrie et la Fondation Jasmin Roy, qui a pour mission de lutter contre la discrimination, l'intimidation et la violence faites aux jeunes en milieu scolaire.« Comme parents, nous devons être des modèles pour nos enfants. Si nous sommes violents, nos enfants le seront probablement aussi. Si nous sommes stupides sur les réseaux sociaux, ils seront stupides aussi », en affirme le fondateur, l'animateur Jasmin Roy. Selon lui, la communauté doit être organisée et bienveillante pour confronter et lutter contre l'intimidation. Estrie Plus

*** Event highlights injustices faced by indigenous women**
There were several sobering and disturbing facts, thoughts and observations shared at an event at Memorial University Thursday night. The gathering, which included several speakers, was called "Know the Truth: Injustice and Indigenous Women in Canada." Anybody in the audience might very well have learned some general facts about indigenous peoples, but some words spoken by Amelia Reimer, a cultural support worker at the St. John's Native Friendship Centre, were much more powerful than trivia.

"Just this week, actually, I was given two more names of Mi'kmaq women here on the island who went missing a few decades ago. But still no one has ever heard from them and no one knows what happened," Reimer said. Reimer has been attempting to account for all the indigenous women who have gone missing in this province since 1980. It was recently revealed as many as 1,200 indigenous women may have gone missing in Canada since that time, but even that number is thought to be inadequately low by some. The number 4,000 has been emerging lately. The first questions that might come to mind would be why so many indigenous women are going missing, and why the public hasn't heard more about it. The Telegram, A4, VOCM

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Indigenous victims: more than a body count**
Indigenous Affairs Minister Carolyn Bennett recently outlined how she sees the scope of a national inquiry into missing and murdered aboriginal women shaping up. Ms. Bennett believes the fact-finding must also hear the stories of those victims not yet counted. So the official number — set at 1,181 by the RCMP in 2014 — will rise. The tally of the missing and murdered indigenous women and girls has been a moving target for years. From the hundreds first believed to be in RCMP files, the 582 counted by the Native Womens' Association of Canada in 2010, to the 800-plus painstakingly collected by a University of Ottawa PhD candidate. The organizers of the cross-country Walk4Justice say they've gathered upwards of 3,000 stories. Brandon Sun

*** An inquiry that seems to have no start, and no end**
An opinion piece, by Jeffrey Simpson states, "The inquiry into missing and murdered aboriginal women, promised by the Liberal government, is getting wider and wilder Its scope, length, cost and focus keep growing with every new pronouncement by Indigenous Affairs Minister Carolyn Bennett, who has become an echo chamber for the Native Women's Association of Canada, whose every claim the minister seems to endorse. This week, Dr. Bennett insisted that the number of women murdered or missing is "way bigger" than the nearly 1,200 cases the RCMP have investigated and reported on in considerable detail. How does she know this? By talking to aboriginal women's groups and individuals who have been making this claim all along. The cases that the RCMP have investigated occurred from 1980 to 2012 - more than three decades. In addition, the RCMP provided an update for cases in 2013 and 2014. How many did the RCMP miss or were not reported? Who knows? It is impossible to know, especially from 1980 to 2014. But Dr. Bennett is sure it is "way bigger," in which case this inquiry will be engaging in a massive fishing expedition. If the government chooses the vehicle of a public inquiry, then it will stretch on for many years and cost huge amounts of money - to produce outcomes that mostly can be predicted today, including that of the first-year criminology student's understanding that the majority of assaults were committed by men who had intimate or close relations with the victims (that is, aboriginal men); that sociological problems contributed to violent behaviour; that racism infected certain cases; that, in some instances, the police might have been late to the file; and that, of course, non-aboriginal people are largely, if not wholly, responsible for the entire tragedy. Do we need an inquiry to tell us more than these likely, if not obvious, conclusions? The straightforward answer is no, but you have to hand it to the Native Women's Association because it has been persistent and exceptionally media-savvy and has the minister entirely under its spell. Even the Conservative Party, which while in office rejected the idea of an inquiry, has swung around to favour one, such being the carefree ability of opposition parties to take positions devoid of responsibility. Globe and Mail, A13

*** Indigenous women inquiry may backfire**
An editorial states, "The promised inquiry into missing and murdered indigenous women hasn't started yet. But it is already growing in scope. During the election campaign, Liberal Leader Justin Trudeau vowed to authorize a full public inquiry into the roughly 1,200 aboriginal women and girls who, according to the RCMP, went missing or were murdered between 1980 and 2014. The aim, as expressed in the Liberal platform, was to come up with concrete recommendations "to solve these crimes and prevent future ones." But after talking to aboriginal people across Canada, Indigenous Affairs Minister Carolyn

Bennett has announced she wants something more. Specifically, she wants the inquiry to also determine whether the police have lowballed the number of women and girls murdered. She said she now believes there are "way more" than 1,200 victims. She also told reporters that the inquiry should hear evidence from indigenous females who were assaulted but not killed. At one level, casting a broader net could prove useful. There have been public probes into the murder of native women before. The most recent was British Columbia's two-year investigation into women who disappeared around the time of the Robert Pickton pig-farm murders. That Missing Women Commission of Inquiry was dismissed by aboriginal critics as too narrow. Bennett, it seems, is trying to avoid this particular problem. She may, however, be in danger of doing the reverse - of making her government's proposed inquiry too broad. Once started, public inquiries tend to take on a life of their own. At the best of times, they can take years to complete. The Royal Commission on Aboriginal Peoples, for instance, was launched in 1991 on a wave of public goodwill. But by the time it issued its report five years later, public interest in native issues had waned." Waterloo Regional Record, A8

*** Get reliable stats on missing**

An editorial states, "The editorial Indigenous victims: more than a body count (Feb. 18) suggests yet another dangerous initiative contrary to the common good. This national inquiry into missing and murdered aboriginal women and girls, in its own right, will likely be divisive, troublesome and prove nothing within the aboriginal community, and it is doubtful it will be useful or helpful to the country at large. However, the lack of common sense or practical execution of the inquiry, and the lack of truth gathering as represented by the Free Press in its editorial, is a perfect recipe for disaster. Mere talking points by a highly politicized minister, the research by a PhD student, the biased representations made by a cross-country "Walk-4Justice" and the unsubstantiated stories of families simply do not cut the mustard. If the RCMP estimate is not to be believed, which makes little to no sense, the process leading to a number acceptable to the entire country, including the investigation, gathering of irrefutable evidence, verification of the irrefutable evidence and the conclusion as to an acceptable estimate, must be conducted through a process every bit as reputable and respected as a full and open court; for example, a royal commission." Winnipeg Free Press, A8

*** Faire la lumière**

Un article d'opinion déclare, « Depuis la publication d'un rapport de la GRC en 2014, tout le monde croyait qu'environ 1200 femmes autochtones avaient disparu ou été assassinées entre 1980 et 2012. Cette semaine, le portrait s'est noirci. On a soudainement fait état de 4000 victimes. Est-ce vraiment le cas ? Et est-ce la question essentielle ? Que le nombre de victimes soit nettement supérieur à ce qu'a calculé la Gendarmerie royale est fort probable. Pour les ministres fédérales des Affaires autochtones, Carolyn Bennett, et de la Condition féminine, Patty Hajdu, cela ne fait d'ailleurs aucun doute à la suite des consultations qu'elles ont tenues depuis décembre avec des familles des victimes. Plusieurs d'entre elles ont fait état de cas traités comme des suicides ou des accidents et non comme des meurtres. Des cas où la police n'a pas pris l'affaire au sérieux. Des cas où aucune plainte n'a été déposée tant la méfiance à l'endroit des forces de l'ordre et du système judiciaire est grande. Certaines familles sont aussi persuadées que leurs proches n'apparaissent pas sur la liste de la GRC. Mais 4000 victimes ? Ce sont des activistes du groupe Walk 4 Justice qui en sont arrivés à ce nombre après avoir réuni, entre 2008 et 2011, des noms de femmes tuées ou disparues, dont 60 % étaient autochtones, rapportait la CBC cette semaine. Le chiffre a été cité par la présidente de l'Association des femmes autochtones du Canada, Dawn Lavell-Harvard, lors des consultations et repris cette semaine par la ministre Hajdu. » Le Devoir

*** Citizen X: Missing But Remembered**

When federal Indigenous Affairs minister Carolyn Bennett and Justice Minister Jody Wilson-Raybould stopped in Saskatchewan for phase one of the national inquiry into missing and murdered indigenous women, they mentioned Darlene Rose Okemaysim-Sicotte by name. She's the co-chair of Iskwewuk E-wichiwitochik (Cree for Women Walking Together), a grassroots organization which supports the families and survivors of the missing or murdered women in Saskatchewan. Community support has always been central to Okemaysim-Sicotte. She grew up on the Beardy's and Okemasis Willow Cree First Nation as one of 14 children. She says they were a big, happy, family, but they always faced poverty. But neighbours helped each other when they could, which sparked her interest in community involvement.

Okemaysim-Sicotte continued her community work at the University of Saskatchewan, and later while working in the Department of Native Studies (now Indigenous Studies). In 2005, she gathered with around 80 other people to find a way to tackle the unaddressed issue of missing and murdered indigenous women. That was the beginning of Iskwewuk E-wichiwitochik. I sat down with Okemaysim-Sicotte at her day job at the Gordon Tootoosis Nikaniwin Theatre to see what the proposed inquiry means to someone on the front lines. Planet S (2016-02-16)

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

Ottawa to restore refugee benefits
Starting in April, Ottawa will fully restore health-care coverage for all refugees and asylum claimants to pre-2012 levels, before cuts were made by the previous Tory government. In a surprise twist, the Liberal government said it will also expand the Interim Federal Health Program by including coverage for refugees designated for resettlement to Canada before they arrive - a plan that was not part of its election pledge. By April 2017, these selected overseas refugees waiting to come here will receive coverage for their immigration medical exam, pre-departure vaccinations, services to manage disease outbreaks in refugee camps and medical supports during travel to Canada. Currently, the health program for refugees has a $51-million annual budget and the new measures will cost an additional $12.5 million in expenditures per annum, Immigration Minister John McCallum said on Thursday. "Canadians from many walks of life, from premiers to front-line health-care professionals to Canadians who privately sponsor refugees, spoke with one voice in rejecting the changes made to the Interim Federal Health Program in 2012. We have listened, and coverage will be restored," he said. "However, that expenditure is still below the amount that has already been budgeted of $51 million per year, so there will be zero net addition in the fiscal framework. All of these expenditures will be within the existing budget." Toronto Star, A1; Globe and Mail, A3; * Canadian Press (Red Deer Advocate, A6, Cape Breton Post, Guardian, times and Transcripts, Telegraph-Journal, StarPhoenix, Windsor Star, Vancouver Sun, Montreal Gazette. Province, Leader-Post, Waterloo Region Record, Ottawa Citizen, Calgary Herald, Edmonton Journal, Hamilton Spectator, London Free Press); * La Presse, 12

25,000 refugees: enough?
More than 70% of Canadians don't support taking in more than 25,000 Syrian refugees, according to a new poll from the Angus Reid Institute. About two in five respondents (42%) think Canada should stop taking in Syrian refugees immediately. As of Tuesday, more than 21,000 refugees had arrived in Canada, according to the government's website. The government is working to meet its target of 25,000 Syrian refugees by the end of February. Immigration Minister John McCallum recently promised the Liberals would exceed their original commitment and accept between 35,000 and 50,000 Syrian refugees by the end of 2016. The Angus Reid poll suggests this is at odds with what the majority of Canadians want. Support for exceeding the 25,000 benchmark is lowest in the Prairies and Quebec, where less than a quarter of respondents were in favour, and tops out in B.C., where roughly two in five respondents were in favour. B.C. was the province with the highest overall support for the refugee resettlement plan. The poll results come just days after a Calgary school was vandalized with the message "Syrians Go Home and Die." That incident is one of several across the country that suggest brewing anti-refugee sentiments. McCallum has said the potential for negative attitudes towards the arriving refugees. "It's a delicate balance," he said at a January press conference in Ottawa. "We want to welcome all of these refugees with open hearts and with love the way Canadians have, but at the same time we are mindful that we don't want to offend Canadians who have themselves been waiting for a long time for social housing and things of that nature." Winnipeg Sun, A17 (Toronto Sun, Ottawa Sun, Edmonton Sun, Calgary Sun, National Post, Cornwall Standard Freeholder, Sault Star, CNews); * Metro News

*** Avalanche of refugees about to hit B.C.**
British Columbia will receive 1,100 Syrian refugees in the next 10 days, effectively doubling the number already in the province. It will be the largest influx of government-assisted refugees to British Columbia, according to Chris Friesen, settlement services director with the Immigrant Services Society of B.C. Almost half the arrivals will be moved outside Metro Vancouver, which is unprecedented for government-assisted refugees in B.C., because Metro has been the only part of the province with the necessary

supports in place. About 240 will go to Victoria, designated last week as an alternative arrival city for refugees, and another 160 to Abbotsford, Friesen said. About 30 each will go to Nanaimo, Prince George, Kelowna and Vernon, he added. Friesen and other Immigrant Services Society staff will be on the road early next week, training settlement workers in those cities to deal with the coming arrivals. (...)The Abbotsford Community Services Society began planning for the arrival of Syrian refugees in October, said Manpreet Grewal, the society's director of multicultural and immigrant services. They had expected to assist privately sponsored refugees being brought to Abbotsford by many church groups. However, the governmentassisted refugees, due to start arriving Monday, pose an additional challenge because they don't have the supports of a community sponsoring group. Housing is the biggest issue, Grewal said. The Syrian families tend to be large, and the government support rates aren't enough to rent accommodation large enough to house them, especially in pricey Metro Vancouver. Vancouver Sun, A1/Front

*** Newcomers make schools busy places**

The recent arrival of close to 700 Syrian refugees has some Manitobans worried about the impact they will have on resources and services. A Winnipeg teacher who has worked with newcomer kids for more than a decade in the province's most diverse neighbourhood has some advice. "Don't freak out." Anita Riedl, an English as an additional language teacher at General Wolfe School in Winnipeg's West End, has seen the EAL program at the school double in size with the resettlement of families from around the world. "The kids just want to learn," she said. In the heart of the most diverse neighbourhood in Manitoba, staff and students have worked to make the school "newcomer-friendly." Winnipeg Free Press, A4

*** Syrian and Indochinese Refugee Movements**

He arrival of Syrian refugees fits within the longstanding Canadian tradition of providing solace and protection to the oppressed around the world who are directly threatened by political events beyond their control. That tradition began with the post-World War II movement of displaced persons, although there had been earlier informal movements of people to Canada in search not only of a better life, but also safety. The Hungarians, Czechoslovaks, Ugandan Asians, Indochinese and Kosovars — these are just a few of the many communities who have found refuge in Canada. As we reach the midpoint of the movement of Syrian refugees to Canada, it becomes possible to draw some comparisons with past resettlement initiatives. New American Media

*** Des réfugiés syriens au Nouveau-Brunswick ciblés par des fraudeurs**

Une famille de réfugiés syriens établie à Saint-Jean, au Nouveau-Brunswick, a perdu 400$ en tombant dans une arnaque téléphonique. Une personne s'exprimant en arabe a communiqué avec la famille, lundi soir. La personne a proposé à la famille d'acheter des DVD de cours d'anglais pour les enfants. La famille n'avait qu'à fournir quelques renseignements bancaires, a déclaré le fraudeur. Lorsque l'interprète qui aide la famille a compris ce qui se passait, les Syriens avaient déjà perdu des centaines de dollars. La directrice du YMCA de Saint-Jean, Shilo Boucher, qui aide la famille en question et d'autres réfugiés syriens, explique que la famille est très heureuse d'être à Saint-Jean, au Canada, et que la situation est décevante. Le YMCA distribue maintenant un dépliant rédigé en arabe afin de prévenir les autres réfugiés des risques associés à la divulgation de renseignements personnels au téléphone. Radio-Canada

*** Syrian refugees: New arrivals struggle to find work**

Ahmad Abu Nokta reaches into his breast pocket and pulls out a business card with his name printed against a bright blue-green background. Underneath, he lists his job titles-'art, paints and decorator.' The same message is printed in Arabic. The 54-year-old Syrian artist and painter fled the southwestern city of Daraa with his wife and four children three years ago. "My house got bombed," he said, through a translator. "My kids are young. I was afraid for my family. We ran away from the war." The family went to neighbouring Jordan, where they lived in a refugee camp for the next three years. Then came a chance to start over when a new Canadian government pledged to house thousands of Syrian refugees in cities across the country. CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Culture of presenteeism' blamed as Ottawans travel to work in snowstorm**
During Tuesday's record-breaking snowstorm in Ottawa, thousands of people braved the weather and went to work despite the city's suggestion that employees stay home. That fact doesn't surprise Robyn Bews."I think there's an incredible culture of presenteeism that permeates most organizations still, but particularly, probably, federal government," said Bews, the Calgary-based executive director of WORKshift, on CBC Ottawa's *All In A Day* Thursday afternoon. "This is about valuing seeing employees in the office ... organizations that still feel like they need to see their employees physically in the office are a little bit antiquated." Mass transit came to a near standstill Tuesday after the federal government decided at around 1 p.m., without telling OC Transpo, to let thousands of public servants go home early. Keith Egli, chair of the city's transportation committee, told CBC Ottawa on Wednesday that if the workers left waiting at bus stops were instead working from home, the commute wouldn't have been so cumbersome. "We've already entered into some discussions with them around what happened [Tuesday] and how it could've been handled better," said Egli. CBC News

OTHER / AUTRE

*** Liberals rule out cutting military manpower**
Defence Minister Harjit Sajjan has ruled out cutting the size of the Canadian military, despite the country's bleak economic and fiscal picture. In fact, Sajjan says he eventually wants to see the force grow, but for now the Liberals will concentrate on filling the ranks to the existing approved levels of 68,000 full-time and 27,000 part-time soldiers. A recent federal report from last year's budget shows military reserves are running at roughly 20,000 paid members - about 19 per cent short of full strength. The numbers are only slightly better for the regular forces with roughly 66,000 full-time members in uniform. Sajjan says recruiting has slowed over the last few years and he wants to see measures stepped up so the country always has an agile, optimal force. National Defence is the largest single discretionary item in the federal budget and previous governments - Liberal and Conservative - have often used military cuts as a way to balance the books. Finance Minister Bill Morneau and Prime Minister Justin Trudeau have both indicated that the Liberal promise to balance the budget over four years has morphed into returning to black ink over the long-term. Canadian Press (Chronicle Herald, A6, Winnipeg Free Press)

*** Une pétition réclame la citoyenneté honorifique pour Raif Badawi**
Le député de Sherbrooke Pierre-Luc Dusseault donne son appui à une pétition électronique lancée par Ensaf Haidar, épouse de Raif Badawi, demandant au gouvernement canadien d'accorder la citoyenneté honorifique au blogueur saoudien. M. Dusseault dit vouloir ajouter de la pression sur l'Arabie Saoudite et demander au gouvernement du Canada de faire preuve de leadership en matière de droits de la personne. «M. Badawi est un homme de grandes convictions. Nous devons honorer les efforts, le courage et la détermination de cet homme», écrit-il dans un communiqué de presse. «Il purge aujourd'hui encore, et depuis beaucoup trop longtemps, cette sentence injustifiée et barbare.» Rappelons que Raif Badawi, dont l'épouse et les enfants vivent à Sherbrooke, a été condamné à la prison et aux coups de fouet pour avoir tenu des propos trop libéraux au goût des autorités saoudiennes. Il s'est vu décerner, pour son dévouement dans la défense des droits de la personne, le prix Sakharov par le Parlement européen en 2015, en plus d'avoir été finaliste pour le prix Nobel de la paix. La Presse Canadienne (La Tribune, 4)

*** PTSD bill on table**
Ontario's first responders diagnosed with post-traumatic stress disorder will automatically qualify for WSIB benefits under legislation introduced Thursday by Labour Minister Kevin Flynn. "If passed by the house, this legislation is going to provide a sense of security to our first responders," Flynn said. "That claim process can be very evidence-based and it can be very onerous for somebody that's undergoing the symptoms of PTSD." The bill would require the WSIB to treat PTSD in first responders, such as police and paramedics, as a workrelated illness. NDP MPP Cheri DiNovo, who has introduced four private member's bills on PTSD in first responders, said the legislation appears to address the concerns she has

been raising for eight years. "I have cases upon cases in my office. We have actually phoned first responders to respond to first responders attempting suicide," DiNovo said. "This is prevalent, this is everywhere." DiNovo first began advocating for presumptive legislation when Toronto paramedic Shannon Bertrand came to her office looking for help. Toronto Sun, A16 (Ottawa Sun)

*** Windsor first responders welcome speedy PTSD treatment**

Emergency responders in the Windsor region applaud the Ontario government for proposed legislation that aims to speed up treatment for post-traumatic stress disorder (PTSD). The legislation, introduced Thursday, aims to help first responders get mental-health treatment to help them cope with work-related trauma. Under the proposed law, first responders will no longer need to prove their condition was caused by a specific event, which should speed up approvals for access to benefits and treatment, explained Jim Jeannette, a clinical social worker who specializes in working with first responders. "There are countless stories of firefighters and police that I know, that I have talked to, who have spent so much time trying to prove that they have it," he said. "It's just more agony than what they are going through." Details of the proposed Supporting Ontario First Responders Act were revealed at Queen's Park by Labour Minister Kevin Flynn and Community Safety and Correctional Services Minister Yasir Naqvi. CBC News

INTERNATIONAL

N. Korea plans terror attacks, Seoul says

North Korean Leader Kim Jong-un recently ordered preparations for launching "terror" attacks on South Koreans, a top Seoul official said Thursday, as worries about the North grow after its recent nuclear test and rocket launch. In televised remarks, senior South Korean presidential official Kim Sung-woo said North Korea's spy agency has begun work to implement Kim Jong-un's order to "muster anti-South terror capabilities that can pose a direct threat to our lives and security." He said the possibility of North Korean attacks "is increasing more than ever" and asked for quick passage of an anti-terror bill in parliament. North Korea has a history of attacking South Korea, such as the 2010 shelling of an island that killed four South Koreans and the 1987 bombing of a South Korean plane that killed all 115 passengers aboard. But it is impossible to independently confirmclaims of any such attack preparations. The South Korean presidential official did not say where the latest information came from. Earlier Thursday, Seoul's National Intelligence Service briefed ruling Saenuri Party members on a similar assessment on North Korea's attack preparations, said one party official who attended the privatemeeting. During the briefing, NIS, citing studies on past North Korean provocations and other unspecified assessments, said the attacks could target anti-Pyongyang activists, defectors and government officials in South Korea, the party official said. Attacks on subways, shopping malls and other public places could also happen, he said. Associated Press (London Free Press, B1/Front, Calgary Sun, Vancouver Sun, Edmonton Sun, Toronto Sun)

*** Syrian no-fly zone comes 'four years too late'**

The daily drumbeat of death in Syria goes on: hospitals bombed, civilians fleeing for the borders, children starving under siege, homes reduced to rubble. Amid such carnage the call for protecting civilians inside a no-fly zone sounds like a no-brainer for humanitarian action. But the realpolitik of the widening war will keep those dreams of safety from becoming reality. This week, Germany and Turkey revived a years-old call for a safe zone to shelter displaced people inside Syria's borders. Turkish President Recep Tayyip Erdogan blamed the U.S. for not taking action sooner and preventing "tens of thousands" of deaths. German Chancellor Angela Merkel - under fire at home for accepting more than 500,000 Syrian refugees - told the German parliament Wednesday that a no-fly zone agreement should be reached with Syria's backers and the coalition fighting the Islamic State Group. The U.S. also has its no-fly advocates. Former officials Nicholas Burns and James Jeffrey wrote in the Washington Post that a protected zone south of the Turkish border would have "manifold benefits," including keeping refugees from flooding into Europe, restricting the operations of the Syrian air force and curbing attacks by Russia, Lebanon's Hezbollah militia and Iran. Former Liberal leader Michael Ignatieff, now a professor at Harvard University, wrote with Leon Wieseltier in the Washington Post that "operating under a NATO umbrella, the United States could use its naval and air assets in the region to establish a no-fly zone from Aleppo to the Turkish border." Toronto Star

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PS.PSPMediaCentre/CentredesmediasPSP.SP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
March 17, 2016 / le 17 mars 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

* **Facing deportation, Mohamed Harkat plans to ask government to let him stay in Canada**
Terror suspect Mohamed Harkat, facing deportation to Algeria, plans to ask **Public Safety Minister Ralph Goodale** to allow him to remain in Canada. Harkat is preparing a formal submission to **Goodale** requesting that he decide it would not be "contrary to the national interest" to let him continue living in Ottawa with his wife Sophie, said Barbara Jackman, one of the Algerian refugee's lawyers. At the same time, Harkat and his counsel will prepare a reply to the Canada Border Services Agency, which recently concluded he poses a risk to Canada and that he could be returned to his homeland. "They haven't relied on any kind of current evidence," Jackman said in an interview. "So I am assuming that there is no current evidence because otherwise they would have relied on it." Both submissions are due in early May, Jackman said. Harkat, 47, was taken into custody in Ottawa in December 2002 on suspicion of being an al-Qaida sleeper agent. He denies any involvement with terrorism and fears torture if sent back to Algeria. The federal government is trying to deport the former pizza-delivery man on a security certificate - a rarely used legal tool for removing non-citizens suspected of extremism or espionage. Harkat's lawyers argued the process was unfair because the person named in a certificate doesn't see the full case against them. In a 2014 ruling, the Supreme Court of Canada said the security certificate regime does not violate the person's right to know and challenge the allegations they face. However, the high court provided detailed guidance on applying the process to ensure it is fair. Federal Court Justice Simon Noel ruled in 2010 that

there were grounds to believe Harkat is a security threat who maintained ties to Osama bin Laden's terror network after coming to Canada. Two years ago, the Supreme Court concluded Harkat "benefited from a fair process" when Noel reviewed his case, meaning the certificate against him stood. But little has happened since. Many supporters, including Prime Minister Justin Trudeau's brother Alexandre, have written to the government on Harkat's behalf. That says a lot about the man, Jackman said. "Some of those letters are very powerful. Those are the people who are best able to judge the kind of character he is." Canadian Press (CTV News, CP 24)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** 'Krazy Canadian' snowmobiler Dan Davidoff killed in B.C. avalanche**
His last post to Facebook was "Norm. Look I can fly, Lol." and he was famous for doing just that with his high-powered machines. But sometime on Monday while out in the mountains alone, extreme snowmobiler Dan Davidoff, 45, was buried in an avalanche near his home in Castlegar and did not survive, the B.C. Coroners Service has confirmed. CBC News; CTV News; Canadian Press (Times Colonist, A2; Charlottetown Guardian, Maclean's, St. John's Telegram, Ottawa Sun, Toronto Sun, Edmonton Sun, Calgary Sun); Postmedia Network (Vancouver Sun, Vancouver Province)

*** Sherwood Park men killed in B.C. avalanche**
Both men killed in an avalanche near Blue River, B.C., on Monday were from Sherwood Park, RCMP have confirmed. At 5:45 p.m. Monday, Clearwater RCMP received a call from a group of snowmobilers that an avalanche had buried two men from their group 30 kilometres southwest of Blue River. Five of the seven snowmobilers escaped the avalanche. Members of the group, including family members of the two men killed, were able to dig the men from the snow. However, efforts to resuscitate them were unsuccessful. Edmonton Sun, A5; Edmonton Journal

*** Au pire, des dégâts de 620 M$**
Dans le pire des cas imaginables, un déversement de pétrole du pipeline Énergie Est causerait un maximum de 620 millions $ de dommages, incluant les opérations de nettoyage et de restauration des berges, ont estimé mercredi après-midi les représentants de TransCanada devant le Bureau d'audiences publiques sur l'environnement (BAPE). En incluant les dépenses des différents ordres de gouvernement, qui devraient également être remboursés par la compagnie, l'intervention d'urgence (confinement du pétrole, évacuation, etc.) coûterait environ 200 millions, principalement pour nettoyer les berges (85 millions $). La restauration des sites après ce premier nettoyage coûterait environ 110 millions $, et les indemnisations pour les tiers - réparation de routes brisées par l'équipement lourd, propriétés endommagées, etc. - s'élèverait à près de 310 millions, estime la compagnie, qui dit s'appuie sur la «littérature internationale» détaillant des déversements réels (…) Notons qu'à Lac-Mégantic, où près de 6 millions de litres de pétrole se sont déversés lors de l'accident de 2013 (une partie a brûlé, 100 000 litres ont coulé dans la rivière Chaudière et le reste a contaminé le sol), les coûts du nettoyage sont estimés à 200 millions. Le Soleil, 7 (Le Nouvelliste); Journal de Montréal (Journal de Québec)

*** Survival 101**
(…)"Research has determined that 29 to 92 seconds are normally required for an occupant to escape from a submerged helicopter. One study has shown that the median breath-holding time of 228 offshore oil workers immersed in warm 25 C water was 37 seconds," stated the Transportation Safety Board's report on the Cougar crash. "In near freezing water, breath-hold drops as low as 5 to 10 seconds." The North Atlantic off Newfoundland averages 12 to 14 C in the summer and 1 to 2 C in the winter. Having been through Helicopter Underwater Escape Training, it's hard to picture surviving a real world ditching, even if it's controlled by the pilots."The more often you do (the training), the more comfortable you're going to be with it and the better your chances of being successful are going to be," said Dan Chicoyne, chief safety officer with the Canada-Newfoundland and Labrador Offshore Petroleum Board, in an interview at the CNLOPB offices in downtown St. John's. He does not use terms like "live" or "die." Chicoyne has a military background working as a helicopter pilot and, for a time, as a search and

rescue pilot in Labrador. His military training would include completing the same helicopter simulation, in the dark. St. John's Telegram, A1/A2

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Un terroriste pourrait s'infiltrer**

Alors que des soldats canadiens ont été visés lundi par un troisième attentat en public en 18 mois, les Forces armées canadiennes (FAC) craignent qu'un « sympathisant de groupes terroristes » réussisse à infiltrer une base militaire en usurpant l'identité d'un soldat. Ce terroriste mettrait alors en péril la « protection des forces », a prévenu l'été dernier la police militaire de l'armée dans un document obtenu par La Presse en vertu de la Loi sur l'accès à l'information. Le cas du Québécois Franck Gervais en novembre 2014 a eu l'effet d'un coup de semonce pour l'armée canadienne. Vêtu d'un béret rouge et d'un uniforme militaire, Franck Gervais avait assisté avec sa femme aux cérémonies du jour du Souvenir au Monument commémoratif de guerre à Ottawa... La Section du renseignement criminel de la police militaire met en garde les membres des FAC des graves conséquences qu'une telle usurpation pourrait engendrer, « surtout dans le cas d'un acteur solitaire qui aurait des affiliations avec des terroristes ou qui serait un sympathisant de groupes terroristes ». Dans un bulletin interne du 25 mai 2015, intitulé Extrémistes criminels - ce qu'il faut surveiller et signaler, la police militaire rappelle en préambule que des « organisations terroristes étrangères », comme le groupe État islamique, ont « demandé à leurs partisans de cibler et d'attaquer activement les membres et les établissements des organismes militaires et d'application de la loi de divers pays, dont le Canada ». Le Quotidien, 22; La Presse, 4

*** Turning suspect's life upside down**

Police hope a laptop will provide quick clues into the life of Ayanle Hassan Ali. Police agencies know Ali once worked close to passenger jets at Pearson International Airport as a groundskeeper, but what they consider a priority right now is tracking his most recent movements before he allegedly tried to kill three Canadian Armed Forces soldiers with a knife at a recruitment centre in North York on Monday. "We want to determine not only where he has been, but who was he with and who influenced him," a police source said. Still, many people felt the hair on the back of their neck stand when news of Ali's former airport job broke Wednesday. "Mr. Ayanle Hassan Ali is not an employee of the Greater Toronto Airports Authority (GTAA) nor does he currently work at Toronto Pearson," spokesman Siobhan Desroches assured my colleague Maryam Shah. "Mr. Ali worked for a third party tenant at Toronto Pearson and possessed a Restricted Area Identification Card (RAIC) from December 2008 to March 2009." So this computer police removed from his Albion Rd. apartment is their quickest ticket into his world. "The computer is already being analysed and information shared amongst Toronto Police, the RCMP, OPP and CSIS," a source said. Every e-mail will be scrutinized. Every Google search and website, too. "His whole life will be looked up and down," a police source said. "Everybody he met or communicated with will be looked at, and his travels." The nice thing about having the Integrated National Security Enforcement Team (INSET) working on this, an officer said, is there's no red tape to ask officers in Calgary to talk to people Ali knew while attending the University of Calgary, or in Edmonton, where his cousin tells media he started talking about conspiracy theories and religion. Ottawa Sun (Toronto Sun)

Imam calls attack on soldiers 'disturbing'

The head of a council of Canadian imams has condemned an attack on soldiers at a recruitment centre in Toronto. Dr. Mohammad Iqbal Al-Nadvi called the violence, which saw two soldiers injured and a third threatened, "disturbing." Ayanle Hassan Ali, a 27-yearold Toronto man, allegedly told people at the scene "Allah told me to do this." "It was shocking for us," Al-Nadvi, of the Canadian Council of Imams, said. "He put the responsibility on religious reasons. It's a disturbing notion." Al-Nadvi said the council found the attack particularly upsetting because it has connections to, and supports, the Canadian Forces. Three Muslim chaplains are part of an interfaith community network that works with the Forces. "When we go there, we see how we can make the Forces a good and friendly environment for Muslims," he said. Al-Nadvi said Muslims share the concerns of their fellow Canadians about the security of their country. "We are not living in isolation," he said. "We are part of the national fabric. It's also important we make our point very clearly. "It's important to make our national security a shared responsibility. In the Muslim

community, we are part of it and we will do whatever we can do to denounce (wrongdoing) going on inside the Muslim community and what is going on outside." Calgary Sun, A12 (Toronto Sun, Ottawa Sun)

Expert says too early to tell if attack against soldiers is terrorist related
A terrorism expert with the Gregg Centre for the Study of War and Society at the University of New Brunswick says he's reserving judgment on an incident in Toronto this week that saw two uniformed soldiers at a military recruitment centre stabbed and wounded. David Charters said it's hard to classify what happened as terrorism because not much is known about the individual. "I'd like to know more and maybe we will know more when the guy is brought to trial," Charters said in an interview. "Was he completely by himself or was there someone else he was working with? Do we know anything about his motives or his mental state? The whole thing seems a little bit bizarre. It doesn't even sound terribly well planned." Police have named the suspect as Montreal-born Ayanle Hassan Ali, 27, who moved to Toronto in 2011. The incident occurred mid-afternoon Monday, when a man walked into the government building that houses a Canadian Armed Forces recruitment centre on the ground floor. He arrived with a "large knife" in hand and began striking a uniformed master corporal, who fell to the ground. The soldier was able to get to his feet, at which point the suspect slashed his right arm. As military personnel moved civilians to safety, investigators said the man tried and failed to slash a female soldier before other soldiers were able to subdue him and hold him for police. Another military member was injured as the suspect was apprehended. Daily Gleaner, A4

*** Islamophobia? What about knife-o-phobia?**
An opinion piece states "Ayanle Hassan Ali is facing nine charges after he allegedly walked into a Canadian Armed Forces recruitment office wielding a large knife, and went on a stabbing rampage. According to Toronto Police Chief Mark Saunders, the accused stabbed two members of the Canadian military, and narrowly missed a third, saying: "Allah told me to do this, Allah told me to come here and kill people." That's probably why CSIS has joined the RCMP and local police in investigating this incident. It will be up to the courts to determine if Ali, 27, is guilty of the crimes he has been charged with committing. Saunders said it's too early to know if the accused was connected to or inspired by a radical Islamic terrorist group, or was acting on his own, or whether mental health issues were involved. His lawyer, David Burke, said Ali, who has no prior criminal record, is "very scared and very, very upset to be in the position he finds himself in." Toronto Sun, A15 (Ottawa Sun, Edmonton Sun)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Arafat Ally thrown out
A Palestinian man - once wounded alongside Yasser Arafat in his Ramallah headquarters during an Israeli Defence Forces siege - has been thrown out of Canada for being a member of Fatah, which was deemed a terrorist group despite its role governing Palestinian territory with financial support from the Canadian government. The decision by the Immigration and Refugee Board (IRB), recently upheld by the Federal Court of Canada, highlights the awkward transition from violent roots to government entity. Akram Muslih Anteer, 30, said he is dismayedbyhis deportation. "I told them Fatah is not terrorist group. It is a group that works with Canada, it is a group that works with the Stephen Harper; the United Nations works with Fatah," said Anteer. "I don't have any history like that," he said when asked if he is a security risk. "President Arafat made the people inside Palestine to see outside Palestine. He worked for peace. I promise you, I worked with him for the peace. "Arafat came to Palestine and signed for peace with Israel. I was a volunteer with Arafat. I was a young guy. He talked about stopping the problems in Palestine; war wasn't good. Just talking to him about the problems; I talked to him like that." Fatah was founded in the 1950s by Palestinian activists, including Arafat, and for years promoted violent struggle to achieve its goals of a Palestinian state. It is through Fatah that Arafat became chairman of the Palestine Liberation Organization. Fatah has, like its founder, been moving from revolution to politics. Postmedia Network (London Free Press, N1, Leader-Post, Windsor Star, StarPhoenix, Edmonton Journal, Montreal Gazette, Calgary Herald, Ottawa Citizen, National Post, Vancouver Sun)

*** Heroin seized at HSIA by CBSA**
Close to five kilograms worth of heroin was seized by the Canadian Border Services Agency (CBSA) from a traveller at Halifax Stanfield International Airport, the federal agency announced on Feb. 19. During a routine secondary examination of a traveller on February 14, CBSA officers discovered inconsistencies in the traveller's suitcase. "Upon dismantling it, they uncovered a large package concealed within the suitcase liner," CBSA said in a release. "Tests identified the package as suspected heroin." CBSA officers arrested the male traveller and turned him and the narcotics over to the Royal Canadian Mounted Police. He has been charged under the Controlled Drugs and Substances Act. "Every day our border services officers use their extensive skills and training to protect Canada's borders," said Colin Murchison, Acting Chief, Newfoundland & Labrador, Nova Scotia Division, Atlantic Region. "A significant seizure like this one is crucial in keeping hard drugs off Canadian streets." Enfield Weekly Press (2016-03-16)

*** CBSA conducting raids on caregivers in B.C. and Yukon**
Project Guardian is a Canada Border Services Agency project targeting foreign caregivers in their employer's homes. Advocates say workers are being penalized for leaving exploitative workplaces. The West Coast Domestic Workers Association is one of the groups calling for fairer treatment for temporary foreign workers. Natalie Drolet is executive director of the West Coast Domestic Workers Assocaition. She speaks with Redeye host Jane Williams. Rabble.ca (podcast)

Ottawa eases restrictions on seasonal foreign workers
The Liberal government has quietly approved changes aimed at helping Atlantic Canadian seafood processors that will allow them to bring in unlimited numbers of low-skilled temporary foreign workers to fill seasonal jobs this year. Ottawa approved the foreignworker exemption in response to lobbying from Atlantic seafood processors and Liberal MPs, who warned that recent restrictions to the temporary foreign worker program were hampering business. New Brunswick Fisheries Minister Rick Doucet recently said the labour shortage in his province is so bad that some lobster processing plants have had to throw lobsters in the trash. The Liberals - who swept all 32 ridings in Atlantic Canada in last year's federal election - are justifying the exemption as a shortterm measure to buy time until a full review of the foreign worker program can be conducted later this year. Other industry groups - such as Restaurants Canada - are questioning why exemptions are being allowed for some sectors and not others, and why they were never told of the change. Globe and Mail, A1

Worker shortage hits consumers
A severe shortage of workers is costing Canada's farm industry an estimated $1.5 billion a year in lost revenue and is driving up the cost of food for Canadian consumers, anew industry study states. The study, conducted by the Conference Board of Canada on behalf of the Canadian Agricultural Human Resource Council, found there are currently about 59,000 unfilled farm jobs in Canada. And that number is expected to balloon to 114,000 by 2025, as the demand for food and agriculture-industry workers continues to grow and older workers retire. "What that (worker shortages) does for businesses and for industry is that it really constricts them," human resource council executive director Portia MacDonald-Dewhirst explained in an interview Wednesday. "The businesses aren't running efficiently, they're unable to meet their production targets and they're unable to meet any export opportunities that are presented to them because they don't have enough bodies to do the work." The release of the council's labour market information study coincided with a national three-day Growing the AgriWorkforce summit, which wrapped up Wednesday in Winnipeg. The event drew agriculture industry and government representatives from across the country to discuss worker shortages and ways to address the problem. MacDonald-Dewhirst and Debra Hauer, manager of the labour-market study, said the types of workers needed include farm owner/operators, farm managers, general farm workers, equipment operators, truck drivers and dairy workers. (...)Hauer noted about 12 per cent of the agriculture jobs in Canada are currently being filled by temporary foreign workers. That's up from six per cent a decade ago. "And we still don't have enough workers," MacDonald-Dewhirst said. Winnipeg Free Press, B6

Convicted Canadian narwhal tusk smuggler extradited to U.S. on money-laundering charges
A retired RCMP officer from New Brunswick who has already been convicted and fined in Canada for smuggling narwhal tusks has been extradited to the United States to face money-laundering charges related to the scheme. Narwhals, sometimes called the unicorns of the sea, are found in Arctic waters

and known for the long, spiralling tusk - actually a tooth - that in males can grow through the creature's upper lip into a sword-like tusk nearly three metres long. The tusks are collectors' items. Narwhals are protected under the Convention on International Trade in Endangered Species of Wild Fauna and Flora and it is illegal to import narwhals, or their parts, into the United States without a permit. A legal hunt for a few hundred animals each year is restricted to Inuit in Canada and Greenland. Gregory R. Logan was extradited on March 11 to face trial in U.S. District Court in Bangor, Me., the U.S. Department of Justice said Wednesday. A U.S. judge ruled Wednesday that Mr. Logan, a retired member of the RCMP, must remain in custody until his trial, which is currently scheduled for May 3. U.S. authorities allege that Mr. Logan committed "specified unlawful activities" by smuggling narwhal tusks into the United States, sold them to collectors and then laundered the proceeds by having the money transferred out of the United States. Globe and Mail, A6; * Associated Press (Daily Mail UK)

*** Québec veut le libre-échange avec les États-Unis**

Le gouvernement Couillard estime que son nouveau régime forestier lui permet de plaider le libre-échange en matière de commerce du bois d'oeuvre avec les États-Unis. Néanmoins, la ministre de l'Économie, Dominique Anglade, ainsi que son collègue aux Forêts, Laurent Lessard, sont bien au fait que ce scénario n'enchante guère les Américains. En point de presse à l'Assemblée nationale, mercredi, les deux ministres ont prévenu que les négociations entre le Canada et son voisin du Sud ne s'annonçaient pas faciles pour renouveler l'entente sur le bois d'oeuvre, venue à échéance l'an dernier. Entre-temps, les autorités américaines ne peuvent imposer de tarifs douaniers sur les produits canadiens du bois d'oeuvre jusqu'en octobre prochain en vertu d'une période d'interdiction de 12 mois. La semaine dernière, au terme de leur rencontre à Washington, le président américain Barack Obama et le premier ministre Justin Trudeau ont affiché leur confiance de trouver un terrain d'entente rapidement. L'accord de 2006 entre le Canada et les États-Unis sur le bois d'oeuvre s'était conclu après cinq ans de batailles devant les tribunaux. Presse canadienne (Le Nouvelliste, 14, Le Devoir)

Trump taps into opposition to free trade

Canadians used to fret over free trade. They don't much anymore. The notion that trade and investment deals are good things to pursue has become part of this country's political orthodoxy. The Liberals, who famously called the original 1984 Canada-U.S. Free Trade Agreement a threat to Canada's very existence, now take credit for implementing the 1993 North American Free Trade Agreement, its far more intrusive successor. Even the New Democrats have become accepting. They may oppose the looming Trans-Pacific Partnership trade and investment deal. But they broke with their union allies to support the 2015 free trade pact between Canada and South Korea. So it is intriguing to see free trade emerging front and centre as one of the key political issues in the U.S. presidential election. Free trade has been a part of modern American politics since NAFTA integrated the economies of the U.S., Canada and Mexico. Ross Perot based much of his 1992 third-party presidential campaign on his opposition to signing NAFTA. Bill Clinton, the Democratic candidate and eventual president, essentially supported it. Over time, Democrats, including U.S. President Barack Obama, played a more devious game - criticizing trade deals on the hustings, but supporting them once in power. In those years, only the Republicans could be counted on to support unfettered free trade in both word and deed. With Donald Trump, however, all of this has changed. Barring a miracle, the billionaire developer is poised to become the Republican Party's presidential nominee this summer. Toronto Star, A9

Bois d'oeuvre: la bataille «loin d'être gagnée»

La ministre de l'Économie et le ministre des Forêts ont promis mercredi d'être «très actifs» dans le processus menant à un nouvel accord sur le bois d'oeuvre. Ils se sont réjouis que, lors de son passage à Washington, le premier ministre Justin Trudeau plaide pour la fin des quotas et des taxes sur le bois d'oeuvre canadien. «On est content de la position canadienne, a affirmé M. Lessard. Elle est forte, elle est bien affirmée. […] La voix du Québec va être portée partout là où c'est nécessaire.» Le précédent accord sur le bois d'oeuvre est arrivé à échéance l'année dernière. M. Trudeau et le président Barack Obama se sont donné 100 jours pour en négocier une autre. Le bois d'oeuvre est celui qui est utilisé pour bâtir la charpente des maisons et pour la fabrication de plusieurs produits liés à la construction. (…)L'industrie forestière a été passablement ébranlée au cours des dernières années et l'imposition de tarifs douaniers élevés aurait des conséquences, souligne la ministre Anglade. «C'est 60 000 emplois

dans l'industrie de la forêt, a-t-elle noté. Ça aurait un impact direct sur la rentabilité des entreprises.» La Presse (Le Soleil)

*** Border officer honoured**
Twenty years of commendable service earned a Calgary border services officer recognition from Canada's governor general. Scott Jenkinson, senior officer trade compliance for the Canada Border Services Agency, received a Peace Officer Exemplary Service Medal from Gov. Gen. David Johnston on March 4 at a presentation in Vancouver. This honour is bestowed upon peace officers "who have served in an exemplary manner, characterized by good conduct, industry and efficiency." Only those who have at least 20 years of service - including 10 on the front lines performing duties involving potential risk - are eligible to receive the honour. "I have enjoyed my career as a peace officer and with the CBSA. Every day there is something new to learn and a wide variety of duties within this Agency," said Jenkinson in a statement. "I felt honoured to receive the medal and humbled to be included with such diverse recipients." Calgary Sun, A10 (Calgary Herald, Edmonton Sun, Toronto Sun, Ottawa Sun, Winnipeg Sun)

*** Roof replacement forces tunnel to close at night**
The Windsor-Detroit Tunnel will be closing overnight five days a week beginning in August for replacement of its original concrete roof. "It's a scheduled project and if you look at tunnels in the United States and Canada they have a lifespan, just like the roof on your house has a lifespan, and so this is just a scheduled replacement," said tunnel president Neal Belitsky. The roof replacement will be part of extensive renovations to the tunnel which will begin in May. "In the first part of the project is work that will be behind the scenes and so there will be no interruption to the travelling public," said Belitsky. "From May through sometime in August. Then sometime in August we plan on doing scheduled removal of the tunnel ceiling and that will run through, we're anticipating, through to December." The tunnel will be closed from 9 p.m. until 5:30 a.m. from Sunday through Thursday. "So we will be open on weekends, we plan on being open for the morning commuter rush," said Belitsky. "And the contractor will have to work around any special events that happen during that period." Attending an evening event in Detroit during the construction period days will require returning to Windsor on the Ambassador Bridge. Windsor Star, A5

CYBER SECURITY / CYBERSÉCURITÉ

*** Fredericton Mayor Brad Woodside's tweet about jobs causes stir**
A speech from Premier Brian Gallant followed by a tweet from Fredericton Mayor Brad Woodside has led to some confusion as to how many jobs would be coming to the capital and from where. On Wednesday morning Woodside tweeted, "Cyber security centre of excellence coming to Fredericton creating upwards to 400 jobs. Great announcement (...)"Gallant has voiced his intentions of creating "a centre of excellence in cybersecurity" in New Brunswick. The premier spent time earlier this month at a major cybersecurity conference in San Francisco promoting the province as an IT hub. CBC News

*** Canada's national cyber threat centre looking to expand**
Everyone looks forward to April 1 as a sign that spring will really be here. Gwen Beauchemin, director of the federal government's Canadian Cyber Incident Response Centre (CCIRC) is looking forward to it even more. That's because her budget for the new fiscal year starting on that date will allow here to up its staff to 87 from 43, which will help it expand its threat gathering capabilities as well as its threat intelligence services to Canadian organizations. "We're very thankful that we're seeing messages now that the [new Liberal] government would like us to be more forward leaning and outward," she said in an interview, "so I can only think that will raise awareness and the success of getting that information out to all." The centre, part of Public Safety Canada, has 1,200 provincial, municipal and private sector subscribers in the country — largely organizations in critical infrastructure — a number she'd like to substantially increase. It pulls in over 1 million pieces of spam a day and identifies 300,000 different vulnerabilities. In 2015 it discovered over 87 million new pieces of malware. The centre categorizes information in four levels based on the Traffic Light Protocol used by 14 countries. IT World Canada

*** Google intent on encrypting all online activity**

Google is disclosing how much of the traffic to its search engine and other services is being protected from hackers as part of its push to encrypt all online activity. Encryption shields 77 per cent of the requests sent from around the world to Google's data centres, up from 52 per cent at the end of 2013, according to company statistics released Tuesday. The numbers cover all Google services except its YouTube video site, which has more than one billion users. Google plans to add YouTube to its encryption breakdown by the end of this year. Encryption is a security measure that scrambles transmitted information so it's unintelligible if it's intercepted by a third party. Google began emphasizing the need to encrypt people's online activities after confidential documents leaked in 2013 by former National Security Agency contractor Edward Snowden revealed that the U.S. government had been vacuuming up personal data transferred over the Internet. The surveillance programs exploited gaping holes in unencrypted websites. Associated Press (Chronicle-Herald, B4)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Funds given to sham canvasser passed to charity

Nanaimo RCMP have located a woman in connection with reports of the unauthorized collection of donations on behalf of the B.C. Open Heart Society. After warning the public of fraudulent door-to-door canvassing last week, police followed up on tips from the public and found the suspect in her Nanaimo home. She voluntarily turned over the money she had collected to the investigating officer, who decided to deal with the matter informally. The woman was warned that further offences could lead to criminal charges. The money was given to the B.C. Open Heart Society, one of the groups the woman said she was collecting for. If you have doubts about the authenticity about an individual collecting funds, call the organization in question to see whether they have canvassers in your neighbourhood. Fraudulent fundraisers can be reported to your local police department's non-emergency line. Times Colonist, A3

RCMP clears senators under review: sources

After nearly four years of scandal, Prime Minister Justin Trudeau Wednesday said the Senate is "on the right track" with word the RCMP has cleared most, if not all, of the 30 senators under police review for questionable expense claims. Police won't comment on their findings, but sources said many of the senators under scrutiny have been notified in writing that RCMP reviews of their expense account files found nothing to warrant full criminal investigations. "The majority of 30 have received word (that) after a preliminary review (the case) didn't merit investigation," said one source. Another said it is "99 per cent sure all 30 will be cleared." Several of the senators were informally notified as far back as last July. Trudeau, in New York seeking a United Nations Security Council seat for Canada, said the damaging series of internal financial audits, police scrutiny and the related and continuing criminal trial of Sen. Mike Duffy, "have led us to a place where I think we're on the right track." (…) He is expected to soon name five new senators to sit as independents and to start filling 22 Senate vacancies. The RCMP review of the senators' expense claims was triggered last June when federal auditor general Michael Ferguson released the results of a sweeping audit that found what he characterized as repeated abuses of taxpayer dollars and a need for wholesale culture change. Leader-Post, N4 (London Free Press); Canadian Press (ChronicleHerald, Le Droit, L'Acadie Nouvelle); Le Devoir, A3

De fausses alertes à la bombe simultanées dans quatre écoles

Différents corps policiers enquêtent sur une série de menaces à la bombe perpétrées au même moment mercredi dans trois écoles du Nouveau-Brunswick et dans un autre établissement d'enseignement situé à Bangor, au Maine. Le premier incident est survenu mercredi matin à l'école Bangor High, qui a dû être évacuée en raison d'une alerte à la bombe. Le personnel de l'école a reçu un appel à 11h30 indiquant la présence d'un engin explosif à l'intérieur des murs de l'établissement. De son côté, la Force policière de Fredericton a dû intervenir au même moment à l'école Devon Middle, qui est située sur la rue Dobie. La direction de l'école a informé la police à 11h30 après avoir reçu un appel faisant état de la présence d'une bombe à l'intérieur de l'établissement. Les policiers de Saint-Jean ont pour leur part dû intervenir à 11h30 à l'école Forest Hills Junior High après que le personnel a reçu un appel disant qu'il y avait une bombe à l'intérieur de l'école. Le Service régional Codiac de la GRC a quant à lui mené une opération à l'école Riverview High peu après 11h30 mercredi après un appel faisant une fois de plus état de la

présence d'une bombe à l'intérieur de l'école. «L'appel logé par le directeur de l'école faisait mention d'un appel informatisé indiquant que l'engin allait exploser s'il y avait intervention policière», a indiqué le sergent de la GRC André Pépin. La GRC affirme que le contenu des appels téléphoniques logés au même instant dans les différentes écoles était similaire et pourrait fort bien être l'oeuvre d'une seule et même personne ou d'un groupe d'individus. La GRC a indiqué avoir institué une enquête en collaboration avec les autres corps policiers afin de tenter de faire la lumière sur ces appels à la bombe. Dans les quatre cas, les élèves ont pu réintégrer leurs classes après une fouille des lieux. L'acadie Nouvelle, 2

Sécurité renforcée après une «menace»
Le transporteur ferroviaire canadien Via Rail a renforcé mercredi les mesures de contrôle et de surveillance dans certaines gares après avoir reçu une menace qualifiée de « non fondée » par l'entreprise, mais prise au sérieux dans le contexte sécuritaire mondial. La société parapublique a demandé à ses employés « d'être vigilants » et va augmenter « ses patrouilles policières et canines dans certaines gares », a indiqué à l'AFP sa porte-parole, Marie-Anna Murat, disant travailler « en étroite collaboration avec les autorités policières ». Des contrôles accrus étaient notamment menés aux gares de Toronto et Montréal, les deux plus grandes villes du pays, selon les médias locaux. La Gendarmerie royale (GRC) a indiqué à l'AFP que ses agents étaient déployés aux côtés des forces de police municipales « afin d'assurer la sécurité des passagers qui transitent aux stations ferroviaires à travers le pays ». La menace visant Via Rail a entraîné l'ouverture d'une enquête par le service de police de la ville de Montréal (SPVM), a souligné la GRC. Cela semble indiquer que la gare de la métropole québécoise serait visée. Agence France-Press (Le Droit, 25)

RCMP applies to have man's dog destroyed
The RCMP is looking to have a Conception Harbour man's dog destroyed. The application was brought forward Wednesday morning when Robert Brant appeared in provincial court in St. John's. The 34-year-old faces charges of failing to tether a dog and unlawfully allowing a companion animal to cause a hazard under the Animal Health and Protection Act. The offences are said to have happened Nov. 9, 2015, in Conception Harbour. RCMP officer Adrian Cox, who filed the application, was in the courtroom. He told Judge Mike Madden that he served Brant with it on Feb. 10. Brant spoke up, saying he didn't know why he was in court because he had told the officer back then that he already agreed to have the dog destroyed. Telegram, A2

POLICE PROBE MYSTERIOUS DEATH
Police are being tight lipped on whether a blood-smeared van in Pines is connected to the death of a man found in a city alley. Red Deer City RCMP were called to a report of a man in distress at an alley around 4: 54 a.m. on Wednesday. The man was taken to hospital where he later died. Police had a street cordoned off in Normandeau. The Calgary RCMP Major Crimes Unit were called in to help with the investigation. Around the same time, one Pines resident looked out his window to see something out of the ordinary unfold on Page Avenue near Pamely Avenue. The resident did not give his name. "I just looked out the window and saw the van roll up slowly," he said. "It was eerie." The man said he walked away from the window and when he returned a few minutes later, the white cube van had plowed into a car. He did not want to speculate on what happened. The white cube van had what appeared to be blood smeared on the driver's side near the back tire. It appeared to have rammed into a small car. Details are few as police are continuing to investigate. A section of Page Street was taped off for most of the day as police went door to door to talk to residents. There was heavy police presence in both neighbourhoods throughout the day. Red Deer Advocate, A1

Ivvavik National Park meeting Aklavik...
A meeting to discuss Ivvavik National Park took place in Aklavik on March 14, according to Parks Canada. The meeting was scheduled to begin at 10 a.m. in the hamlet council chambers. Representatives from Aklavik's Hunters and Trappers Committee were invited to attend, as well as the directors of the Aklavik Community Corporation. Topics included an infrastructure update for the Sheep Creek base camp, cultural resource monitoring and Aklavik's role in managing the park. The meeting was scheduled to finish around 4 p.m. Gwich'in invited to Inuvik fracking workshop. The Gwich'in Tribal Council was inviting residents to attend a two-day workshop on fracking March 12 and 13 in Inuvik, according to a post on Fort McPherson's Facebook page. The workshop was done in partnership with

the Southern Alberta Institute of Technology and, according to the post, aimed to "gain knowledge and overall understanding of fracking." It was scheduled to take place at the council chambers in Inuvik and included lunch. (...) Members of the RCMP were also scheduled to visit the school the week of March 14 to host an anti-bullying and cyberbullying workshop, but many students were away sick, Berger said. INUNIK Drum

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Report identifies prison challenges
There's room for improvement in with the way Correctional Service Canada (CSC) operates, according to the annual report released last week from the office of the Correctional Investigator. The office, which acts as an ombudsman for federal offenders, released 18 recommendations addressing such challenges in the CSC as prison health care, aboriginal corrections, conditions of detention, how to handle federally sentenced women, offender employment, and resolution of offender complaints and grievances. According to the office's website, its primary function is to investigate and try to bring resolution to individual offender complaints and make recommendations on CSC's policies and procedures associated with inmate complaints and to make sure areas of common concern among the inmate population are brought up and investigated. (...) In his report, Howard Sapers, the correctional investigator, said some cost-cutting measures over the period may have had a detrimental effect on the prison system. Sapers brought up a variety of cancelled initiatives that affect reintegration and release programs by the former Conservative government, including the prison farm issue, saying the closure at Frontenac Institution and other prison farms in Canada and other support programs "effectively undermine reintegration efforts." (...)His report also said more than 70 per cent of women have children under the age of 18 and recommend that CSC reintroduce and strengthen their motherchild program, which has been "progressively eroded by operational, population and security concerns." Kingston Whig-Standard, A3

*** Jailed biker now facing weapons charges**
A Fallen Saints motorcycle club member serving prison time for kidnapping and viciously beating his ex-girlfriend faces new charges of weapons trafficking after getting caught up on the edges of a massive police investigation. Clint James McLaughlin, 38, made his first appearance Wednesday in Saskatoon provincial court on the weapons charges, which date back to March 28, 2014. He appeared via video from the Saskatchewan Penitentiary at Prince Albert, where he's serving his six-year kidnapping and assault sentence. McLaughlin's alleged involvement with a "big bag of guns," was the subject of testimony at a murder trial in Saskatoon last year, when police informant Noel Harder was being grilled about why he started working with the police. (...) Harder said that in early 2014, he was caught transporting a hockey-sized bag of guns "from a guy named Clint McLaughlin's house." To avoid prosecution, Harder said he volunteered to become a police informant. His role as an informant led to an investigation police dubbed Project Forseti, which culminated in January 2015 with police raids, arrests and the seizure of $8 million worth of illegal drugs and hundreds of firearms. By that time, McLaughlin was in prison - he was arrested in early June 2014 on the kidnapping and assault charges and remained in custody until his sentencing in December 2014. The 17 new weapons charges that McLaughlin faces relate to rifles, including an assault rifle, shotguns and handguns. Postmedia Network (StarPhoenix, A3, Leader-Post)

14-year sentence for preying on men
An Ottawa man who deliberately contracted HIV then had sex with unsuspecting victims - infecting a 17-year-old boy - has been sentenced to 14 years in prison and declared a long-term offender. The sentence Steven Boone, 35, received in Ottawa comes almost three years after he was sentenced to four years in prison for not disclosing his HIV status to sex partners in Waterloo. (...) The Ottawa sentence was for seven offences in 2010 - including three counts of attempted murder. (...)Boone's local crimes, committed in March 2010 with accomplice Noel Bowland of Kitchener, involved group sex with two men while high on marijuana at the Waterloo apartment of one of the victims. Boone and Bowland did not reveal they were HIV-positive. The victims did not contract HIV. The two were convicted of two counts of aggravated assault. Boone got four years; Bowland got 18 months. Waterloo Region Record, A1

In the Courts
Mazon Arbaji, 38, was convicted of violating probation he received in October 2014 in Toronto by failing to report to his probation supervisor. Arbaji, who is currently serving time in federal prison and nearing the end of his sentence, had the charge waived to Kingston in order to deal with it. He had 30 days added to the federal sentence he's currently serving. Federal inmate Gordon Craig, 44, was convicted of committing mischief by wilfully damaging a stolen truck he and another federal offender used to drive to Ottawa while they were both supposed to be living at the Henry Traill Community Correctional Centre. He had 90 days added to his existing sentence and a freestanding restitution order for $900 was issued against him. Kingston Whig-Standard, A7

* **In the courts, Feb. 16 to 19**
Federal inmate John Mensah, 28, was convicted of having illegal possession of marijuana while serving a sentence at Joyceville Institution. He had four months added to the nine-year-four-month sentence he's already serving for robbery and weapons offences. Federal Crown prosecutor Joe Dart said Mensah was caught with 12.4 grams of marijuana in early October after a young woman visiting him was seen to pass it to him inside a potato chip bag. Dart said there was a second substance inside the bag as well, which was initially thought to be MDMA (ecstasy) but turned out to be an unscheduled substance. Defence lawyer Phil Casey disclosed that Mensah's original statutory release date was August 2017. Kingston Whig-Standard (2016-03-16)

* **Segregation an 'essential tool' for officers**
An opinion piece by Jason Godin, VP of the Union of Canadian Correctional Officers, states, "Recently, there have been many interest groups calling for the abolishment of administrative segregation units inside Canada's federal institutions and restrictions on the amount of time spent in segregation. The Union of Canadian Correctional Officers represents more than 7,000 officers working the front lines inside Canada's penitentiaries. Segregation for us is an essential tool of our trade that allows us to keep inmates, staff, and ultimately the Canadian public, safe. Without it, our institutions would be chaos, become more dangerous for inmates and our safety would be more at risk in an already dangerous workplace. The interest groups also refer to our segregation as solitary confinement, implying that we put the inmate in a cell with no contact with the outside world. Nothing could be further from the truth, and the notion of solitary confinement only exists in the movies. (…)As correctional officers, we are concerned that various groups are creating a false misunderstanding of this essential tool for correctional officers. If radical changes are made into policy, they may jeopardize the safety and security of our institutions. We are proud of the work we do and the vital service we perform on behalf of Canadians, but we need to ensure that we have the proper tools in place to carry our mandate to protect the public and assist in the offenders' rehabilitation." Kingston Whig-Standard, A4

* **The deadly cuckoo's nest of solitary confinement**
An opinion piece states, "When prison watchdog Howard Sapers began penning his annual report on the litany of ills he continues to see within the federal corrections system, he did so thinking it would be his last kick at the can. His pink slip had already been signed. The Harperites, long on law and order but short on any expressed compassion for the incarcerated, made no secret about Sapers being an increasingly irksome pain in their collective psyche since his appointment in 2004. He was a watchdog who would not give up the bone. If his recommendations were not acted upon, for example, he would bring it up in his next annual report in a bolder fashion and with a louder denunciation. (…) Besides, the federal prison system, through solitary confinement, is doing a pretty good job anyway at killing off the tormented souls behind bars. As Sapers pointed out in his report, half of the 30 federal inmates who committed suicide between 2011-2014 did so in solitary confinement, with nearly all of them having known mental health issues. Further troubling, said Sapers, is that these suicides took place in what is supposedly the most closely-monitored part of a prison, and where suicide watch is one of the prime purposes of these cells existence. Yet 14 inmates were somehow able to find the means and opportunity to kill themselves with all those eyes watching. This could be interpreted, perhaps, as corrections officers figuratively asleep at their watch, or simply not caring about the mentally ill offing themselves in solitary. It's either one or the other." Winnipeg Sun, A15 (Calgary Sun, Toronto Sun, Ottawa Sun, Edmonton Sun)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** More overdoses from bootleg fentanyl reported**
More people are dying of drug overdoses than they are in car crashes in Waterloo Region. And that's because powdered fentanyl is 100 times more powerful than morphine and 50 times more potent than heroin, says Staff Sgt. Shirley Hilton, head of Waterloo Regional Police's drug branch. Hilton said that in three recent drug seizures it appeared that police had busted dealers selling cocaine and heroin, but after analysis, the white powder was found to be a blend of powdered fentanyl and heroin. The appearance of bootleg fentanyl means drug dealers are creating the drug in illicit labs, mixing it with other drugs, and passing off the new concoction as heroin or cocaine, Hilton said. "They are creating their own recipes," she said. "I wouldn't say we have a crisis, but we need to be aware. Fentanyl is definitely here." The Waterloo Region Crime Prevention Council created the Waterloo Region Integrated Drug Strategy, which also involves the police, so community partners can keep track of overdoses in the region. Waterloo Region Record, B3

*** Needle site cost?**
How much will safe injection sites cost Toronto? Dr. David McKeown, the city's chief medical officer of health, can't say right now, but they hope the province will help fund the three proposed drug injection sites that will be scattered across the city. McKeown is in the midst of consulting the public about his recommendation to allow three existing clinics that offer harm reduction services to begin to provide supervised injections. (...) Councillor Joe Cressy, chairman of the Toronto Drug Strategy, said the city's needle exchange program distributes 75% of its clean needles at the three proposed supervised injection sites. "That's where the people are using right now," Cressy said. "The reality is it is in our backyard here. This is a way for us to go to where the users are ... they're coming in the doors now to get their needles, this way they're not walking them around the corner." Cressy said overdose deaths, which are on the rise in the city, are "preventable deaths." "We have 206 people dying due to overdose in the most recent numbers," he said. "If we had 206 people dying due to an annual plane crash, we would demand, as a city, plane safety." He pointed out that in 2005, the year of the Summer of the Gun in Toronto, there were 52 gun murders. "It was a horrible, atrocious loss of life and we acted," Cressy said, adding that he believes safe injection facilities can save lives. Toronto Sun, A10

*** Le budget de la police ne sera pas augmenté, dit Brian Bowman**
Le comité exécutif de la Ville de Winnipeg refuse d'augmenter davantage le budget du service de police. Au terme d'un débat houleux, où des membres du conseil de police ont affirmé qu'il y aura des mises à pied sans une augmentation de 2,4 millions de dollars, le comité a décidé de maintenir le budget du Service de police de Winnipeg à 280,7 millions de dollars pour l'année 2016-2017. « Nous croyons qu'il y a suffisamment de financement pour assurer qu'il n'y aura pas d'ajustements au personnel », déclare le maire de Winnipeg Brian Bowman, tout en rappelant que le budget du Service de police a augmenté de 80 % au cours des 10 dernières années. Radio-Canada; CTV News (2016-03-16)

*** Ottawa Police blow overtime budget by $2.1 million**
Ottawa Police blew their overtime budget by 2.1 million dollars in 2015. According to a report to be presented at next week's Ottawa Police Services Board meeting, the deficit was due to several factors, including the taxi strike at the airport and homicide investigations. Chair of the Police Services Board, Eli El-Chantiry, says the main reason they went over budget was due to staffing shortages. "Hiring 25 police officers, you don't see the results right away," says El-Chantiry. "They are hired now but it's going to take time ... you're not going to see a lot of benefit until probably the last quarter of the year." All of this money was made up in the end, mostly because of paid duty revenue and compensation costs. The police service would have ended the year in the black, if it weren't for a $2.2 million shortfall in the amount of money expected from tax payers. CFRA News (2016-03-16)

*** BCTF calls for children's minister to resign after latest teen death**
The B.C. Teachers Federation is calling for the resignation of Stephanie Cadieux, minister of children and family development, after another young aboriginal person died months after her 19th birthday and the loss of government support. Patricia Lee Evoy, also known as Indigo, died last week. She was not in

foster care, but was on a youth agreement, which is a form of financial support for people under 19 whose families cannot care for them, said Mary Ellen Turpel-Lafond, B.C.'s representative for children and youth. Evoy turned 19 in October and her youth agreement expired, Turpel-Lafond said. "I'm still gathering information, but at this point what I can say is that after she turned 19, things pretty much fell apart," Turpel-Lafond said. "I'm very sad about this death and deeply concerned." Cadieux said she did not have a response to the teachers' call for her resignation. (...) Evoy appears to have died from a drug overdose, Turpel-Lafond said. A male and a female were found dead in an apartment in Burnaby on Willingdon Avenue on March 10 and the coroner is investigating, said coroner Barbara McLintock. Turpel-Lafond said it's possible that Evoy, like many young aboriginal women, was pressured to make money through dancing or working as an escort. Vancouver Sun (2016-03-16)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Target causes of violence against indigenous women**
An opinion piece states, "The government of Canada is finally launching a national inquiry into missing and murdered indigenous women and girls. But why has it taken so long? Why have thousands of aboriginal women and young girls disappeared with barely a blip on the national radar? I believe this has to do with the continued failure to acknowledge and address the past, present and unfortunate future effects of colonization. The Feminist Alliance for International Action Canada, The Native Women's Association and the Canadian Journal of Women and Law hosted a symposium in January to design a plan for the inquiry. Its most important recommendation was the need for Canada's focus to be on ending the gendered and racialized violence against indigenous women and girls. Dawn Lavell-Harvard, president of NWAC, argued that "gendered, sexualized and racialized violence against indigenous women and girls violates our commitments to equality and causes lasting inter-generational harm to families." The abuse and violence will not be eliminated until Canadians demand social and economic inequalities that perpetuated them are addressed. Intersecting factors boil down to the fact that the victims are both female and indigenous. Somehow, that has allowed these women and girls to be continually subjected to racialized and sexualized violence. It is as if to say they are not as important as other human beings." Chronicle-Herald, A11

*** 9 choses à surveiller lors du budget fédéral 2016**
Le ministre des Finances, Bill Morneau, dévoilera son premier budget le 22 mars 2016 qui affichera un déficit de 30 G$ - soit trois fois plus que prévu – selon Bloomberg. (...) « Nous n'avons besoin de rien de moins qu'un renouveau total de la relation entre le Canada et les peuples autochtones. Aucune relation n'est plus importante pour moi que celle-là. » C'est en ces termes que Justin Trudeau s'est engagé à appliquer les 94 recommandations de la Commission de vérité et réconciliation du Canada. Depuis son élection, il a promis de rétablir les relations avec les peuples autochtones du Canada, peu importe le coût. Son gouvernement a déclenché une enquête nationale sur les femmes autochtones disparues ou assassinées. Il promet également d'importants fonds pour que tous aient accès à de l'eau potable, à des logements salubres et à une éducation de qualité. Huffington Post (2016-03-16)

*** Survivors say Nordic model is our only hope**
People were turned away from a packed, standing-room only panel, addressing the impacts of various prostitution legislation around the world, on Monday afternoon. Organized by SPACE International, the parallel event, which took place in New York City in connection with the 60th session of the Commission on the Status of Women, featured the voices of survivors-turned-front-line-workers from around the world -- women we rarely hear from in the so-called "sex-work" debate, despite their expansive experience in various aspects of the sex trade. Moderated by Rachel Moran, co-founder of SPACE, Bridget Perrier, who is a survivor of child prostitution and human trafficking, spoke first, addressing the dire situation faced by Indigenous women and girls in Canada. An Ojibaway woman who lives in Ontario, Perrier was heavily involved in the passage of Bill C-36, Canada's new prostitution legislation, which criminalizes sex buyers as well as people who profit from the exploitation of women and girls, but decriminalizes

prostituted women. (...) Perrier called the Downtown Eastside of Vancouver, where Indigenous women are far overrepresented in the sex trade and where many have gone missing and been murdered, "a war zone," saying the link between prostitution and the missing and murdered women is undeniable. Beyond holding men who buy sex accountable, Perrier put forth another demand to the Canadian government: "We are asking that when a man kills an Indigenous women, he be charged with a hate crime." Rabble (2016-03-16)

PUBLIC SERVICE / FONCTION PUBLIQUE

* **National Defence reports IT headaches over Shared Services support**
More documents obtained by CBC News illustrate serious complaints about Shared Services Canada this time at the Department of National Defence. Briefing notes prepared for commander of the army Lt.-Gen Marquis Hainse in February 2014 detail how governance at Shared Services caused "significant inefficiency at every level," including service delivery, procurement, resource management and delegation of authority. CBC obtained the defence document following earlier reports about the dismal support Shared Services has provided to the RCMP. Shared Services is the federal department created in 2012 to take over the delivery of email, data centre and network services for 43 government agencies. At Defence, a memo authored by Lt.-Col M.C. Arguin and released under access to information described several mishaps that would have affected operations of the army. Defence employees stepped in to perform tasks that should have been done by Shared Services. "As a result the CA's [Canadian Army] C2 [command and control] systems that support exercises and operations have, up until now, remained slightly sheltered (although not completely) from the majority of the issues experienced across DND." Arguin noted that the deterioration of service delivery had affected army training. CBC News

OTHER / AUTRE

* **Trudeau announces Canadian bid for 2021 seat on UN's Security Council**
Canada will vie for a seat on the Security Council for a two-year term starting in 2021, Prime Minister Justin Trudeau said today. The members of the General Assembly won't vote on candidates for the vacancy until the fall of 2020, which means Trudeau will have to win another federal election in 2019 if he wants to personally see Canada return to the UN's most powerful body. If Canada succeeds, it would end the country's longest absence from the council in the history of the United Nations - 21 years since the end of Canada's last two-year stint in 2000. Trudeau launched the campaign this morning from the lobby of the United Nations building in New York in front of a crowd of staffers, visiting students and foreign diplomats. Officials said they could only recall the room being used once this way for a public event in the last few years -for the Pope. In his speech, Trudeau said Canada wants to revitalize its entire relationship with the world body and he underlined peacekeeping as an area where Canada can have an impact. "We are determined to revitalize Canada's historic role as a key contributor to United Nations peacekeeping, in addition to helping advance current reform efforts," he said. "And Canada will increase its engagement with peace operations, not just by making available our military, police, and specialized expertise, but also by supporting the civilian institutions that prevent conflict, bring stability to fragile states, and help societies recover in the aftermath of crisis. He repeated his oft-made claim that Canada is back as a player on the UN stage. "It's time. It is time for Canada to step up once again." Foreign Affairs Minister Stephane Dion said later that the government is still considering possibilities for peacekeeping missions. Canadian Press (Chronicle Herald, A9, Whitehorse Daily Star, Waterloo Regional Record, Hamilton Spectator, Ottawa Citizen, Telegraph-Juuornal, Times & Transcript, Daily Gleanor) National Post (London Free Press) ; National Post, A4

* **Canadian causes stir at UN with drugs speech**
The Liberal government used its first foray into the global anti-narcotics arena this week to signal a clear shift from the war on drugs philosophy, promising more safe-injection sites, promoting "harm reduction" and touting its plan to legalize marijuana. The speech by Hilary Geller, an assistant deputy minister of

health, caused a stir at the generally staid Commission on Narcotic Drugs conference in Vienna, observers said. The audience of government and non-governmental organization officials from around the world "erupted in applause" midway through the address and gave a prolonged ovation at the end, said Jason Nickerson, an Ottawa-based researcher who is attending the meeting. The talk not only contrasted with the Stephen Harper government's international stance on drugs, but stood out from the cautious pronouncements most other nations made, said the Bruyère Research Institute scientist, who favours more liberal policies. "There are some countries here that are coming out and saying important, progressive things," he said. "But it's certainly not as explicit as what Canada is saying." A Conservative opposition critic had a different reaction, sounding the alarm about Geller's prediction of more government sanctioned injection sites - where opioid users can use illicit intravenous drugs under a nurse's supervision. While the Supreme Court of Canada ruled such sites legal, the Conservatives passed legislation requiring extensive public consultations and other measures before they could be set up, said Rob Nicholson, the party's justice critic. "Drugs that are used at these injection sites, mostly heroin, are dangerous and addictive and they kill Canadians," said the former justice minister. "I disagree with the idea they are safe. There's nothing safe about taking heroin." Nicholson also stressed that the Conservatives invested hundreds of millions of dollars in drug-abuse treatment and prevention. Windsor Star, N3 (Edmonton Journal, N3, StarPhoenix, Calgary Herald, Gazette; National Post

INTERNATIONAL

*** Hunt on for pair in raid linked to Paris attacks**

Belgian investigators were hunting Wednesday for two suspects who fled an apartment linked to the Nov. 13 attacks in Paris, one day after a police sniper killed a gunman holed up inside and authorities found a stock of ammunition and an Islamic State flag, officials said. Prosecutors on Wednesday released without charges two men they held in the wake of Tuesday's joint French-Belgian raid in Brussels, leaving the hunt on for two unidentified suspects. The dead man was identified as Mohamed Belkaid, an Algerian living illegally in Belgium, said Thierry Werts, a prosecutor. Belkaid, 35, was shot to death by a police sniper as he prepared to fire on police from a window, Werts said. A Kalashnikov was found by his body, as well as a book on Salafism. Inside the apartment, police found the banner of the Islamic State extremist group as well as 11 Kalashnikov loaders and a large quantity of ammunition. The anti-terror raid was linked to the Nov. 13 gun-and-bombing attacks in Paris that left 130 people dead. The Islamic State group claimed responsibility for the attacks, in which Belgian citizens played key roles. Among the fugitives is Belgian Salah Abdeslam, who fled the Paris attacks that night, slipped into Brussels and has not been seen since. The Associated Press (Record, A6, National Post, Whig-Standard)

*** EU leaders push on with contested Turkey migrant plan**

European Union leaders will push ahead Thursday with contested plans to send tens of thousands of migrants back to Turkey amid deep divisions over how to manage Europe's biggest refugee emergency in decades. With European unity fraying in the face of more than 1 million migrant arrivals over the last year, Turkey -- the source of most refugees heading to Greece -- is seen as the key partner to contain the influx. The U.N. refugee agency has reservations about asylum standards in Turkey and rights groups are concerned over Ankara's crackdown on the media and its bloody conflict with Kurdish rebels. The EU, however, feels it has no better option. "How are you going to help Greece without having an agreement with Turkey to handle the issue? Do you really want to condemn Greece to become a refugee camp for the rest of Europe?" EU Commission vice-president Frans Timmermans said, on the eve of the two-day summit in Brussels. Destabilized by the passage of hundreds of thousands of migrants, countries in the Balkans have begun to tighten border controls, with Macedonia north of Greece having all but locked the gates. Thousands have been camped on the Greek side desperately hoping to move on toward Germany or Scandinavia. CTV News

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PS.PSPMediaCentre/CentredesmediasPSP.SP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
October 4, 2016 / le 4 octobre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Spies use C-51 on detained Canadians
Canada's spy agency is using controversial powers under the C-51 anti-terrorism legislation to gather intelligence from Canadians held in foreign prisons, a newly released memo reveals. Amnesty International Canada and the New Democratic Party are expressing concerns about the potential pitfalls of the previously unknown information-sharing arrangement between the Canadian Security Intelligence Service and Global Affairs Canada. The spy service and Global Affairs made the sharing deal this year through the Security of Canada Information Sharing Act, part of the omnibus security legislation known as C-51, says a secret memo to **Public Safety Minister Ralph Goodale** from Michel Coulombe, CSIS director. The provisions, ushered in by the previous Conservative government, expanded the exchange

of federally held information about activity that "undermines the security of Canada." "Information collected by (Global Affairs Canada) through the provision of consular services can be directly relevant to investigations of threats to the security of Canada," says the heavily censored CSIS memo, obtained by The Canadian Press under the Access to Information Act. However, it is often difficult for consular officials to determine when a detained Canadian has been tortured and what impact that has on the information they may be sharing, said Alex Neve, secretary general of Amnesty International Canada. Canadian Press (National Post, A5, Times & Transcript, Ottawa Citizen, Edmonton Journal, Calgary Herald, Vancouver Sun, Times Colonist, London Free Press, Red Deer Advocate); La Presse Canadienne (Le Droit, L'Acadie Nouvelle); SputnikNews.com

TOP STORIES / MANCHETTES

*** Bill C-51: Less Free Speech, Undermines De-radicalization**
An opinion piece written by Micheal Vonn, policy director of the BC Civil Liberties Association states, "The Anti-Terrorism Act passed by the Conservative federal government last year — Bill C-51 — created a new law criminalizing speech that "advocates or promotes the commission of terrorism offences in general." Unlike the hate propaganda offence that it is based on, the new offence contains no exemptions for private conversations or provisions for legal defences (such as a public interest defence). The federal government's national security consultation Green Paper offers a suggestion as to what "terrorism offences in general" might mean, but the Canadian legal community has no clear agreement on how courts would interpret this troublingly open-ended language. Presumably "terrorism offences in general" goes beyond the already broad definition of "terrorist activity" set out in Section 83.01 of the Criminal Code. Leading legal scholars in the field note "this is a potentially infinite number of offences." ... The government Green Paper describes a model in which law enforcement plays an important role in supporting individuals at risk of radicalization to violence and responding if individuals progress to criminal activities. Community capacity-building could include "mentorship, multi-agency interventions and training and support for front-line intervention work (such as youth workers, corrections and parole officers, social service providers, faith leaders and mental health practitioners)." Many countries are stressing the importance of measures to counter radicalization to violence. Unfortunately, we really don't know at this point which measures are effective. So far, the limited research and the experience of other countries have mostly served to show us what is not effective." TheTyee.ca (iPolitics)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Government wildfire relief funding for Fort McMurray to end Oct. 31**
Emergency funding from the Alberta government to help evacuees following the Fort McMurray wildfire is coming to an end. The province says almost $100 million has been paid out to 96,000 people who were forced to flee their homes in the Wood Buffalo area in early May. The money was intended to cover immediate housing needs, to help with day-to-day purchases and to limit outof-pocket expenses. But longer-term supports now are available to help fire victims rebuild, so the government is ending the emergency payment program on Oct. Eligible Albertans who have not yet applied for wildfire relief funding have until the end of the month to do so. Postmedia Network (Red Deer Advocate, A7; Edmonton Journal); CBC News

*** Ontario OK ' s Windsor-area disaster relief**
The province has declared parts of Windsor, Tecumseh and Lakeshore disaster areas and activated a relief program to help residents affected by last week's flooding. Municipal Affairs Minister Bill Mauro visited the area Monday to announce relief measures after the region received a month ' s worth of rain in two days, flooding many streets and homes." This morning I signed off and we have activated the ministry's and the province's disaster relief programs," Mauro said at a news conference "People are now eligible to apply to one of the two disaster programs that the province has." (...) According to Mauro, home-owners now will be able to apply for provincial assistance with the cost of essentials destroyed by the floods beyond what their insurer will cover. Postmedia Network (London Free Press, Windsor Star)

*** Flooding repairs to exceed $25M**
Unlike the August tornadoes in Windsor and LaSalle, last week's flooding in Windsor and Tecumseh will make it onto a list of 2016 Canadian insurance catastrophes. Damages stemming from the most recent flooding will take weeks to calculate, but a spokeswoman for a company that keeps track of the nation's costliest disasters said it will certainly exceed $25 million. That's the minimum threshold at which individual insurable weather events are reported by CatIQ (Catastrophe, Indices and Quantification Inc.) to the Insurance Bureau of Canada based on surveys of individual insurers. Windsor Star, A3

*** Keeping an eye on Hurricane Matthew**
Environment Canada and the Canadian Hurricane Centre in Dartmouth, N.S., are keeping a close eye on hurricane Matthew. Meteorologist Linda Libby said Monday it's far too early to say if it will have an impact on P.E.I., and if it does it would likely hit towards the end of the upcoming Thanksgiving holiday weekend. Heavy rains from the outer bands of hurricane Matthew drenched Jamaica and Haiti on Monday, flooding the streets and sending many people to emergency shelters as the Category 4 storm approached the two countries. Matthew had sustained winds of 220 kilometres per hour as it moved north, up from 210 kilometres per hour earlier in the day. "We are most assuredly keeping an eye on this thing and were before it developed," Libby said, noting that the Canadian Hurricane Centre was preparing to issue an advisory simply stating that it was officially watching the system (…) Right now, Environment Canada simply wants to make people aware that the track could take **hurricane** Matthew into Atlantic **Canada** so people can pay close attention to the forecast. TC Media (Guardian); Associated Press (Times Colonist)

*** Des Canadiens sur un pied d'alerte**
Les étalages vides des supermarchés de Port-au-Prince témoignent de l'état d'urgence qui commence à se faire sentir depuis dimanche soir, en Haïti, à quelques heures de l'arrivée de l'ouragan Matthew. Avec plus de 3000 personnes déployées sur le terrain, la Croix-Rouge haïtienne travaille actuellement à sensibiliser les populations les plus vulnérables face au réel danger que représente l'ouragan (…) Lundi après-midi, la Croix-Rouge canadienne n'avait toujours pas reçu de demande officielle afin d'appuyer l'équipe locale. «Tout le monde est en stand-by et nous sommes prêts à intervenir, a assuré Brigitte Gaillis, porte-parole de l'organisme en Haïti. « Nous avons un système de réponse aux urgences si nos collègues haïtiens n'ont pas la capacité de répondre. » Presse Canadienne (Nouveliste, Le Devoir)

*** Search continues for Shalyn Sabine**
Summerside police have not yet located a woman who hasn't been seen since leaving Prince County Hospital early Monday morning. A ground search continued into the evening for Shalyn Sabine (…) Members of P.E.I. Ground Search and Rescue, as well as the RCMP, were in the area of the hospital, spending the day and into the evening searching a nearby park and woods for any signs of Sabine. Guardian, A3

*** Arctic cruise boom poses conundrum for Canada's indigenous communities**
Authorities in the northern Canadian territory of Nunavut are considering new regulations on marine tourism after the first successful voyage of a mammoth luxury liner through the North-West Passage. Nearly three football fields in length, the 13-deck Crystal Serenity docked in Manhattan last month after a 32-day voyage that saw it become the largest cruise ship to sail the once impenetrable passage (…) "Now that marine tourism is a significant and steadily growing presence in the territory," said Bernie MacIsaac of Nunavut's department of economic development, "it is important that new legislation be created that will effectively regulate the sector." (…) Many Inuit want to see more stringent controls of marine traffic in the Arctic, said Eegeesiak: "We're all worried about the potential for a disaster that will affect our livelihood, our food sources." The risks facing the industry were laid bare in 2010, after a small cruise ship carrying 128 passengers struck an uncharted rock shelf in the North-West Passage. It took 40 hours for a Canadian icebreaker to reach and evacuate the ship's passengers. (…)The idea of mass tourism in the Arctic, said Eegeesiak, is woefully out of step with the region's glaring lack of infrastructure and limited capacity for search and rescue. Guardian (UK)

*** Lacombe Firefighters Association donating more equipment to Paraguay**
Central Alberta firefighters have a hand in saving lives a continent away. Lacombe Firefighters Association began a fire engine donation campaign for Paraguay with a single truck last year. It was a life

changer for firefighters in the community of Caazapá, who had no fire truck and little other equipment to tackle fires. A second was shipped to the South American this past summer and two more pumpers have already been lined up as future donations. Besides the trucks, crates of donated equipment from fire departments around the province have been sent to grateful colleagues in Paraguay. Red Deer Advocate, A1, A8

*** 'Guardians' need $500m to watch over native lands**
The Trudeau government is being pushed to invest $500 million over five years on a 1,600-member national "Guardians" team to patrol, and assert aboriginal sovereignty in, the vast traditional territory of Canada's First Nations. Modelled in part after a land stewardship initiative by B.C.'s Haida Nation on the north coast, the initiative would help boost economies and build leadership in remote communities, members of the Indigenous Leadership Initiative said at a news conference Monday. The Guardians could operate as land managers, planners, community consultation officers, emergency response officers and even fisheries management officers, they said. But the hired stewards could also play a role in peacefully asserting sovereignty on traditional territories that are not yet part of settled land claims. Postmedia Network (The Province, A4; Vancouver Sun; National Post)

*** Rail firm great news, but strings attached**
An opinion piece states, "While an official statement might be weeks away, an American company has already announced on its website its intention to restore some of the lustre to Metro Moncton that our community has not seen since 1982. That year, the CN Rail Shops shut down, resulting in the loss of thousands of jobs. While Miami-based ARS Rolling Stock doesn't aim to quite bring Metro back to glory days, it aims for up to 700 well-paid employees (…)The new company appears focused on manufacturing, mainly grain hopper cars and the new, safer petroleum tankers demanded since the Lac Megantic rail disaster in July of 2013, in which older tank cars derailed and exploded, killing 47 people. Times & Transcript, A6

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Bill C-51: Less Free Speech, Undermines De-radicalization**
An opinion piece written by Micheal Vonn, policy director of the BC Civil Liberties Association states, "The Anti-Terrorism Act passed by the Conservative federal government last year — Bill C-51 — created a new law criminalizing speech that "advocates or promotes the commission of terrorism offences in general." Unlike the hate propaganda offence that it is based on, the new offence contains no exemptions for private conversations or provisions for legal defences (such as a public interest defence). The federal government's national security consultation Green Paper offers a suggestion as to what "terrorism offences in general" might mean, but the Canadian legal community has no clear agreement on how courts would interpret this troublingly open-ended language. Presumably "terrorism offences in general" goes beyond the already broad definition of "terrorist activity" set out in Section 83.01 of the Criminal Code. Leading legal scholars in the field note "this is a potentially infinite number of offences." … The government Green Paper describes a model in which law enforcement plays an important role in supporting individuals at risk of radicalization to violence and responding if individuals progress to criminal activities. Community capacity-building could include "mentorship, multi-agency interventions and training and support for front-line intervention work (such as youth workers, corrections and parole officers, social service providers, faith leaders and mental health practitioners)." Many countries are stressing the importance of measures to counter radicalization to violence. Unfortunately, we really don't know at this point which measures are effective. So far, the limited research and the experience of other countries have mostly served to show us what is not effective." TheTyee.ca (iPolitics)

*** Vie privée - Moderniser les outils du Commissaire**
Une pièce d'opinion dit, « Dans son récent rapport annuel, le Commissaire à la vie privée explique la nécessité de " moderniser les outils du XXe siècle ". Il a raison : les lois sur la protection des renseignements personnels ont été mises en place avant Internet. Dans l'univers en réseau, le défi est de protéger la capacité des individus de contrôler l'information relevant de leur vie privée. Mais il importe aussi de garantir le fonctionnement des espaces publics, ces lieux désormais virtuels, dans lesquels les autres ont le droit de nous critiquer ou de connaître nos faits et gestes à caractère public. Évidemment, il faut regarder de très près les dispositions des lois mises en place afin de lutter contre le terrorisme. Les pouvoirs accrus accordés aux forces de sécurité doivent être balisés et surtout leur exercice surveillé efficacement. Le Commissaire préconise de réviser les lois sur la protection des renseignements personnels qui relèvent d'un contexte informationnel qui n'existe plus. » (…) Alors que le pays se prépare à affronter le pire, les Canadiens en Haïti sont invités à s'inscrire sur le site du gouvernement du Canada avec leurs coordonnées complètes afin d'être rejoints plus facilement en cas de désastre. Actuellement, environ 2000 Canadiens se sont inscrits sur le site. Le Devoir

*** @Kady's Watchlist for Oct. 4 – Senators, prepare to be… modernized**
Also on the Hill media circuit this morning: Later this afternoon, Privacy Commissioner Daniel Therrien and University of Ottawa visiting professor Wesley Wark will provide their respective perspectives on the state of Canada's national security framework at **Public Safety**. OttawaCitizen.com

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Contractors in alleged paving scam arrested, ordered deported
Four people have been ordered removed from Canada after police warned the public about an alleged paving scam. The Canada border services agency and Ottawa police's fraud unit teamed up to arrest the quartet on Sept. 24 and seized $70,000 in cash four days after police warned the public to beware of door-to-door paving contractors with Irish accents who would quote an inexpensive price to repave a driveway or lane, only to do the work and then demand more money. The CBSA said Monday that the four foreign nationals suspected of being involved were working without a permit. Ottawa Sun, A3 (Ottawa Citizen); * CBC News

Union calls for review of temporary foreign workers program
A union is calling for a review of the impact the temporary foreign worker program has had on the construction industry in Western Canada, saying a federal government report ignored the issue. The Western Canadian arm of the Labourers' International Union of North America says a report released last month by a House of Commons committee fell short, and failed even to acknowledge a 123-page submission from the union. Mark Olsen, the manager of the union's regional office, said on Monday that concerns include the effect of the temporary foreign worker program on the prevailing wage and how it is enforced. "Companies should have to pay whatever the going rate is for construction in a given area, because if they're allowed to advertise at a much lower rate and they're allowed to pay at a much lower rate, then they won't have as many Canadians applying, maybe none," he said in an interview. "And on top of that, they will be depressing the wage rates of companies that are competing for the same work, and workers that are competing for the same work." Mr. Olsen said that in some instances, a Canadian worker could be paid significantly more than a temporary foreign worker for the same task, which is discriminatory. Tom Sigurdson, executive director of the B.C. and Yukon Territory Building and Construction Trades Council, said his organization supports the union's call for a separate review. Globe and Mail, S1

Immigration detention of children, families must end
An opinion piece states, "As a psychiatrist who works with children and families, I am not supposed to cry. As a researcher, I strive to engage but remain an observer. Nevertheless, while sitting across from two parents incarcerated in an immigration holding centre, as they described the agony of being separated from their two young daughters, I felt my throat tighten and tears roll down my cheeks. Their pain filled the small interview room; my job could not insulate me. The parents told me how they had tried to convince their girls the reason they had not seen them in a month was that the parents were both working

overtime. But the Canadian-born children, who were staying with relatives so the girls would not be detained alongside their parents, knew something was wrong and were frightened. They had seen their parents taken away in handcuffs. "We are never apart," wept the girls' mother. The father, defeated and hopeless, told me with shame that he thought of suicide because he could not bear what the family was living through and his feelings of powerlessness. This was one of hundreds of families who face immigration detention in Canada each year. What happens to young children when their parents are sent to immigration jails? Luckier ones can stay with relatives. Some go into the child welfare system. Others join their parents in detention facilities. Our research shows all these scenarios have negative consequences for children's mental health. When separated from their parents, children - who have often lived through war and trauma in their country of origin - deteriorate. Being incarcerated alongside their parents is no better. Some children stop eating, others stop talking, and most have sleep difficulties and show signs of depression, anxiety or post-traumatic symptoms." Toronto Star, A11

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Cyber Security Awareness Month isn't only for consumers, says Canadian expert**
Cyber Security Awareness Month is often seen as a burst of news, videos and blogs aimed at consumers. But CSOs and infosec teams also have a role to play during October to ensure their employees are keenly aware of online dangers. ITWorldCanada.ca

*** WikiLeaks fête une décennie d'existence sous le feu des critiques**
WikiLeaks fête mardi ses dix ans en se targuant d'avoir lancé le phénomène des plateformes internet de divulgation de documents secrets et son controversé fondateur Julian Assange a promis de poursuivre son travail malgré les vives critiques (...) Dix ans après sa fondation, le site voit son image de plus en plus écornée par ceux qui l'accusent d'être manipulé par des gouvernements ou des partis politiques et de manquer de discernement dans ses divulgations. Julien Assange se voit accusé de servir les intérêts de la Russie, voire de recycler des documents fournis par Moscou, ou de «rouler» pour Donald Trump en vue de l'élection présidentielle américaine (...)À la veille de l'ouverture de la convention démocrate américaine fin juillet, WikiLeaks avait publié quelque 20 000 emails internes au parti démocrate révélant un possible biais de ses responsables en faveur d'Hillary Clinton pendant la campagne des primaires. M. Assange avait refusé de révéler comment WikiLeaks avait obtenu les messages piratés. La Russie est soupçonnée par de nombreux experts et responsables d'en être l'instigatrice --ce que n'a pas écarté non plus le président Barack Obama-- mais Moscou a démenti toute intervention. Tirant son nom de «wiki», en référence à l'idéal d'ouverture et d'auto-gestion par les usagers du site Wikipedia, et de l'anglais «leaks» (fuites), l'organisation non gouvernementale a publié en une décennie plus de 10 millions de documents fournis par des lanceurs d'alerte. Ces dernières années, l'exemple de WikiLeaks a été largement suivi, par l'informaticien Edward Snowden en particulier, qui a permis à la presse de révéler l'étendue des activités de surveillance de l'Agence de sécurité nationale (NSA) en matière de télécommunications, y compris pour espionner les conversations de dirigeants de pays alliés. AFP (Journal de Québec, Journal de Montréal)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Two suspected Vikings biker gang members arrested in raids still behind bars
Two suspected outlaw biker gang members are still behind bars as their lawyers attempt to make progress with their cases. Vince Aloysius Leonard Sr., 58, and Wayne Johnson, 57, were back in provincial court in St. John's Monday. Mike King, who represented Leonard Sr. in the courtroom, told Judge Mike Madden that his firm is still in the process of finalizing the retainer for Leonard Sr. He requested the case be postponed until Oct. 25 to work that out. Johnson's lawyer, Mark Gruchy, told the judge that Johnson wants a bail hearing heard as soon as possible. He said he had just received a substantial amount of information from the police evidence package, which he would like to review with his client. Gruchy and Crown prosecutor Trevor Bridger agreed to have the two-day bail hearing begin Wednesday. Due to scheduling issues, the second day won't be heard until Oct. 10. Leonard Sr. and Johnson were two of eight men arrested last week by RCMP officers as part of a two-year investigation

dubbed Project Bombard, an RCMP operation, with assistance from the Royal Newfoundland Constabulary, which delved into the criminal activities of the Vikings Motorcycle Club and the murder of Dale Porter in North River. Telegram, A1, A4

* **Quick-thinking Mounties use cruiser seat as flotation device to rescue man from Peace River**
Onlookers who watched as quick-thinking Mounties saved a man from drowning Saturday in the Peace River were on the edge of their seats. The two rescuers were, too. Just after 9 a.m., constables Brandon Goudey and Tim Stevens of the Peace Regional RCMP detachment received a call on the radio about a man in distress in the river as it flowed through the northwestern Alberta community's downtown. Along with EMS crews and firefighters, the officers tried to encourage the man to swim to shore. A rescue boat was on its way, but when it became clear the man was not getting closer to shore and beginning to lose the struggle, the two officers decided to improvise. Goudey said he remembered a lesson from police training that helped save the day - that the back-seat cushion of a Ford Crown Victoria can float. "I guess I was lucky that I remembered," Goudey said. Immediately after they arrived, Goudey asked his partner to pull the seat from the cruiser in case they needed it. "We noticed that he was struggling to stay above water," Goudey said. "At one point, we lost sight of him for a little bit." They stripped off their heavy equipment belts and both jumped in, using the cushion like a pool float and kicking their way to the drowning man. The water was frigid and flowing about 12 kilometres per hour. Edmonton Journal (Edmonton Sun)

* **Protest in Surrey addresses 'theft' of homeless belongings by RCMP**
A few dozen people marched the area around Surrey City Hall today protesting what they call theft of their belongings by RCMP and bylaw officers. Alliance Against Displacement organizer Dave Biewert says it happens on a regular basis on the strip near 135A Street and 106 Avenue. "Every morning at about 8:30 a.m. the RCMP and the bylaw officers roll onto the strip and make sure everybody tears down their tent, packs up their stuff and makes it movable. And if people aren't with their belongings, or are if they are slow at it, they will take their stuff and throw it into a truck." Surrey Bylaw Manager Jas Rehal says officers give people ample time to take their belongings and move off of the sidewalk. Surrey RCMP has not responded to our request for an interview. AM730.ca

* **Self-described millionaire found beaten in Brampton ditch charged with fraud**
A self-described millionaire and business coach found beaten and half-naked in a Brampton, Ont., ditch earlier this year has been charged with fraud. Reza Mokhtarian has been charged with one count of fraud against the public over $5,000 in connection with an alleged breach of the Criminal Code between July 1, 2013, and Dec. 31, 2015, the Ontario Securities Commission said in a release Friday. In February, Mokhtarian identified himself as the man found in the ditch, claiming on Facebook that his assailants were competitors. The Mississauga, Ont., man said he was dragged into a van after playing a game of soccer with friends before being held captive in his home for 15 hours by four "large individuals." He alleged another three men guarded the exits to his home, though details were murky because, he said, he had a concussion at the time. (...) The release from the OSC says the charges followed an investigation by the commission's joint serious offences team, which includes the RCMP's financial crime program and Ontario Provincial Police's anti-rackets branch. CBC News

* **Police practice skills with harbour side hostage situation**
Heavily armed police practiced a simulated hostage situation at the harbour in St. John's on Monday. Nicknamed Port Risk, the exercise in the pouring rain tested the skills of various enforcement and rescue groups. The Royal Newfoundland Constabulary's tactics and rescue unit, along with RCMP, Port Authority, Canadian Border Services Agency, Newfoundland and Labrador Search and Rescue Association and Suncor Energy all participated. In the scenario, people entered the harbour and disembarked from a boat before taking a hostage. CBC.ca; The Telegram

* **Kamloops ex-Mountie expected to plead guilty to trafficking cocaine**
A former high-profile Kamloops police officer accused of trafficking cocaine while still employed by the RCMP last summer is expected to enter a plea later this week. Randi Love did not appear in person on Monday for a brief hearing in Kamloops provincial court, at which her arraignment was set for Thursday. Her lawyer, Brad Smith, appeared on her behalf. The 40-year-old is facing three counts of trafficking

cocaine stemming from a trio of alleged incidents on separate dates in June 2015. At the time, Love was on injury leave from her job as an RCMP constable. Police launched an investigation into Love in the weeks that followed. She submitted her resignation papers to the national police force in October 2015. Love made headlines in 2013 when she testified at the fraud trial of her former boyfriend, then-RCMP Const. Trent Wessner, who was convicted of bilking Costco out of $400 based largely on Love's testimony. Wessner left policing following the conviction. In 2008, Love worked as the media-relations officer at the Kamloops RCMP detachment, acting as the de facto face of the city's police. Vancouver Sun (The Province)

*** Crash kills officer facing 34 charges**
What was described as a dark chapter in the history of the Winnipeg Police Service came to an abrupt end Monday morning when the officer charged with dozens of criminal offences last month died after his pickup truck slammed head on into the front of a gravel truck. Little more than two weeks after Const. Trent Milan, 42, an 18-year veteran of the force, was charged with 34 offences, including breach of trust, attempting to obstruct justice, possession of prohibited weapons and possession of various drugs for the purpose of trafficking, he was pronounced dead inside his heavily damaged pickup truck after it came to a rest on its side in a ditch on Garven Road at about 11:30 a.m. Monday. Milan's death occurred before he made his first court appearance on the charges. He wasn't set to appear in court until Nov. 1 on the weapons-related charges and Nov. 10 on the drug charges. He had been released on a promise to appear in court. A Manitoba Justice source said the Crown had recently told Milan and his lawyer that if the officer agreed to a plea bargain, he would have to accept a prison sentence of six years. During a brief press conference held just down the road from the scene of the collision, RCMP spokeswoman Tara Seel would not confirm whether Milan intentionally turned his pickup into the path of the gravel truck. The gravel truck driver suffered minor injuries in the collision. "It appears the eastbound pickup truck collided with the westbound gravel truck," she said. "The driver of the pickup truck was not ejected... He was pronounced dead at the scene." Winnipeg Free Press, A3; Winnipeg Sun

*** A year after approval, new RCMP officers may finally be hired for Kamloops**
More than one year after the City of Kamloops approved funding for 10 new officers, those positions may finally be filled, bringing staffing levels in the local detachment to the highest they've been in more than two years. Kamloops RCMP spokesperson Cpl. Jodi Shelkie says the additional funding will take the detachment to 130 officers from 120. "For the past 16 months we have been working with E Division Staffing to have these 10 new positions filled," Shelkie says. She says the funding was approved in May of last year. InfoTel.ca

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Man who threw book at judge back in prison
A violent offender who made headlines in New Brunswick for throwing a Criminal Code book at a judge and escaping custody, both in 2010, has lost his legal fight over what he complained was a deprivation of his liberty while serving his prison time for armed robbery. Peter Monteith, who has an extensive criminal history and been deemed a high risk to reoffend, had been living in Saint John when his parole was suspended in August and he was sent to isolation at Atlantic Institution, a maximum-security prison in Renous. Justice Hugh McLellan, with the Court of Queen's Bench in Saint John, ruled earlier this month that the Parole Board of Canada and Correctional Service of Canada's handling of Peter Monteith's case was "regrettable but also reasonable." Monteith had been transferred from a maximum security prison to Parrtown Community Correctional Centre, a federal halfway house in Saint John, on June 15, according to court documents obtained by Brunswick News. There were several conditions tied to his parole. He had to return to the facility nightly, abstain from alcohol and non-prescribed drugs, participate in drug and violence counselling and take all prescribed medication. According to the parole board, Monteith had to be segregated nine times, for lengthy periods, in prison due to his behaviour. He racked up 26 charges in custody and was involved with other institutional incidents. He was called "assaultive, aggressive and unmanageable." Telegraph-Journal, B1

Inquest called in 2010 death of inmate at Shepody Healing Centre

Glen Edward Wareham, 28, of New Waterford, N.S., died 2010 while an inmate in mental health facility. A inquest has been called into the death of an inmate at the Shepody Healing Centre in Dorchester in 2010. Glen Edward Wareham, 28, of New Waterford, N.S., died on April 29, 2010. The Shepody Healing Centre is a Correctional Service of Canada facility for prisoners with mental health issues. Chief coroner Gregory Forestell announced Monday that an inquest into Wareham's death will begin Oct. 17 at Crandall University in Moncton. Two weeks have been set aside for the inquest. Forestell will preside over the inquest and a jury will hear testimony from subpoenaed witnesses to determine the facts around Wareham's death. CBC News

Associate of accused in Stacey Adams murder has a spotty past
A known associate of the man accused of killing Stacey Adams has a history of deception and drug crimes, parole board records show. Parole Board of Canada records show Ryan Belanger was ordered this month to stay on day parole until early 2017, after breaking several conditions during his first six-month stint. Belanger and his brother Jeff were cocaine traffickers, according to appeal court documents. Their known associate was Steven Skinner — who was caught in Venezuela on an international warrant and now awaits extradition to face charges of the second-degree murder of Adams. Adams, a 20-year-old man with no criminal record and a child on the way, was found shot in a car in front of a house Ryan Belanger was listed as owning in 2011. Chronicle Herald; 1

* **Advocates rally for alternative jails**
An alternative correctional facility for indigenous people who have been convicted of minor offences could be effective in the Thunder Bay area, based on positive experiences in other provinces, like Saskatchewan, local advocates argue. “There are examples of these facilities in western Canada, which are an alternative to jail and in the spirit of (an aboriginal) healing lodge,” Thunder Bay’s Moffat Makuto said Monday. (…) Wednesday’s meeting is also to include a presentation from Correctional Services of Canada deputy commissioner Peter Linkletter. Kevin Haynen, the acting executive director of Thunder Bay’s John Howard Society branch, said he planned to attend to get more information. “We’re always looking to learn something new in our field,” said Haynen. Chronicle Herald

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

* **Health Canada OK's non-prescription nasal spray overdose antidote: Needle-free nasal spray easier to administer**
Canadians will now be able to acquire naloxone nasal spray without a prescription, Health Canada says. Health Minister Jane Philpott authorized the nasal spray, which works to temporarily reverse a potentially fatal opioid overdose, after an expedited review, the department said in a release on Monday. The needle-free nasal spray is easy to administer and ensures that anyone can reverse an opioid overdose and save lives within a few minutes, said Dublin-based Adapt Pharma. The company intends to market the product in Canada. Health Canada said more information on when the newly approved product will be available will be provided "in the near future." Health Canada says the nasal spray's manufacturer can now take the steps needed to officially bring the product to market in Canada. Until then, the U.S.-approved product will continue to be available in Canada to avoid interruption in supply. The interim order called the authorization "an emergency public health measure in response to the current opioid crisis." CBC News; CTV News

* **'Gun culture' arrives in Ottawa, as city reaches 51 shootings**
As the city once again grapples with uncharted levels of gun violence in its borders, police now say they are seeing a growth in non-gang-related shootings and that "gun culture" has come to quiet Ottawa. Acting Supt. Chris Renwick told Monday evening's Crime Prevention Ottawa board meeting that police are seeing more gunfire that isn't the result of gangs. "It tells us that the gun culture has arrived in Ottawa," Renwick said. "It's a problem we're going to be dealing with it.'" Renwick told the Citizen that nearly half of the 51 shootings on record for 2016 - the most the city has seen in any one year - are gang-related. But non-gang related shootings have doubled from just eight last year to 15 in a year that is still three months away from being over. Of the 13 homicides in Ottawa to date - also nearing record levels -

10 have been the result of gunfire, and five of those have been gang-related. Renwick refused to answer questions on whether police would increase the number of officers doing anti-gun and anti-gang work, saying instead that "it's counterproductive to get into details of where investigative resources are placed." "That number fluctuates depending on investigations," he said. Yet the same gang strategy report received by the CPO board Monday offered a glimpse of what happened when the guns and gangs unit was temporarily boosted. Ottawa Citizen

* **Moncton personal trainer offers anti-bully program for kids**
Growing up in Dakar, Senegal, Issa Seck learned early in life what it's like to be bullied. Today, he's a martial arts fighter and personal trainer in Moncton who is about to launch a new program designed to teach kids how to stand up to bullies and get the most out of life. "As human beings, we want to be part of the pack. And if you want to get rid of someone and get them out of the pack because of the way they talk or they look, that is social bullying, that is social exclusion," said Seck, 36, in an interview at FitCamp90, a gym and fitness centre on Halifax Street in Moncton. This month, he is launching a new Bullyproof program, an eight-session course designed for children aged five to 12. The course deals with different types of bullying and ways to stand up to bullies and the benefits of good nutrition, exercise and a positive attitude toward life. The first course will begin Oct. 17 with 15 children in the first group. The fee is $150. Seck is hopeful his Bullyproof program will eventually be supported by police, schools and social assistance agencies that can sponsor children whose families cannot afford the fee. Seck said bullying, in all its forms -peer pressure, verbal attacks, physical attacks and cyberbullying - can have long-lasting effects on an individual's self-esteem. He said he was bullied at school as a youngster. Times & Transcript, A4

* **Parents blamed for kids' cyberbullying: Expert suggests mom and dad's poor social behaviour sets bad example**
Even as a mom of elementary schoolchildren, I was completely engrossed by the #Being13: Inside the Secret World of Teens documentary on CNN. The kids featured in the documentary made their vexing online behaviour seem normal, and that gnawed at me for weeks. But what really left an impression on me was the parents near the end of the special, who shared their frustrations about their teens' online behaviour and excessive use of technology. Many said that their kids may have a real addiction to social media. During on-camera discussions with parents, documentary host Anderson Cooper displayed one teen's Instagram post, which belittled women. It left the boy's father shocked and visibly distressed. Why do kids engage in bullying or inappropriate behaviour online? The answer could lie in their parents. Robert Faris, an associate professor of sociology at the University of California, Davis, is one of the people behind the study that was the foundation of #Being13. He believes that certain parental behaviours could inadvertently promote aggression in kids. Parents who set poor social priorities, or don't encourage healthy social relationships, could be unintentionally playing a role in their teens' disturbing online activity, he said in an interview. Faris dispels the notion that most kids directly model behaviours online that they witness at home, dismissing the idea that many kids cyberbully because their parents engage in similar actions. However, he does suspect that parents' priorities could affect how their kids behave online. Washington Post, C4 (Red Deer Advocate)

* **Activists rewriting history of West End prostitution**
An editorial piece states, "Did a gang of racist vigilantes drive sex workers from the safety of Vancouver's West End into the dangerous streets of the Downtown Eastside, where they were murdered by sexual predators? This is the fevered concoction put forward by longtime activists Jamie Lee Hamilton and University of B.C. professor Becky Ross, who've successfully pushed for a memorial in the West End to commemorate the sex workers who lost their lives as a result of their expulsion from the West End in 1984. The most disturbing element of this story is that West End residents, Vancouver city council and the late B.C. Supreme Court Justice Allan McEachern have blood on their hands for having forced the young prostitutes out of the West End and into the hands of Robert Pickton. Nobody has tracked the whereabouts of the sex workers since they were ordered out of the West End by McEachern's injunction in 1984 and Hamilton and Ross cannot provide evidence of this allegation. Their allegation makes for a gripping story but it is nothing more than conjecture. What we do know from eyewitness accounts is the male sex workers simply relocated a few blocks outside the area covered by the injunction to Yaletown and many of the female sex workers moved to Mount Pleasant. In time, some of the female prostitutes

moved to the Downtown Eastside, but there is no evidence they were murdered. The assertion by Hamilton and Ross that vigilantes drove the sex workers from the West End is equally disturbing to those of us who lived in the West End in the 1980s. The West End residents most affected by the noise and squalor of the sex trade in their residential streets formed a citizens' group called." The Province

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Vancouver candlelight vigil for missing women one of hundreds nationwide**
Vancouver advocates for missing and murdered women are holding a solemn event in the Downtown Eastside, a neighbourhood where many have gone missing. The candlelight vigil on Tuesday evening hopes to honour families of the missing, and to coordinate efforts across the country for justice and an end to a crisis the RCMP admits has claimed more than 1,200 Indigenous women. "October 4 is a day where we honour the lives of missing and murdered Aboriginal women and girls," the event's Facebook page stated. "The violence experienced by Aboriginal women and girls in Canada is a national tragedy." The event will include a moment of silence, as well as performances by the dance troupe Butterflies in Spirit, hiphop duo Entertribal, and speeches from Angela Marie MacDougall of Battered Women's Support Services and other violence against women campaigners, as well as Gertie Pierre and Lorelei Williams, both family members of missing and murdered women. MetroNews.ca

*** First Nation vigils planned across Thompson-Okanagan to honour missing and murdered women**
First Nations across the country will be holding vigils this week to call attention to the increasing number of missing and murdered Aboriginal women and girls. Okanagan Indian Band spokesperson Shaylen Smith calls the Sisters in Spirit National Day of Vigils a "movement for social change." "Each year, family members, Aboriginal community members, and concerned citizens gather for a vigil on Oct. 4 to honour the memory of missing and murdered Aboriginal women and girls," she says in a media release. According to the Native Women's Association of Canada website the number of vigils has grown from 11 in 2006 to 216 in 2014. Vigils will be held in Kelowna, Vernon, Enderby, Penticton and Kamloops as well as other communities across Canada. InfoTel.ca

*** Confronting violence against indigenous women and girls**
An opinion piece states, "In late September, Inuit artist Annie Pootoogook died tragically in Ottawa. Pootoogook was an award-winning illustrator from Cape Dorset, Nunavut. Her ink-and-crayon depictions of everyday life in the north - families sitting to eat a meal of seal meat or shopping at the Arctic co-op - received international acclaim. In contrast to the idealized vision many Canadians have of the north, of majestic rock and ice landscapes or charismatic wildlife, such as polar bears, Pootoogook's drawings often reflected the crushing poverty northern families face and its devastating effects on their health and well-being. Ottawa police believe Pootoogook's death is suspicious - she may have been the victim of foul play. If so, Annie Pootoogook is yet another indigenous woman to die violently in Canada. Indigenous women and girls are three times more likely to experience violence than nonindigenous women and six times more likely to be murdered. On any given day, thousands of First Nations, Inuit and Métis women and children are living in emergency shelters to escape abuse (though on-reserve shelters remain woefully underfunded). The RCMP hasn't kept accurate statistics on the number of murdered or missing people, but indigenous women's organizations and affected families have reported hundreds of cases of loved ones who have been victims of violent crime. After years of indifference and inaction, Canada's government has finally launched an inquiry into the many lives lost to violence. Although the national inquiry into murdered and missing indigenous women won't investigate cases police previously examined, it will look at broader factors that put indigenous women and girls at such great risk. According to the UN Committee on the Elimination of Discrimination Against Women, this includes institutional racism, social and economic marginalization and inadequate access to affordable housing so women can escape abusive relationships. Police forces have often failed to deal with violence against indigenous peoples, and officers themselves have been implicated or charged with assaults and sexual abuse. Human-rights organizations, such as Amnesty International and Kairos, have also drawn attention to resource

development in indigenous territories, where the influx of transient workers - along with money, alcohol and drugs from outside the community - puts indigenous women at risk of aggressive harassment and violence by men." Toronto Star, A11

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Joint effort key in legalizing marijuana**
An opinion piece by Dan Kelly, president of the Canadian Federation of Independent Business states, "...about a month ago, there I was at a Government of Canada consultation on marijuana legalization and regulation led by Anne McLellan, a former deputy prime minister. From the start, it was made clear the consultation was on the "how" not "if" of legalization. Leading a member-driven organization whose mandate is exclusively business issues, not social policy, I worried I would have little to add. The one survey the Canadian Federation of Independent Business conducted on how recreational marijuana should be sold provided no clear direction. Many of the comments actually suggested there are divisions among business owners on whether legalizing marijuana is a good idea in the first place. For example, many small business owners expressed concern about the workplace safety and health implications of legalizing it. Still, while we have limited experience with cannabis regulation, CFIB has a wealth of experience on regulation in general - including how to get it right and what not to so. This includes experience with liquor and tobacco regulation, which offers some guidance - albeit imperfect. Based on CFIB's 45-year history with regulation making, here's what I have to offer: Focus on critical regulatory imperatives: Too often, governments examine a new area where regulation is needed and quickly expand the mandate to include every moving part. This automatically means proper enforcement is near impossible. Choosing a few critical regulatory priorities, such as preventing sales to minors, ensuring proper product safety information and rules, and prohibitions at work or while driving, seems to be a great place to start. Choose the most important aspects to regulate and then do them well. Leave the rest alone." Vancouver Sun, B4 (Windsor Star, Calgary Herald, Edmonton Journal, Montreal Gazette, Ottawa Citizen)

*** Un sénateur passe à l'offensive contre la drogue au volant**
Avec la légalisation prochaine de la marijuana, un sénateur conservateur veut s'assurer que les policiers ont les moyens de lutter contre la conduite avec les facultés affaiblies. Le leader de l'opposition officielle au Sénat, Claude Carignan, déposera aujourd'hui un projet de loi modifiant le Code criminel pour permettre aux patrouilleurs d'utiliser des appareils de dét ection pouvant déceler la présence de drogue dans le sang. «C'est un projet de loi d'une importance capitale qui cible un problème urgent: le manque d'outils pour permettre de détecter les drogues chez les conducteurs», a déclaré le sénateur Carignan en conférence de presse, hier. Le Journal de Québec, 12 (le Journal de Montréal)

*** 'How can this be possible?' Ottawa prepares for pot shops**
Tom Poirier, the owner of an army surplus store in a strip mall off Merivale Road, watched with curiosity as a new business prepared to open next door. Poirier discussed the odd renovations with Bill Chappell, who owns a hobby shop in the mall on Roydon Place. The tenant next door is CannaGreen, one of the city's newest marijuana dispensaries. The back room at CannaGreen contains an ATM machine and a couple of display cases filled with dried weed and cannabis-laced cookies, brownies, candy and cola with names like Grow-op Grape. But they are dumbfounded that a shop illegally selling pot can operate freely. The dispensaries are opening across the country, their owners emboldened by the federal government's promise to legalize recreational pot. They operate in what some have dubbed a "legal limbo." Police in some jurisdictions are reluctant to enforce drug laws when pot may soon be legal, and there is growing public acceptance both of marijuana use and its sale in stores. There are about 15 dispensaries in Ottawa. Dispensaries are illegal, selling products from the black market that may be unsafe, according to the federal government. Ottawa police say they are investigating - and consulting with - the Public Prosecution Service of Canada, which is responsible for prosecuting drug crimes. Ottawa Citizen, A6

*** Lessons from Denver**

The legalization of pot in Colorado has profoundly changed Denver, a city about the size of Ottawa that is now home to 1,054 marijuanarelated businesses. Dozens of municipal agencies have jumped in to help regulate the green-rush businesses, from the fire department to building inspectors, according to Ashley Kilroy, Denver's director of marijuana policy. She gave a presentation to the Association of Municipalities of Ontario in August that summarized the lessons learned in Denver since stores began selling pot on Jan. 1, 2014. Ottawa Citizen, A6

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Meet the new budget**
An opinion piece states, "People on the receiving end of federal government cheques can perhaps be forgiven for getting their hopes up. The Liberals had just won an election on a platform that called for deficit spending, and almost the first thing they did in power was to announce that their new government was preparing to run deficits two or three times as large as the $9-billion shortfall they had campaigned on. Prime Minister Justin Trudeau was promising to negotiate with respect and in a spirit of collaboration. After a decade of being invited by the Harper Conservatives to take it or leave it, these words were probably enough to make public sector workers' and the provinces' heads spin, and they were apparently enough to overlook one important fact: the Liberals never actually promised them much in the way of new money. This detail could be glossed over in their first budget, put together in a hurry and focused on the new government's priorities. But the absence of concrete Liberal spending commitments is getting harder to ignore as the 2017-18 budget cycle gets underway." National Post, A11

OTHER / AUTRE

*** Sister continues 8-year fight for Victoria man imprisoned in Iran**
It was eight years ago today that Victoria's Saeed Malekpour was snatched off a Tehran street and thrown into Iran's notorious Evin prison. That means it has been eight years that his kid sister Maryam Malekpour has been fighting for his release. Yet it feels like he's no closer to freedom than he was before. In fact, Maryam feels let down by Canada's year-old Trudeau government, which she says is doing less for her 41-year-old brother than the Harper Conservatives did. Saeed's story has been told here before. A gifted software designer who had worked for several top Iranian companies, he came to Canada in 2004 with his wife, Fatima Eftekhari, who wanted to study in the West. In 2006, they moved to Victoria, where Malekpour freelanced as a website designer while Eftekhari completed her doctorate in medical nanotechnology and taught at the University of Victoria. They earned permanentresident status. Saeed was planning to take his master's degree at UVic in 2008 when he was called back to Tehran to be with his dying father - only to be arrested and charged with distributing porn. Nonsense, his supporters say. All he had done was design software that was used, without his knowledge, to upload images. It was like charging the inventor of the typewriter with authoring the contents of a book. Times Colonist, A3

Family optimistic after UofT student released on bail in Bangladesh
The family of a Toronto university student who was detained in Bangladesh after surviving a terrorist attack is expressing cautious optimism now that the young man has been released on bail, apparently cleared of involvement in the deadly raid. Tahmid Hasib Khan, a permanent resident of Canada, was detained after a bloody attack this summer at a restaurant in the Bangladeshi capital, but his family has firmly maintained his innocence. On Sunday, a Bangladesh court released Khan on bail in Dhaka, the country's capital. Canadian lawyer Marlys Edwardh, who was hired by his family, said the decision came after police filed documents with the court saying investigators found no evidence against the 22-year-old in connection with the terror attack. Khan's older brother, who is a Canadian citizen and lives in Toronto, said the bail development was a relief for his family. Canadian Press (Times & Transcript, B4, National Post, Globe and Mail, Waterloo Region Record, Times Colonist, Cape Breton Post))

Ottawa offering cash, not advice, to aid Iraqis
The Iraqi bombdisposal experts Canada has promised to help are losing colleagues almost every day as they try to defuse bombs jihadists hide by the dozens beside the roads. The officer was speaking at the King Abdullah II Special Operations Training Centre outside Amman. It is here NATO is training Iraqi soldiers and security officials in such skills as defusing improvised explosive devices (IEDs). At a NATO summit in July, Prime Minister Justin Trudeau said Canada would contribute to this initiative, but provided no details. A Global Affairs Canada spokesman said this week no Canadian soldiers or government officials are involved. Instead, Canada will contribute $400,000. However, Ottawa has deployed some members of the military to Jordan. A small team arrived in late August to assess how Canada might develop bilateral training programs for the Jordanian military. A second team from Canadian Special Operations Forces Command is also here as part of Canada's Global Partnership Program and Counter-terrorism Capacity-Building Program. Canada also has about 200 special forces trainers with Kurdish peshmerga in northern Iraq. National Post, A6 (Kingston Whig-Standard)

*** Canadian photographer killed by her driver, Mexican official says**
Robbery appears to be the motive behind the murder of Canadian photographer and artist Barbara McClatchie Andrews, says a Mexican prosecutor. Yucatan state Attorney General Ariel Aldecua alleges the woman was killed by a man she hired to drive her from Cancun back to where she lived in Merida, the state's capital. Authorities said the body of the 74-year-old woman was discovered Friday, tossed on the side of a highway that connects the two cities. They said there were signs she had been strangled. McClatchie Andrews ran a non-profit art gallery in Merida called In Lak'Ech for several years that supported emerging artists, but she maintained close ties to Canada. Recent work on her website showcases abstract photos taken in British Columbia, from the scenic Sechelt Peninsula to Vancouver's bustling Main Street. CBC News

INTERNATIONAL

*** Hurricane Matthew pounds southwest Haiti, heads north**
Hurricane Matthew pounded the southwestern coast of Haiti on Tuesday, threatening a largely rural corner of the impoverished country with devastating storm conditions as it headed north toward Cuba and the eastern coast of Florida. Rain from the dangerous Category 4 storm fell across Haiti before dawn as the centre of the storm moved directly across the tip of the southern peninsula, where many people live along the coast in shacks of wood and corrugated steel that stand little chance of withstanding the force of the system's maximum sustained winds of 145 mph (230 kph). Matthew was also expected to bring 15-25 inches of rain, and up to 40 inches (100 centimetres) in isolated places, along with up to 10 feet (3 metres) of storm surge and battering waves, said Dennis Feltgen, a meteorologist and spokesman for the U.S. National Hurricane Center in Miami. ``They are getting everything a major hurricane can throw at them,'' Feltgen said. The storm was moving along the Windward Passage between Haiti and Jamaica, where it was also dumping heavy rain that caused flooding in parts of the country. It was headed for southeastern Cuba and then into the Bahamas. The hurricane centre said it would likely issue a tropical storm watch or hurricane watch for the Florida Keys or the Florida peninsula and that it could create dangerous beach conditions along the East Coast later in the week. Associated Press (MetroNews.ca); Reuters.com; News.Sky.com; CNN.com; NBCNews.com; ABCNews.go.com

Hurricane Matthew shifts closer to Florida, forecast says
Hurricane Matthew slightly grew stronger early Tuesday and shifted closer to Florida, according to the National Hurricane Center in Miami. The Category 4 hurricane headed toward Haiti with top sustained winds near 145 mph, up from 140 mph earlier, the hurricane center said. It was moving northward at 8 mph and was nearing the southwest peninsula of Haiti. ''The threat to Florida and the southeastern U.S. coast has increased,'' the National Hurricane Center said. Life-threatening rain and storm surge was expected in parts of Haiti by early Tuesday morning. USAToday.com

Morocco arrests 10 women linked to ISIS
Morocco's Interior Ministry says authorities have detained 10 women linked to the Islamic State group who are suspected of plotting suicide attacks and trying to recruit other women to join the extremists. The ministry said in a statement that the Central Bureau of Judicial Investigations dismantled the cell of women extremists Monday, in operations in eight towns. The ministry chemical products seized at the home of one suspect could be used in explosives. The women allegedly declared allegiance to IS, and some have family ties to Moroccan fighters with IS in Syria or Iraq, the statement said. The women are in custody pending further investigation. Associated Press (Edmonton Sun, A20)

U.S., Russia relations worsen over Syria: Peace Talks Falter
Ties between Russia and the U.S. deteriorated further on Monday after the Obama administration proclaimed bilateral peace talks over Syria dead and Moscow suspended a 16-year-old treaty meant to reduce the risk of nuclear proliferation. ''Everybody's patience with Russia has run out,'' White House spokesman Josh Earnest said in Washington, blaming Vladimir Putin's government for undermining the fight against Islamic State and for indiscriminate bombing that has killed civilians and targeted hospitals in Syria. ''Russians have been complicit'' in the Syrian tragedy, Earnest said, and ''there is nothing more for

the United States and Russia to talk about." The U.S. said Monday it was withdrawing personnel who had been dispatched to the Middle East in anticipation that a Syrian ceasefire deal reached Sept. 9 would go into effect, a move that would pave the way toward greater co-ordination between the U.S. and Russian militaries. That followed Putin's decision earlier Monday to withdraw from a 2000 accord that committed both countries to eliminating their stockpiles of the plutonium used as the core material in some types of nuclear weapons. Halting the plutonium pact is a "forced measure," Russian Foreign Minister Sergei Lavrov said, according to the ministry's website. Russia viewed the 2000 treaty as an "important step" toward nuclear disarmament, he said. Putin's decree withdrawing from the treaty accused the U.S. of "unfriendly" actions that posed a "threat to strategic stability." Bloomberg News, N5

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Sent to: !DMS External; PS.F DL_DMS F.SP

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
October 6, 2016 / le 6 octobre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

RCMP to settle suits: Sources
The RCMP commissioner is expected to issue an apology on Thursday as part of a historic settlement reached with the plaintiffs in two proposed class-action lawsuits alleging systemic gender-based harassment and discrimination within the force, sources say. Any female member who experienced harassment or discrimination will be eligible to apply for damages. Amounts will depend on the injuries, a source said. The potential number of Mounties who could be eligible is in the thousands and compensation could potentially reach as much as $100 million. As part of the settlement, the force will announce new details of how it plans to change its workplace culture. Reaching a settlement is a significant event, said Angela Workman-Stark, a former RCMP chief superintendent who played a key

role in helping the force address harassment and bullying. "For the women, it's a resolution for them. I think it's an acknowledgment of the issues they brought forward. I think it's great for the organization to move forward and take responsibility. Resolution and recognition is an important piece," said Workman-Stark, who left the force earlier this year. Thursday's announcement will take place at 11 a.m. ET in Ottawa. Bob Paulson, the commissioner, and **Public Safety Minister Ralph Goodale** will be joined by the lead plaintiffs in the proposed class-action lawsuits, Janet Merlo and Linda Gillis Davidson. National Post, A1 (Windsor Star, Leader-Post, London Free Press, The Province, Edmonton Journal, Montreal Gazette, Vancouver Sun, Calgary Herald, StarPhoenix, Ottawa Citizen); Globe and Mail; Canadian Press (680 News); * La Presse Canadienne (L'actualité); La Presse+; Le Journal de Montréal (Le Journal de Québec); Toronto Star; * Global News; The Hill Times; iPolitics; * Ottawa Citizen

Espionage bill will allow PM to muzzle watchdog, report says
Canada's new spy-accountability legislation will create a parliamentary watchdog that prime ministers can keep on a short leash, or even muzzle, a report on the bill by the Library of Parliament says. The Liberal government has said the national-security legislation will create an independent committee of MPs that will have regular briefings from government spy agencies on their activities. However, a report on Bill C-22 suggests the national security and intelligence committee of parliamentarians could end up "in effect, accountable to the Prime Minster alone." The report, done by the nonpartisan Library of Parliament and released this week, is a synopsis of the bill for parliamentarians. Such reports are among the information services the staff of the library provide to MPs and senators. The Library of Parliament's report points out that the bill would allow prime minsters and cabinet to shape, block or censor the committee's work. This hits a decidedly different tone from an essay published this week by **Public Safety Minister Ralph Goodale**, who said Bill C-22 creates a committee that "will set its own agenda and report when it sees fit. Every democracy has to determine how far legislators should be able to go to act as a check on government spies, who typically work under secret orders from presidents and prime ministers. Canada gives its elected politicians less information about and fewer review powers over the security agencies than most governments do. And, unlike its closest allies, Canada has not cleared any parliamentarians to hear state secrets. Under C-22, that would change. Globe and Mail, A1

* **Canadian government re-opens privacy debate on access to telecom subscriber info**
The Canadian government has revived a discussion on a particularly controversial privacy topic: how much access law enforcement should have to telecom subscriber information in the name of public safety. In September 2016 the government opened a public consultation on national security, releasing a 'green paper' and background document that details issues, challenges and general questions surrounding national security threats like domestic terrorism. Many topics are covered in the documents, but there's one in particular that may sound familiar to Canadians: the issue of warrantless access to subscriber information from telecom companies. Michael Geist, Canada research chair in internet and e-commerce law at the University of Ottawa, states in an article for The Globe and Mail that the government has been pushing for easier access to carrier data since the early 2000s, with the initiative seeing setbacks such as the defeat of Bill C-30. Lawful access legislation eventually passed in 2014, resembling something near a compromise between consumer and government interests. Warrant-less disclosure of information and government surveillance capabilities for telecoms were nixed, but the legislation also eliminated liability concerns for Internet service providers (ISPs) that voluntarily disclose basic information and gave the police new powers to require access to digital data. The above-mentioned public consultation — started by **Public Safety Minister Ralph Goodale** — has put the issue back up for debate, however. "The Public Safety consultation skips over the years of lawful access debate by putting everything back on the table," writes Geist, "acknowledging that the law was updated less than 24 months ago but suggesting that more change may be needed." As for **the Minister's** thoughts on the matter, a spokesperson stated to Motherboard: "***While both basic subscriber information (BSI) and a phone book can both be used to identify someone, BSI requires safeguards because some of it can reveal intimate details of a person's activities when linked to other information. That principle has been affirmed by the courts. The government is committed to protecting both Canadians' safety and their rights, including their privacy rights***." **The spokesperson** added that the green paper was meant to "***provoke discussion***." The public consultation remains open until December 1st, 2016 and can be accessed here if you'd like to add your voice to the conversation. MobileSyrup.com

*** Inondations : les élus de Windsor et Tecumseh veulent plus de soutien d'Ottawa et de Queen's Park**

Des élus de Windsor et Tecumseh réclament plus de soutien financier aux gouvernements fédéral et provincial pour venir en aide aux sinistrés touchés par les inondations. Le député Percy Hatfield veut que le gouvernement provincial change la législation pour étendre la couverture du programme d'aide en cas de catastrophe naturelle aux personnes qui ont subi des dommages en raison de refoulement d'égouts. M. Hatfield a soulevé le problème au cours de la période de questions à Queen's Park mardi après-midi. Plus tôt dans la journée, les autorités provinciales avaient indiqué que les sinistrés dont les dommages avaient été causés par les refoulements d'égouts n'étaient pas admissibles au programme d'aide pour la reprise après une catastrophe. La députée de Windsor-Tecumseh, Cheryl Hardcastle, a également plaidé la cause de ses concitoyens à la Chambre des communes à Ottawa. Elle a notamment pris Justin Trudeau à partie et lui a demandé de rétablir le fonds d'indemnisation en cas de catastrophe naturelle supprimé par le gouvernement précédent. **Le ministre de la Protection civile, Ralph Goodale**, a indiqué que le gouvernement étudiait la possibilité de rétablir les programmes coupés par les conservateurs. Radio-Canada (2016-10-05)

*** Understaffing on the Canadian side led to summer border delays**

Canada-bound drivers on the Peace Bridge had to wait an average of more than 18 minutes – and sometimes much longer – to cross the span during busy summer weekends thanks to a variety of factors that led to understaffing at the customs booths on the Canadian side of the border, sources familiar with the border backups said. Budget cuts, a new policy that Canadian border agents be armed, union rules and changing traffic patterns all played a part in the delays, according to government and union officials as well as people managing U.S-Canadian border crossings. The border delays have eased as the weather has cooled, but Rep. Brian Higgins, D-Buffalo, vowed Wednesday to keep up the pressure on Canadian officials in hopes that the delays don't reappear during next year's busy summer travel season. The long delays prompted Buffalo Mayor Byron W. Brown and six other mayors on both sides of the border to write a letter to **Ralph Goodale, the Canadian minister of public safety and preparedness**, to complain. "The situation is intolerable," the mayors said, noting that some travelers had to wait as long as 90 minutes to cross into Canada. "The local economies, the safety of our residents and workers at the bridge, commercial shipments and the proper management of our border crossings are all at the mercy of the Canada Border Services Agency." The mayors complained of understaffing at the borders, which has its roots in former Prime Minister Stephen Harper's Deficit Reduction Action Plan, a 2011 effort to cut federal spending in Canada. That led to a cut of 1,053 positions at the Canadian border agency, or about 10 percent of its workforce, said Jean-Pierre Fortin, national president of the Canadian Customs and Immigration Union. A spokesman for the Canadian border agency, Esme Bailey, said jobs were cut through attrition, with a focus on reducing employment at the agency's headquarters. "The focus was not to reduce capacity at ports of entry," Bailey said. Yet people who manage those ports of entry said unmanned booths on the Canadian side are proof that staffing is a central issue behind the delays – although budget cuts are not the only reason for the staffing issue. Buffalo News (2016-10-05)

*** Why Americans With DUIs Can't Enter Canada**

An opinion piece written by lawyer Henry Chang states, "Last month, the Canadian media reported on several instances of Canadian citizens being barred from the United States because they admitted to smoking marijuana, even if they had never been charged with or convicted of controlled substance possession. **Canadian Public Safety Minister Ralph Goodale** described the banning of Canadians as a "ridiculous situation" that needed to be addressed. However, in order to examine this issue in the proper context, we should consider how the Government of Canada treats United States citizens who seek entry into our country..." Huffington Post (2016-10-05)

TOP STORIES / MANCHETTES

*** Members of dormant national security roundtable seeking answers**

A group of Canadians who advise the federal government on national security issues are in the dark about the future of a 16-member roundtable they were appointed to. Members of the Cross-Cultural Roundtable on Security are supposed to meet in-camera at least twice a year, yet the group hasn't met

since October 2014. The roundtable was set up in 2005 to act as a sounding board for cabinet ministers and other high-ranking federal executives on how security matters and government policies affect different ethnic communities. Over the years, it has covered topics such as countering violent extremism, migration and cyber-security. (…) Myrna Lashley, a psychologist, was appointed to the roundtable in 2005 and has been the group's chairperson since 2007. But after receiving the letter in March, Lashley suspects her involvement has come to an end. "Effectively when you get that letter, you have been told 'thank you,'" Lashley said. In the meantime, Lashley is concerned the federal government is not communicating as effectively on national security issues with Canada's ethnically diverse communities, such as Syrian refugees. In the past, Lashley says the group met with and advised ministers of public safety and justice as well as senior executives from the RCMP, CSIS and Canada Border Services Agency on all sorts of issues that could or would affect an array of cultural groups. CBC News

* **'This is a way for everybody to heal': ex-Mountie on RCMP compensation for harassment**
A former Manitoba RCMP officer says it's time to heal, but no amount of money will ever pay for what she and others in the force had to endure. Sherry Benson-Podolchuk was following closely Wednesday after CBC reported that 500 past and present female RCMP officers were expected to be compensated at a Thursday news conference for allegations of sexual harassment, unwanted touching, and rape. "This is a way for everybody to heal," she said. Benson-Podolchuk, 53, isn't one of the 500 women being compensated but did reach out to the group to offer her support when she heard of their allegations a few years ago. Benson-Podolchuk was a single mom living on welfare in 1990 when she first joined the RCMP at a detachment in Tisdale, Sask. Benson-Podolchuk was excited to start a career in policing but said she was chronically harassed for being a woman at the detachment. "They always said tell the truth and obey the law and that you'd be protected by the RCMP, but they didn't tell you what would happen when you come to work and they'd start calling you beaver and raisin tits," she said. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

* **STORM CHANGES COURSE**
Despite its brawn and fury, hurricane Matthew no longer poses much of a threat to Canada's East Coast, the Canadian Hurricane Centre said Wednesday after it dropped a tropical cyclone statement from its website. Meteorologist Bob Robichaud said the powerful, slow-moving storm is now expected to veer into the Atlantic Ocean after scraping along the coast of Florida, and it may double back for another run at the state later this week. Canadian Press (Chronicle Herald, A1), CBC News; Daily Gleaner

* **Up to 50 cm of snow in Prairie forecast**
As much as 50 centimetres of snow is expected to fall on parts of the Prairies as a pre-winter storm continues to pound the region. Environment Canada issued winter storm and snowfall warnings for northern Manitoba and a large chunk of Saskatchewan stretching from the northeast to the southwest. Times Colonist, A6

* **Dormant B.C. volcano sparks with activity**
Experts are taking a closer look at Mount Meager, a dormant volcano north of Pemberton, after they discovered activity on the peak earlier this summer. Volcanologist Melanie Kelman with Natural Resources Canada said sulphur smells and volcanic openings known as fumaroles were spotted on the the long-dormant volcano... While fumaroles pose no risk to the public, she said it would be unsafe to approach or enter them as they are letting off hydrogen sulfide - a poisonous gas - and the ice around them is crevassed and potentially unstable.Her team is now monitoring the area for increased seismic activity - the key sign of an upcoming eruption… Mount Meager was the site of one of the largest volcanic explosions in Canada. About 2,400 years ago, the mountain erupted, triggering a major landslide and spewing ash as far as Alberta. Although the mountain hasn't erupted for over 2,000 years, Kelman said that doesn't mean the volcano will never erupt again... Kelman added there is usually plenty of warning before a volcanic explosion takes place - mainly intensifying seismic activity - and B.C. scientists are well equipped to move in with intensive monitoring. She also emphasized the province is well-prepared for emergencies. "We've certainly talked to Emergency Management B.C. about the unrest in Meager and explained what's going on ... It doesn't pose a threat to public safety." CBC News

*** Tecumseh mayor praises flood response**

The Town of Tecumseh provided an update on flood recovery on Wednesday, a week after 195 millimetres, or 7.74 inches, of rain fell over two days. "I always say the people of Tecumseh are fantastic and this is true this week," Mayor Gary Mc-Namara said in a news release. "What this town has been through is unprecedented. No mayor likes to see their municipality in crisis, however, I'm proud of how the people of our town have responded." There have been 1,200 flood responses completed and more than 300 calls and visits to town hall..."I acknowledge the efforts of town staff and contractors for their emergency response," chief administrative officer Tony Haddad said in a news release. Postmedia Network (Windsor Star, A4)

*** Insurance workers take flak from frustrated public**

Last week's devastating floods in east Windsor and Tecumseh packed a double wallop of worry and work for Michelle Tremblay. As a career woman, Tremblay is the managing director of an east end insurance brokerage that was deluged with claims in the days that followed the Sept. 29 flood. As a Riverside resident, she suffered the same damage from basement flooding as many of her friends and neighbours. Frustrated by news accounts of people angry at their insurance providers about coverage limits or the spread of outright misinformation, Tremblay decided to speak out. "The insurance industry does a really poor job of promoting themselves and what we do for people," she said. She said people often don't understand the difference between an agent and a broker and too many fail to read and understand their policy and its limits. Postmedia Network (Windsor Star, A4)

*** Training exercise helps emergency personnel practice for potential disaster**

Some were in shock, some were trying to help friends, and some were rocking back and forth. They were victims in a simulated train disaster held Wednesday morning in Truro, used as a training exercise for a number of emergency services, including firefighters and paramedics... The province's Department of Health and Wellness hosted the simulation, which was held in the parking lot at the former Colchester Regional Hospital. Along with firefighters and paramedics, police and the local Hazardous Materials unit responded. Emergency Measures was also on site. This is a special day," said Jim MacDougall, manager of planning, exercise and training with the provincial department. "It's an opportunity to test our plans and practice our teams for a potential disaster." Truro Daily

*** La poursuite fédérale prête à fixer une date de procès**

La poursuite fédérale est prête à fixer le procès contre la compagnie ferroviaire Montréal, Maine & Atlantic (MMA) de même que certains dirigeants et employés à la suite de la tragédie de Lac-Mégantic. La MMA et certains employés en fonction le 6 juillet 2013 font face à des accusations pénales en vertu de la Loi sur les pêches ainsi que celle sur la sécurité ferroviaire du Canada à la suite de la tragédie de Lac-Mégantic, en juillet 2013. Lors du retour de la cause, mercredi, au palais de justice de Sherbrooke la procureure aux poursuites pénales du Canada, Me Josée Pratte, a déposé le cahier de procès, la liste des admissions et exposé sa théorie de la cause basée sur une culture de négligence. La Voix de l'Est, La Tribune, La Presse

*** Red Cross appeals for help for hurricane victims**

The Canadian Red Cross has started a fundraising appeal for Haiti and other Caribbean countries that have been affected by hurricane Matthew. In a news release, Hossam Elsharkawi, head of international operations for the Canadian Red Cross, said thousands are now in desperate need of emergency relief, including shelter, water, food and healthcare... Two Canadian Red Cross staff members were already in Haiti, helping with ongoing rebuilding and recovery work from the massive earthquake of 2010. Three more are being immediately sent as part of an international team to assess needs and co-ordinate a global Red Cross response while others are being placed on standby to deploy if needed, including medical and support staff of a field hospital, the agency stated. The Canadian Red Cross also contributes to a stockpile of tents, blankets, tarps and other emergency relief supplies warehoused at an airport in Panama for rapid deployment anywhere in the Caribbean or Central America, and these supplies are now being prepared for shipment to Haiti and other countries in Matthew's path, the Red Cross said. Daily Gleaner, A5

*** Aid rushing to Haiti**
Samaritan's Purse, a Christian relief and development organization that has been in Haiti for several years providing a variety of relief and development help, is sending specially trained staff and emergency supplies in response to the harm caused by Hurricane Matthew. The response team is travelling on Samaritan's Purse's DC-8 airplane loaded with 20 tons of essentials including clean water, blankets, hygiene items and plastic sheeting for immediate shelter. "We're asking Canadians to support us through their prayers and donations as we hurry to help Haiti's struggling hurricane victims," said Fred Weiss, executive director of Samaritan's Purse Canada. "They desperately need our help." Canadian Press (Chronicle Herald, A9)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Members of dormant national security roundtable seeking answers
A group of Canadians who advise the federal government on national security issues are in the dark about the future of a 16-member roundtable they were appointed to. Members of the Cross-Cultural Roundtable on Security are supposed to meet in-camera at least twice a year, yet the group hasn't met since October 2014. The roundtable was set up in 2005 to act as a sounding board for cabinet ministers and other high-ranking federal executives on how security matters and government policies affect different ethnic communities. Over the years, it has covered topics such as countering violent extremism, migration and cyber-security. (…) Myrna Lashley, a psychologist, was appointed to the roundtable in 2005 and has been the group's chairperson since 2007. But after receiving the letter in March, Lashley suspects her involvement has come to an end. "Effectively when you get that letter, you have been told 'thank you,"' Lashley said. In the meantime, Lashley is concerned the federal government is not communicating as effectively on national security issues with Canada's ethnically diverse communities, such as Syrian refugees. In the past, Lashley says the group met with and advised ministers of public safety and justice as well as senior executives from the RCMP, CSIS and Canada Border Services Agency on all sorts of issues that could or would affect an array of cultural groups. CBC News

Ottawa will attempt to close Fintracs lawyer loophole
The federal government will try to close a loophole in Canada's anti-money laundering system that excludes lawyers from having to report suspicious transactions, Postmedia has learned. In 2015, the Supreme Court of Canada ruled that, unlike other professionals such as bankers and real estate agents, lawyers do not have to report to Canada's anti-money laundering agency, Fintrac. Lawyers in B.C. won that case based on a constitutional argument about solicitor-client privilege, and the argument that law societies already regulate lawyers to prevent involvement in money laundering. But Canada faces increasing international scrutiny as concerns over money laundering in Vancouver real estate grow. In September, the Financial Action Task Force, a Paris-based intergovernmental group that makes recommendations for fighting money laundering, asked Canada to close the lawyer loophole. An agency report suggested there is a close relationship between money laundering in real estate and the services provided by lawyers, such as placing wire transfers in legal trusts and creating investment vehicles that can shield true ownership of property. (…) Kim Marsh, of due diligence company IPSA International, said that before the 2015 Supreme Court case, the company was asked by the federal Justice Department to do a report on money laundering risks connected to lawyers. "I think there are some people in the legal industry that are aiding and abetting money laundering, with impunity," said Marsh, a former RCMP organized crime unit leader. "There is no other English common law country that has given lawyers this reporting exemption. So Canada is unique. And the problem is coming to light now with the huge amount of money flowing into the property market, some of it stinky." Marsh said he believes Canadian law societies neither provide adequate member training on money laundering nor have the internal auditing and investigation needed to crack down on bad apples. Postmedia Network (Vancouver Sun, A3)

Let expert review security bills
Prominent security expert says legislation is fatally flawed, Oct. 3
A letter to the editor states, "Hopefully, the Star will soon report that, in fact, Paul Cavalluzzo has been hired to oversee a review of Bills C-51 and C-22. If nothing is done, then perhaps Canadians will have to await their own Edward Snowden some years down the road." Toronto Star, A18

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

New app provides border wait times
Border wait times across southern Ontario are expected to be lengthy during this Thanksgiving holiday weekend. The Canada Border Services Agency has unveiled a new app - CanBorder - which drivers can use to check the latest border wait times. Services under the app such as "Near Me" and "Favourites" make it easy to find and access information on ports of entry that are nearby, the agency said. CBSA also encourages the use of NEXUS lanes or ensure each passenger has proper travel documents prior to arriving at the border crossing. It also helps to have receipts ready and be familiar with personal exemptions. For information on food products or restrictions, visit the CBSA website at www.cbsa-asfc.gc.ca. Windsor Star, A4

*** Bridge closing briefly on Sunday**
The Ambassador Bridge will be shut down to vehicle traffic briefly on Sunday morning to allow cyclists to take part in the annual Bike the Bridge ride. The bridge will close to traffic at 9 a.m. and be shut down for about 15 minutes to allow 750 registered cyclists to ride across the bridge to the Detroit side and back. It's the only time during the year where cyclists are allowed on the Detroit River international crossing under a ride sponsored by the Tour de Troit group. Windsor Star, A4

*** Finches in hair rollers and other cases**
Wildlife is now the fourth largest illegal trade globally after drugs, counterfeit money and human trafficking, according to the World Wildlife Fund. Here are a few cases in which Canadians faced charges relating to illegal importation of exotic animals: - Turtles in pants: A student at the University of Waterloo who repeatedly entered Michigan to buy and ship thousands of turtles to his native China only to be caught with 51 of them strapped to his legs was sentenced in April to nearly five years in a U.S. federal prison for smuggling. The U.S. government said Kai Xu, 27, shipped turtles to China from Canada and the United States, or hired people to fly with turtles in their luggage to China. It's not illegal to buy turtles from breeders in the U.S., but Xu's crime was shipping them overseas without a federal permit. Turtles in pants: This year, another man - Dong Yan of Windsor, Ont.- was fined $3,500 and placed on probation for two years after getting caught smuggling nearly 40 turtles in his pants. Yan was convicted in February of illegally importing reptiles into Canada that were transported in contravention of a foreign state's law. Finches in hair rollers: A Toronto man was fined $2,500 four years ago after he was caught at Pearson International Airport with finches and seed-eaters hidden inside hair rollers in his coat. Ali Niamath had pleaded guilty to unlawfully importing live birds into Canada from Trinidad and Tobago. Federal law bars people from importing animals taken or transported in contravention with the laws of a foreign state and officials said Niamath did not have the proper export permits. The lesser seed-finch and ruddy-breasted seedeater are prized for their song and their population is in decline as they are often trapped in the wild and exported illegally. Times Colonist, C3

*** Chinese accused of visa fraud remanded to prison**
Two Chinese nationals, who were intercepted at the VC Bird International Airport attempting to board a flight with fake Canadian visas in their passports, have been remanded to prison. Jianming Chen, 43 and Qianqian Chen, 22 appeared before Magistrate Conliffe Clarke in the St John's Magistrates' Court, yesterday, and were remanded until Monday. The duo, through an interpreter, pleaded not guilty to two separate charges of uttering a Chinese passport containing a forged Canadian visa, and fraud. (...) The accused men claim their passports were taken by that unknown individual days later and when it was returned it contained the fake document along with a one-way ticket to Canada. While at the airport, the West Jet Airlines agent who checked in Jianming and his companion Qianqian on WS2739 destined for

Canada, observed some irregularities with the visa. A check with the Canadian Border Security confirmed the visa was not authentic. Upon his arrest, Jianming said he never requested nor applied for a Canadian visa. Antigua Observer

*** Expect to experience 'a whole new terminal'**
Fifteen years of planning, five years of construction, a $2.6-billion investment. The numbers give a sense of the scale of YYC's airport development project, the most ambitious undertaken on Calgary International Airport property since the opening of the existing terminal building in 1977. For most Calgarians, however, the magnitude of this project - which included the construction of a new runway, operational since 2014 - won't be apparent until the morning of Oct. 31, when the Calgary Airport Authority throws open the doors to its new International Terminal. On that day, travellers headed to U.S. or international destinations will see first-hand what all that time, money and e ort has produced. (...) For departing passengers, that experience will start in the spacious, light-filled check-in hall. Automated kiosks and a selfserve bag drop system will speed the check-in process, while a new, state-of-the-art baggage system - the first of its kind in North America - will track each bag individually through 10 kilometres of track and conveyor belt. Travellers will then proceed to security, where the Canadian Air Transport Security Authority (CATSA) has installed CATSA Plus, a combination of new technologies and procedures the agency hopes will improve passenger experience and decrease wait times. Calgary is the first airport in Canada to feature a full checkpoint with the CATSA Plus technology, which - among other things - will feature a remote screening room where a team of security o cers analyze x-ray images on multiple screens, a continually moving conveyor belt and an automated bin return for transferring empty containers to the start of the screening line. CATSA Plus is expected to eventually become the standard nationwide. There are new technologies and procedures at U.S. pre-clearance as well, where automated passport control kiosks are expected to reduce the amount of time travellers spend in front of a U.S Customs and Border Protection officer. (Similar kiosks will also be in place for arriving passengers clearing customs when entering Canada.) Calgary Herald, A8

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** NSA contractor arrested over 'stolen secret code used to hack Russia'**
The FBI has secretly arrested a National Security Agency (NSA) contractor suspected of stealing highly classified computer codes used to hack the computer systems of foreign governments including Russia and China, raising fears of another embarrassing intelligence leak to rival the Edward Snowden affair, the New York Times reported on Wednesday (...)The contractor in this case, who was reportedly arrested "in recent weeks", is suspected of stealing the NSA's "source code", used to break into the computer networks of rival powers such as Russia, China, Iran and North Korea. Independent (UK), New York Times, Washington Post, Associated Press (Times Colonist, Calgary Sun, Edmonton Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun)

*** FBI's new San Francisco head will try to mend fences with Silicon Valley**
Special Agent Jack Bennett was at the FBI's computer investigation lab in Quantico, Va., on a Sunday in March when an outside company showed the bureau how it could hack into an iPhone used by one of the San Bernardino, Calif., shooters. The tool would end the FBI's high-profile fight with Apple over access to the phone, but Bennett said there was no celebration... The iPhone fight exposed a rift between the FBI and Silicon Valley technology companies over encryption, and sparked a debate about the right balance between privacy and national security. Bennett, 52, was a key figure in that battle as head of the bureau's digital forensics labs, which extract evidence from computers and other devices and were tasked with accessing the San Bernardino shooter's phone. Bennett is now in charge of the agency's San Francisco division, where he views his role, in part, as trying to bridge the divide between Silicon Valley and the FBI. Associated Press (Toronto Star, B2)

*** Yahoo's Mayer suffers a new hit to privacy reputation**
Yahoo was ordered last year to search incoming emails for the digital "signature" of a communications method used by a state-sponsored, foreign terrorist organization, according to a government official familiar with the matter. The Justice Department obtained the order from a judge of the Foreign

Intelligence Surveillance Court. To comply, Yahoo used a modified version of its existing systems that were scanning all incoming email traffic for spam, malware and images of child pornography. The system stored and made available to the FBI a copy of any messages it found that contained the digital signature. Yahoo was forbidden to disclose the order, and the collection is no longer taking place, the official said Wednesday. The news story has opened a new chapter in a public debate over trade-offs between security needs and privacy rights that has cast a spotlight on the sometimes cooperative, sometime antagonistic relationship between Silicon Valley companies and the U.S. government... Although the digital signature was individually approved by a judge, who was persuaded that there was probable cause to believe that it was uniquely used by a foreign power, the collection was unusual because it involved the systematic scanning of all Yahoo users' emails. More typical surveillance court orders instead target specific user accounts. Toronto Star

*** Reported Yahoo email scanning revives surveillance concerns**
Yahoo's reported agreement to assist U.S. investigators by searching all email sent to hundreds of millions of accounts has stoked fresh concerns about mass government surveillance - not to mention questions over just how much privacy tech companies owe their users. Associated Press (Red Deer Advocate, D1; ABC News)

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** 'This is a way for everybody to heal': ex-Mountie on RCMP compensation for harassment**
A former Manitoba RCMP officer says it's time to heal, but no amount of money will ever pay for what she and others in the force had to endure. Sherry Benson-Podolchuk was following closely Wednesday after CBC reported that 500 past and present female RCMP officers were expected to be compensated at a Thursday news conference for allegations of sexual harassment, unwanted touching, and rape. "This is a way for everybody to heal," she said. Benson-Podolchuk, 53, isn't one of the 500 women being compensated but did reach out to the group to offer her support when she heard of their allegations a few years ago. Benson-Podolchuk was a single mom living on welfare in 1990 when she first joined the RCMP at a detachment in Tisdale, Sask. Benson-Podolchuk was excited to start a career in policing but said she was chronically harassed for being a woman at the detachment. "They always said tell the truth and obey the law and that you'd be protected by the RCMP, but they didn't tell you what would happen when you come to work and they'd start calling you beaver and raisin tits," she said. CBC News

*** Alberta man involved in police standoff opens up about incident, says he's turned his life around**
Nine months ago, an Alberta man was shot and critically wounded after being at the centre of a tense and dramatic standoff with police west of Edmonton. The bullet's still sitting on top of my C1," Caleb Seeton, 30, says of the bullet that hit him in the head. "It hit the stabilizing disc on the side and that's millimetres away from the brain or just disconnecting the spine from death or paralysis." But today, Seeton says his life is very different and that he is now addressing the issues in his life that led up to the event that nearly ended it. He says he was suicidal at the time, overwhelmed by work problems exacerbated by Alberta's beleagured economy. (...) On Jan. 5, 2016, RCMP were called to a home in the Greenbury neighbourhood of Spruce Grove, Alta. after receving reports of shots fired. The neighbourhood was put on alert , streets were blocked off and residents were asked to seek refuge in their basements. Seeton fired several rounds before turning a gun on himself. He was taken into custody following a tense standoff, and rushed to hospital in critical condition. (...) Incredibly, Seeton survived his self-inflicted gunshot wound and is now receiving mental health treatment. He says he is grateful to the police and first responders who ended up saving his life. "You know, I took a lot from the community that day, so if i could start giving it back, that would be a good place to start," he says. Global News

*** Five teens exploited**
Okotoks RCMP have laid a series of charges after they say some local teens were recruited through social media and exploited for sex. Mounties say the investigation launched by a school resource officer revealed five teenage girls between the ages of 13 and 16 had been victimized. The teens are being helped by Child and Family Services and Foothills Victim Services. Samantha Pedersen, 23, of High River is facing five counts of trafficking in persons under 18 years, five counts of procuring persons under

18 years, four counts of living off the avails of prostitution, four counts of sexual exploitation of a young person and one count of assault. Okotoks Mayor Bill Robertson called the case distressing. "My full sympathies go out to the families of those that are involved in this," he said. Postmedia Network (Calgary Sun, A2, Calgary Herald)

Montreal police renew programs targeting contraband, money laundering
The Montreal police will renew two programs that give the department a financial incentive to crack down on contraband tobacco and alcohol and follow the money-laundering trail of criminal organizations in the city. Montreal's city executive committee gave its approval on Wednesday for the police to renew both programs with the province retroactively from April 1 of this year to March 31, 2017. It's the ninth consecutive year the police force is renewing one of the programs, known as Actions concertées contre les crimes économiques et financiers. Under ACCEF, a Montreal police unit specialized in proceeds of crime works with Revenue Quebec to investigate money laundering and tax evasion related to the underground economy. The program has allowed authorities to "drastically increase" the seizure of illicitly obtained assets, a report to the executive committee from the Montreal police says. The department's $2.4-million budget for ACCEF this year, which includes the salaries of 12 officers and a civilian employee, is fully subsidized by the province. (...) This year, the Montreal police are contributing 33 police officers and two civilian employees, who work with the Sûreté du Québec, RCMP, the Régie des alcools des courses et des jeux and other agencies. Montreal's $5.7-million budget for ACCES is fully subsidized by the province. Montreal Gazette, A2

Grow-op dismantled
Fish and Wildlife Enforcement officers discovered a marijuana grow-op near LaManche Tuesday. Officers alerted the RCMP, who dismantled the 95-plant operation. The plants and equipment used to grow and harvest them have been seized. This is the third outdoor grow-op dismantled by police in the eastern Avalon region in just over a week, with a total of 249 mature marijuana plants seized. Sixty-five plants were found in an area off Salmonier Line Sept. 26, while another 89 plants were found in Makinsons last Saturday. The Telegram, A6

*** Alberta RCMP officer resigns, faces no disciplinary action after accusations of sexual misconduct**
A well-known and decorated Alberta RCMP officer facing allegations of sexual misconduct involving female co-workers has resigned and will face no disciplinary action, RCMP told Global News Wednesday. Const. Pernell Cardinal of the Maskwacis RCMP detachment was being investigated for six counts of sexual misconduct. An RCMP spokesman confirmed in late September that three of those counts were substantiated during an internal RCMP hearing. The exact details of the incidents were not released by the RCMP. Cardinal was suspended by the force in September, although it's not known if he was suspended with or without pay. He was given two weeks to appeal the decision. Cardinal has been in the news often, as an RCMP spokesperson for the Chelsea Yellowbird case. Yellowbird, 23, was shot and killed outside a residence on Samson Cree Nation in September 2011. Global News (2016-10-05)

*** Disgraced former RCMP officer sued over sexual misconduct allegations**
A B.C. correctional officer alleges that a disgraced Chilliwack RCMP officer stalked and sexually assaulted her in her home while she was on disability for post-traumatic stress disorder. The officer claims that Daniel Marshall, a constable who was last year forced to resign over allegations of on-duty sexual misconduct, was dispatched to her home in September 2014 in connection with concerns over her mental health. In a notice of civil claim filed in B.C. Supreme Court, she says that she and Marshall discussed her mental health and substance abuse issues. In the following two weeks, Marshall, while on duty, returned to her home several times, stalking her and ultimately sexually assaulting her a number of times, says the lawsuit. "At all material times, the defendant, Daniel Marshall, was well aware of the mental instability and vulnerability of the plaintiff," says the suit. (...) In December an internal board of the RCMP found that all six allegations brought against Marshall were established. Marshall was ordered to resign from the force. Two complainants testified that they had sexual encounters with Marshall after meeting him during the course of his police work. Another case involved Marshall's alleged failure to properly investigate a report of a sexual assault. Vancouver Sun (2016-10-05)

*** Clown capers a problem, say police**

Incidents involving people dressed as clowns are on the rise in Nova Scotia. A 24-year-old man was arrested Tuesday evening after witnesses reported he grabbed at the clothing of a young boy walking with other youths along School Street in Clark's Harbour. "The man was wearing a clown mask and a T-shirt with a clown on it at the time of the incident," said RCMP Cpl. Jennifer Clarke. The suspect faces charges of breach of undertaking. He is scheduled to appear in Shelburne provincial court on Nov. 2. Police are also investigating after a photo posted on social media appeared to show a clown standing on a sidewalk outside a Halifax high school, the Canadian Press reported Tuesday. Chronicle Herald, A6

*** Police fire out warning to bomb, gun hoaxers**

Halifax police are warning would-be hoaxers that they could be charged and if convicted could do up to five years in jail. The force has had to deal with a string of bomb threats, with a dozen false alarms in less than a month. Halifax Regional Police and Halifax District RCMP have responded to a total of 12 bomb threats since Sept. 15. "We have a responsibility to treat each one as a legitimate call and do everything possible to mitigate the threat and work with the affected organization and other stakeholders," said the release. The range of charges under the Criminal Code of Canada include: public mischief (false report), five years' imprisonment mischief (render property or interferes with use), two years' imprisonment uttering threats, five years' imprisonment false messages (intent to alarm), two years' imprisonment hoax regarding terrorist activity, five years' imprisonment Halifax police and RCMP said in a news release that they take false reports seriously. Chronicle Herald, A4

*** People pack into Westview to hear about fentanyl scourge in Maple Ridge**

The question that Sherry Hebeler wanted answered Wednesday at the fentanyl forum in Maple Ridge was where was the help for her son when he needed it. Her son Bradley Hebeler, 33, died in a hospital washroom in Novermber 2015, after apparently taking crystal meth that had been laced with fentanyl. He had been admitted to the hospital and was addicted to painkillers but had gone missing. "Nobody found him for two hours," Hebeler said, adding it was only hospital security that found him. And on three times previously when her son overdosed, Hebeler had called police and asked that he be picked up on outstanding warrants when he was released from hospital. She felt that being in jail might be the safest place for him. But Ridge Meadows RCMP never did send a car to pick up her son. (…) Ridge Meadows RCMP Supt. Dave Fleugel said dealers are selling fentanyl and lacing other drugs with it because it's cheap and profitable. It's also powerful and easily obtainable. "It's very difficult for our border services and our postal services to detect." Fentanyl so far has killed 20 people in Maple Ridge this year. That number could hit 30 by the end of the year. Provincewide, it's killed 488 people since the start of the year. Fleugel said it's hard to prove a manslaughter charge against a dealer for selling fentanyl that leads to an overdose. Maple Ridge News

*** Saskatoon man, 25, charged after police seize fentanyl, cocaine, methamphetamine, guns**

A Saskatoon man is facing charges after police seized guns and drugs, including hundreds of fentanyl pills, from a vehicle. Officers from the Combined Forces Special Enforcement Unit searched the vehicle in the 3300 block of 8th Street E. Friday. A duffel bag containing 682 fentanyl pills, 22 grams of cocaine and a loaded handgun was seized. A further search of the vehicle found 550 grams of methamphetamine, about half a kilogram of crack cocaine, a handgun with a silencer and approximately $5,000 in cash. A 25-year-old man was arrested. He was carrying approximately $4,000 in cash at the time. The man now faces a number of charges, including possession and trafficking of fentanyl and cocaine. Both the RCMP and the Saskatoon Police Service say the investigation is continuing. CBC News (2016-10-05)

*** SQ breaks up crime ring that stole big rigs, dealt drugs**

The Sureté du Quebec says it has broken up a crime ring that stole heavy equipment and machinery, and trafficked in drugs. About 200 police officers conducted raids early Wednesday morning on the South Shore, in Laval and in and around Montreal. Police arrested 19 people including Patrick and Steve Daraiche, the owner of the Metaux St. Jean scrapyard and his brother. Police said the Daraiche brothers were the ringleaders of a group that stole big trucks and tore them down in order to resell parts. Investigators say it was a very organized network. "The parts were being stolen to put on other stolen vehicles or to recover the metal," said SQ investigator Eric Stevens. Police said they received many tips from the public as they conducted their three-year investigation into the ring. In addition to dealing in

stolen parts, the family was also dealing drugs, according to police. Officers seized $3 million worth cocaine, as well as firearms, 500 marijuana plants, and about 10 kg of cannabis. "We seized 65 kilos of cocaine that were hidden in a truck that was actually in the garage," said Stevens. Police found about two dozen stolen trucks on the lot, several in the process of being dismantled. CTV News (2016-10-05)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Man who killed and dismembered Calgary landlord Wendy Marie Hewko granted full release
Nearly a decade after the killing and dismemberment of his Calgary landlord, the man responsible has been given full release. Last month, the Parole Board of Canada (PBC) gave the green light for Dean Victor Gosse, 46, to leave a halfway house where he'd been subject to a nighttime curfew since May, 2015. But the board won't release information on where Gosse is expected to settle, stating to do so could "jeopardize the safety of any person" and "adversely affect the reintegration of the offender in the society." In its reasons for decision, the PBC said his behaviour in the past few years has been "positive" and that its statistics show two of three similar offenders won't commit an indictable offence within three years of release. "Your integration potential is assessed as moderate," it stated. Gosse was sentenced to 10 years for manslaughter in the killing of Wendy Marie Hewko, 48 in 2007. He admitted to the killing that occurred amid a cocaine-fuelled argument over rent owed on the basement suite of the woman's Castleridge home. Postmedia Network (Calgary Sun, Calgary Herald)

*** Cellphone stun gun**
Kingston Police seized a stun gun disguised as a cellphone after a traffic stop Tuesday afternoon. At about 3:30 p.m., a patrol officer was westbound on Princess Street near Albert Street when he noticed a General Motors SUV with no front licence plate but a rear Ontario plate. The Highway Traffic Act requires all vehicles in Ontario to have front and rear plates. Turning around, the officer stopped the vehicle near the Princess Street and University Avenue intersection. Running the rear plate through the Ministry of Transportation database, it showed it hadn't been reported stolen but was supposed to be attached to a Volvo sedan. (…) The provided name yielded no results in the Canadian Police Information Centre (CPIC) database. Speaking with the occupants of the vehicle, the officer formed grounds to believe the man was lying about his identification and was arrested for obstructing police. While the man exited the vehicle, officers saw a jacket filled with multiple cellphones and knives. There was also a wallet in the jacket with photo identification of the male passenger with his actual name and a Correctional Service Canada parole card. A search on CPIC showed the man was on a recognizance out of the Niagara Falls area to remain in his residence. He was also on a weapons prohibition following a prior conviction involving multiple weapons. Kingston Whig-Standard, A3

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

House of Pain
An editorial states, "The College of Physicians and Surgeons of New Brunswick and the provincial government merit recognition for their concern and timely action to better control the prescribing of opioids, thus lessening addiction rates to these narcotics. Recently I've discussed the rising death tolls from illegal narcotics, especially the synthetic fentanyl that can be many times more potent than morphine, and it's deadly variant carfentanyl, 10,000 times more potent than morphine. Just three salt-sized grains of the latter can kill a person. It's only legitimate use is to tranquilize large animals like elephants. New Brunswick isn't immune from the continent-wide problem. Canadians are the second heaviest abusers of opioids in the world. Exactly why merits some well-funded research. Part of the relatively new fentanyl problem is that authorities have taken fairly successful steps to stop other legally prescribed opioids like oxycontin and dilaudid from reaching the illegal street trade. Criminal drug suppliers thus turned to manufacturing their own synthetic versions, with no controls, little regard for dosages, and mixing it with other narcotics. It's cheaper and supply is reliable. Policing agencies can deal with the organized criminals, but a significant part of street-trade users does not involve the stereotypical, homeless, zonked-out drug addict shooting needles in dingy alleyways. Many addicts are

people who became so via legal prescriptions, often for chronic pain. And as physicians are cutting back, their only source is the street trade, which is now alarmingly risky and deadly. Yet if physicians have been inadvertently complicit in the past, so too have patients. Pain, especially chronic pain, persistent pain, is debilitating. " Times & Transcript, A10

*** Alberta steps up surveillance in new measures to tackle opioid drug crisis**
The Alberta government is announcing new measures it has put in place in response to the opioid crisis. It follows the latest information released by Alberta Health Services that shows 153 people in Alberta died from apparent fentanyl-related overdoses in the first half of this year. Now the office of the Chief Medical Examiner is gathering additional data in every death where opioids are believed to have been a factor. A statement from Justice Minister and Solicitor General Kathleen Ganley describes the previous data collection as "inadequate" and explains the medical examiner is working closely with the Chief Medical Officer of Health to gather as much data as possible. It's a move that's being described as long overdue by critics who have been calling for it for some time. The additional data comes from the fact that, starting in July 2016, the OCME now lists the drugs that caused a person's death on their death certificate. The department of Justice and Solicitor General said this will allow for the OCME to better collect and review information which, in turn, will allow the OCME to provide comprehensive data regarding opiod death to the Alberta Health. CBC News

*** "People need to be aware"**
Five near-fatal overdoses last weekend in Barrie have put the dangers of recreational drug use in the spotlight, say front-line professionals. "At the end of the day you don't know what you're getting," said Barrie Police Const. Sarah Bamford. "That's why we're telling people consuming any type of drug there's great risk associated with that." County of Simcoe Paramedic Services have recorded 564 overdoses so far this year. Those numbers include alcohol overdoses or drug-alcohol combinations and are not broken down into specific categories such as types of drugs. If the overdosed patient fits the protocol of a opiate overdose then a drug called Narcan is given by the paramedic in the field, explains Meredith Morrison, Deputy Chief, Performance, Quality and Development with County of Simcoe Paramedic Services. (…) Preliminary 2015 figures from the Office of the Chief Coroner, subject to change once the statistical year has been completed, show 6 fentanyl toxicity deaths in Barrie and a total of eight in Simcoe County. The Barrie numbers in the previous three years were less than five and are undisclosed as a result. Five young people in their 20's overdosed last weekend in Barrie after they all attended the same party at an apartment on Dunlop Street East. Barrie Today

*** Both violent and non-violent crime up in Waterloo Region**
Crime is up in Waterloo Region and the increase is larger than national and provincial averages, according to Statistics Canada. A report presented to the Waterloo Regional Police Services Board on Wednesday indicated both violent and non-violent crime had risen in 2015. The report showed there were three homicides in the region in 2014 compared to six last year. Attempted murders were down year-over-year, going from seven in 2014 to two in 2015. The Crime Severity Index, a weighted measure based on both the volume and severity of crime, increased in Canada, Ontario, and Waterloo Region by 5%, 2%, and 7.4% respectively. Focusing on violent crimes alone, Canada saw a 6% increase, Ontario a 3% increase, and Waterloo Region a 6.2% increase last year. The report points out however, that while violent crime is increasing in the region, it remains lower than national and provincial levels. Locally, person-to-person robberies were up 27% and assaults were up 7%. CTV News

*** Cities just don't get the danger of rural Saskatchewan crime**
The saddest days in Saskatchewan are when we see people divided, especially when that division is caused by a lack of understanding. Such days have been all too common in this province this year. And what's even sadder is when the misunderstanding relates to issues of safety, which is definitely not something that should divide us. Sadly, though, city people seeing the issue from the outside may not fully appreciate how unsafe some rural people feel. One of the flashpoints in the debate on rural crime has clearly been the racially charged incident near Biggar in which Colten Boushie of the Pheasant Rump First Nation died from a gunshot wound in the farmyard of Gerald Stanley. Stanley has been charged with second degree murder and has received bail that confines him to the vicinity of his farm until his trial date. (…) That has created policing challenges in two ways. There is sometimes no easily accessible

neighbour to watch properties and it's tougher to get law enforcement to remote locations to deal with an incident. Also, with fewer people in rural Saskatchewan, it is harder for those who remain to afford the policing costs. Municipalities of fewer than 5,000 people with RCMP detachments pay $77.06 per capita while those communities without a detachment pay $47.68 per person for policing. Any additional positions at a detachment would cost an additional $130,000 per year, so simply paying for police is getting harder. Canora Courier

* **Use health-care dollars on treatment and recovery, not on supervised drug-use sites**
Thirteen years ago, Vancouver's Downtown Eastside opened the first supervised drug-injection site in North America. This was to be a three-year clinical trial with an evaluation summary and reports for each year to determine the significance of Insite with regards to harm reduction in overdose mortality. The very rationale for the endeavours in Sydney, Australia, and Vancouver were specifically to gather data, they were created as scientific pilot projects. Beginning in 1996, snowball sampling was used to recruit injection drug users in the Downtown Eastside for a prospective cohort study. Data for the study comparing service users were obtained from 400 members of this cohort who returned for a semi-annual follow-up interviews and who reported using drugs by injection in the past six months. Snow balling is when the first respondent refers an acquaintance and that friend refers a friend and so on. Such samples are biased because of the higher response rate. In another study in 2005, those reported to have used Insite tended to be younger, inject in public, homeless or unstable, use cocaine daily and recently to have had a non-fatal overdose. Kamloops This Week

* **Sex Workers Explain the Struggles of Running An Illegal Business**
An editorial piece states, "When Dane gets into a car with a client, the first thing he does is ask the guy to pull out his dick. It's a measure he developed after nearly getting arrested for having an escort ad on Craigslist. "I met up with the person, and we drive around the block and he starts talking," said Dane, a Seattle-based escort. "The way he was talking was weird, and you could tell he didn't know anything about gay sex. After a while I told him to stop." That's when the cop pulled out a badge, terrifying Dane before letting him off with a lecture. Since then, Dane does what he can to ensure that his clients are honest about their intentions. He previously used Rentboy.com, but federal regulators seized the site over a year ago, and its legal status today remains unclear. Once the most visible site for male escorts, Rentboy allowed them to check client reputations and block minors, providing a peek at what a regulated escorting marketplace might look like. Because their work is illegal, escorts face a near-total lack of access to the protections and professional services that other entrepreneurs take for granted, from marketing to legal advice to insurance and beyond. As a result, sex workers who already face physical risks and financial volatility endure a unique form of economic isolation." VICE News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

* **NWAC Says Get to Work on Murdered and Missing National Inquiry**
At the October 4th Sisters In Spirit vigils throughout the country, we heard family members describe their disappointment and concern about the delays in starting the National Inquiry. The Native Women's Association of Canada (NWAC) would also like to express our disappointment and frustration with the lack of substantial progress in the National Inquiry into Missing and Murdered Indigenous Women and Girls since its official launch on August 3rd, 2016. "We are very concerned. The two-year mandate that the National Inquiry Commission has been given leaves a very short time for the mandated tasks of establishing regional and issue-specific advisory bodies, creating trauma-informed and culturally aware counselling services, and beginning the substantive process of listening to family members, loved ones, and survivors express their stories all across Canada," said NWAC President Francyne Joe. (…)The time has come for the Inquiry Commission to illustrate its competence in being able to adequately address the systemic causes behind the high rates of violence against Indigenous women and girls. The immense responsibility associated with the tremendous task of addressing one of the gravest human rights abuses in Canada's history leaves no time to waste. The time to begin this important work is now. Net News Ledger

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

City has high expectations
Hand over a share of the tax revenue and give up the addresses of medical marijuana grow ops. Those are among the requests City of Calgary officials have for Ottawa along with a zero-tolerance policy for drivers under the influence of cannabis as the feds hammer out legislation for legalized pot. In an Aug. 24 submission to the federal government's Task ForceMarijuana Legalization and Regulation, CityManager JeffFielding calls for ongoing discussions "throughout the legalization process to ensure clear delineation of roles and expectations" between the three orders of government. "Municipalities will be an important partner in developing, implementing and enforcing new regulations in this area," Fielding wrote. The four-page document outlines concerns held by the Calgary police and various city departments on the implications of legalizing pot. Postmedia Network (Calgary Police, A3, Calgary Herald)

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Government accused of hiding full scope of Phoenix fiasco**
The federal government is being accused of hiding the full scope of the Phoenix payroll fiasco. The largest union representing public servants is demanding the government release updated information about the number of workers experiencing pay problems. "What is it that they're trying to hide?" said Chris Aylward, the national vice-president of the Public Service Alliance of Canada. Since trouble with the government's computerized pay system emerged, Public Services and Procurement Canada has said nearly 82,000 workers have experienced irregularities with their pay. But that number only includes workers who came forward with problems before July 1, 2016. The government has not publicly released the number of employees who have experienced trouble after that date. During a Phoenix update on Wednesday, the deputy minister of PSPC was asked about new numbers, but didn't offer any details. "It's an ongoing queue ... I can't really answer the question specifically, it's an ongoing flow," said Marie Lemay, the deputy minister. She explained the new cases are being dealt with separately from the backlog bulk. "The others that are coming in, we're treating them, there's a queue. But sometimes we are not treating them as fast as we will when we'll be in our steady state." Workers who formally registered problems before July 1 have been told their issue will be dealt with by the end of October. There is no solution timeline for employees who joined the queue after that date. CBC News

*** Ottawa says it has 'no reason to sue' IBM over issues with payroll system**
The head of the federal department overseeing the effort to fix the Phoenix civil-servant payroll system says the government isn't contemplating legal action, even though at least one other country has gone down that path. Tech giant IBM created the Phoenix pay system, basing it on the PeopleSoft program that is used worldwide and tailoring it to the federal civil service. The state government in Queensland, Australia, unsuccessfully tried to sue IBM for a similar paysystem problem in a case that wrapped up earlier this year. That case was getting started just as the Canadian government went to tender for its new pay system. Now, the federal Liberal government has budgeted an extra $50 million to handle issues related to Phoenix, including millions to IBM to make fixes to the system. "We have no reason to sue IBM right now. IBM is respecting its contract. They have been good partners," Marie Lemay, deputy minister at Public Services and Procurement Canada, said. "When we find issues that have to be corrected, they're right there, they're correcting it." Globe and Mail, A14

Phoenix backlog deadline no cure all
The senior bureaucrat overseeing the federal government's botched payroll system confirmed Wednesday that not all pay problems affecting Canada's public servants will be resolved by the promised Oct. 31 deadline. Marie Lemay, Public Services' deputy minister, insisted the government is on track to clear the backlog of 82,000 cases created by the Phoenix pay system that were sent by 46 federal departments for processing to the pay centre in Miramichi, N.B., by officials' self-imposed Oct. 31 deadline. "We're really on target," she told reporters during a briefing Wednesday. "The next month is a

big month, but we believe we are on target. ... We believe we will clear the backlog for the 31st." But the deadline only applies to the 46 departments that were sending their payroll processing to Miramichi, which covers about 191,000 employees and has 550 compensation advisers. Lemay was unable to say what happens to employees facing Phoenix foulups who work for 55 other departments that manage their own compensation and don't use Miramichi. Ottawa Sun, A8 (Ottawa Citizen); * Le Droit; * Canadian Press (The Guardian, Times & Transcript, Daily Gleaner); * Le Journal de Québec (Le Journal de Montréal)

OTHER / AUTRE

*** Un tribunal bangladais innocente un étudiant canadien**
Un tribunal bangladais a blanchi un étudiant de l'Université de Toronto de toutes les allégations qui pesaient contre lui relativement à une attaque terroriste qui a fait 25 morts cet été. Le juge Nur Nabi a rendu sa décision mercredi après qu'un enquêteur eut demandé que soit innocenté Tahmid Hasib Khan, un résidant permanent du Canada. Le procureur Abdullah Abu a dit que M. Khan a été blanchi de tout soupçon concernant sa participation possible à l'attaque perpétrée le 1er juillet contre le restaurant Holey Artisan Bakery, à Dacca. M. Khan avait été libéré sous caution dimanche. L'attentat a été revendiqué par Daech (le groupe armé État islamique), mais le gouvernement pointe plutôt du doigt des militants locaux. Un avocat canadien embauché par la famille a expliqué que la libération de M. Khan a été ordonnée dimanche quand la police a présenté au tribunal des documents indiquant que les enquêteurs n'avaient trouvé aucune preuve de la participation du jeune homme de 22 ans à l'attentat. La Voix de l'Est, 25; Canadian Press (Red Deer Advocate, Winnipeg Sun, Toronto Sun, Ottawa Sun, Calgary Sun, Times Colonist, Hamilton Spectator, Waterloo Region Record, Toronto Star, Times & Transcript, Kingston Whig-Standard)

*** Détention - Homa Hoodfar a été victime de torture psychologique en Iran**
Homa Hoodfar avait beau être terrorisée dans sa cellule de la prison d'Evin, elle savait qu'elle pourrait, tout au long de sa détention, se raccrocher à une lueur d'espoir : ses geôliers ne feraient pas d'elle une seconde Zahra Khazemi, cette photojournaliste irano-canadienne torturée et violée avant d'être assassinée, dans la même geôle, il y a maintenant 13 ans. " Ils me disaient qu'ils renverraient ma dépouille au Canada. [...] J'étais prête mentalement à passer quelques années en prison, ou, comme ils disaient, peut-être 15 ans ", a relaté la professeure à la retraite de l'Université Concordia, relâchée le 26 septembre dernier après 112 jours de captivité. Le Devoir, A8; CBC News

*** Saeed Malekpour's story matters too**
An opinion piece states, "Actions speak louder than words. And in the case of Saeed Malekpour, Prime Minister Justin Trudeau's words are being put to the test. Tuesday was the eighth anniversary of the Canadian permanent resident and Iranian national's arrest in Iran on dubious charges. The web developer came to Canada in 2004 and worked in Richmond Hill, Ontario. He returned to Iran in 2008 to see his ill father and it was then that he was arrested. According to Amnesty International, which is lobbying for his release, Malekpour was originally sentenced to death on charges including "acting against national security by spreading propaganda against the system"; and "insulting and desecrating Islam." He is now sentenced to life in prison on charges of "insulting and desecrating Islam". The charges reportedly relate to his work on writing computer coding that was in turn used by a pornography website, with which Malekpour denies having any involvement. While the Canadian government hasn't so far been successful in securing Malekpour's release, that didn't stop it from speaking up in the past when he was faced with the death penalty..." Winnipeg Sun, A12 (Toronto Sun, Edmonton Sun)

*** Liberals urged to press Iran on executions of prisoners during Iran-Iraq war**
A group of Iranian Canadians is calling on the government to add a tough new element to its annual United Nations resolution on Iran's dubious human rights record an international call for a war crimes investigation. The group, which calls itself Canadian Friends for a Democratic Iran, will make the request later today at press conference on Parliament Hill. The group will present what it says is new evidence that shows complicity in a mass killing of Iraqi prisoners by senior Iranian government officials in 1988 at the end of the Iran-Iraq war. An audio recording from the era surfaced in August that implicates high-level

members of the current Iranian regime, including the country's current justice minister, said Shahram Golestaneh, the group's director. Canada has taken the lead each year since 2003 in sponsoring a resolution at the UN condemning Iran's human rights record. The Guardian

*** Canadian general: Fighting Islamic State will grow harder after retaking Mosul**
A Canadian general who directs training of Iraqi security forces says the widely anticipated ousting of the Islamic State group from its stronghold of Mosul in northern Iraq is likely to transform the extremist group into an even more dangerous force. Brig. Gen. Dave Anderson, speaking from a U.S.-led coalition military facility in Iraq, told reporters at the Pentagon on Wednesday he is certain the Iraqis will prevail in Mosul. "But the fall of Mosul does not mean that Daesh is defeated by any stretch of the imagination," Anderson said, using an acronym for the Islamic State group, or ISIL. "It just means it's defeated in its current format." Associated Press (Waterloo Region Record, A4, Telegraph-Journal, Times & Transcript)

INTERNATIONAL

Hurricane Matthew heads to Bahamas after killing 15 across Caribbean
Hurricane Matthew took aim at the Bahamas on Thursday after leaving behind a humanitarian crisis in Haiti. At least 15 people died from Matthew's wrath in Haiti, the Dominican Republic and St. Vincent and the Grenadines, officials said. Haiti, still recovering from the catastrophic 2010 earthquake, was hit the hardest. As the death toll rises and crucial infrastructure crumbles, thousands have been displaced. Mourad Wahba, the UN secretary-general's deputy special representative for Haiti, described Matthew as the "largest humanitarian event" since the earthquake. CNN

*** Rescuers battle to reach remote areas of Haiti hit by Hurricane Matthew**
Rescue workers and aid agencies were hoping to begin reaching remote areas of south-west Haiti on Thursday to assess the damage wrought by Hurricane Matthew, which has killed at least 35 people, displaced 15,000 and left hundreds of thousands in need of assistance. The hurricane, which hit Haiti on Tuesday, brought 145mph winds and torrential rains that have destroyed more than 3,200 homes, ruined plantations and drowned animals. Efforts to access the worst-affected areas – including the Grand'Anse and Sud departments – have been hampered by flooding, the collapse of communications networks and the destruction of a key bridge. But as the weather clears, Haitian authorities, the UN and national and international non-governmental organisations are starting to get a better idea of the scale of the destruction. The airport in the capital, Port-au-Prince, has reopened for humanitarian flights and two portable satellites are being used to restore communications with cut-off areas. Marie Alta Jean-Baptiste, the head of the country's civil protection directorate, warned the death toll was likely to rise as emergency workers reached the stricken regions. The Guardian

*** US Braces For Hurricane Matthew, 2 Million Urged to Evacuate as Deadly Storm Batters Bahamas**
Hurricane Matthew tracked closer to the U.S. coast on Thursday, strengthening over the warm waters of the Atlantic as officials warned residents of coastal areas to get out while they can. "The extreme winds of a major hurricane can do a lot of damage and not just at the coast," Rick Knabb, Director of the National Hurricane Center, told "Good Morning America." "Those winds can penetrate inland and that would be more so the case the closer it gets to the coast," Knabb warned. "In addition to the wind, you have storm surge potential. People who have been told to evacuate, they need to get out this morning, right away, because time is running out fast. You don't want to be caught in the storm surge which is the deadliest hazard of all." Officials in three states urged some 2 million people to head to safer ground as the most powerful storm to threaten the Atlantic coast in more than a decade continued on its path toward the U.S. at about 10 mph, packing 125 mph winds. Some 8 million Florida residents scrambled to make last-minute preparations as the deadly storm was expected to strengthen to a Category 4 hurricane with 145 mph winds before approaching the state on Thursday night. Up to 15 inches of rain may fall in spots, and a storm surge of up to 8 feet was expected along the coast from central Florida to Georgia. The National Hurricane Center extended its hurricane warning and its hurricane watch further north into Georgia and South Carolina, respectively, as the eye of the storm churned about 255 miles southeast of West Palm Beach, Florida at 5 a.m. Thursday. ABC News; FOX News; Sky News

* **Airlines Cancel Over 2,500 Flights Ahead of Hurricane Matthew, MIA to Close at Noon**
As Hurricane Matthew bears down on the southeastern portion of the country, residents of coastal communities in the south are not the only ones preparing their next move. Airlines and airports are working around the clock to weather the storm and ensure a quick restoration of their schedules. More than 2,500 flights have been cancelled from Wednesday through Friday so far, according to FlightAware.com as of Thursday morning. There have been more than 1,400 cancellations today alone and over 1,100 and counting for tomorrow. The most impacted airports were Miami International Airport and Fort Lauderdale-Hollywood International Airport, both of which plan to shut down today. Fort Lauderdale will halt operations at 10:30 a.m. with Miami to follow at noon. ABC News

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Sent to: !DMS External; PS.F DL_DMS F.SP

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
October 19, 2016 / le 19 octobre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Canada's cybersecurity strategy is anemic: expert
Canada's cybersecurity strategy is so outdated, the last time it was revised was in 2010 when Conservative Vic Toews was public safety minister. Six years doesn't seem like a long time for a policy to lay untouched, but in the world of espionage it's an eternity. "I would suggest that our cybersecurity strategy is somewhat anemic," Stephanie Carvin, a former Government of Canada national security analyst, said. The assistant professor at Carleton University's Norman Paterson School of National Affairs said she believes Canada's strategy on the public safety department's website lacks any teeth. "The government has principles and it has a document that's called the cybersecurity strategy, but it's not clear to me that we actually do have a strategy that is behind it with any kind of meat." **Public Safety Minister Ralph Goodale** acknowledges the gaps in our system and has said he is committed to plugging them. ***"We're looking at the governance of our cyber security systems, we're looking at the technology,***

we're looking at the financing to see what's necessary to make us stronger," **Goodale** said. When he was appointed **minister**, **Goodale** was mandated to lead a full review of infrastructure to protect Canadians from cyber-threats. Department officials say that consultation will be done in December. There is no fixed timeline for the changes to be implemented, but **Minister Goodale** is looking to other nations for advice. "Israel for example, is considered to be very good at this, as well as the United States and the Brits and others," **Goodale** said. Surghar Daily

* **Chinese billionaires take interest in Canadian clean technology**
Canadian clean technology companies could be the next major investment for China's business elite. But cyber-security experts and the opposition are warning that the keen interest from Chinese investors must be treated carefully. "For us at the moment, natural resources is not the top priority," said Wang Chaoyong, the chairman and CEO of ChinaEquity, one of the country's most successful independent venture capital firms. "We are more interested in investing in environment technology, clean tech [and] innovative sectors such as creative industries," Wang said in an interview with CBC News. (…) As the federal government tries to strengthen ties with China, it is also downplaying concerns about investment and security. "There's a well-established Canadian process for dealing with these issues under the Investment Canada Act with all of the appropriate safeguards in place," said **Public Safety Minster Ralph Goodale**. "Canada's a country that welcomes foreign direct investment. Obviously, it needs to be a net benefit to Canada and all the security requirements need to be met. The procedure is there already in the law to deal with that," he added. CBC News

Who will pay for the RCMP's epic failure?
An opinion piece states, "The careers and lives of women in the RCMP were ruined. Yet an apologetic RCMP refuses to truly be accountable. On Oct. 4, Canadians were whipped into a froth of righteous indignation by an act of criminal harassment toward someone just trying to do his job—the odious beer-can toss by a Blue Jays fan at a Baltimore Orioles' left fielder during the American League wildcard game. Toronto police issued a photograph of the presumed suspect within a day. The *Toronto Sun* ponied up a $1,000 reward. (…) So where was the similar chant for accountability two days later, on Oct. 6, after RCMP Commissioner Bob Paulson's shockingly inadequate apology for far more grievous workplace assaults against potentially thousands of female RCMP officers? (…) Meanwhile, a Liberal government—one that claims to take violence against women seriously—stood by in nodding accord, represented by **Public Safety Minister Ralph Goodale** and Labour Minister MaryAnn Mihychuk. **Goodale**, who inherited the cesspool file, took a "Move along, folks, nothing to see" stance: The apology and payout "closes the door on a deeply troubling and unfortunate period in the history of our national police force," he said. (…)Yet **Goodale** expressed hope that the actions taken will ***"help strengthen Canadians' faith and trust in their national police force."*** That police force was once famous for always getting its man. No more." Macleans

A national security report card: Trudeau benefits from peaceful times, but must finish agenda,
An opinion piece states, "The Liberal government, in its first year in power, has enjoyed the benefit of a highly advantageous environment for national security policy-making: a majority in Parliament; ineffective political opposition; no terrorist attacks; a public whose attention is largely elsewhere. The pressure has been offand the government has been able to pursue its agenda at a measured pace. There was one close call, when Aaron Driver, placed under a terrorism peace bond, came very close to slipping the attention of the authorities and conducting some kind of attack using home-made IEDs. A dramatic shootout in August in front of his residence in Strathroy, Ont., ended in his death and the foiling of a plot. There was some fast intelligence and law enforcement work in this outcome, but also a good deal of luck. But even the best of political environments comes with its own challenges. No pressure doesn't mean a government is offthe national security hook. The Liberal government has some big election and mandate promises to live up to. (…) The most radical promise the Liberals made was to consult Canadians and increase transparency around intelligence and security issues. In fulfilling this promise, the government launched in September a "Green" (discussion) paper on national security, addressing 10 issues about which it encourages public discussion and input. An online portal is open until Dec. 1 and has already seen some 8,000 responses. In addition, the government has consulted with experts and stakeholders; the parliamentary Standing Committee on **Public Safety** and National Security is touring the country, holding "open mic" sessions; **Public Safety Minister Ralph Goodale** is on the road; and even his

officials have been thrust onto the public parapet. How the government will digest and respond to the Green paper exercise remains to be seen. But this is an unprecedented and welcome experiment, whether it succeeds, fails or fizzles." Ottawa Citizen, A9

TOP STORIES / MANCHETTES

Blank passports found in theft ring bust
A major investigation by Winnipeg police that recovered hundreds of thousands of dollars in stolen property has raised national security concerns after blank passports were among the items officers found. Tuesday, police announced Project Heavy Metal identified 20 suspects, including nine arrested in Manitoba, who are facing 140 charges related to a theft ring that operated across Western Canada. Calgary and Edmonton police, as well as the RCMP, helped with the investigation, which recovered more than $300,000 worth of goods stolen during break-ins and other thefts. Two RCMP uniforms and police equipment were recovered after a search warrant was executed at a Calgary home in September, Insp. Barry Kostchuk said. Vehicles, camper trailers, snow blowers, lawn-care equipment, new tires, tools, key-cutting machines and electronics were recovered. The most alarming items discovered may be the blank passports and birth certificates. Winnipeg police weren't ready to comment Tuesday about the blank identity documents - how many were found or if they were taken from government offices or are fakes, such as bogus Canadian passports sold online for less than $200. The theft of genuine blank Canadian passports has opened doors in the past for criminals such as human traffickers and raises concerns about dangerous people being allowed into the country. In 2002, the RCMP foiled a scheme to sell 246 stolen blank Canadian passports - but not before some of them found their way into the hands of international people-smuggling rings. An informant tipped off RCMP the black-market "books," stolen in June 2002 from the Scarborough passport office, were being sold on the streets of Toronto for $1,000 apiece. Winnipeg Free Press, 1

* **Businesses must buck surveillance**
Resisting government mass surveillance isn't just the right thing to do - it's good for business, whistleblower Edward Snowden told a Toronto cybersecurity conference Tuesday. Speaking via video link to the annual Canadian industry event SecTor, Snowden brought up the recent revelation that Yahoo Inc. had agreed to scan customers' emails for U.S. intelligence. Shortly after, Verizon Communications Inc. asked for a US$1 billion discount on its US$4.8 billion agreement to buy the company, according to a report in the New York Post. "If you collaborate with the government in this regard, far beyond what the law requires, it can actually have a significant, substantial consequence for your valuation," Snowden said. "Yahoo, which is a very powerful, very rich organization, cooperated beyond what was legally required. And it damaged its brand (...)"Snowden cited Open Whisper Systems, which makes the encrypted messaging app Signal, as an example of an organization that benefited from pushing back against a government request for cooperation in a surveillance program. With the help of the American Civil Liberties Union, Open Whisper Systems fought a gag order on a subpoena for information associated with two phone numbers. Ultimately, Open Whisper Systems had to comply with the subpoena, but the damage was mitigated because of another Snowden-approved policy: Only retaining as much personal data as absolutely necessary. The subpoena asked for browsing history and tracking data stored in web browsers, but Signal doesn't collect that information. "Companies work for their customers first. This means they should only hold the data that's absolutely necessary for the operation of their businesses," Snowden said. "When this story broke about Open Whisper Systems abiding by this principle, the fact they were being compelled through the state's monopoly on use of law actually benefited their brand." Postmedia (Financial Post, FP3; National Post);

* **Snowden says Trudeau afraid to kill anti-terrorism bill**
Whistleblower. Hero. Traitor. Patriot. These words and more have been used to describe former cybersecurity contractor Edward Snowden, who in 2013 copied and distributed thousand of documents to reporters and whose stories of Western intelligence agencies — including Canada's Communications Security Establishment (CSEC) — shook the world. This morning Snowden told the the annual SecTor cyber security conference in Toronto that Prime Minister Justin Trudeau want to amend the controversial Bill C-51 anti-terrorism law and not repeal it because he "is afraid of being attacked for being soft on

terrorism." Speaking by video from Russia, where he fled to avoid prosecution by U.S. authorities, Snowden said the legislation, needs three fixes: First, a judicial body should have oversight over federal intelligence agencies that has the power to prosecute authorities that have broken the law. Second, because intelligence agencies are trading personal information of citizens "like baseball cards" citizens should be told if the data sharing hasn't led to an arrest for criminal activity. And finally, what Snowden called the criminalization of speech through vague definitions of terrorism should be taken out of C -51. A lot of what police call terrorism is the activity of what he called "common criminals" or those who are trying to make a political point but don't constitute a "super criminal threat." IT World Canada (2016-10-18)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Oil cleanup criticized as storm brews**
With a storm threatening to disrupt operations, oil-spill response crews have been busy around the clock pumping fuel out of a tug that ran aground on B.C.'s central coast last week. But Kelly Russ, chair of Coastal First Nations, said the spill response was too slow when the tug Nathan E. Stewart hit a reef while pushing a massive fuel barge north of Bella Bella. The barge was empty but the tug contained more than 60,000 gallons of fuel, an unknown amount of which has spread in a huge slick throughout the region in the heart of the Great Bear Rainforest. "From a Coastal First Nations perspective, what we are seeing unfolding on the water is a crystallization of our worst fears, not only for the catastrophic event that's unfolded, but because the response, which we have been advocating for to be improved for at least a decade, is just not there," Mr. Russ said in an interview Tuesday. The Canadian Coast Guard and the industry-funded Western Canada Marine Response Corporation both reacted promptly to the accident, but the response has come under fire because the nearest oil-spill crews were based in Prince Rupert, more than 20 hours away by boat. Globe and Mail, S1

*** Hundreds attend Sydney flood meeting**
The water rose through Robin Nathanson's south end Sydney home so quickly on Thanksgiving Day that he and his girlfriend only had time to pack a few clothes and their pets into the car and flee to a relative's house. Now, just over a week later, he's finally had time to think about the big picture. While the immediate problems are trying to find a place to live and replacing 95 per cent of their possessions, he's now wondering if they'll ever be able to return to their house at the bottom of Cabot Street (…) Cape Breton Regional Municipality Mayor Cecil Clarke told the meeting that 18-20 households, including Nathanson's, have been declared unfit for occupancy as the result of a torrential rainstorm that saw some areas of the municipality hit by more than 220 millimetres of rain. Clarke told Nathanson he will meet to talk one on one with those hardest hit by the disaster but he also acknowledged that people less affected - nearly 1,000 people have now registered as flood victims through the CBRM helpline - are now beginning to get irritated. "The numbers continue to rise because people who have been able to, fortunately, take care of their own situation, they're now dealing with the 'What next?' he said. "When you have a once-in-a-200-year event, you can't help but have lessons learned. Cape Breton Post, A1/A4; Cape Breton Post; CBC News

*** App speeds up claims: Encircle was used in Fort McMurray by contractors to help see wildfire damage**
When Paul Donald left BlackBerry in 2009 he was looking for a startup opportunity, so he searched for an industry where mobile technologies had little or no uptake. He soon focused on insurance and founded Encircle, along with Ronuk Raval, and Christoph Bioccaa. Encircle built an app and platform for insurance carriers, policyholders and adjusters. It helps them quickly resolve claims using photos snapped from smartphones (…) Encircle's app was used by restoration contactors - firms hired by insurance companies to repair the properties of policyholders - after wildfires destroyed much of Fort McMurray this past summer, and heavy rains flooded thousands of basements in Windsor. Waterloo Region Record, C1

*** Kautex manager shares lessons learned from August tornado**
Kautex plant manager Steve Phillips was sitting down to dinner with his family when he got a call that a tornado had torn through his plant. Less than an hour later he was walking through a disaster area. "I'm so used to the plant being spotless," he said, describing a scene where roof debris littered the floor and

water from sprinklers and torrential rain had flooded parts of the building. "There were forklifts where they had just stopped," he added. "I've been to Pompeii, it's where time stopped and that's what it was like, walking though a place where time had just stopped (…)"After the storm an army of recovery workers descended on Kautex, which makes fuel tanks for cars, and just five days after the tornado one of the company's production lines was back in business (…) Phillip's presentation included CCTV footage from a camera that survived the storm and showed the moment a calm exterior shot was suddenly overtaken with pounding rain before a transformer exploded with a flash and swirling debris filled the frame. "You're in the eye of a tornado now," he told the group as audience members gasped. Phillips explained that safety measures such as bolting down equipment likely saved lives and passed along recovery strategies and best practices to other area companies should "worse come to worst." Windsor Star

*** Action is needed on PTSD**
An opinion piece by MP Todd Doherty states "On Oct. 4, the Standing Committee on Public Safety and National Security released a report calling on the Liberal government to introduce a plan of action for public safety officers and first responders dealing with mental health issues and post-traumatic stress disorder. According to the all-party committee study, between 10 and 35 per cent of first responders will develop PTSD at some point in their lives. These numbers are significant, and action needs to be taken immediately to help address an issue that affects Canadians from coast to coast to coast. Last January, I introduced private member's bill C-211, which seeks to establish a national, comprehensive federal framework to address the challenges of recognizing the symptoms and providing timely diagnosis and treatment of PTSD for all veterans and first responders. Since introducing Bill C-211, my office has been inundated with calls and emails from firefighters, first responders, military personnel, and corrections and police officers. These brave men and women face many dangers in their day-to-day duties, including protecting the lives and property of their fellow citizens and our nation's critical infrastructure. They are our silent sentinels. Only through bipartisan support and co-operation can we hope to achieve effective and viable strategies to ensure those in need receive direct and timely access to PTSD support. I hope that all members will join me in supporting Bill C-211 when it comes to the floor of the House of Commons." Vancouver Sun, A11

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Nil

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Quel sort attend les djihadistes canadiens qui rentreront au bercail ?**
Le Canada est-il prêt à gérer un retour massif de djihadistes sur son territoire ? Non, répondent des experts. Pourtant, une éventuelle chute de Mossoul, dernier fief du groupe armé État islamique (EI) en Irak, risque de pousser de jeunes Canadiens partis gonfler les rangs de l'EI à tenter de revenir au pays. Que faire avec eux ? « Avec ses pertes militaires quotidiennes ainsi que la perte éventuelle de la ville emblématique de Mossoul, la notoriété de Daech [acronyme arabe de l'EI] s'effrite, explique Jocelyn Bélanger, expert des questions de terrorisme et de radicalisation et professeur adjoint à l'Université de New York à Abou Dhabi. Par conséquent, nous pouvons prévoir que l'engouement pour ce groupe, qui connut son apogée en 2014, va s'estomper très fortement et que plusieurs djihadistes retourneront au bercail, ce qui veut dire, dans bien des cas, revenir en Occident. » Selon son confrère Amarnath Amarasingam, chercheur à l'Université Dalhousie d'Halifax qui étudie l'extrémisme islamiste, des Canadiens et d'autres étrangers tenteront de profiter du chaos de la bataille pour faire défection. (…) Invité à expliquer les mesures concrètes prises par le gouvernement pour se préparer au retour de djihadistes au pays, le bureau des communications du **ministère de la Sécurité publique du Canada** a fourni à La Presse une réponse générique. « Le Canada surveille avec vigilance toutes les menaces potentielles et des mesures solides sont en place pour y répondre. Les menaces potentielles font l'objet d'une surveillance constante par les organismes canadiens de renseignement, de sécurité et d'application de la loi, et le Canada dispose de mesures robustes pour les contrer. Le gouvernement du Canada reste

ferme dans son engagement à protéger la sécurité des Canadiens. Il continuera de prendre les mesures appropriées de lutte contre les menaces terroristes visant le Canada, ses citoyens et ses intérêts partout dans le monde. » Une porte-parole de la Gendarmerie royale du Canada (GRC) a pour sa part indiqué que le corps de police doit « veiller à ce que les Canadiens qui rentrent au pays après avoir participé à des activités terroristes ne mettent pas en péril la sécurité nationale du Canada, écrit Julie Gagnon. La GRC n'a pas de solution universelle à appliquer aux voyageurs de retour au pays. Chacun pose un défi multidimensionnel et chacun a ses propres motivations et intentions. » La Presse +

* **Blank passports found in theft ring bust**
A major investigation by Winnipeg police that recovered hundreds of thousands of dollars in stolen property has raised national security concerns after blank passports were among the items officers found. Tuesday, police announced Project Heavy Metal identified 20 suspects, including nine arrested in Manitoba, who are facing 140 charges related to a theft ring that operated across Western Canada. Calgary and Edmonton police, as well as the RCMP, helped with the investigation, which recovered more than $300,000 worth of goods stolen during break-ins and other thefts. Two RCMP uniforms and police equipment were recovered after a search warrant was executed at a Calgary home in September, Insp. Barry Kostchuk said. Vehicles, camper trailers, snow blowers, lawn-care equipment, new tires, tools, key-cutting machines and electronics were recovered. The most alarming items discovered may be the blank passports and birth certificates. Winnipeg police weren't ready to comment Tuesday about the blank identity documents - how many were found or if they were taken from government offices or are fakes, such as bogus Canadian passports sold online for less than $200. The theft of genuine blank Canadian passports has opened doors in the past for criminals such as human traffickers and raises concerns about dangerous people being allowed into the country. In 2002, the RCMP foiled a scheme to sell 246 stolen blank Canadian passports - but not before some of them found their way into the hands of international people-smuggling rings. An informant tipped off RCMP the black-market "books," stolen in June 2002 from the Scarborough passport office, were being sold on the streets of Toronto for $1,000 apiece. Winnipeg Free Press, 1

* **Action is needed on PTSD**
An opinion piece states, “On Oct. 4, the Standing Committee on Public Safety and National Security released a report calling on the Liberal government to introduce a plan of action for public safety officers and first responders dealing with mental health issues and post-traumatic stress disorder. According to the all-party committee study, between 10 and 35 per cent of first responders will develop PTSD at some point in their lives. These numbers are significant, and action needs to be taken immediately to help address an issue that affects Canadians from coast to coast to coast. Last January, I introduced private member's bill C-211, which seeks to establish a national, comprehensive federal framework to address the challenges of recognizing the symptoms and providing timely diagnosis and treatment of PTSD for all veterans and first responders. Since introducing Bill C-211, my office has been inundated with calls and emails from firefighters, first responders, military personnel, and corrections and police officers. These brave men and women face many dangers in their day-to-day duties, including protecting the lives and property of their fellow citizens and our nation's critical infrastructure. They are our silent sentinels. Only through bipartisan support and co-operation can we hope to achieve effective and viable strategies to ensure those in need receive direct and timely access to PTSD support. I hope that all members will join me in supporting Bill C-211 when it comes to the floor of the House of Commons.” Vancouver Sun, A11

* **Why are three of the world’s richest countries doing so little to stop corruption?**
An opinion piece states, “One of the best-known data points in the anti-corruption field is the estimate from Global Financial Integrity that US$ 1.1 trillion in proceeds of corruption, crime and tax evasion are taken from developing countries every year and invested in Western banks, real estate, and luxury goods. The volume of illicit financial flows is higher than the total value of development aid and foreign direct investment into poor countries combined. The revenues lost by poor countries through tax dodging alone are estimated at US$ 160 billion every year, money which could be used to build thousands of schools and hospitals. (…) Following a Supreme Court decision in 2015, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its regulations were found to breach attorney-client privilege insofar as record-keeping, client identification and verification, and compliance inspection by Canada’s Financial Intelligence Unit (FINTRAC) were concerned. The Government had previously withdrawn the

reporting requirement for the law profession following injunctions by law societies." Transparency International

*** Après un an**
Un éditorial note, "Il y a un an aujourd'hui, le ton changeait à Ottawa. La victoire des libéraux de Justin Trudeau levait une chape de plomb virtuelle sur le gouvernement fédéral. D'un gouvernement conservateur où toute initiative était mesurée à l'aune de la menace que cela représentait pour la sécurité nationale, l'économie canadienne ou l'emploi, les électeurs embrassaient tout d'un coup une vision d'un pays mû plutôt par l'espoir et l'optimisme. Mais c'est plus difficile à dire qu'à faire et 12 mois plus tard, les Canadiens attendent encore des résultats dans bien des domaines. Les premières semaines ont été prometteuses. Sous un radieux ciel d'automne, des centaines de Canadiens sont allés à Rideau Hall pour voir une nouvelle génération de politiciens franchir les portes du pouvoir. Quelques mots sont devenus emblématiques des premiers pas de cette administration : «Sunny Ways» («Voies ensoleillées»), évoquant Wilfrid Laurier, puis «Parce que nous sommes en 2015», pour justifier la parité homme-femme de son cabinet. Il fallait rapidement se mettre à l'ouvrage sur les sujets les plus urgents. Le monde entier s'interrogeait sur ce qu'il fallait faire pour résoudre un tant soit peu la crise des migrants syriens. Radicalement différente des conservateurs qui craignaient une intrusion terroriste, la position libérale s'articulait vers l'ouverture à 25000 réfugiés. Ce fut un succès et on aura déjà oublié le fait que le gouvernement aura mis deux mois de plus que prévu pour tous les accueillir. L'autre urgence, c'était l'imminence du sommet de Paris sur les changements climatiques. Aussitôt, M. Trudeau et sa ministre de l'Environnement, Catherine McKenna, ont signifié au monde que «le Canada était de retour». Cela s'est enchaîné récemment avec une politique contraignante pour forcer les provinces vers une tarification des émissions de CO2 - ce qui ne passera pas comme lettre à la poste en Saskatchewan et en Alberta. Au même moment, le fédéral a approuvé le plan d'un nouveau gazoduc vers le Pacifique : monnaie d'échange pour un accord national? » Le Droit, 14

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Aspirant Hells Angel et employé du Port de Montréal
Un motard en voie de devenir membre en règle des Hells Angels est au nombre des 800 débardeurs du Port de Montréal, a appris La Presse. Roger Bishop fils, 46 ans, est sorti de l'anonymat la semaine dernière lorsqu'il a échangé quelques mots avec un journaliste venu couvrir une perquisition policière dans un centre de conditionnement physique du chemin de Chambly, à Longueuil. Selon nos informations, Bishop est actuellement « prospect », l'ultime étape durant laquelle un motard doit faire ses preuves durant au moins un an avant de devenir membre du club. Il pourrait devenir membre de la section South des Hells Angels dans quelques mois. Le port de Montréal est, depuis des décennies, considéré par la police comme une importante porte d'entrée de la drogue dans la métropole. En 2011, un rapport de l'Agence des services frontaliers du Canada que La Presse avait obtenu affirmait que le port de Montréal demeurait un haut lieu du crime organisé au pays. « Plusieurs groupes du crime organisé opèrent dans la région du port de Montréal. Des employés sont reliés à divers groupes du crime organisé, y compris des groupes italiens, les Hells Angels et le gang de l'Ouest. Ces groupes continueront de faciliter le passage de la contrebande », écrivaient les auteurs du rapport. La Presse+, 7

*** Markham, Ont., man back home after U.S. no-fly list left him stranded in Amsterdam**
The Markham, Ont., man stranded in Amsterdam after he says he learned he was on the U.S. no-fly list has returned home to Canadian soil. Nanak Partap Singh had been travelling back to Toronto from Delhi when he made a connecting stop in the Netherlands on Oct. 12. There, he had been unable to print off his boarding pass and was told to check in at a counter where he learned that he was unable to fly because his name had been flagged by the United States, Singh said last week. It's unclear exactly when the Markham man returned home, but his wife sent CBC News an email Tuesday night to confirm her husband was back in Toronto. CBC News

*** Engineer on coast guard ship charged with smuggling child porn**
A Canadian Coast Guard employee was arraigned in Dartmouth provincial court Tuesday on charges of bringing child pornography into the country. Julien Pierre Marceau, 55, of Fredericton works as first

engineer on the CCGS Hudson. Judge Dan MacRury scheduled the case to return to court in late November. According to a search warrant, the Canada Border Services Agency opened an investigation in early August based on information it received from the Halifax Regional Police-RCMP Internet child exploitation unit. Border agents examined the vessel after it docked at the Bedford Institute of Oceanography in Dartmouth. A thumb drive found in Marceau's personal effects allegedly contained images of children "engaged in explicit sexual activity," the warrant says. An investigator with the border agency obtained a search warrant last month to seize three hard drives and another USB device that had been locked in a safe by a DFO security officer. Local Xpress

*** Man arrested in unprovoked 2014 Seattle slaying**

Seattle police arrested a 22-year-old man earlier this month in connection with a 2014 Seattle shooting that left one man dead and another injured. Meanwhile, the suspect's co-defendant remains at large. Officers arrested Jesus Chavez-Carrillo on Oct. 9. He and Jose Ortega-De La Mora, formerly of Auburn, left the area shortly after 26-year-old Mykola Shevchuk was killed in a drive-by shooting in Seattle's Sodo neighborhood. Both men were charged in August 2014 with second-degree murder and two counts of first-degree assault. The Seattle Police Department declined to discuss the case or how they found Chavez. De La Mora still has a bench warrant for his arrest. The incident occurred the night of June 22, 2014. Weeks later, on July 6, a Canada Border Services Agency officer stopped Ortega and his girlfriend at the border and turned him over to United States authorities after finding text messages on his phone that appeared to implicate him in a shooting. Seattle PI

Hunt for origin of unknown chemicals sent to drug producer led police to Portugal

In the search of Richard Valiquette's north end apartment following the discovery of Gavin Adams's body on Dec. 17, 2013, members of the Saint John Police Force found several invoice sheets from the business Avanztec. According to the officers executing the search, it was believed the invoices may have had something to do with drug production. As Valiquette stands trial for criminal negligence causing Gavin's death, mystery still surrounds those documents. Avanztec supplies chemical products. Const. Sean Rocca, the lead investigator looking into Gavin's death, said the invoices were linked to an address in Kanata, Ont. That address was for a postal box, said Rocca, which was connected to a man he later found living in Portugal. Rocca said he had the man flagged with Canadian Border Services. Telegraph-Journal, B3

Ottawa moves up review of drywall duties after complaints of high prices

The federal government has asked for an accelerated review of anti-dumping duties on drywall imports, but the new schedule isn't expected to immediately rollback duties blamed for higher prices for consumers. The Finance Department says it wants to help middle-class families in Western Canada, especially those involved in the reconstruction of Fort McMurray, Alta., following last spring's devastating wildfires. "With this action, we are putting in place an expedited process to look into the unintended impacts that these duties may be having," Finance Minister Bill Morneau said in a statement. The Fort McMurray fire destroyed about 1,800 houses as well as buildings containing 600 multifamily housing units, plus two hotels and a 665-room work camp. The federal move was welcomed by Alberta MLA Brian Jean, whose house was one of those destroyed in the wildfire. "I am grateful to hear the federal government is responding to our concerns and the concerns of people across Fort McMurray with the recent ruling by Canada Border Services Agency that effectively closed Western Canada from imported drywall," said the leader of the Opposition Wildrose Party in a statement. "We will continue to ask the federal government to suspend the tariff during its review or at the very least use its authority to exempt drywall coming into Fort McMurray from this new tariff." In September, the CBSA imposed preliminary tariffs of up to 276 per cent on U.S. gypsum board or drywall imported into Canada for use in British Columbia, Alberta, Saskatchewan, Manitoba and the Yukon and Northwest Territories. The agency said it was reacting to a complaint filed in April by CertainTeed Gypsum Canada Inc. of Mississauga, which resulted in a preliminary determination of dumping - meaning the products are being sold in Canada at less than normal prices. Canadian Press (Globe and Mail, Telegraph-Journal, Times & Transcript)

Air authority renews security contracts

The federal agency in charge of security at Canada's airports has renewed screening contracts with three private-sector firms, Garda World Security Corp., Securitas Transport Aviation Security Ltd. and G4S

PLC. The Canadian Air Transport Security Authority (CATSA) says the total value of the contract extensions is about $2.6-billion. They'll run from April, 2017, through March, 2022. Canadian Press (Globe and Mail, Times Colonist)

Screening at Canadian airports should be faster, smarter, safer
An editorial states, "If you've flown anywhere in Canada recently, you will have noticed that wait times are getting worse. Since 2013, the length of screening times has deteriorated so badly that the Canadian Airport Council referred to security screening services as a being in a state of crisis. Not only are we waiting more, we are paying more. And getting less service. According to the World Economic Forum, Canadians pay some of the highest air travel prices in the world. One part is a fee for the so-called Air Traveller's Security Charge (ATSC). The Air Traveller's Security Charge was introduced after 9/11 by the Chrétien government to fund air transport security and the newly minted Canadian Air Transport Security Authority. Instead of improving security, it has turned into a major cash grab by the Finance Department. Since 2011, the budget of CATSA has declined even though ATSC revenue has steadily increased. From 2010 to 2013, $260 million was siphoned away from airport screening into the Consolidated Revenue Fund... Another problem with airport security highlighted in David Emerson's 2015 Review of the Transportation Act, is the strange restrictions faced by CATSA. Essentially, CATSA has no control over security screening policy. This has led directly to poor service and long wait times. Emerson recommends adopting the U.S. model wherein a single "agency has responsibility for both regulatory oversight and operations." ... But perhaps the greatest failing of the Canadian model is with our trusted traveller program: NEXUS. That's the background check where travellers volunteer their information to border officials to become pre-screened. They are then deemed "trusted travellers" and expedited through customs. NEXUS cardholders are also offered a special line at security screening. The problem is, it's not that special. NEXUS users are still forced to submit to the same cumbersome screening procedures as other passengers. The question is: If our border officials allow these prescreened travellers to enter the country quickly and safely, why doesn't the same practice apply at airport security?" Montreal Gazette, A11

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Businesses must buck surveillance**
Resisting government mass surveillance isn't just the right thing to do - it's good for business, whistleblower Edward Snowden told a Toronto cybersecurity conference Tuesday. Speaking via video link to the annual Canadian industry event SecTor, Snowden brought up the recent revelation that Yahoo Inc. had agreed to scan customers' emails for U.S. intelligence. Shortly after, Verizon Communications Inc. asked for a US$1 billion discount on its US$4.8 billion agreement to buy the company, according to a report in the New York Post. "If you collaborate with the government in this regard, far beyond what the law requires, it can actually have a significant, substantial consequence for your valuation," Snowden said. "Yahoo, which is a very powerful, very rich organization, cooperated beyond what was legally required. And it damaged its brand (...)"Snowden cited Open Whisper Systems, which makes the encrypted messaging app Signal, as an example of an organization that benefited from pushing back against a government request for cooperation in a surveillance program. With the help of the American Civil Liberties Union, Open Whisper Systems fought a gag order on a subpoena for information associated with two phone numbers. Ultimately, Open Whisper Systems had to comply with the subpoena, but the damage was mitigated because of another Snowden-approved policy: Only retaining as much personal data as absolutely necessary. The subpoena asked for browsing history and tracking data stored in web browsers, but Signal doesn't collect that information. "Companies work for their customers first. This means they should only hold the data that's absolutely necessary for the operation of their businesses," Snowden said. "When this story broke about Open Whisper Systems abiding by this principle, the fact they were being compelled through the state's monopoly on use of law actually benefited their brand." Postmedia (Financial Post, FP3; National Post)

*** Over 100 groups cashing in on ransomware, Canadian infosec pros told**
Ransomware is such big business that security vendor F-secure is tracking 110 gangs making money from the malware, the company's chief research officer has told annual SecTor cyber security conference.

It's the biggest single problem infosec teams face today, Mikko Hypponen told the Toronto conference on Tuesday, because once a machine is infected "it will stop you dead in your tracks." Things are so bad that a number of organizations are buying digital wallets with Bitcoin as protection for the day they are infected – and their willingness to pay ransoms only makes things worse, Hypponen added, because the more victims that pay the more attackers are encouraged. IT World Canada (2016-10-18)

*** Only do penetration tests if your security program is up to it, say experts**
Penetration testing is an exam that cyber security experts tout for finding out the true strengths and weaknesses of an organization's personal and technology defences. However, if your organization doesn't have a mature security program pen testing is a waste of time and money, two veterans warned infosec pros Tuesday at the annual SecTor cyber security conference in Toronto (…) In an interview later West and Baseggio expanded on this and other points. "If you have a very immature security program and you know it – which most clients do – then that's a very clear indication you should probably put your money into the building blocks that make you secure rather than a shot in the dark," said Baseggio. "You already know your network is insecure because you haven't put any effort into it." IT World Canada (2016-10-18)

*** Province's cellphone security sub-par, but getting better**
The B.C. government's lax rules on taxpayer-paid iPhones and tablets has left it blind to the security risks of viruses, hackers and unauthorized applications used by public officials - some of whom wait months to report lost devices, according to two new investigations. Auditor General Carol Bellringer and acting Information and Privacy Commissioner Drew McArthur issued joint reports Tuesday that raise red flags about government security for thousands of smartphones and tablets. But they also admitted the province has plugged the most serious security holes since their audits concluded in November 2015, and they didn't investigate whether there were any cases in which data was inappropriately accessed. "While I'm encouraged, there's also some work to be done," McArthur said. "The highest of the risks have been addressed, or we would not have released the report publicly," Bellringer added. Postmedia (Vancouver Sun, A6)

*** Politics this morning: EU-Canada Arctic Conference takes place in Ottawa**
(…) There will be a panel discussion on cyber security in Canada, and how the country can increase the protection of important data. The event will take place from 9:15-11:15 in Room 160S, Centre Block, Parliament Hill in Ottawa. The speakers include: David Murakami Wood, Canadian research chair for the Surveillance Studies Centre at Queens University; Claude A. Sarrazin, president of SIRCO; Bonnie Butlin, national coordinator and chair of the National Council of the Canadian Cybersecurity Alliance; and Peter Sloly, executive director, risk advisory/cyber, national lead for security & justice sector, at Deloitte Canada. Hill Times

LAW ENFORCEMENT / APPLICATION DE LA LOI

856 Gang member charged with Hells Angel's murder
The man accused of killing Hells Angel Bob Green was out on bail at the time of the shooting. Jason Francis Wallace, 27, was charged Tuesday with second-degree murder for slaying Green on a rural Langley property Sunday morning. Wallace was on $1,000 bail on drug-trafficking charges he faces with Green's cousin. Cpl. Meghan Foster of the Integrated Homicide Investigation Team would not disclose Wallace's gang links. (…) Postmedia News has learned Wallace himself called police to say he was a suspect in the fatal shooting Sunday. That led to his dramatic arrest by Surrey RCMP on 152nd Street about 10 a.m. Monday. Foster said she couldn't comment on whether Wallace had turned himself in. "I can't speak to the details of what led up to Mr. Wallace's arrest," she said. "While police are learning some specifics of what took place preceding the homicide, the motive remains unclear." (…) Wallace has a long and violent history in B.C. He pleaded guilty eight years ago to aggravated assault for stabbing a student after a high school graduation party in Langley. He received a 21-month conditional sentence. "The attack was completely unprovoked and the victim did not know his assailant," RCMP Cpl. Diane Blaine said at the time. Wallace had been charged with attempted murder for the stabbing. Postmedia

Network (Province, A4, Vancouver Sun, Calgary Sun, Edmonton Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun)

*** Five arrested after week-long human trafficking investigation**
Winnipeg police arrested five people as the result of a week-long human trafficking investigation in a phase of the Operation Northern Spotlight that has been sweeping across North America for five years. The five in Manitoba were among 32 people facing a total of 78 offences. All five were charged with obtaining sexual services for consideration. The Counter Exploitation Unit (CEU) interviewed a total of 22 women aged between 19 and 44 in areas known to be frequented by sex trade workers, such as hotels and massage parlours, in the city during the investigation. Police did not identify those who were arrested. "The five arrested here were exploiters more involved in street prostitution, but not the typical human traffickers," Sgt. Darryl Ramkissoon said Tuesday. "But the media attention this has garnered has sent a message to exploiters." A total of 54 police services in Canada, the RCMP and the FBI in the United States participated in the most recent phase of the operation. It is an ongoing investigation into human trafficking involving mainly young women who are participating in the sex trade against their will. "We've definitely connected them with the resources to either stay safe or exit the trade," Ramkissoon said. "We have helped some of them exit the trade in the past." Winnipeg Sun, A6; Winnipeg Free Press; Hamilton Spectator; Canadian Press (Toronto Star); Globe and Mail

*** Acts of bravery, courage honoured at RCMP awards in Calgary**
When Matthew Doane arrived at a bridge about 50 feet (15 metres) above the North Saskatchewan River after calls of a suicidal youth, he knew he had to act quickly. Several people had tried desperately to get a hold of the 12-year-old girl through the guardrails, but without success. The Rocky Mountain House RCMP constable crawled to the unsecured side of the bridge and used his body to protect the girl, preventing her from falling or jumping, possibly, to her death. Along with civilians and the local fire department, they potentially saved the girl's young life. That was back in March of 2014. Const. Doane's actions, along with other officers, were honoured at the RCMP Commendation Awards at a private ceremony in Calgary on Tuesday. "I am so honoured to be here today to recognize the inspirational efforts our employees have made," Deputy Commissioner Marianne Ryan said. Doane is now posted at the Didsbury RCMP detachment. In early June 2010, an armed man showed up at the Alberta Serious Incident Response Team (ASIRT) office in Calgary looking to speak with Andrew Johnson, an RCMP sergeant at the time. CBC News (2016-10-18)

Over 'n' out
Back to square one. In a tech-driven world where even the latest, greatest smartphone can simply burst into flames, square one is where the Calgary Police Service finds itself, three years after bodyworn cameras were officially touted as the tool of the near future for city cops. Well, that future just got pushed back over the distant horizon, and now it's back to the starting line. "Unfortunately, that's the case. It's a huge disappointment," said Deputy Chief James Hardy. The eagerly anticipated body-worn cameras ordered by Calgary cops under a $1.3 million, three-year contract have proven unreliable in the field after the initial units, worth about $800 each retail, were issued to officers for real-world testing. With CPS preparing for a possible legal fight in recovering that money from the camera supplier, Safety Innovations, exactly what went wrong is being kept vague - but last February, Postmedia reported glitches in the microphone buttons causing interference over the entire network. In any case, the combination camera/microphones, which were expected to be fully in use by early 2017 - making Calgary the first major police organization in Canada to implement body-worn cameras service-wide - are now considered ill-suited for police work and cannot be used. Calgary Herald, A7

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Le nouveau poste de police d'Edmundston coûte encore cher aux contribuables
Cinq ans après la construction de l'édifice qui abrite le poste de police d'Edmundston, 15 % des locaux sont encore vides. Les contribuables doivent donc continuer de payer pour le bâtiment. Cet édifice ultra-moderne a pignon sur rue à Edmundston depuis 2011. Il s'agit d'un bâtiment vert, ultramoderne et plus sécuritaire que le précédent. La moitié du bâtiment est occupé par les locaux du poste de police

municipale. L'autre moitié du bâtiment est occupé par les bureaux administratifs de la bibliothèque du haut Saint-Jean, Facilicorp et Service correctionnel du Canada. Le projet a coûté un total de 11 millions de dollars. Radio-Canada (2016-10-18)

Rafferty appeal irks Tori kin
For the family of Victoria (Tori) Stafford, the hearing is stalling time and the healing that goes with it. For Michael Rafferty, it a small hope for a different future. For Ontario legal community, it an essential lookback at a critical decision. The Ontario Court of Appeal will hear Rafferty arguments Monday for a new trial in the first-degree murder of Tori Stafford April 8, 2009. " It just a waste of everybody time ," one of Tori grandmothers, Doreen Graichen, said. "We talk about it and we try not to dwell on it. It upsetting, but there nothing we can do. I hope they stop wasting taxpayers ' money. The man is guilty without a doubt." Guilty or not, sending a person to prison for life is a crucial decision that often demands a second look, said Frank Addario, a former president of Canada Criminal Lawyers ' Association and winner this year of its lifetime achievement award in criminal law. London Free Press, A1 (Ottawa Sun, Toronto Sun)

L'ex-juge Jacques Delisle veut retrouver sa liberté
L'ex-juge Jacques Delisle, reconnu coupable du meurtre prémédité de son épouse Nicole Rainville, était de retour au palais de justice de Québec, mardi, pour la première fois depuis le verdict de juin 2012. L'ancien magistrat âgé de 81 ans purge une peine de prison à perpétuité pour le meurtre prémédité de sa femme trouvée morte en novembre 2009. Jacques Delisle espère pouvoir quitter le pénitencier de La Macaza en attendant la conclusion de la révision judiciaire de son dossier par le ministère fédéral de la Justice. L'octogénaire s'est présenté mardi au palais de justice de Québec visiblement amaigri. Il est entré dans le box des accusés vêtu d'un t-shirt blanc et d'un veston noir trop grand. La Tribune, 15 (Le Droit); * Canadian Press (Montreal Gazette, Squamish Chief); * Journal de Québec; * Le Soleil (2016-10-19); * Radio-Canada; * CBC News (2016-10-18)

* **«Mom» Boucher subira son enquête à Gouin**
L'ex-motard Maurice Boucher devra subir son enquête préliminaire pour tentative de meurtre sur un codétenu au Centre judiciaire de Gouin plutôt qu'au palais de justice de Saint-Jérome, afin de limiter les risques, a tranché la cour hier. Le centre de Gouin est effectivement directement relié à la prison de Bordeaux par un tunnel souterrain. Pendant l'enquête préliminaire, prévue en 2017, Maurice «Mom» et son coaccusé René Girard seront donc incarcérés au centre de détention de Montréal. Les deux hommes sont actuellement emprisonnés à la prison de Sainte-Annedes- Plaines. Ils sont accusés de tentative de meurtre et de voies de fait à l'endroit de Ghislain-André Gaudet. Journal de Québec, 28 (Journal de Montréal)

* **Top judge rejects Dennis Oland's relationship with father as 'fine'**
New Brunswick's top judge rejects the notion that Dennis Oland had a normal relationship with his murdered father, multimillionaire businessman Richard Oland. Chief Justice Ernest Drapeau of the Court of Appeal of New Brunswick made the comment on Tuesday during Dennis Oland's appeal hearing, which resumes Wednesday at 10 a.m. AT in Fredericton. Oland's defence team is seeking to have his second-degree murder conviction in the 2011 death of his father overturned and either an acquittal entered or a new trial ordered. CBC News; Telegraph-Journal, A1 (Times & Transcript, Daily Gleaner)

High ratio of isolated inmates have mental-health issues
Ontario's solitary-confinement cells hold a high proportion of inmates who have mentalhealth issues and other medical challenges, including one prisoner who has spent more than four years in isolation, according to figures released by the Ontario Human Rights Commission. The commission made the numbers public on Tuesday, at a briefing where Chief Commissioner Renu Mandhane relayed the case of one aboriginal inmate she'd met who has languished in segregation so long - more than 1,500 days - that his capacities for speech and memory have deteriorated. "It was really disturbing for me personally," Ms. Mandhane said of the encounter at Thunder Bay Jail. "I've been in a lot of prisons and spoken to a lot of prisoners. (...)The restarting of segregation clocks was found to be a factor in the cases of Ashley Smith and Eddie Snowshoe, two federal inmates whose deaths in solitary confinement cells three years apart galvanized public support for segregation reform across the country. The federal correctional service has

since phased out the practice. Globe and Mail, A1; Postmedia Network (Ottawa Citizen, Ottawa Sun); * Toronto Star; * London Free Press

*** When in politics, do another review**
An editorial states, "Ontario Corrections Minister David Orazietti actually said this on Monday, about his government's overuse of solitary confinement in provincial prisons: "After a thorough internal review and extensive consultations with a broad range of experts, it is becoming apparent to me ... that a more thorough and comprehensive review into the complex nature of the corrections system in Ontario needs to be conducted." (...)The United Nations, for instance, says putting a healthy, adult prisoner in solitary for more than 15 days in a row is a form of torture, and that it should never be used on youths and mentally ill inmates. Howard Sapers, the federal prisons ombudsman, says the maximum time in solitary should be 15 days. The Ontario Human Rights Commission has called for a complete ban on solitary in Ontario prisons. The union representing Ontario corrections workers says segregation is no place for inmates with mental illness, and that the province should build separate facilities for them. (...)There is no question that corrections systems are complex. But the issue of solitary confinement is not. It is abusive, and it harms inmates suffering from mental illness, making it harder for them to rejoin society when their sentences are complete." Globe and Mail, A12

Solitary changes a good first step
An editorial states, "Prisoners in Ontario's jails will no longer be dumped in solitary confinement as punishment for 30 days straight. New rules announced Monday will cut the maximum time for solitary to 15 days. That may sound reasonable to some, but the province needs to do better. We understand that many are worried about this change. Safety is important, and sometimes tossing rowdy prisoners into solitary is the only way to keep guards and other inmates safe. Sometimes it's the only way to keep the prisoner in question safe. We've long said safety should be the government's priority, not pandering to those who believe time in jail should be a comfortable experience. But a United Nations expert on torture says solitary confinement should end. The Ontario ombudsman has called for it to end. Instead, one-fifth of Ontario inmates spent time in solitary in the last three months of 2015. And 40 per cent of them had mental health issues." Ottawa Sun, A12

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Cyberintimidation
Le site Internet Ado-Parlons santé (www.adosante.org) contient un module sur la cyberintimidation. Tu y trouveras de l'information pertinente sur les formes de cyberintimidation et sur les conséquences pour le cyberintimidateur et pour la victime, ainsi que des conseils pour les victimes de cyberintimidation. Tu es invité à consulter ce module du site Ado-Parlons santé qui a été conçu pour répondre aux questions des jeunes âgés de 13 à 25 ans concernant leur santé mentale et physique. Acadie Nouvelle, 21

*** City crime rate and severity increase**
St. Albert saw more crime, and crime of a more severe nature, in 2015 compared to previous years – but crime rates here are still the lowest in the province for a city this size. Policing services manager Aaron Giesbrecht presented the 2015 annual policing report to council at the Oct. 17 meeting, explaining the crime severity in St. Albert is below the provincial and national averages, and the increase is likewise comparable to provincial and national rates. He explained one incident in particular had a major influence on the increase in crime severity at the local level. In January, Const. David Wynn was killed and auxiliary officer Derek Bond was seriously injured in a shooting at the Apex Casino. Serious crimes have a major influence on crime severity in the city. "Despite that, St. Albert still has the lowest crime severity amongst Alberta municipalities," Giesbrecht said. St. Albert Gazette

*** Don Atchison endorses street checks as part of Saskatoon crime prevention**
Mayoral candidate Don Atchison is making his stance on street checks very clear: he supports them. "Street checks and carding I think are two different scenarios," said Atchison during a Tuesday afternoon press conference. "Carding is racial profiling. I don't believe that's where our police service is

going by any stretch of the imagination." In a release, Atchison also pointed to repairing relations between police and First Nations people in Saskatoon. He said that when he first became mayor in 2003 there was a dangerous divide between police and First Nations people. "Members were demoralized and embarrassed to say they were officers," said Atchison. "Today morale on the service is extremely high." The issue of street checks and carding was raised at a sold-out mayoral debate held at the Broadway Theatre in Saskatoon last week. During that debate, Atchison spoke strongly in favour of street checks, saying it was an integral part of policing. He argued it could also help improve safety for young people on the street by helping them find a safe place to sleep. CBC News (2016-10-18)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Tanya Tagaq's overdue call for retribution**

In a year that's presented us with the disheartening acquittal of Jian Ghomeshi, a paltry three months of imprisonment for convicted Stanford rapist Brock Turner, an American presidential campaign buoyed by racism, xenophobia and accusations of sexual assault, a class-action sexual-harassment lawsuit against the RCMP - 500 accusers strong - and little follow-through on Prime Minister Justin Trudeau's promise to repair relations with indigenous peoples, the hunger for amends is ubiquitous. Tanya Tagaq's Retribution, the follow-up to her 2014 Polaris Music Prize-winning Animism, is an embodiment of this. ("The retribution will be swift," go the lyrics to the title track.) (...)Retribution features a striking cover of the Nirvana song Rape Me, which Tagaq recorded with the thought of Canada's missing and murdered Indigenous women in mind. "I didn't know what it was going to be like," Tagaq says. "I thought I was going to be more aggressive with it. But when I recorded the cover, I was just so sad. I'm devastated that this is how we live. It came out very soft. I am in mourning of all the women who have been taken." (...)Behind her, the names of 1,200 missing and murdered indigenous women were projected onto a screen, which prompted the term "missing and murdered indigenous women" to appear in subsequent international media coverage of the event. Now that she's become a recognizable figure, she consistently uses her platform for protest. "I've been labelled an activist, but I'm just trying to survive and make sure that the people I love and care about are okay. I wouldn't be a responsible human being if I didn't point these things out," Tagaq says. Globe and Mail, L1

*** Stop selling 'racist garbage,' shop selling Indigenous Halloween costumes told**

A company with locations across Canada is coming under fire in Edmonton for selling Indigenous-themed Halloween costumes described as "racist garbage" and "keep us stuck in the past." Last Thursday, Zoe Glassman was surprised to come upon an entire section at Party City displaying items such as fringed dresses and headdresses with the package showing white models donning dark wigs, braids and face paint. "We're still trying to find truth and reconciliation," said Glassman, who was shopping at South Edmonton Common, one of four Party City locations in the city. (...) Indigenous artist and activist Todd Houseman said in the context of missing and murdered indigenous women, the sexualized costumes promote harmful attitudes such as: "I can now treat them like that," which, he says, "can lead to a lot of horrific things across the board." He said the costumes reinforce stereotypes of Indigenous people, undermining efforts to reclaim power and leadership. CBC News (2016-10-18)

*** Parties respond to questions from CYFN**

The Council of Yukon First Nations (CYFN) asked each political party to respond to five questions about how it would, if elected, work with First Nations governments. "Our relationship with the territorial government spans many generations and has weathered many difficult moments," reads the introduction to the questionnaire. "Our relationship is now one of equals since we are governments." (...) Liberals: The Liberals say the Yukon government must create culturally sensitive programs and services in the spirit of the TRC's recommendations. The TRC report lays out myriad ways governments, and people, can improve social, health, economic and education outcomes for indigenous peoples and therefore all Canadians. The party says it would support the the national inquiry into missing and murdered indigenous women and girls, but that First Nations should take the lead. It would also revise the

Prevention of Violence Against Aboriginal Women Fund to open up access to funds in the communities. Whitehorse Daily Star, 4

*** Youth, First Nations need more from next budget**
The House Finance Committee is once again in the middle of its pre-budget consultation process, marked, as in previous years, by crowded panels of diverse witnesses. With more than 120 witnesses and over 400 briefs received, it would be easy for an op-ed on the process to take the form of a laundry list. Instead, let's focus on just a few of the key electoral commitments that witnesses warned have fallen by the wayside since the Liberals formed government. Finally, on the social front, promises made to First Nations by the Liberals during the 2015 elections have to be kept. Unfortunately, one year into this government's mandate, while some progress has been made, it falls far short of the expectations that had been created. The Liberal government did launch an inquiry into Missing and Murdered Indigenous Women, but is falling short in key areas like police practices and child welfare. Hill Times

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Cannabis 101**
Call it a crash course in cannabis. Alberta's Justice Minister and Solicitor General is Coloradobound to see how the state has handled legal weed. Kathleen Ganley said with marijuana's legalization in Canada imminent, it's prudent to look at best practices and lessons learned from a place that's pioneered the way. "The federal government will set the tone, if you will, or set the broad strokes for how restrictive the model is going to be and a whole number of other things, but then provinces will have to step in because some of it will be in provincial jurisdiction ... and of course our policing partners, as well, will have a large role to play, and municipalities probably as well," Ganley said. "We're looking to all move together. "It's important that the province be prepared to ensure that we are doing our part to keep Albertans safe. Postmedia Network (Edmonton Sun, A22, Calgary Sun)

*** Ganley off to Colorado to probe policies on pot**
With legalization imminent in Canada, Alberta's Justice Minister and Solicitor General is headed to Colorado to see how the U.S. state has handled policies and procedures around pot, which has been legal there since January 2014. Kathleen Ganley flies out Thursday to Denver, where she's slated to meet with the attorney general, police and fire services and a host of municipal and state officials. "The federal government will set the tone, if you will, or set the broad strokes for how restrictive the model is going to be and a whole number of other things," Ganley said, "but then provinces will have to step in because some of it will be in provincial jurisdiction. "And, of course, our policing partners will have a large role to play, and municipalities ... We're looking to all move together. Calgary Herald, A5

PUBLIC SERVICE / FONCTION PUBLIQUE

Phoenix payroll update today as government deadline looms
Senior federal officials are expected to give an update on the Phoenix payroll mess Wednesday afternoon as the government's self-imposed Oct. 31 deadline to deal with the backlog of cases looms. CBC News will carry the briefing live online, beginning at 1:15 ET. The government's deadline is for the backlog of more than 80,000 cases filed by federal workers before June — not new cases filed later. But the government also committed to dealing with new high priority cases within two weeks of the claim. CBC News

OTHER / AUTRE

We grade the grits
An editorial states, "Is it fair to judge a government only a year after an election? If the government in question made 325 promises during the campaign, as the Liberals did, then yes. Given our four-year election cycle, they had better be one-quarter of the way through checking off their pledges. Of course,

only a deliverology guru could calculate this for sure. So let's just do a quick flyby: (…) INDIGENOUS AFFAIRS: A "renewed nation-to-nation relationship" was among the government's most significant promises to indigenous Canadians. Some things did happen: budget funding of $8.4 billion over five years is coming, and an inquiry is underway into missing and murdered indigenous women. Not accomplished: equal funding for First Nations children. SECURITY: Canadians still haven't seen the changes coming to the "problematic" anti-terrorism act, Bill C-51. But there will be an all-party national security oversight committee and there are broader security consultations. (…) PUBLIC SERVICE: Unions complain the Liberals aren't bargaining fairly, naturally. But any government has to negotiate hard on behalf of taxpayers. We don't think that's the problem. The problem is the poor rollout of the Phoenix pay system. No private enterprise would survive this kind of fiasco for long. It wasn't in your election agenda, Grits, but you own it and you have to fix it. Welcome to Year Two." Ottawa Citizen, A8; * Times Colonist

*** The canadian on death row**

An opinion piece states, "On Sunday, The Canadian Press presented a new interview with Ronald Allen Smith, the Albertan who is on death row in Montana for randomly murdering two young men in 1982 while hitchhiking on LSD (as one does). Smith, who had originally passed up a plea deal and asked for the death penalty, seems to grow more attached to life every time someone chats with him. Now 59, he says cheerfully that the election of a Liberal government in Ottawa "bodes well for (him)" and that he is "ready to come home ... if you're willing to take me back." With a carelessness that has practically become a tradition in Smith's case, the CP writes that a court "forced the (former Conservative) government to abandon the policy" of refusing to extend assistance to Canadians convicted of murder in democratic countries. Canadian courts, happily, do not have the power to revise foreign policy. The issue that came before the Federal Court was that there was no actual policy at all, and that various federal ministers seemed to be setting the conditions for consular assistance on the fly, in press releases and interviews. The new Liberal government is free, in principle, to create a policy that would leave Smith to face his fate in Montana State Prison. It would be a matter mostly of writing the policy down, which the Conservatives never bothered to do." National Post, A9

*** Markham, Ont., man back home after U.S. no-fly list left him stranded in Amsterdam**

The Markham, Ont., man stranded in Amsterdam after he says he learned he was on the U.S. no-fly list has returned home to Canadian soil. Nanak Partap Singh had been travelling back to Toronto from Delhi when he made a connecting stop in the Netherlands on Oct. 12. There, he had been unable to print off his boarding pass and was told to check in at a counter where he learned that he was unable to fly because his name had been flagged by the United States, Singh said last week. It's unclear exactly when the Markham man returned home, but his wife sent CBC News an email Tuesday night to confirm her husband was back in Toronto. CBC News

INTERNATIONAL

*** Suspected ISIS bomber killed in raid in Turkey: official**

Turkish police on Wednesday fatally shot a suspected Islamic State group militant who was believed to be planning a suicide bomb attack in the capital. The man was killed in a raid on a ninth-floor apartment on the outskirts of Ankara after he ignored warnings to surrender and opened fire on police, Ankara Gov. Ercan Topaca said. The state-run Anadolu Agency quoted Topaca as saying the man was believed to be planning a suicide attack in the city -- either targeting large gatherings or to coincide with two national ceremonies in the coming weeks. Topaca said police seized explosive materials from the apartment. Turkey has been rocked by a series of deadly suicide bombings over the past 18 months that were carried out by ISIS or Kurdish militants. Officials banned demonstrations or large gatherings in Ankara until the end of November citing intelligence over possible attacks. Interior Minister Suleyman Soylu told reporters that the man was spotted scouting Turkey's old parliament building as well as the mausoleum of Mustafa Kemal Ataturk -- the founder of the Turkish republic -- where ceremonies are scheduled to take place. "The Daesh militant was rendered ineffective following very important tracking and intelligence work," Soylu said, using the Arabic acronym for IS. "These operations are continuing." CTV News

*** Iraqi forces met with car bombs, mortars in military advance on Mosul**

Islamic State militants have deployed suicide car bombs and fired mortar rounds to slow down the advance of Iraqi troops outside a key town near the militant-held city of Mosul, an Iraqi army officer said Wednesday. The officer from the 9th Division told The Associated Press that his troops were now around 1 kilometre (half mile) away from Hamdaniyah, a historically Christian town also known as Bakhdida. Since Tuesday, IS has sent 12 car bombs, all of which were blown up before reaching their targets, he said, adding that Iraqi troops suffered a small number of casualties from the mortar rounds. The officer, who spoke on condition of anonymity because he was not authorized to talk to reporters, did not provide specific figures. Global News

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Sent to: !DMS External; PS.F DL_DMS F.SP

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
October 21, 2016 / le 21 octobre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Liberals are consulting, but listening, too?
Justin Trudeau's Liberals swept to power last October with a promise of a more open government that better reflects the values and expectations of Canadians. A year later, they're getting credit for a willingness to listen. But it's too early to tell whether that is resulting in decisions and policies the public truly wants. The Liberals have launched a flurry of consultations on matters big and small. At last count, there were 84 consultations accepting online comments about everything from food additives and species at risk to a national housing strategy and security policy. (…) The Liberals promised during the election campaign to fix several specific "problematic elements" of the law. The NDP has chastised the government for embarking on a full national security review before changing even a single line of the legislation. **Public Safety Minister Ralph Goodale** recently defended the Liberals' unhurried approach, saying the government wants to take the necessary time to ***"get this right"*** after the Conservatives

rushed legislation onto the books without properly consulting Canadians. ***"A lot of people felt shut out, and we promised to give them the opportunity to be heard."*** New Hamburg Independent

TOP STORIES / MANCHETTES

* **Record Drug Bust: Seizure of 202 kg of cocaine at Coutts crossing largest in Prairie history**
Authorities intercepted $10 million worth of cocaine at Alberta's Coutts border crossing in the biggest seizure of the drug in Prairie history. The 202 kg of drugs were packed with goods in three separate shipments aboard commercial trucks, beginning with 60 packages of cocaine weighing 69 kg secreted in a cargo of televisions discovered Sept. 2. "Officers noted a small, dense package in a vacuumsealed bag that tested positive for cocaine," said Ana Maria Coutu of the CBSA. Another 40.5 kg of the drug was found two days later amid cargo of 2,000 Halloween costumes - the two making up the largest weekend seizure numbers for the Canada Border Services Agency's (CBSA) Prairie region. But the largest was yet to come on Oct. 10, when 83 bricks of cocaine weighing 92.74 kg were seized from another commercial truck, where it was hidden throughout its cab, said Coutu. "This is the largest cocaine seizure in Prairie region history ... it was destined for an Alberta business," she said. In all, five men have been charged in the three busts with importing a controlled substance and possession for the purpose of trafficking. The RCMP continues to investigate for any links between the three, whose suspects hail mainly from B.C., said Insp. Allan Lai. Calgary Sun, A3 (Edmonton Sun, * Calgary Herald, * Ottawa Sun, * Winnipeg Sun, * Toronto Sun); * Global News; * iNews880

* **DEPORTATION DRAMA: Mother of four fights order to leave**
A young mother facing deportation to the U.K. after spending much of her life in Canada issued a plea Thursday to be allowed to stay in the country she considers home, a day before her strange saga goes before a hearing that may determine her fate. Propped up in a hospital bed and groggy from pain medication, Fliss Cramman said she is terrified of being forced to return to England, where she was born but left at the age of eight when her parents moved to Ontario. "I'm just so scared to go back - I don't know anybody, I don't know anything," she said through tears, while two corrections officers stood guard in her drab hospital room. "If I leave here, I'm leaving my heart behind big-time. This is my homeland." The 33-year-old mother of four young daughters, who were all born in Ontario, only became aware that she was not a Canadian citizen following a recent drug conviction and incarceration. The Canada Border Services Agency looked into her status while she was in custody, discovering that her parents and several foster care families that took her in starting at the age of 11 failed to secure her Canadian citizenship. As a result, the agency says it wants to deport her by Dec. 16, despite her physician's assertion that she is in fragile health and needs to remain in the country for about 18 months to properly recover from a series of colon surgeries done after she was rushed to hospital from a prison facility in Dartmouth on Aug. 12. At a hearing in the basement of the hospital late last month, the Immigration and Refugee Board agreed Cramman would not be able to travel for "at least a couple of months." It said it would review the matter, along with a possible release from custody, at another hearing Friday. Advocates with the Elizabeth Fry Society and a local refugee group agree and have taken on her case, which has attracted attention from across the country. She was convicted of offering to traffic heroin in 2014 and sentenced to 27 months in prison. She served two-thirds of her sentence and was released on parole, but was detained by the Canada Border Services Agency to start the deportation process. Canadian Press (Chronicle Herald, A1, The Guardian, B5, Cape Breton Post, Whitehorse Daily Star, Times Colonist, London Free Press, Vancouver Sun, * StarPhoenix, * Windsor Star; * The Province, * Waterloo Region Record, * Edmonton Journal, * Calgary Sun, * Calgary Herald, * National Post, * Leader-Post)

Drug overdoses take a grim toll in B.C
The fentanyl crisis continues its grim toll with the latest statistics showing more people in B.C. have died from drug overdoses in the first nine months of this year than in all of 2015. There have been 555 deaths as a result of illicit-drug overdoses from January through September, eclipsing the 508 drug-related deaths in B.C. in 2015. The total number of illicit-drug overdoses in September was 56, up from 49 in August, according to the latest statistics released Thursday by the B.C. Coroners Service. The powerful opioid fentanyl was detected in 302 deaths - 61 per cent of all drug deaths from January through August

this year - more than triple the number of fentanyl-related deaths compared with the same period last year. "The ongoing high rates of fatal overdose in British Columbia demonstrate the need for continued collaboration, focus and energy," Evan Wood, interim director of the newly created B.C. Centre on Substance Times Colonist, A1; Canadian Press (Red Deer Advocate, National Post, The Guardian, The Telegram, CTV News, Calgary Herald, Globe and Mail) (2016-10-21); * CBC News (2016-10-20)

*** Tighter security could be coming to Parliament Hill: RCMP**
Parliament Hill security may be beefed up two years after the attack that claimed the life of Corporal Nathan Cirillo. Two years after Michael Zehaf-Bibeau stormed Centre block, the head of Parliamentary Protective Services (PPS) says he's open to putting measures in place to better screen people who want to access the front lawn of Parliament Hill. Currently, people can enter the grounds unhindered, but that may not be the case forever. In the 16 months since he was appointed the head of the new merged security force several measures have been put in place to prevent another attack on Parliament hill. Communications have been harmonized so that all levels of security can actually speak to each other, guards have been given hand guns and RCMP officers are now more visible and more heavily armed on the grounds. C8 carbine rifles are now in the hands of Mounties as they patrol Parliament Hill. The directive follows the report into the shooting deaths of four RCMP officers in Mayerthorpe, Alberta. Global News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Nova Scotia under heavy rain and flood warnings**
Nearly all of Nova Scotia is under a weather warning for heavy rain that could lead to flooding this weekend - but it's still unclear where it will hit the hardest. CBC meteorologist Jim Abraham says the interaction of three systems - a low-pressure system combined with a cold front over the St. Lawrence Valley and a low-pressure system over the Bahamas - will bring tropical moisture to the Maritimes. That means bands of heavy rain and strong southeast winds gusting as high as 70 km/h will start Friday afternoon and continue into Saturday. The latest prediction is that between 30 millimetres and 60 millimetres will fall with peak amounts of 80 millimetres in some areas. There's still much uncertainty as to where most of that rain will fall. Environment Canada's latest statement said it's not just how much rain falls, but the rate at which it falls, that creates problems. Heavy, sudden downpours can cause flash floods and water pooling on roads as well as localized flooding in low-lying areas. CBC News; Charlottetown Guardian; Chronicle-Herald; Cape Breton Post

*** Disaster deductible for storm claims waived**
The province is waiving the $1,000 deductible for people applying to the disaster financial assistance program as a result of the Oct. 10 storm. Announced shortly after the Thanksgiving Day storm that especially ravaged parts of Cape Breton, the program helps homeowners, small businesses, farmers and not-for-profit organizations recover from emergencies. It also provides support for municipalities. The program will cover up to $200,000 per household, an increase from $80,000. "We understand how difficult this situation is for people and how disruptive it is in their lives," said Zach Churchill, minister responsible for the Emergency Management Office. Chronicle-Herald, A7

*** First Nations recovering from flash flood emergency**
Neyaashiinigmiing is getting back to some sense of normalcy after flash floods led to a state of emergency being declared there earlier this week. " Things are progressing quite well and we have addressed most of the road issues ," Greg Nadjiwon, chief of the First Nation at Cape Croker, said Thursday afternoon. " It will be a while yet before we are back to normal, but we are well on our way ." On Monday afternoon, the Chippewas of Nawash Unceded First Nation was hit by heavy rains that led to flash floods that washed out roads and flooded properties and basements. Environment Canada didn ' t have rainfall totals for the region, but radar estimates indicated more than 50 millimetres of rain fell in a short period Monday. London Free Press, A4

*** Fortes pluies et risques d'inondations**

Une quantité de pluie plus grande que ce que l'on reçoit normalement en un mois devrait tomber en quatre jours au Québec, entraînant des risques d'inondations et de glissements de terrain de l'Outaouais jusqu'à Charlevoix. «On parle de 100 mm d'ici à dimanche, c'est une très grande quantité de pluie», estime le météorologue d'Environnement Canada Jean Brassard. La moyenne de précipitations des 30 dernières années pour le mois d'octobre en entier est de 78mm, selon les données compilées sur le site de MétéoMédia. Journal de Montréal, 7

* **Toronto citizens group not satisfied with lists of dangerous cargo released by railways - Crude oil tops list of dangerous substances being transported by rail**
Canada's major railway companies have released lists of the kinds of dangerous goods being transported on tracks that run through Toronto neighbourhoods, but a group of concerned citizens says it's still not enough information to make them feel safe. Canadian National Railway and Canadian Pacific Railway both gave reports to the city earlier this month listing the top 10 dangerous goods they transported in 2015, which account for less than 10 per cent of all the materials they ship. For both railways, crude oil topped the list, making up 44.9 per cent of all the dangerous goods CP carries. For CN, that figure is 34 per cent. The lists, which are posted at the bottom of this story, also contain figures for such substances as liquefied petroleum gases (CN: 16 per cent), sulfuric acid (CP: four per cent, CN: 11 per cent), propane and other petroleum products. Patricia Lai, co-founder of Safe Rail Communities — a non-partisan group that advocates for safe, transparent, and regulated rail — says she's not surprised by the types of dangerous goods the railroad companies have admitted to carrying. But she says the information is of limited value. CBC News

* **Le centre-ville revit à Lac-Mégantic - Les citoyens sont conviés à célébrer la réouverture de la rue Frontenac**
Plusieurs citoyens de Lac-Mégantic pousseront un soupir de soulagement, le mardi 1er novembre prochain, lors de la réouverture tant attendue de la rue Frontenac au complet, la rue principale, et les autres rues du centre-ville perdues à la suite de la tragédie ferroviaire du 6 juillet 2013. L'événement marquera une nouvelle étape dans le cheminement des Méganticois. Les autorités municipales de Lac-Mégantic veulent d'ailleurs marquer l'événement d'une pierre blanche dans l'histoire de la ville, en présentant toute une fête populaire, trois jours plus tôt, le samedi 29 octobre. «Une fête familiale, conviviale, sans fla-fla, du type rencontre entre les gens pour se réapproprier le centre-ville est prévue pour l'occasion», indique le maire Jean-Guy Cloutier. La Tribune, 4

* **'Was that an earthquake?': don't ask 911**
On the day when hundreds of thousands of British Columbians are learning how to survive an earthquake, the province's largest 911 call centre is reminding the public not to call them for information during a natural disaster. More than 800,000 people took part Thursday in the Great British Columbia ShakeOut. Participants were invited to stop, drop, cover and hold on for at least one minute in a simulated earthquake scenario. Last December, on the night a 4.7 magnitude earthquake rocked B.C.'s south coast, E-Comm was inundated with calls... The centre received 318 calls in 15 minutes. That's a 1500 per cent increase compared to normal call volume for that time of day. Most of the calls were for non-emergencies. CBC News

* **Earthquake swarm recorded outside Sussex**
A series of low magnitude earthquakes have been recorded in southern New Brunswick over the past month. A total of ten earthquakes were recorded between Sept. 19 and Oct. 5 in an area south of Route 111, between Sussex and St. Martin's. The earthquakes were recorded by the seismographs that Natural Resources Canada installed in the area. Despite the shallow focus of less than five kilometres, the earthquakes have not been reported as felt by people in this sparsely populated region. "This sequence is what we'd refer to as an earthquake swarm. A swarm is a series of earthquakes that occur within a short period of time and located within a small area." said Maurice Lamontagne, Natural Resources Canada seismologist. Telegraph-Journal, B1

* **Search-and-rescue training facility planned for Comox**
The national training facility for Canada's next generation of fixedwing search-and-rescue aircraft will be located in Comox, the commander of the Royal Canadian Air Force told the editorial board of The

Vancouver Sun and The Province. Bids from three groups are currently being evaluated for an estimated $3-billion contract to replace the country's aging fleets of six CC-115 Buffalo and 12 early model CC-130 Hercules searchand-rescue aircraft, Lt.-Gen. Mike Hood said Wednesday. The training facility at the Comox air-force base would include flight simulators to help pilots train on whichever new aircraft is selected by the federal government. That decision is expect before the end of the year, the general said. A new maintenance program would also be established at the base. The new aircraft would begin to arrive in 2019, said Hood, with the full fleet coming into service over three years and deployed to Canada's four search-and-rescue bases at Comox, Winnipeg, Trenton, Ont., and Greenwood, N.S. Hood said three aircraft are being considered by non-military evaluators, who will make recommendations to the defence minister and cabinet: n The Italian-built Leonardo C-27 turboprop aircraft, part of a joint venture led by General Dynamics Canada and DRS Technologies Canada; n The C295 turboprop military transport, manufactured by Europe-based Airbus; and the KC-390, a jet-powered military transport built by Brazilian aircraft manufacturer Embraer. Hood, a former Hercules pilot, noted the spinoff economic benefits of the new training facility and the additional personal that will based in Comox. Vancouver Province, A3

*** Deep scars left by whale boat tragedy - Pain of West Coast disaster lingers for survivors, families and rescuers**

Entire communities have been honoured, individuals cited for heroism and boats blessed, but one year after the sinking of a whale-watching vessel offBritish Columbia that tossed 27 people into the churning Pacific, the wounds have barely started to heal. Five Britons and one Australian died on Oct. 25, 2015, when the 20-metre Leviathan II capsized in waters near Tofino, about 320 kilometres northwest of Victoria. The cause of the tragedy remains under investigation. The Transportation Safety Board of Canada is expected to release its report next year. Calgary Herald, A7

*** Life-saving heroes honoured by city's fire department - Avalanche rescuer, man who saved LRT passenger, among 27 recognized**

One saved a fellow transit passenger. Another performed first-aid on an unconscious cyclist in a city park. In all, 27 civilians and emergency personnel were honoured by Calgary Fire Chief Steve Dongworth with a Medal of Bravery or certificate of recognition for their heroic acts. "To see folks stepping up in very difficult situations, often putting themselves at risk to help out other Calgarians ... you're often left speechless by the stories," said Dongworth during Thursday's Beyond The Call luncheon. Benoit St. Pierre was awarded the medal for his role in saving a group of skiers buried in an avalanche in March 2014. He used an avalanche beacon locator and a snow probe to dig out two people from under the snow. Calgary Herald, A10; CBC News

*** Windy, stormy weather complicates clean-up operations for sunken B.C. tug**

Blustery, wet weather thwarted efforts Thursday to assess the fallout of a sunken tugboat leaking diesel in a remote region off British Columbia's central coast. All small boats involved in the salvage effort were ordered to stand down at midday, including crews responsible for environmental sampling, wildlife surveys and shoreline assessment for eventual clean-up operations. Crews have recovered more than 88,000 of the estimated 200,000 litres of fuel from the Nathan E. Stewart, which ran aground and sank Oct. 13 in Seaforth Channel, about 20 kilometres west of Bella Bella. A situation report released Thursday afternoon said divers located diesel on the roof of the engine room, which they intend to vacuum out before emptying the boat's submerged fuel tanks. Some experts say the spill is a wake-up call as the provincial and federal governments consider giving permission for larger vessels carrying far greater volumes of fuel in Canada's West Coast waters. Canadian Press (Cape Breton Post; Chronicle-Herald) (2016-10-20)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

*** La Ligue des droits et libertés demande à Ottawa d'abroger la Loi antiterroriste**

Environ 70 personnes ont participé jeudi aux audiences publiques sur la sécurité nationale, à Montréal, qui ont donné lieu à l'expression de plusieurs inquiétudes sur les moyens employés par le gouvernement

canadien pour lutter contre le terrorisme et la radicalisation. Plusieurs organismes ont pris la parole, dont l'Association des juristes progressistes, le Congrès maghrébin au Québec et la Ligue des droits et libertés. Le porte-parole de la Ligue, Dominique Peschard, a demandé que la Loi antiterroriste soit complètement abrogée ou, sinon, substantiellement modifiée. «On est préoccupé, entre autres, par toutes les nouvelles dispositions introduites par la loi qui permettent à 17 agences gouvernementales de partager tous les renseignements que le gouvernement détient sur les citoyens. Les nouveaux pouvoirs accordés au Service canadien du renseignement de sécurité de poser des gestes illégaux sont aussi inquiétants. Ça rappelle les années 60 et 70, où la GRC a volé les listes de membres du Parti québécois par effraction, brûlé des granges et commis toutes sortes de gestes illégaux.» Radio-Canada

*** National security framework needs major overhaul**
An opinion piece states, "Human rights are being abused by CSIS and the RCMP, which will hurt Canada in the end. Over the next few weeks, rights groups, lawyers, activists, experts and concerned individuals will all weigh in on how to achieve a National Security framework upholding both security and rights. The problems with the existing framework are too many to canvass here, but there are a few things that must be done. First, CSIS must stop its practices of: showing up at homes and workplaces unannounced at odd hours; speaking with employers (who are ordered not to disclose this fact); offering incentives for "information"; intimidating newcomers; questioning people about specific institutions; inquiring about one's religiosity; and discouraging people from legal counsel. The situation is so dire that rights groups have had to distribute thousands of "know your rights" guides and organize workshops across the country on dealing with security agencies. (…)The government says it is committed to openness, transparency, and accountability. It must address the above if it wishes to have any real success recruiting Muslims in fighting terror. Otherwise, the anti-radicalization and counter-terrorism office may be a non-starter with the community it seeks to engage." Thestar.com

*** Bill C-51 under review as public hearings take place in Calgary, Vancouver, Toronto, Montreal, Halifax**
When Bill C-51 passed in 2015, a public outrage ensued that Canadians rarely experience.
This past Wednesday, the Canadian government revisited the bill by holding a public hearing in Toronto where citizens were able to voice their views. Motherboard reports that the turnout was dismal compared to the protests that took place just under a year ago, but that those who did show up were passionate. While the bill was under discussion, Canadians protested that their personal privacy was being "eroded by giving the police latitude to essentially do whatever they deem is necessary to stop domestic terrorism," wrote *Motherboard* reporter Jordan Pearson. Speakers took to the mic with just three minutes to voice their concerns. Politicians reportedly looked exhausted, having gone through the same routine the night before in Calgary and the night before that in Vancouver. *Motherboard* reports that the hearing will continue in Montreal on October 20th and in Halifax on Friday. Mobile Syrup

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Security measures being added to protect legislature grounds
Large concrete posts are being erected in front of the legislature grounds at a cost of up to $400,000 to stop a truck bomb or other terrorist attacks. But there's no security measures being introduced to the back of the legislative assembly, close to where many of the politicians park, a seemingly big hole in the plan meant to foil bad guys. House Speaker Chris Collins said the priority was to protect scores of people who gather and demonstrate on the grounds in the provincial capital each year. (…) The politicians discuss security behind closed doors and their deliberations are secret. Collins said they were following the advice of the **federal Department of Public Safety**, which forwarded a threat and risk assessment for legislative buildings. "The people who come to voice their opinion about the legislature don't do that at the back. They congregate in front and we need to roll this out in phases. We can't have our building security brought up to 100 per cent in the first couple of years. This is an ongoing issue, we're making changes, and the bollards in front are the priority for this year." Security specialist Veronica Kitchen argued that if authorities in New Brunswick really wanted to improve security, they should ensure there's good co-ordination between security personnel at the legislature and the local Fredericton Police Force, a shortcoming that was cited in the chaos that surrounded the 2014 lone gunman attack on Parliament Hill

that led to the death of a soldier on ceremonial duty. "One of the lessons learned in Ottawa was that the officers tasked with protecting Parliament Hill were not communicating as well as they might with the Ottawa police and RCMP." She also said it would make sense to have more outreach programs for people who might be on a path to radicalization. "We shouldn't have blinkers on to think those might be just people who are associated with a mosque," she said. "There is also right-wing terrorism and extremism." Postmedia Network (Daily Gleaner, A1, Telegraph-Journal, Times & Transcript)

* **Tighter security could be coming to Parliament Hill: RCMP**
Parliament Hill security may be beefed up two years after the attack that claimed the life of Corporal Nathan Cirillo. Two years after Michael Zehaf-Bibeau stormed Centre block, the head of Parliamentary Protective Services (PPS) says he's open to putting measures in place to better screen people who want to access the front lawn of Parliament Hill. Currently, people can enter the grounds unhindered, but that may not be the case forever. In the 16 months since he was appointed the head of the new merged security force several measures have been put in place to prevent another attack on Parliament hill. Communications have been harmonized so that all levels of security can actually speak to each other, guards have been given hand guns and RCMP officers are now more visible and more heavily armed on the grounds. C8 carbine rifles are now in the hands of Mounties as they patrol Parliament Hill. The directive follows the report into the shooting deaths of four RCMP officers in Mayerthorpe, Alberta. Global News

* **We need an inquiry into the Ottawa shootings**
An opinion piece states, "On Oct. 22, 2014, Hamilton's Cpl. Nathan Cirillo, standing guard at the National War Memorial in Ottawa, was shot to death. The perpetrator, Michael Zehaf-Bibeau, then entered the Centre Block of Parliament with his loaded rifle, creating the worst security breach on Parliament Hill in Canada's history. Cirillo lost his life, and his family and friends suffered grievously. The repercussions of the event, however, go beyond this. Stephen Harper's government used this attack, as well as an assault on two soldiers on Oct. 20, 2014 in Saint-Jean-sur-Richelieu, near Montreal, to push Bill C-51 through Parliament. This controversial bill, now law in Canada, gives intelligence agencies increased power and diminishes the civil rights of Canadians. (…) Why did the RCMP commissioner say there had been "no advance warning" when the evidence suggests there were at least six warnings? Why was the B.C. legislature taking precautions because of these warnings while security forces in Ottawa were caught flat-footed? Why did security forces find it necessary to shoot Zehaf-Bibeau 31 times? Postmedia Network (Hamilton Spectator, A11, Waterloo Region Record, Ottawa Citizen)

* **Defending liberal democracy**
An opinion piece states, "Canadians are truly privileged to live in a stable liberal democratic country. We enjoy rights and freedoms that people in other parts of the world can only dream of but dare not push for out of fear of being killed. However, there are dark forces determined to destroy liberal democracy and kill Canadians. Thankfully, the people of this country can count on the brave women and men of the Canadian Armed Forces to defend democracy. And that makes our military personnel targets for cowardly terrorist attacks. (…) In a compelling chapter about the Islamic State, also known as ISIS, ISIL or Daesh, Welsh chronicles the rise of the terrorist force in the summer of 2014. The jihadists captured large swaths of territory in Iraq and Syria, launching a reign of terror and religiously motivated mass murder targeting Assyrian Christians and other ancient ethnic and religious minorities. (..) The threat to liberal democracy posed by Islamism was raised over a decade ago by American author Daniel Pipes. For years, he was lambasted for writing and speaking about the Islamist threat. But world events have vindicated his work." Kingston Whig-Standard (2016-10-20)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Record Drug Bust: Seizure of 202 kg of cocaine at Coutts crossing largest in Prairie history
Authorities intercepted $10 million worth of cocaine at Alberta's Coutts border crossing in the biggest seizure of the drug in Prairie history. The 202 kg of drugs were packed with goods in three separate shipments aboard commercial trucks, beginning with 60 packages of cocaine weighing 69 kg secreted in a cargo of televisions discovered Sept. 2. "Officers noted a small, dense package in a vacuumsealed bag

that tested positive for cocaine," said Ana Maria Coutu of the CBSA. Another 40.5 kg of the drug was found two days later amid cargo of 2,000 Halloween costumes - the two making up the largest weekend seizure numbers for the Canada Border Services Agency's (CBSA) Prairie region. But the largest was yet to come on Oct. 10, when 83 bricks of cocaine weighing 92.74 kg were seized from another commercial truck, where it was hidden throughout its cab, said Coutu. "This is the largest cocaine seizure in Prairie region history ... it was destined for an Alberta business," she said. In all, five men have been charged in the three busts with importing a controlled substance and possession for the purpose of trafficking. The RCMP continues to investigate for any links between the three, whose suspects hail mainly from B.C., said Insp. Allan Lai. Calgary Sun, A3 (Edmonton Sun, * Calgary Herald, * Ottawa Sun, * Winnipeg Sun, * Toronto Sun); * Global News; * iNews880

DEPORTATION DRAMA: Mother of four fights order to leave

A young mother facing deportation to the U.K. after spending much of her life in Canada issued a plea Thursday to be allowed to stay in the country she considers home, a day before her strange saga goes before a hearing that may determine her fate. Propped up in a hospital bed and groggy from pain medication, Fliss Cramman said she is terrified of being forced to return to England, where she was born but left at the age of eight when her parents moved to Ontario. "I'm just so scared to go back - I don't know anybody, I don't know anything," she said through tears, while two corrections officers stood guard in her drab hospital room. "If I leave here, I'm leaving my heart behind big-time. This is my homeland." The 33-year-old mother of four young daughters, who were all born in Ontario, only became aware that she was not a Canadian citizen following a recent drug conviction and incarceration. The Canada Border Services Agency looked into her status while she was in custody, discovering that her parents and several foster care families that took her in starting at the age of 11 failed to secure her Canadian citizenship. As a result, the agency says it wants to deport her by Dec. 16, despite her physician's assertion that she is in fragile health and needs to remain in the country for about 18 months to properly recover from a series of colon surgeries done after she was rushed to hospital from a prison facility in Dartmouth on Aug. 12. At a hearing in the basement of the hospital late last month, the Immigration and Refugee Board agreed Cramman would not be able to travel for "at least a couple of months." It said it would review the matter, along with a possible release from custody, at another hearing Friday. Advocates with the Elizabeth Fry Society and a local refugee group agree and have taken on her case, which has attracted attention from across the country. She was convicted of offering to traffic heroin in 2014 and sentenced to 27 months in prison. She served two-thirds of her sentence and was released on parole, but was detained by the Canada Border Services Agency to start the deportation process. Canadian Press (Chronicle Herald, A1, The Guardian, B5, Cape Breton Post, Whitehorse Daily Star, Times Colonist, London Free Press, Vancouver Sun, * StarPhoenix, * Windsor Star; * The Province, * Waterloo Region Record, * Edmonton Journal, * Calgary Sun, * Calgary Herald, * National Post, * Leader-Post)

*** FDFA reports September land border and airport results**

The Frontier Duty Free Association (FDFA) has released the latest duty-free sales statistics, provided by the Canadian Border Services Agency for September 2016. The overall national land border duty-free sales figure for the month was C$15.7m ($11.8m) an increase of 7.80% on September 2015. January/September 2016 sales increased around 5.95% compared to the same period in 2015, while sales at land border duty-free shops for January/September 2016 equalled C$117m. On the airport front, the national duty-free sales figure for September was C$36m, an increase of 8% compared to September 2015. January/ September 2016 sales saw an approximate 7.3% increase compared to the same period in 2015. Sales at Canadian airport duty-free shops for January/September 2016 reached C$306m. DFNI Online

*** Airport delays costing economy, critics say**

Officials at Pearson International Airport are pressing Ottawa to cough up more funding to ease backlogs at security and customs checkpoints that have left thousands of air travellers fuming. The problem even has the attention of the prime minister's office after Gerald Butts, the principal secretary to Justin Trudeau, took to social media to express his frustration at recent lineups. "Friday of Thanksgiving weekend and half the security lines are closed at Pearson. #fail," Butts said on Twitter on Oct. 7. But the long lines at peak times are testing more than the patience of passengers - they mean delays, even

missed flights that give Canada's busiest airport a black eye and ultimately cost the economy. Transport Minister Marc Garneau told the Star this week that he's heard the complaints and is looking to act. Certainly Ottawa has been feeling the heat on the issue. The Toronto Board of Trade has joined forces with its counterparts in other major cities to demand Ottawa fix the problem. And now the Greater Toronto Airports Authority, which operates Pearson airport, is adding its voice too. In a Friday presentation to the Commons' finance committee - which is conducting pre-budget hearings - the authority will press Ottawa to invest millions of dollars more to improve security and border services. Scott Collier, the authority's vice-president of customer and terminal services, will call for at least $5 million in extra funding for the Canada Border Services Agency, responsible for customs and immigration screening of arriving international passengers, to improve services at Pearson. During May, authority staff were forced to hold passengers outside a jammed customs hall an average of twice a day with wait times topping 30 minutes. The authority is also urging Ottawa to earmark another $20 million to the Canadian Air Transport Security Authority (CATSA) to improve security screening at Pearson alone. Toronto Star, A7

*** CATSA testing new, improved security system in Montreal, in Calgary later in October**

The agency that oversees airport security is testing a new way of screening that it hopes will ease the backlogs and hassles endured by travellers. Known as CATSA Plus, the new system features motorized rollers to help move bins, a remote room where agents monitor the X-ray images and an automatic return system that ensures a steady supply of bins. It also has a redesigned area where passengers can collect and repack their belongings after screening. "This was designed to improve the passenger experience and the flow of passengers through the checkpoint," Mathieu Larocque, spokesperson for the Canadian Air Transport Security Authority (CATSA). The agency installed the new arrangement on a single security line at Montreal's Pierre Elliott Trudeau International Airport in mid-August. "Early results show it's very positive of the flow of passengers and passenger satisfaction," Larocque said. The new process will get a bigger workout later this month. That's when six security lines begin operating in the new international terminal at Calgary's airport. Toronto Star, A7

Airport screening could be faster, smarter, safer

An opinion piece by Senator Colin Kenny states, "If you've flown anywhere in Canada recently, you will have noticed that wait times are getting worse. Since 2013, the length of screening times has deteriorated so badly that the Canadian Airport Council referred to security screening services as a crisis. Not only are we waiting more, we are paying more. And getting less service. According to the World Economic Forum, Canadians pay some of the highest air travel prices in the world. One part is a fee for the air traveller's security charge (ATSC). The charge was introduced after 9 /11 by the Chretien government to fund air transport security and the new Canadian Air Transport Security Authority (CATSA). It has turned into a major cash grab by the Finance Department. Since 2011, the CATSA budget has declined even though ATSC revenue has increased. From 2010 to 2013, $260 million was siphoned into the consolidated revenue fund... Perhaps our greatest failing is NEXUS, the trusted traveller program. That's the background check where travellers volunteer their information to border officials to become pre-screened. They are then deemed "trusted travellers" and expedited through customs. NEXUS cardholders are also offered a special line at security screening. The problem is, it's not that special. NEXUS users are still forced to submit to the same cumbersome screening procedures as other passengers. If our border officials allow these pre-screened travellers to enter the country quickly and safely, why doesn't the same practice apply at airport security? Replacing this "one-size-fits-all" approach to passenger screening with a risk-based, intelligence-driven approach was a key recommendation in the Emerson review. The United States long ago adopted this model. As a result, "trusted travellers" are able to pass through security quickly. In fact, the processing rates at U. S. airports are twice as fast as in Canada. We could have a security screening system that works not just for a select few, but for everybody. Trusted travellers shouldn't have to take off their belt or shoes or separate their laptops. This would be particularly beneficial to elderly and disabled passengers." London Free Press, N7 (Kingston Whig-Standard)

*** Windsor's weather, traffic and gas price for Friday**

Ambassador Bridge: Traffic is heavy for Canada-bound trucks. Windsor-Detroit Tunnel: No unusual delays. CBC News Windsor

*** McCallum doesn't want to let fraudsters 'off the hook' through moratorium on citizenship revocation**

The federal government is trying to revoke the citizenship of fraudsters, and that's why it won't agree to a moratorium on citizenship revocation, says Immigration Minister John McCallum. "We have large numbers of a criminal element unveiled by the RCMP, and reported on by the auditor general. It was actually under the previous government that [investigations began that] we are now dealing with... and those people have really, truly abused our citizenship. So it would not be right to have a moratorium, and let them off the hook," he said in a phone interview Thursday. Pressure ramped up on the government to stop revoking citizenships after a refugee lawyer said that Democratic Institutions Minister Maryam Monsef could be at risk of losing hers, and even being deported. She revealed last month that she had recently learned she was born in Iran and not Afghanistan, like she had thought. Her mother, she said, hadn't thought it mattered. Ms. Monsef said she was in the process of fixing the mistake on her passport. But Ms. Monsef's citizenship could be revoked if her birthplace was misrepresented on her refugee claim to Canada and that was relevant to the decision on her case—even if it was an honest mistake or her mother was responsible, Toronto immigration lawyer Lorne Waldman told the Canadian Press last month. He is part of a group bringing a constitutional challenge against a law brought in by the previous Conservative government, known as it was as C-24, that means a person who's received notice of citizenship revocation doesn't have a right to an appeal or court hearing. In a written statement provided to The Hill Times, Mr. McCallum's office said "the recent increase in citizenship revocations is the result of large-scale fraud investigations led by our RCMP and [Canada Border Services Agency] partners that began under the former Conservative government. "These investigations led to criminal convictions of several immigration consultants, and notices of intent to revoke citizenship were sent to their clients who had provided fraudulent documents to suggest they were living in Canada when they were living abroad, in order to gain citizenship. Others changed their identity in order to hide criminal backgrounds. "These applicants were never entitled to Canadian citizenship." According to the statement, 80 per cent of citizenship revocations since May 2015 were due to "residency fraud, criminality, and identity fraud," while the remainder were "for other serious misrepresentations." The Hill Times

*** Lululemon warns it might move HQ out of Vancouver**

Lululemon is warning that it may forced to move its headquarters out of Canada because the federal government's temporary foreign worker program is limiting its ability to stretch its wings. The Vancouver-based apparel company best known for its yoga pants currently has 1,200 employees working in its head office in Vancouver and says it needs to hire specialized workers to further expand. "In order to continue growing in a very competitive marketplace, we depend on highly skilled and specialized talent. Currently, there is a shortage of the kind of specialized talent our industry needs here in Canada," wrote the company in a report submitted to the House of Commons Finance Committee. Lululemon was among dozens of other companies that presented the Government of Canada with recommendations on the temporary foreign workers program last month. The report will be responded to with a plan within 120 days. CBC News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Snapchat, Skype, BBM not protecting users' privacy, says Amnesty International**

Major messaging services like Snapchat, Skype and BlackBerry's BBM are not taking basic steps to ensure privacy, according to Amnesty International. The organization said this failure has serious human rights repercussions since it leaves users, and particularly activists, vulnerable to spying from cybercriminals and government agencies. "If you think instant messaging services are private, you are in for a big surprise," Sherif Elsayed-Ali, the head of Amnesty International's technology and human rights team, said in a news release. "Young people, the most prolific sharers of personal details and photos over apps like Snapchat, are especially at risk," he added. The organization conducted a privacy assessment of the most popular messaging apps in the world. Some of the other apps included in the report are Facebook's messaging service and WhatsApp, Apple's iMessage and Facetime, Google's Allo, Duo and Hangouts, Tencent's QQ and Wechat, and Telegram. CBC News

*** Security breach caused online frenzy**

Last month Yahoo announced that at least 500 million accounts were hacked, leaking important personal information. This security breach caused an online frenzy that left many people afraid of having their online information stolen, both in the U.S. and right here at home in Nova Scotia. "People in Nova Scotia are at no greater nor lesser risk than anyone else in the world," said Dr. Wayne Patterson, professor of Computer Science at Howard University. ". . . some prominent Nova Scotians such as Premier Stephen McNeil, Sidney Crosby or Ellen Page might need extra levels of protection." But Patterson suggested keeping information as secure as possible by backing up documents onto a removable device, such as a memory stick. "Some vendors may suggest that you protect your data by storing it in a 'cloud,'" said Patterson, a New Brunswick native. "This is certainly becoming more and more popular, but it is a fairly unsettled issue amongst those of us who do research in cybersecurity." In Yahoo's case, they had recently shut down the division of research staff specifically addressing security issues and were in the process of rebuilding. But Yahoo is not the only company that has been breached in the past. "Microsoft was notorious for many years in putting the most minimal effort in their software development on providing strong security," said Patterson, director of the Cybersecurity Research Center, associate vice provost for Research and senior fellow for Research and International Affairs in the Graduate School at Howard. Chronicle-Herald, E3

*** Verizon relooking at Yahoo deal after millions hacked**

Verizon is doubling down on language it used last week to describe the massive, historic data breach affecting an estimated 500 million Yahoo accounts - a move that puts even greater pressure on the beleaguered web company as it seeks to close a sale to the telecom giant. At the moment, "we have to assume (the breach) will have a material impact on Yahoo," said Verizon chief financial officer Fran Shammo on an investor call Thursday. A change in Yahoo's business that's deemed "material" is one that could make the Internet firm much less attractive to Verizon financially, and under the terms of the deal could allow Verizon to back away from the transaction. Verizon's lawyers talked by phone with Yahoo for the first time Wednesday to discuss the impact of the breach on Yahoo's business, according to Shammo. Verizon will take "some time" to determine the fate of the deal, Shammo said, unless Yahoo "comes up with a different process" for interacting with its buyer. Washington Post (Waterloo Region Record, C7; Toronto Star)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Drug seizure said to be one of largest in B.C.

A routine traffic stop in Nanaimo led to the seizure of one kilogram of fentanyl, one of the largest seizures of the potent drug in B.C. A Vancouver Island man has been arrested as the investigation continues. Nanaimo RCMP officers checked a suspicious vehicle near Cassidy Airport on Oct. 10 about 5 p.m. Officers pulled over the vehicle and arrested the driver. Police found one kilogram of a powdered substance that, after lab testing, has been confirmed to be fentanyl. Island District RCMP spokeswoman Cpl. Tammy Douglas said the seizure is one of the largest for the B.C. RCMP in recent years. A kilogram of fentanyl can be ordered over the Internet and shipped from China or Mexico in small packages that go undetected by the Canada Border Services Agency. Times Colonist, A4

Don't bother coming here if you're a crook

Mounties in B.C. announced this week they were a mapping out a "red zone" for downtown Maple Ridge, a suburb east of Vancouver. A 15-block section known for high crime would become a "designated area" where habitual offenders could be arrested on sight. The National Post's Tristin Hopper called up the experts to get the details on the new crime-fighting tool. (…) Red zones are mainly a B.C. thing. They exist in Vernon, Kelowna, Kamloops and Nanaimo, for example. "I've never heard of it, and I've served all over Alberta," said Sgt. Darrin Turnbull, a spokesman with the Alberta RCMP. However, it's routine for offenders to be ordered to avoid locations connected to their crime. The notorious Atlantic Canadian art thief, John Mark Tillmann, has been ordered to stay away from museums, libraries and archives. Judges may also impose banishment when a regular restraining order doesn't work. In 2002, spousal abuser Ronald Felix was banished from his hometown of Tuktoyaktuk, N.W.T., because it was deemed to be too

small for him to keep the requisite 100 metres or so distance from his victim at all times. (...) Sort of. Red zones can be great at clearing a specific area of crime. But, as has been noted in other communities, the ultimate effect can be to push criminals into another part of town. Vernon RCMP have reported their red zones instantly clear areas of drug activity and property crimes, but that as offenders were driven out "they move to another coordinate around the city." In Kamloops, a similar result prompted city officials to compare red zones to a balloon: push down on one part of the balloon, and the air rushes to another part. (...) Parole conditions can be extensive and, with proper justification, a geographic ban isn't that big of a stretch. Where it might get murkier is in cases where someone has not yet been convicted, yet is still banned from the red zone under release conditions. This is the idea with the Maple Ridge red zone: it is being used to deal with offenders who continue break-ins "even after they have been arrested and are awaiting their court process to begin." Imposing behaviour conditions is standard procedure when an accused criminal is released. The standard Canadian "promise to appear" form even includes a blank section where an arresting officer can write in all the places the accused can't go. Still, there is a judge in the equation - a red zone ban can't simply be a unilateral action by the RCMP. National Post

Dealer jailed as fentanyl conference gets underway

A baby-faced drug dealer nabbed in the first Edmonton seizure of the deadly fentanyl opioid by organized crime investigators was sentenced to 5 1/2years in prison on Thursday. Adrian Laureno Cambiazo, 21, earlier pleaded guilty to possession of fentanyl for the purpose of trafficking, possession of cocaine for the purpose of trafficking and possession of ecstasy for the purpose of trafficking in relation to a March 18, 2015, bust by members of the Alberta Law Enforcement Response Teams (ALERT) - their first such seizure in Edmonton. (...) Speaking at the opening of a fentanyl conference hosted by the RCMP in Sherwood Park on Thursday and Friday, Edmonton Police Service Insp. Dwayne Lakusta said his force has provided extensive training to front-line officers about how to recognize and manage the drug if they come across it, and has introduced safe handling procedures for dealing with fentanyl. Lakusta, who leads the force's Edmonton Drug and Gang Enforcement (EDGE) unit, said they have also acquired an instrument used to safely analyze drugs through their packaging. Police are also hoping to tackle the fentanyl issue through the courts, and are working with Crown prosecutors and the medical examiner's office on a number of cases where investigators are trying to gather enough evidence to lay manslaughter or criminal negligence causing death charges against traffickers or dealers who have supplied drugs that have led to overdose deaths, Lakusta said. Although many of the 400 attendees at the RCMP's conference work in law enforcement, several speakers stressed that "we cannot arrest our way out of the problem." Much of the focus was on safety for responders who encounter fentanyl. A dose of just 2 mg, about the size of two grains of salt, is lethal. British Columbia RCMP Cpl. Eric Boechler showed offwhat he said was one of the first Naloxone nasal spray kits to arrive in Canada. Naloxone blocks and reverses the effects of opioids. Police forces, health workers and social agencies across Canada have begun using injectable doses of Naloxone to prevent overdose deaths, but Alberta RCMP is in the process of switching to a nasal spray version that is easier to use. Edmonton Journal, A3

* **B.C. attempts to seize Burnaby house once used as grow-op**

Vancouver real estate agent Maurizio Mastronardi says he plans to fight the B.C. government's attempt to seize a North Burnaby property he owns, which was once the site of a marijuana grow-op. Earlier this month, B.C.'s Director of Civil Forfeiture filed a claim in the Supreme Court of B.C. seeking to seize a property on Braeside Drive in Burnaby. Mastronardi, a licensed realtor with an east Vancouver brokerage, said a marijuana grow operation at the rental property had been installed by former tenants without his knowledge. He said he was surprised on Wednesday to learn of the civil forfeiture action, coming three months after criminal charges against him were stayed because of court delays. (...) In February of 2011, Burnaby RCMP officers arrested Mastronardi as he left the property, which was assessed last year at $1.65 million. Soon after, Mounties executed a search warrant and found a marijuana grow operation with 152 plants, 41 pounds of recently harvested marijuana bud, a hydroelectric bypass, and other growing equipment, according to court filings. Mastronardi and four others were charged with possession and production of a controlled substance and theft of electricity. A day before the 2011 Burnaby bust, Ridge Meadows RCMP executed a search warrant on a different property in Maple Ridge also owned by Mastronardi, the civil claim notes, where officers found a 443-plant marijuana grow-op. Vancouver Sun, C1

*** Items gathered at Baylee Wylie death scene presented in murder trial**
The jury in Devin Morningstar's first-degree murder trial heard about and saw a number of items of interest Thursday as the Crown started presenting evidence gathered by the RCMP in the death of Baylee Wylie in December. Those items included a box cutter, a piece of broken mirror, a curtain rod, a Big 8 bottle of green liquid, rubber gloves and a rope. The items were presented or mentioned during the testimony of RCMP Cpl. Patrick Gould. His testimony is to continue Friday. CBC News

*** Decision in Yellowknife journalist's obstruction trial expected today**
A ruling is expected this afternoon in the case of a Yellowknife reporter charged with obstruction of justice. John McFadden, a journalist with Northern News Services, was arrested in 2015 while taking photographs of RCMP officers searching a parked van outside the Elks Club in downtown Yellowknife. His trial began in June and wrapped up in September. Today's decision is scheduled to be delivered by territorial court judge Justice Garth Malakoe at 1:30 p.m. in the Yellowknife courthouse. CBC News

*** La GRC enquête sur plus de 80 incendies suspects dans le comté de Kent**
La GRC enquête sur une série d'incendies jugés criminels. Plus de 80 feux suspects se sont produits depuis septembre 2014 dans différentes localités servies par les détachements de Richibucto, Bouctouche et Elsipogtog. La force policière a déterminé que tous ont été allumés délibérément. Environ la moitié sont survenus en soirée ou pendant la nuit dans des résidences, des chalets, des granges, des remorques et des véhicules vacants ou abandonnés. Les autres incendies sont survenus dans d'autres structures et propriétés, comme des commerces et des logements inhabités qui n'étaient pas occupés au moment de l'incident. Personne n'a été blessé jusqu'à présent. Les communautés de Saint-Paul, Harcourt, Beersville, Pine Ridge, Saint-Norbert ou encore West Branch ont été victimes du ou des malfaiteurs. L'Acadie Nouvelle

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Dangerous offender's sentence is reduced**
Although he failed in his attempt to have his conviction and dangerous offender designation overturned, Donald Francis Wilton had some success in appealing the length of his sentence. Wilton was found guilty in November 2012 of break, enter and commit sexual assault, resulting from an offence in the summer of 2008 in which he broke into a residence and stripped to his underwear before lying on top of a 13-year-old girl and touching her sides. DNA evidence linked Wilton to the crime. With 25 convictions for violent or threatening behaviour, the Crown applied for, and received, a dangerous offender designation against Wilton. He was handed a prison sentence of 8½ years (with 45 months remaining after remand credit) to be followed by eight years community supervision. The 39-year-old appealed and, in June, the Saskatchewan Court of Appeal heard arguments from Crown prosecutor Dean Sinclair and Wilton's lawyer Kevin Hill. (…) While the province's highest court didn't agree with Wilton's position on conviction or the DO finding, it found Chicoine had erred in sentencing and replaced the 45 months with 36. Leader-Post, A11

*** Drug-smuggling lawyer offto prison... again**
A lawyer convicted of drug trafficking for smuggling meth into the Edmonton Remand Centre and giving it to an inmate has been ordered to surrender himself into custody after losing his appeal. According to a Court of Appeal of Alberta decision Thursday, Justin Sidhu, 33, was given a week to turn himself in. Sidhu had begun serving a four-year prison sentence in September 2015, but was released on bail a week later pending his appeal. His conviction appeal was heard Oct. 7 and a three-judge panel reserved its decision. In the decision, the panel dismissed the appeal. Postmedia Network (Edmonton Sun, A7, Edmonton Journal, Calgary Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun)

*** Convicted priest faces new sex abuse allegations**
New allegations of sexual assault have emerged against a Winnipeg priest and convicted sex offender, CBC News has learned. Four men have come forward alleging Ronald Léger sexually assaulted them beginning when they were children aged 10 to 12, during the 1980s. All frequented the youth drop-in centre he founded, Teen Stop Jeunesse (TSJ). (…) Léger was sentenced to two years in prison for those

assaults. In September, his application for full parole was denied. A federal parole board determined he is an "undue risk." Instead, the board voted to grant him day parole for six months after determining Léger had a one-in-five chance of reoffending and he scored "just over the low threshold" as a moderate risk to reoffend sexually. CBC News

*** Le suicide et l'homicide possibles**
Nicole Rainville peut s'être suicidée ou avoir été victime d'un homicide. La preuve pathologique laisse les deux portes ouvertes, convient l'expert de la défense. Depuis le début, les avocats de Jacques Delisle défendent une thèse : Nicole Rainville, dépressive et handicapée, s'est enlevé la vie le 12 novembre 2009 en se tirant une balle dans la tête à l'aide du pistolet de calibre 22 de son mari. Selon la défense, la septuagénaire tenait l'arme à l'envers, de sa main gauche, la seule valide. D'abord pour les émissions Enquête et Fifth Estate, puis pour la défense, le Dr Michael Shkrum, pathologiste judiciaire de London en Ontario, a révisé le cas à l'aide de photos et de radiographies. A la lumière de la preuve pathologique, l'expert réputé affirme depuis qu'il y a un doute raisonnable que Nicole Rainville se soit suicidée. Contre-interrogé par le procureur de la Couronne Me Michel Fortin, le pathologiste expert du clan Delisle a admis que si le suicide ne peut être exclu, l'homicide est aussi une possibilité. Le Soleil, 8

Oland decision could come Monday
Dennis Oland should know on Monday whether he'll be able to walk out of court a free man or be sent back to federal penitentiary in Renous to continue serving a life sentence for killing his father, Richard. The New Brunswick Court of Appeal hopes to hand down a decision at 11 a.m. on Monday, providing the three judges involved in the Oland appeal can reach agreement over complex issues in the case. The court could reject the appeal and uphold Oland's second-degree murder conviction, as argued by Crown prosecutors. It also could overturn the conviction and either enter an acquittal or order a new trial - options suggested by Oland's defence team. Daily Gleaner, A1 (Telegraph Journal, Times & Transcript); Canadian Press (The Guardian, National Post, Chronicle Herald); * Presse canadienne (Acadie Nouvelle)

Ontario to limit inmate isolation
Ontario is changing regulations to make the use of segregation in its jails and correctional facilities "a measure of last resort" and cutting in half the amount of time inmates can be kept in isolation. Correctional Services Minister David Orazietti says segregation should be used under the least restrictive conditions possible while still maintaining inmate and staff safety. There will also be a limit of 15 consecutive days in disciplinary segregation, down from the current maximum of 30 consecutive days. Orazietti says the loss of all privileges in disciplinary segregation will be eliminated and replaced with alternative sanctions and increased incentives for inmates to maintain good behaviour. Windsor Star, SR5.

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Drug overdoses take a grim toll in B.C
The fentanyl crisis continues its grim toll with the latest statistics showing more people in B.C. have died from drug overdoses in the first nine months of this year than in all of 2015. There have been 555 deaths as a result of illicit-drug overdoses from January through September, eclipsing the 508 drug-related deaths in B.C. in 2015. The total number of illicit-drug overdoses in September was 56, up from 49 in August, according to the latest statistics released Thursday by the B.C. Coroners Service. The powerful opioid fentanyl was detected in 302 deaths - 61 per cent of all drug deaths from January through August this year - more than triple the number of fentanyl-related deaths compared with the same period last year. "The ongoing high rates of fatal overdose in British Columbia demonstrate the need for continued collaboration, focus and energy," Evan Wood, interim director of the newly created B.C. Centre on Substance Times Colonist, A1; Canadian Press (Red Deer Advocate, National Post, The Guardian, The Telegram, CTV News, Calgary Herald, Globe and Mail) (2016-10-21); * CBC News (2016-10-20)

Surdoses mortelles en hausse en C.-B.

Le nombre de surdoses mortelles en Colombie-Britannique pour les neuf premiers mois de 2016 a dépassé le total de l'an dernier, a rapporté le ministère de la Sécurité publique de la province. Depuis le début de l'année, le bilan s'élève à 555 morts contre 508 cas pour toute l'année 2015. Le fentanyl est la substance la plus souvent en cause, souligne le Ministère. Dans plus de 60 % des cas mortels, des traces de l'opioïde ont été retrouvées. Le bureau du coroner presse les consommateurs de drogue de prendre des mesures pour réduire les risques. Le Soleil, 29

* **Increase in fentanyl deaths sparks justice, health summit in Nova Scotia**
The province's deputy ministers of health and wellness, and justice are calling a meeting to respond to opioid overdoses that are claiming the life of a Nova Scotian every six days. That rate is expected to surge with the rise in street fentanyl. A government email leaked to CBC shows Nova Scotia has averaged 60 opioid overdose deaths per year for the last decade. That's the first time the province has put a number to the deaths from opioid misuse. The deaths are mostly from OxyContin alone, or in combination with alcohol, benzodiazepenes and other prescription and/or street drugs, said the email. But the death toll is even higher so far this year, according to Dr. Gus Grant, the registrar and CEO of the College of Physicians and Surgeons of Nova Scotia. He said approximately 70 Nova Scotians have fatally overdosed. "Can you imagine another health crisis that took the lives of 70 young people? Can you imagine the impact that would have, and it's still only October?" said Grant. CBC News

* **Les drogues de plus en plus contaminées avec du fentanyl**
Consommer de la drogue est plus dangereux que jamais au pays, s'il faut en croire Santé Canada, qui trouve de plus en plus de traces de fentanyl dans les échantillons de substances illicites qu'elle analyse. Selon des données obtenues par Global News, du fentanyl a été découvert dans 2503 échantillons de différentes drogues analysés depuis le début de l'année, en hausse de 43 % par rapport à 2015. Plus de 20 % de l'héroïne vendue dans la rue, et près de 5 % de la cocaïne, serait contaminé avec cet analgésique 100 fois plus puissant que la morphine. «2016 est une année comme on en a jamais vu dans l'histoire canadienne de la drogue et il n'y aura pas de retour. Il n'y a probablement pas eu d'époque plus dangereuse pour être un consommateur de drogue», s'est inquiété Michael Parkinson, un spécialiste du conseil régional de prévention du crime de Waterloo, en Ontario. La mortalité associée à la consommation de fentanyl, voulue ou non, a grimpé en flèche au Canada. Alors que 655 décès par surdose avaient été répertoriés à la grandeur du pays entre 2009 et 2014 par le Centre canadien de lutte contre les toxicomanies, 238 ont été recensés lors des six premiers mois de 2016 seulement en Colombie-Britannique. Un nombre en hausse de 20 % par rapport à la même période en 2015. Journal de Montréal (Journal de Québec) (2016-10-21); Global News (2016-10-20)

* **Bitter Pills**
They lost their children to a powerful drug and hope to spare others from enduring the same pain. "I'm trying to change it so they don't have to walk around with their son's ashes," said Arlene Last-Kolb, whose 24-year-old son Jessie died of a fentanyl overdose on July 18, 2014. "I don't want others to go through what we went through," added Last-Kolb as her voice cracked with emotion. Fentanyl, carfentanil - a drug 100 times more toxic than fentanyl - and other powerful opioids have triggered police warnings across the country. In Manitoba, 29 deaths were linked to the drugs last year, up from 75 such deaths between 2009 and 2013. Several mothers were among those who came to the Manitoba Legislature Thursday to support an NDP resolution for a provincial anti-opiate strategy. That resolution aimed to ensure the antidote naloxone, which can prevent deaths from fentanyl, is equally accessible throughout the province. Fort Garry-Riverview MLA James Allum's resolution also called to reduce treatment wait times for fentanyl users. Winnipeg Sun, A3; Winnipeg Free Press

* **Maple Ridge seeks overdose kits in schools**
The Maple Ridge school board is asking the provincial government to put anti-overdose kits in all B.C. high schools as part of a package of measures to combat the rising number of fentanyl deaths. Board vice-chairwoman Susan Carr's motion, passed this week, seeks "provincial standards for addressing drug use and possible incidents of overdose in B.C. schools, including protocols for training and administering of naloxone (Narcan) in all middle and secondary schools in B.C." Postmedia Network (The Province, A16, Vancouver Sun); CBC News

* **P.E.I. getting fentanyl patch exchange program**
A program to stop fentanyl abuse and the deadly overdoses it can cause is coming to P.E.I. A patch exchange program could be in place by the spring. Fentanyl is an opioid, much more powerful than morphine or heroin. It's prescribed in patch form to treat extreme pain, but if those patches aren't disposed of properly they can easily be used to make and sell the drug on the street. There have only been two fentanyl-related deaths on the Island, according to Michelle Wyand, the registrar of the P.E.I. College of Pharmacists, but she said the program is worth implementing. CBC News

* **Fentanyl filled drug vacuum, and brought waves of deaths**
It is known as the law of unintended consequences. When the opioid painkiller oxycodone, widely sold under the brand name OxyContin, was discontinued in 2012 because of widespread abuse, a cheap, deadly drug filled the vacuum. Drug traffickers began to import low-cost, highly potent fentanyl from China to create counterfeit OxyContin pills. Fentanyl, a prescription painkiller 50 to 100 times more powerful than other narcotics, began turning up in heroin, cocaine, crystal meth and fake Oxy. And the body count began to rise. In 2014, of the 300 illegal-drug overdose deaths, 25 per cent involved fentanyl, according to the B.C. Coroners Service. Last year, 465 people died in B.C. from illicit drug overdoses, and fentanyl was detected in 30 per cent of those deaths. So far this year, 555 people have died of illicit-drug overdoses. Fentanyl was detected in 61 per cent of the deaths recorded January through August. If the trend continues, more than 700 people will die from drug overdoses this year. Vancouver Island has been particularly hard hit: The region has the worst rate of illicit-drug overdose deaths in the province. In the first nine months of 2016, there were 107 deaths on the Island and 44 in Victoria, placing the city behind only Vancouver (110) and Surrey (71). What makes fentanyl so dangerous is its potency. A dose the weight of a grain of sand can bring on a heroin-like high. A dose the weight of two grains of sand can kill a healthy adult. Times Colonist, A3

* **Police board: Policy on carding being posted**
The Hamilton Police Services Board has approved the police capital expenditure plans for 2017 to 2026 — including a new $25 million police Mountain station in 2025. No capital expenditures were listed for 2017 because the board and city council have already approved capital expenditures in 2017 for the new $24-million investigative and forensic building to be constructed next year, said board chair Lloyd Ferguson. (...)A draft of the proposed new Hamilton police policy on carding is being posted to the police website to allow for public input. The draft policy on the "collection of identifying information in certain circumstances — prohibition and duties" is to be posted Friday. The public can register online to make presentations on it to the next police services board meeting on Nov. 17. Carding is an intelligence gathering measure involving the stopping, questioning, and documenting of individuals when no particular offence is being investigated. The draft states that the chief shall ensure the collection of identifying information is done in a manner consistent with the Police Services Act, the Ontario Human Rights Code, and "shall not be based on racial/biased profiling or done in any arbitrary way." See hamiltonpolice.on.ca for more. Hamilton Spectator

* **Campaign underway to help protect youth from cybercrime, cyberbullying**
Efforts are underway to help Fredericton's youth protect their online reputations and avoid cybercrime and cyberbullying. The Fredericton Police Force, Canadian Association of Chiefs of Police and a Telus Wise are working together to roll out a cybersecurity campaign called Smart Social. It will run until the end of the year and is designed to engage local 15 to 22 year olds and their schools in a discussion about cybersecurity. In a press release, Chief Leanne Fitch said everyone has seen the often devastating impact of cybercrime and cyberbullying. "Youth are among the most vulnerable segment of our community and suffer the most from victimization. We hope this campaign has a positive impact on the youth of our community in making their school and young adult experiences safer and happier," Fitch said. Police resource officers will be providing information on cyberbullying, sharing intimate images and identity theft with schools. Daily Gleaner, A3

* **Renowned Communicator Visits School, Focuses on Dangers of Bullying**
Elementary school students in Bulyea took in a powerful presentation Wednesday regarding bullying and cyber-bullying. Retired Saskatoon Police Force Detective Brian Trainor has traveled from coast to coast spreading the word about the sometimes tragic effects of harassment. He specifies that his police work

dealt with bullying on almost every call. "Most of the calls that the police are called to deal with some form of a power abuse or a power imbalance and that's the very definition of bullying. Getting into talking to kids about bullying and then extending into cyber-bullying is just kind of a natural progression from my years of policing." Without trying to be too blunt, especially for online targeting he says it starts with education at home and the raising of the children. Discover Humboldt (2016-10-20)

La violence n'est pas attribuable qu'aux bandes de rue
Les bandes de rue ne sont pas les seuls responsables de la violence, selon Prévention du crime Ottawa (PCO). Les responsables de la Stratégie relative aux bandes de rue dénombraient huit bandes de rue en activité qui regroupaient 435 membres, en 2015. «Le commerce de la drogue, les infractions relatives aux armes, la violence et le commerce du sexe ne sont plus l'apanage de bandes de rue bien organisées. Actuellement, la violence dans la rue est plutôt attribuable à des individus vaguement reliés. Il s'agit surtout de jeunes hommes entre 20 et 30 ans», peut-on lire dans le rapport qui fait état des trois premières années d'opération de la Stratégie relative aux bandes de rue. Malgré la hausse des fusillades depuis le début de l'année 2016, l'important est de changer la façon d'opérer afin d'enrayer la violence dans les rues et mieux répondre aux activités criminelles qui surviennent dans les rues d'Ottawa, soutient PCO. Bien que la criminalité soit en baisse, selon eux, les infractions en lien avec les armes à feu inquiètent. Le Droit, 9

* **Gangs de rue et prostitution : le silence des victimes complique les choses**
Les gangs de rue se livrent notamment à la prostitution comme source de revenus. Or, les femmes qui sont embrigadées de force dans cette forme de commerce du sexe observent souvent la loi du silence, ce qui complique le travail des intervenants communautaires. C'est là l'un des constats faits à l'occasion du forum public sur les gangs de rue à Ottawa et à Gatineau, organisé par Radio-Canada, jeudi après-midi, au collège La Cité. Des spécialistes en traite de personnes et en intervention communautaire ont raconté la difficulté qu'elles éprouvent à obtenir des témoignages des victimes lorsque des accusations sont portées contre de présumés recruteurs ou proxénètes. « Ça prend beaucoup de temps avant que la victime soit prête à pousser pour dire : "Voici, c'est cette personne-là qui est venue me chercher." », a expliqué la responsable du volet éducation chez Personnes en action contre la traite des personnes (PACT-Ottawa), Pauline Gagné. Radio-Canada

* **Police board OKs $500,000 request for bodycam bids**
The Toronto police board has approved a pricey second step in an ongoing examination of body-worn cameras, taking the service closer to equipping all front-line officers with the increasingly popular technology. One month after a much-anticipated report on the Toronto police body-worn camera pilot project was released, the civilian board agreed to spend $500,000 on a non-binding request for proposals to find the best, most affordable camera technology. The money will also pay for a fairness commissioner and outside experts to ensure the search is above-board - something city councillor and police board member Shelley Carroll said is costly but necessary. "The reality is, we absolutely need this. This will be the biggest contract for a new technology in the country," she said at Thursday's board meeting at Toronto police headquarters. A supporter "in principle" of the deployment of body-worn cameras, Mayor John Tory said the cost of ensuring the police service does a proper technology evaluation "will pay itself back many times over. Toronto Star, GT1

* **Study shows EPS and Somali community making progress**
Edmonton's Somali community and its police service have not always been working from the same playbook. But that trend is slowly changing. A study brought to the Edmonton Police Commission on Thursday suggests both police in the city and young Somali Edmontonians are interested in working with each other to tackle issues facing the Somali community. "We interviewed and surveyed 301 young Somali Canadians in the city ... 81 per cent of these young people identify that they are hoping to build a stronger relationship with EPS," said Sandra Bucerius, associate professor of sociology at the University of Alberta, who was part of the team that did the study. Researchers also spoke with 57 police officers of all ranks and all areas of the city except the southeast and found that police were also enthusiastic about learning more. The question is, what community should that education be focused on? "Do we need training? Absolutely. But it becomes a bit exhaustive, too," said Chief Rod Knecht. The committee heard that, despite their willingness to learn about Edmonton's smaller community groups, there are just too

many groups to do that with and still do the job of policing. The Somali community was the focus of the study because of ongoing concerns that peaked a decade ago when violent crimes in that community reached record levels. Postmedia Network (Edmonton Sun, A8, Edmonton Journal)

*** Lots of green for Boys in Blue**

Ottawa police are expecting to blow their overtime budget by $2.4 million by year's end and are blaming the "significant pressure" on what officers counter are understaffed units and a record year for shootings and homicides. Despite the forecast on overtime, the force still expects to have a balanced budget by the end of year and won't increase its overtime budget for 2017. In a financial status update expected to be received by the police board Monday, the force said the overtime deficit ballooned by an additional $250,000 after a national outlaw biker run by the Hells Angels at the now-defunct Nomads clubhouse in Carlsbad Springs. Police said the additional costs were coming from "a number of sources" and, for the first time, detailed which units had the most "significant" costs during the first nine months of the year. The force attributed high overtime numbers to the homicide squad, "special projects," the tactical unit, the guns and gangs squad and emergency services unit. Postmedia Network (Ottawa Sun, A3, Ottawa Citizen)

Poll reveals crime a concern among public

Almost a decade after an infamous Maclean's magazine article dubbed this city "rotten Regina" and claimed it was home to "Canada's worst neighbourhood" (North Central), perceptions about crime continue to provoke debate. Newcomers to the city whose opinions might have been coloured by them hearing repeated statistics on Regina's admittedly high crime rate often express surprise (and delight) at the relative safety of most streets and neighbourhoods. Sure, like anywhere else some serious crimes are committed here, but for most residents, Regina is a safe place to work, live and raise a family. Still, it only takes something like a dramatic increase in the number of guns seized by police combined with several shootings - as has happened this year - to make people uneasy and fearful. It is certainly an issue for new police chief Evan Bray, a 21-year veteran of the Regina Police Service, who said this week the escalation of gun crimes was "concerning" and he was making it one of his priorities. That's good to hear. We don't want to overstate it, but a new Postmedia poll conducted by Mainstreet Research reflects some significant public concern about crime. Though 56 per cent of Reginans surveyed felt the city was "very" or "somewhat" safe, compared with 39 per cent calling it "not too safe" or "not at all safe," a substantial number - 45 per cent - believe crime is increasing. Just 15 per cent felt it was decreasing, while 34 per cent said it was staying the same. The rest didn't know. StarPhoenix, BR18

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** 'Pig Girl' - a Play About #MMIW Portrayed by Akwesasne Mohawk Women**

Sacred Roots Productions is a Native production company owned by Akwesasne Mohawk women, Shelby Mitchell-Adams and Jessica Loft-Thompson. In October 2015 they began production on a culturally appropriated adaption of "Pig Girl," a riveting, intense play by Governor General Award Winning Playwright Colleen Murphy, loosely based on serial murderer Robert Picton. Many of Picton's victims were Indigenous women and along with "The Highway of Tears," the infamous Highway 16 in northern British Columbia where at least 19 women disappeared and probably many more, these events sparked the #MMIW movement. (…) Sacred Roots' sole intention at the outset was to remind people why it is important for the government to continue to push forward with a National Inquiry into Missing and Murdered Indigenous Women. Which they finally did on September 1, 2016. Indian Country Today Media Network (2016-10-20)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Riding high: Tougher penalties now in place for drug-impaired drivers**

Sarnia Police say they are ready to enforce a new provincial law that can cost motorists their licence if caught driving high. As of Oct. 2, drivers under the influence of drugs face an immediate three-day licence suspension, a $180 fine and, following further testing, a possible 90-day licence suspension. But unlike alcohol, there is no universally accepted roadside test for marijuana impairment, which is where things get hazy. Const. John Sottosanti said until a proven and available drug detection device becomes available Sarnia Police will rely on a specially trained officer called a Drug Recognition Expert, or DRE. "He's been trained to determine if the person is actually impaired by drugs, and to make a determination of what type of drug the person has taken," Sottosanti said. "The final step of the whole process involves that a urine sample be taken and sent off for testing." As Ottawa inches closer to legalizing recreational marijuana use, police departments are working to improve their methods of detecting roadside impairment. RCMP in Vancouver are testing Breathalyzer-like devices able detect trace amounts of THC, the active chemical in marijuana, in a person's saliva. "Such devices can aid in the identification and apprehension of drug-impaired drivers and are becoming increasingly commercially available and are currently being used in other countries," the RCMP said in a statement. Officers ask drivers to stick out their tongue and saliva is taken with an instrument similar to a tongue depressor. Sarnia Journal

*** Grits' plan to legalize pot hazy: province**

The Manitoba government said Ottawa must provide more information about its plans to legalize marijuana as soon as possible because the provinces have work to do in order to implement the change. Justice Minister Heather Stefanson said all her provincial counterparts agreed at their recent meeting in Halifax they're going to need details before legislation is introduced. "We need to know what the framework is going to look like so we can prepare," she said. The federal government has said it intends to begin the legislative process to legalize marijuana next spring, but it hasn't released details. A task force led by former health minister Anne McLellan is studying the issue. Bill Blair, former Toronto police chief-turned Liberal MP, said this week the issue is complex, but he spent two hours on the phone with the task force Monday, and its members will be ready to deliver their report on time next month. Provincial health ministers got an update from McLellan Tuesday during their meeting in Toronto, but Stefanson said the province is still mostly in the dark about the direction Ottawa intends to take. "Whatever happens, they have to provide clarity," she said. The province could have to pass its own legislation or regulations on aspects of the change, including the setting of an impaired-driving limit, as well as determining whether police and court resources require adjustments and how and where marijuana will be sold. Stefanson said distribution is going to fall under provincial jurisdiction. Manitoba's former NDP government was leaning toward marijuana sales at provincial liquor stores, which is also the route Ontario Premier Kathleen Wynne has said she prefers. Winnipeg Free Press, A3

*** Ottawa police only want to hear 'legitimate' complaints about illegal pot shops**

Don't approve of marijuana? Please, don't call the police to share your views. But if you have "legitimate" concerns about an illegal marijuana dispensary that's opened in your neighbourhood, by all means, Ottawa's finest want to hear from you. That's the message from a report to be presented by Chief Charles Bordeleau at the Ottawa Police Services Board meeting on Monday. At the last board meeting the chief was asked for the force's position on marijuana dispensaries currently operating illegally in Ottawa, in response to several councillors' concerns about having these illegal shops in their wards. Bordeleau's response came in the form of a report that asked "councillors to encourage people to contact the OPS to file legitimate complaints regarding a dispensary. By legitimate we are referencing something that goes beyond personal beliefs about marijuana or beliefs that marijuana should not be available to anyone at any time." CBC News

*** The black market turns grey**

Meet the boss of Canada's illegal marijuana trade, Don Briere. To police and the criminal courts, he is already a familiar face, a maverick dealer and convicted grower who has served multiple prison sentences for refusing to obey this country's longstanding prohibition on pot. Briere has fought the law and lost, most of the time. And yet, even at an age when most Canadians are entering retirement, this 65-year-old British Columbian is more involved in the underground cannabis business than ever. (…) None of Briere's Vancouver stores passed muster with the city; none received the required permits. They have remained open, racking up thousands of dollars in municipal fines, which Briere refuses to pay. He is not waiting for the federal government to introduce legislation that will legalize and regulate the sale of

recreational marijuana to adults in Canada, either. Briere doubts the new rules - expected to come into force in the next year or two - will make room for his stores. (...) According to several sources, even the regulated medical marijuana market in Canada has been compromised. For decades, police have used a breathalyzer to test whether a driver has had too much alcohol. Now that Canada is on the verge of legalizing marijuana, is there a similar roadside test to detect pot-impaired motorists? The answer, according to the RCMP, is yes ... and no. Q So, what are police doing to get ready to crack down on stoned drivers? Public Safety Canada and the RCMP are investigating three roadside devices that will collect saliva from drivers. It's easier to collect, compared to blood or urine, which typically require warrants. Q How do they work? Unlike a breathalyzer, they will not tell police how impaired a person is. They will not quantify the amount of pot in the system, the RCMP says, but instead will indicate when a drug is present so further followup can be done to confirm the amount. Postrmedia Network (National Post, A2, Ottawa Citizen, Edmonton journal, Calgary Herald, StarPhoenix, London Free Press, Vancouver Sun, Windsor Star, Leader-Post)

* **Légalisation de la marijuana : boom économique au Colorado**
Le gouvernement de Justin Trudeau souhaite déposer un projet de loi visant à légaliser la marijuana au printemps 2017. Plusieurs craignent les effets de cette mesure sur la santé et la sécurité publique. Radio-Canada Acadie s'est rendue au Colorado où la marijuana est légale depuis 2012 et où la vente est réglementée depuis 2014 pour voir comment l'État s'est adapté à cette nouvelle réalité. Voici le premier d'une série de reportages sur la question. L'année 2016 s'annonce historique au Colorado. Les revenus de la vente de marijuana sont en hausse. Depuis 2015, les ventes dépassent celles de l'alcool. Les ventes de marijuana ont atteint 996 millions en 2015 au Colorado. Cent trente-cinq millions de dollars reviennent dans les coffres du gouvernement. Tout indique que l'État atteindra de nouveaux records en 2016. Selon le plus récent rapport du gouvernement, les revenus des taxes et droits perçus sur la marijuana ont augmenté de 45 % comparativement à l'an dernier. Radio-Canada

PUBLIC SERVICE / FONCTION PUBLIQUE

* **From a courageous ocean rescue to using a robot to deliver health care**
The young crew of a Fisheries and Oceans rescue boat who braved the North Pacific in weather that tested their small craft to rescue a survivor of a capsized fishing boat, then continued searching tirelessly through the night for the other fishermen. A Health Canada team that used a robot dubbed Rosie to allow people in a fly-in community to have real-time remote virtual visits with doctors doing everything from directing emergency resuscitation to psychiatry. The Elections Canada group tasked with turning around the dismally low number of young Canadians turning out to vote - and shaping their own futures - in the run-up to last year's election. Their unsung stories were highlighted Thursday as the Public Service Award of Excellence was handed out to 238 recipients by Gov. Gen. David Johnston and Clerk of the Privy Council Michael Wernick. (...) centres overseas, reception centres and charter flights to Canada, working with all levels of government at home and abroad, and service groups and community organizations in Canada, requiring "considerable diplomacy." Mieke Bos, Treasury Board of Canada Secretariat, Élaine Chatigny, Public Health Agency of Canada, Devin Conley, National Defence, C. Mark Cosenzo, Canadian Security Intelligence Service, Alain Desruisseaux, Privy Council Office, Dawn Edlund, Immigration, Refugees and Citizenship Canada, Eric Gordon, Royal Canadian Mounted Police, Mark Gwozdecky, Global Affairs Canada, Brenda HenslerHobbs, Transport Canada, Shawn Hoag, Canada Border Services Agency, S. Craig Oldham, Public Safety Canada... Ottawa Citizen

OTHER / AUTRE

Investment, immigration, infrastructure keys to growth, say fed's advisers
The Trudeau government's influential team of economic advisers unveiled a batch of growthlifting recommendations Thursday that focused on immigration, infrastructure and investment strategies. The objective, the experts say, is to double Canada's projected growth trajectory and add $15,000 to the annual incomes of Canadian households by 2030. The suggestions comprise a first tranche of ideas from the group of external experts who have been enlisted by Finance Minister Bill Morneau to help

Ottawa find ways to resuscitate Canada's lacklustre economy. The recommendations zeroed in on three areas: productivity-boosting infrastructure, attracting more foreign investment and opening Canada's doors wider to a larger number of talented immigrants. "Now is the time where we have to take very bold actions," council chair Dominic Barton, who is global managing director of consulting giant McKinsey Co., told a news conference in Ottawa. "[The suggestions] may not be new, these have been talked about before - but they haven't been done. And so what we're keen to do is to jolt it." It also recommended that the federal government ramp up permanent immigration to 450,000 people a year over the next five years - with a focus on top business talent and international students. "An increased immigrant population has positive implications for business and job creation for Canadians through entrepreneurship and innovation, international trade and if done right, can raise living standards for all Canadians," the document said. But Immigration Minister John McCallum, who was briefed on the recommendation, has already described that kind of a spike in immigration levels as overly ambitious. Canadian Press (Times Colonist, B2); * Postmedia News (Vancouver Sun, StarPhoenix, Edmonton Journal, Leader-Post, Calgary Herald, Ottawa Citizen)

INTERNATIONAL

Germany passes new spy law allowing espionage against allies
German lawmakers have approved a bill that allows the country's foreign intelligence agency to spy on European Union institutions and fellow EU member states. The legislation passed Friday is part of a range of measures meant to improve oversight of espionage in the wake of the revelations by former U.S. National Security Agency contractor Edward Snowden. A panel of independent judges will have to be informed when the BND spy agency eavesdrops on Germany's allies. Judges will also have the right to undertake spot checks of the agency's work. Parliament's intelligence oversight powers will also be increased and intelligence chiefs will have to attend a public hearing before lawmakers every year. Critics say that instead of clamping down on questionable BND activity the law will merely legalize them. Metro News

ISIS fighters kill at least 11 in Kirkuk attacks: Suicide bomb attack occurs at power plant north of Kirkuk
Islamic State militants armed with assault rifles and explosives attacked targets in and around the northern Iraqi city of Kirkuk early Friday in an assault that appeared aimed at diverting Iraqi security forces from a massive offensive against the ISIS-held city of Mosul. At least 11 workers, including two Iranians, were killed when ISIS militants stormed a power plant north of Kirkuk and then blew themselves up. Multiple explosions meanwhile rocked the city, and gun battles were ongoing, said witnesses in Kirkuk, speaking on condition of anonymity as they were concerned for their safety. Much of the fighting was centred on a government compound in the city. They said the streets were largely deserted out of fear of militant snipers. ISIS said its fighters targeted the provincial headquarters. The claim was carried by the ISIS-run Aamaq news agency and could not immediately be verified. Local Kurdish television channel Rudaw aired footage showing black smoke rising over the city as extended bursts of automatic gunfire rang out. It quoted Kirkuk Gov. Najmadin Karim as saying that the militants have not seized any government buildings. CBC News

*** Syrie: 500 morts en un mois à Alep et risque de pénurie alimentaire**
Le secrétaire général de l'ONU Ban Ki-moon a fustigé jeudi les résultats "horribles" des bombardements russes et syriens sur Alep-est qui ont fait, selon lui, près de 500 morts et 2.000 blessés depuis le 23 septembre. Un quart des personnes tuées sont des enfants et la nourriture se raréfie dans la partie assiégée de la ville syrienne, a-t-il souligné lors d'une session informelle de l'assemblée générale de l'ONU consacrée au martyre d'Alep. Aucun convoi de l'ONU n'est entré dans cette partie de la ville depuis le 7 juillet "et, dans ces conditions dignes du Moyen-Age, les plus vulnérables sont ceux qui souffrent le plus", a-t-il rappelé. "La faim a été utilisée comme arme" dans cette offensive, a estimé M. Ban. "Les rations alimentaires seront épuisées à la fin du mois". Tout en "accueillant favorablement" la pause décidée par la Russie dans les bombardements --ce qui devrait permettre des évacuations médicales dès vendredi--, il a ajouté: "C'est le strict minimum". Il a exigé "un plein accès humanitaire à la partie Est d'Alep". "N'avons-nous rien appris de Srebrenica et du Rwanda?", a-t-il lancé aux ambassadeurs réunis.

"Quand la communauté internationale va-t-elle s'unir pour mettre fin à ce carnage?" Cette réunion avait été convoquée à l'initiative du Canada, soutenu par 71 pays, après que le Conseil de sécurité eut échoué à adopter une résolution pour mettre fin aux bombardements russes et syriens sur Alep. Ces 72 pays, sur les 193 membres de l'ONU, ont signé une lettre adressée à M. Ban lui demandant que l'assemblée se saisisse de la crise humanitaire en Syrie. La Russie et la Chine, ainsi que de nombreux pays africains et quatre autres membres du Conseil (Angola, Sénégal, Japon, Venezuela) n'avaient pas signé cette missive. TRT

* **Turkey ramps up fight against Kurdish fighters in Syria**
Turkey escalated its offensive Thursday against Kurdish fighters in northern Syria, pounding them with airstrikes and artillery, and complicating the battle against the Islamic State group by Ankara and Washington, both NATO allies. In the fight for Aleppo, meanwhile, the Syrian military used a lull in violence to urge residents and rebels to evacuate the besieged opposition-held part of the city. Turkey's state-run Anadolu news agency said as many as 200 members of the Kurdish-led forces were killed in Syria's Aleppo province by the Turkish bombing and shelling. A senior commander with the main Syria Kurdish militia confirmed the Turkish attack on his forces north of Aleppo but disputed the casualty toll, saying that no more than 10 fighters were killed. Like in Iraq, where Kurdish fighters are at the forefront of the offensive to retake the city of Mosul from the Islamic State group, Kurdish forces in Syria also have been battling IS militants and made significant territorial gains in Aleppo province. That has dismayed Turkey, which is dealing with a homegrown Kurdish insurgency and trying to prevent an expansion of Kurdish influence in Syria. "We will not back down," senior Kurdish commander Mahmoud Barkhadan of the People's Protection Units told The Associated Press by telephone from the region. "We are fighting Daesh. Why are they striking at us?" he asked, using the Arabic acronym for IS. Barkhadan accused Turkey of aiding IS militants by turning the fight into a Turkish-Kurdish battle. Turkish artillery also hit near Afrin, a Kurdish enclave in northwestern Syria, he said, adding that his forces have not retreated but that Turkey's actions allowed IS fighters to wage a counteroffensive. Times & Transcript, B5

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Sent to: !DMS External; PS.F DL_DMS F.SP

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 23, 2016 / le 23 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Big Brother et « Five-eyes »
La consultation sur la sécurité nationale menée par le gouvernement Trudeau tire à sa fin et deux événements récents appellent les Canadiens à la plus grande vigilance pour la suite des choses. L'affaire de la surveillance des journalistes au Québec et le jugement de la Cour fédérale sur la collecte et la rétention de données personnelles par le Service canadien du renseignement de sécurité (SCRS) montrent bien que l'équilibre entre la sécurité et la protection de la vie privée reste au centre des préoccupations devant les demandes incessantes de pouvoirs accrus des autorités. Les libéraux ont promis en campagne d'« annuler les dispositions problématiques » du projet de loi C-51 adopté en vitesse après les attaques d'octobre 2014, législation qu'ils avaient appuyée avec réserve. Ils ont inclus cet engagement dans une consultation plus large basée sur un livre vert qui lance les discussions. Le

gouvernement est déjà passé à l'action sur un aspect de la consultation, soit la supervision politique des agences et organismes chargés de la sécurité nationale. Le projet de loi C-22 prévoit la formation d'un Comité parlementaire sur la sécurité nationale et le renseignement. Tenus au secret, ses membres auront un accès sans précédent au Canada aux informations sur les opérations liées à la sécurité nationale. **Le ministre de la Sécurité publique, Ralph Goodale**, a expliqué son empressement en indiquant que le Canada était une « ***anomalie*** » en la matière par rapport à ses partenaires de ce club du renseignement qu'est le « Five-Eyes », qui regroupe aussi les États-Unis, la Grande-Bretagne, l'Australie et la Nouvelle-Zélande. Il s'est d'ailleurs rendu en début d'année à Londres, se disant inspiré par le modèle britannique, qui a le grand mérite selon lui de ne pas avoir donné lieu à des fuites qui auraient pu mettre en danger la sécurité nationale. La participation du Canada aux échanges du groupe Five-Eyes est d'ailleurs un élément central du contexte dans lequel les nouvelles normes canadiennes sur la sécurité nationale seront définies. C'est un aspect que les Canadiens doivent garder à l'esprit quand ils évaluent les positions des autorités compétentes et des défenseurs de la vie privée. Étant donné l'attirance britannique du **ministre Goodale**, l'adoption jeudi dernier à Londres du projet de loi sur les pouvoirs d'investigation mérite l'attention. Fait intéressant, d'autres dispositions de la même loi se retrouvent parmi les hypothèses soumises aux Canadiens par **le ministre Goodale** dans son livre vert. C'est ainsi que les fournisseurs britanniques de services de communication (FSC) devront conserver pendant une année les données de navigation en ligne de leurs clients et que les enquêteurs pourront accéder sans mandat aux données de connexion. Les FSC seront contraints d'aider les autorités lors d'interceptions ciblées, en plus de devoir retirer sur demande leur propre chiffrement des données. Le Devoir, A3

Senator tables bill to protect source confidentiality

The relationship between a journalist and a confidential source is sacrosanct, according to a Parliamentarian who wants to enshrine that relationship in law. Amid a scandal over revelations that police in Quebec spied on several journalists, Conservative Senator Claude Carignan has introduced a private member's bill that aims to keep police from ferreting out reporters' sources. "It's a fundamental principle. It's very important to protect the journalist and also the whistleblower," Mr. Carignan, the Senate's opposition leader, told reporters in Ottawa on Tuesday. While Quebec recently announced a commission of inquiry into press-freedom issues, Prime Minister Justin Trudeau has resisted calls for a Canada-wide inquiry. But Mr. Carignan said Parliament cannot afford to wait. Bill S-231, the Journalistic Sources Protection Act, seeks to "protect the privilege of journalistic sources, and secrecy," he said. Last year, the RCMP ordered a Vice News reporter to surrender materials related to conversations with a Canadian member of the Islamic State. And the Mounties briefed **Public Safety Minister Ralph Goodale** last year about the fact that some detectives had shadowed a Quebec reporter who obtained a leaked CSIS document. Globe and Mail, A4

Watchdog wants rules for spies sharing info

Other national security agencies may be taking the same broad view of the law that led CSIS to illegally keep data on innocent people for almost a decade, the federal privacy watchdog says. Privacy commissioner Daniel Therrien said he's calling on Parliament for clearer rules about how spy- and law-enforcement agencies obtain, retain and destroy information on Canadians. Therrien said information-sharing powers granted in Bill C-51, the former Conservative government's controversial spying bill, need restrictions on what agencies can share and how long they can keep the information. "Security agencies, with (Bill C-51 powers) and with the absence of rules around retention, for instance, would be able to collect and retain information that they don't really need," Therrien told the Star outside a House of Commons committee Tuesday. "I don't dispute that CSIS needs to analyze information in order to do their job ... but once the analysis has been completed and the vast majority of people about whom they're collecting information are found not to be a threat, and that's the case, then they should destroy that information." "I don't think that's the kind of country we want, where the security services of the country hangs onto information on vast amounts of people in case it might be helpful one day," Therrien added. In his testimony before the access to information, privacy and ethics committee, Therrien noted Canadian spy agencies misusing powers is not a "theoretical" issue. He noted that CSIS was recently found by a federal court to have illegally kept data on an unknown number of innocent Canadians between 2006 and 2015. Therrien's comments come as the governing Liberals are in the midst of a wide-ranging review of Canada's national security agencies and issues of oversight for spies. They also come as Canada's

national police force, the RCMP, are publicly arguing for expanded investigative powers in the online world. A spokesperson for **Public Safety Minister Ralph Goodale** said the minister looks forward to the Commons committee's report on Bill C-51's information-sharing powers and appreciates Therrien's insight into these issues. Toronto Star, A10

Territorial government preparing for federal marijuana legalization
The territorial government has formed an inter-departmental working group to prepare for the eventual legalization of marijuana across Canada. The group is also in discussions with the federal government, according to Department of Justice spokesperson Sue Glowach. The task force was established by the minister of Justice and Attorney General of Canada, **the minister of Public Safety and Emergency Preparedness** and the minister of Health, according to Glowach. She stated the task force's mandate is to inform the federal government's commitment legalize and regulate marijuana. The report is expected to be released to federal ministers by the end of the month ahead of next April's anticipated marijuana legalization legislation. "The information on potential systems for production, distribution, promotion and taxation provided in the report should make it possible to determine what the role of the ... territories will be," she stated. Yellowknifer

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Lesson learned in Japan**
Japan learned through a series of hard lessons, culminating 20 years ago, that it needed to make a more concerted effort to reduce the damage from earthquakes before they happened. Although the country had made progress in improving seismic resiliency through improved building codes and early-warning systems, there was a major shift toward this preventive approach following the catastrophic 1995 earthquake in southern Japan near Kobe, which killed more than 6,000 people... "There was a call for a nationwide movement of disaster reduction," Satoru Nishikawa, executive director of research for the Japan Center for Area Development Research, told a disaster forum at the University of B.C. this week... The event Monday - organized by the Japanese and B.C. governments - attracted about 100 provincial, local government, emergency, academic, business, engineering and aid representatives. The forum was held as the B.C. government is attempting to increase its preparation for a major earthquake. Scientists say there is a 30 per cent probability of a damaging earthquake hitting a populated area in southwest B.C. in the next 50 years. Underscoring the need for preparedness was a report released Tuesday by the Conference Board of Canada that says a major quake in British Columbia could devastate the Canadian economy, lead to longlasting costs and potentially the failure of the insurance industry... The B.C. government has seismically retrofitted schools and bridges, but shown little interest in addressing thousands of privately owned buildings that do not meet modern seismic safety standards, an examination by Postmedia has shown. The province's minister of state for emergency preparedness, Naomi Yamamoto, told the forum she does not believe British Columbians are prepared for a major earthquake. Postmedia Network (Vancouver Sun, A8)

*** Red tape, uncertainty slows rebuild for some in Waterways**
For months, demolition crews frantically razed thousands of pounds of ash and debris in Waterways to clear the way for a hasty rebuild. With construction on new homes starting, there is no trace of the anticipated non-stop frenzy at roughly half of the empty lots in the neighbourhood most devastated by May's wildfire. When municipal council stripped rebuild restrictions in early October, it came with a caveat: anyone rebuilding in a flood hazard zone - properties below the 250-metre land contour mark - would be doing so at their own risk. Council assured the dozens of homeowners in the floodway they would receive financial aid from Alberta's Disaster Recovery Program if floodwaters engulfed the community before mitigation measures were built. Homeowners willing to take that risk needed to sign a legal waiver, absolving the municipality of any responsibility if their homes flooded in the future. Even for those still

willing to return to Waterways, construction cannot begin because the waiver is still being written by the municipality's legal and planning departments. Fort McMurray Today

*** Some Cape Breton flood victims live with mould as they await cleanup info**
Until this past weekend, Kenny MacLean was living in a house so infested with mould his eyes were burning and he was getting headaches. During the Thanksgiving Day storm, overland flooding coming in through ground-level windows filled the finished basement of MacLean's Sydney Mines, N.S., home with more than half a metre of water. Yet he left the damage largely untouched for almost six weeks... MacLean - who does not have homeowner's insurance - had been calling the Cape Breton Regional Municipality's flood helpline and the Emergency Management Organization office in Halifax, but was getting conflicting advice... MacLean finally turned to the Cape Breton Flood Facebook page for help. New Waterford resident Neil Rideout created the page on the day of the storm as a way to share photos, but it has since developed into a platform for connecting flood victims with help... In an emailed statement an EMO official said "the disaster financial assistance claim does not interfere with your cleanup," meaning an application for disaster relief should not hold up the cleanup process. The statement also said "it is important to ensure your safety from any contaminated materials." CBC News

*** Flood victims to finally have homes**
More than half the residents who were flooded out of their homes in Lake St. Martin First Nation more than five years ago should be able to move to a new home in a new community within a year. Indigenous and Northern Affairs Canada issued a tender earlier this month to build 150 new homes on the reserve's new land, located adjacent to the community destroyed by flooding in May 2011. The tender was to have closed Tuesday but was extended by a week-and-a-half after a meeting with more than 20 interested companies. The winning bid should be determined before the end of December and construction will be timed for completion next fall... The process of rebuilding the community has been fraught with problems, including mismanagement of the program by the Manitoba Association of Native Firefighters, which gave up control of the evacuee program in June 2013. The Canadian Red Cross took over. An audit of the INAC program overseeing the evacuations and rebuilding, dubbed Operation Return Home, found the whole program was poorly resourced, plagued with delays and very disorganized. Winnipeg Free Press, 3

*** LaSalle residents offered last chance to provide feedback on flooding plan**
LaSalle is hosting an information meeting for residents of the Heritage Estates and Oliver Farms neighbourhoods to provide information on a proposed plan to prevent future flooding in those areas. The meeting on Dec. 1 will be a final opportunity to provide feedback on plans to install a pond in Heritage Park, along with storm system improvements in Oliver Farms. Conceptual drawings will outline the options being considered. Postmedia Network (Windsor Star)

*** Inondations à Brigham: identifier les causes et les solutions**
L'Institut national de recherche scientifique (INRS) se penche sur ces questions à la demande du ministère de la Sécurité publique. L'organisme devrait remettre un rapport l'été prochain. L'administration municipale a hâte de s'y référer. « On s'attend à avoir un rapport qui va nous donner un portrait précis de la situation », indique Me Jean-François Grandmont, directeur général de la municipalité. « Quand on a des inondations, des fois, nos véhicules d'urgence ne peuvent même pas se rendre sur place. On ne peut pas continuer comme ça. C'est un gros problème pour nos citoyens. Ils sont exaspérés. » L'INRS, explique Me Grandmont, étudiera la récurrence des inondations et estimera les dommages causés. Ces données aideront le ministère à décider si les résidents touchés pourront se prévaloir d'un programme de rachat de leur propriété. La Presse; La Voix de l'Est

*** Get ready for lots of storms this winter with plenty of snow, ice and freezing rain**
It's coming and it's not going to be pretty. The winter outlook for Atlantic Canada is calling for a lot of messy weather. The Weather Network has released its winter forecast for December, January and February. It's calling for an active season with plenty of storms and above-normal precipitation levels including snow, ice pellets, freezing rain and rain. Daily Gleaner, A3

*** Lobster season around the corner**

Wharves all along the south shore are piled high with lobster fishing gear and boats are at the ready for dumping day and the start of the commercial lobster fishery on Monday, Nov. 28 in Lobster Fishing Areas (LFA) 33 and 34... A full compliment of resources will be on standby on the water and in the air for the season start, said Sean Arbour, search and recue coordinator at the Joint Rescue Coordination Centre (JRCC) in Halifax. "The three lifeboat stations at West Port, Clark's Harbour and Sambro will have the cutters on the water in position about 20 to 30 miles out on stand-by," said Arbour. "Offshore we will have two large vessels on-site tasked to search and rescue. Typically, one is stationed off Yarmouth and the other one stationed off Liverpool about two hours off." From their positions, they will be reporting weather and sea conditions "so we are in the know," said Arbour. The vessels will be on standby most of the day, said Arbour. On land at the lifeboat stations, extra crews for the zodiacs will be on standby. As for air resources, a cormorant helicopter will de deployed to the Yarmouth airport, said Arbour, where it be fueled up and the crew suited up. A Hercules airplane will also be "tasked and deployed" patrolling up and down the coast. Chronicle Herald, S26

*** Chris Metallic search continues 4 years after disappearance**

New searches for a Mount Allison University student who disappeared four years area will be taking place in the coming days. Chris Metallic was reported missing on Nov. 25, 2012, after a party at a residence in Sackville. Sackville RCMP say the new searches by police officers are being organized in an effort to get more information that could help find Metallic. "We continue to receive information about the disappearance of Chris Metallic," Sgt. Paul Gagné said. CBC News (2016-11-22); Guardian; Times & Transcript

*** Body of missing Trail, B.C., senior found - Ida Cragnolini had dementia and had gone missing in the past**

The body of a 70-year-old woman with dementia has been found. Ida Cragnolini went missing in Trail B.C. on Sunday, according to the RCMP. RCMP, search and rescue teams and members of the public had been searching for Cragnolini after she left her residence near the Waneta Plaza shopping mall Sunday morning. She was last seen around 4 p.m. PT in the east Trail area. Her body was located before noon on Tuesday in the Miral Heights area not far from where she was last spotted, according to a family friend. CBC News (2016-11-22)

*** Everything counts in Yarmouth search and rescue exercise**

Search and rescue teams from the tri-counties were combing local shores on Nov. 19 during a training exercise. The scenario was that a collision had occurred between a fishing boat and a pleasure craft stolen from the Chebogue River Aquatic Club. The fishing boat, with three people aboard, was taking on water. The whereabouts of the stolen vessel were unknown. Searchers were tasked with scouring the shores from Comeau's Hill to Chebogue Point for survivors or objects that could be from the collision. Shelburne County Coast Guard (2016-11-22)

*** Government right to tighten waste rules**

An opinion piece by Jim Emberger, a spokesman for the New Brunswik Anti-Shale Gas Alliance, states, "We applaud the Gallant government's decision to amend the Clean Environment Act to ban the disposal of fracking waste water in municipal and provincial sewage treatment systems. The scientific studies behind the decision have long noted that municipal waste water systems were not designed to deal with industrial waste. They cannot remove substances for which they were not designed and the plants themselves can be damaged. Fracking waste water added an overwhelming new set of problems stemming from the large numbers of fracking chemicals used, and the variety of naturally occurring toxic substances brought up from the earth by fracking... No one really knows how well-contained the waste is at hundreds of different sites, or how long it will stay contained, or how far it could migrate. But the main problem is that high-pressure pumping of billions of litres of liquid, containing lubricants among other things, can cause geologic faults to move, thus causing earthquakes. These earthquakes have been documented in B.C., Alberta, and widely in the U.S.A., where the state of Oklahoma has gone from having almost no earthquake activity to becoming one of the earthquake capitals of the world, and the evidence points to waste water injection. This deep injection well method of waste water disposal is currently not allowed in New Brunswick, but remains the "best practice" for the industry, illustrating the

uselessness of that term... A study from Alberta this week tied earthquakes more closely to the fracking process itself (not waste water injection as discussed above.)..." Telegraph Journal, A9

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Rendu malade par le pot, il menace Trudeau**
Favorable à la légalisation du cannabis, le premier ministre Justin Trudeau a été victime de menaces de mort d'un jeune Montréalais en proie à des troubles psychiatriques aggravés par la marijuana, cet été. «La drogue, je ne veux plus en prendre», a dit ce dernier devant un tribunal après avoir été déclaré criminellement nonresponsable de ces délits, puis enfermé dans un hôpital du-rant deux mois. Selon une décision récente de la Commission d'examen des troubles mentaux, le Montréalais, dont l'identité n'a pas été rendue publique, a acheminé un courriel au bureau du premier ministre, le 10 juin dernier. «Je te jure, Justin, je commence à m'entraîner pour te tuer si tu ne fais rien pour mon cas», a-t-il écrit dans un message confus. Sans réponse, il a ensuite téléphoné au bureau de M. Trudeau et réitéré ses menaces avant d'être arrêté par la GRC. Le Journal de Montréal, 15

*** Youth charged over alleged terror...**
A youth arrested Thursday in Yellowknife faces a charge of making a hoax terrorism threat, RCMP stated in a news release. The youth, who cannot be identified, lives in the territory. An investigation started Nov. 1 that included the RCMP's Integrated National Security Enforcement Team in Alberta determined the threat was a hoax. It's unclear what the hoax allegation involves and RCMP aren't elaborating. "The rest of the information will come out in the court process," RCMP spokesperson Marie York-Condon stated in an e-mail. The youth's next court date was not known. Yellowknifer

*** Government surveillance overshadows free speech for Canadian journalists**
Mass surveillance causes reporters to avoid writing or speaking about some topics, according to a recent survey of journalists by Ryerson's Centre for Free Expression (CFE). "Journalists and writers are society's eyes and ears and [when] they feel they have to self-censor because of government surveillance, then we as a public lose," CFE director James Turk said. Twenty-two per cent of respondents to the CFE survey said they deliberately avoided writing or speaking about certain topics and 15 per cent said they seriously considered doing so. Nine per cent of respondents said they had chosen not to cover or write about a protest, demonstration or controversial political event because of mass surveillance. Twenty per cent of respondents said they refrained from conducting internet searches or visiting certain websites. Another 17 per cent said they thought about doing that because of surveillance. The survey, published Nov. 14, was prepared by Turk. A total of 129 Canadian writers and journalists volunteered to complete the survey between May 27 and June 20. The federal government is currently consulting Canadians about the state's security apparatus by holding hearings to solicit public opinion. Turk is "very pessimistic" about the prospect of the Trudeau government limiting surveillance, despite the federal Liberal Party campaigning on a promise to reform Bill C-51, a security bill passed in 2015 that expands security powers. The Eyeopener

Big Brother sleeps easy
An opinion piece states, "The revelation that Montreal police secretly monitored several journalists' smartphones for months, ostensibly in hopes of discovering the source of internal information leaks, has brought home for many people the troubling reality of government snooping. The fact that thousands of students recently lined up to watch whistleblower Edward Snowden at a video conference at McGill University is another sign of the public's growing concern about respect for the right to privacy. Indeed, it is not just journalists who are targeted by electronic surveillance. Revelations about the National Security Agency (NSA) in the United States also touch Canadians, since in the age of the Internet and social

networks, telecommunications knows no borders. It is reasonable to imagine that practically all our communications could be intercepted, filtered and recorded by governments. This is now the world in which we live. Thanks to Snowden's revelations, Canadians know our federal government is actively helping the United States with surveillance programs of its own. For example, it was revealed in April that the RCMP had decrypted about one million private messages from BlackBerry smartphones. In addition, we know that the number of communications intercepted in Canada grew by a factor of 26 in 2015, without the authorities giving any reasons. This opacity is at the heart of the problem: "Big Brother" is completely lacking in transparency. A Federal Court ruling revealed recently that the Canadian Security Intelligence Service (CSIS) had acted illegally by conserving personal data for 10 years. It is alarming to discover just how unclear the limits imposed on surveillance agencies and police forces are. It is probably this lack of clarity that allowed Montreal's police force and the provincial Sûreté du Québec to put so many journalists under watch for such specious reasons." National Post, A11

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Border agency touts drug, gun seizures

Loaded guns, stolen vehicles, child pornography, weed, booze and tobacco are all things that have been seized by the Canadian Border Services Agency in Atlantic Canada in the last quarter. The agency processed about three million travellers at its 50 service locations in the Atlantic region from April to October 2016. Details of its activities were released Tuesday. On Oct. 3, border officials at the the St. Stephen 3rd Bridge port of entry in New Brunswick searched a motorhome and found four tasers, five pepper spray canisters, a loaded 9mm handgun and a loaded .357 Magnum, which are prohibited weapons in Canada. A traveller got $2,300 in fines after pleading guilty the next day to failing to report weapons and providing untrue statements under the Customs Act. "It is important that anyone travelling to Canada understand that undeclared and prohibited firearms are not allowed in our country," said Calvin Christiansen, CBSA director general for the Atlantic region said in a news release. "We welcome our United States neighbours but remind them to leave their guns at home." On their way to inspect a vessel with three foreign nationals arriving in Shelburne, CBSA officials received a tip that a number of bags containing wine, rum, tobacco and marijuana were found in the woods in the region. Officers were able to determine that the bags belonged to the individuals on the vessel, and each traveller was charged with three offences under the Customs Act: non-report of alcohol, tobacco and marijuana; making false statements; and smuggling. They each pled guilty to non-reporting. Fines of $2,500 (for the captain), $1,000, and $500 were charged to the travellers. Total seizures from the hidden bags and boat totalled 39.9 litres of alcohol, 0.79 kg of tobacco and 17.46 grams of marijuana. CBSA officers, along with members of the Internet Child Exploitation unit of the Integrated Halifax Regional Police/RCMP Criminal Investigation Division unit, discovered child pornography on an electronic device belonging to a crew member while searching a vessel Aug. 16. Chronicle-Herald, A4

*** Visa denial to Serbs has created 'negative picture of Canada' says Serbian foreign minister**

Too many Serbs are being wrongly caught up in a visa rule intended to keep human rights abusers out of Canada, says Ivica Dačić. By backing Canada's bid to secure a temporary seat on the United Nations Security Council, and finalizing a bilateral travel agreement to establish a direct air link between Toronto and Belgrade, Serbia views itself as extending a hand in friendship toward Canada. But now Serbia would like to see some reciprocity, as the country's foreign minister made clear during a visit to Ottawa last week. The Balkan country, which Canada bombed in 1999 during the NATO mission in support of ethnic Albanians in the then-Serbian province of Kosovo, would ideally like the federal government to lift the visa requirement for Serbs seeking to enter Canada. (Canadians can visit Serbia without a visa.) But first, Serbia wants Canada to stop denying visas to Serbs perceived to have been associated with the regime of former Serbian president Slobodan Milošević. The current Serbian government estimates that almost one in 10 (nine per cent) of its citizens are prevented from entering Canada based on section 35 (1) (b) of the Immigration and Refugee Protection Act (IRPA), which designates someone inadmissible if that individual was a senior official in a government considered to have been involved, or still involved, in "terrorism, systematic or gross human rights violations, or genocide, a war crime or a crime against humanity." Hill Times

First Lumber, Now Drywall as Canada-U.S. Trade Tensions Escalate
A new trade dispute has broken out between Canada and the U.S. that threatens to raise prices in Canada's already overheated housing markets. The Canada Border Services Agency imposed a provisional tariff as high as 277 percent on U.S. drywall imports in September after ruling that manufacturers were dumping the product, or selling it below the price in their home market, undercutting local suppliers. The tariff has raised the price of drywall, or gypsum board as it's also called, by as much as 30 percent and is causing "chaos" and delays as contractors scramble for alternative sources. Some builders say the tariff could add as much as C$13,000 ($9,671) to the cost of a new home, which would amount to a C$2.6 billion increase to the roughly 200,000 homes built in Canada each year. Bloomberg

À Vancouver, de l'héroïne contient un sédatif pour éléphants
Santé Canada a confirmé que quelques grammes d'héroïne saisis par la police lors d'une arrestation le 20 septembre à Vancouver contient du carfentanil, un sédatif longtemps utilisé pour tranquilliser les éléphants. La police a découvert cet opiacé toxique lors de la fouille d'un suspect qui avait été aperçu muni d'une arme à feu dans une ruelle du quartier Downtown Eastside. Il s'agit de la première présence confirmée de carfentanil à Vancouver. Le carfentanil est 100 fois plus puissant que le fentanyl, une drogue responsable de nombreuses surdoses en Colombie-Britannique et qui se propage vite au Canada. Selon la police, il suffit de 20 microgrammes, soit moins d'un grain de sel, pour tuer un humain. La drogue est moins chère et plus facile à obtenir que d'autres stupéfiants. Radio-Canada

Guenther: Canada's beef export sector waiting, watching
As speculation swirls around U.S. President-elect Donald Trump's promise to renegotiate NAFTA, officials with Canada's beef industry are taking a measured approach. They're not ignoring the possibility of trade disruptions in the U.S., said Ryder Lee, CEO of the Saskatchewan Cattlemen's Association — "but neither are we lighting our hair on fire yet at each proposal you catch wind of." Lee expects to hear plenty of proposals between now and the Jan. 20 inauguration, and even through the next year. "And a lot of the things we'll hear now are kind of spitballs. They're waiting to see what sticks and what doesn't." (…) But while Canada's beef industry supplies other markets, the U.S. remains an important trading partner. "A lot of the time it's our home market that's most important," Lee said. "And the U.S., we can service it fresh and on a truck. So those two are always the biggest ones." Canadian Cattleman

*** Morneau open to trade talks with Trump**
Canada's finance minister says the federal government will work in a "collaborative" manner with the incoming U.S. administration, which has pledged to scrap or heavily amend the North American Free Trade Agreement. Finance Minister Bill Morneau said Tuesday the Liberals "look forward to working with the new administration in the United States." "Our goal, of course, is to work on the behalf of Canadians to present the issues that are important to us in our discussions with all of our international partners," Morneau told a gathering of the Federation of Canada Municipalities in Ottawa. "And that's something we will continue to do." The Nov. 8 election of controversial candidate Donald Trump has thrown into question the continued existence of the 22-year-old NAFTA, or what shape a new trade agreement would take under the presidentelect. Trump also campaigned on a promise to pull out of the 12-nation Trans-Pacific Partnership, of which Canada, the U.S. and Mexico are partners. TPP was agreed to early this year, but still requires ratification by signatories to the pact, which was expected to expand bilateral trade with many key Asian markets - including Japan, Indonesia, Malaysia and Singapore. StarPhoenix, C5 (London Free Press, Kingston Whig-Standard, Windsor Star, Leader-Post)

*** Hire Canadians first for new infrastructure jobs**
The federal government has embarked on an ambitious infrastructure program to stimulate the national economy, and has also announced plans to revamp the temporary foreign worker program that may allow companies to bring in offshore workers. Finance Minister Bill Morneau has further announced the formation of an infrastructure bank to try to secure private financing for a portion of the billions of dollars needed to build everything from bridges and roads to rail and port improvements. To attract that private-sector investment, the minister's advisers are also telling us that Canadians need to embrace the idea of user fees and tolls, just as we see in the Lower Mainland with the Golden Ears and Port Mann bridges. (…) He is advising Morneau that companies need more temporary foreign workers. Although we still await the details of how many workers and in what sectors the Liberals would import workers, there is no doubt

that temporary foreign worker quotas may be raised. The trade unions in Canada represent more than 400,000 highly skilled workers. In B.C., we represent more than 35,000 of Canada's mostly highly skilled construction workers and we have serious qualms about Barton's advice and how the government will interpret it for the construction sector. Province; L'Acadie Nouvelle

*** Disruptions loom at Ojibway Parkway intersection: Overpass to link it with Howe plaza**
One of the city's busiest intersections and a primary route for commuters from LaSalle and Amherstburg is about to face disruptions again for up to two years. Lane closures are planned for a section of Ojibway Parkway, just west of E.C. Row Expressway, during construction of a new multilane overpass that will link the Herb Gray Parkway to the Canadian plaza of the Gordie Howe International Bridge. The work is expected to begin in a few months. This is the second time in two years the intersection will be disrupted because of construction involving the new border crossing. Ojibway Parkway and E.C. Row Expressway in 2015 was under repair for nearly a year due to the Herb Gray Parkway construction. Up to 25,000 vehicles travel through the intersection each day. "It should start late spring, then you are looking at a two-year project," said Dennis Regan, senior project manager for Ontario's transportation ministry which will oversee the project. Two separate bridges to carry traffic in both directions will have a total of eight lanes rising above Ojibway Parkway. Windsor Star, A4

*** 21 proches tués en quelques heures : Une étudiante syrienne réfugiée à Sherbrooke vit dans l'angoisse**
Une étudiante est arrivée en larmes, lundi, au Centre d'éducation populaire de l'Estrie parce que 21 membres de «sa famille» avaient été tués dans les frappes aériennes en Syrie. La réfugiée syrienne de 28 ans, qui est arrivée au Canada il y a huit mois avec son mari et ses enfants, est reconnaissante d'être aujourd'hui installée en pays de paix, mais vit dans une inquiétude permanente pour tous ses proches laissés derrière. A 3 h, dans la nuit de dimanche à lundi, Rinam, un nom fictif, a appris que son oncle, sa femme et ses enfants étaient décédés tout comme le frère de son mari et son fils. Du même coup, elle apprenait que les trois générations d'une famille, des voisins qu'elle considère comme des membres de sa famille, étaient tombées sous les bombes. (…) Rinam est originaire d'Ar-Raqqah, une ville syrienne située à environ deux heures d'Alep. Il y a environ quatre ans, Rinam, son mari et leurs trois enfants quittaient la Syrie pour se rendre dans un camp de réfugiés au Liban, un trajet de 12 h en autobus qui les éloignerait de la guerre. Au cours des trois années qu'elle a vécues dans ce camp de réfugiés, Rinam a mis au monde deux enfants. Mais peu de temps avant de recevoir son laissez-passer pour le Canada, le plus jeune est décédé à l'âge d'un mois. Tribune, 4

*** How you can use tech to score the best deals**
Bargain hunters use online tools to wade through all the salesand decipher the best offers: With Canadian retailers trying to keep people shopping on this side of the border on Black Friday, the best deal might come from the soft warm glow of your computer, tablet or phone screen. Even if you're out and about, there are plenty of ways to use technology to make sure you are actually getting a deal. Do your research: Most of the big retailers already have their flyers out, and plenty of sites are compiling them so you can decide if it's worth heading out or just clicking away at home. Flipp is an app that collects all your local flyers and lets you search them. Redflagdeals.com also has a Black Friday section, but its forums are one place that hardcore deal hunters share their tips year round. Toronto Star, B1

A vulnerable person
A letter to the editor states, "I've been following with incredulity the story of Fliss Cramman and how, until Immigration Minister John McCallum intervened at the eleventh hour, Canada Border Services agents were about to deport the unfortunate woman to Britain because her papers were not in order. Neither she, nor her parents on her behalf when she was a child, had ever thought to take out Canadian citizenship, despite her having resided in this country for 25 years, since the age of eight. If this stress weren't enough following major surgery, she was was shackled to her hospital bed and a guard posted on her door. How somebody hooked up to an intravenous machine in a recovery room could be considered a flight risk is quite beyond me. It took a direct order from Nova Scotia Justice Minister Diana Whalen for the shackles to be removed. Thankfully, due mainly to the efforts of the Elizabeth Fry Society and Ms. Cramman's lawyer, good sense prevailed and the threat of deportation was lifted on this mother of four

children. But that doesn't explain how this situation was allowed to develop to the point it did before John McCallum picked up a pen and ticked the appropriate box." Chronicle Herald, A9

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Online voting deserves a try
An opinion piece states, "If there's any place that would use new technology to drive local democracy, you'd think it would be Waterloo. Once voted the smartest city in the world, it is respected and celebrated as one of Canada's most thriving high-tech hubs. So, when faced with dismally low turnouts in local municipal elections, you might expect Waterloo's civic leaders to leap at the chance to employ online voting to increase voter participation. Unfortunately, you'd be wrong to do so. On Monday, city councillors rejected trying something new and chose to stick with traditional paper ballots… Waterloo councillors were spooked by the possibility hackers could break into the electronic voting system. They worried it would be hard to prove such a vote was free of fraud and that, if a problem arose, it would be impossible to do a recount." Record, A6

LAW ENFORCEMENT / APPLICATION DE LA LOI

Late Mountie honoured at YMCA Peace Breakfast
Peace was everything Lisa Gallagher's late husband fought for. Gallagher, addressing the annual YMCA Peace Breakfast on Tuesday morning, spoke to an audience of Metro Moncton politicians and volunteers about the legacy of her husband, former Codiac RCMP Sgt. Mark Gallagher, and what he taught her. Mark Gallagher died in Haiti in January 2010 when a devastating earthquake hit the country. He died the same day he arrived in the Caribbean nation to serve a six-month stint with a UN mission that was training a national police force. The retired RCMP member had spent the holiday season with his wife and two kids, but felt he still had more to give, and wanted to return to Haiti. "It was only that morning he was leaving, I realized what a brave man he had become," Lisa Gallagher said of her husband of 31 years. During her talk, Gallagher spoke at length about the idea that peace comes from respecting each person and understanding that they have value. Daily Gleaner, B3 (Times & Transcript)

*** Moncton woman sentenced for kicking Mountie in head**
A Moncton woman will spend the next 18 months on probation after assaulting police officers and saying Justin Bourque should have shot more of them. Lia Olivia Chase, whose adoptive father is a retired Mountie, was in court for sentencing on six charges, including two counts of assaulting police, resisting arrest, uttering death threats and two counts of breaching an undertaking by consuming alcohol. Judge Irwin Lampert ordered her to take anger-management counselling, avoid drugs and alcohol, do 30 hours of community service and write a letter of apology to Codiac Regional RCMP. "I would only describe your behaviour as disgusting and disgraceful," said the judge. "To say that about the RCMP, after what's happened in this community in the last couple of years? And your father is a retired RCMP member?" Chase made no comment to the court when given the chance during her sentencing. The prosecutor told the court the incident occurred on Sept. 19, 2015 in Moncton. Her partner called police after a domestic incident, saying she was assaulting him and tearing up the apartment. When they arrived he said she was gone and he didn't want to pursue the matter. Police learned the woman was "wandering the streets intoxicated" and set out to find her. They heard she was hiding in Victoria Park but she fled when they approached. She fell and they found her lying on the ground, barefoot and crying. Times & Transcript, A6

*** Investigators examining death of man in Prince George jail**
An investigation has been launched into the death of a man found unresponsive in a jail cell in Prince George. RCMP say officers responded Sunday night to reports of an intoxicated man causing a disturbance. He was arrested and taken to the police detachment, where he was placed into a cell. RCMP say the unidentified man was found unresponsive during a check at about 2 a.m. Monday and that emergency crews were called. Paramedics took over resuscitation efforts but the man was pronounced

dead shortly before 3 a.m. The Independent Investigations Office is now looking into the case in an effort to determine whether there is a connection between police actions and the man's death. Vancouver Sun

* **Ex-RCMP recruiter charged with sex assault**
A Winnipeg woman has filed a lawsuit alleging a former RCMP recruiter sexually assaulted her in his home. Court records confirm former Const. Michael Adam Timmer, 34, has been criminally charged with one count of sexual exploitation in connection with the alleged August 2014 incident. According to a statement of claim filed last week, the then-17-year-old female met Timmer at a career fair in January 2014. A month later, Timmer - whose image was used on RCMP recruitment posters, the lawsuit alleges - invited the teen to apply to attend a RCMP youth camp in Regina, where Timmer was to act as a chaperone. The teen attended the youth camp the following August. Within days of returning home, Timmer texted her and the two made arrangements to meet for coffee. As the coffee date ended, Timmer kissed the teen "without her invitation or consent," the lawsuit alleges. Later that week, Timmer invited the teen to a party at his house. "Upon her arrival , it became apparent to (her) that no one else had been invited," says the lawsuit. Timmer then led the teen to his bedroom where he sexually assaulted her, the lawsuit alleges. The lawsuit also names the RCMP as a defendant, alleging the police service breached its position of trust by exposing the woman to "sexual conduct and harm" and took no steps to uncover the alleged abuse. "The RCMP in particular, in placing Timmer in charge of recruits and displaying him on the poster for recruiting as an inducement to the public, had a duty to investigate his character and personality and failed to do such," the lawsuit alleges. Winnipeg Sun, A5

* **Surrey's top cop concerned by ages of suspected shooters**
The officer in charge of the Surrey RCMP says he's troubled that nine young people have been arrested in connection with a shootout in south Surrey. "To say anything other than the fact that they are youths would probably be saying too much," said Chief Supt. Dwayne McDonald. "I don't want to risk identifying them but youths involved in crimes such as that is definitely a concern for me and for the Surrey RCMP and for the city of Surrey." Several shots were fired in a hotel parking lot early Monday morning near King George Boulevard and 11th Avenue. One person was cut by broken glass but no one was seriously hurt. McDonald says he's heard false reports about the accused. "It was reported that some of the youths or many of the youths involved in yesterday's incident were part of our Wrap Program and that is not the case," he said. CBC News

* **Crime on decline in Surrey**
Surrey's new top cop wants to change the perception that his expanding city is a hotbed of crime. "I believe, having lived and worked in Surrey for a number of years, the perception of crime in Surrey tends to be that crime is high," Chief Supt. Dwayne McDonald said Tuesday during a keynote address at a Surrey Board of Trade luncheon. "That's something that I want to address as an officer in charge." McDonald, appointed officer in charge of Surrey's RCMP detachment last month, pointed to the recently released third-quarter crime statistics as one reason for optimism. "We have work to do, but I'm pleased by the results," he said. According to the latest police statistics, there's been a 13 per cent decrease in violent crime, a slight decrease in property crime, a 38 per cent decrease in robberies, a 21 per cent drop in business break-and-enters, and a 17 per cent curtailment in incidences of theft under $5,000. Residential break-and-enters are up, however, and McDonald said that's an area police need to target. Province, A12 (Vancouver Sun)

* **Surrey police deny suspects were part of Wrap program**
Surrey police deny that any suspects in a shooting Monday were participants in an anti-gang program for youth. On Monday, Kash Heed, a retired police officer and former B.C. MLA who served as minister of public safety and solicitor general, said a source had informed him that of the nine people arrested following a shootout in the parking lot of the Pacific Inn Resort and Conference Centre, five were students in Surrey schools and a person alleged to have had a gun was in Grade 8. Heed said three of the accused were involved in the Wraparound (Wrap) Program, a Surrey RCMP and school district initiative that works with at-risk youth to help them stay out of gangs and the criminal lifestyle. But following a keynote address Tuesday at the Surrey Board of Trade, Surrey RCMP Chief Supt. Dwayne Mc-Donald told reporters that none of the suspects was involved in Wrap. "It was a bit disappointing," Mc-Donald said. "It was factually inaccurate yesterday. It was reported that some of the youth or many of the youth

involved in yesterday's incident were part of our Wrap program, and that is not the case. I won't get into too many details on that other than to say that that's inaccurate." As many as 20 shots were fired between two vehicles on Monday and one person was treated for minor injuries. Vancouver Sun, A11

*** Police bust fentanyl lab in city's S.W**

Two men have been charged after police busted a fentanyl powder reprocessing lab. Calgary police evacuated an apartment building in the 0-100 block of Westpark Link S.W. last week after officers found signs of the lab. Police initially entered the building on a search warrant for what was believed to be a heroin trafficking investigation. The RCMP Clandestine Laboratory Enforcement and Response Team was brought in to identify and remove the substances found in the residence. No one was injured as a result of the investigation. Police found 11 grams of methamphetamine, more than 26 gram of power cocaine, 65 grams of crack cocaine, 263 grams of fentanyl powder and 645 fentanyl pills as part of the search. Calgary Sun, A19

*** Alarm raised on fentanyl after overdose death**

A Nova Scotia woman is raising awareness after her 21-year-old granddaughter's fentanyl overdose. Charly Ann Torikka, a young mother and Maple Ridge, B.C., resident, was found dead in bed by her boyfriend on Nov. 6. An autopsy report revealed fentanyl-laced cocaine was in her system, and her father used the media to warn others in B.C. about the drug. Now, the girl's grandmother, Lynda Koile, is doing the same on the East Coast. (…) RCMP spokeswoman Cpl. Jennifer Clarke said the department now has a supply of Naloxone, a drug that reverses or blocks the effects of opioids. "(It) is being distributed to employees across the province in stages. The first to receive the Naloxone kits are the employees who are the most likely to come into contact with it, then to those employees who are at a lower risk of contact," she wrote in a late October email. "We are actively rolling them out to the rest of the division." Chronicle-Herald, A1

*** Investigation into child's death delayed**

A police investigation into the death of a four-year-old girl who died in care is waiting on paperwork, said an RCMP spokesman Tuesday. "There are different agencies involved here," said Sgt. Jack Poitras of Edmonton's K Division. "Investigators are waiting for reports to come in." He said he couldn't release further information on what the reports are and doesn't know the timeline for the investigation. Serenity died on Sept. 27, 2014, while in kinship care, being looked after by family members. Her death prompted a review of the case by Alberta's child and youth advocate, who found that no workers had checked on Serenity or her two older half-siblings in almost a year before she died, despite reports she was unwell, malnourished and bruised. Medical records obtained by Postmedia showed Serenity weighed 18 pounds when she died. She was suffering from hypothermia and had multiple bruises, including around her genitals, when she arrived at hospital. Her hymen was gone. The Alberta medical examiner's report on her death was completed almost two years after her death before being given to the RCMP, who asked that the report not be released. Poitras said the autopsy report will be withheld until the investigation is concluded. He added that due to the different agencies involved with children in care, it isn't uncommon for investigations to be delayed. Edmonton Sun, A9 (Calgary Herald, Edmonton Journal)

*** Athol man arrested on child pornography charges**

A 24-year-old Athol man has been charged with offences allegedly related to child pornography. The RCMP's Provincial Internet Child Exploitation Unit has charged Darryl Wayne Baxter with luring a child and six counts of breach of conditions. On Nov. 18, police searched a home in Athol and arrested Baxter at the scene without incident. He was held in custody pending an appearance in Amherst Provincial Court Tuesday. Chronicle-Herald, A5

*** Search for Chris Metallic continues four years later**

Four years after a 20-year-old man was reported missing, Sackville RCMP continue to investigate the disappearance of Chris Metallic, and police officers will conduct new searches in the Sackville area in the coming days in hopes of getting more information that could help find him. Metallic was reported missing on Nov. 25, 2012, following a party at a residence in Sackville. A few days after his disappearance, footwear belonging to him was located off the Haute-Aboujagane Road. We continue to receive

information about the disappearance of Chris Metallic. By conducting these new searches we will be following up on some of that information in order to see if it provides any more information about what happened to Chris. Sgt. Paul Gagné. Metallic is described as aboriginal, measuring six feet tall, and weighing about 180 pounds at the time of his disappearance. He has short, dark, black hair and was last seen wearing a shiny bright blue sweater and jeans. "We continue to receive information about the disappearance of Chris Metallic," says Sgt. Paul Gagné with the Sackville RCMP. "By conducting these new searches we will be following up on some of that information in order to see if it provides any more information about what happened to Chris." Times & Transcript, A8 (Guardian)

*** Claims of attacker in clown mask could lead to charges in Port Hardy**

Port Hardy RCMP are preparing to bring mischief charges against a 19-year-old man suspected of clowning around with the law. The move follows a month-long investigation of a reported October assault where the man said he had been set upon by someone wearing a clown mask. Police allege the report was false and misled the detachment. The incident mirrors the "creepy clown" phenomenon in Canada and the United States that has seen people dress up as clowns to scare or surprise others. Victoria police had an experience with the phenomenon when a man possibly disguised with a clown mask was arrested in October for a burglary at Frank White's Dive Store. Port Hardy RCMP Cpl. Stuart Foster said every report received by the detachment is taken seriously. "Investigations such as these, where there are no witnesses and [they] allege a violent offence, are especially difficult and time-consuming to investigate," Foster said in a statement. He said specialized RCMP units were brought to Port Hardy to help investigators. "It is not only a waste of resources, it is a criminal offence and one for which we will seek charges," Foster said. Times Colonist

Jury Hears Of Suspected

An ex-girlfriend of an accused gangster boss killer told an Edmonton jury Tuesday she saw her boyfriend give a suspected gun to one of his drug thugs a few days before the killing. Testifying at the first-degree murder trial of Josh Petrin, Karissa Dow, 24, told jurors she dated Petrin from 2010 to November 2012 culminating in the birth of their daughter following his arrest. 'Patched' member Dow testified that Petrin, 33, revealed to her that he was a "patched" member and a "boss" with the "drug-dealing" White Boy Posse street gang and said he has a WBP tattoo on his arm. (…) Under cross-examination, Dow told defence lawyer Markham Silver that she never saw Petrin hand anything to Halbauer and agreed she does not know what he might have given him. She also agreed that drugs were sometimes stashed in the same places where guns were. Dow also said in crossexamination that she was pressured to speak with the RCMP and told jurors that one Mountie threatened to have her jailed and to have her newborn baby taken away. She clarified to Rudiak that the officer told her after Petrin's arrest that they could take away her child. She also said the officer told her friends she was going to deliver the baby while in jail. She added her daughter was never taken away and she was never charged. Postmedia Network (Edmonton Sun, A5, Edmonton Journal)

*** Denecho King murder case moves to preliminary inquiry**

A preliminary hearing for a man charged with second degree murder and attempted murder began Monday, almost two years after police found two men seriously injured in a downtown apartment building. John Wifladt, 39, succumbed to his injuries while Colin Digness, who is in his early 40s, was medevaced to Edmonton for further medical treatment. Denecho Noel Calvin King, 24, was charged with second degree murder and attempted murder months after police responded to the early morning incident Dec. 14, 2014, at the Sunridge Place apartment building on 51A Avenue. Eleven days have been set aside for NWT Territorial Court Judge Robert Gorin to hear evidence in the case and to decide whether it is strong enough to proceed to trial on the charges police announced against King on May 1, 2015. The Crown may call up to 40 people to testify, defence lawyer Jay Bran has previously said. Crown prosecutor Alex Godfrey was expected on Tuesday to call paramedics who transported the two men to hospital as the hearing continued. A publication ban was imposed on testimony and exhibits, such as photos of items in the apartment. The ban means little can be reported about what occurred. The preliminary inquiry began with testimony from five RCMP officers Monday in Courtroom 4, one of the smallest courtrooms in the building. There was added security, with two RCMP officers keeping watch. A third RCMP officer in a suit watched from the gallery as evidence was given. King also faces a charge in connection with an escape from the North Slave Correctional Centre on Aug. 10. King, wearing grey sweatpants, a white T-shirt with

a graphic print, remained in leg shackles during the hearing as he sat beside his lawyer. He listened without any obvious reaction to the testimony of five RCMP officers, slumping in his chair as the hearing wore on through Monday afternoon. The public gallery remained largely empty on the first day of the hearing. Yellowknifer

*** Sask. community up in arms over RCMP carbine training**

Drew Erickson thought he knew what he was getting into when he built his home in Stone Pointe Estates in 2011. Stone Pointe is an up-scale neighbourhood located east of Regina. The community has about sixty-five homes, many valued at more than a million dollars. For the last two summers, it has also had some very noisy neighbours. Across the road is the Regina Wildlife Federation and its gun range. At first, Erickson's family heard what they expected: small caliber fire and the odd shotgun. That all changed one summer morning in 2015. "We awoke, about a quarter after seven, to what sounded like automatic rifle fire, very loud, rapid succession." According to the Regina Police Service which uses the same weapon, C8 Carbines are noisier than typical rifles or shotguns because the projectile travels faster than the speed of sound. The gun fire could be heard in Emerald Park and White City two kilometres away. Erickson, who lives just a few hundred metres away, says it's like living in a war zone. He said the gunfire woke his wife, who is from South Africa, and sent her into a panic. "When she heard that noise when she was a kid, that meant somebody nearby was in peril," Erickson explained. It's not just his wife either. When the matter was brought before the RM by Erickson and a group of concerned community members, it was mentioned some members of the group had immigrated to Canada from a war-torn country. Erickson said a man and his wife heard the gunfire on their first day in the community. "She effectively thought she was back in a war zone," he said. "This is not why they came to Canada. This is not why they came to live in a rural community." Erickson says closing doors and windows does little good. He says the RCMP needs to find another range, away from the community. "Our community is at the point where we've done our time, we've taken our turn, this is two summers in a row, and if it's a third it's unnaceptable." CBC News

Accused UN killer tells undercover cop he dreamed about his arrest

Cory Vallee, a United Nations gang member and accused killer, had a dream he was going to be arrested the day before Mexican police raided his Guadalajara house and took him into custody. Vallee described the dream to an undercover cop posing as a criminal and planted in the accused killer's cell at the Richmond RCMP detachment on Aug. 17, 2014. A secretly recorded video of the conversation was played for B.C. Supreme Court Justice Janice Dillon at Vallee's murder trial Tuesday. "I started packing the day before I got arrested because I had a dream that I got arrested. I swear to God," Vallee said to the cop, whose identity is shielded by a court order. "I had a dream that someone was coming in my house and I woke up and thought I saw a shadow and they were trying to arrest me. It was like a nightmare." He said he started packing all his clothes, books and DVDs the same day. So when police arrived and shouted his name the following day, "everything was in boxes." Replied the undercover cop: "That is f-king trippy." The jail cell conversation took place about 2:40 a.m. after Vallee had been escorted back to Canada by two other RCMP officers. Vallee met the undercover cops at Vancouver airport when they were all placed in the same Canada Border Services Agency holding cell early on Aug. 17. He also said that going to jail won't be so bad, since he had already cut offall contact with family and friends years earlier when he went on the run. Vancouver Sun, A11, 1

*** De la colère à l'action**

Un article d'opinion note, « S'il veut faire toute la lumière sur les violences subies par les femmes autochtones, le gouvernement Couillard doit commencer par ouvrir les yeux. Depuis une semaine, son plan d'action se résume ainsi : se cacher derrière la commission d'enquête fédérale, et ne pas faire grand-chose en même temps. M. Couillard a d'abord proposé une vague « table de concertation ». Mais avant de lancer cette idée, il aurait dû consulter les communautés touchées. Acculé au mur, il accepte maintenant de le faire. Il a parlé hier avec le chef de l'Assemblée des Premières Nations du Québec et du Labrador, et d'autres entretiens sont prévus dans les prochains jours. La pression augmente pour déclencher une enquête judiciaire québécoise sur les relations entre les femmes autochtones et les policiers (violences sexuelles, abus de pouvoir et autres formes de discrimination). Québec refuse de bouger, en invoquant que le fédéral fait déjà ce travail avec la nouvelle commission d'enquête lancée sur les femmes autochtones tuées et disparues. Cette excuse ne convainc pas. Certes, la commission fédérale se penchera entre autres sur le Québec, et son mandat inclut maintenant les violences

sexuelles. Mais le Canada est un vaste pays, et le temps de la commission sera limité. Le gouvernement Couillard pourrait rétorquer que la commission pourra compléter cet examen, car les causes sont en partie déjà connues. Mais si c'est le cas, cela signifie qu'on les connaît aussi déjà assez pour trouver des solutions ! Or, Québec n'a encore rien proposé pour mieux former les policiers et protéger les femmes. Le refus de Québec aurait également été plus crédible si les policiers étaient eux aussi prêts à agir. Mais contrairement à la Gendarmerie royale du Canada, la Sûreté du Québec (SQ) refuse de reconnaître la discrimination envers les autochtones. » La Presse, 2

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Dog daycare gives B.C. prison inmates a second chance**

By all accounts, Chilko and Riley are well behaved and haven't been convicted of any crimes, yet every day they end up behind the razor wire and heavily fortified walls of a federal prison. Chilko, a border collie-cross, and Riley, a golden retriever, are part of of a program called The Doghouse, a dog daycare and kennel inside a women's prison in Abbotsford, B.C., where inmates look after dogs while their owners are away at work. (…) More than 150 women prisoners have worked in the Doghouse program in the decade since the Langley Animal Protection Society (LAPS) partnered with Corrections Canada on the project. The latter provides the space and facilities, but staff say the program is otherwise revenue neutral. LAPS handles day-to-day operations, and pet owners pay $18 a day — cheaper than the going rate at many private facilities. (…) The Nova Institution for Women in Truro is the only other federal women's prison with a dog program, though the focus there is on training assistance dogs. The women's prison in Edmonton is also planning a program that teaches prisoners dog-grooming skills. Catherine Latimer, executive director of the national John Howard Society, says she's a firm believer in the power of animal therapy for prisoners. "Dogs have a remarkably strong impact on people," Latimer says, and they can help foster "soft skills" such as being in a trusting relationship. "Being exposed to a situation where prisoners learn empathy is important." CBC News

Shooting victim was trying to turn his life around after time in prison

Tyler Keizer had been trying to turn his life around after a history of violence and criminal activity, when he was shot dead Monday night. According to parole documents, the 22-year-old man had been in prison since his teenage years, had dropped out of school after Grade 10 and had links to organized crime. Keizer landed in prison after he was convicted of robbery and possession of prohibited substances. (…) Keizer was sentenced to two years and nine months in prison, but within six months of being incarcerated was involved in a stabbing at the Springhill Institution that left another offender with punctures to his lung. That attack, according to parole board documents, was suspected to have been a result of the victim owing money to an organized crime group. Keizer was eventually convicted of assault as a result of the attack and had a year added to his sentence. Keizer was then sent to the Atlantic Institution, a maximum security prison in Renous, N.B. (…) But at his most recent parole hearing on Aug. 30, Keizer seemed to be going straight. (…) As a result, the board granted him a one chance statutory release with strict conditions. Less than three months later, he was killed in Halifax's 12th homicide of the year. CBC News

Un nouveau pardon pour Bernard «Rambo» Gauthier

Bernard «Rambo» Gauthier est de nouveau «pardonné». La Commission des libérations conditionnelles, qui avait révoqué le pardon du leader syndical au printemps, revient sur sa décision, a appris Le Soleil. «La logique vient de tomber», a réagi le principal intéressé, qui venait d'apprendre la nouvelle. En avril, le syndicaliste de la Côte-Nord s'était vu retirer son pardon, octroyé en 2007 pour des gestes posés il y a 18 ans, parce qu'il avait «cessé de bien [se] conduire», avait fait valoir la Commission en raison de ses récents démêlés avec la justice. La décision a rapidement été contestée devant l'instance fédérale par le local 791 de l'Union des opérateurs de machinerie lourde, dont Bernard Gauthier est le représentant. «On a eu la permission d'en appeler, explique-t-il. Ça prouvait selon moi que c'était un peu abusif, que ça n'avait comme pas de bon sens.» Dans ses conclusions initiales, la Commission s'appuyait sur des événements «qui avaient nécessité l'intervention du système de justice», notamment lorsque M. Gauthier a été reconnu coupable en décembre 2014 d'intimidation sur un chantier de construction, une condamnation pour laquelle il a ensuite été absous conditionnellement. Le Soleil, 20

*** Demande d'appel refusée pour Jean-Paul Néashish**
Reconnu coupable de plusieurs chefs d'accusation de nature sexuelle et condamné à six ans de prison, l'ancien chef de police de la communauté atikamekw de Wemotaci, Jean-Paul Néashish, souhaitait aller en appel du verdict de culpabilité rendu en première instance. Toutefois, l'accusé a été débouté devant la Cour d'appel du Québec. Les requêtes ont été entendues, lundi. On demandait une prolongation du délai d'appel, la permission d'en appeler du verdict de culpabilité du 9 décembre 2015 et la remise en liberté de Jean-Paul Néashish durant les procédures. «J'en viens à la conclusion que le requérant n'a pas fait preuve de diligence en attendant, sans raison valable, près d'un an avant de se pourvoir en appel. Les moyens qu'il invoque ne sont pas, non plus, sérieux», a écrit le juge de la Cour d'appel Jean Bouchard avant de rejeter les requêtes. Le Nouvelliste, 5

Suspect wanted for robbing woman at gunpoint
Police are asking for the public's help to find a Red Deer man after he allegedly robbed a woman at gunpoint in West Park on Remembrance Day. Michael Wayne Lamontagne, 47, is wanted on Alberta-wide warrants. (…) He is also wanted on a Canada-wide warrant for violating his parole. Police ask residents not to approach Lamontagne because he may have a weapon. Red Deer Advocate, A3

*** Federal inmate convicted of armed robbery testifies against alleged partner in crime**
A federal prison inmate convicted of a brazen armed robbery earlier this year testified against his alleged partner in crime in a Saint John court testifying against his alleged partner in crime. Mark Lejeune's shackles clinked as he shuffled his way to the witness stand Monday morning. He says Matthew Paul Martin, who's pleaded not guilty to a total of five offences, formulated the plan to rob Alan Roy's west side home with him, and it was Martin who followed him inside the home, sword in hand, after he booted in the rear door on the morning of May 7. Lejeune, who has a shaved head and a thick, salt and pepper ducktail beard, admitted to the robbery shortly after his arrest. He's now serving a five-year prison sentence, incarcerated at Springhill Institution in Nova Scotia. Presented on the witness stand with the sawed off 16-gauge shotgun he says he used during the robbery, Lejeune's back stiffened and his eyes darted down and away from the firearm. "It was mine and I modified it," said Lejeune, recognizing the weapon, "and I don't really care to look at it, what was going on what could have happened." Telegraph Journal, B3

*** Killer denied unescorted visits to Sudbury**
A convicted killer of a husband and wife won't be coming to a Sudbury halfway house for a limited number of unescorted visits, after the Parole Board of Canada ruled against his request. George Harding Lovie, 58, had applied for six unescorted temporary absences – each lasting 72 hours – over a period of a year. Lovie has served 25 years of his life sentence for the brutal murders of Donna and Arnold Edwards on March 21, 1991. He was also convicted of attempted murder of their daughter, Michelle, with whom he had a brief relationship. (…) The family is opposed to any release program for Lovie, who is being housed at the Beaver Creek Institution, a minimum security prison near Gravenhurst. Sudbury.com (2016-11-22)

Solitary conditions 'unacceptable': Ontario
Ontario's Corrections Minister has appealed to the Premier for new prison spending and dispatched a 25-member team to examine conditions in segregation cells across the province as part of a response to revelations about the use of solitary confinement in provincial institutions. David Orazietti divulged the new steps during a sit-down interview that came on the heels of a series of Globe and Mail articles focusing on the plight of a young aboriginal inmate at Thunder Bay Jail. Adam Capay, 24, has spent over four years in solitary confinement awaiting trial, much of it inside an acrylic-glass-lined cell with 24-hour artificial light. (…) The minister said there are currently "under 20" inmates in Ontario whose elapsed time in solitary confinement tops one year. That's well above the 15-day maximum guideline set out by the United Nations General Assembly's Mandela Rules. Outgoing federal Correctional Investigator Howard Sapers has said the cap in Canada should be 30 consecutive days - with an absolute prohibition on the segregation of inmates with serious mental-health issues. Globe and Mail, A1

*** A smarter approach**
An editorial states, "The parents of Fouad Nayel will not likely see justice done in the case of their son, who was found murdered in Ottawa four years ago. Adam Picard, who had been charged with Nayel's

killing, was allowed to walk free last week after a Superior Court judge ruled that long delays in the case had violated the right of the accused "to be tried within a reasonable time." It's the latest reminder that the crisis in court delays in Ontario and across the country is a threat not only to timely justice but also to public safety. (…) On this last front, a valuable model has emerged from Nova Scotia - one that ought to spur a national rethinking of how to be smart, not just tough, on crime. The province announced this week that its restorative justice pilot project will be made permanent and province-wide this month, the first program of its kind in Canada. Restorative justice emphasizes the importance of offenders taking responsibility for their actions, addressing root causes, offering support to victims and helping to undo the damage their crimes caused in the community. Initial government studies suggest such programs have the potential to save huge sums of money by averting long trials and incarceration, to modestly decrease recidivism and to help address racial inequities in the justice system." Toronto Star, A18

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

City, cops clash on carding

City council sent a clear, precedent-setting message to London police Tuesday: end street checks now. The only hitch? Chief John Pare and the board overseeing city police don ' t have to listen to them, and probably won ' t. But in a symbolic, emotionally charged vote, Coun. Mo Salih and Mayor Matt Brown led council to unanimously back a citizen group ' s request that Brown urge police to end a practice critics call racially biased. It's believed London is the first municipal government in Ontario to make such a request of its local police. "We have heard this is an important tool for the police to use, to help them solve crimes. But there are many tools they could use," Coun. Maureen Cassidy said, citing tapping everyone's phone or emails as examples. (…) London police statistics from 2014 showed officers collected information from a disproportionate number of black and indigenous citizens compared with white people. Pare downplayed the conflict over carding. "We all have a voice ," he said. "It's (about) working together and resolving those issues." London Free Press, A1

End of program puts public at risk

Criminal trial lawyers in Alberta are worried the public could be at risk if a treatment program for sex offenders is shut down. The Criminal Trial Lawyers Association in Edmonton and the Criminal Defence Lawyers Association in Calgary say they've been told the Alberta government will end the Phoenix program by next March. The program is offered in a secure, 19-bed facility operated out of Alberta Hospital Edmonton and provides intensive therapy to convicted sex offenders serving provincial jail sentences. Ian Savage with the Calgary lawyers association said the treatment involves 35 hours of therapy a week, while a potential replacement program operated by Alberta Health Services would offer six hours. "It's essentially world-renowned and quite successful, particularly with the numbers that matter. The recidivism rate is extremely low compared to other similar programs," said Savage. The lawyers say the program has reported recidivism rates as low as 3.3 per cent in 120 offenders who received treatment and were tracked over a three-year period. Red Deer Advocate, A9; * Postmedia Network (Edmonton Sun, Edmonton Journal); * Calgary Herald (2016-11-23); * CBC News; * Global News (2016-11-22)

* Unions won't back down

Leaders of two of the three civic unions whose contracts expire this year say they won't be intimidated by the city's 2017 budget during bargaining. Gord Delbridge, president of CUPE 500 - the city's largest union - and Moe Sabourin, president of the Winnipeg Police Association, said the city's budget for 2017 will have no affect on how they bargain on behalf of their members. (…) Sabourin said he's troubled to see the police budget is increasing only 1.3 per cent, adding it's not a realistic target. "Calls for service are continuing to skyrocket (35 per cent increase since 2007)," Sabourin said. "Criminals don't take into account inflation rates when they're planning to do their crimes. We're definitely concerned this is going to cause a decrease in service to the citizens of Winnipeg." Sabourin said the fentanyl epidemic, which is blamed for several drug overdose deaths in Winnipeg recently, is already straining police operations. "The time we have to take, the precautions we have to take... The job becomes that much more dangerous, that much more complex," he said. "The time constraints required by the members to respond to these calls has increased, which will cause an increase in costs. A one per cent increase (in the police

budget) definitely has me concerned." Bowman said there's no chance he'll support more funds for police. Bowman said the funds set aside in the 2017 budget for police had been proposed by the police board. Winnipeg Free Press, B1

*** Nelson police request $253,000 budget increase for 2017**
The Nelson Police Department is asking for an increase of $253,000 for 2017, which would bring its total budget to $3,178,291. Police Chief Paul Burkart presented the figures to city council on Monday on behalf of the Nelson Police Board. The board is required to provide a provisional budget in November of each year in anticipation of council's budget deliberations in the spring. The increase will cover the cost of two new employees — one officer and one civilian support person — whom the department recently hired after being ordered to do so by the provincial director of police services in March. Burkart said the two positions will cost about $180,000 in 2017 and the remainder of the requested increase would go toward anticipated costs resulting from a new collective agreement, which is still being negotiated with the city. The police department has been without a contract since 2012. Nelson Star (2016-11-22)

*** Fentanyl scourge seen up close in DTES alleyway**
It's not quite noon, and three people have overdosed after using drugs at an unsanctioned injection site set up inside a filthy alleyway, in Vancouver's Downtown Eastside. Next to a fixing table, under a portable canopy, a thin, middle-aged woman pitches forward and then slumps back in a chair. She has almost certainly injected herself with fentanyl, enough to kill her. She is today's alleyway overdose No. 4. There will be many more. (...)It is everywhere. It's why B.C. declared a state of public health emergency in April, why federal and provincial politicians met in Ottawa last weekend to discuss a national fentanyl strategy, why activists and volunteers are throwing together "pop up" injection sites in the DTES. (...)Drug dealers mill around the Insite entrance. Chances are, everything they sell contains fentanyl. Postmedia Network (Vancouver Sun, N3, Montreal Gazette, StarPhoenix, Ottawa Citizen, London Free Press, Kingston Whig-Standard, Windsor Star, Leader-Post, Calgary Herald, National Post, Edmonton Journal)

Drug users warned about carfentanil
Vancouver police are warning drug users to be cautious following the seizure of an opioid that is used to tranquillize elephants and believed to be 100 times more powerful than fentanyl. Police said two samples of a drug seized in September have been confirmed by Health Canada to contain trace amounts of carfentanil. The drug was believed to be heroin when it was confiscated from a man reported to be carrying a firearm in the city's Downtown Eastside, police said. "It's the first time we've seen it in Vancouver in any of the seizures we've done," Sgt. Brian Montague said Tuesday. The drug has been seen elsewhere in Canada, including Alberta, Manitoba and Ontario. Vancouver police don't know where the carfentanil came from, though fentanyl is believed to be exported from China, Montague said. Times Colonist, A5; * Radio-Canada; * Postmedia Network (The Province, Vancouver Sun)

*** At least two dozen dead from opioids this year: Goertzen**
Manitoba has recorded "at least" two dozen deaths from opioid overdoses in 2016 - nine confirmed to be caused by or related to fentanyl, Health Minister Kelvin Goertzen told the legislature Tuesday afternoon. The confirmed deaths occurred in the first five months of 2016, Goertzen said. "This number is expected to go up," he said. "Sadly, we know as the toxicology reports come back from other overdose cases, this number will almost certainly be higher than in previous years." Goertzen dismissed demands from NDP health critic Matt Wiebe to declare a provincial public health emergency and to open up safe injection sites for addicts. He did, however, agree the situation is an emergency. "Many (users) are unaware it is the drug they are taking, and of its deadly consequences," he said, adding the problem does not recognize provincial borders. "We need national action on this issue," he said. "It is not a problem that can be legislated away." Winnipeg Free Press, B2 (2016-11-23); CBC News (2016-11-22)

*** Fentanyl crisis requires B.C. pill press ban, NDP MLA says**
After 14 overdoses in Vancouver's Downtown Eastside on Sunday night, an NDP MLA is renewing his call for strict regulation of pill presses that can be used to manufacture fentanyl pills. Mike Farnworth is the MLA for Port Coquitlam and the NDP's public safety critic, and over the summer, he tabled a bill modelled after one in Alberta that would limit pill press ownership to pharmacists. However, the government cancelled the fall session, which means the legislature won't see the bill again until January.

"Right now, there are companies in this province selling those machines and they know exactly the purpose they are being used for," Farnworth told *On The Coast* host Stephen Quinn. "These businesses and these individuals are profiting from the overdose crisis. They are profiting from the deaths of people in this province." Farnworth said it was "unacceptable" that pill presses are still available in B.C. to anyone who can afford one. CBC News (2016-11-22)

*** More overdoses as fentanyl epidemic grows in Penticton**
The suspected overdose death of a 43-year-old Penticton woman Monday at the Black Forest Motel was just another in what is believed to be the growing, fentanyl-related epidemic locally. It was one of at least two overdoses that day. The second was in the early evening at a Government Street residence. However the male victim survived after being given two doses of the opiate antidote Narcan and taken to Penticton Regional Hospital. "We're seeing more than usual. I can't say for sure but I'd say we've had 13 overdoses and one death (Monday) in the last two weeks," said Cpl. Don Wrigglesworth of the Penticton RCMP. "We'll see in a week or a month what we normally see in a year, in fact it's daily, it's a huge problem." Penticton Western News (2016-11-22)

*** A path to healing**
An editorial states, "Rev. Anthony Bailey of Parkdale United Church believes in forgiveness - and that includes the 17-year-old youth who is charged with painting racist graffiti on his church last week. "It has to do with an understanding (of) our Christian teaching around loving neighbour, loving enemy, reaching out in love," Bailey says. So he's among those who suggest we depart from traditional justice - charge someone, hold a trial, send them to jail - and think more about constructive ways of dealing with some crimes. The youth in this particular case, who cannot be named because of his age, faces 20 charges related to the racist and anti-Semitic graffiti spray-painted on Ottawa churches, mosques and synagogues recently. Several charges are related to past breaches of the Youth Criminal Justice Act; he was on probation for assault, robbery and bail violations. Bailey and some others believe an approach known as "restorative justice" should be at least considered. Under restorative models, the accused meets with victims or members of the affected community to repay the harm done and understand the true consequences of his or her actions. Restorative justice can proceed in parallel to charges, be part of sentencing, or, in some cases, lead to charges being stayed or dropped. " Ottawa Citizen, A6

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Aboriginals seek inquiry into alleged abuse by police**
Premier Philippe Couillard has promised to meet with indigenous leaders to discuss ways to investigate alleged "systemic racism" in Quebec. "We're aware of the enormous trauma in aboriginal communities, we're not trivializing it ... we'll find concrete ways to bring some answers," the premier said. Couillard made the remarks Tuesday at the National Assembly, where a dozen women stood wearing small, red felt dresses pinned to their shirts, reminiscent of the red square worn by student protesters in 2012. They said the red dress symbolizes the murdered and missing aboriginal women. The Couillard government has suggested that Canada's national inquiry into missing or murdered indigenous women is a sufficient vehicle for examining alleged abuse of aboriginal women by police forces. But on Tuesday, aboriginal women argued Quebec's problems will be lost in a national inquiry. Montreal Gazette, A10; Le Devoir; TVA Nouvelles; La Presse Canadienne (L'actualité, Radio-Canada); La Presse; Huffington Post Québec

*** Elsipogtog hoops player takes a knee in support of missing and murdered aboriginal women**
Quentin Sock has some personal experience with the issue of missing and murdered aboriginal women and girls. The 30-year-old student athlete at St. Thomas University, a member of the Elsipogtog First Nation, and the men's basketball team at the school, was one of the organizers of an awareness campaign/protest at the Tommies' Atlantic Collegiate Athletic Association basketball home game against the University of Kings College Blue Devils earlier this month in Fredericton. Before the playing of the national anthem prior to the game, the entire Tommies team quietly took a knee. Sock and team co-captain Jeremy Speller, a native of the Gesgapeplag First Nation in Quebec, bowed their heads and

raised a red shawl, a symbol of the plight of missing and murdered aboriginal women across the country. They did so with the blessing of the university president, Dawn Russell, and the university community. Literature handed out with the program, quoting the Native Women's Association of Canada and the Government of Canada, noted that 16 per cent of all women murdered in Canada between 1980 and 2012 were of aboriginal descent and notes that, "the RCMP has identified that there may be 1,181 missing and murdered Aboriginal women and girls." Times & Transcript, D3

* **Anti-violence campaign to begin Friday**
A coffee house, panel discussions, the Take Back The Night march and a family day are all part of the list of events on tap for this year's 12 Days to End Violence Against Women campaign. Set for Nov. 25 to Dec. 6, the annual campaign that's organized by a variety of local groups aims to draw attention to the issue of violence against women. Panelists will include Patricia Bacon, a human sexuality expert and executive director at the Blood Ties Four Directions Centre; Mark Rutledge, a White Ribbon Yukon member and father; and Sara Tillett, a counsellor at Golden Horn Elementary School. That will be the first of two panel discussions included in the campaign's schedule. The other one will focus on missing and murdered indigenous women in Canada and is scheduled for noon on Dec. 5 at Yukon College. Whitehorse Daily Star, 5

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Pour ou contre la légalisation de la marijuana?
C'est au printemps 2017 que le gouvernement Trudeau déposera son projet de loi pour légaliser la marijuana à des fins récréatives. D'ici le 30 novembre, le Groupe de travail sur la réglementation et la légalisation de la marijuana, présidé par Anne McLellan, déposera ses recommandations au gouvernement. Plus de 30 000 commentaires ont été émis depuis le début des consultations, dont 500 de différentes organisations. Pour ou contre la légalisation de la marijuana? Les partisans (Line Beauchesne, professeure de criminologie à l'Université d'Ottawa, et Philippe Hurteau, chercheur à l'Institut de recherche et d'informations socio-économiques) en débattent avec les opposants (Jean-Pierre Chiasson, médecin spécialisé en toxicomanie et fondateur de la Clinique Nouveau Départ, et Claude Carignan, leader de l'opposition officielle au Sénat). Radio-Canada (2016-11-22)

PUBLIC SERVICE / FONCTION PUBLIQUE

Shared Services fiasco reveals federal sprawl
An editorial states, "hared Services Canada was supposed to do the following: Collapse 63 email systems into one; decommission more than 500 data centres, replacing them with a mere handful; upgrade 50 telecommunications centres connecting 3,500 federal buildings. And do this with staff pulled from 43 different departments, running 14,000 software applications. What could possibly go wrong? In a special report, journalist James Bagnall has offered a meticulous examination of exactly what did, from the time Shared Services appointed its first president in 2011 to the present day, as it staggers under project delays, financial challenges and general mistrust across government. As significant as the Phoenix pay system scandal is, the Shared Services challenge dwarfs it. As Bagnall points out, several concrete problems have undermined the task of Shared Services: It was born in secrecy - through an administrative services review conducted on the QT by the Privy Council Office. From the start, people who could have offered additional depth and expertise were shaded out. As a result, many experts feel the initial business case was flawed or incomplete." Kingston Whig-Standard, A4

OTHER / AUTRE

NIL

INTERNATIONAL

*** 2 attack plotters arrested in France may have visited Syria**

French officials say that two suspects - one a school employee - arrested in an alleged attack plot on France apparently travelled briefly to Syria. An official said Wednesday that two others among the seven suspects arrested over the weekend have been freed. Interior Minister Bernard Cazeneuve said on Monday that the arrests in Strasbourg and Marseille culminated a six-month investigation that thwarted an attack. Two officials close to the investigation said that two of the four people arrested in Strasbourg had travelled to Cyprus as if on a vacation, then apparently made a quick trip to Syria. One, identified as Yassine B., 38, worked in a Strasbourg school. The officials spoke on condition of anonymity because they were not authorized to speak publicly on the case. Associated Press (The Telegraph)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
December 8, 2016 / le 8 décembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

*** Welcome to the capital, outgoing Vice-President Biden!**
On the eve of his second pre-holiday First Ministers Meeting, Justin Trudeau is set to host an "official dinner" for visiting US Vice-President Joe Biden, who is scheduled to arrive in Ottawa later this afternoon in advance of what the draft itineraries provided to media suggest will be an event-packed day in the capital on Friday. Before lifting his glass to toast the outgoing Veep, however, the prime minister will hold a pre-summit meeting with Yukon Premier Sandy Silver, who will stop by his Centre Block office this morning. For those keeping track, the PMO-issued advisory indicates that Trudeau also intends to be in his seat for Question Period. Meanwhile, Public Safety Minister Ralph Goodale and Canadian Security Intelligence Service director Michel Coulombe will field questions from Public Safety committee members on a recent federal court ruling that found the agency failed to properly advise the court on its data retention policies, which the court views as a "breach of candour." MPs will also spend an hour quizzing

Goodale, Coulombe, RCMP Commissioner Bob Paulson and other officials on the latest requests for add-on budget boosts included in the most recent supplementary estimates. Ottawa Citizen

Biden's visit to Ottawa could damage Canada-U.S. relations, Tory MPs warn
Outgoing Vice-President's presence in the capital a little more than a month before Mr. Trump takes over the White House is seen as an effort to "calm the waters," one MP says. U.S. Vice-President Joe Biden's visit to Ottawa this week is intended to reassure the public that the bond between the two countries is strong, but Canada's Conservative opposition warns the trip could sabotage the country's relationship with the incoming Trump administration. Mr. Biden will be celebrated at an official dinner in Ottawa on Thursday, and on Friday will meet with Prime Minister Justin Trudeau and the country's premiers already in town to discuss climate change at a first ministers' meeting. (…) "We look forward to him perhaps sharing his perspectives in this time of transition," Transport Minister Marc Garneau told reporters. "I'm sure that we'll have an opportunity to speak to him and ask him some questions, so it, I think, is going to be very valuable for Canada." **Public Safety Minister Ralph Goodale** said there are always important cross-border issues for Canada and the United States to discuss. ***"So keeping that relationship in very good shape, whether it's at the beginning of a new administration or at the end of a departing administration, all of that is high on the agenda for Canada,"*** he said. Globe and Mail

Trump's view on torture may change secrets sharing, spy watchdog executive says
The civil servant in charge of the government's spy-watchdog agency says Canada may have to reconsider how it shares intelligence with the United States if president-elect Donald Trump makes good on his promise to torture terrorists to gather intelligence. The federal official also remarked that had former U.S. intelligence analyst Edward Snowden worked for Canadian intelligence and leaked secrets, "he should be shot," but quickly backed off the opinion. Michael Doucet, the executive director of the Security Intelligence Review Committee, made the off-the-cuff remarks to a small audience in Toronto last week. An audio recording of his talk was provided to The Globe and Mail by a student journalist from the Eyeopener, a campus newspaper at Ryerson University, which was the venue for the talk. For 11/2 hours, the former intelligence analyst held forth on intelligence issues. Members of SIRC rarely make unscripted or unguarded remarks publicly because they are sworn to secrecy about their work reviewing the highly classified spying operations of the Canadian Security Intelligence Service. (…) During his talk, Mr. Doucet highlighted that **Public Safety Minister Ralph Goodale** recently called SIRC ***a "whistle-blower"*** agency. That followed a Federal Court ruling this fall, when judges responding to a SIRC report accused CSIS officials of "breaching their duty of candour" in their applications for surveillance warrants by not revealing what they do with the data. One broad theme of Mr. Doucet's talk was that CSIS and its foreign counterparts are veering far from their roots of building cases with intelligence from informants by increasingly using technological surveillance instead. Globe and Mail, A1

*** Liberals' Digital Surveillance Proposals Far Scarier Than Bill C-51**
An opinion piece states, "Imagine how you would feel if the government installed cameras in your home that recorded everything you did, then gave police the power to review the footage without a warrant, whenever they want. If that sounds to you like a gross violation of your privacy, you should probably be aware that the federal Liberals are contemplating pretty much exactly that for the digital world. (…) **Public Safety Minister Ralph Goodale** has vowed to remove ***"problematic elements"*** of Bill C-51, but his department's survey suggests it's looking at ways of enhancing the bill instead. (…) What alarms me most about the C-51 review is not the proposals themselves, but how the government appears to be selling them to the public. In short, they want you to agree to these ideas without realizing what you've agreed to. The Public Safety department's survey contains questions that are imprecise, confusingly long and sometimes misleading. Understanding things is essentially what I do for a living, and I had to read these questions three or four times before they started to make some sense, and even then." Huffington Post

TOP STORIES / MANCHETTES

$1B RCMP overtime bill proof of 'exhausted and depressed' members, retirees say
The Royal Canadian Mounted Police (RCMP) has paid its members more than $1 billion of overtime since 2009, according to documents obtained by CBC News. Recent retirees from the force say the costs

confirm anecdotes that many officers are stressed, overworked and depressed. "The rank and file - especially the patrol guys and girls - are burnt out," said Derek Snow, a recently retired RCMP member with 29 years of policing experience. "You want to do a good job and you want to do extra," Snow said, who lives in Shediac, N.B. "But there's only so much anybody can take." Between April 2009 and June 2015, the RCMP paid $1.01 billion in overtime, according to documents obtained via access to information requests. (...)Terry McKee advocates for RCMP members and acts as a spokesperson for the Mounted Police Professional Association of Canada (MPPAC). He says the money spent on overtime should instead be used to hire more officers. "You're putting members' health at risk because they're always being called to supplement for shifts that are not staffed properly," McKee said, who is based in Moncton. (...) Contained within the documents obtained by CBC News is the RCMP's response to the work-life balance report. "Human Resources and Corporate Management will benefit from the content of this report and are committed to providing the enhancements needed to improve operational management and oversight. We will also address the concerns outlined in this report, many of which have already been actioned," wrote Dan Dubeau, chief human resources officer. CBC News

Border bill gains traction in U.S. Congress
A bill to simplify crossing the Canada-U.S. border moved ahead in the American Congress on Wednesday, with little time left to get it passed before U.S. lawmakers break to form a post-election legislature in the new year. It's a long-awaited development on both sides of the international border. The Harper and Trudeau governments both signed socalled preclearance deals with the Obama administration, but the arrangement required implementing legislation and U.S. lawmakers have not made it a priority. The bill finally got some attention from Congress on Wednesday evening. It sailed through the House of Representatives without objection. Lawmakers there urged the Senate to adopt it quickly, and make it law before breaking next week for the Christmas-season holidays. Lawmakers from different parties and different parts of the U.S. spoke in favour of the bill, before moving it forward. "[This] is great news for U.S.-Canadian relations," said New York Republican Elise Stefanik. "Canada is more than just a bordering nation. They are our neighbours, our friends and our largest trading partner. Plattsburgh, a city in my district, has even branded itself as Montreal's U.S. suburb." Canadian Press (Times Colonist, A8); Presse canadienne (Voix de l'Est, Métro)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Anxious days: Residents to learn flood disaster aid details during EMO meetings this week**
Anna Mae Muise is filled with many emotions as she prepares to enter a meeting with the province's Emergency Management Organization officials. Muise is one the many Cape Breton victims of record Thanksgiving Day flooding who will be at Cambridge Suites in Sydney today through Saturday to learn the status of financial assistance that could come their way... She's been told that EMO officials will meet with families on a one-on-one basis to go through assessments of damage to their homes, their appraisal of the homes and costs associated with flood damage. Cape Breton Post, A1

*** Mossey River, Man., declares state of emergency after lake ice piles up in river**
A state of emergency has been declared in the Winnipegosis, Man., area because of lake ice that caused river levels in the village to rise to critical levels Tuesday night. Mossey River Municipality declared the state of emergency Tuesday evening due to an "ice event" on the Mossey River, head of council Kate Basford said Wednesday. Winnipegosis, Man., is about 280 kilometres northwest of Winnipeg on the west shore of Lake Winnipegosis. "The wind had pushed the ice off the lake and down the river," she said. "We had never really experienced an ice event where it was piling up." She said in the end, the municipality declared a state of emergency out of an abundance of caution. CBC News

*** Des citoyens interpellent Trudeau**
Des citoyens de Lac-Mégantic et des élus de l'opposition reprochent au premier ministre Justin Trudeau de manquer à son « obligation morale » de construire une voie de contournement. Des représentants de la Coalition des citoyens et organismes engagés pour la sécurité ferroviaire à Lac-Mégantic ont fait le déplacement à Ottawa, mercredi, pour l'exhorter à bouger dans ce dossier. Le porte-parole du regroupement, Robert Bellefleur, a fait remarquer qu'en juillet 2013, peu après le drame ferroviaire, Justin

Trudeau a signé une pétition réclamant la construction d'une voie. La Coalition brandissait d'ailleurs, au bénéfice des journalistes, une grande affiche reproduisant cette pétition avec la signature de M. Trudeau en évidence. Une autre pancarte indiquait le trajet actuel de la voie ferrée au centre-ville de Lac-Mégantic et le tracé suggéré pour la voie de contournement. Mais depuis qu'il a été élu premier ministre, c'est silence radio, a déploré le Méganticois en conférence de presse au parlement, aux côtés d'élus du Parti vert et du Bloc québécois. Tribune, 5; Le Droit; Postmedia Network (Cape Breton Post; Calgary Sun; Times & Transcript)

*** Fort McMurray horse owners getting special delivery of hay**
Horse owners in Fort McMurray are being "baled" out by the Alberta Equestrian Federation. The organization is sending 1,500 bales of hay to the fire-ravaged region of northern Alberta on Dec. 16 to help support owners through the winter after much of their own supply was destroyed. It is hoped the delivery will help alleviate some of the feed costs over the winter months. Horse owners who registered with the federation during the disaster will be able to pick up hay bales Dec. 17 and 18. Postmedia Network (Edmonton Journal)

*** The future of online giving**
The Fort McMurray wildfires spurred the largest collective donation by Canadians toward any single event on the fundraising platform GoFundMe in 2016, says its chief executive, Rob Solomon. That outpouring - 10,200 individual donations to 183 separate campaigns for a total of $1.1-million - is an example of how Canadians' online generosity continues to grow, Solomon says, with an estimated $66 million in donations on the website so far in 2016, up from $55 million in 2015. GoFundMe, which uses crowdfunding to raise money for personal causes such as paying for steep medical bills or supporting a family hit by tragedy, hit US$3 billion in total donations globally in October, roughly six years after it was founded. Postmedia Network (National Post, FP 5)

*** Be prepared for more 'extreme' rainfalls - think biblical floods - U.S. climate scientists warn**
In a research paper that reads like it was written by a horseman of the apocalypse, U.S. climate scientists are predicting more frequent extreme rainfalls, the kind of downpours that cause flooding, landslides and massive infrastructure damage, especially in cities where paved ground cannot absorb water. The same goes for snowstorms and ice storms, according to the team from the National Center for Atmospheric Research, which also found the expected frequency of these "extreme precipitation events" increases five-fold in large parts of Canada and the western United States in the coldest winter months. The effect is dramatically lessened south of the 30th parallel, which runs through Houston, Texas. The reason is simple physics, playing out in the chaos of continental weather patterns. Warm air can hold more moisture than cold air. That is why storms from the Arctic, or the famed Alberta clippers, tend to be windy but dry, while the ones that come up from the southern United States are warm and full of precipitation, and can become ice storms if they run into a cold front. If climate change raises atmospheric temperature by one degree, the air can hold about 12 per cent more moisture. According to the study, this same increase would cause precipitation intensities to increase by about seven per cent. Postmedia Network (National Post)

*** N.L.'s seasonal SAR stations close for the winter**
The Canadian Coast Guard's seasonal search and rescue (SAR) stations in Lark Harbour and Port aux Choix are closed for the winter Wednesday. Vessels from the seasonal SAR stations are unable to operate in the Gulf of St. Lawrence's ice-covered waters. The coast guard uses icebreakers and calls on other local, commercial or recreational vessels for its winter SAR operations in the Gulf when necessary. Aircraft with the Department of National Defence are also used. The seasonal stations resume operations in April. Telgram, A2

*** Feds set to pick new military rescue planes**
One of the longest and most contentious defence procurements in Canadian history will inch closer to conclusion today when the federal government announces a replacement for the military's ancient search-and-rescue planes. The decision comes 14 years after the Chretien government first launched plans to replace the air force's Buffalo and Hercules aircraft, the oldest of which have been flying since the 1960s. What followed was a series of missteps and controversies eerily reminiscent of those that

have plagued the effort to replace Canada's aging CF-18 fighter jet fleet. Public Procurement Minister Judy Foote and Defence Minister Harjit Sajjan will announce the winning bid during an event at Canadian Forces Base Trenton alongside air force commander Lt.-Gen. Mike Hood. Canadian Press (Chronicle Herald, A8; Guardian; Cape Breton Post; Times & Transcript)

*** Side-scan sonar used in search for missing St. Anthony woman**
Just before 3 p.m. Wednesday afternoon, a search and rescue unit of the RCMP began their search of the harbour around St. Anthony. Hillier-Penney has been missing since last Wednesday, when she was seen in the area of her family's home on Husky Drive. Following an extensive investigation, the RCMP now considers the disappearance of St. Anthony resident Jennifer Hillier-Penney to be suspicious. A side-scan sonar boat was brought to the area for the search of the water. Cst. Toby Acreman of the St. Anthony RCMP detachment was onboard the vessel, along with other search and rescue personnel. Telegram, A5; Canadian Press (Cape Breton Post; Calgary Sun; Edmonton Sun; Ottawa Sun; Toronto Sun; Whig-Standard; London Free Press); Labradorian

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Garratts recount dark odyssey through China's security apparatus
The Garratts didn't realize they were being set up until it was too late. It was August, 2014, and the Christian aid workers were at a restaurant in the remote northern Chinese city of Dandong, on the North Korean border, where they had lived and run a café for years. An acquaintance had asked them for advice on sending his daughter to study in Canada - so there they were, prepared to offer assistance, as they had been doing in China since falling in love with the country 30 years before. Shortly after arriving amid what looked like a wedding party, Kevin and Julia Garratt were grabbed by strange men and driven away in separate cars. The surprise arrest launched a dark odyssey through the Chinese state security apparatus: Mr. Garratt was imprisoned for two years on espionage charges, Ms. Garratt was detained, then placed under surveillance, and the family was traumatized, immiserated and finally reunited, with troubling questions to spare. (…) Former foreign affairs minister John Baird requested a meeting during his tenure. And in 2009, the Garratts were contacted by Canadian Security Intelligence Service, the Canadian spy agency, to ensure the couple hadn't violated sanctions through their aid work. (They hadn't.) Ms. Garratt now believes all of the attention from foreign diplomats and security agencies put a bull's eye on their backs. Unbeknownst to them, another drama was playing out, as the United States sought the deportation from Canada of Su Bin, a Chinese man accused of masterminding a plan to steal U.S. military secrets. Diplomatic discussions suggested very strongly the Garratts had been seized in retribution. Globe and Mail, A1/front

Ces Québécois sont secrètement partis combattre en Syrie
Un groupe de jeunes Québécois s'est joint secrètement aux milliers de combattants étrangers en Syrie pour lutter contre le régime de Bachar Al-Assad. Aujourd'hui, ils sont soupçonnés d'avoir commis des actes terroristes. Nous avons découvert qui ils sont. Une enquête de Sonia Desmarais, Chantal Lavigne et Karine Bastien Une dizaine d'amis se retrouvaient régulièrement dans un centre de tir de la région de Montréal pour s'entraîner avant le départ de sept d'entre eux pour le Moyen-Orient entre l'été 2012 et l'été 2013. Les jeunes hommes y apportaient deux armes, selon des témoins. L'une d'elles était une imitation de carabine semi-automatique soviétique appelée SKS, similaire à celle qu'utilisent les rebelles en Syrie. Certains d'entre eux s'y sont exercés durant des mois, de deux à trois fois par semaine. Lors des séances de tir, ils prennent souvent des pauses pour prier. Plusieurs d'entre eux s'étaient convertis à l'islam. Un jour, un client aurait entendu un jeune dire qu'il était malheureux que les cibles ne soient pas des mécréants. Avertis de l'incident, les propriétaires contactent les autorités, qui décident de déclencher une enquête. Les policiers seront à partir de ce moment présents lorsque les jeunes s'exercent et la

Gendarmerie royale du Canada (GRC) met plusieurs d'entre eux sous écoute électronique. Certains sont surveillés de près, parfois jour et nuit. Ces jeunes représentent la première vague de Québécois à avoir quitté le pays pour combattre le dictateur syrien, a appris l'émission *Enquête* en collaboration avec CBC. Certains auraient rejoint l'Armée syrienne libre, des rebelles qui luttent contre Al-Assad et qui collaborent avec des islamistes liés à Al-Qaïda. Radio-Canada; CBC News

*** La menace invisible des revenants**
Le recul du groupe EI renvoie chez eux des jeunes désillusionnés, mais toujours radicalisés. Après avoir répondu à l'appel du groupe armé État islamique (EI), être allée en Syrie, Mali est de retour en France où dans les derniers mois, elle ne rêvait que d'une chose : repartir. " Elle a pourtant connu les pires injustices là-bas, résume à l'autre bout du fil le journaliste français David Thomson, auteur de Les revenants (Seuil), essai percutant dans lequel il détaille ses nombreuses discussions avec de jeunes djihadistes partis en Syrie et en Irak, puis revenus en France. Elle a été emprisonnée, elle s'est fait confisquer ses biens, mais elle continue de légitimer les actes terroristes et voulait rejoindre la branche libyenne de l'organisation, là où, dit-elle, il y a moins de Français qui corrompent l'esprit du djihad avec leur culture des cités. " La disparition de cette branche, cette semaine, dans la foulée de la reprise de la ville de Syrte, en Libye, va la contraindre à changer ses plans. Le recul de l'organisation terroriste donne peut-être des signes d'espoir dans des régions qui subissent depuis des années ces fanatiques obscurantistes, mais elle s'accompagne aussi d'un effet secondaire que plusieurs pays, dont la France, mais également la Suisse, la Belgique ou le Canada, ne peuvent plus ignorer : le retour sur leur territoire de jeunes partis combattre pour le groupe EI et qui reviennent chez eux désillusionnés, certes, mais toujours aussi radicalisés, estime l'essayiste, journaliste à Radio-France international (RFI). L'homme a signé en 2014 Les Français jihadistes (Les Arènes), bouquin dans lequel il relatait déjà ses rencontres avec des jeunes appelés par la guerre sainte, jeunes qu'il a côtoyés de près, après les avoir découverts en Tunisie, au coeur du printemps de 2012. Le Devoir, A1, A8

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Border bill gains traction in U.S. Congress
A bill to simplify crossing the Canada-U.S. border moved ahead in the American Congress on Wednesday, with little time left to get it passed before U.S. lawmakers break to form a post-election legislature in the new year. It's a long-awaited development on both sides of the international border. The Harper and Trudeau governments both signed socalled preclearance deals with the Obama administration, but the arrangement required implementing legislation and U.S. lawmakers have not made it a priority. The bill finally got some attention from Congress on Wednesday evening. It sailed through the House of Representatives without objection. Lawmakers there urged the Senate to adopt it quickly, and make it law before breaking next week for the Christmas-season holidays. Lawmakers from different parties and different parts of the U.S. spoke in favour of the bill, before moving it forward. "[This] is great news for U.S.-Canadian relations," said New York Republican Elise Stefanik. "Canada is more than just a bordering nation. They are our neighbours, our friends and our largest trading partner. Plattsburgh, a city in my district, has even branded itself as Montreal's U.S. suburb." Canadian Press (Times Colonist, A8); Presse canadienne (Voix de l'Est, Métro)

'Visa lift' gives Mexican cartels chance to expand in Canada
Violent drug cartels are expected to expand their reach in Canada now that a visa requirement for Mexicans has been lifted, according to government documents obtained by Postmedia News. The Canada Border Services Agency report says "the visa lift will make travel to Canada easier in order to establish or strengthen existing cartel smuggling chains." "In the next three years, Mexican drug cartels are expected to expand their presence in Canada by sending operatives and recruiting local airport or marine port workers with ties to Mexico," says the document, obtained from a source. The Sun obtained only a section of the document titled: Implications for the Canada Border Services Agency and Canada. Postmedia earlier reported on the increasing presence of Mexican cartels in Canada, as well as the fact that gangsters and organized criminals were working at the Port of Vancouver. As of Dec. 1, Mexicans are no longer required to obtain a visa to come to Canada. The previous visa program had existed for

seven years. The CBSA document said the cartels generally don't use tourists to smuggle drugs for them. Postmedia Network (Vancouver Sun, A1/Front, Calgary Herald, Montreal Gazette)

*** Canadian coalition wants Ottawa to reduce security screening times at borders, airports**
A coalition of business leaders in Canada's largest cities is putting pressure on Ottawa to reduce security screening times and cut travelling costs to bolster a prime engine of the country's economy. In its first political foray, the Canadian Global Cities Council is pushing to make airports more internationally competitive in order to attract more tourists, enhance economic activity and improve the travelling experience. (…) The council is calling for increased funding for CATSA and the Canada Border Services Agency to meet growing demands. It also wants Canada to harmonize immigration and trusted traveller programs with other countries. That means only requiring visas for citizens of high-risk countries and increasing the use of automated border clearance systems. Canadian Press (Global News, CTV News, CP24)

*** Des accusations contre Vaporium et ses administrateurs**
Même si l'entreprise Vaporium n'existe plus, les accusations fédérales contre l'entité ainsi que ses deux anciens administrateurs Sylvain et Christian Longpré se poursuivent. Ces dossiers étaient de retour, mercredi, au palais de justice de Sherbrooke. L'entreprise Vaporium se spécialisait dans la distribution de cigarettes électroniques et la fabrication de liquides aromatisés nécessaires à leur utilisation. Vaporium et son président Sylvain Longpré font face à quatre accusations pénales en vertu de la Loi sur les douanes. Entre le 21 novembre 2013 et le 9 juin 2014, des indications fausses ou trompeuses auraient été fournies lors de l'importation de nicotine liquide au Canada. Sylvain Longpré aurait aussi fait des déclarations trompeuses et tenté d'introduire illégalement de la nicotine liquide au Canada par le poste frontalier de Stanstead. La même accusation d'avoir introduit ou tenté d'introduire illégalement des marchandises passibles de droits ou dont l'importation est prohibée a été portée pour des événements qui se seraient déroulés au poste frontalier d'East Hereford. Christian Langlois, qui était le vice-président de l'entreprise dont la boutique était située aux Galeries 4-Saisons, est accusé de deux chefs en semblable matière. Pour sa part, les gestes reprochés seraient survenus le 6 janvier 2015 au poste frontalier de Stanstead. La Tribune, 7

Ruling on drywall tariff expected in early January
Final arguments started Wednesday in a hearing on whether to continue a controversial drywall tariff one Edmonton contractor says has cost his company almost $35,000. The federal government imposed preliminary anti-dumping tariffs Sept. 8 that now reach up to 324 per cent on gypsum board products imported to Western Canada from the United States following a complaint by manufacturer CertainTeed Gypsum Canada Inc. The Canada Border Services Agency ruled companies were selling the product below the price in their home market, undercutting local suppliers - CertainTeed, with the only drywall plants in the West, has said dumping was making it impossible to compete. But David Lessard, vice-president of Edmonton's DCL Drywall Inc., said the industry wasn't consulted about the tariff, which boosted drywall costs by 30 per cent, including products the company agreed to supply for jobs but hadn't purchased yet. "I can tell you that we have been paying most of that 30-percent increase. There's been small percentages that suppliers have agreed to take, and we had to go to homebuilders to try to pass on some (of it)." The average 200-square-metre bungalow has about 630 square metres of drywall. The price rise will add approximately $600 to the cost of the house, cutting DCL's profit on a typical residential project by as much as half, Lessard said. DCL has 20 full-time workers and employs 60 contractors. Edmonton Journal, A9

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

$1B RCMP overtime bill proof of 'exhausted and depressed' members, retirees say

The Royal Canadian Mounted Police (RCMP) has paid its members more than $1 billion of overtime since 2009, according to documents obtained by CBC News. Recent retirees from the force say the costs confirm anecdotes that many officers are stressed, overworked and depressed. "The rank and file - especially the patrol guys and girls - are burnt out," said Derek Snow, a recently retired RCMP member with 29 years of policing experience. "You want to do a good job and you want to do extra," Snow said, who lives in Shediac, N.B. "But there's only so much anybody can take." Between April 2009 and June 2015, the RCMP paid $1.01 billion in overtime, according to documents obtained via access to information requests. (...)Terry McKee advocates for RCMP members and acts as a spokesperson for the Mounted Police Professional Association of Canada (MPPAC). He says the money spent on overtime should instead be used to hire more officers. "You're putting members' health at risk because they're always being called to supplement for shifts that are not staffed properly," McKee said, who is based in Moncton. (...) Contained within the documents obtained by CBC News is the RCMP's response to the work-life balance report. "Human Resources and Corporate Management will benefit from the content of this report and are committed to providing the enhancements needed to improve operational management and oversight. We will also address the concerns outlined in this report, many of which have already been actioned," wrote Dan Dubeau, chief human resources officer. CBC News

Wall concerned about reports that RCMP staffing in north is in 'dire straits'
Premier Brad Wall says he is concerned about reports of serious RCMP staff shortages in some communities in northern Saskatchewan. Wall was responding to internal RCMP emails obtained by radio station CKOM that indicate some Mountie detachments in the region are operating well below full strength. One memo says they are running out of people and are in "dire straits." RCMP Supt. Kris Vibe says they sometimes operate with fewer officers due to retirements, people being away on leave or training courses and redeployment. He says the RCMP does the best it can with the people they have and that staffing levels are ultimately a provincial and municipal funding responsibility. Wall says with crime rates up his government plans to speak with the RCMP about staffing levels. "The provincial government has as its provincial police force the RCMP - there is a contract between the government on behalf of the people of Saskatchewan and the RCMP," Wall said in Regina on Wednesday. Postmedia Network (Leader-Post, A3, Star Phoenix)

La GRC reporte l'installation des caméras corporelles sur ses agents
Les agents de la Gendarmerie royale du Canada (GRC) ne seront pas munis de caméras vidéo corporelles (CVC). Du moins, pas pour l'instant. La GRC a indiqué qu'elle reportait l'adoption de ces appareils par ses agents après que des tests eurent révélé certains problèmes technologiques, notamment concernant la durée de vie des piles et la durabilité des caméras. Le déploiement des CVC implique l'achat de milliers de dispositifs destinés à plus de 750 détachements, souligne-t-on. La police fédérale veut d'abord être certaine qu'elle peut faire confiance à la technologie choisie, plaide la GRC dans un communiqué. Les dispositifs seront installés, en règle générale, sur l'uniforme des agents de la GRC. Ils pourront par exemple être fixés à des lunettes ou à un casque. Acadie Nouvelle, 14; Canadian Press (The Guardian, Red Deer Advocate, The Telegram, Cape Breton Post, Times Colonist, Globe and Mail, Times & Transcript, Prince George Citizen); * The Register UK

RCMP, securities regulator team up to target repeat financial criminals
The long arm of the law just got a little longer in Alberta thanks to a new unit focusing on white-collar crime. The Alberta Securities Commission, the regulatory agency responsible for administering provincial securities laws, and the RCMP are forming the Joint Serious Offences Team. The unit is to investigate and prosecute cases under Alberta's Securities Act as well as more serious offences that fall under the Criminal Code. A specialized prosecutor will pursue any criminal charges resulting from investigations. The nine-member unit - comprising investigators, forensic accountants, legal professionals and RCMP officers - will target repeat offenders, serious frauds and breaches of court orders and bans. (...) RCMP Insp. Allan Lai said the collaboration will provide more access to information and intelligence collected provincially, as well as through national and international networks. In the end, he said, it will bolster the case for stricter punishment of those found guilty. "It's looking at the recidivists, targeting repeat offenders of the securities act that continue to violate the regulatory process," said Lai. Postmedia Network (Calgary Herald, A3, Times Colonist, Edmonton Journal); Red Deer Advocate (Globe and Mail)

Whistler RCMP to review officer conduct after cellphone seizure complaint
RCMP in Whistler will launch a review after a Vancouver woman filed a complaint, alleging officers seized her cellphone after she used it to film an arrest. The officer in charge of Sea-to-Sky RCMP, said she found - in her initial review of the incident - that parts of the complaint from Valerie Connelly and the corresponding police report were "unclear." "For this reason, I have initiated a comprehensive review of the matter in addition to the public complaint," said Insp. Kara Triance in a statement. Connelly told CBC News she was capturing what she believed to be was an undercover arrest on Saturday, Nov. 19. As Mounties wrapped up the arrest, she says a uniformed officer grabbed the phone out of her hands and said he was taking it for evidence. When she refused to give officers the passcode to her phone, she herself was arrested. CBC News (2016-12-07)

Cops arrest 10 people in organized-crime dragnet
Officers with Alberta Law Enforcement Response Teams (ALERT) have arrested 10 people and laid 111 charges after a year-long investigation into an organized crime group. ALERT began its investigation in November 2015 and wrapped up on Nov. 21 this year with the arrest of 40-yearold Calgary man Timothy Varga, who police allege was the central figure in a criminal network that extended from Alberta to B.C. and had ties to Manitoba. (...) Police say they seized a variety of drugs, including 147 grams of cocaine, 26 grams of heroin, 106 grams of methamphetamine and 1.2 kg of ketamine, in addition to a loaded handgun from the home of Varga, who has a lifetime firearms prohibition from a previous manslaughter conviction. RCMP StaffSgt. Barry McCurdy said the investigation focused primarily on disrupting the group's suspected streetlevel drug sales. The estimated value of the drugs seized was about $115,000. McCurdy said there could be more charges pending. Postmedia Network (Calgary Sun, A5, Calgary Herald)

Police returned abused boy to what looked like 'loving home,' superintendent says
Ottawa police say there was no indication a nine-year-old boy was being abused when officers spoke to him 15 months before his father, a former RCMP officer, and stepmother were arrested. "If hindsight was 20/20 could we have done anything differently? I don't think so," Ottawa police Supt. Don Sweet said Wednesday. Sweet was responding to mounting questions about why officers returned the boy to his father and stepmother after he told police he was being mistreated. The boy first spoke to police in November of 2011. His father had reported the boy missing, and within an hour he was located at a neighbour's house. Sweet said he reviewed the report from the two officers who responded to the missing person's call "from beginning to end." CBC News

Carfentanil seized in Toronto for first time
Police in Toronto say they've made their first confirmed seizure of the deadly drug carfentanil. They said Wednesday in a release that analysis of recently seized substances purported to be heroin tested positive for carfentanil, cocaine and caffeine. Carfentanil is a synthetic opioid that is used to sedate large animals and is not for human consumption. The drug is fatal in small doses and has a potency approximately 10,000 times that of morphine and 100 times that of fentanyl. (...) The Canada Border Services Agency has made three carfentanil seizures in the Pacific region this year and the RCMP announced late last month it had reached an agreement with China aimed at halting the transpacific flow of fentanyl into Canada. The force said Commissioner Bob Paulson and Chen Zhimin, the vice-minister of China's public security ministry, agreed to boost efforts to disrupt the flow of fentanyl and other opioids. Paulson has said opioids pose a grave threat to community safety in Canada. Canadian Press (Hamilton Spectator, A10, Waterloo Region Record, Thunder Bay Chronicle-Journal, Cape Breton Post, Red Deer Advocate); * Agence QMI (Journal de Montréal)

«Les policiers n'accordent aucune valeur aux promesses effectuées»
Si Jean-Claude Savoie a été acquitté des accusations criminelles qui pesaient contre lui, il pourrait bien décider, à son tour, d'emprunter la voie des tribunaux pour obtenir justice. Ses avocats étudient la possibilité de poursuivre la GRC pour certaines fautes commises préalablement au dépôt des accusations contre leur client. C'est qu'en janvier 2014, l'enquêteur principal au dossier à l'époque, le caporal Gabriel Deveau, a contacté Me Leslie Matchim (également avocat de M. Savoie) afin de l'informer de la fin de son enquête et qu'aucune accusation ne serait déposée. Afin de clore le dossier pour de bon, le policier a toutefois demandé s'il était possible d'obtenir certains compléments

d'information de la part de M. Savoie. Réticent au départ, Me Matchim a fini par accepter sous la promesse écrite qu'aucune accusation ne serait déposée contre son client. Mais voilà, peu de temps après, l'enquêteur a été muté et son remplaçant a porté des accusations, faisant fi de l'enquête et de l'entente du caporal Deveau, ainsi que de deux révisions indépendantes (interne et GRC d'Halifax) aux conclusions similaires: pas d'accusation. Acadie Nouvelle, 6

*** St. Albert man charged after stealing prisoner transport van**

Police in Fort McMurray have charged a 21-year-old man after he escaped custody by stealing a van used to transport prisoners. Wood Buffalo RCMP responded to a call from the courthouse after he escaped in a sheriffs' prisoner van about 5 p.m. Monday. Police said they also received a report about dangerous driving in the area before they found the man. Lyndon Rankin of St. Albert is charged with escaping lawful custody, theft of a motor vehicle, dangerous operation of a motor vehicle and possession of cocaine. Postmedia Network (Calgary Sun, A38, Edmonton Sun, Edmonton Journal)

*** Kitimat welcomes crisis dog**

Everyone loves a man in uniform, right? The newest team member at the Kitimat RCMP detachment is no exception to that rule. Ozzie, a two year old Corgi/Labrador mix, is currently being trained to become a therapy dog with the Victim Services section, run by liaison Leisl Kaberry, who is also Ozzie's owner. Kaberry and her family adopted Ozzie from the Kitimat Humane Society when he was just four months old. He has a naturally calm demeanour, says Kaberry, which makes him a great candidate for the therapy dog training. Kaberry is hoping to get Ozzie tested for his full therapy dog certification in the spring, after he completes his four levels of training. He's already got a good handle on some of the behavioural commands, such as laying down and sitting when asked. He can also high five, which he is keen to do when there's a treat involved. Northern Sentinel (2016-12-07)

High time for province to act on deaths in care

An opinion piece states, "I've never yelled at a cabinet minister before. But I did Wednesday night. That's when Human Services Minister Irfan Sabir told me his department neglected to give the RCMP its internal report into the death of four-year-old Serenity, the First Nations girl who died after being placed in kinship care on a central Alberta reserve, until Tuesday of this week. (…) There have never been any charges laid in Serenity's death. Last month, the RCMP told Postmedia their investigation was on hold, awaiting further reports. What reports? Now we know. Elden Block, the statutory director of children's services, said his department did an internal review of Serenity's death. The review, said Sabir, was forwarded to the First Nations child welfare authority, responsible for the First Nations reserve where Serenity had been living in a kinship care guardianship arrangement. Sabir said it was the job of that band welfare authority to forward the file to the RCMP for investigation. That never happened. No one ever gave that information to the police. Instead, the Mounties had to contact Sabir's department to ask for the information - after they read the news stories about Graff's report into the little girl's death. That was in mid-November. Yet for reasons no one could explain to me, the RCMP didn't actually get the critical report until Tuesday, Dec. 6." Postmedia Network (Edmonton Journal, A1, Calgary Herald)

*** Le retrait de la SQ serait progressif, selon Coiteux**

Le ministre de la Sécurité publique, Martin Coiteux, dément le retrait immédiat de la Sûreté du Québec du territoire de Lac-Simon, en Abitibi-Témiscamingue. En entrevue à Radio-Canada, mercredi, la chef Adrienne Jérôme disait avoir été informée du départ de la police provinciale quelques heures après avoir déclaré qu'elle ne pouvait plus faire confiance à ses agents et qu'elle ne souhaitait plus leur présence. Le ministre Coiteux, qui dit ignorer la source de ces informations, soutient qu'une telle décision nécessiterait d'abord une demande formelle de la communauté algonquine. Il insiste sur le fait que le départ de la SQ, s'il se confirme, se réalisera de manière progressive, et qu'il ne fait pour l'instant que l'objet de discussions. Les renforts de la SQ visent à réhabiliter le corps de police autochtone, secoué par deux incidents mortels survenus en février et en mars dernier. Une intervention policière ayant tourné au vinaigre avait entraîné la mort de l'agent Thierry LeRoux, puis, quelques mois plus tard, le jeune Autochtone Sandy Tarzan Michel avait perdu la vie lors d'un affrontement avec les forces de l'ordre. Le Droit, 17; Radio-Canada; Journal de Montréal

*** Vancouver police seize 56 kilos of cocaine**

A traffic stop by Vancouver police has resulted in a large cocaine bust. Police say patrol officers stopped a SUV with two people inside on Tuesday after they saw some suspicious behaviour. Officers found four kilograms of what they believe is cocaine and had the vehicle towed for a continued search after a warrant was obtained. Police now say that search turned up an additional 52 kilograms of the suspected drug inside the vehicle. The two men have been released pending lab tests on the drugs, and police say charges of possession for the purpose of trafficking are expected to be recommended. Officers estimate the drugs have a street value of between $3 million and $4.5 million. The Telegram, A7

* **Teen accused of threatening attack on Toronto school**
The Toronto Police Service has charged a 17-year-old boy for allegedly threatening to attack Oakwood Collegiate Institute, with fears he might have acted on the 27th anniversary of the École Polytechnique massacre. Detective Len Nicholson said Wednesday that on Dec. 1 someone in the United States tipped off the force about a threat, directed at a Toronto school, on a blogging site. Nicholson said the Montreal massacre - the horrific killing spree of Dec. 6, 1989 - was mentioned in the alleged threat, a detail that made the police's investigation more urgent. (...) Officers raided the suspect's home in the early hours of Tuesday morning and seized several weapons - a machete, two swords, four knives, and arrows - along with computer equipment and clothing; all of them items that can be purchased legally at a hardware store. Nicholson said the teen's plan allegedly involved concealing his weapons under his clothing while en route to the attack. Toronto Star

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Grand Valley prison locked down for search
The Grand Valley Institution for Women was put on lockdown on Wednesday for a search of the multilevel correctional facility. Correctional Services Canada said in a news release that the prison was locked down at about 11:30 a.m. on Wednesday to conduct an "exceptional" search, "ordered to ensure the safety and security" of staff and inmates. The prison has multiple security levels and a capacity for about 200 inmates. Visits are on hold until the search is complete. This is the third lockdown at the women's prison this year. The most recent one was in October and lasted six days. Unauthorized items were discovered, but Correctional Services Canada did not specify what was found. Waterloo Region Record, B2

Springhill prison in lockdown after inmate assaulted
The Springhill medium security institution was put on lockdown Tuesday and all visits suspended following an assault against one of the 400 inmates. "It usually takes two or three days to do a full search," assistant warden Shannon Oickle said Wednesday. "During that time all inmates will get their food and their medication in their cells." Oickle said in a news release that an inmate was the victim of an assault shortly after noon on Tuesday. The inmate was evaluated by staff members and transported to an outside hospital for treatment. No staff members or other inmates were injured. The incident is under investigation by Correctional Service of Canada and the Springhill RCMP. Times & Transcript, A12; * 100.9 Big Dog Truro (Cat Country 99.5 Truro)

* **Inmate death at Millhaven Institution**
An inmate serving time on sex related charges has died at Millhaven Institution. Bryen Madill, 72 was serving an indeterminate sentence for invitation to sexual touching and sexual interference. He was sentenced in March 2009. **Correctional Services** did not give a cause of death. CKWS (96.3 Big FM) (2016-12-07)

* **Federal inmate accused of assaulting sheriff's officer**
A man who allegedly punched a Fredericton sheriff's officer in the face while awaiting transfer to court in Woodstock appeared via video conference to answer to the charge Wednesday. Thomas Joseph Travis (TJ) Ferguson, 36, of no fixed address, faces a charge of assaulting a peace officer in Fredericton - specifically, sheriff's officer Dale Kozak. The charge alleges an incident at the Justice Building in Fredericton on Nov. 7. Wednesday marked his first appearance on the charge, and he appeared in

Fredericton provincial court via video conference from the Atlantic Institution in Renous. Daily Gleaner, A2

* **Protect Kingston Penitentiary**
An opinion piece states, "... Every city has highrises and subdivisions, but not the history and architecture of which Kingston should be proud and should protect. Kingston Penitentiary, with its beautiful buildings and unique history, should not fall prey to the seeming determination to fill it with yet another housing development, highrise condos and the introduction of roadways. Much of the waterfront is already lined with highrises and housing. I hope that it can instead be maintained as a historic site that would be a destination for tourists, already proven by the popular penitentiary tours in the summer, and would be made available to the public at all times, not just to those who reside in the planned housing and condos." Kingston Whig-Standard, A5

* **Notorious rapist released: Police warn public of violent sexual offender living in Edmonton**
Edmonton police are warning that a man once dubbed the "Mill Woods rapist" will be out of prison and living in the city, a warning they have issued several times before. In 1994, a 16-year-old Dana Fash forced his way into the Mill Woods home of a 65-year-old woman and threatened her with a knife. In 1997, he was convicted as an adult and sentenced to 12 years in prison. In December 2008, soon after his third release - he had breached his conditions on two prior releases already - Fash breached his conditions to stay away from alcohol and drugs, prompting police to issue a warrant for him. At the time, Fash's mother approached the media, asking for a stop to coverage of her son's case and saying it would have negative effects on his daughter. She also said the media attention was the reason he fled police. But colleagues of his victims spoke said Fash, who had been described by a top sex crimes police investigator as one of the two worst sex offenders he'd ever dealt with, should not have been paroled at all. On New Year's Day 2009, Fash entered a Vancouver police station and turned himself in after a month-long manhunt. Six months later, police were once again warning Edmonton residents that Fash would be released into the city, describing him as "a violent sexual offender who poses a risk of significant harm to the community and, in particular, adult females." Less than a year after that, Fash was again in court, having breached a court-ordered peace bond for high-risk offenders that allowed police to keep close tabs on him. Fash had been approached by police officers investigating a mischief report. He gave them his identification, but while officers were speaking with another man, Fash fled the scene. He was picked up the following day and found to be in possession of crack cocaine. He went back to prison, charged with obstruction of justice, possession of a controlled substance, and six breach charges. On Wednesday, police issued a statement warning of Fash's latest release, calling him "a violent and sexually violent offender." Edmonton Sun, A5; iNews880

* **Sex offender's penis-injury appeal dismissed**
An appeal by a convicted Edmonton sex offender who argued a judge refused to grant him an adjournment to get medical evidence on his injured penis has been tossed out. Robert Allen Cote, 60, was sentenced to 6-1/2 years in prison after being convicted of sexual assault with a weapon, possession of a dangerous weapon and uttering death threats. However, Cote - who testified in his own defence that he could not have sexually assaulted the victim as he was "incapable of getting an erection" - appealed the 2014 conviction, saying he was denied an opportunity to present medical evidence on his injury. In a decision issued this week, a three-judge panel of the Court of Appeal of Alberta dismissed the appeal after ruling the judge's denial of an adjournment was reasonable in the circumstances. Edmonton Sun, A5

* **Les audiences sur la remise en liberté de l'ex-juge Jacques Delisle se prolongent**
Le juge qui entend la demande de libération de l'ex-juge Delisle veut que le débat prenne fin cette semaine. « Et la semaine se termine samedi à minuit », a prévenu le juge Benoit Moulin au terme d'une longue journée mercredi. En principe, l'audition de la cause devait prendre fin jeudi après trois jours d'audience qui ne seront de toute évidence pas suffisants. Au départ, les partis avaient évalué qu'ils allaient régler le débat en deux jours en octobre, mais la cause avait débordé sur un total de cinq jours. Jeudi, l'avocat de Jacques Delisle va poursuivre le contre-interrogatoire de l'expert en balistique de la Couronne qui écarte la thèse d'un suicide pour expliquer la mort de Nicole Rainville. Radio-Canada; La Presse; Canoë (2016-12-07)

*** Mental health is an issue for more than one-quarter of Ontario's prison population**
More than a quarter of Ontario's prison population has been flagged for a possible mental health issue, according to new numbers provided to VICE News in the days after an inmate diagnosed with schizophrenia hanged himself. Justin St. Amour was in the health care unit of the Ottawa-Carleton Detention Centre when he attempted suicide by using a bedsheet to hang himself, sources told the Ottawa Citizen. Now he's on life support, and his mother is preparing herself for the worst. Laureen St. Amour wants to know why her son, who correctional officers said repeatedly threatened or attempted suicide, wasn't in a psychiatric hospital instead, she told the Citizen. And even as St. Amour lay in the intensive care unit, no one thought to notify his lawyer. Over the past year, 16,387 provincial inmates had a 'mental health alert' attached to their files, or 28 percent of a total of 58,313 prisoners. Those alerts include not only inmates reporting issues themselves, but also "possible management concerns" identified by correctional staff. But the problem may actually be much worse, correctional officers fear, since conditions such as depression or suicidal thoughts are not always visible and can be missed by the untrained eye. VICE News (2016-12-06)

*** Inmate who attempted suicide at Ottawa jail removed from life support**
An inmate with mental illness who attempted suicide by hanging himself in his segregation cell in the health care unit of the Ottawa jail has been removed from life support. The family of Justin St-Amour made the decision to remove the 32-year-old from his ventilator and feeding tube on Wednesday, a week after he attempted suicide at the Ottawa-Carleton Detention Centre. He's not expected to survive for much longer, his mother said. Ottawa Citizen (2016-12-07)

«Un mythe populaire»
La violence en prison existe, mais dans une ampleur moindre que tend à l'indiquer la croyance populaire. Il s'agit davantage d'un «mythe populaire» qui remonte à une autre époque, sans qu'elle soit révolue. Selon Mathieu Lavoie, président du Syndicat des agents de la paix en services correctionnels du Québec (SAPSCQ-CSN), la situation a «évolué à travers le temps» et a été atténuée par la mise sous protection de plusieurs détenus. De plus, les agents correctionnels «ne peuvent fermer les yeux sur de tels événements ni tolérer une menace». «Ça existe quand même. A certaines personnes, quand elles ont certains types d'accusations ou que leur dossier a été très médiatisé, on leur propose de ne pas les mettre dans la population régulière. Souvent, ce sont les détenus qui le demandent, mais ça peut être une décision administrative, toujours pour assurer la sécurité dans nos établissements», a commenté M. Lavoie. La mise sous protection est d'ailleurs une mesure fréquente. «Les secteurs de protection débordent dans les prisons de la province. Dans le cas d'Yves Martin, puisque son dossier a été très médiatisé, s'il se sent menacé, il pourrait s'y retrouver», a-t-il ajouté. Le Quotidien, 18

Libération possible au tiers de la peine
Un article d'opinion déclare, « Peu importe la sentence qu'il recevra, Yves Martin sera admissible à une libération conditionnelle après avoir purgé le tiers de sa peine. Par exemple, s'il écope de 15 ans, il pourrait reprendre sa liberté au bout de cinq ans. Si cela existe, c'est que le système judiciaire canadien favorise la réinsertion et la réhabilitation des détenus. Le législateur croit qu'il est préférable de relâcher un individu afin de lui permettre de réintégrer la société, plutôt que de lui faire purger la totalité de sa peine et ensuite de l'envoyer dans la rue. En revanche, même si Yves Martin devait profiter d'une libération conditionnelle après cinq ou six années de détention, il demeure tout de même sous le joug de la justice pour la balance de sa sentence. S'il commet la moindre erreur, il est possible qu'il soit ramené derrière les barreaux. » Le Quotidien, 18

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Racist comments cost cop his rank**
An Ottawa cop has been demoted for three months for posting "insulting and racist" comments about the death of acclaimed Inuk artist Annie Pootoogook. Sgt. Chris Hrnchiar, a veteran officer who works in the forensic identification unit, was demoted Wednesday to the rank of firstclass constable and must take

multicultural training within three months. The police force and his defence had submitted a joint submission on penalty. The officer's actions "were clearly inappropriate and an embarrassment to the Ottawa Police Service," said Ret. Deputy Chief Terrence Kelly, who oversaw Hrnchiar's sentencing hearing Wednesday. In September, the officer openly discussed Pootoogook while off duty using his personal Facebook account, writing in the comment section of a online article about her death that it "has nothing to do with missing and murdered Aboriginal women" while the probe into her death was still ongoing and continues to this day. Postmedia Network (Ottawa Sun, A5, Ottawa Citizen, National Post)

* **Late teen 'a catalyst for change'**
Shelby Maunder wants to put a local campaign out of business. That's what she told a crowd of people Tuesday in the lobby of the Yukon Government Main Administration Building, during the final event in the 12 Days to End Violence Against Women campaign. "I was feeling really discouraged. I don't want us to need this campaign anymore," said Maunder, the executive director of Bringing Youth Towards Equality (BYTE). "It can be easy to feel that way. In the fight to end violence against women, it seems like, for every gain we make, there are setbacks to accompany it." However, she said, the theme for this year's campaign - prevention - is one that gives her hope. That was the message of many speakers at the event, meant to remember the 14 women killed at Montreal's École Polytechnique on Dec. 6, 1989. The date marks a National Day of Remembrance and Action on Violence Against Women. Sarah Murphy, one of the event's hosts, said the memorial also served as a reminder of violence closer to home. "In the Yukon, this ceremony is also an opportunity to recognize the continued injustice of missing and murdered aboriginal women across our country, and here in our territory," said Murphy, the program co-ordinator with the Victoria Faulkner Women's Centre. "We will take the time today to remember and honour the 39 Yukon First Nations women who have disappeared or been killed in the last 30 years." Whitehorse Daily Star, 4 (2016-12-07)

* **Ottawa paramedics warned to wear masks over fear of powerful new drug**
A new drug called carfentanil, an animal tranquillizer that's 100 times stronger than fentanyl, is so dangerous Ottawa Paramedics are being warned to wear masks on the job. Carfentanil has now been detected in drugs sold on the streets in Ontario. Green pills seized last month in the Waterloo region contained the potentially lethal opioid, Health Canada confirmed. Yesterday, Toronto Police also warned they found carfentanil in heroin sold on city streets. "From Toronto it's going to make it's way here in a week or two or three," expects Ottawa Paramedic Service spokesperson J.P. Trottier. "This is a huge concern for us." The drug is commonly used at zoos to sedate large animals. In humans, it's so potent it has been linked to the deaths of 15 people in Alberta and one overdose in Vancouver. Ottawa paramedics have been watching the crisis unfold out west over the past year in an effort to prepare first responders. Staff are being briefed on how to treat patients and stay safe themselves by wearing masks whenever possible. CBC News

Muslim group denounces Edmonton LRT incident as 'hate crime' calling it 'absolutely horrifying'
The national organization representing Canadian Muslims is calling on Edmonton police to lay hate crime charges against a man after two Muslim women were threatened with a noose on a city LRT platform. Amira Elghaway, communications director for the National Council of Canadian Muslims, said the incident on Nov. 8 at the University LRT Station was "absolutely horrifying." Cellphone video shot by one of two young women shows a man pulling a rope from his pocket and tying it into a noose before dangling it from his hand while threatening them, saying “This is for you.” He then proceeded to sing the Canadian national anthem. "For an individual to specifically be walking around with a noose looking for that opportunity to basically instil fear in someone or people is rather troubling," Elghaway said. On Tuesday, the Edmonton police hate crimes unit said it had a suspect in custody. "A vast majority of Canadians do not support these racist or anti-Muslim acts but unfortunately it's the few that, with one act, can send out a very scary message to the community," said Elghaway. "That's why hate crimes are so dangerous in our society because they are not just targeting an individual, they are targeting an entire community. Edmonton Sun

* **Let's not sugar-coat the issue**
An editorial states, “Communication is more than just understanding language. It's also an understanding of the social construction of meaning that underscores language. Take for example the phrase: "How are

you doing?" When said in a coffee shop to a co-worker, it's a greeting. When said to a loved one at a funeral, it's a condolence. When said to someone at a bar, it's a pickup line. (…) There's a 'but' here. Ms. Poorman's occupation had everything to do with her murder. While the police were very careful not to call Ms. Poorman a sex-trade worker, the assertion that hers was a high-risk lifestyle could be seen as victim-blaming. But it isn't untrue. There are countless efforts being made by both the police and indigenous groups to assist women working in the sex trade to get off the streets for that very reason. Sex-trade work is very often high-risk, and police make it safer by arresting those who prey on the exploited. Communication is also two-way. Saying "How are you doing" in the workplace could be taken as a pickup line by the recipient, even if that's not the intention. Ms. Spillett made an assumption the description used by police reinforced negative stereotypes. Others may not hear it that way, particularly as more information is made available daily about the vulnerability of women involved in the sex trade. For some, it may make her death even more tragic and increase resolve to end the cycle of violence and poverty First Nations women inordinately face. If we are to fully understand the issues facing First Nations women, particularly those who are missing and murdered, then the public needs to be aware of their circumstances. Sex-trade workers are more likely to be victimized, making this a high-risk situation." Winnipeg Free Press

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Reference, reframed**
A letter to the editor states, "Re Agnes Macphail Becomes Canada's First Female MP (Moment In Time, Dec. 6): With great respect to Agnes Macphail, 1921 was not "the first year all Canadian women could cast a ballot in a federal election." That didn't happen until another 39 years had passed. As Canada undertakes an inquiry into the many missing and murdered indigenous women and girls, it seems appropriate to recognize First Nations women as worthy and valued citizens. It was not until 1960 that these citizens could vote in a federal election." Globe and Mail, A16

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Panel to tell Ottawa to monitor legal pot
A federal panel reporting to Ottawa on the next steps toward legalizing marijuana is expected to call for a comprehensive regime to monitor the impacts of bringing the substance out of the shadows and into the mainstream. And that could make Canada the world's first national case study on the dangers - and potential benefits - of cannabis when the drug becomes legal, some of the country's leading drug researchers say. Researchers must study the dangers, such as impaired driving and more young people using it, says Dan Werb, director of the Toronto-based International Centre for Science in Drug Policy. But, he adds, they must also be open to looking for pot's potential public-health benefits, such as people substituting cannabis for alcohol or opioids. Globe and Mail, A14

*** Aphria determined to power on**
Leamington pot grower Aphria Inc. is so high on the prospect of Canada soon legalizing the recreational use of marijuana that it's giving Hydro One an ultimatum - guarantee extra power or the company builds its own power plant. (…) The Trudeau Liberal government's point man on the marijuana file, Scarborough MP and former Toronto police chief Bill Blair, is expected as soon as next week to divulge recommendations on how Ottawa should proceed with legalization. Former deputy prime minister Anne McLellan recently handed in her task force report on pot legalization and regulation, and Prime Minister Justin Trudeau reiterated on the weekend that voters gave his government "a clear mandate" to proceed on legalization of recreational weed. The Liberals have stated repeatedly that legalization will not open the doors to homegrown pot. Neufeld anticipates recreational use for adults will likely begin in 2018 and that licensed producers such as Aphria (there are currently 36 Health Canada-approved LPs across

Canada) will become the legal source of all marijuana for medicinal and recreational purposes. Windsor Star, A1

*** Start the pot talk early**
Mom Scarlett Ballantyne wonders if Ottawa's plans to legalize marijuana will make her 14-and 16-year-old daughters more inclined to try it. But she's not waiting to find out. Ballantyne says her family has been discussing the dangers of drug use since the girls were 13 - a pre-emptive strike as pot shops and marijuana headlines have been popping up everywhere they turn. She's proud to say they are athletic, self-confident kids, but she also gets the impression that their generation sees marijuana as "not that big of a deal." "As parents, it's just [about] stressing to them that it is a big deal," she says from her home in White Rock south of Vancouver. (…) Many questions remain about what restrictions Ottawa might impose when it introduces legislation next year to legalize recreational use. In the meantime, experts say parents should be prepared for any questions their kids might have - but don't wait until you find a stash in their room. (…) Researchers generally agree that adolescents should be strongly discouraged from using marijuana. The Canadian Paediatric Society notes brains develop well into our 20s and that cannabis can affect both the structure and functionality of young brains. They also warn that heavy users are at risk of mental-health issues later in life. Last month, the society urged that the federal government ban sales to those younger than 18 or 19, depending on their location in Canada, to align with age limits for alcohol and tobacco sales. Times Colonist, D1

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Where are the checks and balances on public spending?**
An opinion piece states, "What can really get many of us riled up is government waste. We've all heard at least one story that's a real head-shaker. For some, the answer is to cut government. For me, that's just shooting ourselves in the foot, or worse. Public services have already deteriorated thanks to years of cutbacks in the public service. What we need is to ensure public monies allocated to government departments, and to the health and education systems, are spent effectively and prudently. That is the job of MLAs. (…) Much of the spending by the Aboriginal Affairs Secretariat is actually done through the Regional Development Corporation. However, during the shale gas protests in 2013, Aboriginal Affairs paid for a person retained by the **Department of Public Safety** to de-escalate tensions between the protesters, the RCMP and the community of Elsipogtog. In that instance, **Public Safety** failed to get much value for the money it spent from Aboriginal Affairs after violence flared. (…) The **Department of Public Safety** which is increasingly responsible for enforcing many of the province's laws, governing everything from liquor control to private eyes, spends $15 million a year on inspections and investigations. Apparently, the compliance rate for the laws they enforce is 65 per cent, yet, the department does not track the number of cases it refers for prosecution, nor does it hear back about the results of the court cases. **Public Safety** funds an intelligence gathering service called the Criminal Intelligence Service of New Brunswick at a cost of $588,000. Yet its employees and activities are nowhere to be found on the department's website or in its annual report, making it impossible to determine whether this is an effective use of public funds." Daily Gleaner, A9

*** Public service pay unsustainable**
An editorial states, "A new review from the Fraser Institute shows that Canada's public sector workers earn 11% more than their private sector counterparts. And, in most cases, they enjoy generous, even "gold-plated" pension and other benefits relative to the private sector. The Fraser study examined wages across all levels of government and compared them to employees doing similar work in the private sector. They adjusted for factors such as level of education and years of experience. All things being equal, government workers doing the same work, with the same qualifications as private sector workers earn more, and are better offin retirement. The wage-gap between the public and private sector has been growing for years. But there is now a significant inequity in compensation between our public servants and those who pay taxes to support them." Winnipeg Sun, A10 (Ottawa Sun, Toronto Sun)

OTHER / AUTRE

NIL

INTERNATIONAL

*** Pakistan plane recorder found as crash investigation, recovery continue**
Pakistani military helicopters on Thursday ferried remains of plane crash victims to the capital, Islamabad, as aviation authorities said they opened a probe into the crash that killed 47 passengers and crew the day before in the country's northwest. The small twin-propeller aircraft was travelling from the scenic mountain resort city of Chitral to Islamabad on Wednesday when one of its engines failed shortly after takeoff and crashed in the hillside village of Gug in the district of Abbottabad, according to Pervez George of the Civil Aviation Authority. The plane belonged to the Pakistani national carrier, the Pakistan International Airlines, and had 42 passengers and five crew members on board, PIA spokesman Daniyal Gilani said. Witnesses said they saw the plane suddenly tilting and going down, then bursting into flames upon crashing in Gug. The village is located next to another, Saddha Batolni, from where residents also joined the rescue work. CBC News

*** Search for survivors continues in Indonesia as death toll climbs to 102**
Humanitarian organizations descended on Indonesia's Aceh province Thursday as the government in Jakarta promised tons of emergency aid and officials raced to assess the full extent of damage from an earthquake that killed more than 100 people. Search efforts involving volunteers and nearly 1,500 rescue personnel were concentrated on the hard-hit town of Meureudu in Pidie Jaya district near the epicentre of the magnitude 6.5 quake that hit before dawn Wednesday. Humanitarian assessment teams were fanning out to other areas of the district. National Disaster Mitigation Agency spokesman Sutopo Purwo Nugroho said the death toll had risen to 102 and warned it could increase. Search teams were using devices that detect mobile phone signals with a 100-metre radius to help guide their efforts as they scoured the rubble, he said. Aceh's disaster mitigation agency said more than 600 people were injured. CBC News

*** Gatlinburg fire: 2 juveniles face aggravated arson charges**
Two juveniles face charges of aggravated arson in connection with a deadly Tennessee wildfire that began in late November and spread to Gatlinburg, Tennessee, according to Mark Gwyn, director of the Tennessee Bureau of Investigation. Additional charges are being considered, 4th District Attorney General James Dunn said, including the possibility of seeking a transfer to adult criminal court. He said the youths were from Tennessee, but not from Sevier County, where the fires started. Neither their ages nor genders were released. Fourteen people lost their lives in the fires and more than 175 more were injured, according to officials. Residents and visitors to the resort-heavy area were among the dead. CNN

*** ISIS launches advice show**
Even terrorists have problems - and ISIS wants to help. The terrorist organization's radio station has launched a new program. The show, Fatwas Over the Airwaves, features a host, along with Muslim clerics answering queries on lust and religious law. The biggest query is women's roles. Should they be allowed to watch executions? Do women lustover executioners? "Some of the scholars have tended not to permit women to look at male strangers," one cleric answer a troubled jihadi. "It is fundamentally permissible for the Muslim women to watch ISIS videos." He added some jihadis have been uncompromising on forbidding women from looking at strangers. The cleric couldn't say whether it was pure desire or the executioner that was causing temptation. This puzzle was debated after ISIS released footage of the tubby terror known as the Bulldozer using a chainsaw to execute nine teens. Swoon. Calgary Sun (Toronto Sun)

*** Iraqi forces face fierce IS attacks after new Mosul push**
Significant Islamic State group counterattacks in southeastern Mosul inflicted heavy losses on Iraqi forces overnight after a new push deeper into the city this week, according to an Iraqi Army officer. Despite the counterattacks, the fresh Iraqi push appears to have relieved pressure on Iraq's special forces who have been largely leading the fight inside the city on the eastern front. Wednesday afternoon, the special forces

announced new gains. The troops retook another neighbourhood bringing them closer to the Tigris River that divides Mosul's east from west, according to the commander of a joint operations centre that oversees the Mosul campaign. Lt. Gen. Abdul-Amir Yarellah, said in a statement that troops had "fully liberated" the al-Elam neighbourhood and raised the Iraqi flag over its buildings. Yarellah added that IS militants "suffered losses" without elaborating. (...) "Daesh waited until night to attack the troops," Iraqi Army Sgt. Maj. Hakim Saranbii told The Associated Press. He added that the attacks "inflicted heavy losses," without giving specific casualty figures or further details. Iraqi Defence Ministry officials in Baghdad did not immediately comment. Telegram, B10

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
December 10, 2016 / le 10 décembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Lawyers say cops' crime database is full of holes

Lawyers say they regularly receive incomplete or inaccurate criminal records from the national police database which can lead to wrongful arrests, unfair sentences or critical information missing at bail hearings. The consequences of this were most recently seen when a man convicted of sexual assault fled to Pakistan in November before he could be sentenced. Moazzam Tariq was allowed to remain out on $10,000 bail after his conviction, because the Toronto police and Crown didn't know he'd fled the country before while on bail after being criminally charged in Peel Region in 2010. Tariq, now 29, came back to Canada in 2011 and was arrested at the airport. He eventually pleaded guilty to dangerous driving in 2012. However, that conviction and his withdrawn charges - including for a failure to appear for his court date - were not recorded in the Canadian Police Information Centre (CPIC) database, a Toronto court heard Thursday. It's unclear whether Peel Regional Police failed to submit the information to the RCMP, which is in charge of the database, whether it was part of the backlog of convictions the RCMP has yet to

enter into the database, or whether it fell through the cracks. The RCMP was not able to respond to questions by deadline on Friday and questions to the **Minister of Public Safety** were referred to the RCMP... While the RCMP is working on modernizing the system, CPIC records continue to fail to show an up-to-date and accurate criminal history across jurisdictions, lawyers say. Toronto Star

No concrete timeline for prison farm decision

Kingston and the Islands MP Mark Gerretsen told members of the Prison Farm Co-op last night that he has no news for them yet on the possible return of the farms. "I was really hoping to hear from the **minister's office** on what their decision was prior to the holidays, but they informed me two or three weeks ago they wouldn't have a decision before then," Gerretsen told the Whig-Standard on Friday afternoon before heading to the meeting. The decision on whether to reopen the prison farms rests with **Public Safety Minister Ralph Goodale...** Last month, Correctional Service Canada released a report from a survey on its website gauging Canadians' opinion on reopening the farms in some form or another. More than 6,000 people responded to the online survey, conducted between June 2 and Aug. 4, and the main factors supporting reopening the farms included the need to help the rehabilitation process of inmates and the positive impact the farms could have in their communities. Specifically, 95 per cent of respondents "strongly agreed" or "agreed" that an institutional agribusiness initiative would contribute to rehabilitation, the consultation report said. "My understanding, from what I've been told by **the minister's office**, is that they are currently reviewing the findings," Gerretsen said. Gerretsen said he doesn't have a timeline on a decision from the **minister's office**. "Not that I haven't been asking," he said. "I've been continually asking the **minister's office** for an update, but I haven't received anything to date."... Gerretsen said the challenge will be to combine the prison farm co-op plans along with plans from CSC and the **minister's office**. Postmedia Network (Whig-Standard, A4)

Has terror suspect been de-radicalized?

During the 14 years that he has been a terror suspect, Mohamed Harkat has put down roots in Ottawa. Although branded by the federal government an al-Qaida terrorist - an opinion upheld by the Supreme Court of Canada - Harkat has managed to establish relationships with relatives, friends and neighbours, many of whom have submitted letters of support as he campaigns to remain in the country. A federal official known as the **minister's delegate** must now decide whether those letters are evidence that Harkat has been de-radicalized, or whether he still poses a threat to Canadians. The Algeria-born Harkat, who works as a custodian at a church, has lived under court-ordered conditions in the Heron Gate area since he was released on bail more than a decade ago. The letters offer a rare glimpse into his life. "My uncle gave me my first driving lessons: He was very patient. He has also helped me with my school projects," wrote Harkat's 16-yearold niece, Gabrielle, in one of 70 letters sent to **Public Safety Minister Ralph Goodale,** and shared with the Citizen... The portrait that emerges is either the product of a sustained con job by an al-Qaida sleeper agent, or it is hard evidence of Harkat's mainstream assimilation... The issue of whether Harkat has been de-radicalized is now frontand-centre in his case since the government must decide whether to deport him to his native Algeria. Earlier this year, a Canada Border Services Agency official filed a confidential report with the **minister's delegate**, arguing that Harkat should be sent back to Algeria despite facing "some risk" of torture. The report was prepared by Anne-Marie Charbonneau, manager of the agency's danger assessments section. If Harkat is not removed, she warned, he would be free to resume contact with members of the Islamic extremist network... Harkat's defence team has until Dec. 19 to make submissions to the minister's delegate, who will have to weigh Harkat's personal risk in Algeria against the risk he poses to Canadians. A decision on deportation is expected next year. Postmedia Network (Ottawa Citizen, A11)

Goodale keeps door open to CSIS use of metadata gathered from innocent people

The **federal public safety minister** is keeping the door open to the idea of Canada's spy agency crunching potentially sensitive data about innocent people. **Ralph Goodale** told MPs at a House of Commons committee Thursday he is weighing views on whether the Canadian Security Intelligence Service should be allowed to retain and use such information... **Goodale** told MPs on the public safety committee the government would ***"consider all of the factors that are relevant in these circumstances"*** as it completes a review of national security policy. Canadian Press (Whitehorse Star, 19)

TOP STORIES / MANCHETTES

Crown rests case in Montreal terror trial
The Crown rested its case Friday at the trial of a Quebecer charged with attempting to leave the country to participate in the activities of a terrorist group. Ismael Habib, 29, is also charged with giving false information in order to obtain a passport. The trial was adjourned until Jan. 23, when lawyers will debate the admissibility of a confession by Habib extracted by an undercover police officer last February when Habib said he intended to join Islamic State of Iraq and the Levant in Syria. Habib's lawyer, Charles Montpetit, has suggested it was obtained in a Mr. Bigtype operation where officers pose as criminals to obtain confessions... The RCMP scenario for Habib involved reeling him into a fictitious crime organization specializing in counterfeit passports and a fake human-smuggling ring. On Friday, the Mountie who designed the elaborate scenarios was the final prosecution witness as he provided details from behind a divider about a civilian source used to reel in Habib. The RCMP handler, under cross-examination by Habib's lawyer, described the source, a Muslim man in his 40s who was paid per piece of information... Described as a "mentor," the man was used to gain Habib's trust and steer him to the collection of RCMP agents in the sting. Upon learning Habib had gone to Syria in 2013 and returned, the civilian source raised concerns, without proof, that Habib might be a sleeper agent returning to commit a terror act. An RCMP document filed in the case suggests the force wanted to discover where he was trained, why he'd returned to Canada, what his intentions were and whether he presented a public security risk. Postmedia Network (National Post, A11; Guardian; Telegram; Cape Breton Post; Toronto Sun); La Presse; La Voix de l'Est; Le Droit; Gazette

Border officer faces charge in smuggling probe
The RCMP says a Canada Border Services Agency officer has been charged in a smuggling investigation. The Mounties say the arrest came as part of an investigation that focused on a criminal organization allegedly smuggling tobacco into Canada from the U.S. They allege the smuggling activities were facilitated by a CBSA border services officer in Fort Erie, Ont. Investigators say arrests and seizures were made in Canada and the U.S. Police say 37-year-old Chad Gale of Welland, Ont., is charged with breach of trust by a public officer. CBSA regional director Rick Comerford called it a very serious matter. "It is an isolated incident and in no way reflects the integrity and professionalism of the thousands of dedicated CBSA officers who carry out their duties each day in an exemplary manner," Comerford added. Postmedia Network (National Post, A11; Whig-Standard)

*** Mountie sues over stress suffered in child-sex unit**
An RCMP officer has filed a lawsuit alleging he nearly suffered a nervous breakdown after being assigned to a child sex offences unit in Surrey. Const. Michael Wardrope says he was exposed to too much child pornography and claims the conduct of his superiors amounted to intimidation and harassment and resulted in him suffering from post-traumatic stress disorder. Wardrope, who became a Mountie in January 2007 and is a resident of Maple Ridge, says in the lawsuit filed in B.C. Supreme Court that in 2009 he was recruited to the child abuse and sexual offence unit... Wardrope says his health was deteriorating and his mental health was affected by unforgettable images and memories from the files he had worked on and he was never offered a debriefing in the entire period he was in the unit. Postmedia Network (Vancouver Sun, A23)

*** Investigation clears RCMP officers of any wrongdoing in shooting death**
An investigation has cleared Morinville RCMP officers of any wrongdoing in the 2015 shooting death of a man with a "history of significant mental illness and conflict with the law." In a detailed report released Friday, the Alberta Serious Incident Response Team found the officers involved were "acting lawfully and the use of force was reasonable and justified in all the circumstances." The incident happened May 22, 2015, when Mounties attended a rural home near Morinville after receiving a 911 call from a family member who was concerned for their safety. Postmedia Network (Edmonton Sun, A10; Edmonton Journal; Calgary Herald)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Toronto joins 100 Resilient Cities group to prepare for the next crisis**
With the three-year anniversary of the 2013 Toronto ice storm approaching, the city is taking steps to improve how it responds to extreme weather events and other potential disasters... The mayor's remarks followed an event that formally marked Toronto's acceptance into 100 Resilient Cities, an initiative funded by the New York-based Rockefeller Foundation, dedicated to building "urban resilience" in cities around the world. The objective is resilience to more than just ice storms. 100 Resilient Cities was formed to respond to three major trends impacting cities: urbanization, globalization and climate change - trends that are causing both "acute shocks" and "chronic stresses." The ice storm is one example of acute shocks, a category that includes fires, floods, extreme weather, an infectious disease outbreak, terrorism, riots or other natural and man-made disasters. CBC News

Rescuers to try drones in two cities
Drones will be used by searchand- rescue crews in two cities in British Columbia as part of a one-year pilot project. The drones will be used in Coquitlam and Kamloops with the blessing of Emergency Management B.C. The provincial government said the devices have the potential to help emergency management personnel and are increasingly being used by public safety agencies across North America. Emergency Management said it will ensure the drones are used in ways that consider privacy and Transport Canada regulations. Tom Zajac, vice-president of Coquitlam Search and Rescue, said in a statement the organization is always looking at using new technologies and techniques to improve its search capabilities or reducing risks to people involved in search-and-rescue operations. Postmedia Network (Times-Colonist, A8; National Post)

*** Federal government upgrading coast guard headquarters in St. John's**
The federal government announced $4 million will be spent on harbourside improvements to the Canadian Coast Guard Atlantic Headquarters in St. John's. The government will remove sediments from the bottom of the harbour near the dock to increase water depth, allowing for larger Coast Guard vessels to tie up at the wharf on the south side of the harbour. "Having larger vessels close to the Atlantic Regional Headquarters building will also facilitate increased efficiency in the day-to-day operations of shore-based personnel," the Coast Guard said in a news release. The work is already underway and is expected to be completed by February 2017. Telegram

Spread by trade and climate, bugs butcher America's forests
In a towering forest of centuries-old eastern hemlocks, it's easy to miss one of the tree's nemeses. No larger than a speck of pepper, the Hemlock woolly adelgid spends its life on the underside of needles sucking sap, eventually killing the tree. The bug is one in an expanding army of insects draining the life out of forests from New England to the West Coast. Aided by global trade, a warming climate and drought-weakened trees, the invaders have become one of the greatest threats to biodiversity in the United States. Scientists say they already are driving some tree species toward extinction and are causing billions of dollars a year in damage - and the situation is expected to worsen... Insect pests, some native and others from as far away as Asia, can undermine forest ecosystems. For example, scientists say, several species of hemlock and almost 20 species of ash could nearly go extinct in the coming decades. Such destruction would do away with a critical sponge to capture greenhouse gas emissions, shelter for birds and insects and food sources for bears and other animals. Dead forests also can increase the danger of catastrophic wildfires. Whitehorse Star, 26

Search continues for missing Islander
Police are trying to piece together the activities of a Murray Harbour man Wednesday when he failed to show up at work. Kings County RCMP Corp. Alexis Triantafillou told The Guardian police have "reason to believe" that Alan Richards, 68, spent the night in Summerside Tuesday... The RCMP Police Dog Service, Ground Search and Rescue volunteers, a Cormorant rescue helicopter, and boats have all been deployed in the search. Guardian, A5

*** Jennifer Hillier-Penney search moves to other bodies of water**
The search of St. Anthony Harbour for missing person Jennifer Hillier-Penney has concluded, but the search continues. RCMP Media Relations Officer Trevor O'Keefe said the search for the 38-year-old St. Anthony woman, who was last seen on Nov. 30 on tHusky Drive, will continue in other bodies of water in

the area. O'Keefe would not confirm which bodies of water were being considered at this time. Telegram, A3

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Crown rests case in Montreal terror trial
The Crown rested its case Friday at the trial of a Quebecer charged with attempting to leave the country to participate in the activities of a terrorist group. Ismael Habib, 29, is also charged with giving false information in order to obtain a passport. The trial was adjourned until Jan. 23, when lawyers will debate the admissibility of a confession by Habib extracted by an undercover police officer last February when Habib said he intended to join Islamic State of Iraq and the Levant in Syria. Habib's lawyer, Charles Montpetit, has suggested it was obtained in a Mr. Bigtype operation where officers pose as criminals to obtain confessions... The RCMP scenario for Habib involved reeling him into a fictitious crime organization specializing in counterfeit passports and a fake human-smuggling ring. On Friday, the Mountie who designed the elaborate scenarios was the final prosecution witness as he provided details from behind a divider about a civilian source used to reel in Habib. The RCMP handler, under cross-examination by Habib's lawyer, described the source, a Muslim man in his 40s who was paid per piece of information... Described as a "mentor," the man was used to gain Habib's trust and steer him to the collection of RCMP agents in the sting. Upon learning Habib had gone to Syria in 2013 and returned, the civilian source raised concerns, without proof, that Habib might be a sleeper agent returning to commit a terror act. An RCMP document filed in the case suggests the force wanted to discover where he was trained, why he'd returned to Canada, what his intentions were and whether he presented a public security risk. Postmedia Network (National Post, A11; Guardian; Telegram; Cape Breton Post; Toronto Sun); La Presse; La Voix de l'Est; Le Droit; Gazette

How 'sigint' nabbed a Canadian al-Qaeda operative
Communications intercepted by U.S. and British spy agencies led to the arrest of the first al-Qaeda inspired terrorist caught in Canada, according to a newly leaked document. The memo, circulated within the U.S. National Security Agency more than a decade ago, provides a rare and detailed look at the world of intelligence-sharing. In early 2004, a cell of British terrorists was caught scheming to explode a bomb in London. After Scotland Yard launched "Operation Crevice" to round up the conspirators , Canadian police simultaneously moved to arrest an Ottawa software engineer. Momin Khawaja had helped build detonators for the conspirators. The suspects, including Mr. Khawaja, were twenty something Westerners whose families had hailed from Pakistan. They had travelled to a terrorist training camp in that country and emerged from it wanting to bomb Britain for its role in the invasions of Iraq and Afghanistan. Evidence included discussion of close co-operation between British and Canadian police. But prosecutors glossed over how "signals intelligence" (or sigint) captured long before the bust had laid a foundation for detectives. The details are revealed in a document flowing from Edward Snowden, the fugitive former American contractor who took volumes of files from the NSA in 2013 to leak them to the media... The leaked NSA memo, which is to be officially declassified in 2032, says that "well over 100 Sigint reports were issued on Operation Crevice." Most came from GCHQ but "the NSA reporting contributed significant pieces to the jigsaw." A Canadian agency called the Communications Security Establishment is a close NSA and GCHQ ally, but the Operation Crevice memo makes no mention of it. At that time, the Canadian agency was beginning to get secret authorizations from cabinet ministers to expand its powers. Globe and Mail, A8

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Border officer faces charge in smuggling probe

The RCMP says a Canada Border Services Agency officer has been charged in a smuggling investigation. The Mounties say the arrest came as part of an investigation that focused on a criminal organization allegedly smuggling tobacco into Canada from the U.S. They allege the smuggling activities were facilitated by a CBSA border services officer in Fort Erie, Ont. Investigators say arrests and seizures were made in Canada and the U.S. Police say 37-year-old Chad Gale of Welland, Ont., is charged with breach of trust by a public officer. CBSA regional director Rick Comerford called it a very serious matter. "It is an isolated incident and in no way reflects the integrity and professionalism of the thousands of dedicated CBSA officers who carry out their duties each day in an exemplary manner," Comerford added. Postmedia Network (National Post, A11; Whig-Standard)

Canadian government tests automated border crossing

First there were automated drive-through carwashes. Then automated drive-through banks. Now, the Canadian government is experimenting with an automated drive-through border crossing. While the fate of the wall along the U.S.-Mexico border promised by President-elect Donald Trump remains uncertain, Canada is carrying out a pilot project with an opposite aim: to use the latest technology to ease the flow of traffic across the United States' northern frontier. If you drive into the province of Quebec via the crossing at Morses Line, Vt., after 4 p.m. on any day, no live Canadian customs agent will stop and interrogate you. Instead, a gate opens and you drive into a large, garage-like building. There, under the gaze of several TV cameras, you are invited by a customs officer to insert your passport or other border ID into a document reader and are asked the usual questions put to visitors seeking to enter Canada. The customs officer addressing you over a microphone is located at a service center operated by the Canadian Border Services Agency in Hamilton, Ont. "So far, it's going very well. We've seen an increase in the use of the border crossing," said Dominique McNeely, a spokesman for the agency. The experiment's budget is $16 million, most of which has been spent on the new building and its high-tech equipment. The year-long pilot program ends in a couple of months, at which time it will be decided whether to expand it to include other small crossings... The union representing Canada's 10,000 border guards thinks the automated-crossing experiment is a waste of money and a threat to security. "To cut two jobs, they've invested $16 million," said Jean-Pierre Fortin, the union president. "We are the first line of defence for this country. Technology should be there to assist us, not to replace us." Fortin said that if criminals were to be flagged trying to enter Canada via the drive-through, they could easily abandon their cars and escape on foot, with no guard around to stop them. Also, he says, there is no way a camera can determine whether a driver has been drinking and driving. The Border Services Agency says that no jobs have been lost, since the alternative was a border that was closed 16 hours a day, and that the automated post is more secure than simply having a gate across the highway. Washington Post (Winnipeg Free Press)

Accused in 2010 slaying nabbed in Kuala Lumpur

A suspected killer who has been sought for six years was finally tracked down in Malaysia and brought back to the city to face the music. Toronto Police named a suspect in the murder of Nanthi Eashan Dharmaratnam almost immediately after he was allegedly deliberately run down by a car in a Scarborough parking lot on March 13, 2010. But the 25-yearold's killing remained unsolved until cold case homicide investigators found Seran Kasilingam, aka Kutty Shawn, halfway around the world over the summer. Kasilingam was located in Kuala Lumpur on Aug. 26 and "arrangements were made to return him to Toronto," Det.-Sgt. Stacy Gallant said Friday, explaining an RCMP liaison in Malaysia and the Canadian Border Services Agency helped with the 28-year-old murder suspect's extradition. Postmedia Network (Toronto Sun, A4)

Span, staff settle strike

A nearly three-week strike by toll collectors and other workers at one of Oanada's busiest border crossing ended Friday when the 47 workers at the Blue Water Bridge voted to accept a new contract deal. The agreement with the striking workers, members of the Public Service Alliance of Canada, was reached a day earlier following a day of bargaining by the union and the Federal Bridge Corp., with a conciliation officer. London Free Press, A7

Where Is Timloh (Butchang) Nkem
Two years ago, Timloh (Butchang) Nkem just disappeared. He'd been convicted of rape and was supposed to appear in Saskatoon Court of Queen's Bench for sentencing arguments on Oct. 31, 2014... Court was adjourned with the sense that the worst had happened: A convicted rapist who was allowed to remain out of custody pending his sentencing had fled... Danyliuk decided Nkem could be managed in the community and would return to court for his sentencing. He released the rapist on the same conditions he had been on since he got bail in 2013, including showing up to court when expected and surrendering his passport to the court if it were ever returned by border services... Then it took seven weeks for Saskatoon city police to post Nkem's photo to the wanted section of the police website... A Canada wide arrest warrant was also issued and applications were made for an "Interpol Red Notice." It means the province committed to have Nkem extradited if he is arrested in a foreign country that has an extradition treaty with Canada... The Canada Border Services Agency (CBSA) seized Nkem's passport and retains all travel documents until a person is deported, an agency spokesperson confirmed by email... Canada and the United States currently exchange entry information on foreign nationals; entry into one country serves as an exit record from the other but only if the person enters the United States by land. That means the CBSA has no exit records for people who leave Canada by air, travelling through a country other than the United States. Postmedia Network (Leader-Post, D1; StarPhoenix)

Canadian officials ask U.S. residents to leave guns home
Canadian officials are asking Alaska residents to leave their guns stateside before travelling. The Canadian Border Service Agency seized about 300 undeclared firearms from travellers in 2015, with more than half coming from travellers crossing into Canada from Alaska, The Ketchikan Daily News reported earlier this year. "Many of these travellers faced criminal charges and/or a monetary penalty that could have been avoided by simply declaring the guns," read an announcement from the agency. Whitehorse Daily Star, 10

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Fintech as a Force for Social Good**
For enterprises concerned about network security, identity verification has become a top-of-mind issue in an era of ubiquitous cyber-crime. But for millions around the world with no valid identification, standard computer access and identity authentication measures such as passwords pose a formidable barrier to not just public services, but also to the formal economy and traditional financial institutions. Postmedia Network (National Post)

*** Students in province to become 'Cyber Patriots' to battle hackers**
A worldwide search for the next generation of cyber-security experts landed in a New Brunswick high school on Friday. A quartet of Grade 12 students at Hillsborough's Caledonia Regional High School spent the day warding off virtual attackers targeting a hypothetical company's computer system as part of a multinational contest called Cyber Patriot IX. The contest is hosted by the United States Air Force Association which hopes to recruit new talent through it for the flourishing industry. Telegraph Journal, A7

*** It's online scam season and 'the phishing is good'**
As Christmas approaches, experts suggest an extra dollop of caution before clicking on email package delivery notices. Fake notifications are proliferating, bringing not holiday cheer - but holiday ransomware. The holiday phishing season began just before U. S. Thanksgiving and will likely extend until after Christmas, said Caleb Barlow, vice-president for IBM Security. "This is a US$445-billion business. These are campaigns, run by the criminal equivalent of marketers," he said. Security company FireEye sees a significant increase in fake package email alerts beginning in November, an almost 100 per cent increase from the average of September-October. USA Today (Winnipeg Free Press)

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Mountie sues over stress suffered in child-sex unit**

An RCMP officer has filed a lawsuit alleging he nearly suffered a nervous breakdown after being assigned to a child sex offences unit in Surrey. Const. Michael Wardrope says he was exposed to too much child pornography and claims the conduct of his superiors amounted to intimidation and harassment and resulted in him suffering from post-traumatic stress disorder. Wardrope, who became a Mountie in January 2007 and is a resident of Maple Ridge, says in the lawsuit filed in B.C. Supreme Court that in 2009 he was recruited to the child abuse and sexual offence unit... Wardrope says his health was deteriorating and his mental health was affected by unforgettable images and memories from the files he had worked on and he was never offered a debriefing in the entire period he was in the unit. Postmedia Network (Vancouver Sun, A23)

*** Investigation clears RCMP officers of any wrongdoing in shooting death**
An investigation has cleared Morinville RCMP officers of any wrongdoing in the 2015 shooting death of a man with a "history of significant mental illness and conflict with the law." In a detailed report released Friday, the Alberta Serious Incident Response Team found the officers involved were "acting lawfully and the use of force was reasonable and justified in all the circumstances." The incident happened May 22, 2015, when Mounties attended a rural home near Morinville after receiving a 911 call from a family member who was concerned for their safety. Postmedia Network (Edmonton Sun, A10; Edmonton Journal; Calgary Herald)

*** Police did as trained, inquest told**
An inquest into the 2008 police shooting death of an indigenous man in Winnipeg - the first in Manitoba to specifically consider the role of racism - heard from its final witnesses Friday. Two officers responsible for use-of-force training with the Winnipeg Police Service and the RCMP said the police who shot Craig McDougall acted appropriately, and bias-free police training wouldn't have changed the outcome. Patrol Sgt. Julio Berzenji, co-ordinator of the police officer safety unit, said officers are trained to make preservation of life their priority, so getting to the stabbed person they believed was in the house was their goal. Winnipeg Free Press, B2

*** The cost of accountability: Can Canadian police services afford body cam technology?**
One of the clearest conclusions following the recent Toronto Police Service pilot project of body-worn cameras was how positive the public felt about them. A police commissioned survey found 95 per cent strongly supported the idea and 85 per cent of the police officers involved agreed, according to Insp. Michael Barsky who led the program, adding many officers didn't want to give the cameras back at the end of the pilot. Less clear was the cost. A report following the pilot project pegged the price tag at $85 million over 10 years. But Barsky concedes, while the technology may be the wave of the future: "I don't know if that means today, though. It may mean that we need this to mature a little bit more." It seems that's the conclusion this week by the RCMP following a feasibility study. The national police force would have been the largest to don body-worn cameras. A statement said the study found the technology wasn't ready for the realities of RCMP policing... RCMP officers are disappointed, but not surprised, said Sgt. Brian Sauvé, on leave from his position on the force to co-chair the National Police Federation. "They're probably making the right decision," said Sauvé. He notes officers across the country were alarmed to find out police involved in the Toronto pilot project were spending as much as two hours dealing with video at the end of the day. He said the RCMP is already wrestling with budget constraints and out-of-control over-time costs. The RCMP is just the latest police service to abandon body cams — at least for now. Edmonton and Vancouver police services have also agreed to shelve the idea following concerns over price. CBC News

Nearly half of B.C.'s most expensive homes secretly owned
Critics say the B.C. government must work to close loopholes that allow homeowners in the province to hide their identities behind false fronts such as shell companies. NDP housing critic David Eby and Green MLA Andrew Weaver called for changes after reading about a Transparency International report that slams Canada for failing to close loopholes that allow homes to be owned through shell companies, trusts and nominees. The report shows almost half of Vancouver's 100 most expensive houses were bought using shell companies or other methods that obscure the identity of the owners. Report author Adam Ross found that use of tactics to obscure ownership has increased in the past five years in B.C. He also concluded the prevalence of opaque ownership in B.C. luxury real estate makes it impossible to measure

how much offshore cash is invested in B.C. homes, even though B.C. is attempting to collect data on foreign ownership... "Though Canada is not known as a global hub for money laundering and tax evasion, our legal framework and lax enforcement environment make it easy for individuals to misuse private companies and trusts," [the report] says. "Anonymous companies and trusts are the getaway cars of financial crime. ... Canada is an increasingly attractive destination for those looking to park and invest the proceeds of crime."... The report highlights lawyers are exempted from reporting to Canada's anti-money laundering agency, Fintrac, under a 2015 Supreme Court of Canada ruling. Canadian lawyers won the case by arguing that attorney-client privilege prevented them from reporting transactions to Fintrac. One of the case studies in the Transparency International report suggests lawyers are often central to money-laundering schemes... Ross said that he believes the federal government must find a way to include Canadian lawyers in Fintrac reporting, or many of the loopholes his report reveals, will remain open. Postmedia Network (Vancouver Sun)

'Common sense legislation'

The grieving widow of a murdered RCMP officer made an emotional plea Friday in St. Albert, calling on the federal government to not let partisan politics get in the way of public safety... Wynn's husband, Const. David Wynn, was shot and killed outside of a St. Albert casino in January 2015 by Shawn Rehn, a man wanted on numerous outstanding warrants. Rehn was granted bail a month earlier despite facing 29 Criminal Code charges. In response, a federal bill was drawn up to close a loophole in the law that allows bail hearings to take place without requiring a full disclosure of the applicant's criminal history, something Wynn believes may have prevented the murder of her husband and the wounding of auxiliary Const. Derek Bond during the same encounter... The bill, first proposed by Conservative Sen. Bob Runciman, passed swiftly through the Senate, finding support from both Liberals and Conservatives, and was unanimously supported by the Senate legal and constitutional affairs committee. But Liberal MPs, including federal Justice Minister Jody Wilson-Raybould, have since said they will not support the bill, claiming it will cause delays in an already backlogged bail system as criminal history is collected. Postmedia Network (Edmonton Sun, A4; Edmonton Journal); Postmedia Network (Guardian; Telegram)

RCMP give computers to Eskasoni students - but there's a catch

Students in Eskasoni, N.S., were excited to be given new computers yesterday - but they may not be allowed to keep them. It's part of the national Connecting Kids with Cops through Technology program that helps local RCMP officers sit down with elementary and middle-school children to work on projects. If the 27 students complete the workshops, they can keep the computers. CBC News

* **Hot on the trail**

An RCMP dog and his handler followed a scent that started near a Cornwall break-in to where the alleged "screencutter" parked his car, a judge heard Friday in provincial court. That was part of the testimony during the fourth day of Richard Joseph Arsenault's trial before Chief Judge Nancy Orr in Charlottetown. Arsenault is on trial for 17 charges, including numerous break and enters. The court heard from Cpl. Marc Periard, one of the RCMP's dog handlers in P.E.I. In August, Periard was the province's only dog handler, and he testified that Charlottetown Police Deputy Chief Brad MacConnell asked him to go to Cornwall where Arsenault had been spotted... The court also heard from RCMP Cpl. Shaun Brown who compared a shoe impression left at the scene of the Cornwall break-in to sneakers the police seized from Arsenault. Guardian, A4

Project Red Ribbon resumes

As part of Project Red Ribbon, Mothers Against Drunk Driving (MADD) Whitehorse and the Yukon's chief coroner will join RCMP tonight as they conduct impaired driving enforcement check-stops on Whitehorse roads. Project Red Ribbon is an annual holiday campaign that raises awareness of the dangers of impaired driving... With more frequent traffic stops planned for the coming weeks, Yukon RCMP are also asking motorists to slow down and move over if possible when approaching emergency vehicles that have their flashing lights on. Earlier this week, two Whitehorse RCMP officers were waiting roadside on Two Mile Hill for a suspected impaired driver's vehicle to be towed. Whitehorse Daily Star, 7

Family of man who died in Toronto police Taser incident speaks out

On the morning of November 4, Rui Nabico awoke in his family home on Sagres Cres., in a quiet residential corner of the city's northwest. He spoke to his parents before they left for work and, according to his sister, "all was perfectly normal." Hours later, the family would learn there had been a serious incident involving police on their street. Officers were called after reports of a man brandishing two knives and screaming. After a Taser was deployed, a 31-year-old man died. It was Nabico... Nabico's death has also prompted larger questions about the safety of Tasers, with some critics saying his death is a tragic reminder that the health risks of conducted energy weapons are still not understood. Pat Capponi, co-chair of the Toronto police services board mental health sub-committee, told the Star justdays after Nabico's deaththat his fatality "contradicts assurances that Tasers don't kill." Toronto Star

*** A'burg cops deploy less lethal weapon to minimize casualties**
Amherstburg police officers are now armed with beanbags. The police department is the first in Ontario to arm all frontline officers with shotguns that fire a "lesslethal projectile" that looks similar to a beanbag. The service made the move to be "more progressive" after also becoming the first Ontario police service to make body-worn cameras standard equipment for frontline officers early this year. "This is another tool on our belt when it comes to less lethal," said Const. Shawn McCurdy. "It gives us another option if you're engaging somebody who is assaultive and there is time and distance on our side." Officers have been receiving training with the projectiles and the "sock guns" that fire them, over the last month. McCurdy said all of the police service's seven patrol cars have one of the guns. Toronto police also have the beanbag guns, he said, but they're not fully deployed. Postmedia Network (Windsor Star, A2)

*** Organized crime suspect turns himself in**
Police have arrested another suspect as part of an investigation into an organized crime group active in Alberta, British Columbia and Manitoba. Calgary police say Andrew McGuire has turned himself in. McGuire and nine other people face drugs, firearms and organized crime charges. Earlier this week police announced the arrest of Timothy Varga - who police allege is the central figure in the criminal network. Varga faces multiple charges including recruiting members for a criminal organization. Red Deer Advocate, A10

Mississauga man charged in counterfeit goods probe
Toronto police say a Mississauga man is facing charges as a result of an investigation into the sale of counterfeit merchandise. Investigators say they received reports from the public about personal safety incidents involving recently purchased merchandise, including skin irritations and products overheating. They say the merchandise was traced to three businesses - Lucky's Import and Wholesale, Beach GLO and Jazz Casuals. All three locations were searched and police say officers seized 16 trucks of evidence worth an estimated $2.5 million... Police say two other people face immigration-related charges. Toronto Star (Record, A7); Postmedia Network (Toronto Sun)

When the case doesn't close: tales from the Toronto police cold-case unit
More than 500 cold-case files haunt the Toronto police major crimes unit like unfinished business. It's Det.-Sgt. Stacy Gallant's job not to forget about them - and he won't, if the victims' families have anything to say about it... The majority of the files are "DNA case" crimes, such as sexual assault and murder, where DNA would normally be found at the scene. But for the cases that stay cold, not a trace was recovered. And where DNA evidence is found, it isn't always the breakthrough that crime television shows lead viewers to believe. Gallant says that DNA samples merely read like a random set of numbers if they don't match any that are stored in the national DNA data bank. Even a positive ID can fall through for several reasons, according to Gallant... Canada's DNA data bank contains the blood, saliva and hair of roughly 266,000 people who have been convicted of a crime. The DNA is harvested after conviction, not upon arrest, which Gallant and RCMP Commissioner Bob Paulson have argued would help solve more crimes faster. CBC News

Un homme de Bécancour interpellé par les policiers
Un septuagénaire résident à Bécancour a été interpellé dans le cadre d'une opération en lien avec la contrebande de tabac, mercredi, alors qu'il se trouvait dans un véhicule circulant sur l'autoroute 20 est près de la sortie 138 à Saint-Hyacinthe. L'individu en question fera face à des accusations en vertu de la Loi concernant l'impôt sur le tabac. Lors de son interpellation, les policiers ont aussi procédé à une

perquisition dans le véhicule et y ont saisi 224 sacs de type Ziploc contenant 200 cigarettes chacun et 1095 $ en argent comptant en devises canadiennes. Cette opération, qui découle d'une enquête amorcée en 2016 à la suite d'informations reçues du public, a mobilisé trois policiers de la division des enquêtes sur la contrebande de tabac. Le Nouvelliste, 9

*** Jonathan Bettez traqué par la SQ**
Les policiers de la Sûreté du Québec (SQ) ont mené une traque intensive contre Jonathan Bettez et trouvé des traces de fichiers de pornographie juvénile dans ses possessions, révèlent des documents judiciaires rendus partiellement publics à la demande d'un consortium de médias. L'homme de Trois-Rivières, qui a été rencontré pendant l'enquête sur la disparition de Cédrika Provencher, a été surveillé étroitement après son arrestation pour possession et distribution de pornographie juvénile, le 29 août. La SQ a installé un GPS sur sa voiture, effectué de la surveillance physique et perquisitionné sa résidence et son lieu de travail à son insu, rapporte ICI Radio-Canada. La surveillance a permis de découvrir qu'une des adresses IP utilisées par M. Bettez a servi à télécharger des fichiers qui pourraient être de la pornographie juvénile. Le Devoir, A8; La Voix de l'Est; Le Nouvelliste (Le Quotidien; Le Nouvelliste); La Tribune; Le Soleil; La Presse

*** Professeur accusé de leurre informatique**
Un enseignant de mathématiques suppléant de la commission scolaire de la Capitale et de la commission scolaire des Premières-Seigneuries, Marc-Olivier Cloutier, 26 ans, a été accusé de leurre informatique après une perquisition menée à son domicile de Sainte-Foy jeudi. Cette perquisition a également permis aux policiers de mettre la main sur de la pornographie juvénile. Le Soleil (Le Soleil, 24; La Voix de l'Est; Le Quotidien)

*** Edmonton man charged with sex trafficking woman across the Prairies**
Police say an Edmonton man is facing a list of charges related to firearms and human trafficking for allegedly forcing a woman to work in the sex trade. Police arrested Prince Opoku, 25, following an investigation into his alleged connections to the sex trade. It's alleged he forced a woman in her early 20s to travel to cities in Manitoba, Saskatchewan and Alberta in order to work in the sex trade starting in early 2015. He is facing a variety of charges, including: procuring, trafficking in persons, material benefit from sexual services, advertising sexual services, knowingly possessing an unauthorized firearm, and careless storage of a firearm. Postmedia Network (Whig-Standard, B1)

*** Saskatoon teacher faces child porn, sex charges**
A 39-year-old teacher at a Saskatoon high school faces child pornography charges after an investigation by the Saskatchewan Internet Child Exploitation unit. Rhett Jeffrey Lundgren, 39, is charged with two counts of arranging to commit a sexual offence against a child and one count of attempting to access child pornography, Saskatoon police announced Friday after Lundgren appeared in provincial court. He was released from custody on several conditions. According to a police news release, the ICE unit arrested Lundgren and executed a search warrant on Thursday, nine days after starting an investigation into the online sexual exploitation of children through social media applications. Postmedia Network (Leader-Post, A11)

*** RCMP looking for new information in 2007 murder of Portage grandmother**
RCMP re-visited the scene of Charlene Ward's death nine years ago and continued to encourage anyone who knows something about her last day to contact police. After bringing the case back into the public eye on Nov. 22, the RCMP's Historical Case Unit investigators visited the scene of Ward's Nov. 1, 2007 death in Portage la Prairie. Her death has been ruled a homicide. Winnipeg Free Press, 4

***Saddling up for the red serge**
The RCMP Musical Ride held its graduation ceremony, known as "Passing-Out," on Friday. Among the new graduates is Const. Mathieu Crousset, who says he's "very humbled to have this opportunity to represent the RCMP." The Musical Ride's mounties and horses are invited to perform at about 50 events a year in Canada and abroad. The equitation course, which teaches horsemanship, is the second-longest RCMP course, with only recruit training in Regina taking longer. As the newest graduates, these riders will

be among the official riders in the Canada 150 tour. We asked Const. Crousset a few questions. Postmedia Network (Ottawa Sun, A2)

*** 'Heroic' rescue**
Footage from the dashboard camera of an RCMP cruiser has captured the dramatic efforts to save a man overdosing on fentanyl. "The only word that I feel accurately describes it is 'heroes,' " said deputy commissioner Marianne Ryan, commanding officer for the Alberta RCMP. "Without regard for their own personal safety, they did what they were trained to do without hesitation." On Sept. 28, around 9:15 a.m., an Athabasca RCMP officer was waved down by two people in a black pickup on Hwy. 55. The female driver told the officer a 27-year-old man in the backseat was overdosing on fentanyl, the potentially deadly synthetic opioid... While the officer began attending to the man, a woman in another vehicle pulled up to report she had narrowly escaped being hit by the same truck. Recognizing the severity of the situation and understanding it would be at least 20 minutes until an ambulance could arrive, the officer and the woman loaded the unresponsive man into the back of the truck and performed CPR while the truck barrelled down the highway to the nearest hospital. Postmedia Network (Calgary Sun, A17)

***RCMP investigation of Winnipeg police HQ remains active**
The RCMP investigation into Winnipeg's police headquarters remains active as the two-year anniversary of the criminal probe approaches. Winnipeg Mayor Brian Bowman said the Mounties recently contacted the city to request additional information pertaining to their investigation of the $214-million police-HQ project, which was completed this summer after three years of delays, $79 million worth of cost overruns and two external audits... The Mounties launched a criminal investigation into Winnipeg's police headquarters on Dec. 17, 2014, when officers executed a search warrant at McGillivray Boulevard headquarters of Caspian Construction, the primary contractor on the city project. Court documents later revealed RCMP were looking into fraud and forgery allegations pertaining to the construction. The RCMP also raided the police headquarters itself in June 2015. Information used by the Mounties to obtain their initial search warrant also revealed former Winnipeg mayor Sam Katz received thousands of dollars in personal cheques from Caspian Construction. CBC News

*** Residential burglaries up 42% over last year in Richmond**
Richmond police say the city has seen a significant spike in burglaries in recent weeks - which they say is being committed largely by drug users looking to feed their habit. RCMP say residential burglaries were up 42 per cent between November and December 2016, compared to the same period last year. "We normally see a slight increase around this time of year," said Cpl. Dennis Hwang in a release. "However, our numbers are above normal, and we are tracking them carefully." RCMP say they are reassigning officers from other units to address the increase. CBC News

***RCMP launch holiday CounterAttack campaign**
Holiday season revelers are being urged to think twice before getting behind the wheel after a night on the town. The annual winter CounterAttack program is up and running. It means RCMP will be out in force, setting up roadblocks and generally keeping an eye out for drivers who've had too much to drink. "The Prince George detachment is committed to improving public safety," said Prince George RCMP Supt. Warren Brown. Prince George Citizen

*** Man wanted for assault, intimidation of witness in Fort McMurray**
Wood Buffalo RCMP are trying to identify a man who assaulted and threatened a witness to not testify at an upcoming trial. Postmedia Network (Edmonton Journal)

*** Saint John cocaine kingpin gets 11-year sentence**
It took police almost three years of investigation, the help of a covert agent who turned on his criminal partners, and more than two years of prosecution, but a Saint John-based cocaine kingpin has received an 11-year prison sentence. Shane Stephen Williams, the head of one of the criminal organizations targeted by Operation J-Tornado, was sentenced on Friday at noon. He was sentenced alongside his co-conspirator Joshua Eldon Kindred, with whom he shared a courtroom dock at trial between April and June. The Crown's key witness at trial is a former associate, friend and groomsman of Williams, who agreed to work with the RCMP for a payout of hundreds of thousands of dollars. His identity can't be

reported due to a publication ban, and he appeared in court with a heavy security presence. The agent had been providing Williams' crew with Army-level encrypted Blackberry devices that police couldn't crack. But police devised a plan for the agent to funnel similar new devices, that routed through an RCMP server and allowed officers to track their messages. Times & Transcript, B1

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** ATTEMPTED MURDERER RELEASED**
The mother of a shooting victim now confined to a wheelchair is devastated by the early release of his would-be killer. Mykel Smith shot Mike Patriquen point blank on Nov. 11, 2008, the bullet piercing the 25-year-old's lung and spine. He'll be in a wheelchair for the rest of his life. Smith received a nearly-13 year sentence for attempted murder after he and Sergio Bowers attempted to rob Patriquen of bracelets and a necklace he was wearing in his home. Smith was given day parole on Tuesday, less than halfway through his sentence... The board was not optimistic about Smith's prospects in society. "CSC is of the opinion that you will re-offend in a violent manner if your need areas are not addressed adequately," the document reads. "You are described as having no empathy, traits of narcissism, anti-social personality disorder and psychopathy; you are superfluously charming but have no real depth for any emotions." More recent assessments show an improvement in demeanour and attitude. He is said to have been involved in many programs in prison and achieved his GED. Stephen doesn't understand how the board let someone out they believed could be a risk to re-offend. Chronicle Herald, A7

*** Murder casts a long shadow**
There's a saying that time heals all wounds. But it's not really true. Some wounds can never be healed. Nearly 25 years ago, a solitary man named Patrick Dombroskie walked into the Ontario Glove factory in Waterloo. He had been suspended from his job as a leather cutter a few days earlier, for not doing his work properly. It was Feb. 3, 1992. Dombroskie, 28, carried a hunting rifle and 60 rounds of ammunition. He chose his victims carefully, while stunned colleagues hid or ran away. He killed Elizabeth Travassos, who was at work on the floor. He killed Greg More, co-owner of the company, and Larry Strack, a supervisor who, like Dombroskie, was from Barry's Bay, a small community 150 kilometres west of Ottawa. Then Dombroskie got into his car and drove away... Dombroskie was convicted of murder and sent to jail for life with no chance at parole for 25 years. That chance was denied at a hearing near Kingston last week. Toronto Star (Record, B1)

*** Un violeur trop dangereux pour être libéré de prison**
Léopold Boies, 51 ans, est tellement dangereux qu'il est impossible de le laisser sortir de prison, estime la Couronne qui demande de l'enfermer sans date prévisible de libération. La procureure aux poursuites criminelles et pénales, Me Nicole Ouellet, recommande au tribunal de le déclarer délinquant dangereux parce qu'il attaque des gens dès ses sorties de prison. Il est détenu préventivement depuis plus de deux ans pour avoir agressé sexuellement deux femmes après quelques semaines de liberté. Pendant sa plus récente incarcération, Boies a attaqué deux agentes des services correctionnels en leur lançant un seau de matières fécales. Les deux agentes ont dû être traitées préventivement contre une gamme de rétrovirus et d'hépatites. Agence QMI (Journal de Québec; Journal de Montréal); La Presse; Le Quotidien; Radio Canada

*** Le sort de Jacques Delisle entre les mains du juge**
Alors que la couronne soutient que le suicide est «impossible» dans le dossier de Jacques Delisle, les avocats de l'ex-juge demandent la libération de leur client, un homme qui a perdu «son honneur, sa réputation et sa liberté» après avoir été condamné sur une «preuve inexacte». Les parties ont présenté leurs plaidoiries hier au neuvième et dernier jour de l'enquête sur cautionnement de l'ex-juge, qui se dit condamné à tort pour le meurtre prémédité de son épouse. Le sort de Jacques Delisle, 81 ans, repose maintenant entre les mains du juge Benoit Moulin, qui devrait rendre sa décision d'ici les Fêtes. Agence QMI (Journal de Québec)

*** Contraband seized at Atlantic Institution**

A package containing 65 grams of marijuana was seized by guards at the Atlantic Institution in New Brunswick on Nov. 29. The estimated value of this seizure is about $10,000. The Correctional Service of Canada uses tools including ion scanners and drug-detector dogs to search buildings, personal property, inmates and visitors. Such activities may be related to drug use or trafficking that may threaten the safety and security of visitors, inmates and staff members working at federal jails. Chronicle Herald, A4

*** Contrebande: iPad, Game Boys et vibrateurs saisis en prison**
Les agents des services correctionnels saisissent de tout dans les prisons québécoises, allant de l'alcool frelaté jusqu'à un banc de toilette en passant par une poivrière et de l'huile à massage. «C'est problématique. Oui, nous sommes pour la réinsertion des détenus, mais il faut aussi un encadrement», a réagi le président du Syndicat des agents de la paix en services correctionnels du Québec Mathieu Lavoie. Des documents diffusés par le ministère de la Sécurité publique du Québec montrent en effet que les articles de contrebande ne se limitent pas à la drogue, aux cellulaires et aux armes. Agence QMI (Journal de Québec; Journal de Montréal)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Rewards set to a maximum of $2,000
Crime Stoppers has had previous kicks at the can in the Yukon, Mayor Dan Curtis acknowledged Thursday, but he's optimistic about the program's recent re-launch... Crime Stoppers previously folded in the territory in 2011, when it was shut down due to a lack of community involvement. Last spring, the Yukon government contributed $21,000 to start-up costs for the program... Crime Stoppers can accept government money for administrative costs, but it must rely on donations to make up the reward money paid out to tips that result in arrests. When a Yukoner calls the tip line, the information they give is attached to a number, rather than the name of a person. The information is relayed to Yukon RCMP liaisons, who assess the information. RCMP Supt. Brian Jones said tips aren't enough to obtain warrants, but they give officers a starting point, or a new direction to investigate. They become, he said, "another piece of the puzzle." If the RCMP determine a tip has contributed directly to solving a crime, they tell the Crime Stoppers board. The board then pays out the tipster. Whitehorse Daily Star, 2

Un fraudeur de personnes âgées condamné à cinq ans de prison
Un homme de 31 ans qui a arnaqué des dizaines de personnes âgées de Montréal a été condamné jeudi à cinq ans de prison pour fraude, complot de fraude et trafic de bien criminellement obtenus. André Westerhout faisait partie d'un réseau criminel spécialisé dans les fraudes «grands-parents» démantelé par les policiers ce printemps. Le Nouvelliste, 12

*** Drug death 'didn't need to happen'**
Two of Winnipeg's most important advocates for our most vulnerable people lined up at city hall this week in a way we normally associate with their homeless and often substance-addicted clients. With their hands out. Siloam Mission was asking for $2 million. Main Street Project, which provides the drug treatment Siloam doesn't, was all but begging for $70,000 more. By comparison, the facility once known callously as "the drunk tank" was asking for spare change; a mere pittance of an increase to the city's long-standing allotment of $96,000 toward Main Street Project's 34-bed Mainstay Residence. But Thursday, when the shelter's executive director, Rick Lees, spoke in front of Mayor Brian Bowman and his executive policy committee members, he wanted to stress why the money is so desperately needed in a way they would understand not just as politicians, but as people. Winnipeg Free Press

*** Lighthouse funding shortfall means more people in jail cells**

Saskatoon police Chief Clive Weighill says the decision to cease funding to the stabilization unit at the Lighthouse has meant more intoxicated people are again ending up in police cells. In September, the province ended partial funding for the 38-bed unit that provides emergency shelter for people who are intoxicated by drugs or alcohol. Such people are not typically allowed into other emergency shelters. Weighill said many of them are now ending up back in police cells. Postmedia Network (StarPhoenix, A3)

***Councillors bicker over funding while fentanyl kills two a day**
For Vancouver city councillor Geoff Meggs, raising property taxes to help stem the current overdose crisis is a complete nobrainer. His argument goes like this: First responders such as firefighters and police are funded with property taxes; there is unprecedented pressure on those first responders because of the number of people overdosing on fentanyl; and so when more resources are needed to support those emergency services, property tax is the obvious source. Globe and Mail, S1

*** It's about to get easier to set up supervised drug injection sites in Canada**
As the number of Canadians dying from opioid overdoses continues to grow, the federal government is preparing to make it easier to open supervised drug injection sites. Federal Health Minister Jane Philpott is set to bring forward on Monday proposed legislation to make changes to the Controlled Drugs and Substances Act. For months, Philpott has been facing pressure to speed up the process to open new sites, where addicts use intravenous drugs in a safe and medically supervised environment. B.C. in particular has been vocal. The province has seen hundreds die from drug overdoses this year alone, and provincial officials have labelled the opioid crisis a public health emergency. CBC News

***Police chief backs safe-injection sites for Edmonton**
Edmonton police Chief Rod Knecht says he's in favour of a plan to open four safe-injection sites in the city. "We, Edmonton, have an opportunity to get it right," Knecht said after visiting safe-injection sites in Vancouver. "I think we can build a safe-injection site that serves everybody's needs in the broader community." An advisory committee for medically-supervised injection sites presented a report to city council on Monday, asking councillors for support. Coun. Dave Loken said it is something the city should have done long ago. Couns. Scott McKeen and Bev Esslinger agreed. At the same meeting, the city's community and public services committee unanimously supported four injection sites in Edmonton - one at the Royal Alexandra Hospital and three others in existing community organizations. CBC News

*** Public health gets green light to study bringing safe injection sites to town**
City councillors have given public health the green light to study the possibility of bringing safe injection sites to Hamilton. The pitch for such a study was first made to the Board of Health earlier this year, in light of a deadly opioid crisis that has led to a spike in overdoses across the country... The Hamilton study was initially estimated to cost $250,000, but after some councillors expressed concern about the cost, public health staff established a partnership with McMaster University to get that cost down to $92,000. Hamilton Spectator

*** Winnipeg called strong for inclusion of Muslims**
With a rise in anti-Muslim hate crimes and divisive rhetoric in Canada and the United States, the National Council of Canadian Muslims is training youth to be more media-savvy - and thinks Winnipeg can teach the rest of the country a thing or two. Today, the non-profit human rights and advocacy group is holding a workshop in Winnipeg, the last stop on a four-city tour that includes Montreal, Ottawa and Calgary. The plan is to help young people identify stereotypes in popular culture related to Islam and Muslims and to learn how to counter them by sharing their own stories, said organizer Amira Elghawaby in Ottawa. She said Winnipeg has fewer anti-Muslim hate crimes reported than most Canadian cities, and the council wants to learn why. Winnipeg Free Press

*** Police Odd Squad Enjoys Financially Fruitful Evening**

Composed of off-duty police officers, the Odd Squad Productions Society reportedly raised over half its $100,000 basic budget at a party in the Imperial Theatre. That Main-off-Hastings facility is located in what Vancouver Chief Constable Adam Palmer calls "arguably the most challenging beat in Canada." It's where Odd Squad officers have produced 20 documentary films and many youth-oriented drug-and gangeducation programs. Vancouver Sun, G2

*** Pharmacists urge government to expand addiction treatment**
New Brunswick's pharmacists are urging the government to devote more resources to drug addiction treatment, as the province prepares to roll out a prescription monitoring program. Paul Blanchard, executive director of the New Brunswick Pharmacists' Association, says pharmacists aren't sure where to refer people who will be identified through prescription monitoring as abusing their medication. CBC News

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Auditor raps B.C. for stopping progress reports on missing women programs
British Columbia's auditor general rapped the province Thursday for dropping its public progress reports on a commission of inquiry that reviewed the disappearances of 67 women - some of them victims of serial killer Robert Pickton - from Vancouver's Downtown Eastside. Carol Bellringer said the tragedies continue to affect families and communities, and the government must keep British Columbians informed of its progress in meeting more than 60 recommendations from the inquiry. She said the government stopped public reporting in 2014, two years after former attorney general Wally Oppal tabled his report. Whitehorse Daily Star, 18

*** How to make a 'nation-to-nation' relationship genuine**
An opinion piece states, "The dispute over the North Dakota Access pipeline has been resolved, but the months-long protest by the Standing Rock Sioux has already served as a beacon to First Nations of Canada feeling the aggravation of their accumulated injuries - the Missing and Murdered Indigenous Women and Girls, Laloche, Val d'Or, Grassy Narrows, the Site C Dam, the Trans Mountain pipeline - and for this Canada has only itself to blame..." Toronto Star

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** High-flying pot stocks could soon be in the weeds**
The surge of capital into Canada's nascent marijuana industry has sent stock prices soaring - and brought warnings it's a bubble that could soon burst. The value of 26 marijuana stocks listed in Canada has swelled to almost $4 billion from close to nothing in the past two years, as investors rushed to bet on the country's move toward legalizing recreational use... How Ottawa will regulate, tax or distribute the products remains unknown, and some of the publicly traded companies have yet to make a sale. "Oh, they're going to pop," Nick Brusatore, the largest shareholder of Affinor Growers Inc., said by phone. Once a mining company, the Vancouver firm now develops greenhouse technology for crops, including cannabis. "It's going to pop hard." Bloomberg News (Winnipeg Free Press)

*** Chief right to put pot shops on notice**
An editorial states, "Saint John police Chief John Bates is right to have the city's two marijuana-selling dispensaries "in our radar screens." Simply put: the law is the law, until it changes. There is little wisdom in speculating on how it might change in the future, and adjusting enforcement in the present on the basis of that speculation. Such a speculative standard would surely be rejected even by those who advocate increased access to marijuana. Laws are enforced as they are, not as they might someday be. And there is no court ruling suspending the current legislation -- as has been a factor in some circumstances when police choose to turn a blind eye. If the chief of police believes, as he's said, that the city's two storefront pot-sellers are operating outside of the bounds of the law, it's his force's job to enforce that law. Prime

Minister Justin Trudeau's clear support, in evidence from comments he made this week, is certainly helpful, but the ultimate standard is the law on the books..." Telegraph Journal, A11

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Feds, union near deal for 5% hike over 4 years**
The federal government and the union representing professionals working in the public service wound up three days of contract talks early Friday morning with what some say are the makings of a tentative deal that could boost salaries by five per cent over four years. The Professional Institute of the Public Service of Canada, which had publicly resolved to have a contract deal by the end of the year, appears to have broken the logjam that has dogged negotiations for more than two years. Union and Treasury Board negotiators met until early Friday morning, when they wrapped up discussions for three of the union's bargaining groups. Two other groups return to bargaining today for another session. Ottawa Citizen, A3

*** MP backs payroll protesters**
Approximately 80 members of the Public Service Alliance of Canada staged a noisy protest on Friday afternoon in front of Kingston and the Islands MP Mark Gerretsen's Princess Street office over the beleaguered Phoenix pay system. But what the protesters may not have known is they were preaching to the converted. "I'm behind them." Gerretsen said in an interview on Friday afternoon a few hours before the protest. Whig-Standard, A4

OTHER / AUTRE

*** Journalists seek asylum in Canada amid Turkish crackdown**
In March, shortly after the Turkish government took over Zaman, the country's best-selling English daily, the paper's political writer Arslan Ayan lost his job. In the days after a short-lived failed coup on July 15, more media outlets were shut down with more journalists arrested and jailed. Fearing repercussions from his critical writings of the regime, Ayan fled Istanbul to stay at his parents' home in a small Turkish town. On August 1, he said, police came to the house and seized his books and computer. By the time his neighbours saw the return of the authorities the next day, Ayan had made it back to Istanbul to find a way out of Turkey. With a still-valid U.S. visa, he flew to New York on August 5 to join a contingent of Turkish journalists seeking protection abroad, and arrived Toronto via Montreal on October 10. Ayan is among at least 15 Turkish journalists who have fled to Canada in the last few months seeking asylum. Many have fled to Africa, to countries like Chad and Tanzania where visas are not required. Toronto Star

Dreaded 'Month 13' looms for newcomers
Bedrettin Al Muhamad and his wife, Mariam, have been taking English classes and making every effort to immerse themselves in Canadian culture since arriving here from Turkey in February... But the honeymoon will soon be over... For many of the 35,000 Syrians who have arrived in the country - 15,000 in Ontario - since Canada started bringing in planeloads of newcomers last Dec. 9, what is commonly known in the refugee resettlement circle as "Month 13" is looming. After a year of being warmly welcomed into communities across the country, the 12-month financial commitment to these refugees by Ottawa and private sponsorship groups will start to come to an end. Many of the adult Syrian newcomers will be faced with the reality of choosing between quitting English classes, working or living off provincial welfare - an income that is less than the meagre resettled refugee assistance they currently receive from the federal government. Officials estimated half of the privately sponsored refugees and 10 per cent of those supported by the government would have employment income in their first year. Toronto Star, A1

Solidarité - Plus de 7000 réfugiés syriens attendent de venir au Québec
Sprint final ; la ministre québécoise de l'Immigration promet que quelque 400 réfugiés syriens vont arriver d'ici le 31 décembre, ce qui permet d'atteindre la cible de 7300 pour 2015-2016. Or, la priorité sera donnée aux réfugiés pris en charge par l'État et non aux réfugiés parrainés au privé par des familles québécoises, qui devront prendre leur mal en patience jusqu'en 2017. Encore très nombreux, 7705

Syriens parrainés au privé, et qui ont été acceptés, attendaient toujours de prendre un avion pour le Québec en date du 8 décembre. Le Devoir, A8

CANADA MUST LEARN TO INTEGRATE REFUGEES

An opinion piece states, "Syrian refugee Assam Hadhad's story is bittersweet. The bitter part was fleeing his war-ravaged country with his family, leaving behind the chocolate factory it took him 30 years to build. The sweet part is that in August, only seven months after he landed in Canada, he opened a new chocolate shop in tiny Antigonish, N.S... Still, while Hadhad's example is inspiring - Prime Minister Justin Trudeau shared it when he visited the United Nations - it is not representative of the harrowing stories of most of the 35,745 Syrian newcomers who have arrived in Canada over the past year. Indeed, this past week the Senate rang a cautionary bell, suggesting in a report that the federal government is not doing enough to support them. It landed only days before the Dec. 10 anniversary of the arrival of the first wave of 25,000 Syrian refugees that Trudeau had promised would land before the end of February. "We can't abandon them," said Sen. Jim Munson. "We can't let indifference set in. We need to help them in their next resettlement steps." Among the report's recommendations: The federal government must boost access to language training, provide daycare so that parents can attend classes, increase mental health supports for those who suffer from post-traumatic stress disorder, and work with the Canada Revenue Agency to make sure refugees quickly qualify for the Canada Child Benefit..." Toronto Star

Most Syrian refugees taking English classes, few find work

More than threequarters of the Syrian refugees in B.C. have been able to access English classes, but just 17 per cent have been able to find work in the year since they arrived, according to a report released Friday. The Immigrant Services Society of B.C. surveyed 300 Syrian refugee families by phone and 60 Syrian refugee youths last month. All of those interviewed were government-assisted refugees who arrived in Metro Vancouver between Nov. 4, 2015 and Feb. 28, 2016. Those surveyed overwhelmingly expressed their gratitude to Canada and its people for taking them in. They were particularly happy with their children's experience in the school system. Times-Colonist, A5; Globe and Mail

Lawyers seek aid for Hong Kong refugees

A group of Montreal lawyers is urging the Canadian government to help impoverished asylum-seekers in Hong Kong who say they have faced harassment for having housed whistle-blower and U.S. fugitive Edward Snowden. The lawyers have launched a Canadian organization named For the Refugees to raise money for the families and to lobby Ottawa to give them sanctuary as they come under pressure in Hong Kong - a jurisdiction known for being tough on asylum-seekers. Since the refugees' involvement with Mr. Snowden rose to global prominence this fall - including in scenes in a recent Oliver Stone film on the fugitive - they say they've been questioned on Mr. Snowden by welfare authorities, seen welfare benefits cut and had visits from police. Globe and Mail, A16

STANDOFF

Melina Laboucan-Massimo, a Lubicon Cree, grew up in Alberta's oil country. Since the age of 7, she has joined blockades and protests aimed at protecting her community's traditional lands from resource development. "I was born into it," she said in an interview. "It's my inheritance."... The high-profile protest at Standing Rock against the Dakota Access Pipeline has galvanized Canadian indigenous communities, who watched as one community stood up against an oil company and its powerful backers. The Standing Rock tribe was empowered by thousands of allies - indigenous and non-indigenous alike - who flooded into the area from both sides of the border to stand with the Sioux. They faced threats of rubber bullets, attack dogs and water cannons in frigid weather. Now, some indigenous leaders are pledging to use the tactics of Standing Rock to block the two pipeline projects approved last week by the Liberal government: the bitterly fought expansion of Kinder Morgan's line that runs to Vancouver Harbour, and Enbridge's lessernoticed plan to rebuild and expand its Line 3, a main oil export line from Alberta to the U.S. Midwest. Globe and Mail, F1

A bishop's quest

The millions in ransom money came in dollar by dollar, euro by euro from around the world. The donations, raised from church offerings, a Christmas concert, and the diaspora of Assyrian Christians on Facebook, landed in a bank account in Iraq. Its ultimate destination: the Islamic State of Iraq and the

Levant (ISIL) group. Deep inside Syria, a bishop worked around the blurred edges of international law to save the lives of more than 200 people - one of the largest groups of hostages yet documented in ISIL's war in Syria and Iraq. It took more than a year, and videotaped killings of three captives, before all the rest were freed. Paying ransoms is illegal in most of the West, and the idea of paying the militants is morally fraught, even for those who saw no alternative. "You look at it from the moral side and I get it. If we give them money we're just feeding into it, and they're going to kill using that money," said Aneki Nissan, who helped raise funds in Canada. But, he said, there were more than 200 lives at stake, "and to us, we're such a small minority that we have to help each other." Postmedia Network (Edmonton Journal, B1)

*** HMCS Kingston returns to Halifax in time for Christmas**

The Royal Canadian Navy welcomed HMCS Kingston home after a two-month deployment with a special homecoming ceremony in Halifax Friday. The vessel participated in Operation Caribbe, which is Canada's contribution to Operation Martillo, a U.S.-led multinational effort by Western and European nations to prevent illicit drug trafficking in the Caribbean Sea, eastern Pacific Ocean and the coast of Central America. This week also marked 10 years of participation in Martillo for Canada. According to a news release issued by the Department of National Defence, since 2006 the Royal Canadian Navy and the Royal Canadian Air Force have supported the seizure or disruption of more than 66 metric tonnes of cocaine and just under four metric tonnes of marijuana. Just in the past year, Canada directly contributed to the seizure or disruption of 5,750 kilograms of cocaine and 1,520 kg of marijuana. Chronicle Herald

INTERNATIONAL

*** French government seeks extension of state of emergency**

French Prime Minister Bernard Cazeneuve says 17 attacks have been thwarted in the country so far this year and he is asking Parliament to extend the state of emergency until July 15. Speaking after an extraordinary cabinet meeting, Cazeneuve said Saturday that Parliament will vote on the bill next week. He said the extension for seven more months is "absolutely necessary" to ensure the highest possible level of protection in the country in the context of next spring's presidential and general elections. Associated Press (Metro News)

Russia intervened to elect Trump

The CIA has concluded in a secret assessment that Russia intervened in the 2016 election to help Donald Trump win the presidency, rather than just to undermine confidence in the U.S. electoral system, according to officials briefed on the matter. Intelligence agencies have identified individuals with connections to the Russian government who provided WikiLeaks with thousands of hacked emails from the Democratic National Committee and others, including Hillary Clinton's campaign chairman, according to U.S. officials. Those officials described the individuals as actors known to the intelligence community and part of a wider Russian operation to boost Trump and hurt Clinton's chances. "It is the assessment of the intelligence community that Russia's goal here was to favour one candidate over the other, to help Trump get elected," said a senior U.S. official briefed on an intelligence presentation made to U.S. senators. "That's the consensus view." Toronto Star, A30

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
December 17, 2016 / le 17 décembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Correctional investigator calls riot at P.A. prison 'devastating'
Canada's prison watchdog is investigating the deadly 24-hour prison riot that left one inmate dead and several others injured at Saskatchewan Penitentiary in Prince Albert. The riot started Wednesday afternoon, forcing the federal institution to lock down its medium and maximum-security units. Canada's correctional investigator, Howard Sapers, said his office has dispatched two staff members to collect information from the scene... Correctional Services Canada spokesman Jeff Campbell said lockdown procedures were still in place Friday and visitations remain cancelled. **CSC Commissioner Don Head was at the penitentiary on Friday to lend *"his support and assistance,"* according to a statement from the office of federal Public Safety Minister Ralph Goodale.** Star-Phoenix, A4; Postmedia News (Vancouver Sun); * Canadian Press (Cape Breton Post)

Halifax police test 'drugalyzers' before pot legalization
Halifax police are "happy to participate" in a project testing a new tool to nab suspected impaired drivers, Supt. Robin McNeil says. Canadian police forces may soon be armed with the "drugalyzers," as they've been nicknamed. They'll use those to test whether drivers are high from cannabis, opioids or other drugs. **Halifax Regional Police is one of several police forces across the country taking part in a national pilot project announced earlier this week by the federal public safety minister...** With the legalization of marijuana on the horizon, MADD Canada has been lobbying for the introduction of the devices here. Currently police officers are limited to drug sobriety tests, such as asking drivers to touch their nose or walk straight on a line. Some officers have specialized training to catch small movements of the eye as signs of drug impairment. CBC News; * Radio-Canada

Opioids, pot and economics: three ways politics touched Canadians this week
... The government has announced a two-pronged approach to confronting the opioid crisis. Health Minister Jane Philpott has tabled legislation that would give cities more leeway to open up supervised drug injection sites. The law would essentially remove the high bar set by the previous Conservative government, which required communities to meet 26 conditions in order to qualify. For now, there are only two safe injection sites in Canada, both in Vancouver. **At the same time, Public Safety Minister Ralph Goodale proposed measures to crack down on illegal drugs and their ingredients coming over the border.** Border guards would be allowed to examine very small suspicious packages and also restrict the import of equipment used to make drugs. In British Columbia alone, officials say there have been 622 fatal drug overdoses between January and October this year, of which about 60 per cent were linked to fentanyl. Canadian Press (Cape Breton Post)

Canada's federal jails may stop sorting trans inmates by their genitalia
Canada's federal prison system could soon scrap a longstanding policy of housing trans and intersex offenders based on their genitalia while effectively barring them from gender-confirming surgeries, Xtra has learned. Since at least 1999, Correctional Service Canada (CSC) has sorted trans inmates who haven't transitioned based on their genitalia... Scott Bardsley, a spokesman for **Public Safety Minister Ralph Goodale** says CSC is currently monitoring Bill C-16 — which is on track to add gender identity and gender expression to Canada's human-rights legislation — to see if it requires a change in federal prison policy. CSC houses all adult Canadians serving sentences of two years or more, representing about 40 percent of the almost 40,000 adult prisoners in Canada. The rest are in provincial and territorial jails, including people awaiting a trial or serving community sentences. Ontario and British Columbia jails have sorted inmates based on their self-identified gender since 2015. Daily Xtra

TOP STORIES / MANCHETTES

Martin Couture-Rouleau voulait tuer d'autres militaires
Le terroriste Martin Couture-Rouleau, qui a heurté à mort l'adjudant Patrice Vincent, le 20 octobre 2014 dans le stationnement d'un centre commercial de Saint-Jean-sur-Richelieu, s'en serait pris à d'autres militaires s'il en avait eu l'occasion. C'est ce que démontre la conversation qu'a eue Couture-Rouleau avec un préposé du 9-1-1 dans les minutes suivant l'attentat, dont des extraits se trouvent dans le rapport d'enquête du coroner André Dandavino sur le décès du militaire, rendu public vendredi. L'auteur du délit de fuite, pourchassé par les policiers après avoir heurté l'adjudant Vincent et un autre militaire qui a eu la vie sauve, a appelé le 9-1-1 pour, disait-il, « passer un message ». Il a alors refusé de se rendre, disant qu'il allait peut-être « croiser un autre de vos soldats » et qu'il allait « l'abattre. » Il demandait au service d'urgence « d'avertir le Canada, le gouverneur » et d'autres de quitter la coalition qui était opposée à « l'État islamique. » La Tribune, 14 (Le Nouvelliste; Le Droit); La Presse

Peace bond target denies terror links - British Columbia
The latest target of Canada's terrorism peace bond system insisted he has no connection to extremist violence and turned up at a B.C. police station to complain about press coverage of his case. "I throw your newspaper in the garbage," Khalid Ahmad Ibrahim, 39, told a reporter at the door of a New Westminster, B.C. apartment. "There is no terrorism," he added. The RCMP told the provincial court on

Dec. 8 there were "reasonable and probable grounds to believe. that Khalid Ahmad Ibrahim may commit a terrorism offence." He was released on $1,000 bail and must adhere to 25 bail conditions, including not accessing or viewing any materials related to a terrorist group. He was due back in court Dec. 20. Peace bonds are not a criminal charge but rather impose conditions on the conduct of those subjected to them. Police have been using them to control suspected violent extremists. Postmedia News (London Free Press, N4; Windsor Star; Montreal Gazette; Whig-Standard)

CSIS aware of terror suspect's flight while RCMP investigated

In 2013, while the RCMP were still investigating how a suspected terrorist had quietly left Canada to join ISIL the previous year, Canada's spy agency informed the Mounties they had in fact already known the intimate details of the terrorism suspect's final hours before he boarded a plane for Syria, new court records reveal. John Maguire left Canada in December 2012 to join ISIL in Syria, where he was featured in a propaganda video declaring religious war on his home country. The Islamic State reported Maguire died fighting in 2015, though his death has never been confirmed. Before he left for Syria, Maguire was the alleged star terrorism recruit of Ottawa's Awso Peshdary, 26, who was charged in February 2015 with recruiting, financing and facilitating terrorism. And the RCMP's case against Peshdary is where new details have emerged about the Mounties' investigation into an alleged Ottawa terror network. The RCMP's case that yielded charges against Peshdary, 26, was built on a foundation so shaky that investigators were twice turned down when they went to get search warrants against Maguire. Whig-Standard, B1

Obama warns Putin that US could strike back on cyber

President Barack Obama has put Russia's Vladimir Putin on notice that the U.S. could use offensive cyber muscle to retaliate for interference in the U.S. presidential election, his strongest suggestion to date that Putin had been well aware of campaign email hacking. "Whatever they do to us, we can potentially do to them," Obama declared Friday. Caught in the middle of a post-election controversy over Russian hacking, Obama strongly defended his administration's response, including his refusal before the voting to ascribe motive to the meddling or to discuss now what effect it might have had. U.S. intelligence assessments say it was aimed at least in part on helping Donald Trump defeat Hillary Clinton, and some Democrats say it may well have tipped the results in his favour. Associated Press (iPolitics; Chronicle-Herald); AFP (Le Devoir)

Thirteen deaths in one day linked to drugs - Cause of 'dangerous upsurge' in overdoses is unknown, coroner says

The B.C. Coroners Service has issued an urgent warning to illicit-drug users after an unprecedented number of drug overdose deaths in B.C. As many as 13 people died of suspected drug overdoses on Thursday, and Premier Christy Clark said the rising death toll is one of the most difficult issues she has faced this term. "I can't remember anything in the last four years that has felt like such a crisis - such an urgent crisis - where so many lives are being lost every single day, and that is so complicated to get our hands around," she said. Within eight hours, six people died after using drugs in Vancouver's Downtown Eastside, said coroner Barb McLintock. Two other deaths, at the same time, in the same area, are believed to be drug-related. Five other people died after using drugs on Thursday. The deaths occurred in Vancouver, Burnaby, northern B.C. and two in the Fraser region... Health Minister Terry Lake and Minister of Public Safety Mike Morris later said in a joint statement that the province expects to meet its goal of adding 500 substance-use beds by the end of March. The province has earmarked $43 million to respond to the crisis by expanding access to naloxone, establishing overdose prevention sites and working with the federal government to stop drugs from entering Canada. Times-Colonist, A3; Vancouver Sun; Globe and Mail; Canadian Press (Cape Breton Post); Le Droit; La Presse

Jusqu'à 38 000 doses de furanyl-fentanyl saisies à Ottawa

Un homme de 42 ans se retrouve derrière les barreaux après que les policiers de la Gendarmerie royale du Canada eurent saisi environ 19 grammes de furany-lfentanyl, une drogue mortelle. La perquisition a eu lieu dans le secteur d'Orléans, à Ottawa. Cette saisie aurait été assez puissante pour tuer des milliers de personnes. La quantité saisie peut sembler minime, mais elle représente jusqu'à 38 000 doses. Un quart de milligramme de furanyl-fentanyl peut être mortelle, selon la GRC. C'est beaucoup plus dangereux que le fentanyl. Selon Santé Canada, il ne suffit que de 2 mg de fentanyl pur - soit l'équivalent

de quatre grains de sel - pour tuer un adulte. Les accusations ont été déposées après l'intervention des policiers de la GRC au croissant Clearcrest, jeudi. L'homme doit faire face à des accusations d'importation d'une substance contrôlée et d'autres infractions liées aux drogues. Radio-Canada

Drug flow into prisons top priority for officials
With more than three-quarters of incoming inmates having addictions, stemming the flow of drugs and other contraband in prisons is a priority, officials say. It has become even more crucial as toxic narcotics such as fentanyl are being smuggled into institutions and unsuspecting staff and prisoners are exposed." Almost 80 per cent of offenders arrive at federal institutions with some level of substance abuse problem, and many have multiple addictions," said Jeff Campbell, spokesman with the Correctional Service of Canada (CSC). "We acknowledge the prevalence of substance abuse problems among offenders and assist in addressing those problems through a drug strategy." A Bowden Institution guard collapsed this week during a search for drugs. It's believed he was exposed to fentanyl. Staff at the federal medium-security facility administered naloxone to reverse the effects of the opioid, which is 50 to 100 times more potent than morphine. While it produces an intense high, it also can cause nausea, vomiting, sedation and death. The officer is now back at work. Campbell said CSC has security and intelligence measures to monitor and investigate inmate activity, potential drug-smuggling attempts and seizure of illicit substances. Postmedia News (Edmonton Journal, A10; Calgary Sun)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Snow, freezing rain will make driving dicey
The Ottawa region entered the weekend under a winter storm watch, with a mix of snow and freezing rain expected to bring icy, dicey driving conditions into Sunday. The snow was expected to begin late Friday night and continue through all day Saturday, according to an Environment Canada bulletin issued at 3:59 p.m. Friday. There's a chance the precipitation could change to "an extended period of freezing rain Saturday night," the news release said. With a Colorado low system moving into southern Ontario Friday night and driving conditions expected to worsen, **Public Safety Canada** encouraged travellers to make emergency kits with drinking water, food, medicine, a flashlight and a first-aid kit. Total accumulation was expected to be about 9 cm, with five of that to come through the day Saturday and another two that night. Canadian Press (Ottawa Sun, A2; Ottawa Citizen)

Storm closes the Island - Snow and wind force drivers to abandon vehicles and keep tow truck operators busy across P.E.I.
RCMP Const. Jamie Parsons knew it was going to be a long day before he even got to work on Friday morning. Travelling into the Maypoint detachment in Charlottetown for his shift, which started at 6:30 a.m., he passed by vehicles that were abandoned in the snowstorm. "And that's just within the city itself," Parsons said late Friday afternoon. "Once I got to work a lot of other calls were coming in with motorists stranded out in the country where we patrol. "Most of them we couldn't get to. It was too dangerous for us to go out. We called Department of Transportation and let them know where these people were stuck and, unfortunately, the plows were even off the roads at the time." As the province dealt with a bevy of weather issues - snow squalls, winds gusting to 90 km/h blowing the white powder around and temperatures that plunged to -18 C (with wind chill value of -30 C) - RCMP kept checking in with people who were stranded. Charlottetown Guardian, A1

*** More power outages hit P.E.I. - About 3,800 Maritime Electric customers in Albany, Victoria and Kinkora have no power**
About 3,800 Island households and businesses were without power Saturday in Albany, Victoria and Kinkora. A spokesperson with Maritime Electric said crews are out investigating the problem and the cause of the outages isn't yet known. Power crews were busy dealing with outages caused by Friday's storm. At one point, more than 1,000 customers had lost power. CBC News

Power outages continue for thousands of Nova Scotians
High winds and snow are the causes of most of the power outages in Nova Scotia Saturday morning. As of 6:50 a.m., there were 90 active outages in Nova Scotia affecting 3,155 customers as far west as

Freeport to as far east as Meat Cove. Most of the power outages are concentrated in Cape Breton, with 1,488 affected customers in the Judique area and 1,174 customers in the Ingonish, Meat Cove and Pleasant Bay. There are also outages reported in Cumberland County and New Glasgow. Power is expected to be restored to most places by 2 p.m. Saturday, according to Nova Scotia Power's outage map. The cause of outages near Hart Lake in Cumberland County is still under investigation. Nova Scotia Power expects electricity will be back on there by midnight. CBC News; Chronicle-Herald; Cape Breton Post

Government puts more money into flooding, drought programs
The Alberta government has announced more funding for flood and drought protection. The province is to invest an additional $31 million over four years in flood resiliency projects through the Alberta Community Resilience Program. The 10-year, $500-million program has so far helped to build flood barriers, as well as other safeguards. Another $14 million is to go to the Watershed Resilience and Restoration Program, which supports wetland and riverbank areas. That program had been set to wrap up in 2017. Environment Minister Shannon Phillips says the money will help communities adapt to changing climate and more common severe weather. Red Deer Advocate, A8

Letter to Ottawa was sent 'inadvertently' - B.C. minister
A B.C. cabinet minister is apologizing to the federal government for a letter that called on Ottawa to reopen the Coast Guard communications base in Comox. Naomi Yamamoto, the Minister of State for Emergency Preparedness, said Friday that her ministry made a mistake in sending the letter and is not, in fact, asking Ottawa to reopen the Comox base as part of the federal government's $1.5-billion ocean protection plan. "Earlier this week, a letter was inadvertently sent to the federal government from my office," Yamamoto said in a statement. "The letter dealt with the federal government's ocean protection plan and ensuring there is reliable communications along the entire British Columbia coast. "I want to be clear, under the federal government's oceans protection plan, that marine communications capacity is being improved to a world-leading standard." Yamamoto's letter came at a sensitive time for the two governments, which are trying to hammer out the details of the ocean-protection plan into specifics for British Columbia after Ottawa's approval of the Kinder Morgan pipeline. Vancouver Sun, A22

*** Search continues for missing 79-year-old man**
Eskasoni band members resumed their search for a missing elder Friday, despite the continuing storm. Camilius Alex, 79, has not been seen for days, said his son Rodney Alex. "There were quite a few (searchers)," Rodney said. "I just put it out there that I needed help, and the residents responded quickly. He's on a lot of medications - he received a triple bypass two years ago and he has a little dementia." The searchers are concentrating their efforts on Mountain Road, near the elder's home. "He loves walking and last week was really nice days," Rodney said, adding he believes that Camilius did not have his medication with him. RCMP described Camilius as being 6-foot-1, about 190 pounds, with grey hair and brown eyes. He was last seen wearing a dark coat, hoodie and dark gloves and had a walking cane. Chronicle-Herald, A4

Pipelines draw a line in the sand
An opinion piece states "Pipelines have become the new pariah in Indian Country. From Standing Rock to The Assembly of First Nations pipelines opposition to pipelines has become a rallying cry and a hill many political leaders have staked out as their preferred location for death. Pipelines come in many different forms and risk factors. The Gateway pipeline was a none starter because it passes through ecologically sensitive terrain with a myriad of mountains, lakes and rivers. A spill in this pristine area would be catastrophic... The chiefs of the Assembly of First Nations are split on the issue and those opposed to pipeline are becoming increasingly shrill. Other First Nations leaders see resource development as one of the roads to financial independence. The issue has the potential to pit First Nations against one another. I think it's time to we stood back and did a little critical thinking. Right now oil is being shipped by rail. Each day oil trains travel through Saskatoon and across the prairies. The risk of a spill and serious accident is much greater with rail cars than a pipeline. The tragedy at Lac Megantic stands out as an especially serious case. Rather than a wholesale ban on pipelines each case must be reviewed separately. Some are replacing existing lines which will be safer and more efficient in the future; others are heading into

pristine wilderness and creating a ticking environmental time bomb never mind the mess that the pipeline construction will create." Star-Phoenix

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Martin Couture-Rouleau voulait tuer d'autres militaires
Le terroriste Martin Couture-Rouleau, qui a heurté à mort l'adjudant Patrice Vincent, le 20 octobre 2014 dans le stationnement d'un centre commercial de Saint-Jean-sur-Richelieu, s'en serait pris à d'autres militaires s'il en avait eu l'occasion. C'est ce que démontre la conversation qu'a eue Couture-Rouleau avec un préposé du 9-1-1 dans les minutes suivant l'attentat, dont des extraits se trouvent dans le rapport d'enquête du coroner André Dandavino sur le décès du militaire, rendu public vendredi. L'auteur du délit de fuite, pourchassé par les policiers après avoir heurté l'adjudant Vincent et un autre militaire qui a eu la vie sauve, a appelé le 9-1-1 pour, disait-il, « passer un message ». Il a alors refusé de se rendre, disant qu'il allait peut-être « croiser un autre de vos soldats » et qu'il allait « l'abattre. » Il demandait au service d'urgence « d'avertir le Canada, le gouverneur » et d'autres de quitter la coalition qui était opposée à « l'État islamique. » La Tribune, 14 (Le Nouvelliste; Le Droit); La Presse

Peace bond target denies terror links - British Columbia
The latest target of Canada's terrorism peace bond system insisted he has no connection to extremist violence and turned up at a B.C. police station to complain about press coverage of his case. "I throw your newspaper in the garbage," Khalid Ahmad Ibrahim, 39, told a reporter at the door of a New Westminster, B.C. apartment. "There is no terrorism," he added. The RCMP told the provincial court on Dec. 8 there were "reasonable and probable grounds to believe. that Khalid Ahmad Ibrahim may commit a terrorism offence." He was released on $1,000 bail and must adhere to 25 bail conditions, including not accessing or viewing any materials related to a terrorist group. He was due back in court Dec. 20. Peace bonds are not a criminal charge but rather impose conditions on the conduct of those subjected to them. Police have been using them to control suspected violent extremists. Postmedia News (London Free Press, N4; Windsor Star; Montreal Gazette; Whig-Standard)

CSIS aware of terror suspect's flight while RCMP investigated
In 2013, while the RCMP were still investigating how a suspected terrorist had quietly left Canada to join ISIL the previous year, Canada's spy agency informed the Mounties they had in fact already known the intimate details of the terrorism suspect's final hours before he boarded a plane for Syria, new court records reveal. John Maguire left Canada in December 2012 to join ISIL in Syria, where he was featured in a propaganda video declaring religious war on his home country. The Islamic State reported Maguire died fighting in 2015, though his death has never been confirmed. Before he left for Syria, Maguire was the alleged star terrorism recruit of Ottawa's Awso Peshdary, 26, who was charged in February 2015 with recruiting, financing and facilitating terrorism. And the RCMP's case against Peshdary is where new details have emerged about the Mounties' investigation into an alleged Ottawa terror network. The RCMP's case that yielded charges against Peshdary, 26, was built on a foundation so shaky that investigators were twice turned down when they went to get search warrants against Maguire. Whig-Standard, B1

La liberté, c'est l'esclavage - Qui s'offusque encore si Big Brother nous regarde? - La surveillance généralisée et une soumission volontaire aux données numériques
Le Royaume-Uni a adopté en novembre la Loi sur les pouvoirs d'enquête. Cette loi donne aux services de sécurité de Sa Majesté le droit d'utiliser à peu près n'importe quel moyen pour espionner ses citoyens. Aucun autre pays de l'Occident n'en permet autant. " Le Royaume-Uni vient de légaliser la surveillance la plus extrême de l'histoire des démocraties occidentales, a ensuite gazouillé le lanceur d'alerte sur la

surveillance planétaire Edward Snowden. La mesure va plus loin que bien des régimes autoritaires. " M. Snowden est maintenant réfugié en Russie, pays-continent héritier de l'URSS, l'empire rouge qui implosait il y a tout juste 25 ans, le 26 décembre 1991. Le régime totalitaire soviétique, obsédé de surveillance et de répression, a en partie inspiré le roman dystopique 1984. La prophétie du cauchemar sous l'angsoc (le socialisme anglais, en novlangue) ne s'est évidemment pas réalisée comme telle. N'empêche, dans notre monde postorwellien, libre jusqu'au vertige, Big Brother vous regarde, beaucoup, passionnément, à la folie. " En fait, plusieurs Big Brothers vous surveillent maintenant ", corrige le professeur de l'Université Laval Stéphane Leman-Langlois, spécialiste du renseignement et du contrôle social. " La différence est là, dans le foisonnement de points de collecte de données qui permet d'en amasser beaucoup plus au profit de plusieurs centres de surveillance. " Le Devoir, A4

Has Harkat been 'de-humanized'?
A letter states "I must object to the assumption made in this article that Mohamed Harkat was a radical Muslim. That was not what the courts said. It is not possible to de-radicalize someone who has never been a radical. He cannot stop being what he's not been. Perhaps the title should have read 'has he been de-humanized?' since Harkat is one of the kindest humans I've met, despite our justice system's attempt to change that. A retraction would be a good first step to change the image your paper conveys of him." Ottawa Citizen, B7

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

*** City man faces 136 immigration-related fraud charges**
A Winnipeg man has been hit with a slew of charges after he is alleged to have fraudulently collected fees as an immigration consultant. The Canada Border Services Agency announced 56-year-old Vladimir Bibilov is facing 102 counts under the Immigration and Refugee Protection Act, and another 34 counts under the Criminal Code for alleged offences between January 2009 and December 2015. Bibilov is alleged to have acted as a paid immigration consultant when he was not licensed to do so and allegedly took fees from clients. The CBSA alleged Bibilov "misrepresented himself to foreign nationals with the promise to provide immigration services to Canada," and also alleged he "provided false and misleading information to induce or deter immigration to Canada." He will appear in a Winnipeg courtroom on Monday. "The CBSA takes immigration fraud very seriously and is committed to fully investigating and prosecuting those who violate our laws and seek to profit illegitimately from our immigration system," CBSA spokeswoman Kim Scoville said in a release. Winnipeg Sun, A8

*** Faster border isn't a win**
A letter to the editor states "I believe The Globe and Mail's editorial board and our Prime Minister may be seriously underestimating the extent to which the world will change when Donald Trump assumes the presidency. For example, both The Globe and Justin Trudeau view the recent agreement with the United States with regard to transborder travel as a victory. The devil is in the details (A Faster Border, Dec. 14). We have been told that this is just like the present prescreening arrangements in place at some Canadian airports. It is not. U.S. border guards in Canadian airports have the right to question, but not to detain Canadian citizens. The new arrangements will allow armed U.S. border guards on Canadian soil to detain Canadians. Under the current arrangements, U.S. border guards must obey Canadian laws. The new arrangements do not allow Canadian law enforcement to arrest or charge U.S. border guards for actions taken while on the job. The U.S. may choose to act, but it will be entirely up to the U.S. Department of Homeland Security." Globe and Mail, F2

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Obama warns Putin that US could strike back on cyber
President Barack Obama has put Russia's Vladimir Putin on notice that the U.S. could use offensive cyber muscle to retaliate for interference in the U.S. presidential election, his strongest suggestion to date that Putin had been well aware of campaign email hacking. "Whatever they do to us, we can potentially do to them," Obama declared Friday. Caught in the middle of a post-election controversy over Russian

hacking, Obama strongly defended his administration's response, including his refusal before the voting to ascribe motive to the meddling or to discuss now what effect it might have had. U.S. intelligence assessments say it was aimed at least in part on helping Donald Trump defeat Hillary Clinton, and some Democrats say it may well have tipped the results in his favour. Associated Press (iPolitics; Chronicle-Herald); AFP (Le Devoir)

FBI agrees - Russia hacks helped Trump
The FBI is supporting the CIA's conclusion that Russia interfered in the presidential election with the goal of supporting Republican candidate Donald Trump. In a message sent to employees, CIA Director John Brennan said he had spoken with FBI Director James Comey and James Clapper, the director of national intelligence. Brennan said in the message that "there is strong consensus among us on the scope, nature, and intent of Russian interference in our presidential election." Associated Press (Ottawa Sun, A10)

Des Canadiens demandent un recours collectif contre Yahoo
Des Canadiens dont les informations personnelles pourraient avoir été volées lors de failles informatiques de Yahoo demandent un recours collectif de 50 millions $ contre le géant internet. Un cabinet d'avocats de Toronto affirme que l'avis de demande en justice a été déposé vendredi, à la Cour supérieure de l'Ontario. Le recours collectif comprendra des Canadiens dont les données d'utilisateurs ont été volées ou dont les comptes ont été piratés dans les dernières années. La représentante des demandeurs utilisait Yahoo pour sa correspondance électronique. Originaire de Barrie, en Ontario, Natalia Karasik dit avoir transmis par courriel des informations sur son état de santé ou encore d'ordre financier. Selon l'avis, elle ignorait que des pirates pourraient y avoir accès, et ce, depuis 2013. Au mois de septembre, l'entreprise de Sunnyvale, en Californie, a signalé à certains de ses utilisateurs que les données figurant à leurs comptes avaient été volées lors d'une cyberattaque survenue en 2014. Le Nouvelliste, 27; Canadian Press (Red Deer Advocate; St. John's Telegram)

Un nouveau piratage massif fragilise Yahoo ! face à Verizon
Décidément, la fin de règne de Marissa Mayer à la tête de Yahoo ! s'apparente de plus en plus à un long chemin de croix. Le mercredi 14 décembre, le portail Internet a indiqué avoir été victime d'un nouveau piratage informatique, « probablement » différent de celui révélé fin septembre et qui concernait 500 millions de comptes d'utilisateurs. La portée de cette deuxième cyberattaque est de plus grande ampleur : plus d'un milliard de comptes ont été compromis. Il s'agit du plus important vol de données de l'histoire. Selon la direction, l'attaque a été menée en août 2013 mais n'a été détectée que très récemment. Ses auteurs ont pu dérober de nombreuses informations personnelles : noms, dates de naissance, adresses électroniques, numéros de téléphone. Ils ont aussi mis la main sur les réponses aux questions de sécurité qui permettent de modifier le mot de passe en cas d'oubli. Mais ils n'auraient en revanche pas récupéré les coordonnées bancaires. La société indique que les utilisateurs touchés vont être avertis et devront changer leur mot de passe. Le Devoir

Literacy test goes paper-only - move comes after online test hacked in October
The next province-wide literacy test for Ontario high school students will be administered on paper, after an online trial last time was hit with a cyber attack. In October, the agency that runs the Ontario Secondary School Literacy Test was forced to cancel an online trial run due to technical glitches, later determined to be a distributed denial of service attack. Most of the province's 900 secondary schools - representing a maximum of 147,000 students - had signed up to participate in the online test, and only about 15,000 students managed to complete it. Canadian Press (London Free Press, A7; Ottawa Sun; National Post; Globe and Mail)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Plan emerges for security barriers around police HQ
City hall is moving ahead on a plan to install security barriers around the new downtown police headquarters. The city recently issued a request for proposals for engineering consulting services for the design of a downtown cycling network. Included in the RFP was the design and installation of security

bollards around the police HQ. Security bollards were not included in the project's final price tag, which climbed to $214 million - $75 million over budget. The RFP, which closes Jan. 20, said the bollards are needed to protect the building and staff from a terrorist attack. "The headquarters was not designed or built to withstand large-scale attacks," states the RFP. "The increased level of global terrorism against government institutions, including emergency services, dictate basic and affordable security measures be considered to ensure essential services are maintained." The document states a vehicle could drive over the sidewalk and into the building, and security bollards need to be installed around it. No cost estimate is provided in the RFP documents for the bollards, but police officials said in September the project could would likely cost $1.7 million. The HQ and the adjoining commercial tower have proven to be a headache for politicians and administrators. The city purchased the former Canada Post building and warehouse in 2010 for $29 million. The plan was to convert the warehouse into a new home for the Winnipeg Police Service and the officer tower would be sold, expected at a price of $18 to $20 million. The renovations costs for the warehouse ballooned to $214 million from $139 million. A two-year-old RCMP investigation has been probing allegations of fraudulent billing. Winnipeg Free Press, B1

* **Jusqu'à 38 000 doses de furanyl-fentanyl saisies à Ottawa**
Un homme de 42 ans se retrouve derrière les barreaux après que les policiers de la Gendarmerie royale du Canada eurent saisi environ 19 grammes de furany-lfentanyl, une drogue mortelle. La perquisition a eu lieu dans le secteur d'Orléans, à Ottawa. Cette saisie aurait été assez puissante pour tuer des milliers de personnes. La quantité saisie peut sembler minime, mais elle représente jusqu'à 38 000 doses. Un quart de milligramme de furanyl-fentanyl peut être mortelle, selon la GRC. C'est beaucoup plus dangereux que le fentanyl. Selon Santé Canada, il ne suffit que de 2 mg de fentanyl pur - soit l'équivalent de quatre grains de sel - pour tuer un adulte. Les accusations ont été déposées après l'intervention des policiers de la GRC au croissant Clearcrest, jeudi. L'homme doit faire face à des accusations d'importation d'une substance contrôlée et d'autres infractions liées aux drogues. Radio-Canada

* **Car slides off highway into deep water - Strange accident happens on Trans-Canada Highway in rural Holyrood**
A motorist was lucky someone saw their car slide off the road and into a pond Friday. An ambulance was called, and paramedics transported the driver to hospital. The incident happened shortly after noon on the Trans-Canada Highway near the Foxtrap Access Road, the RCMP stated in a news release. It is unknown whether the driver suffered serious injuries, the RCMP stated. "The driver was taken by EMS before police arrived, so the sex and age of the driver are yet to be confirmed." The RCMP in Holyrood was busy Friday responding to calls arising from the snowy and slippery road conditions, but the pond incident was the only accident reported, and it is under investigation, the release stated. Charlottetown Guardian, A7

* **Saskatchewan RCMP officer charged with firearms offences**
A Saskatchewan Mountie is facing firearms charges in Alberta. Const. Dale Malbeuf of the Morse detachment in southern Saskatchewan was arrested this week at a home in Edmonton. Police allege the officer produced and pointed a firearm at a woman in the home. Malbeuf appeared in Edmonton court Wednesday on charges of pointing a firearm and careless use of a firearm. He was released on conditions and is to attend court again Jan. 6. RCMP say Malbeuf, on the force for 12 years, has been suspended with pay. Red Deer Advocate, A8; Edmonton Journal

* **RCMP still investigating body found in burned vehicle**
The circumstances of a body found in a burned vehicle earlier this week remain a mystery as Mounties continue their investigation. On Friday, police involved in the investigation said reports were being reviewed, and the investigation was continuing. An autopsy was performed on Monday at the office of the Chief Medical Examiner in Calgary. The results have yet to be released. On Dec. 10, Stettler RCMP were called to a complaint of a burned vehicle in the rural Stettler area. Through their investigation, they found there was a dead person inside the vehicle. RCMP Major Crimes are assisting Stettler RCMP with the investigation. Red Deer Advocate, A7

* **Man arrested after murder on reserve**

A 37-year-old man has been charged with a homicide on the Little Black Bear First Nation. Sherman Luke Bellegarde made his first appearance in Regina Provincial Court on Friday morning on a charge of second-degree murder. According to the charge read out in court, Bellegarde is accused of killing 33-year-old Lauren Quewezance. Both are from Little Black Bear. Bellegarde, who sought the assistance of Legal Aid, was remanded in custody. He'll return to court in Fort Qu'Appelle on Dec. 22. The RCMP has not yet released any information about the incident. Little Black Bear is located in the Fort Qu'Appelle area, about 130 kilometres east of Regina. Star-Phoenix, A6 (Leader-Post)

* **WHO IS TRAVIS VADER? - The man at the centre of one of Alberta's highest-profile homicide cases says a lot, but answers little**
In an Edmonton courtroom on a frigid Monday morning, members of a grieving family attempted to express the many ways their lives have been torn apart by the killings of Lyle and Marie McCann. There were the familiar scars that homicide leaves on survivors: Deep anxiety, nightmares, a fear of ringing phones and of people not answering. There were the unanswerable questions: How could someone do this? Why?... In the years since 2010, when the McCanns disappeared, Mr. Vader has become one of the province's most recognizable figures: A man with a villain's last name and a widely disseminated mugshot, charged - and now convicted - in the killings of a kindly couple in their late 70s, one of the biggest RCMP cases in Alberta's history. Globe and Mail, S1

* **Cops wrong to act on hunch that suspect would poop drugs, judge rules**
A judge has found that the RCMP unlawfully arrested a man who later excreted from his rectum small quantities of heroin, cocaine and fentanyl while in custody. Ronjot Dhami, who has been charged with three counts of possession for the purpose of trafficking, was a passenger in a Mercedes that was pulled over by police in Kelowna in June 2014. An RCMP officer, who had earlier been conducting surveillance on an apartment building where the Mercedes was initially spotted, saw Dhami vigorously rubbing his hands together and reaching into the vehicle's glove box, according to a ruling by B.C. Supreme Court Justice Peter Rogers. Vancouver Sun

* **Un homme accusé de possession de pornographie juvénile**
Une enquête ayant débuté l'été dernier a mené au dépôt d'accusations liées à la pornographie juvénile contre un homme de 28 ans d'Ottawa. La police d'Ottawa a procédé jeudi à l'arrestation de Michael Lalonde, à la suite d'une perquisition menée dans le pâté de maisons des 400 du chemin Montréal. L'enquête avait pris naissance à la mi-juin. Le Centre national de coordination contre l'exploitation des enfants avait alors fourni à la police d'Ottawa des rapports reçus par le biais de la ligne d'appel du National Centre for Missing and Exploited Children des États-Unis. Des rapports ont ainsi été relayés à la police d'Ottawa jusqu'à la fin août, et ont démontré que des images d'exploitation sexuelle d'enfants avaient été déposées, à partir d'une adresse IP d'Ottawa, sur une plateforme privée de clavardage appelée ChatStep. Michael Lalonde devait comparaître vendredi pour être formellement inculpé de trois chefs de possession de pornographie juvénile et de deux chefs d'avoir rendu accessible de la pornographie juvénile. Le Droit, 12

* **N.B. should be wary of joining 'police militarization' trend**
An opinion piece states “Fredericton City Council Monday managed to step into the middle of a highly contentious debate across North America about 'the militarization of police forces.' It did so by approving a police force request for the lease to purchase of a 'light-armoured vehicle,' setting aside a whopping $350,000 for it, according to a CBC report of the meeting. At the same time, the council rejected a $440,000 police department request to hire two new officers and some civilian staff... Need for militarization of policing appears limited. Much expert opinion involves evidence showing it tends to make dangerous situations more dangerous and confrontational rather than significantly helping to de-escalate a situation. If there are justified uses, albeit rare, for such vehicles, perhaps the solution would be to have the province buy three or four and station them strategically so every region is reasonably quickly reached. The cost would be shared by every municipality. Let them be manned by the RCMP, who also emphasize de-escalation whenever possible. It'd be a good compromise, though even then I suspect they'd be underused.” Times and Transcript, A12

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Man's 911 call leads to his arrest - Twenty-eight-year-old charged with multiple probation breaches, driving offence, mischief

... An inmate serving a life sentence for second-degree murder was found dead on Tuesday in the minimum-security unit of Joyceville Institution. Robert Brunet, 71, was convicted in September 2008 of murdering 81-year-old Violet Graves in Hawksbury eight years earlier. Brunet, who lived in the same building as Graves at the time of the murder, broke into her basement apartment, then beat, sexually assaulted and strangled her. Her body was found in the apartment on July 30, 2000. He was arrested by police in 2005 after voluntarily giving a DNA sample. Justice Robert Maranger, who was also the judge of the 2011 Shafia trial in Kingston, called the elderly woman's killing brutal and vicious, before sentencing Brunet to life in prison with no chance of parole for 20 years. Emergency services were called on Tuesday and Brunet was taken to hospital. He was pronounced dead at 2:51 p.m. A release from Correctional Service Canada said the inmate's family has been notified of his death. Whig-Standard, A3

Ontario hiring more jail staff to help mentally ill inmates

Ontario is hiring more corrections staff, including officers, nurses, psychologists and segregation managers in an attempt to address issues with solitary confinement and inmates with mental-health challenges. The dedicated segregation managers will work at institutions with higher segregation rates to try to reduce the use of isolation and help inmates who have been in solitary transition back to the general population. "This is a first step towards implementing dedicated segregation teams across the system," said Correctional Services Minister David Orazietti. The announcement comes shortly before federal correctional investigator Howard Sapers is set to officially lead an Ontario review into the use of segregation. Orazietti said he didn't want to prejudge what Sapers will recommend, but this is work that could be done in the meantime. Postmedia News (Windsor Star, A9)

*** Bowden Institution locked down**

Between a corrections officer potentially exposed to a toxic substance and a subsequent lockdown, Bowden Institution has been busy. It was reported that an officer was exposed to the substance while searching a cell in the correctional facility south of Red Deer. The substance is being tested, but the reaction was described as similar to an opioid, or fentanyl exposure. Naloxone was administered, and the officer is recovering. The lockdown was initiated on Tuesday, and an exceptional search was conducted. Red Deer Advocate, A6

*** Drug flow into prisons top priority for officials**

With more than three-quarters of incoming inmates having addictions, stemming the flow of drugs and other contraband in prisons is a priority, officials say. It has become even more crucial as toxic narcotics such as fentanyl are being smuggled into institutions and unsuspecting staff and prisoners are exposed." Almost 80 per cent of offenders arrive at federal institutions with some level of substance abuse problem, and many have multiple addictions," said Jeff Campbell, spokesman with the Correctional Service of Canada (CSC). "We acknowledge the prevalence of substance abuse problems among offenders and assist in addressing those problems through a drug strategy." A Bowden Institution guard collapsed this week during a search for drugs. It's believed he was exposed to fentanyl. Staff at the federal medium-security facility administered naloxone to reverse the effects of the opioid, which is 50 to 100 times more potent than morphine. While it produces an intense high, it also can cause nausea, vomiting, sedation and death. The officer is now back at work. Campbell said CSC has security and intelligence measures to monitor and investigate inmate activity, potential drug-smuggling attempts and seizure of illicit substances. Postmedia News (Edmonton Journal, A10; Calgary Sun)

*** A Hells Angel-turned-police informant pleads for 2nd chance**

On a warm June day in 1997, Diane Lavigne, a widow with two adult daughters, got into her van and headed home. She left Montreal's Bordeaux jail, where she had worked for more than 10 years. As she drove north on the Laurentian Highway, a motorcycle pulled up beside her. She was gunned down in what has been described as a "hail fire" of bullets, becoming one of more than 100 victims of Quebec's infamous biker wars. Hells Angel Stéphane "Godasse" Gagné, 47, pleaded guilty to first-degree murder in Lavigne's death and was sentenced to life in prison, where he has now served more than 19 years.

Gagné, slated to be released in 2023, filed a motion last year to be released before the end of his sentence. The motion was granted. At his Parole Board of Canada hearing for conditional release, held earlier this week, Gagné detailed the path that landed him behind bars and brought him to the point of seeking a second chance. CBC News

*** Family of murder victim Kate Reid will speak for her at parole board hearings**
Kate Reid's family members say they will speak for her at any parole hearings for the man who murdered her. Her family said in a statement on Friday that when Hugh McColl becomes eligible for parole, "someone from the Reid family will sit in front of the parole board to ensure she always has a voice." On Wednesday, a jury found McColl, 63, guilty of second-degree murder in the killing of Reid, 51. They were roommates in an apartment on Burn Place in Kitchener. McColl killed her with a hammer on Jan. 2, 2015. McColl will get an automatic life sentence with no chance of parole for at least 10 years and possibly as long as 25 years. His parole eligibility date will be set by a judge on Feb. 17. Waterloo Region Record

*** Indigenous prisoners face discrimination, violence, say frontline workers - 'I've seen inmates get beaten black and blue,' says First Nations activist**
Armand MacKenzie spent 15 years representing Indigenous offenders before he quit the practice. MacKenzie, an Innu lawyer, said when an offender showed up for a court appearance at the Sept-Îles courthouse on Quebec's North Shore, he'd face a room filled with white people: the judge, the constable, the prosecutor and the support staff... Once an Indigenous person is convicted and goes from being a suspect to an inmate, that person can face a whole new set of challenges, said Albert Dumont. Dumont, who worked for three years in one of Ontario's toughest prisons, said Indigenous prisoners are treated differently, including when it comes to punishment. "I've seen inmates get beaten black and blue and be thrown in segregation for upwards of two months and not have a hearing. They'd only be let out when I'd get involved," said Dumont, who worked in the maximum security "J-Unit" at Millhaven Institute in Bath, Ont. "The sins of the system are far greater than what the offender ever committed, in a lot of cases," Dumont told Quebec AM. In his autumn 2016 report, Canada's Auditor General Michael Ferguson highlighted that Indigenous people make up just three per cent of the country's adult population, but they account for 26 per cent of the inmates in federal institutions. CBC News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Thirteen deaths in one day linked to drugs - Cause of 'dangerous upsurge' in overdoses is unknown, coroner says
The B.C. Coroners Service has issued an urgent warning to illicit-drug users after an unprecedented number of drug overdose deaths in B.C. As many as 13 people died of suspected drug overdoses on Thursday, and Premier Christy Clark said the rising death toll is one of the most difficult issues she has faced this term. "I can't remember anything in the last four years that has felt like such a crisis - such an urgent crisis - where so many lives are being lost every single day, and that is so complicated to get our hands around," she said. Within eight hours, six people died after using drugs in Vancouver's Downtown Eastside, said coroner Barb McLintock. Two other deaths, at the same time, in the same area, are believed to be drug-related. Five other people died after using drugs on Thursday. The deaths occurred in Vancouver, Burnaby, northern B.C. and two in the Fraser region... Health Minister Terry Lake and Minister of Public Safety Mike Morris later said in a joint statement that the province expects to meet its goal of adding 500 substance-use beds by the end of March. The province has earmarked $43 million to respond to the crisis by expanding access to naloxone, establishing overdose prevention sites and working with the federal government to stop drugs from entering Canada. Times-Colonist, A3; Vancouver Sun; Globe and Mail; Canadian Press (Cape Breton Post); Le Droit; La Presse

Alert issued in B.C. after 11 deaths
An urgent warning has been sent out to illicit drug users in British Columbia after 11 people died in the province on Thursday alone, six of them in Vancouver's Downtown Eastside. The warning from the B.C. coroners' service on Friday came at the same time police, firefighters, the mayor and health officials in Vancouver collectively called on the provincial government to provide treatment on demand for drug

users... Premier Christy Clark described the overdose crisis as a complex issue that requires more police and treatment options. But she stopped short of promising more money or programs. "The thing that frustrates me has been people who say, 'Here's the one thing we need more of, "' she said. "We're not going to simplify it down to just detox beds. We need more police. We need more RCMP on the ground. We need more Canada Border Services Agency drug interdictions. We need more treaties. We need more health care. We need more naloxone." Canadian Press (Red Deer Advocate, A7)

* **Fentanyl crisis: November death tally expected to reach 35 in B.C. - Vancouver had 9 drug overdose deaths on Thursday**
The B.C Coroners Service is expected to release a tally of November overdose deaths on Monday, and officials expect the worst — predicting that 35 or more people may have died. Health Minister Terry Lake and Provincial Health Officer Perry Kendall have both said that, while finalized numbers have not been confirmed, early estimates of opioid deaths during November appear grim. Both say they were optimistic earlier this year after numbers from the summer appeared to indicate the crisis was improving, but statistics since then have deteriorated. During a recent cold spell, the fentanyl crisis hit a brutal low point. On Thursday officials reported 13 deaths across the province in one night, nine of them in Vancouver. CBC News

New centres offer 'rapid access' to drug addicts
Two "rapid access" centres for those addicted to drugs will open in Cambridge and Kitchener-Waterloo in the new year, says the co-ordinator for the Waterloo Region Integrated Drugs Strategy. Addicts - whether using prescription drugs or those sold on the street - will be able to see a doctor and access an addiction counsellor, said Lindsay Sprague. "For someone in the ER department or a user, here is where you go next," she said. "Anyone can come. You can self-refer." In Ontario, there are seven similar centres where any substance user can get help without waiting weeks to get treatment. The pilot project clinic will be open two days a week and donations will pay for the centre, Sprague said. A firm date has not been set. For Waterloo Region, the "rapid access" addiction centre is welcome news for police, paramedics and emergency room doctors who are dealing on a daily basis with the opioid crisis - often heroin laced with the deadly drug fentanyl. Waterloo Region Record, B1

* **Services d'injection supervisée : fini le déni**
Les demandes pour ouvrir de tels lieux devront répondre à cinq questions, indique le projet de loi déposé lundi par le gouvernement Trudeau. C'est cinq fois moins que le processus actuel. Et surtout, c'est beaucoup plus ciblé, et justifié. Les cinq facteurs dont Santé Canada devra tenir compte sont directement inspirés du jugement de la Cour suprême qui avait confirmé la légitimité de la clinique vancouvéroise InSite, a souligné la ministre fédérale de la Santé Jane Philpott. C'est autrement plus pertinent que la liste d'épicerie actuelle. Celle-ci, rappelons-le, comprend 26 critères, et c'est bien parce que notre alphabet ne compte pas plus de lettres : avec les requêtes hétéroclites regroupées sous des points comme b) ou i), on frise la trentaine de questions. La Presse

* **In need of full services - Future Edmonton supervised injection sites should offer counselling and medical services, police say**
When Edmonton drug and gang enforcement detective Guy Pilon toured the Insite supervised injection site in Vancouver's Downtown Eastside several months ago he didn't like what he saw. He had visited it three years prior and wanted to see the progress of it and other drug treatment facilities in the city. "There are users now waiting outside of Insite just waiting to get in," Pilon said. "They are shooting up in the street, they are shooting up around the corner. There are just users everywhere." Insite, he said, was less about the treatment of drug addictions and more about allowing people to do it safely. Two blocks away at another of Vancouver's drug treatment facilities, Providence Crosstown Clinic, they were taking a different approach for drug addicts to seek support. Postmedia Network (Edmonton Sun, A3; Edmonton Journal); CBC News

* **Calgary police chief sees supervised injection sites as part of bigger strategy**
Calgary's police chief is open to introducing supervised facilities for drug users, so long as such programs are part of a larger strategy to lower addiction rates and address problems that accompany drug dependency, such as crime and joblessness. "It always makes police chiefs look resistant when they say

no to these things. My answer has been: 'Sure, as long as it is part of a better strategy,' " Calgary Police Service Chief Roger Chaffin said in an interview this week. "I'd be more mindful of it if it was part of a more robust strategy to lower the issues of addiction." Alberta is in the midst of a drug crisis that has also hit several other provinces, most notably British Columbia, with opioids such as fentanyl at the centre of the problem. Supervised drug-use sites, such as two already operating in Vancouver, are designed to reduce risks for drug users because health professionals are there to quickly treat overdoses. The federal government this week proposed legislation that would make it easier for cities to open supervised drug-use facilities, so long as they can prove there is a need, consult the community, show they will reduce crime, demonstrate they have the resources to run the facilities and follow regulations. Globe and Mail, S1

*** Relations avec les autochtones: une enquête publique au mandat très large**
Au terme d'une enquête de près d'un an menée par le SPVM, le Directeur des poursuites criminelles et pénales avait décidé cet automne qu'aucune accusation ne serait déposée contre les policiers de Val-d'Or visés par un reportage de l'émission Enquête de Radio-Canada. Des femmes autochtones de Val-d'Or avaient soutenu avoir été victimes de sévices sexuels commis par des agents de la SQ. Selon les informations obtenues par La Presse, le premier ministre Philippe Couillard annoncera à l'issue de la réunion du Conseil des ministres, mercredi, une commission d'enquête publique qui portera sur les rapports entre les autochtones et la police en général, mais aussi sur les rapports entre la communauté autochtone et le réseau de la santé et des services sociaux, le secteur correctionnel et celui de la protection de la jeunesse. On voudra vérifier si la communauté a fait l'objet de « racisme systémique », mais aussi déterminer les problèmes dans la relation entre les autochtones et les réseaux publics. La Presse; Le Nouvelliste; Montreal Gazette

*** A new purpose - Stories of victims turned survivors**
A sexual predator, the murder of a teenage girl, a missing indigenous woman ultimately found slain - shocking crimes that dominated the news years ago. But what happens after the trial ends and the offender goes to prison? Visit any courtroom and you'll hear of the long-term devastation. But these are the other stories, of victims who became survivors. They found ways to move forward to help themselves and others. Star-Phoenix, D1

*** Secrecy around abuse remains to this day - Silence in James scandal is deafening after soccer, gymnastics revelations**
An opinion piece states "It has been the most enduring - and troubling - question in the sickening saga of Graham James right from the beginning: did hockey's most notorious pedophile really act alone? No accomplices? No enablers? No one covering up for him? No other hockey coaches just like him sexually abusing the young players in their charges? No one else? Really? That's the narrative Canadian hockey authorities would certainly like all of us to believe: 'move along, folks... nothing more to see here. And, don't forget to stop by the box office on your way out.' But it's also almost certainly nonsense, as we were all reminded once again this week with new and spiralling abuse scandals from the worlds of soccer and gymnastics strongly suggesting that if James was truly a lone wolf, both he and the institution (religion?) of Canadian hockey are unique in the world of sport." Winnipeg Free Press, C3

*** Editorial - Don't overuse heavy narcotics**
An editorial states "The epidemic of fentanyl deaths sweeping our province has been blamed, in part, on illicit-drug shipments from China. But while there is no question that a major smuggling operation is underway, this is by no means the whole story. That we are in the midst of an epidemic is unquestioned. The number of overdose deaths this year will rise to more than triple the total in 2008. When the final numbers are tallied, more than 600 fatalities are projected across British Columbia. And Vancouver Island, led by Victoria and Nanaimo, has the highest death rate of any health region in the province. Other parts of Canada are also recording heavy fatalities. So why are Canadians caught up in this fentanyl crisis?... Here is part of the answer. Canadian physicians prescribe far more opioid painkillers than their European counterparts. Specifically, they write three times as many prescriptions for fentanyl, and five-and-a-half times as many for oxycodone - another powerful drug in this class. Is this pure coincidence? Likely not. Studies in the U.S. have shown there is a direct correlation between the number of opioid prescriptions written and the number of overdose fatalities. In essence, painkiller medications like these

are the pathway through which many Canadians become addicts. When their prescription runs out, they turn to street drugs." Times-Colonist

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Why inquiry into missing and murdered Indigenous women should stay focused on its name**
An opinion piece states "Last week, a new coalition called Expand the Inquiry met with federal officials to argue for the need to expand the terms and scope of the inquiry into missing and murdered Indigenous women to include men and boys. The coalition's leader, Chief Ernie Crey of Cheam First Nation in British Columbia, became an advocate for Indigenous women after his sister, Dawn Crey, was killed by Robert Pickton. Crey said he refocused his attention after hearing from families across the country about the lack of advocacy for missing and murdered Indigenous men. His coalition argues that because 70 per cent of murdered Indigenous people are men, they should be included in the inquiry. But that statistic doesn't change the fact that Indigenous women face a significantly higher rate of violent victimization than men, including physical and sexual assault. And it doesn't change the fact the MMIW inquiry was created to explain why Indigenous women are targeted and find ways to stop it." CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Montreal police raid illegal pot shops - Ten people arrested
Montreal police launched raids Friday evening against illegal cannabis stores opened one day prior by Vancouver's self-styled "Prince of Pot," Marc Emery, and his wife, Jodie. Police said they made a total of 10 arrests. Local television outlets broadcast images of police taking away Marc Emery outside one of his stores in the city's Plateau neighbourhood. As he was being led by officers into a patrol car, Emery flashed a peace sign with his fingers and said: "It's despicable and an injustice, but we will win. The prime minister is a disgrace... A few hours earlier, Prime Minister Justin Trudeau told reporters in Montreal that "until we've changed the law, the current laws exist and apply." Ottawa is moving "properly and responsibly" to legalize marijuana, Trudeau said, but the current law governing cannabis will stand until new legislation is ratified. "The reason we are legalizing and controlling marijuana is not for any other reason than to better protect our kids and to remove the black market, the criminal elements, organized crime, from profiting massively from the sale of cannabis," he said alongside Quebec Premier Philippe Couillard. Canadian Press (Times-Colonist, A10; Cape Breton Post; Chronicle-Herald)

Le pot n'est plus ce qu'il était
Durant la transaction, l'acheteur avait le coeur qui battait fort. L'excitation de faire quelque chose de défendu s'emparait de son corps. On dissimulait la marchandise au plus profond de son sac à dos. Et chaque fois qu'on croisait un policier, on se disait : « S'il savait... S'il savait... ». On se sentait despérado. Un hors-la-loi, un anticonformiste, un rebelle. On allumait son pétard en faisant un pied de nez à la société. Je quitte votre monde corrompu. À moi les vapeurs d'un monde meilleur. En entonnant du Harmonium : « Pour un instant, j'ai respiré très fort... Hee ! Haw ! » Presque 50 ans plus tard, jeudi dernier à Montréal, des gens faisaient la queue devant la boutique Cannabis Culture pour aller s'acheter du pot. Comme on fait la queue devant la boutique Apple pour s'acheter un iPhone. Au vu et au su de tout le monde. Ça ne peut pas être plus au grand jour que ça. Il y a même des caméras. Personne ne se cache le visage. Pas de pixels ajoutés sur les yeux au montage : « Que faites-vous là ? - Ben, j'm'en viens acheter du pot, c'est une boutique de pot. » La Presse

*** Trudeau says current pot law in place until new legislation passes**
Ottawa is moving "properly and responsibly" to legalize marijuana but the current law governing cannabis will stand until new legislation is ratified, Prime Minister Justin Trudeau said Friday. Cannabis activists opened six shops in Montreal on Thursday in defiance of the current law and said they are considering opening another in Trudeau's riding in the city. Longtime marijuana advocate Marc Emery said Trudeau

would be as much of a criminal as them if they were arrested. Trudeau's response to a question about that comment was as follows: "Until we've changed the law, the current laws exist and apply." "The reason we are legalizing and controlling marijuana is not for any other reason than to better protect our kids and to remove the black market, the criminal elements, organized crime, from profiting massively from the sale of cannabis," he told a news conference alongside Quebec Premier Philippe Couillard. "We will get this done properly and responsibly because that is what Canadians expect us to do . . . and until we have changed the law, the current laws apply." Canadian Press (Chronicle-Herald, A10; Whig-Standard)

*** Vancouver Island cannabis growers high on legal pot prospects**
Licensed medical marijuana producers on Vancouver Island are already angling for expansion into a legalized recreational market as proposed new rules take shape. The Task Force on Cannabis Legalization and Regulation recommended this week keeping a separate framework for supplying recreational pot to Canadians. Meanwhile, two of the three dozen companies licensed to supply medical marijuana to Canadians are already laying the groundwork for diversification into the multi-billion dollar recreational market. Executives for Tilray, based in Nanaimo, B.C., and United Greeneries Ltd., in nearby Duncan, endorse the task force's main recommendations, including a minimum age of 18 for purchase of pot, a ban on advertising and sales through stand-alone outlets or mail-order. Brendan Kennedy, president of Tilray, said the company will expand into recreational marijuana, but it won't be a simple matter of ramping up production. CBC News

*** Les coûts du pot légal sur la santé**
Les économistes s'entendent là-dessus : le pot deviendra bien plus populaire s'il est légalisé. Or, même si cette popularité aura certains effets positifs sur l'économie, elle engendrera aussi des coûts sociaux importants. Plusieurs lecteurs m'ont rappelé ces coûts indirects à la suite de ma chronique « Le pot créera-t-il de la richesse ? », parue hier. La chronique se terminait justement par cette préoccupation de la plupart des études sur les effets de la légalisation sur la santé publique. Courriel du lecteur Daniel Masse : « La hausse de consommation provoquera une hausse des coûts des soins en santé mentale, en oncologie (la fumée de pot est aussi cancérigène que celle du tabac), en accidents de voiture, en accidents du travail et autres accidents causés par l'intoxication. Dans son ensemble, la légalisation de la marijuana aura un impact plus négatif que positif sur les finances publiques. Je demeure pour sa légalisation à la condition que cela se fasse en mode fumeur payeur. » Ce genre de coûts indirects est très difficile à évaluer. Le Conference Board a fait l'exercice pour le tabac et les chiffres sont épeurants. Selon l'organisme, le tabac est la cause de plusieurs maladies, notamment la maladie pulmonaire obstructive chronique (MPOC) et le cancer du poumon. À elles seules, ces deux maladies engendrent des coûts annuels de quelque 10 milliards de dollars au Canada (environ 2,5 milliards au Québec). La Presse, 6

PUBLIC SERVICE / FONCTION PUBLIQUE

Single mom gets Phoenix-related claims approved after going public
Claire Lavallee's kids will get a Christmas after all. The single mom feared she would not be able to put presents under the tree for her two children after getting caught up in the Phoenix pay system fiasco. But two days after the public servant's story aired on CBC News, the government agreed to give her nearly $1,000 to cover most of the out-of-pocket expenses she racked up while being paid improperly. "Everything's going to be great," a relieved Lavallee said in a phone interview. "I'll be able to finish buying gifts for my kids this weekend." Lavallee first went weeks without pay, and was then was underpaid for months, after returning to work from a maternity leave in April... Tens of thousands of public servants have been underpaid, overpaid, or not paid at all since the government launched its new payroll system last April. Ottawa has hired more than 200 compensation advisors for satellite offices across the country to resolve the issues. It has also opened a call centre in Toronto with more than 100 agents to assist public servants. In September, Public Services and Procurement Canada announced it would reimburse workers for certain types of expenses, like interest charges and penalty fees, incurred as a result of improper pay. CBC News

'This was a terrible idea that was always going to be a disaster'
A former senior Conservative advisor says he and others tried to warn the government about a web project that's now at risk of turning into a billion-dollar boondoggle. "This was a terrible idea that was always going to be a disaster," says Kasra Nejatian, a former director of strategy for Citizenship and Immigration Canada. As early as 2011, bureaucrats at the powerful Privy Council Office worked to persuade the prime minister's office that merging the 1,500 different government websites under the single Canada.ca portal was a good idea. An initial contract of $1.54 million was issued in 2013 to Adobe to begin work on the project. It's unclear if the government had any idea of the actual scope of the project. The contract value has since risen to just under $10 million. Yet experts predict the cost of the project - which is only an estimated 0.5% complete despite having already passed its original deadline - could balloon to $1 billion. Ottawa Sun, A8 (Toronto Sun); Postmedia News (Windsor Star)

* **'Dismal' record on hiring of wounded vets**
Just over 25 per cent of veterans who were given priority hiring status in the federal public service because the military released them for medical reasons weren't able to find jobs, according to newly released statistics. Five hundred and eighty-five individuals released from the Canadian Forces for medical reasons between 2005 and early 2016 were unsuccessful in finding work with federal departments within the period for which they were allotted priority status for employment appointments, and as a result lost that status. That has prompted one Liberal senator to call on federal departments to step up. "There's no reason why more of the injured aren't being hired," said Senator Percy Downe, who obtained the job statistics from the government. "Most departments have a dismal record of hiring veterans."... Since 2005, when those medically released from the Forces have been eligible for priority status, the bulk of hiring of those eligible has been by the Department of National Defence. Since 2005, it has been responsible for 70 per cent of the hires of those with priority-status, some 928 veterans. **Correctional Service Canada** hired five per cent, or 66 veterans, according to the figures provided to Downe. Postmedia News (National Post, A8)

OTHER / AUTRE

Military aims to stop ISIL's 'spillage' outside of Iraq, Syria
Two Canadian military teams are in Lebanon and Jordan as the international community searches for ways to keep the Islamic State of Iraq and the Levant from spreading once the city of Mosul falls. Senior military commanders have warned that victory in Iraq's second-largest city will not mark the end of ISIL as a threat, but that the group will instead go underground and resort to suicide attacks and similar tactics. There are also growing fears that defeat in Iraq and Syria will see ISIL attempt to spread into the surrounding region, where it will try to foment fresh havoc and instability. British Defence Secretary Michael Fallon said Thursday that preventing that spread will be a key focus for those countries involved in the fight against ISIL -- also known as ISIS and Daesh -- in the coming months. "We need momentum across the Middle East to defeat Daesh wherever it now disperses to," Fallon said at the start of an anti-ISIL meeting in London. "As they are pushed out of Iraq, they will disperse and move to different theatres and redefine their success not by territory, but by insurgency." Speaking by phone after the meeting, Defence Minister Harjit Sajjan said Canadian troops will remain in Iraq for the foreseeable future to ensure local forces can maintain peace and security. Canadian Press (Cape Breton Post)

* **Quebec woman pleads guilty to smuggling $30.5M worth of cocaine**
A published report says a Canadian woman pleaded guilty Friday to her involvement in allegedly importing cocaine into Australia. The Sydney Morning Herald says 28-year-old Isabelle Lagace entered the plea on a charge of importing a commercial quantity of cocaine into the country. Lagace, along with two other Canadians - 64-year-old Andre Tamine and 23-year-old Melina Roberge - were arrested in late August after the MS Sea Princess berthed in the Australian city. Australian Border Force commander Tim Fitzgerald had said detection dogs helped police allegedly find 95 kilograms of cocaine in suitcases. The drugs were worth an estimated $30.5 million. Toronto Star; Le Quotidien

* **Hope for Canadian pastor imprisoned in North Korea**

Canada is calling the case of imprisoned Toronto pastor Hyeon Soo Lim "absolutely a priority" after Ottawa officials travelled to North Korea this week to visit him for the first time and to discuss his release. Lim, 62, has been detained for nearly two years for what North Koreans say was an attempt to overthrow the government. Global Affairs Canada spokesperson Kristine Racicot confirmed Thursday that a ministry delegation "recently visited Pyongyang and was able to undertake a consular visit to Mr. Lim." "The Government of Canada is very concerned about the health, well-being and continued detention of Mr. Lim," Racicot said. "We have been actively engaged on this difficult case." The visit was arranged with the aid of the Swedish embassy acting as a "protecting power" for Canada, which does not maintain a diplomatic presence in North Korea. Until now, Global Affairs Canada has shared little with the public about the fate of the imprisoned Christian minister. However, on Thursday, the Canadian government disclosed it has been working closely with Lim's family. Toronto Star

*** Ontario cabinet minister quits - Community Safety and Correctional Services Minister Orazietti is leaving for family reasons**
Liberal cabinet minister David Orazietti is resigning from provincial politics, setting the stage for a byelection in his northern Ontario riding about a year before the next general election. The Community Safety and Correctional Services minister made the announcement in his Sault Ste. Marie riding Friday, saying he is leaving for family reasons. "A career in politics comes with many sacrifices - for me, that has meant missing many family events and important milestones in my children's lives," said the father of two. Canadian Press (Hamilton Spectator, A10)

*** The battle within our armed forces**
An editorial states "Numbers in a recently released survey of Canadian military personnel were extremely disturbing. They show nearly 1,000 full-time soldiers, almost two per cent of the regular workforce, report being sexually assaulted in the last year. In November, a proposed class-action lawsuit claimed systemic discrimination in respect to gender and sexual orientation in a Canadian Armed Forces described as rife with sexual misconduct and harassment of women. In October, RCMP Commissioner Bob Paulson delivered an apology to hundreds of current and former female officers and employees subjected to alleged incidents of bullying, discrimination and harassment. This all shines a bright light on a dark corner of our uniformed personnel and an absence of respect for women in the workplace." Chronicle-Herald (Hamilton Spectator, A14)

INTERNATIONAL

Powerful quake hits off Papua New Guinea; no damage reported
A powerful earthquake struck off the coast of the Pacific island nation of Papua New Guinea on Saturday, and a tsunami threat was issued to areas near the epicenter. There were no immediate reports of injuries or damage. The magnitude-7.9 quake struck 46 kilometers (29 miles) east of Taron in Papua New Guinea, the U.S. Geological Survey said. The quake was deep, at 103 kilometers (61 miles). Deeper earthquakes tend to cause less damage than shallow ones. The Pacific Tsunami Warning Center said there was a threat of a tsunami in Papua New Guinea and nearby areas. The quake rattled residents near the epicenter on the island of New Ireland, but was not felt in Papua New Guinea's capital, Port Moresby, said Mathew Moihoi, an official with the Geophysical Observatory. There were no immediate reports of damage, though officials were still assessing the situation, he said. Papua New Guinea sits on the Ring of Fire, the arc of seismic faults around the Pacific Ocean where earthquakes are common. Associated Press (Washington Post)

Navy's underwater drone seized by Chinese warship, pentagon says
A Chinese warship seized a U.S. navy unmanned underwater glider that was collecting unclassified scientific data in the South China Sea, and the U.S. is demanding its return, the Pentagon said Friday. Navy Capt. Jeff Davis, a Pentagon spokesman, said that the U.S. has issued a formal diplomatic complaint over Thursday's incident, but he was not aware of any response yet. He said this may be the first time in recent history that China has taken a U.S. naval vessel. The Chinese Embassy said it had no immediate comment. But the incident is likely to fray the already tense relations between U.S. and China. Beijing was angered by president-elect Donald Trump's decision to talk by phone with Taiwanese

President Tsai Ing-wen on Dec. 2, and by his later comments that he did not feel "bound by a one-China policy" regarding the status of Taiwan. There also have been increased tensions over Beijing's ongoing military buildup in the South China Sea. It includes the development and militarization of manmade shoals and islands aimed at extending China's reach into the Pacific region. Postmedia News (Windsor Star, N6)

*** Turquie: au moins 13 soldats tués dans un attentat**

Au moins 13 soldats turcs ont été tués et 48 blessés dans un attentat visant un bus qui les transportait samedi matin à Kayseri, dans le centre de la Turquie, a déclaré l'armée turque. Les soldats - des non gradés et des sous-officiers - avaient obtenu la permission de quitter le quartier général des commandos pour la journée, a expliqué l'armée dans un communiqué. Elle a précisé qu'il pourrait y avoir des blessés civils. L'explosion, survenue à 8 h 45 (heure locale), s'est produite une semaine après l'attentat qui a fait 44 morts dans le coeur d'Istanbul, revendiqué par un groupe armé kurde. AFP (Journal de Québec)

*** Reprise des évacuations à Alep**

Un nouvel accord a été conclu pour achever l'évacuation des secteurs de l'est d'Alep encore tenus par les rebelles, ont confirmé samedi un chef rebelle et un responsable du gouvernement syrien. L'accord prévoit l'évacuation des deux villages chiites de la province d'Idlib assiégés par les insurgés, Al-Foua et Kefraya, l'évacuation des personnes blessées de Madaya et Zabadani, deux communes bloquées par les forces progouvernementales près de la frontière libanaise, et l'évacuation totale de la partie d'Alep-Est encore tenue par les rebelles. L'évacuation, qui avait commencé jeudi, a été interrompue vendredi par l'armée syrienne, qui a accusé les rebelles de « ne pas respecter les conditions de l'accord », en ayant tenté d'ouvrir le feu et d'avoir voulu sortir d'Alep avec des armes moyennes et des otages. Radio-Canada; Postmedia News (London Free Press, N6; Windsor Star; Leader-Post; Vancouver Sun; Edmonton Journal); Globe and Mail; AFP (Journal de Montréal)

The fall of Aleppo: Four sobering lessons

An opinion piece states “To name a mass atrocity as enormous in scale and as heartbreaking in detail as what Syrian President Bashar Hafez alAssad's forces did to retake Aleppo from his civil-war opponents this week after four years of heartless siege, you have to reach deep into the previous century. Nothing in this century - and it has had several mass atrocities - has come close to the 400,000 lives lost, the 10 million rendered homeless, the gas attacks, the barrel-bombing of residential districts, the mass executions, the denial of medical assistance, the forced starvation and torture delivered by Mr. al-Assad. The fall of Aleppo, delivered with massive Russian support and no concern at all for humanitarian law, UN Security Council resolutions or basic human decency, is a decisive moment: It means Mr. al-Assad will remain nominally in control of the most important parts of Syria. But it is not a terminal moment: His artificially engineered hold on power virtually guarantees the atrocities will continue, the civil war will not be resolved and chaos and extremism will reign in the country's northeast, where the Kurdish-dominated rebels are using adjoining Turkey to battle for control against the Islamic State.” Globe and Mail, F7

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
March 16, 2016 / le 16 mars 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Deaths prompt agency review
The Liberal government says it is looking for ways to improve scrutiny of Canada's border agency amid mounting calls to create an independent watchdog for the organization. The office of Public Safety Minister Ralph Goodale said Tuesday the government "is examining how best to provide the Canada Border Services Agency with appropriate review mechanisms." The statement came as civil rights groups and refugee lawyers decried the second death of someone in the border agency's custody in less than a week. The agency holds people who are considered a flight risk or a danger to the public and those whose identities cannot be confirmed. In 2013-14, it detained 10,088 immigrants - almost one-fifth of them refugee claimants - in a variety of facilities, including federal holding centres and provincial and municipal jails. On March 7, the border services agency was notified by the Ontario Ministry of Community Safety and Correctional Services that an individual in immigration detention at the Toronto East Detention Centre had died. On Sunday, the border agency was advised by the Ontario ministry that a person detained at the Maplehurst Correctional Complex had died. A border agency spokeswoman declined Tuesday to identify the two individuals, citing privacy law. The agency's mandate requires it to use detention ***"only when necessary" and to "safeguard the health, well-being and safety of detainees,"*** noted **Scott Bardsley, a spokesman for Goodale**. The minister is ***"concerned about the two recent deaths" and his thoughts are with their families*****, Bardsley** said. ***"However, we are***

unable to comment about these cases while they are under investigation." Canadian Press (chronicle-Herald, A6, Red Deer Advocate, National Post, Toronto Star, Cape Breton Post, Guardian, Waterloo Region Record, Times Colonist, Times and Transcript)

Detainee deaths spark calls for border services oversight

The government is considering an oversight body for the Canada Border Services Agency following the deaths of two immigrant detainees in CBSA custody last week. Rights and refugee groups have long called for independent oversight of the government agency and the creation of a civilian-led body to investigate deaths in custody. After the two recent deaths, **Public Safety Minister Ralph Goodale's** office said the issue will be examined as part of the government's upcoming public consultations on Canada's national security framework. ***"The government is examining how best to provide the Canada Border Services Agency with appropriate review mechanism,"*** said **Mr. Goodale's press secretary, Scott Bardsley. Mr. Goodale** has said that he is open to considering an oversight body for the CBSA. Josh Paterson, executive director of the BC Civil Liberties Association, said the organization is "encouraged" that the government will consider improved scrutiny of the CBSA. "Any such mechanism has to be completely independent of CBSA," Mr. Paterson said in a statement Tuesday. "At a minimum, it must be able to receive and deal with public complaints and complaints from third parties, initiate its own reviews and investigations of CBSA conduct even when there is no complaint, and include independent civilian investigation of critical incidents of harm or death involving CBSA officers." Globe and Mail, A4; * Radio-Canada

'Allah told me to come here and kill people'

The man accused of a violent attack on a Canadian military recruiting centre comes from a family with a history of severe mental illness, according to a Toronto researcher on extremism and radicalization. Amarnath Amarasingam, a fellow at the George Washington University program on extremism, said he spoke to a close relative of Ayanle Hassan Ali Tuesday. The relative told him Ali's mother has long suffered from either schizophrenia or bipolar disorder and that Ali himself has displayed symptoms consistent with some kind of mental illness for at least the past five years. Ali was charged Tuesday with three counts of attempted murder, one day after he allegedly slashed two Canadian soldiers and narrowly missed a third in a brief, wild rampage in Toronto. The 27-year-old appeared in bail court Tuesday afternoon. He wore a white, prison-issue jumpsuit and spoke only to say his own name. His case was put over until Friday, when a full bail hearing will be held. Toronto Police Chief Mark Saunders told reporters Tuesday that Ali was born in Montreal and moved to Toronto in 2011. In between, he lived for a time in Alberta. He was registered as an open studies student at the University of Calgary for two semesters in 2009; he later lived with his mother's cousin in Edmonton, according to Amarasingam. In court Tuesday, Ali wore a neat black beard that stretched several inches off his chin. He kept his eyes down throughout the hearing and shuffled at times from foot to foot... Toronto Police are working with the RCMP, CSIS and the Ontario Provincial Police to investigate the attack. Saunders would not rule out future terrorismlinked charges but he said investigators had yet to identify any link to an outside organization or individual. "I want to be very, very, very careful, when it comes to the national security piece, that we don't go through that Islamophobia nonsense," Saunders added. "I don't want this categorizing of a large group of people. That would be very unfair and very inaccurate."... "I probably know as much about the actual facts surrounding the case as you people do," Burke said. **Federal Public Safety Minister Ralph Goodale** said Tuesday the attack appears to have been an isolated incident. National Post, A1 (Vancouver Sun, Province); * Canadian Press (Edmonton Journal, N1/FRONT, Windsor Star, Leader-Post, Montreal Gazette, Ottawa Citizen, Calgary Herald, London Free Press, StarPhoenix, Guardian, Whitehorse Daily Star, Red Deer Advocate, Waterloo Region Record, Chronicle-Herald, Telegram, Cape Breton Post, Kingston Whig-Standard, Hamilton Spectator, Telegraph-Journal, Times and Transcript); * Presse canadienne (Le Devoir, A4, Le Quotidien)

Be proactive at stopping radicalization, Goodale says

Public Safety Minister Ralph Goodale says so-called lone-wolf terrorist attacks are some of the most difficult to prevent and that's why Canada needs to be among the best in the world at stopping radicalization. **Goodale** says indications are that the man who attacked two soldiers at a north Toronto military recruitment centre was acting on his own. He says it is important that Canadians remain vigilant against possible terrorist attacks and alert police to any suspicious behaviour. But **Goodale** also says

authorities need to reach out to communities susceptible to radicalization. Canadian Press (Waterloo Region Record, A3, Cape Breton Post)

National security policy under review, says Goodale

Public Safety Minister Ralph Goodale says his department is undertaking a national security review. ***"We want open, inclusive consultations that reassure Canadians that their engagement is not just a window dressing but that it's meaningful and has impact,"*** the minister told a recent Ottawa defence conference. **Mr. Goodale** said the government is looking for ***"thoughtful discussion, analysis [and] debate."*** He specifically cited a National Post op-ed by Luc Portelance, former president of the Canada Border Services Agency and Ray Boisvert, former assistant director of intelligence at Canada's spy agency, the Canadian Security Intelligence Service. Their message was that the government has a ***"timely opportunity to consider a thorough assessment of our national security structure" and advocated a "national security reset."*** That kind of input is **"very valuable," Mr. Goodale** said, adding expert opinion will be ***"taken very seriously into account."*** (…) **Mr. Goodale** told reporters after his remarks that he didn't mean to use the word "review" as a ***"term of art." "We need to examine a broad collection of things related to national security,"*** he said. ***"This will involve a very extensive examination of our security and intelligence operations now and how we can make them better."*** As to the method, **Mr. Goodale** said, ***"we will begin the process by circulating materials that we would invite Canadians to comment on. Where that leads at the end of the process, we'll have to see what the process itself generates."*** It's unclear what those materials might be. But **Mr. Goodale** said some of the work has already started. A committee of Parliamentarians will scrutinize Canada's security groups, while Public Safety is looking to establish a new counter-radicalization office, he said. There is also the issue of Canada's controversial Anti-Terrorism Act. ***"We will be consulting Canadians broadly and Parliamentarians and subject matter experts to revise the provisions in the law,"*** he said, although he didn't provide a timeline. Embassy

Trump shouldn't be allowed into Canada: petition

In a development that might spur even more U.S. electors to thoughts of moving to Canada should Republican presidential nominee Donald Trump win, an electronic petition with more than 2,000 signatures is calling on the Liberal government to prohibit him from entering Canada until he withdraws comments he made about Muslims during his campaign. The e-petition, sponsored by New Democratic Party MP Kennedy Stewart (Burnaby South, B.C.), has been certified by House of Commons officials who verified the electronic signatures and says Mr. Trump's entry should be denied on grounds he is inadmissible to Canada because his call for a ban on Muslims entering the U.S. constitutes a hate crime in Canada. With 2,345 signatures, the e-petition, formally logged under the heading "E-54 (Inadmissibility to Canada)" on Parliament's website numerically ranks well below an e-petition signed by 21,944 gun owners who want **Public Safety Minister Ralph Goodale** (Regina-Wascana, Sask.) to allow over-the-counter sales of semi-automatic AR-15 assault-style hunting rifles. Hill Times (2016-03-15)

DND still conducting full security review 18 months after ISIL-inspired attacks

National Defence launched a full-scale review of security at its installations, including recruiting centres, following the terror attacks of October 2014 — an assessment that officials said Tuesday is still ongoing. The wounding of two uniformed soldiers in north Toronto this week is the second violent incident to take place at a military centre. Defence officials undertook a full review of what's known in army lingo as its "force protection posture" following the Oct. 20, 2014 attack in Saint-Jean-sur-Richelieu, Que., which killed Warrant Officer Patrice Vincent. The 53-year-old soldier and a companion were run down by a "radicalized" Martin Rouleau outside a federal building that offers support to Canadian military veterans and other personnel. Vincent was killed and the second soldier was injured. Rouleau, 25, fled the scene but was later shot dead after a pursuit in which his car rolled over. Friends said he had become increasingly radicalized. The defence department did not advertise its security review, but one of the country's senior operational commanders — Maj.-Gen. Christopher Coates —testified about it before a House of Commons committee four months after the deaths of Vincent and Cpl. Nathan Cirillo, on Oct. 22, 2014, who was gunned down at the foot of the National War Memorial. Almost 18 months down the road, defence spokesman Capt. Thomas Edelson said the review has yet to be finalized. (…)**Public Safety Minister Ralph Goodale** said many recruiting centres are "***storefront operations***" that must balance security and accessibility for the public. "***I'm sure DND of all departments would make sure***

security arrangements were always appropriate," he said. Canadian Press (News 1130, The Telegram, The Guardian, Cape Breton Post, CTV News, Huffington Post), Presse canadienne (L'actualité)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Latest avalanche victims came from Alberta**
The Mounties have confirmed a man killed Monday in an avalanche near Blue River, B.C., is from Sherwood Park. A second Alberta man also died, but his hometown has not yet been made public. At 5:45 p.m. Monday, Clearwater RCMP received a call from a group of snowmobilers that an avalanche had buried two men from their group 30 kilometres southwest of Blue River. Five of the seven snowmobilers escaped the avalanche. Members of the group, equipped with rescue equipment, were able to dig the two men out of the snow. Efforts to resuscitate the pair were unsuccessful. The survivors radioed for help, but due to oncoming darkness and weather conditions they left the area Monday evening. Local search and rescue teams set out at first light Tuesday. Cpl. Mark Labossiere with Clearwater RCMP said poor weather made it difficult to get a helicopter to the site. The deaths came one day after Avalanche Canada official Joe Lammers urged backcountry skiers and snowmobilers to take special care as March is statistically the most deadly month for avalanches. Edmonton Journal (Edmonton Sun, A8; Edmonton Journal); Vancouver Sun (Times Colonist)

*** Survivor tells story of terrifying plunge inside an avalanche**
A relaxing Sunday in the mountains near Jasper took a terrifying turn when Dana Ruddy found himself being swept down the side of a mountain by an avalanche. Ruddy was with his long-time skiing and climbing buddy, Sean Elliott, hiking and skiing through mountain passes about 25 kilometres southeast of Jasper (...) But as they worked their way down a mountain pass above the Maccarib Campground, a large piece of ice and snow Ruddy had just crossed gave way. "It was just like basically a big steep dinner plate that kind of all started breaking up," Ruddy said. "So I kind of pointed my skis downhill and did the best I could to get out of the way, and try to ski out of the avalanche." Elliott was above the avalanche, watching in horror as his friend was swept away. "I called out 'avalanche' as soon as I knew that it was happening, and Dana tried really, really hard to outrun it, to ski out of the avalanche. But it was too big, too broad." CBC News

*** Three more deaths spur renewed calls for avalanche safety**
Experienced riders are urging fellow snowmobilers to get serious about avalanche safety after the deaths of three more sledders this week. Two Alberta snowmobilers were killed Monday while exploring the backcountry as part of a group of seven near Blue River, northeast of Kamloops, and another man died after being buried by a slide near Castlegar. So far this year, 12 snowmobilers and one skier have been killed by avalanches. While the total number of avalanche deaths in 2016 is in line with the 10-year average recorded by Avalanche Canada, officials with the safety organization say the proportion related to snowmobiling is noteworthy. According to Penny Cartwright of the B.C. Snowmobile Federation, most of those deaths could have been prevented with proper training and equipment. Between 7,000 and 8,000 people take avalanche safety courses across Canada each year, but snowmobilers only make up about 10 per cent of each class - even though they're the largest group of backcountry users, according to Avalanche Canada. Vancouver Province, A10

*** Molson Coors faces criticism for ad showing skiers going out of bounds**
The B.C. Search and Rescue Association is criticizing a Coors Light ad campaign that shows skiers having fun as they go out of bounds. The ad, which recently aired on television and was also posted on YouTube, was part of a campaign called #BraveTheCold. It shows three skiers heading down a trail while a narrator asks, "will you brave going out of bounds?" On Tuesday, BCSARA said the advertisement's messaging raised a high level of concern. "Brave The Cold focuses on the thrill of adventure ... and includes 'going out of bounds' as a 'good decision,' which is a complete contradiction of BCSARA's safety message," BCSARA said in a statement. CBC News

*** New choppers ready for action**
Fifteen new helicopters are ready for action in the Canadian Coast Guard fleet. On Monday, Fisheries Minister Hunter Tootoo, Procurement Minister Judy Foote and Canadian Coast Guard commissioner Jody Thomas accepted the last of the model 429 light lift helicopters built by Quebec-based Bell Helicopter Textron Canada Ltd. The $172-million contract was awarded in 2014 and the project delivered on budget and ahead of schedule. Dartmouth-Cole Harbour MP Darren Fisher was on hand at the Canadian Coast Guard hanger at 12 Wing Shearwater in Dartmouth Monday to inspect the newest helicopter. Another one will be delivered to the base later this month. According to a government press release, 12 of the new helicopters are already in service across the country carrying out Canadian Coast Guard missions, including at Shearwater. The remaining three helicopters are undergoing pilot training. "These made-in-Canada light-lift helicopters are faster, safer, more reliable and more efficient than the models they are replacing," said Tootoo in the release. Chronicle-Herald, A5

*** Un organisme bénévole de Rivière-à-Pierre possède de l'équipement de sauvetage**
Alors que les ambulanciers ne sont pas équipés pour s'aventurer dans des voies non carrossables, le groupe de bénévoles Recherche et sauvetage de Rivière-à- Pierre possède son propre véhicule d'urgence pour motoneige, qui aurait pu servir à sauver l'Américain tragiquement décédé, le 2 mars dernier. À la suite du décès de Glenn Dumont lors d'un accident de motoneige survenu dans le parc des Laurentides, Michel Voyer, secrétaire de l'organisme, s'explique mal pourquoi les ambulanciers à proximité des sentiers n'ont pas plus facilement accès à ce type d'équipement. «Ça prend ça, insiste M. Voyer. Les ambulanciers de notre région, ils embarquent avec nous autres, car le ministère de la Sécurité publique nous y oblige», observe-t-il. Le Journal de Québec, 19 (Le Journal de Montréal)

*** Un déversement en mer serait très difficile à contrôler**
Un déversement d'hydrocarbure en eau salée serait extrêmement difficile à circonscrire. Témoignant, mardi, devant le Bureau d'audiences publiques sur l'environnement (BAPE) qui se penche sur le projet d'oléoduc Énergie Est, le professeur Émilien Pelletier, de l'Institut des sciences de la mer de Rimouski, a expliqué qu'une nappe de pétrole en mer n'est pas homogène (...) Les audiences du BAPE portent, mardi après-midi, sur les impacts d'un déversement sur les milieux sensibles, la flore et la faune. David Berryman, du ministère de l'Environnement, a utilisé le déversement survenu lors de la catastrophe de Lac-Mégantic, en juillet 2013, comme point de référence. Il a notamment démontré que la rivière Chaudière avait été affectée de façon importante et, en plus de causer la fermeture de plusieurs prises d'eau pendant quelques mois, le déversement survenu lors de la catastrophe avait entraîné des travaux importants de décontamination qui n'avaient pas réussi à rétablir complètement le cours d'eau. La Presse Canadienne (Le Droit, 41); Le Soleil, 15

*** Vaudreuil's new signage urges trains to slow down**
Vaudreuil-Dorion has installed new speed-limit signs along freight train tracks that evoke the tragedy of the deadly Lac-Mégantic crude oil shipment derailment of 2013.
Mayor Guy Pilon said the recently installed 55 km/h speed limits for passing trains are a symbolic gesture and are not legally binding. A trio of red signs, installed in different locations along the tracks, replaced older ones that were taken down last year by the municipality. "It's to make sure the engineers who drive the train remember what happened in Lac-Mégantic and to slow down," Pilon said. "No one, not even the companies, want that to happen again." Montreal Gazette, D14

*** Les cours d'eau sous haute surveillance**
Signe de l'arrivée imminente du printemps et du temps doux, les autorités auront à l'oeil, au cours des prochaines semaines, les nombreux cours d'eau de la province afin d'y prévoir le débit et de déterminer les endroits où les crues printanières pourraient causer des problèmes (...) De fait, les températures chaudes et les faibles précipitations enregistrées au cours de la saison hivernale ne signifient pas pour autant que la province sera épargnée par les inondations durant l'année 2016. «Difficile de dire pour l'instant si ce sera une saison difficile ou non, tout va dépendre de ce que la météo va nous apporter au cours des prochaines semaines», a indiqué Nadine Caissie Long, du ministère de l'Environnement et des Gouvernements locaux. Selon elle, ce sont les précipitations, sous forme de pluie, qui vont s'abattre prochainement - ou non - sur la province qui détermineront si le Nouveau-Brunswick aura à nouveau à faire face à des risques d'inondations ce printemps. L'Acadie Nouvelle, 7; CBC News

*** Fast-flowing water a concern this week**
Warm temperatures and rain could cause floods in low-lying areas Conservation Sudbury has issued a watershed conditions statement for all parts of the Greater Sudbury watersheds effective 1 p.m. on March 15. This statement will remain in effect until another update is provided. Conservation Sudbury remains in direct contact with the City of Greater Sudbury and all other partners as required. Northernlife.ca

*** Pipe break floods ice road entrance**
A crew from the Department of Transportation was hard at work on Monday, using a grader and a front-end loader to try to smooth out the Yellowknife entrance to the Dettah ice road. That part of the route across Yellowknife Bay was badly rutted and partially flooded over the weekend after a water line break several blocks away. "We found out as early as Friday that there is water seeping in from the city's storm drains," said Michael Conway, the department's regional superintendent. "We had a grader out there and crews worked all weekend trying to move the water and slush to the side and maintain as smooth a driving surface as possible." Yellowknifer

*** Death from flu confirmed**
A Kingston-area person has died of the flu, the region's medical officer of health has confirmed. The recent death from influenza highlights the need for people to do what they can to limit the potential impact of the virus, according to Dr. Ian Gemmill, medical officer of health with Kingston, Frontenac and Lennox and Addington Public Health. The 2015-16 flu season is winding down, but, as of last week, 85 labconfirmed cases of influenza and one outbreak in a long-term care facility had been detected in the Kingston area, said Dr. Gemmill, who would not confirm the identity of the local victim. Kingston Whig-Standard, A1/FRONT

NATIONAL SECURITY / SÉCURITÉ NATIONALE

STABBING SUSPECT FACES NINE CHARGES
Ayanle Hassan Ali walked alone into the Canadian Forces recruitment office Monday afternoon, then the tall, bearded man - now accused of attempting to murder three military officers - allegedly uttered a statement that transformed a disturbing assault into a possible terrorist attack. "Allah told me to do this. Allah told me to come here and kill people," Ali is said to have declared, moments before he was subdued by army members, according to Toronto police Chief Mark Saunders. But as the details of the attack became clearer Tuesday, the possible motivations turned murky, suggesting the case may not have been simply a "lone wolf" terrorist attack. Separate sources close to the family told the Star that Ali, 27, had been struggling with both family and mental-health issues. "This has nothing, nothing to do with crazy terrorist organizations," Mariam Adam, a first cousin of Ali's mother, told the Star of the attack. "He's just a very sick person who needs help," added Adam, who lives in the United States and who lived for a time with the accused. Ali, who has no previous convictions, now faces nine charges stemming from the mid-day attack, including three counts of attempted murder against members of the Canadian Forces: Ryan Kong, Jesus Castillo and Tracy Ann Gerhardt. Gerhardt escaped unharmed, while Kong and Castillo were treated for minor stab wounds. Toronto Star, A1; Toronto Sun, A3; La Presse, 5; * Canadian Press (Record, A3)

*** Attacker said higher power drove him**
In the midst of a frenzied attack on soldiers at the Canadian Forces recruiting centre in north Toronto on Monday, the attacker declared he was driven to violence by a higher power. "Allah told me to do this. Allah told me to come here and kill people," the attacker yelled as he was wrestled to the ground after injuring two people. Those words now have authorities exploring potential terrorism charges. In a Toronto courtroom on Tuesday, police charged Ayanle Hassan Ali, 27, with a litany of offences, including three counts of attempted murder. Yet people who know Mr. Ali say he is not known as a violent fanatic. Rather, the Canadian Muslim of Somali heritage has become increasingly erratic and withdrawn. Lately, he has been given to talking about conspiracy theories, more about the Illuminati than Islam. In cases like this, police and prosecutors are finding that religious motivations and a precarious mental state can mix in the minds of the same suspects. This creates questions about motivation and culpability, and whether

crimes can truly be considered terrorism. "I think there's a lot of assumptions made that people who are mentally ill can't also be radicalized, but people can experience both. That link isn't mutually exclusive," said Amarnath Amarasingam, a terrorism researcher at the University of Waterloo... The chief said his force is working with federal investigators - including the RCMP and the Canadian Security Intelligence Service - to see if AntiTerrorism Act charges can be laid. But such investigations are painstaking, he cautioned. "It's a slow-moving process," the chief said, adding that the wider public should not rush to any judgments. "One of the things I want to be very, very careful of, when it comes to the national security piece, that we don't go through that Islamophobia nonsense."... The case bears some parallels to the events of October, 2014, when two extremists killed two Canadian Forces soldiers in attacks two days apart. Both suspects were shot dead by police. In a speech in Ottawa earlier this year, **RCMP Commissioner Bob Paulson** spoke about how the difficulties of such cases like those were compounded by questions about the suspects' mental states. "I'm very aware that a big chunk of our vulnerable potentially radicalized people in Canada may have mental-health issues," he was quoted as saying at the time. Globe and Mail, A4

*** 'Very Upset'**

"Allah told me to do this." Toronto Police Chief Mark Saunders says a 27-year-old Toronto man uttered those words Monday to people at a Canadian Forces recruitment centre on Yonge St., north of Sheppard Ave., minutes after attacking and injuring two uniformed soldiers with a knife. During a media briefing Tuesday, Saunders said that while he couldn't definitely call it a terror attack, it hadn't been ruled out in light of those cryptic comments. "While at the scene, the accused stated, 'Allah told me to do this,' " Saunders alleged. "'Allah told me to come here and kill people.' " Saunders said investigators have found no indication the man was working with anyone else or with a terror group. The chief declined to comment further on the man's remarks at the scene, but acknowledged they raise the spectre of a terror attack. "Certain comments were made that fit a profile," he said. "There needs to be more ... it can't just be one statement made." The man allegedly arrived shortly after 3 p.m. at the recruitment centre and attacked a soldier near the door. After repeatedly striking the soldier, he drew a knife and slashed him on the upper arm, according to police. As the attacker advanced, he encountered another soldier. He slashed at her, but she escaped unharmed, investigators said. The suspect was allegedly restrained by soldiers before police arrived. Another soldier received minor wounds while apprehending the suspect. Both soldiers were released from hospital Monday night. Saunders cautioned people about leaping to conclusions about the suspect's links to any religion or ethnic group in the city. Toronto Sun, A5 (Ottawa Sun, Winnipeg Sun, Calgary Sun), Toronto Star CBC News, Daily Gleaner, Presse canadienne (La Tribune), Global News; Paris Match, Le Figaro, Atlantico (2016-03-15)

*** Let it play out**

Ontario Community Safety Minister Yasir Naqvi issued a brief statement Tuesday on the attack of three soldiers at a Toronto military recruitment centre: "Yesterday's attack was deeply troubling and I am pleased to hear that the two Canadian Forces members have been released from hospital. I wish them both a speedy recovery. As you know, there are multiple investigations currently underway into this incident. I understand that the OPP are working in close co-operation with Toronto Police, CSIS, and the RCMP. It is important that we allow those investigations to take place." Ottawa Sun, A9 (Toronto Sun)

* **'Very scared, very upset'**

The man accused of trying to kill three soldiers at a recruitment office Monday is terrifi ed, his lawyer says. "(Ayanle Hassan Ali) just seems very scared and very, very upset to be in the position he finds himself in," lawyer David Burke, a member of well-known defence lawyer Calvin Barry's firm, told reporters following his client's first court appearance Tuesday. Earlier, police Chief Mark Saunders told reporters the accused said, "Allah told me to do this. Allah told me to come told me to come and kill people," after he allegedly wounded two soldiers with a knife and tried to hurt a third at the Canadian

Armed Forces recruitment office on Yonge St. in North York. Ali is charged with three counts of attempted murder, three counts of assau lt wit ha weapon, two counts of aggravated assault, and awe offence. Postmedia Network (Winnipeg Sun, A28, Calgary Sun, Toronto Sun, Edmonton Sun, Ottawa Sun)

* **Via Rail steps up security after online threat**
Employees at Via Rail have been asked to be vigilant in the wake of an online bomb threat targeting Central Station , the Dorval train station and the Saint-Lambert train station. The Journal de Montreal says the threat came via an e-mail to Via Rail's IT department. It demanded an unspecified payment in bitcoin. Investigators say similar threats have been sent to passenger carriers around the world, and this one has been found to be "baseless". Via Rail says it has still stepped up patrols by it's private security force. The Journal de Montreal says Montreal police have opened an investigation, but they are refusing to confirm the report. CJAD News

* **Charkaoui faces assault charges**
Adil Charkaoui faces three criminal charges in connection with the alleged assault of a security guard at Collège de Maisonneuve last month. The 42-year-old is expected to appear in court on Friday to be formally charged with two counts of assault and with threatening to use a weapon, a door, while committing assault. All three charges allege the victim was assaulted on Feb. 21. The alleged assault reportedly occurred on a Sunday while a gymnasium at Collège de Maisonneuve was being used for a soccer game. One media report said Charkaoui became involved in an altercation when the students who were playing soccer began throwing balls at the security guard. The incident has generated headlines because of Charkaoui's previous successful challenge of having been detained for years, without being charged, through the use of a security certificate imposed on him by the Canadian government that alleged he had ties to terrorists. Charkaoui challenged the validity of the certificate for years until it was removed in 2009. Montreal Gazette, A4

*** Menace de bombes contre des gares VIA Rail**
Plusieurs gares de VIA Rail seront sous haute surveillance ces jours-ci en raison d'une supposée alerte à la bombe. La menace, jugée non fondée, proviendrait de gens qui exigent une rançon en bitcoins. Dans une note interne dont Le Journal a obtenu une copie, VIA Rail invitait hier ses employés à rehausser leur niveau de vigilance. «Le service informatique de VIA Rail Canada a reçu un courriel de menaces exigeant une rançon en bitcoin [monnaie virtuelle] et indiquant qu'une bombe allait exploser dans une de ses gares de train le 16 mars à 18 h», précise la note. Selon nos informations, les trois gares visées seraient celles de Dorval, de Saint-Lambert et la Gare Centrale de Montréal. «Pour augmenter la sécurité de nos employés et de nos passagers, nous vous demandons d'augmenter votre niveau de vigilance dans les jours à venir », dit la note. VIA Rail confirme qu'une menace a récemment été reçue contre ses installations, sans toutefois valider le contenu de la note interne. La menace serait d'ailleurs «sans fondement», assure le porte-parole Malcolm Andrews. «Depuis quelque temps, il semble que les transporteurs de passagers, à travers le monde, font l'objet de menaces non fondées», remarque- t-il. Journal de Montréal (Journal de Québec)

*** Adil Charkaoui aurait utilisé une porte comme arme**
Adil Charkaoui comparaîtra vendredi sous des accusations de voies de fait et d'agression armée pour une altercation avec un agent de sécurité au Collège de Maisonneuve. «Le ou vers le 21 février 2016, à Montréal, district de Montréal, Adil Charkaoui s'est illégalement livré à des voies de fait», lit-on sur un document de cour que Le Journal a pu consulter. Un autre chef indique, quant à lui, que le prédicateur controversé aurait agressé sa victime alors qu'il a «porté, utilisé ou menacé d'utiliser une arme ou une imitation d'arme (une porte)». Fait à noter, Adil Charkaoui a été accusé par procédure sommaire, ce qui est moins grave que s'il avait été accusé par voie criminelle. Ainsi, s'il est reconnu coupable, il risque une peine maximum de quelques mois de prison ou une amende. S'il avait été accusé par voie criminelle, il aurait pu

écoper de 10 ans d'incarcération, advenant sa culpabilité. Journal de Québec, 32 (Journal de Montréal); CBC News (2016-03-15)

*** 'Lone wolf' terrorist attacks hard to prevent**

'Lone wolf' terrorist attacks aren't new in Canada - but they remain near impossible to prevent. In a seemingly random lone attack on Monday in Toronto, a man attempted to kill three Canadian Forces members. He faces nine charges related to the stabbings, which injured two of the officers. The motivation of the accused is not known. However, "lone wolves are particularly difficult to head off at the pass and that's because, often, their violence is driven on a combination of a personal agenda and some sort of ideological fervour that they wrap themselves in," and there can be mental health concerns as well, said James Ellis of the Canadian Network for Research on Terrorism, Security and Society, who was speaking in general terms about such incidents. "These folks are not connected to an organization that can be easily tracked - quite often they are shunned by organizations because they are too volatile, and as a result it makes it very difficult for traditional law enforcement . . . to pick them up in their surveillance net." And if they have no criminal history, they aren't on anyone's radar. "It's an opportunity for them to gain some sort of prominence . . . it's an opportunity for them to go out in a blaze of glory," he said of the lure to commit violence. With technology and the Internet, "what an individual can do today with a drone and a smart phone and good satellite mapping" gives them advantages they didn't have in the past, he added. The network's research has found that since 1960, there have been 377 incidents committed by a lone perpetrator or small groups with no affiliation. "That suggests this is not a new thing to Canada . . . lone wolves are part and parcel of the terror threat and violent extremism threat in Canada." Some previous lone wolves Parliament Hill, October 22, 2014 Cpl. Nathan Cirillo was shot and killed while standing guard at the National War Memorial in Ottawa during the unprecedented attack on Parliament Hill. The lone gunman, Michael Zehaf-Bibeau, then made his way to Centre Block, where he stormed in and was killed in a gunfight with RCMP and House of Commons officers. Saint-Jean-sur-Richelieu, October 20, 2014 Martin Couture-Rouleau was shot and killed by Quebec police after he rammed two Canadian Forces soldiers with his car, killing one, in this attack south of Montreal. He was reportedly known to anti-terrorism investigators and had tried to leave the country to fight overseas after being radicalized. RCMP later said they'd earlier taken Couture-Rouleau's passport and named him a "high-risk traveller." Toronto Star (2016-03-15)

Domestic terrorism is a terrible fact of life, even in Canada. We can't let it drive us to hate

An opinion piece states '' Canada's borders, and our distance from Islamic terrorism's epicentre in the Middle East and North Africa, can't shield us. All kinds of things are "the kinds of things" that happen in Canada. Among them, acts of terror. Police are still investigating whether Toronto was hit by a terror attack Monday, when Montreal-born Ayanle Hassan Ali barrelled into a military recruiting centre in Toronto, stabbing two Forces members and shouting, "Allah told me to come here and kill people." But whatever this investigation reveals, we should be prepared for domestic terrorism. And our reaction should, I think, be split: some outrage, and something more like preparedness. Not complacency, not anything so passive as acceptance, but understanding that this is the world, and the country, we live in now. Extremism has a platform on the web it has never had before. Dangerous ideas spread rapidly. Individuals can commit terrorism unaided, untethered to an organization. People born in Canada, and people radicalized here. Witness Parliament Hill, 2014. Canada's borders, and our distance from Islamic terrorism's epicentre in the Middle East and North Africa, can't shield us. Our intelligence and law enforcement agencies, however, aren't doing such a bad job, according to security expert Martin Rudner. Last year, the RCMP prevented 30 terrorist plots targeting Canada, Rudner said. Rudner, founding director of the Canadian Centre of Intelligence and Security Studies at Carleton University, argues lone-wolf attacks should be taken very seriously." Metro News

*** Islamist terrorism is real and it's here**

An opinion piece states, "Canadians aren't being "Islamophobic" when they worry Monday's attack on an armed forces recruiting centre in Toronto during which two soldiers were stabbed - thankfully, not seriously - might be linked to Islamist terrorism. Not when Toronto Police Chief Mark Saunders tells them the accused said: "Allah told me to do this. Allah told me to come here and kill people." Not when Prime Minister Justin Trudeau rightly tweets in response to the attack that: "Canadians - and the @Canadianforces - will not be intimidated by terror hate. May the CAf members injured yesterday make a

full recovery." We leave it to our justice system to determine whether Ayanle hassan Ali, 27, the man police have in custody charged with multiple offences in connection with the stabbings, is guilty of any crimes, or what his mental state may have been. Obviously, there will be an investigation by our security agencies to determine whether the accused, a Canadian citizen with no criminal record, is affiliated with any terrorist organizations, acted under their influence, or as a so-called "lone wolf". In that context, we understand why Chief Saunders issued a warning against "Islamophobia nonsense" in the wake of this incident. We agree with him. We must never hold all Muslims responsible for what one individual, who may not be a Muslim for all we know, is accused of doing. Toronto Sun, A18 (Calgary Sun, Edmonton Sun)

Waging peace to counter the allure of extremism

An opinion piece by Evan Hoffman, senior associate at the Canadian International Institute of Applied Negotiation, states "Not surprisingly, in the wake of the Paris attacks we've had all sorts of expert opinions on how to defeat ISIS. The approaches have run the gamut from using non-violent counter-narratives, to bombing ISIS strongholds in Syria, as Britain has recently decided to do. It also isn't surprising that we now have two very distinct camps on this issue. Those in the non-violent camp rightly proclaim that bombing will only create more terrorists, where those in the use-of-force camp rightly fear that, if left unchecked, the ISIS threat will spread and grow.The problem with all these approaches, however, is that they are only partial solutions at best. A problem as big and complex as terrorism can't be adequately addressed by a single tactic. This would be naïve and foolish.While it is true we have no past precedent to base our responses on, we know that-as with any complex problem, from preventing genocide to curbing greenhouse gasses-efforts that are multi-sectoral, multi-level and address both short- and long-term factors are required.Countering radicalization and violent extremism, whether foreign or domestic, is no different. This is a very complex problem that will require long-term efforts occurring in several different arenas simultaneously by numerous different government and non-governmental actors (e.g., legal, policy, education, policing, intelligence, etc.). Indeed, nothing short of a whole-of-problem approach will suffice.One of the areas of activity to especially focus on is working with young Canadians in order to take them out of the reach of terrorist recruiters. A recent United States study suggests that it is neo-Nazi and anti-government groups that have inflicted the most damage in the US, and not radical Muslims as is the popular perception. Other evidence clearly shows that ISIS ideology inspires would-be terrorists: it offers them an exciting meaningful purpose to life." Embassy

*** Canada must address the threat of jihad**

An opinion piece states, "By now, most of us are familiar with the sullen-looking face of Ayanie Hassan Ali, who, according to Toronto Police Chief Mark Saunders, said he was inspired by Allah to kill infidels in his name. What may be the latest chapter in Canada's brush with Islamist extremism happened around 3:00 pm Monday. According to Saunders, Ali, 27, entered a military recruitment centre in a Department of National Defence building in Toronto, pulled out a knife and stabbed a uniformed officer at the front desk. He then tried to get past the desk but was tackled by a group of military officers. One soldier was cut while stopping the suspect, according to Saunders. The two people injured suffered non-life-threatening injuries and were treated in hospital. Toronto's police chief said this incident would have been far more serious had it not been for a group of soldiers who stepped in and grappled the attacker to the ground. Even though the alleged attacker was arrested and witnesses told police they heard him say Allah had told him to kill, authorities were initially reluctant to release the name of the attacker or the precise words used in the attack. The fact the alleged attacker was likely a Muslim Canadian gave it a political dimension and, like the rest of the world, the police seemed uneasy about mentioning this." Ottawa Sun, A15 (Toronto Sun, Edmonton Sun, Calgary Sun, Winnipeg Sun), 1, Calgary Sun (Edmonton Sun), 1 (Toronto Sun, Calgary Sun, Edmonton Sun, Ottawa Sun, Winnipeg Sun), Toronto Sun (Ottawa Sun),

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

New Ambassador Bridge inches closer to reality
The twinning of the Ambassador Bridge inched a step closer to reality on Tuesday after the U.S. Coast Guard issued a permit approving the Detroit International Bridge Company's location and plans for a new span. "The coast guard's permit action is based on the potential impact of the project on navigation and the human environment," said coast guard public relations officer Lisa Novak. "Outside of those parameters, we don't have an opinion on whether the bridge should be built." In a news release out of Washington, the coast guard says it completed an environmental assessment in accordance with the National Environmental Policy Act, and the coast guard determined the new bridge "would not have a significant impact on the environment." (…)While not willing to weigh in on this week's decision by the U.S. Coast Guard, a spokesman for the proposed downriver Gordie Howe International Bridge said it will have no bearing on the publicly owned project. "The announcement about the U.S. Coast Guard permit for the Ambassador Bridge Enhancement Project is a matter between the Detroit International Bridge Company and the U.S. federal government," said Mark Butler, spokesman for the Windsor-Detroit Bridge Authority. "The new Gordie Howe International Bridge is being built to provide redundancy, additional capacity, system connectivity through the Rt. Hon. Herb Gray Parkway and connection to I-75, and improved border processing, resulting in greater crossing time predictability," said Butler. Windsor Star, A3; * Detroit News, * Associated Press (Daily Journal, Brown County Democrat, Clay Center Dispatch, San Antonio Express-News, Chron, My San Antonio, Greenfield Daily Reporter, The Republic), * CTV News, * Windsorite.ca, * MLive, * CBC News, * Blackburn News, * Click on Detroit (2016-03-15)

*** Computer glitch causes truck back ups on border bridges**
A Canadian government computer glitch backed up trucks along the entire northern border at mid-day Tuesday before being resolved early in the afternoon. General Manager Ron Rienas of the Peace Bridge Authority said “extensive delays” resulted in truck lanes only after problems with Customs and Border Protection computers began about 11:15 a.m. and were not resolved until about 12:30 p.m. “This happens periodically, and it affected the entire border,” Reinas said, pointing to similar problems at other key border crossings such as the Lewiston-Queenston, Ambassador and Blue Water bridges. He said the 75-minute problem resulted in truck delays that were expected to take several hours to resolve. Buffalo News (2016-03-15)

Province's biggest cities feeling the strain of settling refugees
There is a growing movement among New Brunswick's biggest cities to ask the federal government to temporarily halt the flow of refugees as volunteer organizations struggle to keep up with demand. Both Fredericton and Moncton have asked Ottawa to temporarily delay the arrival of new refugees, while the president of the province's multicultural association says strain is being felt in Saint John as well. Mike Timani, president of the Multicultural Council of New Brunswick, says the province's major cities are temporarily at capacity when it comes to accepting more refugees. "It's a bit of a crunch, but it will ease off and we'll move forward," he said. Some 1,300 Syrians are now in Fredericton, Moncton and Saint John, said Timani. Another 200 are located at the Riverside Resort and Conference Centre in Mactaquac awaiting resettlement. Meanwhile, the Convention of Atlantic Baptist Churches says the flood of Syrian refugees has overwhelmed New Brunswick's major centres and the next wave of newcomers should be located in rural communities rather than being sent to the province's three big cities. Paul Carline, director of inter-cultural ministries with the Convention of Atlantic Baptist Churches, said nobody who's been working on the resettlement of 1,500 Syrian refugees in the province and more than 25,000 across the country has been happy with the speed of their arrival. "There was a rush on that timeline of the end of February and that really didn't have people's best interests in mind," he said. Carline said Ottawa's push to fulfil its promise on time

has negatively impacted both the Syrian newcomers and the province's three major centres. Daily Gleaner, A1 (Times & Transcript, Telegraph-Journal)

Building a nation, 300,000 newcomers a year
Immigration Minister John McCallum has announced his "levels plan" targets for immigration for 2016. The total is 300,000 and it could go higher. The plan is usually tabled by November, but this year's change in government and the frenzy around Syrian refugee arrivals delayed things until March. If the target is achieved, despite this later start toward the goal, it will be the largest number of immigrant arrivals in more than 100 years. That record happened in 1913 when Canada had a population in the eight million range, and welcomed 400,000 people. The new target reflects both a shift in numbers and in emphasis. (…)But the shift is not coming at the expense of economic immigration categories, despite Opposition clamour in the House on announcement day. The targets for immigrants such as highly skilled workers, caregivers, provincial nominees and others will remain near the average achieved in the last few years. This will still be a cause for concern among some premiers who want higher levels for their provincial programs. And issues still have to be addressed around the supply of temporary foreign workers; these stand outside the levels plan for immigrants. There will also be concern among those who sponsor refugees the allowance for new cases is again severely capped at low numbers, including Syrians, at a time when there is a public appetite to do more. The 2016 focus is on reducing those overseas backlogs, and training and equipping of staff to augment the visa posts will take time. Winnipeg Free Press

Erdogan presses Trudeau on free trade
Turkey wants a free trade deal "as soon as possible" with Canada, and Ankara's top leaders have raised the matter personally with Prime Minister Justin Trudeau and members of his cabinet, says Turkey's ambassador to Canada. Turkish President Recep Tayyip Erdogan and Prime Minister Ahmet Davutoglu brought up trade negotiations during a meeting with Mr. Trudeau on the margins of the G20 summit in Antalya in November, said Selçuk Ünal, Turkey's ambassador to Canada. Turkish Foreign Minister Mevlüt Çavusoglu also talked trade with Foreign Minister Stéphane Dion during a NATO summit in Brussels in December, and Turkish Economic Minister Mustafa Elitas spoke about the deal with Trade Minister Chrystia Freeland during the WTO meeting in Nairobi that same month, added Mr. Ünal. Finally, he said he has raised the matter himself with Global Affairs Canada. (…)Canada's mining companies stand to benefit from a free trade agreement, said Mr. Ünal, though he said it was too early to discuss specific areas the negotiations could cover. Several Canadian mining companies have gold and zinc mining projects in Turkey. The Mining Association of Canada and Prospectors and Developers Association of Canada support freer trade with Turkey and other emerging markets, spokespeople told *Embassy*. Pulse Canada also supports freer trade with Turkey and any other efforts to liberalize international trade, said Gord Kurbis, the organization's director of market access and trade policy. (…)Apart from tariffs, Mr. Kurbis said Canadian pulse farmers want Canada's government to work to reconcile differences in sanitary and phytosanitary rules and regulations with Turkey and other trading partners. Embassy

Family whose son has Down syndrome can appeal immigration 'inadmissibility,' Ottawa says
After a Costa Rican family went public with an allegation that their permanent residency was blocked due to their son's Down syndrome, Canadian immigration officials are urging them to not give up on their application. York University professor Felipe Montoya told CBC News his application for permanent residency was deemed "inadmissible" because his 13-year-old son Nico's Down syndrome would be too much of a burden on taxpayers. The family has until May 3 to respond to a "procedural fairness letter," which was sent by federal officials last December

that outlines the government's concerns, Citizenship and Immigration Canada spokesperson Nancy Caron said in an email statement. The family may still be able to get permanent residency if they can explain how they will cover any costs associated with Nico's Down syndrome. CBC News (2016-03-15)

CYBER SECURITY / CYBERSÉCURITÉ

*** Google aims for more encryption**
Google is disclosing how much of the traffic to its search engine and other services is being protected from hackers as part of its push to encrypt all online activity.
Encryption shields 77 per cent of the requests sent from around the world to Google's data centres, up from 52 per cent at the end of 2013, according to company statistics released Tuesday. The numbers cover all Google services except its YouTube video site, which has more than one billion users. Google plans to add YouTube to its encryption breakdown by the end of this year. Encryption is a security measure that scrambles transmitted information so it's unintelligible if it's intercepted by a third party. Google began emphasizing the need to encrypt people's online activities after confidential documents leaked in 2013 by former National Security Agency contractor Edward Snowden revealed that the U.S. government had been vacuuming up personal data transferred over the Internet. The surveillance programs exploited gaping holes in unencrypted websites. Associated Press (Chronicle-Herald, B2; London Free Press)

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Government tech support putting RCMP, public safety at risk, documents reveal**
Internal RCMP reports and emails obtained by CBC News show that Shared Services Canada's takeover of the Mounties' tech support has been a costly disaster that has jeopardized court cases and investigations while putting the safety of officers and members of the public at risk. The documents received through access to information include correspondence from RCMP Commissioner Bob Paulson in which he refused to give SSC any more control over the Mounties' information technologies. SSC is the federal department created in 2012 to take over the delivery of email, data centre and network services for 43 government agencies, including the RCMP. By all internal accounts, its work on behalf of the RCMP has been a fiasco. At a Sept. 25, 2015 meeting between Paulson and SSC president Liseanne Forand, the commissioner highlighted a number of examples where the department's mistakes and oversights have affected policing operations, including... Overall, the documents raise serious concerns about three major areas — safety and security, loss of service or information, and cost to taxpayers. A January 2014 memo to Paulson from the RCMP's civilian IT employees highlighted dozens of concerns. In December 2013, Mounties reported having to spend almost $1 million to sustain systems critical to two special units, including one that investigates online child sex assaults, because SSC "is neither willing nor able to purchase" the equipment required. "There is simply no appetite to fix any systems until they have failed. When this happens, it will be too late. RCMP will lose court cases," the group of employees told Paulson... "Shared Services has not been paying their bills. Vendors have threatened and have cut-off service to various units such as Shaw Cable, disrupting operations to the RCMP. There is risk to the front line," the employees warned Paulson. Several more egregious examples of ineptitude include how SSC couldn't get the newly opened Berens River RCMP detachment any kind of telecommunications service for two years... No one from the RCMP or Shared Services Canada responded to our requests for comment on the documents. However, in Paulson's Nov. 25, 2014 letter to Forand, the commissioner wrote that the department's proposal to manage even more of the RCMP's information technologies "pose unacceptable risks to public safety, protection of RCMP members and policing across Canada." Paulson went on to explain how he is compelled to exercise his authority to refuse the Mounties' participation in the next phase of Shared Services Canada. CBC News

Two groups duel to represent Mounties

The RCMP may be set for an old-style unionization war as a new organization has sprung up to compete to be the national bargaining unit for Canada's Mounties, the Star has learned. Calling itself the National Police Federation (NPF), the group incorporated last week in order to launch a national certification drive among some 17,000 RCMP front-line policing officers and reservists. This latest development means two organizations - the NPF and the Mounted Police Professional Association of Canada (MPPAC) - are jockeying to become the bargaining agent as a Liberal bill to allow unionization is rushed through parliamentary committee before May 15. That's the extended legislative deadline set by the Supreme Court of Canada, which ruled last year the Mounties have a right to be represented by a bargaining agent that is independent from management. The unionization drive is shaping up as a competitive race. Among the new group's leadership ranks are members of the RCMP's now defunct staff relations representative program - dismantled suddenly via a Feb. 12 internal memo from the RCMP Commissioner Bob Paulson that left Mounties in a labour relations vacuum, and warned them against speaking to media, ministers or MPs about RCMP matters without authorization. The NPF is also drawing on the ranks of its competition. It counts among its co-chairs a former member of the Mounted Police Association of Ontario's executive, Sgt. Pete Merrifield. Merrifield is also plaintiff in a high-profile harassment lawsuit against the RCMP. The MPAO was among three provincial associations to successfully challenge the RCMP's non-unionized labour relations scheme at the Supreme Court. Toronto Star, A6

RCMP clear 24 senators of wrongdoing

The RCMP have ruled out pursuing criminal investigations against 24 of 30 current and former senators whose expenses were flagged by Auditor-General Michael Ferguson after a two-year forensic audit of the Red Chamber, sources say. The Auditor-General's comprehensive audit, released last June, named nine current and former senators whose files warranted RCMP investigation and another 21 whose expenses were questionable. The Mounties decided to review the expenses of all 30 and sources said those probes are nearly complete. "The RCMP has exonerated - in writing - 24 of 30 senators and there are six files left," a source said. "They investigated thoroughly and they did not find anything to warrant any formal investigation of anyone." Another source said RCMP investigators expect that the remaining six senators will also be cleared of any wrongdoing, citing a lack of "strong evidence." Unlike the case of Conservative Senator Mike Duffy, the source said the RCMP do not have detailed diaries of these senators to help in their probe. Five of the senators still under investigation were on the list of the nine that the Auditor-General recommended to be referred to the RCMP, according to two sources. They are: Liberal Senator Colin Kenny and former senators Rose-Marie Losier-Cool (LiberalN.B.); Marie Charette-Poulin (Liberal-Ont.); Donald Oliver (Conservative-N.S.); and Gerry St. Germain (Conservative-B.C.). Conservative Senator PierreHugues Boisvenu and retired Liberal senators Rod Zimmer, Bill Rompkey and Sharon Carstairs received letters from the Mounties saying there was no evidence to mount a criminal investigation. The expenses of a sixth senator, which were questioned by the Auditor-General, are also being reviewed by the RCMP. The Globe and Mail was unable to confirm the name of that senator. Sources say the senator has not yet been interviewed by the RCMP. "Generally, the RCMP and Crown don't like to prosecute unless they have a good case," former House of Commons law clerk Rob Walsh said. "I suspect after Duffy, they don't feel they have good enough cases to warrant prosecution." Mr. Duffy was charged with 31 counts of fraud, breach of trust and bribery. Justice Charles Vaillancourt is set to deliver a ruling in the case on April 21. The RCMP would not comment on the state of its Senate investigation and when it expects to close its files. "Generally, only in the event that an investigation results in the laying of criminal charges, would the RCMP confirm its investigation, the nature of any charges laid and the identity of the individual (s) involved," RCMP Corporal Valerie Thibodeau said in a statement to The Globe and Mail. Globe and Mail, A1; * News Talk 1010

Suspect charged, held in custody

A 21-year-old Red Deer man is accused of shooting up the downtown RCMP detachment with a replica firearm and allegedly threatening to torch the building. Shots were fired from a passing vehicle at the RCMP station at 4602 51st Avenue shortly before 4 p.m. on Monday. second-storey windows at the detachment were pebbled by the rounds' impacts but did not shatter due to a protective coating. RCMP said the trouble began with a 3: 15 p.m. report that the occupants of a maroon truck were taking potshots at street signs in the Normandeau area. A second call around 3: 30 p.m. pegged the location of the truck

near the downtown detachment when the two windows were hit. When the damage was discovered, police evacuated the public from the building, and the large windows were checked to make sure they wouldn't shatter. The truck's driver was soon identified and with help from the public police tracked the vehicle to the Bower subdivision. Two men and two women were taken into custody after a "highrisk arrest" near Boyce Street and Beatty Crescent about 4 p.m. Police took all four into custody and recovered a BB pistol believed to have been used to fire the shots. Cory Daniel Picard has been charged with using an imitation firearm in the commission of an offence, possession of a weapon for a dangerous purpose, mischief damage to property over $5,000, and uttering threats. RCMP said he was alone in the back seat of the truck. The driver and two other passengers were released without charges but the investigation continues. Red Deer Advocate, A1 (Times Colonist); * Postmedia News (Edmonton Journal, A9); * Calgary Sun, A19

12 days in holding cell

After learning a 19-year-old woman spent 12 consecutive days in a barren RCMP cell under 24-hour lockdown, a territorial court judge ordered her immediately sent to the women's jail in Fort Smith. Judge Robert Gorin told court Friday the RCMP detachment isn't suitable for holding prisoners more than a couple days. "The cells at RCMP are meant to hold people overnight," said Gorin. "We have a women's facility in Fort Smith and it's not being used." Tamara Simpson pleaded guilty to trafficking after selling a gram of cocaine to members of a federal RCMP investigations unit last summer. She was taken into custody Feb. 29 and remained in RCMP cells until Friday when Judge Gorin ordered her transfer. It's up to the courts to decide where a person in custody will be remanded, said RCMP spokesperson Const. Elenore Sturko, who confirmed by e-mail the woman was held at the detachment. "Unfortunately there is no other facility which is used to house female prisoners in Yellowknife at this time," she stated. According to Crown prosecutor Brendan Green, a series of short adjournments kept Simpson behind bars at the RCMP detachment. Whereas men awaiting court appearances in Yellowknife do so at the North Slave Correctional Centre where they have access to the outdoors, television and visitors, women must either be sent to Fort Smith, or wait at the detachment. Lights are kept on 24-hours a day at RCMP cells, no visitors aside from lawyers are permitted and no phone calls aside from lawyers allowed. The concrete room has no window and no pillow. Simpson first went before a justice of the peace Tuesday, March 1, who set a bail hearing for March 3. That hearing was adjourned to the next day, then adjourned again to the following Monday, March 7. She was denied bail that day. Green couldn't say why she was denied. The Crown sought to have the sentencing hearing take place March 9 but the defence opted for Friday, March 11. Simpson remained at RCMP cells until that time. Because Judge Gorin needed more time to consider his sentence, that is now set for Friday. Yellowknifer

Elsner asks court to stop probe into alleged improper Tweets

Victoria's chief constable is trying to stop an investigation ordered by the police complaint commissioner into allegations he sent inappropriate Twitter messages to the wife of a subordinate officer. In a petition filed Tuesday in B.C. Supreme Court in Vancouver, Frank Elsner is seeking an order to stop RCMP Chief Supt. Sean Bourrie from investigating the Twitter allegations. Elsner is also trying to prevent the search of his electronic devices and telephone records. Elsner is also asking the court to order police complaint commissioner Stan Lowe to remove from his website the 12-page order outlining the allegations against him. In the petition, Elsner claims Lowe has no authority to order an external investigation into conduct that has been the subject of an internal investigation. In August, Victoria Mayor Lisa Helps and Esquimalt Mayor Barb Desjardins, co-chairwomen of the police board, received information that Elsner had exchanged Twitter messages with a Saanich police officer who was the wife of one of Elsner's officers. They brought the information to the attention of the police complaint commissioner. The matter was treated as an internal discipline matter. On Dec. 4, Helps and Desjardins told the board that Elsner had been disciplined following an internal investigation, and the board expressed confidence in the police chief. The two mayors decided not to make the matter public on the grounds that it was a confidential personnel matter. Two days later, the story was leaked to a reporter. Elsner apologized, saying he was "deeply humiliated." Times Colonist, A1

*** RCMP referrals spark racial profiling concern**

Immigration advocates raised concerns after the *Straight* presented them with statistics on police and RCMP referrals to the Canada Border Services Agency (CBSA). The numbers obtained via a CBSA

freedom-of-information request reveal stark discrepancies in how municipal police forces and RCMP detachments refer cases to the federal agency tasked with immigration enforcement. "This might reflect racism and ethnic profiling," Byron Cruz, an activist and member of Vancouver's mayor's working group on immigration, said in a telephone interview. Cruz said the issue is immigrants' health and safety. "We can see women who have suffered from domestic violence in situations where they don't call the police," he explained. The Vancouver Police Department has the highest numbers, having contacted CBSA on 144 cases in 2015 (up to December 7). That was down from 321 in 2014 and 165 in 2013. Surrey RCMP takes second place, with 114 referrals in 2015, down from 265 in 2014 and 178 in 2013. In third place is Richmond RCMP, which referred 30 cases to CBSA in 2015. Burnaby RCMP had 23 referrals, and North Vancouver RCMP had 21. Across the Lower Mainland, there were a total of 456 police and RCMP referrals to CBSA last year. Georgia Straight

*** Auto theft training for RCMP debuts in Red Deer**

About 35 Red Deer RCMP members gathered with officers from around Alberta and British Columbia for a twoday training session on investigating auto theft in Red Deer on Tuesday. Hosted by the Insurance Bureau of Canada, it's the first time Provincial Auto Theft Network (PATNET) training has been available outside the Atlantic region where it began in 2010. Red Deer RCMP Supt. Scott Tod said PATNET will give his officers a chance to network, share strategies and create a more co-ordinated approach to investigating property crime like vehicle theft which has increased significantly over the last three or four years in the city. Red Deer Advocate, A2

*** Nouveau parcours pour le Défilé de la Saint-Patrick**

Pour sa septième édition, le désormais traditionnel Défilé de la Saint-Patrick de Québec, qui se tiendra samedi après-midi, empruntera un nouveau parcours. Avec comme point de départ le coin Fraser et De Salaberry, le millier de participants attendus déambulera dans l'avenue Cartier, la Grande Allée, la rue Saint-Louis et la rue du Fort, pour terminer son itinéraire sur la rue Saint-Jean. «Ce nouveau trajet [qui évite de traverser Honoré-Mercier] permettra de limiter les arrêts pendant le défilé», a expliqué, mardi après-midi, en conférence de presse, le président de l'événement, Stephen Burke. M. Burke n'était pas peu fier d'annoncer le retour des groupes de cornemuses et percussions de la police de New York et de Chicago. En l'absence de leurs collègues de Boston, retenus à leur propre défilé dimanche, les organisateurs accueilleront les musiciens du Toronto Fire Services Pipes and Drums. La foule verra également défiler des formations musicales de Québec et Montréal, des troupes de danse celtique, des amuseurs publics, des lévriers irlandais, sans oublier deux chevaux du Carrousel équestre de la GRC. Le Soleil, 22

*** Plans for P.E.I.'s first medical marijuana dispensary to open in Summerside**

Craig Gaudet of Summerside, P.E.I., hopes to open the Island's first medical marijuana dispensary this April. Gaudet says he already supplies medical marijuana to people who have approval in P.E.I., but wants to make it easier for others to get medical marijuana at one central location. He told CBC he's already picked out a location - on Water Street in Summerside. He's hoping to open in April. "I really want to help more people. Our patients are having to travel from end to end on the Island just to be able to get their treatments and get their medications. We can't even buy medications here on the Island, we have to send away and get it through the mail," he said. A former reservist, Gaudet says he uses medical marijuana himself to manage pain from an injury he sustained in the 1980s, when his legs were crushed by an army vehicle. Gaudet plans to carry 186 products, and said he will do more than just dispense. "We spend time with our patients, making sure of their medications, making sure their doses, finding out about their licensing, what they are recommended to take per day, how they're taking it per day and helping people find and obtain a license is a lot of what we do," he said. Health Canada says the dispensaries that have been cropping up across Canada for the past 20 years are illegal. CBC News

*** LED light thiefs nabbed**

Northeast District RCMP have arrested three men in connection with an investigation into the thefts of LED light bars on the Acadian Peninsula. On March 11, police arrested a 23-year-old man from Hacheyville and seized a light from his vehicle. Also on March 11, as part of the investigation, RCMP executed a search warrant at a home in Six Roads where a 32-year-old man was arrested at his residence. A total of six light bars were seized. Both men were released from custody and are scheduled

to appear in court at a later date. Since the middle of February, the RCMP on the Acadian Peninsula have been investigating the thefts of LED light bars from all-terrain vehicles and boats. The thefts took place in the Le Goulet, Sainte-Rose and Tracadie areas. On March 14, RCMP arrested 23-year-old Louis-Philippe Bulger-Landry of Haut-Sheila in connection with the investigation. He appeared in Caraquet provincial court on March 15 and was charged with operating a motor vehicle while pursued by police and dangerous driving in relation to his arrest. Times & Transcript, A10

***Second person charged for P.A. man's homicide**

A second person has been charged with murder in connection with the death of a Prince Albert man who was missing for nine months. RCMP announced Tuesday that Skylar Patrick Bird, 29, is charged with first-degree murder in the death of Troy Cecil Napope, who went missing last May. Napope's sister, Christie, said news of the arrests has conjured up mixed feelings. "I was really relieved and really sad at the same time ... it was heartbreaking for us," Christie Napope said in an interview Tuesday after seeing Bird appear in court in Prince Albert. Bird is one of two people charged in the case. On Monday, 27-year-old Braidy Chase Vermette appeared in Prince Albert provincial court, charged with first-degree murder in Napope's death. RCMP said Tuesday that Napope, Vermette and Bird were all known to each other. According to an RCMP news release, Bird was charged on Feb. 25 with one count of forcible confinement and one count of arson in connection with Napope's death. He made his court appearance on those charges on Feb. 26. "Further investigation resulted in the charge of first-degree murder, which will replace the two charges laid on Feb. 25," the release stated. StarPhoenix, A3

*** Solving a homicide**

An editorial states ''The RCMP says that redeploying Mounties to tackle terrorism has strained its resources. The Toronto Police Service says it's so stretched it needs photo radar to free up uniformed officers. Across Canada, officers are feeling the heat as they struggle to meet public expectations for cracking down on crime. It's no surprise, then, that the Ottawa police are under intense scrutiny after the fifth homicide of 2016 - the third in less than a year in the same part of the city. The death of Nooredin Hassan has been quickly politicized: Area Coun. Tim Tierney demanded a meeting with police Chief Charles Bordeleau, then presented a "sevenpoint plan" for the Jasmine Crescent area where the homicide occurred. Bordeleau responded with an article in the Citizen, doling out statistics about arrests, weapons seized and the redeployment of staffto the guns and gangs unit. This political jockeying hasn't been entirely useless: The councillor has made some useful suggestions, and the chief has reached out to specific organizations that can help. All sides have urged community members to come forward with information, even if anonymously. Ottawa has cleaned up violence-ridden neighbourhoods before and can do so again. But the blame for such crimes should be placed squarely where it belongs: not on police, not even on politicians, but on the perpetrators themselves. (Indeed, Canadian cities, including Ottawa, have a pretty strong record tackling violence. The most recent crime-rate statistics, for 2014, show the police-reported crime rate at its lowest since 1969. Ottawa's own numbers, measured against a variety of national markers, are pretty healthy.)'' Ottawa Citizen, A8

Health firings the story that won't end

An opinion piece states **''**While ombudsperson Jay Chalke conducts the latest investigation into the botched firings of a group of drug researchers, the leaked findings of an earlier investigation raise disturbing questions about the B.C. Liberals' handling of the affair. Why did the Liberals order the internal investigation into allegations of wrongdoing by the researchers when they had already, in effect, pronounced the accused guilty by firing them? Why did the Liberals allow the investigation to proceed, even as they were admitting the wrongheadedness of the firings via out-of-court settlements, reinstatements and apologies? ... The health firings followed in September 2012 along with the government announcement that it was calling in the RCMP and the comptroller general. Then came suits for wrongful dismissal, the suicide of one of the fired researchers and, starting in 2014, a series of out-ofcourt settlements, reinstatements and apologies. Still, the office of the comptroller general continued to investigate amid mounting questions about why it was taking so long and whether there was much point in light of the public backdown on the firings. Finally, in the spring of last year, the investigation was completed, two and a half years after the firings and a year after the first of the reinstatements. The findings were passed along to the RCMP, which had closed their barely active file on the investigation for

lack of evidence in 2014 and only reopened it on learning (as a result of a different leak to The Sun) of an ongoing investigation by the comptroller." Vancouver Sun, A10

*** Non-lethal weapon**

An opinion piece by Daniel Bear, professor of criminal justice at Humber College's School of Social and Community Services, states "No person viewing video of the shooting death of Sammy Yatim on a streetcar would hesitate if given the opportunity to magically replace Constable James Forcillo's handgun with one of the Toronto Police Service's newly acquired beanbagshooting shotguns. Such a switch might have saved Mr. Yatim's life, Constable Forcillo's career and whatever amount of the community's trust and confidence in police that was lost that night in 2013. But in even acknowledging that less-lethal weapons may be preferable in specific situations, we must ask ourselves if the continued expansion of those options supports our larger goals for what policing should be in the modern Canadian context. Over the past few years, police forces in several cities, the RCMP and Corrections Canada have adopted new less-lethal weapons that fire projectiles meant to disable rather than kill. They are intended for two primary situations: non-compliant individuals and crowd control. Recently, Toronto Police added blaze-orange shotguns designed to shoot a "super sock round." Like the tasers already used by the force, the sock guns are deemed less lethal, but both beanbags and tasers have killed and maimed before. The primary argument for adding the shotguns is that they provide officers a longer-range option when faced with situations that are dangerous but do not involve an imminent threat to life or grievous bodily harm." Globe and Mail, A10

*** Keeping politicians honest**

An opinion piece by Lauren Heuser, lawyer and journalism fellow at the Munk School of Global Affairs, states " "In politics, questions of ethics cannot be left to the judgment of individual politicians. Clear rules are essential for establishing the standards public officials must meet and the consequences for failing to do so. This point has recently come to the fore with Canada's new justice minister. In the past few weeks, Jody Wilson-Raybould has faced two conflict of interest allegations: the first over revelations that her husband, Tim Raybould, belatedly registered to lobby the justice department on behalf of his First Nations clients; and the second over news that she will be making policy on B.C.'s controversial Site C dam, a project that she protested against before becoming a member of Parliament. Fortunately, the Conflict of Interest Act, Canada's key ethics legislation for federal office holders, includes rules that govern conflicts of interest and does not leave it to impugned individuals to judge whether their conduct is permissible or not. The conflict of interest and ethics commissioner provides expert advice on precisely such matters. Unfortunately, the standard for what constitutes a conflict of interest under the act is far too lax and the penalties that can be imposed for violating its rules are far too inconsequential and uncertain… For example, Ethics Commissioner Mary Dawson's investigation into former chief of staff Nigel Wright's $90,000 payment to Sen. Mike Duffy may well have led to findings that Wright violated the act (the investigation was suspended when a RCMP criminal investigation began). But one can question whether then-prime minister Stephen Harper would have done anything about it, not least because his complicity in the wrongdoing was a live question." National Post, A8

*** Proposed gun registry law draws praise from many sides**

A coalition of police, public health and victims' rights organizations held a news conference Tuesday to express their support for Bill 64, a proposed gun registration law. The Quebec Association of Provincial Police and the Association pour la santé publique du Québec said the long-gun registry was abolished by the federal government, which means they can now be "purchased and transferred without leaving a paper trail." Bill 64, which goes before a parliamentary committee next week, calls for non-restricted firearms to come with a registration number and for business owners to keep a chart tracking the sale of weapons. The organization said Tuesday that 94 per cent of guns in circulation in Quebec are non-restricted - a category that includes hunting rifles but also assault weapons. Pierre Veilleux, president of Quebec's provincial police union, said these tracking measures are crucial to ensure that guns "don't fall into the wrong hands." Bill 64 would be a useful tool for police, he said, because they can better manage interventions knowing if a person owns weapons or not. Yves Francoeur, the president of Montreal's police brotherhood, said gun legislation is an "essential component" that would help police who cannot otherwise rely on a federal gun registry. La Presse Canadienne (Gazette, A2); Le Quotidien, 15

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Lockdown lifted
The lockdown put in place last Thursday at the medium-security unit at Collins Bay Institution has been lifted. The lockdown was ordered so staff could conduct an exceptional search of the institution. Normal operations and visits have resumed, said a news release from Correctional Service Canada. CSC did not say if anything significant was found in their search. Kingston Whig-Standard, A3

Shepard due for release Friday
An elderly woman known as the Internet Black Widow has agreed she won't be romancing any men once she's out of prison unless police are first informed, but it's possible she'll fight this and other conditions of her release at a future court date. Melissa Ann Shepard, now in her early 80s, is set for release from a federal women's jail in Truro on Friday, after being denied parole and serving her full sentence. In her latest conviction in June 2013, she was sentenced to two years, nine months and 10 days in jail for spiking her newlywed husband's coffee with tranquilizers. (…) In 2005, Shepard was also sentenced to five years in prison on seven counts of theft from a man in Florida she had met online. A recent parole board report that said Shepard has a tendency to fabricate and deny events to correctional staff, and is unable to link consequences to actions. Canadian Press (Chronicle-Herald, A1, Kingston Whig-Standard, Whitehorse Daily Star, Cape Breton Post, Times & Transcript, The Guardian, Windsor Star, Leader-Post, Ottawa Sun, London Free Press, Toronto Star, Montreal Gazette, National Post, Edmonton Journal, Ottawa Citizen, Calgary Herald, StarPhoenix); Presse canadienne (Le Droit, L'Actualité)

La mère de la victime pleure encore la perte de son fils
Si l'avocate qui représente les intérêts du meurtrier André Roy a fait entendre plusieurs témoins et experts pour que son client puisse bénéficier d'une libération anticipée, la couronne, elle, n'a déposé en preuve qu'une simple lettre, écrite par la mère de la victime, Victor Lemay. «Je me demande souvent si Victor aurait continué à étudier pour créer des jeux vidéo. Il était très bon en dessin et il avait beaucoup d'imagination», enchaîne- t-elle. «La prison à vie pour moi, ce n'est pas que vingt-cinq années. Pour moi, en tant que mère de Victor, ce sera le restant de mes jours», a écrit Madeleine Lauzé dans une brève missive qui a été transmise aux membres du jury. (…) Comme la preuve est maintenant fermée des deux côtés, le juge devrait donner ses directives, aujourd'hui, aux membres du jury qui, par la suite, seront séquestrés. Si jamais ils acceptent la requête présentée par Roy, ce dernier pourra alors déposer une demande devant la Commission des libérations conditionnelles du Canada pour être entendu, dans l'espoir de bénéficier d'un retour progressif dans la société. Journal de Québec, 13

*** Bad grandpa**
Manitoba's highest court has ordered that a man convicted of sexually abusing four young girls - three of them his grandchildren - serve an additional 2 1/2 years in prison. The 70-year-old accused pleaded guilty to four counts of sexual interference and was sentenced last year to 5 1/2 years in prison. In a written decision released Tuesday, the Manitoba Court of Appeal ruled the sentence unfit and replaced it with a sentence of eight years. The high court ruled provincial court Judge Tim Killeen erred when he calculated what he considered to be an appropriate total sentence, and then apportioned individual sentences for each offence, rather than decide the individual sentences first. Winnipeg Sun, A6

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** La criminalité baisse encore**
Malgré une hausse des crimes contre la personne et des arrestations pour conduite avec les capacités affaiblies, la criminalité continue globalement à diminuer à Bromont. « En deux ans, la criminalité a diminué de 20 %, ce qui est important. Oui, il y a certains écarts, mais rien de dramatique. Le résultat global, en fonction de la population qui croît, est satisfaisant », a indiqué le directeur du service de police de Bromont, Jean Bourgeois, lors de la présentation du rapport annuel de l'organisation, mardi. Une diminution de 17 % de la criminalité avait été enregistrée en 2014. En 2015, la baisse a atteint 3,5 %. Les

crimes contre la personne ont grimpé de 21,7 %, passant de 46 à 56. Une statistique à nuancer, par contre, car les policiers ont reçu plusieurs plaintes croisées (les deux personnes impliquées dans une altercation portant plainte), ce qui fait augmenter les chiffres relatifs à ce type de crime. Les vols de moins de 5000 $ ont connu une importante diminution de 35,7 %, passant de 56 en 2014 à 36 en 2015. Les autres infractions au Code criminel - tel que les bris de condition, la possession de stupéfiants, les délits reliés à la conduite automobile - sont en baisse. On en a dénombré 125 en 2014, contre 105 en 2015. Voix de l'Est, 4 (La Presse)

* **Saskatoon group continues call to end police carding, questions police budget**
A rally in Saskatoon called for the city's police service to end carding and scale back government funding for law enforcement. Tuesday marked the International Day Against Police Brutality, and a group of about 40 gathered at Pleasant Hill Park in Saskatoon to share stories of how they've been mistreated by police through carding; an investigative tactic that allows police officers to randomly stop, question, and document individuals when no criminal offense has been committed. (...) Rally organizer Kota Kimura said carding remains a big issue in Saskatoon, but he's also hoping to win the ear of politicians to change the way law enforcement agencies are funded. "We have four demands in light of International Day Against Police Brutality. First one is to end carding the second is to smash police racism," Kimura said. "More importantly there are some structural issues we want to address. We believe police are getting a disproportionate amount of money, they're getting millions of dollars from the City of Saskatoon when many community organizations and social programs are getting their funding cut and some services are facing closures." CBC News

* **Police budget in red**
The Thunder Bay Police Service is $325,000 in the red for 2015. Police Chief J.P. Levesque reported to the Thunder Bay Police Services Board Tuesday morning that their approved operational budget for last year came in with a 0.087 per cent deficit. That number is considerably lowering than the negative variance of 1.73 per cent or $639,000 projected in October after the third quarter. "We'd be happy if it wasn't a negative variance but it's better than what we had projected, so we're pleased with that," said Levesque. The improvement in the variance came after some unexpected funding for the police service's cyber crime unit from the province. The remaining deficit comes from items that are usually underfunded like overtime and legal fees, said the police chief, adding that 91 per cent of the budget goes towards wages and benefits. Chronicle Journal

* **Services policiers en milieu autochtone : des communautés de la région demandent un meilleur financement**
Le budget du service de police de Lac-Simon est de 1,3 million de dollars pour 5 ans. La communauté connait actuellement un manque à gagner de 300 000 $. « On manque d'argent actuellement pour servir notre corps de police. Juste un exemple, on manque d'autos-patrouilles. Nos autos-patrouilles sont au bout du rouleau », illustre Jean-Marie Papatie, conseiller à Lac-Simon. La communauté de Pikogan, près d'Amos, vit aussi une problématique de sous-financement de son corps policier. Le chef, Bruno Kistabish, explique qu'« il manque deux personnes à temps plein et deux personnes à temps partiel pour combler les horaires, pour avoir toujours deux policiers dans le véhicule. De prime abord, je dirais qu'il en va de la sécurité de nos employés qui sont les policiers, mais il en va aussi de la sécurité de nos membres qui habitent sur la communauté. » Cette problématique se vit dans plusieurs communautés, selon le député d'Abitibi-Baie-James-Nunavik-Eeyou. Romeo Saganash. Il affirme qu'Ottawa doit réformer le programme pour mieux répondre aux besoins des communautés. Radio-Canada

* **Mayor Brian Bowman grills Winnipeg police over planned layoffs, budget shortfall**
A special meeting of the city's executive policy committee got heated in Winnipeg on Tuesday. The committee is mulling over details of the Winnipeg Police Service's $2.45-million budget shortfall. The preliminary 2016 police service budget includes plans to lay off 40 of 68 cadets, cancel the 2016 recruitment class and lay off 20 of 37 members enrolled in the class, the police board revealed at its meeting Friday. Mayor Brian Bowman and the executive policy committee grilled the police board on Tuesday morning over its proposed layoffs. The city has already offered to boost funding to the police service by 6.3 per cent this year, but it's not enough, according to outgoing police Chief Devon Clunis.

The police board is asking the city to shell out more money to help cover the shortfall. CBC News (2016-03-15)

*** Wanted : Political champion to take on gangs in North Central**
A large fence around a home on the 1300 block of Cameron Street has a beautiful mural on it. The homeowner had a community group paint it as part of a neighbourhood improvement initiative. Then a well-known local gang tagged it. This is North Central. Home of the most crime in the city. Ground zero for gangs and the young people being recruited into them. Warren McCall, the NDP candidate running to represent the people of the neighbourhood for another term, grew up here. He still lives in the area - within a block of the tagged mural. "There was a time when I think we had a better handle on even the little things like that, in terms of being vigilant about not giving ground to the gangs in things like tagging and marking out turf, but that has slid over the years," he says. In an effort to stop that slide, community members organized a brainstorming session this week to talk about ways to make the neighbourhood safer - to alleviate the inevitable tragedy gangs bring to any neighbourhood. (…) McCall said long-term funding for specific programs targeting gang exits are "missing in the battle right now" and a properly resourced program is needed. Competing for the same seat this election is Bill Stevenson, who has his own experiences with gangs. "Gang violence has touched my life in many ways. It's touched my family," he said, adding he thinks investments in education and housing will go a long ways to improve conditions within North Central. Leader-Post, A3

*** Children must be armed with the right tools to battle abuse, conference hears**
Children must be empowered through proper sex education in order to keep them safe, a group of community members heard on Tuesday at a child safety conference. The more than 100 people at the conference, hosted by Big Brothers and Sisters at the Delta Hotel, were in awe as panelist Jessica Lanigan shared her story of sexual abuse and the need for blunt education. (…) In 2008, Saint John had the notorious distinction of having the highest rate of violence against children and youth in the country, according to a Statistics Canada Incident-based Uniform Crime Reporting survey. (…) Lanigan said such education needs to be part of daily conversations because about 30 per cent of girls and 20 per cent of boys will encounter unwanted sexual experiences before the age of 18. Panelist Bill Reid, the former Saint John police chief, said in his remarks that in 2015 alone, the force's family protection unit handled 80 reports of sex offences where the victim was under the age of 17. In 36 of those cases, the victim was under the age of 12, he added. "Additionally, there were 169 reports of family violence," he said. "This is precisely why education is so critical to prevention and awareness." Telegraph-Journal, B1

*** Deadly illegal drug**
Local police are warning Ontarian's about a new illegal drug that is deadly. While W-18 hasn't been found on the streets here it has been reported in Calgary and police say it's only a matter of time before it arrives in our neck of the woods. You won't find the drug in any pharmacies. It is an illegal drug that is being sold on the streets as fentanyl or oxycodone pills. It's 100 times stronger than fentanyl patches prescribed by doctors to manage pain and can be addictive. One tablet could be ten times more potent than another tablet which can cause a lot of risk as well for overdose. The man made synthetic opioid is also 1000 times stronger than morphine. These pills come as long acting medications, so they are released over a long period of time. If you crush these pills you end up releasing all of the medication at once. That's where the risk of potency comes and risk of over dose. Both Hamilton and Niagara police have seen an increase in pharmacy robberies specifically targeting fentanyl. Halton police say there has been a consistent number of pharmacy robberies in that region. CHCH News (2016-03-15)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

*** Chief loses credibility**
An editorial states, "Canada used to have three levels of government: municipal, provincial and federal. Now, we've apparently got another layer of bureaucracy, at least when it comes to pipeline applications: aboriginal. "TransCanada will be forced to abide by Mohawk law, including the prohibition to pass the

pipeline through Mohawk lands and waters," says Mohawk Kanesatake Grand Chief Serge Simon regarding the Calgary company's Energy East application. (...) Further, where does Simon think the money is coming from to combat social problems that afflict aboriginals? The federal Liberal government has already committed to spending about $40 million over the next two years on an inquiry into missing and murdered aboriginal women. Now, the national chief of the Assembly of First Nations is calling for a strategy to combat suicides among indigenous communities. "Our young people need hope and inspiration," Chief Perry Bellegarde said. "They don't see that right now. We've got to make those key strategic interventions now. It's a life-and-death situation.'" Calgary Herald, A9

PUBLIC SERVICE / FONCTION PUBLIQUE

Brison to 'work closely' with commissioner on Access to Information Act review
Canada's government will "work closely" with Information Commissioner Suzanne Legault on an upcoming review of the Access to Information Act, the office of Treasury Board President Scott Brison has confirmed. Mr. Brison and Justice Minister Jody Wilson-Raybould will also work with Parliamentarians and "other interested stakeholders" to "make sure we get it right," press secretary Jean-Luc Ferland wrote to Embassy in an email. "Our goal is to have a culture of government open by default," he said. "This change is long overdue, but it's also quite complex." The office couldn't offer a timeline for when the review would be completed and publicly released. (...) Alternative to being found well-founded or not, some complaints are settled, meaning that the institution and complainant agree on a solution to close the file before the end of a full investigation. Some others are discontinued or dropped by the complainant if, for example, they obtain the desired records before an investigation is finished. Other trends emerge too: that in 2015, Global Affairs Canada and the Department of National Defence appear to be of elevated interest for members of the media, but that lawyers are particularly interested in Immigration, Refugees and Citizenship and the Canada Border Services Agency. And that members of the public form, by far, the largest group complaining about the Royal Canadian Mounted Police-to which the most complaints in total were directed. Embassy

Liberals' offer on sick leave dismays union
The Liberal government's decision to propose the same controversial sick leave plan as the previous government is a "missed opportunity" that could lead to labour unrest, warns the president of the largest federal union. Robyn Benson, president of the Public Service Alliance of Canada, said she is surprised a government elected on promises to restore respect for the public service and fair bargaining is pushing the "same old" Tory proposal for a short-term disability plan that the unions solidly ejected for more than a year. "We thought bargaining would be a priority when they got elected and we thought we would get a Liberal mandate," Benson said. "They seem to be recycling the same old positions of the Conservative government. That is a problem." She said treating public servants with respect is also about improving public services after the "slash, cut and burn" of the Conservatives. "I don't think they want labour unrest during the first year in power. If we don't get a tentative agreement, we will follow the process and go into conciliation. "It would be a missed opportunity for this government not to settle with us." PSAC met with Treasury Board negotiators last week, the second major bargaining session since the Liberals came to power. Ottawa Citizen, A4

OTHER / AUTRE

*** Trudeau should push for UN reform**
When Canada lost its bid for a United Nations Security Council seat to Portugal in 2010 it was widely seen as a humiliation, an embarrassment, the dagger through the heart of Stephen Harper's foreign policy. It was the diplomatic equivalent of a loss to Kazakhstan on the ice. At least, that was the view of the chattering class. One could argue that it didn't really bother Canadians, who turned around and awarded a majority government to Harper months later, despite the best efforts of opposition parties to keep the issue on the electoral radar. Wednesday in New York, Justin Trudeau will officially announce the country's bid for a Security Council seat, but one must ask if this is more a matter of returning national prestige - "Canada is Back (again)" - than a sign of the actual value of the seat at the UN inner circle. It is one of the legacies of the Harper era that our historic engagement with the UN was severed. He did

address the General Assembly three times, but there was the 2009 visit to Tim Horton's instead of a speech to the General Assembly, and the 2012 speaking engagement blocks from the UN without dropping in. UN envoys who travelled to Canada to study our treatment of indigenous peoples were aggressively given the bum's rush. Harper famously vowed Canadian foreign policy would not include courting "every dictator with a vote at the United Nations." He said that 1.5 km from the UN headquarters. Toronto Star, A8

* **Sunnier times for Canada's disarmament diplomacy**
Foreign Minister Stephane Dion's March 2 address to the Conference on Disarmament in Geneva represents both a welcome re-engagement at a key if moribund multilateral forum, as well as an indicator that Canada is prepared once again to assume a leadership role in the demanding field of multilateral disarmament activity. Dion's rebuke of the CD was amply deserved. After a 20-year failure to agree on any program of work (let alone undertake any official action pursuant to one) the 65-member state consensus-based forum has egregiously failed its core raison d'être-to serve as the UN's forum for negotiating multilateral arms control and disarmament agreements. The only thing more shocking than the CD's dysfunctionality has been the willingness of leading states to tolerate it as long as they have. Mr. Dion rightly recalls that the major multilateral arms control and disarmament agreements have all been negotiated outside the CD. The 1997 Ottawa Convention banning anti-personnel landmines and the 2008 Convention prohibiting cluster munitions were accomplished through ad hoc diplomatic conferences and the more recent Arms Trade Treaty through a negotiation authorized by the UN General Assembly. If the CD does not find a way to liberate itself from the straitjacket of conflicting national vetoes, it will become irrelevant to the international security community. There is no magic formula for overcoming the CD's impasse and Mr. Dion can only call on the states "to redouble our efforts to find innovative ways of moving forward" and "to set realistic objectives." Embassy

* **How the parties collect your personal info - and why Trudeau doesn't seem to mind**
Numbers are definitely in fashion in the new Liberal government at the moment - and not just because the budget is landing next week. A first-ever session on "behavioural economics" for public servants was filled to capacity last week, according to a *Hill Times* report. "Combining economics with behavioural psychology," said PCO spokesperson Raymond Rivet, "this new tool can help governments make services more client-focused, increase uptake of programs, and improve regulatory compliance. Better government through behavioural economics - the idea was popularized by the 2009 book *Nudge* and almost immediately adopted through the establishment of a "nudge unit" by the British government in 2010. Justin Trudeau's government is already borrowing the concept of "deliverology" from the Brits, so the 'nudge' was never going to be far behind. President Barack Obama, Trudeau's new best friend, also has taken steps to introduce nudge theory to the U.S. government in recent years. But the real motivation for data-based governance in the Trudeau government may have come from a source much closer to home - the recent election, specifically the Liberals' extensive use of big data to win 184 seats last fall. Make no mistake: Trudeau's Liberals may have won the election by promising intangibles like 'hope' and 'change', but they sealed the deal with a sophisticated data campaign and ground war. So now that the Liberals have seen how mastery of the numbers can help win elections, we probably shouldn't be too surprised that they see those same skills as useful for governing as well. Big-data politics is here to stay. (…)It seems odd to me that citizens can get (often appropriately) worked up about "intrusive" government measures, whether it's the census or the C-51 anti-terrorism law, and yet be mostly indifferent to what the chief electoral officer has called the "Wild West" of political data collection. Even Conservatives who resented the gun registry didn't seem to mind that their own party was keeping track of gun owners in its database, so that it could send them specially targeted fundraising messages from time to time. That's just behavioural economics, applied to the political arena. iPolitics

INTERNATIONAL

* **Islamic State flag found after Belgium shooting**
Belgian prosecutors said a flag of the so-called Islamic State group and a jihadist manual were found by the body of an armed suspect who was shot dead during an anti-terrorist operation in Brussels yesterday. The dead man has been named as 35-year-old Mohamed Belkaid, an Algerian living illegally in Belgium.

Belgian federal prosecutors say two people have been detained but it is not clear if they are connected to the shooting. One of those detained was taken to hospital with a broken leg. Brussels police killed Belkaid, who was armed with an assault rifle, after four officers were wounded yesterday during what investigators had expected to be a routine search on an apartment in the south of the Belgian capital. Two other people escaped. Reuters (RTE); Sky News; Independent UK; Mirror UK

*** Gunman Fires On Police During Terror Raid**

Belgian police launched a manhunt in a Brussels neighbourhood on Tuesday after at least one gunman opened fire on officers during an antiterror raid linked to last year's Paris attacks, officials said. Three police officers were slightly injured during the operation. French Interior Minister Bernard Cazeneuve said that "a team composed of Belgian and French police came under fire, apparently from assault weapons, during a raid." Two hours after the first shots were fired, a big swath of the Forest neighbourhood was in lockdown as special police units in body armour and balaclava hoods moved in, several with their guns drawn. A helicopter was hovering overhead to patrol the area as police were still hunting for at least one suspect. "Two individuals, apparently barricaded themselves inside a home," Forest Mayor Marc-Jean Ghyssels told local media. Officials later said a man had been found dead in a Brussels apartment following the anti-terror raid. Police found the body after they stormed the apartment. Four months on, Belgian police and magistrates are still piecing together the role Belgian nationals played in aiding the Paris attackers, as well as trying to track down missing suspects, including international fugitive Salah Abdeslam. Associated Press (Windsor Star, N4, Leader-Post, Ottawa Citizen, London Free Press, Edmonton Journal, Calgary Herald, Montreal Gazette, StarPhoenix); Associated Press (National Post, A10, Toronto Sun, Calgary Sun, Winnipeg Sun, Kingston Whig-Standard, Edmonton Sun, Ottawa Sun, London Free Press)

*** Police Suspect Bomb Caused Fatal Car Explosion In Berlin**

An explosion that destroyed a car and killed the driver in downtown Berlin during rush-hour traffic Tuesday was likely caused by a bomb, police said, but investigators are working on the assumption that it was not a terrorrelated attack. The explosion occurred at about 8 a.m. in the western district of Charlottenburg on a busy street leading into the heart of the German capital. Photos from the scene showed the wreckage of a Berlin-registered silver VW Passat station wagon, its windows blown out and its front end smashed in, about a kilometre from the capital's landmark Victory Column. "(The) explosion occurred inside or on the vehicle," said Carsten Mueller, deputy chief spokesman for Berlin police. "Our investigators are working on the assumption that it was an explosive device that caused this," Mueller said. Nobody else was injured in the blast despite heavy traffic, he said. Hours after the blast police were concentrating on the possibility that the explosion might be linked to organized crime, said Kerstin Ziesmer, a police spokeswoman. The Associated Press (Windsor Star, N4, Leader-Post, Ottawa Citizen, Gazette, Calgary Herald, Edmonton Journal, London Free Press, StarPhoenix)

*** U.S. airstrike kills senior Daesh commander**

Omar al-Shishani, a top Daesh (otherwise known as ISIS or ISIL) commander who was a magnet for fighters from the former Soviet Union, has died of injuries suffered in a March 4 U.S. airstrike in Syria, a senior Iraqi intelligence official and the head of a Syrian activist group said Tuesday. Al-Shishani, who was injured in a U.S. airstrike earlier this month, died on Monday evening outside Daesh's main stronghold of Raqqa in Syria, the two told The Associated Press. A U.S. military spokesman confirmed the reports. The Daesh-affiliated Aamaq news agency cited an unnamed source as denying that al-Shishani was injured or killed, without providing any evidence that he was still alive. The red-bearded ethnic Chechen, who was in his 30s, was one of the most prominent Daesh commanders, appearing in several online videos leading fighters into battle. He served as the top commander in Syria before being appointed to lead three elite units that carried out special missions in Syria and Iraq, according to Hisham al-Hashimi, an Iraqi scholar who follows the group. Al-Shishani, whose real name was Tarkhan Batirashvili, was an ethnic Chechen from Georgia, a former Soviet nation in the Caucasus. He hailed from the Pankisi Valley, a centre of the Chechen community and a former militant stronghold. Associated Press (Toronto Star, A12)

*** Al Qaeda's new reality in Africa**

When an Al Qaeda affiliate makes things go boom, stoking global fear isn't always the main goal, however much the horrible headlines suggest otherwise. Nor is simple competition - Al Qaeda's obsession with winning back jihadist supremacy from the 2.0 upstarts of Daesh, also referred to as ISIS and ISIL - always driving the attacks. Too bad, right? Can't we just think of Al Qaeda versus Daesh as we do the Leafs versus the Habs? Simple one-upmanship, and nothing more? Sorry, no. Not if we really want to understand and counter the loose and often very regional affiliations and intrigue behind the headlines. This is especially true in sub-Saharan Africa, where "specific local and regional dynamics" are "crucial" to understanding the crisis, as the International Crisis Group noted Monday in a nuanced special report on the evolving jihadist landscape. None of this in any way blunts the unprecedented shock that visited the Ivory Coast on Sunday, when gunmen acting in the name of Al Qaeda's North African branch quaffed beer at a beachside bar before unleashing a fusillade of bullets throughout the resort town of Grand Bassam. Toronto Star, A12

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
October 23, 2015 / le 23 octobre 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

WAR MEMORIAL SHOOTING ANNIVERSARY

Gov. Gen. David Johnston rejects the notion that the country was fundamentally changed by the attacks that killed two Canadian military members a year ago. While that may be true, there was certainly evidence of changes, some small, others gapingly vast, as Canadians gathered Thursday to mark the first anniversary of the deadly Parliament Hill attack that killed Cpl. Nathan Cirillo. "Today, I cannot help but think of his boy," said Marcela Coquet, from behind the counter of her downtown Ottawa souvenir store, a block from the National War Memorial... Public Safety **Minister Steven Blaney noted the symbolism of the moment, saying "*our nation is coming together*."** Re-elected Monday and headed for the opposition benches**, Blaney said he has a "*profound sense of mission accomplished*"** after a year of leading the Conservative government's response to the attacks, including a controversial anti-terror law that faces Liberal amendments. Canadian Press (Cape Breton Post, A10/FRONT, Chronicle-Herald, A1/FRONT, London Free Press, Winnipeg Sun, Ottawa Sun, Kingston Whig-Standard, Record, Daily Gleaner, Hamilton Spectator, Times & Transcript, Telegraph Journal)

Here we stand, here we stay

The police officers, first responders and citizens who responded with such bravery and compassion **to the killings of two Canadian military members a year ago exemplified what Canada is, Gov**. Gen. David Johnston said today. Johnston joined soldiers, veterans, dignitaries and hundreds of ordinary citizens at the National War Memorial to mark the first anniversary of the deadly Parliament Hill attack that killed Cpl. Nathan Cirillo. Some suggested a year ago that the country would be dramatically changed by the incident, Johnston said, but he disagreed... **Public Safety Minister Steven Blaney**, who was one of

the Conservatives re-elected in Monday's vote, was among those who strode down Sparks Street towards the commemoration. He says he went for a morning jog to the memorial at 7 a.m. to pay tribute to both fallen soldiers. **Blaney** met Vincent's family earlier. "***Today our nation is coming together,"*** **Blaney** told The Canadian Press. "***We are stronger than we were.... The elected prime minister will be there with our right honourable Mr. Harper***." ... **Blaney** said he has a "***profound sense of mission accomplished***" after a year of leading the Conservative government's controversial response to the attacks. Canadian Press (Whitehorse Star, 8)

*** Preview of Liberal rewrite of security bill**

The incoming Liberal government says it will repeal "problematic elements" of Stephen Harper's anti-terrorism law, known as C-51. Here's a look at 10 things the Liberals are expected to do in the revamped legislation, based on party platform promises and amendments proposed during parliamentary hearings: Guarantee that all Canadian Security Intelligence Service warrants respect the Charter of Rights and Freedoms. This would roll back provisions allowing CSIS to disrupt terror plots through tactics that contravene the charter as long as a judge approves. Critics have called the provisions an extraordinary inversion of the judicial role to uphold - not sanction violations of - the charter. Require the Security Intelligence Review Committee, the watchdog over CSIS known as SIRC, to examine all activities the spy agency carries out under its new threat reduction mandate and have the committee provide an annual report to the **public safety minister** and Parliament on its findings. Canadian Press (Times Colonist, A10, Calgary Sun, Times & Transcript)

*** Hill shooting has lasting impact for MPs, staffers**

The effects of a gunman's assault on Parliament Hill still reverberate for New Democrat MP Nathan Cullen, who can't forget the scene inside the party's caucus room as shots cracked in the hall outside. "As I put my hand on the door to open it, our security came in the other way and then we stood against it or tried to figure out what to do next," Cullen said Thursday. "Me and another MP went and barred the other door." Cullen said it wasn't until later that he realized his colleague was standing just where a bullet lodged in a door. "That sort of brings it home a bit for sure," he said. Michael Zehaf Bibeau stormed into the Centre Block with his lever-action rifle after shooting and killing honour guard Cpl. Nathan Cirillo at the nearby National War Memorial. Cullen says the day's events have had a long-term impact. "It is very much still on my mind," Cullen said. "It certainly affects the place where we all work." Bullet holes can still been seen in the Hall of Honour. There are imprints on people, too. Marc-Andre Viau, a NDP political staffer, remembers leaving the building that day and being told to "get down" by police. He also recalls seeing Zehaf Bibeau making his way toward Parliament Hill. "We took cover and that's when I saw in my peripheral vision, someone running towards the front door," Viau said. "We heard the shots, five, ten shots followed by a short pause and then about 40 shots after that . . . It was hard to believe that shots could be fired in Centre Block, it was kind of surreal." Outgoing **Public Safety Minister Steven Blaney** said he remembers being in the Conservative caucus, across the hall from the NDP meeting, when he heard shots. "***There was a moment of disarray where we realized that something was happening and that we were facing the unexpected***," Blaney said. Canadian Press (London Free Press, B1)

*** Leaders stand together at soldiers' memorial**

Days after contesting a bitter election campaign, Prime Minister Stephen Harper and prime minister-designate Justin Trudeau came together to lay a wreath in remembrance of two soldiers slain last October. It was a striking image of solidarity as the two men paid their respects, along with the Governor General and the families of Warrant Officer Patrice Vincent, killed in separate attacks one year ago this week. "Warrant Officer Vincent and Cpl. Cirillo both had very important jobs - to defend our rights and our freedoms as a people," said Gov. Gen. David Johnston. "This is who we are. "Our Parliament is a symbol of who we are. It, too, was attacked last October. Many of you valiantly rushed to defend it, just as others of you rushed to the aid of the wounded here in Ottawa and in Saint-Jean-Sur-Richelieu. You boldly reminded us that with our rights and freedoms, come responsibilities - responsibilities toward each other and to Canada." It was a moving tribute. Thousands gathered at the National War Memorial in Ottawa to mark the anniversary that featured a 21-gun salute and a flyover of CF-18s in the missing-man formation. After two minutes of silence, prayer and reflection came the laying of wreaths. But it was Johnston's speech that captured a reflective and sombre mood as he recalled the events of Oct. 20 and Oct. 22, 2014, when the two soldiers were slain. "Many people said Canada changed forever last October. But I

don't think Canada changed forever. Canadians are a caring, courageous people and that did not change, and that will not change." As he spoke, Nathan Cirillo's son, Marcus, now 7, fidgeted and gazed around at the cameras, the crowds and all the uniformed men and women… Outgoing public safety minister **Steven Blaney** switched between English and French as he recalled "***the fear, the panic" in the Conservative caucus room that morning as people thought a team of assailants were coming for them: "It was a moment of complete anguish***." … "It was crazy last year," RCMP commissioner Bob Paulson told the Star before the ceremony began. "It was a very challenging time … for the city of Ottawa, for the armed forces, for everyone." Paulson said the RCMP officers who were in the direct line of fire will be publicly honoured for valour soon, but this day was to remember the fallen and to mark "how far we've come since last year." Toronto Star, A4

*** Mountie killer prompted RCMP to test guns that can be converted to fully automatic**
RCMP tests on a variety of semi-automatic weapons sold in Canada have found the guns can be converted temporarily into fully automatic firearms through an improvised technique described on the internet. That was the conclusion of an internal report prompted by last year's shooting deaths of three Mounties in Moncton, N.B. The report was delivered to the public safety minister for possible action. RCMP Commissioner Bob Paulson wrote to **Steven Blaney** last December, detailing test results on six types of semi-automatics and recommending the government consider laws or regulations to ensure the improvisation technique is prohibited. The Mounties also sent a warning, known as an officer safety alert, to Canadian police forces in January this year tipping them to the technique "so that they may take appropriate enforcement or investigation measures." "Criminals could … adopt this technique to work around prohibitions on fully automatic firearms, potentially resulting in an increase in gun violence, mass casualties or copycat crimes as the technique is applied more broadly," Paulson advised the minister. In a response six months later, however, Blaney said changes are not needed. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Magnitude-4.7 earthquake reported off northern Vancouver Island**
An earthquake with a magnitude of 4.7 occurred off northwest Vancouver Island this afternoon. The earthquake occurred at 4:07 p.m., about 200 kilometres west of Port Hardy, according to Earthquakes Canada. It occurred at a depth of 10 kilometres. Port Hardy Coun. Patricia Corbett-Labatt was at a meeting at the district's office and said no one there noticed it. Earthquakes Canada said it had not received any reports from people who felt the quake. There are no reports of damage, and none would be expected, the federal agency said. Times-Colonist

*** Quadrivalent flu vaccine offers extra protection, Alberta health officials say**
Children vaccinated against the flu will be getting additional protection thanks to new vaccines available for the first time this year, according to Alberta health officials. Traditional flu shots and nasal mists protect against the H3N2 virus, the H1N1 virus and one strain of the influenza B virus. The new Quadrivalent vaccines, available for the first time this year, immunize against a fourth type of flu. CBC News

*** Eight Arctic nations to sign historic coast guard deal**
All eight Arctic nations - including Canada and Russia - are to sign a historic deal next week for their coast guards to work together in the treacherous and increasingly accessible waters of the North. Creating the Arctic Coast Guard Forum is considered a significant step forward for international co-operation in the region and will flesh out previous search and rescue agreements. "[The forum] will be an operationally focused organization that strengthens maritime co-operation and co-ordination in the Arctic," said an emailed statement from the United States Coast Guard. "The impetus for creating [it] grew out of the concerns of Arctic Council member countries over the increasing need to ensure safety, security, and stewardship of Arctic waters." The forum will also discuss emergency response, icebreaking and collaboration, said a statement from the Canadian government. "The heads of the eight coast guard agencies, including Canada, have agreed that collaboration on such operational matters is to everyone's benefit," said Carole Swaindon of the Department of Fisheries and Oceans, which runs the Canadian Coast Guard. Canadian Press (Times-Colonist, B5; National Post; Times and Transcript)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Anti-Islamophobia resolution fell short**

On Oct. 2, following an attack on a Muslim woman, the Quebec National Assembly passed a motion condemning Islamophobia. While Muslim Quebecers are supposed to applaud the gesture, it has in fact only strengthened the fears of many. Because, in the very act of officially recognizing the existence of the phenomenon of Islamophobia, our MNAs have drained the concept of any real significance. In fact, the content of the motion and some statements to media following its adoption make clear that our politicians unfortunately still do not understand that, before its expression in criminal acts, Islamophobia is first and foremost an ideology. The function of this ideology is to justify Islamophobic acts; without it, these acts would be condemned for what they are: racist and despicable crimes. And it would not be enough to merely condemn them, but necessary to fight them through concrete action, similarly to how the problem of radicalization has been approached. This, however, is far from our current situation. Postmedia Network (Montreal Gazette, A17)

«Je connais le son d'une détonation d'arme à feu»

Il y a un an, Robert Aubin se trouvait dans la salle du caucus de son parti lorsque Michael Zehaf Bibeau s'est mis à semer la terreur sur la colline parlementaire..«La grande question qui n'a pas été résolue par les conservateurs, c'est quelles sont les mesures de déradicalisation pour prévenir ces faits-là? Je l'ai vécu de très près et de l'interne, j'ai une grande réticence à parler d'un acte de terrorisme», soulève-t-il comme interrogation, évoquant un «gars isolé avec une arme rudimentaire». D'où l'opposition de son parti au fameux projet de loi C-51. «On va certainement revenir là-dessus. Tous les bons coups réussis par la GRC l'ont été par les lois précédentes. Ce n'est pas une question de loi, mais de ressources qu'on n'affectaient pas suffisamment à la GRC. Le projet de loi C-51 empiète sur les droits personnels», déplore celui qui rappelle la fin de l'hymne national, qui parle de protéger nos foyers et nos droits. «On doit faire les deux», a-t-il précisé. La Presse Canadienne (La Nouvelliste, 2/FRONT)

'On that day, we lost a son'

Tears fell where blood had been spilled at the National War Memorial as Canadians gathered Thursday to mark one year since a gunman brought terror and death to the country's capital.
Yet, while the ceremony was punctuated with sadness as Canadians remembered Warrant Officer Patrice Vincent and Cpl. Nathan Cirillo - two soldiers who died within days of each other at the hands of radicalized assailants - there was also strength, compassion and unity. "It's been one year," Gov. Gen. Postmedia Network (Vancouver Sun, B1/FRONT, Ottawa Citizen, A1/FRONT, Windsor Star, N1/FRONT, Leader-Post, Province, Star Phonenix)

*** One year on, a thankful nation pays its respects**

At 10:30 Thursday morning, 200 people ascended the ramp from the National Arts Centre to sunlit Elgin Street, pipers announcing the start of the ceremonies honouring Warrant Officer Patrice Vincent and Cpl. Nathan Cirillo, both victims of terrorism-inspired acts of violence a year ago. The marching group included members of the Argyll and Sutherland Highlanders of Canada (Princess Louise's), the Hamilton unit in which Cirillo served; the Royal Canadian Air Force, in honour of Vincent, an RCAF firefighter; and first responders from emergency organizations involved when Michael Zehaf-Bibeau, after fatally shooting Cirillo as he stood ceremonial guard at the Tomb of the Unknown Soldier, stormed the Parliament Buildings. Ottawa Citizen, A3

*** The shots that shook a country**

In a reflective moment this week, Cpl. Nathan Cirillo's sister Nicole likened her family's grieving experience to that of an overturned snowglobe. Canada has also been shaken by the tragedy, and numerous security procedures, laws and protocols have changed since the Oct. 22, 2014 shooting of Cirillo, 24, at the National War Memorial and the death of Warrant officer Patrice Vincent, 53, who was killed by a political extremist two days before in Saint-Jean-sur-Richelieu, south of Montreal. Here are some changes that have taken place as a response to the killings: Parliament Hill security: In June, a new

Parliamentary Protective Service was formed to handle security on Parliament Hill, inside buildings and out. Previously, the RCMP had jurisdiction over the grounds, while House of Commons and Senate security forces handled activity inside the buildings. The new force reports to the RCMP's national division. Bill C-51: The controversial bill increases powers of the Canadian Security Intelligence Service, criminalizes the promotion of terrorism and gives the RCMP new powers of preventive arrest. Hamilton Spectator, A10

* **Cérémonie en hommage aux deux soldats tués en octobre 2014**
Un an après les deux attentats commis contre autant de militaires canadiens, plusieurs centaines de citoyens se sont massés dans les rues d'Ottawa pour leur rendre hommage. Dignitaires, membres des Forces armées, policiers et premiers répondants se trouvaient hier matin au pied du Monument commémoratif de guerre du Canada, où le caporal Nathan Cirillo est tombé, le 22 octobre 2014, sous les balles d'un tireur qui s'était radicalisé. Cette attaque survenait deux jours après que l'adjudant Patrice Vincent eut été assassiné à Saint-Jean-sur Richelieu, en Montérégie, par un autre individu qui était aussi adepte de l'idéologie djihadiste. Dans un geste d'unité, le premier ministre sortant Stephen Harper et le premier ministre désigné Justin Trudeau ont déposé ensemble une gerbe de fleurs devant la tombe du soldat inconnu. Après avoir froidement assassiné le caporal Cirillo, le tireur Michael Zehaf Bibeau avait fait irruption dans l'édifice du Centre du parlement. Il est passé devant les salles où étaient réunis les caucus du Parti conservateur et du NPD avant d'être abattu par les services de sécurité. De nouvelles mesures de sécurité pourraient être déployées prochainement sur la colline du Parlement qui incluraient notamment un contrôle plus rigoureux des visiteurs se promenant à pied, selon un dirigeant de la Gendarmerie royale du Canada (GRC). La Presse Canadienne (La Presse, A10)

* **Standing firm in the face of terror**
A year ago, Canada was grappling with our first glimpse of radical Islamic terrorism on our own soil. We were trying to piece together the cowardly execution of Canadian soldier Cpl. Nathan Cirillo, gunned down while on ceremonial guard duty in Ottawa. Just two days earlier, another home-grown Islamist terrorist claimed the life of Warrant Officer Patrice Vincent in Saint-Jean-sur-Richelieu, Quebec, using a car as his weapon instead of a gun. Similar to the Ottawa attack, it was perpetrated by a Canadian-born Muslim convert who deliberately targeted members of Canada's armed forces. A year later, it's still impossible to make sense of such senseless acts. Cpl. Cirillo was murdered in front of the National War Memorial as he was standing ceremonial guard over the Tomb of the Unknown Soldier. The few times I've walked past the Cenotaph memorial since the shooting, I've felt a lump in my throat and a chill down my spine.
It's difficult not to get emotional when thinking about the brave men and women who stand on guard for Canada and fight for our freedom and security every day, both here and around the world. Post Media Network (Winnipeg Sun, 17, Toronto Sun)

* **Questions still loom over deadly shooting**
One year after the Oct. 22 attack on Parliament Hill, there are still many lingering unknowns about the events that unfolded that day. And while many of the blanks have been filled in by numerous profiles and news accounts about shooter Michael Zehaf-Bibeau, and numerous reports prepared by the various security agencies involved, many questions still remain.
And under the veil of a still-ongoing national security investigation, some may never be adequately answered. Where did a man with a history of psychological issues, drug abuse and incarceration obtain the long-barrel Winchester rifle used in the attack? In the days following the attack, RCMP Commissioner Bob Paulson acknowledged the source of the weapon wielded by Zehaf-Bibeau-- a Winchester .30-30 lever-action hunting rifle-- "is of tremendous interest to us." Ottawa Sun, 6

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

City's bill for legal fees to battle bridge: $2.9M
The Battle for the Bridge continues to cost Windsor, even before construction starts. The City of Windsor has spent $2.9 million the last five years in legal fees, fighting the Ambassador Bridge in court over a string of issues - though courts have reimbursed the city $1.3 million in awards. And the legal war should only heat up. A financial report going to council Monday shows that city legal costs so far this year are

about $650,000 over budget. Two-thirds of that revolves around the battle with the bridge, the city's single largest legal issue, according to treasurer Onorio Colucci. Also, in the next year or two the city will spar at the Supreme Court, which will cost an estimated $75,000 to $100,000 alone - to determine whether the bridge is deemed a federal undertaking, and therefore immune to municipal bylaws. "The legal investments made by the City of Windsor have led to creating nothing but lost opportunities," Stan Korosec, president of the Ambassador Bridge-owned Canadian Transit Company, said in a statement. "The previous city administration has spent taxpayers' dollars for well over 10 years objecting to any efforts made by the Ambassador Bridge. The end result is the community loses, the Windsor taxpayers lose, the travellers lose, and this region loses because we should have already had a new bridge operating." Korosec said Ambassador Bridge vice-chairman Matthew Maroun recently met with Mayor Drew Dilkens, and believes the parties can work out differences without amassing such high legal fees. (…)Though granting approval rests with Transport Canada, Dilkens does not oppose a second Ambassador Bridge span, as long as the city's concerns are addressed and the Gordie Howe International Bridge proceeds as planned. Windsor Star, A1 (London Free Press)

Let Morouns build new bridge now

A letter to the editor states, "If the Ambassador Bridge is collapsing as many local residents say, it's time to fix the problem. It's probably safe to say someone could get killed. But one cannot fix an old structure forever. Sooner or later, the repairs will not be enough to hold back the crumbling. How about a brand new one? It's time to face that fact. It is the answer to a crumbling bridge. Windsor should get behind bridge owner Matty Moroun and help expedite a new bridge immediately. Without the roadblocks thrown at this project, we could have had a new bridge by now." Windsor Star, A10

*** TPP would allow milk from cows receiving hormones into Canada**

As dairy imports from the United States appear set to increase under the terms of the Trans-Pacific Partnership trade deal, Canadian consumers concerned about drinking milk from cows receiving hormones will need to read their labels more carefully. In the agreement in principle reached Oct. 5, Canada conceded an additional 3.25 per cent of its dairy market to imports from the 11 other Pacific Rim countries signing on, most notably the U.S., New Zealand and Australia. That amount may not seem significant, but until recently, Canada's supply-managed dairy sector offered only the stingiest of tariff-free market access to its trading partners, on specific terms — such as the cheese deal struck with the European Union in 2013. Small levels of imports are possible while maintaining supply management, if they are managed carefully. The ultimate impact of the TPP on the dairy industry might depend on details not yet available on what kinds of products — and in what amounts — make up that 3.25 per cent. CBC News

Les agriculteurs souhaitent davantage de reconnaissance

Au moment où l'agriculture vit un vent de changements importants avec la signature possible de l'entente de Partenariat transpacifique (PTP) et l'imposition de normes environnementales de plus en plus rigoureuses dans un contexte de désengagement de l'État, les agriculteurs du Saguenay-Lac-SaintJean souhaitent obtenir davantage de reconnaissance en tant qu'acteurs économiques d'importance. Réunis à Jonquière dans le cadre de leur 85e congrès annuel sous le thème « On cultive aussi l'économie locale », une soixantaine d'agriculteurs ont pu discuter d'accaparement des terres, d'assurance agricole, de tarification compétitive pour les locataires de bleuetières et de financement de la recherche agricole. (…)Les deux porte-parole ont ajouté que la reconnaissance du travail des agriculteurs devrait se concrétiser également auprès des gouvernements supérieurs afin qu'ils investissent davantage dans le secteur de la recherche et développement ainsi que dans le contrôle à la frontière canado-américaine de l'entrée des protéines laitières. Le Quotidien, 8

Multiculturalism: Canada's ace card in the Trans-Pacific game

An opinion piece states, "The recent announcement of the Trans-Pacific Partnership (TPP) free-trade deal is one more confirmation of the importance of international trade for Canada. I anticipate that the new Liberal government of Justin Trudeau will endorse the TPP agreement. With the arrival of explorer John Cabot on the shores of Newfoundland, it was international trade in 1497 that started the economic heartbeat of the land mass that would become Canada. And international trade has nurtured Canada as one of the most prosperous countries in the world. International trade is an important contributor to

Canada's economic growth, business vitality, employment creation and the standard of living of its citizens. Canada's domestic population is far too small to alone sustain the standard of living that we have become accustomed to. International trade is the trump card that helps us create a larger market, through our exports and outreach. Canada is facing a demographic deficit, a fiscal deficit and a jobs deficit. Our economic salvation rests with an aggressive strategy for global outreach. The TPP will open new doors for our exports and create significant international trade opportunities. (…) In addition, Canadian exports will be granted unrestricted and preferential access to the EU domestic markets once the Comprehensive Economic and Trade Agreement (CETA) is ratified. The removal of the economic burden of tariffs will enhance our ability to be truly competitive in Europe." Times & Transcript, A11

The downsides of a good trade deal
An editorial states, "The Trans-Pacific Partnership is a good deal for Canada. It will give Canadian businesses new access to markets in Asia and provide consumers with less expensive goods. But no deal is perfect. Based on the few details available at this point, Canada may have yielded to changes to its copyright regime by agreeing to extend protections on original works from the current 50 years beyond the death of the author, to 70. In effect, this country and the other TPP partners will adopt U.S. rules that were largely crafted by lobbyists for Disney, which sought to forestall Mickey Mouse entering the public domain. There is no mention of this on the federal government website summarizing the pact. Instead, it emerged via leaks and information released by other countries, and was brought to the fore by intellectual property experts like University of Ottawa law professor Michael Geist, who reckons Ottawa "caved." (…)Since the TPP deal was announced, there have been other concerns. A big one is the inclusion of provisions that may open the door to more temporary foreign workers in Canada. But we don't yet know the scope and details of this. Which is why the most serious issue right now is making the agreement public as quickly as possible, so Canadians can finally see what they are getting into." Globe and Mail, A14

Unveiling for the camera?
A letter to the editor states, "Re: Wrong Side Of The Wedge, Robyn Urback; A Stand Too Far, Barbara Kay, both, Oct. 21. If Zunera Ishaq says she cannot unveil herself in a public citizenship ceremony because of her religion, how does she propose to deal with the requirements for a Canadian passport? Will Justin Trudeau be revising requirements for passport photos to accommodate her or will he insist only female Canadian Border Services agents can view her passport? How much accommodation should the Canadian government make for two women who do not wish to follow the normal procedures expected of all the other 30 million Canadians?" National Post, A13

*** Exercise aids preparation for potential St. Lawrence Seaway disaster**
Resuming ship traffic on the St. Lawrence Seaway as quickly and as safely as possible after a natural or man-made disaster was the topic of a binational exercise led Wednesday by the U.S. Coast Guard at Riveredge Resort. The exercise follows a 2011 initiative by the U.S. and Canadian governments called Beyond the Border, which is designed to address threats to cross-border commerce and promote binational law enforcement activities to mitigate the threats. Wednesday's exercise focused on potential disruptions in trade that could be caused by an interruption in shipping on the Seaway and a "maritime Commerce Resiliency" plan to restore traffic after a disaster. More than 100 participants, from law enforcement to shoppers to environmentalists, considered a scenario in which a foreign cargo vessel had become grounded near an international bridge, spilling fuel into the St. Lawrence River. For many, the scenario called to mind the April 21 grounding of the freighter Juno under the Thousand Islands Bridge, although no fuel or cargo was spilled in that incident and no one was injured. (…) participating in the exercise aside from the Coast Guard were the Canadian Coast Guard, U.S. Customs and Border Protection, Canada Border Services Agency, St. Lawrence Seaway Development Corp. and St. Lawrence Seaway Management Corp., Transport Canada, state Department of Environmental Conservation, Thousand Islands Bridge Authority, St. Regis Mohawk Tribe and Save the River, among others. Watertown Daily Times

*** Cig smugglers busted on St. Lawrence**
Cornwall police have been busy the last couple months stopping illegal tobacco from entering the region.

Five people have been charged, but at least two other suspects managed to flee in a dramatic getaway. The first major shipment of tobacco hauled out of the St. Lawrence River was intercepted by marine police officers who noticed a boat floating eastbound without its navigation lights on Aug. 4. Four people were seen waiting onshore south of Pointe Trepanier, Que. Cops say two people on the boat jumped ship and fled into the darkness. A white van was later spotted peeling away from the scene. Police, however, were able to seize the boat -- a 24-foot orca with two big engines. Onboard, cops found a total of 336 kilograms of tobacco in 30 large green garbage bags. "You open the bag ... and all you see is tobacco," recalled Const. Jean Juneau. (...)He said the tobacco sometimes comes from places in the U.S. or the Akwesasne region. Toronto Sun

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** TalkTalk cyber-attack: Boss 'very sorry for security breach'**
The head of TalkTalk says she is "very sorry" for the frustration and worry caused to customers after a major cyber-attack on the firm on Wednesday. The phone and broadband provider said personal and banking details of up to four million customers may have been accessed in the "significant" attack. Chief executive Dido Harding said the company had been working through the night to try to contact all customers. TalkTalk said it was too early to know exactly who had been affected. "I'm very sorry for all the frustration, worry and concern this will inevitably be causing all of our customers," Ms Harding told BBC News. "We have been working through the night to make sure that we contact all of our customers and can reassure them about how they can keep their data safe." BBC News

*** CIA director's emails published**
WikiLeaks posted material Wednesday from what appears to be CIA director John Brennan's personal email account, including a draft security clearance application containing personal information. The material presumably was taken in a compromise of Brennan's email account by a hacker who told The New York Post he's a high school student protesting U.S. foreign policy. The hacker claimed he posed as a Verizon employee and tricked another employee into revealing Brennan's personal information. Brennan was seeking security clearance while applying for a job as a White House counterterrorism adviser. Associated Press (Calgary Herald, A19; Toronto Star; Leader-Post)

*** Le transfert Europe-USA de données personnelles est compromis**
Dans une décision rendue le 6 octobre, la Cour de justice de l'Union européenne a invalidé le « Safe Harbour », un arrangement administratif qui permettait le transfert de données personnelles entre l'Europe et les Etats-Unis. La décision est une conséquence des révélations d'Edward Snowden au sujet des intrusions de l'agence américaine de sécurité dans les données personnelles de milliers d'internautes. Elle remet en question le cadre juridique qui permet le transfert massif de données d'un continent à l'autre, notamment plusieurs services reposant sur des solutions « infonuagiques », comme Facebook, Google ou Amazon. L'affaire origine d'une plainte logée par un citoyen autrichien utilisateur de Facebook. Comme pour les autres abonnés résidant dans l'Union européenne, les données qu'il fournit à Facebook sont transférées, en tout ou partie, à partir de la filiale irlandaise de Facebook sur des serveurs situés sur le territoire des États-Unis. Le citoyen s'est adressé à l'autorité irlandaise de protection des données personnelles. Il a invoqué les révélations faites en 2013 par Edward Snowden au sujet des activités des services de renseignement des États Unis. Journal de Québec

LAW ENFORCEMENT

Arrests made in $5-billion fraud scheme
Toronto Police helped the FBI uncover a $5-billion fraud and money-laundering conspiracy in a case they say highlights the need for co-operation to track crime proceeds that cross borders more easily than ever. FBI officers and United States Postal Inspection Service investigators watched Thursday in Toronto police headquarters as Detective Sergeant Ian Nichol traced the evolution of the case, which led to

charges against three Toronto-area residents and six south of the border. "We saw significant linkage with what was going on on the U.S. side ... notes were compared, and lo and behold, we were onto something bigger than what we had originally," Det. Sgt. Nichol said. The three charged locally are alleged to have wired funds through accounts in several countries, including the proceeds of "romance scams." They came to police attention through a local case: a 63-yearold Canadian widow who was swindled of her life's savings in 2014. Globe and Mail, A12; Toronto Sun, 4

Twenty rescued in human trafficking investigation

A major investigation into human trafficking has led to the rescue earlier this month of 20 people - some as young as 14 - suspected of working in the sex trade as minors or against their will, police said Thursday. The investigation - called Operation Northern Spotlight - led to the arrest of 47 people who are now facing 135 charges, including trafficking in persons, forcible confinement, child pornography, and sexual assault with a weapon. Officers met with people suspected of taking part in the sex trade in early October at locations across the country. Most of those rescued were under the age of 19, said Ontario Provincial Police Deputy Commissioner Scott Tod. "Human trafficking victims rarely identify themselves to authorities, so we have to take a proactive approach," Tod said at a news conference. Ontario Provincial Police led the latest phase of Operation Northern Spotlight, which involved officers from 40 police agencies across Canada and 350 officers and support staff. Canadian Press (Guardian, A8, Times Colonist, B5, Edmonton Sun, 50, Calgary Sun, 27, Edmonton Journal, N6), 1; Record, B1; Ottawa Sun, 9; Winnipeg Sun, 8; Winnipeg Free Press, B4 * La Presse Canadienne (Le Devoir, A4, Acadie Nouvelle, 19)

Six women interviewed during sex trade probe

Six women were interviewed locally as part of a national investigation into human trafficking and the sex trade that resulted in 47 people being charged with 135 offences. While the Cape Breton Regional Police Service and Eskasoni RCMP contributed to the investigation, none of the charges were laid locally. Earlier this month as part of Operation Northern Spotlight, members of 40 police services arranged to meet with people suspected of partaking in the sex trade, potentially against their will, at urban locations across Canada. The arrests were made over a seven-day period in early October. Police were also able to ensure the safety of 20 people who had been working in the sex trade as minors or against their will. In Cape Breton, Cape Breton Regional Police and Eskasoni RCMP interviewed six women ranging in age from 20 to 40. Cape Breton Post, A1, A4

Clark staff breaks rules, report says

Political staff in Premier Christy Clark's office and in ministries have been routinely destroying government records and violating the province's access to information law, a new report says. Privacy commissioner Elizabeth Denham said Thursday she uncovered evidence of negligent searches for records, failures to document searches and the "wilful destruction" of records in response to requests for information. Denham said "it is difficult to overstate the seriousness of the problems" or the threat they pose to the integrity of access to information in B.C. "I am deeply disappointed by the practices our investigation uncovered," she writes in the 65-page report, Access Denied. "I would have expected that staff in ministers' offices and in the office of the premier would have a better understanding of records management and their obligation to file, retain and provide relevant records when an access request is received. "In conducting this investigation, it has become clear that many employees falsely assume that emails are impermanent and transitory, and therefore of little value." Denham launched the investigation in May after Tim Duncan, a former executive assistant to Transportation Minister Todd Stone, wrote to her complaining about the destruction of records. Duncan said in the letter that he had been on the job only for a few weeks in November 2014 when the ministry received a request for records relating to the disappearance of women along Highway 16, known as the Highway of Tears. He said he searched his emails, turned up more than a dozen relevant documents and informed ministerial assistant George Gretes, who told Duncan to delete the records... "It is government's clear expectation that all government staff follow all legislation without exception," said Citizens' Services Minister Amrik Virk. Victoria lawyer Chris Considine, who is representing Gretes, declined comment. The RCMP confirmed receipt of Denham's report. "We will be reviewing the content of their report and assessing it with respect to possible Criminal Code offences," Staff Sgt. Rob Vermeulen, a media relations officer, said in a statement. "It would be inappropriate to comment further at this time, as the review process has just begun." Times Colonist, A1; Postmedia Network (Vancouver Sun, A1); Globe and Mail, A1; Canadian

Press (Kingston Whig Standard, B1), Calgary Herald, A3); Globe and Mail, A1; Canadian Press (Kingston Whig Standard, B1, Toronto Sun, 16, National Post, A9); * 1

*** B.C. Liberals would like to delete this report**

An editorial states " Premier Christy Clark left it to cabinet minister Amrik Virk Thursday to respond to the information watchdog's devastating findings about the culture of coverup inside the B.C. Liberal government. Clark knew very well what was coming. Information Commissioner Elizabeth Denham, respecting protocol, shared her findings with the government in advance. The government fired back with a legal letter, disputing some aspects of the report and seeking more time to respond. Denham, to her credit, stuck to the scheduled release time of 9:30 a.m. Thursday. By that time Clark, who was in the capital Wednesday, was ensconced in the cabinet office in Vancouver, ostensibly to participate in a telephone conference with other provincial leaders. So it fell to Virk, as minister responsible for the Freedom of Information (FOI) legislation, to handle the press gallery - reporters were given all of 15 minutes to read the 60-page report before the minister met with them - then a barrage of questions in the legislature from the New Democratic Party Opposition. He said much the same as Clark will no doubt say, when she gets around to it. Findings being taken seriously. Recommendations being implemented. Government expects everyone to respect FOI. Unfortunately these isolated incidents crop up from time to time - rarely, mind you - where some rogue staffer - a total miscreant, really - departs from the guidelines that everyone else - and I do mean everyone - follows to the letter and respects without reservation. Or other empty words to that effect. Granted, one finding in the Denham report was both shocking and unprecedented: Transportation ministry staffer George Gretes lied under oath a half-dozen times about deliberately deleting emails and confessed only when confronted with the overwhelming forensic evidence of his deletions. He's now resigned, his case has been sent to the RCMP, and the whistleblower in this affair, ex-Liberal staffer Tim Duncan, stands vindicated. Indeed, one now has to credit Duncan's claim that other Liberal political staffers routinely delete what they shouldn't, and otherwise tamper with the documentary record." Postmedia Network (Vancouver Sun, B6)

*** RCMP boss defends force's actions in 2014 attacks on Parliament**

Terror-attack warnings received in the days before the Oct. 22, 2014, assaults at the National War Memorial and in Parliament were not specific enough for the RCMP to stop the shooter, says the commissioner of the Mounties. Bob Paulson was reacting Thursday to a CBC News story that said the Mounties had received three separate terror-attack warnings in the five days before Michael Zehaf-Bibeau shot dead a sentry at the war memorial, then stormed Parliament Hill where he died in a hail of gunfire in the hall of honour. "There was no specific threat that said, 'Hey, there's a guy named Bibeau who's going to come shooting and run up on the Hill,"' Paulson said at a downtown Ottawa memorial service marking the tragedy. "That said, we responded to those elevated threat levels." Internal documents obtained under access to information show the force distributed three warnings, the first on Oct. 17 alerting all security personnel to potential terror attacks, and raising Canada's threat level to medium from low. None of the documents identified likely dates, locations or targets. Security experts have also said that without more precise details, it is difficult to act apart from instructing officers about an elevated threat level that requires precautions. CBC News (2015-10-22)

*** Mounties who helped take down Ottawa gunman not invited to anniversary ceremony**

RCMP Commissioner Bob Paulson says he doesn't know why four Mounties who helped corner and kill the Parliament Hill gunman one year ago were not invited to Thursday's official commemoration. "We have a troop of 32 people (who are) going to march in here, so I don't know the answer to that question," Paulson told CTV's Ottawa Bureau Chief Robert Fife ahead of a sombre ceremony at the National War Memorial, where Cpl. Nathan Cirillo was killed. Paulson has faced criticism after Sergeant-at-Arms Kevin Vickers was honoured for his part in subduing the gunman, while four heroic officers – including a man who delivered a shot killing Michael Zehaf-Bibeau – did not even receive a handshake or a thank you note from their boss. Sources say the four officers had hoped that Paulson would invite them to Thursday's ceremony. Former RCMP Deputy Commissioner P.Y. Bourduas called the failure to include the men in the ceremony "a regrettable oversight." Paulson said, however, that he has publicly thanked his officers, and that a ceremony is being planned where the four Mounties will get commendations and bravery awards. "Today is not the day to be talking about that," he added. "Today is the day to be

remembering what happened." Since the shooting, one of the officers was briefly assigned to RCMP car wash duty, sources say. CTV News (2015-10-22)

A tribute to the fallen
It was the perfect day for some welcome healing - a warm, midautumn sun, mostly blue skies and a gentle breeze. The specific occasion was to pay tribute to the average citizens and first responders who raced to help, but could not, one year ago; to the police and security personnel who risked their own lives to protect others - but most of all to the two soldiers who were hunted down and killed for reasons that will forever escape. The larger occasion brought together the country's three most significant personalities of the moment: Stephen Harper, the current Prime Minister of Canada, Justin Trudeau, the prime-minister-designate and David Johnston, the Governor-General who will hand power from Mr. Harper to Mr. Trudeau on Nov. 4... Kevin Vickers, the Canadian ambassador to Ireland who was then sergeant-at-arms for the House of Commons, was one of those who put a quick end to the attack, thereby saving countless other lives. "Today," Mr. Vickers tweeted from Ireland as the ceremony took place, "my thoughts and prayers are with Kathy Cirillo, Nathan's mom, all HoC& Senate Security, RCMP, Ottawa Police. Globe and Mail, A1* Calgary Sun, 7 (Ottawa Sun, 5)

Friends of Harry Doyle frustrated by delays in case
There are several steps that must be taken before an arrest warrant is executed for a Fredericton woman facing charges in the Philippines relating to the 2012 shooting death of her husband. Staff Sgt. Julie Gagnon with the RCMP in Ottawa said the force is aware of the International Criminal Police Organization's (Interpol) red notice about Erma (Jane) Doyle, which it has received along with 189 member countries at the request of the Philippine National Police. Doyle came to Canada shortly after former Fredericton businessman Harry Doyle was shot and killed on Aug. 12, 2012, during a family barbecue at Palma Beach Resort in Punta Pilar, Surigao City. In August 2013, the Philippine National Police issued an arrest warrant for Doyle on a charge of parricide. She continues to live in Fredericton along with her sons. Gagnon said the RCMP won't comment on investigations being conducted by foreign authorities. "What should be noted is that an arrest warrant issued by a foreign country is not valid in Canada," said Gagnon. She said a foreign suspect can only be arrested if he or she has committed the crime in Canada or is in violation of the Canadian Immigration Refugee and Protection Act. An arrest warrant would be issued by Canadian authorities following the receipt of a provisional arrest request from a foreign country, Gagnon said. The international assistance group with the federal Department of Justice would first look into a case to determine whether a provisional assistance warrant is required. "It would mostly likely be given to the police of jurisdiction to act upon it then and to arrest the individual based on the request. "People believe that an Interpol red notice is an international warrant which doesn't exist. That's why a provisional arrest warrant needs to be issued after the fact," Gagnon said. In this case a provisional arrest warrant would be served by the Fredericton Police Force. The RCMP said it would be up to justice authorities in the Philippines to send an extradition request to the Department of Justice in Canada. Daily Gleaner, A1

***Police can't 'detain people just because people don't want to talk to them,' judge warns**
A judge has acquitted Susan Lynn Carter, 52, of Chamcook in St. Stephen provincial court on a charge of drinking and driving. RCMP Const. Pierre Phaneuf did not form a suspicion that Carter had alcohol in her system until after he detained her without grounds on Aug. 23, 2014, in Saint Andrews, Judge Henrik Tonning ruled on Wednesday. Phaneuf pulled Carter over for speeding, but it turned into an investigation into possible domestic violence, until a bottle of wine on a bed and a "fruity" smell on Carter's breath tweaked the officer to suspect that he had an impaired driver on his hands, according to testimony at the trial. The officer testified that the suspected speeder on Route 127 pulled into a Saint Andrews driveway. He noted a "fruity" smell on the woman's breath which he attributed to chewing gum, he said. Phaneuf testified that he suspected a domestic assault after the woman pointed to bruises on her arm. They agreed to go to the Saint Andrews RCMP, but Carter insisted that they drive to her mother's home first... "She was arbitrarily detained ... he had no right to keep her there, and no right to keep her licence, and no right to demand that she follow him to the RCMP station," he ruled. Tonning ruled further that the officer detained Carter for obstruction at her mother's house without advising her of her right to consult counsel. The fruity smell might have given grounds to demand that Carter breathe into an approved screening device after Phaneuf stopped her for speeding, but not later after detaining her without legal grounds, he

ruled. The bottle of wine was in the house, not in the car, so could not give rise to suspicion that the woman was drinking, Tonning ruled. "The point is, the police simply can't bird-dog or detain people just because people don't want to talk to them," the judge ruled. Telegraph Journal, B7

A grim reality: 'Grain is dangerous'
When Dennis Becker saw his grandson sinking in a semi-trailer loaded with grain, he did all he could to save him. But as he clawed through the pile of tiny kernels trying to free 14-year-old Layne Langridge, the 63-year-old man became trapped as well. Within minutes, both had suffocated on Becker's farm near Burstall in southwestern Saskatchewan. Family members later realized, after the bodies were freed from the truck, how frantically Becker had been trying to pull the boy out - the nails on his purple fingers were peeled back. Becker's son, Barry, says he and his family replay the Aug. 31 tragedy in their heads every day... "Had I said that back then, when I had a chance, who knows?" Could he have saved those girls? RCMP have said Catie Bott, 13, and 11-year-old twins Dara and Jana were playing in a truck loaded with canola on their family's farm near Withrow when they died Oct. 13. Their funeral is in Red Deer on Friday. Canadian Press (StarPhoenix, A1, Calgary Herald, Leader-Post, National Post); * Canadian Press (Calgary Sun, 12)

***Helicopter goes down on island in North Saskatchewan River**
Emergency services responded to a helicopter crash on an island in the North Saskatchewan River near Paynton on Thursday afternoon. "At 2:05 p.m., STARS Air Ambulance, from our Saskatoon base, began responding to a helicopter crash approximately 23 kilometres northeast of Maidstone," STARS Air Ambulance spokesman Cam Heke said Thursday night. Heke would not confirm if anyone travelling in the downed helicopter was killed or injured. He said STARS personnel landed on the island but that the air ambulance "was not medically required to transport patients." Heke said several people who had perhaps swum out to the island to assist in the aftermath of the crash were assessed by ground emergency services, who were assisted by STARS medical staff. Heke said he didn't know what kind of helicopter crashed or the circumstances surrounding the incident. "Aviation, particularly helicopter aviation in Canada, it's a relatively small world, and so our hearts and our thoughts are with those involved," he said. Officers from the Maidstone, Turtleford and Battlefords RCMP detachments also responded to the crash. Postmedia News (StarPhoenix, A6, Calgary Herald, A11), 1; * Journal de Montréal, 17

***All clear at Come By Chance refinery**
All non-essential personnel were evacuated from the Come By Chance refinery site Thursday after a bomb threat was made, a spokesperson for North Atlantic Refinery said. Shortly before 5 p.m. Thursday, the RCMP, consulting with management at the North Atlantic Oil Refinery, determined the site was safe, and operations returned to normal. Clarenville RCMP Sgt. Greg Hicks told The Packet that police support services, including the explosive disposal unit and police dog service, went to the scene.
"The investigation into the threat is ongoing," Hicks said. Telegram, A5

***Hold people to account for police HQ: Mayor**
Mayor Brian Bowman says that if someone on city council is found at fault in the RCMP investigation of the new Winnipeg Police headquarters, he will hold them accountable. "I'll do everything in my power to make sure that people are held accountable if there's wrongdoing," said Bowman. "I am quite anxiously awaiting the results of the RCMP investigation." Originally estimated to cost $135 million, Winnipeg's new police service headquarters is now expected to cost $214 million and has been delayed multiple times. Media reports earlier this year state the RCMP investigation has "multiple targets" but did not identify individuals. A whistleblower reportedly alleged invoices were altered and a payment was made to a member of city council. It was also alleged that one witness to this was interviewed by Winnipeg police. An external audit found severe mismanagement plagued the project, while an ongoing RCMP investigation will determine if the project involved criminal wrongdoing. To date, no city official has been penalized for their involvement in the project, a fact the Canadian Taxpayers Federation has questioned. Winnipeg Sun, 5

***Traffic crackdown results in 20,000 tickets**

A traffic enforcement initiative by RCMP and city police forces in Saskatchewan - aimed at excessive speeders, distracted and impaired drivers - has resulted in massive numbers of tickets. Officers in the joint initiative, called Combined Traffic Services Saskatchewan (CTSS), issued nearly 20,000 tickets all over Saskatchewan between October 2014 and September 2015. Thirty per cent of the tickets were issued in Saskatoon. CTSS is a two-phase program. The first phase is being enforced in Saskatoon and central Saskatchewan. The second phrase was started in June and is enforced in the Weyburn and Estevan areas. Superintendent Grant St. Germaine, acting criminal operations officer for the RCMP in Saskatchewan, said CTSS will team up with other agencies, such as the ministry of highways, this week.They will undertake an enforcement initiative to educate people about the importance of slowing down in construction zones and passing emergency vehicles. "We've had members from the local communities come up to our members and the RCMP members to appreciate the additional enforcement," Saskatoon city police Insp. Mitch Yuzdepski said. Postmedia News (StarPhoenix, A7)

***Escaped Island inmate captured in Surrey**

A prisoner who was able to run from a B.C. Corrections officer at Victoria General Hospital, smash through a window, and steal a car to aid his dramatic escape has been apprehended. Tyler Desmond Fong, 31, was arrested Wednesday after a quick foot pursuit at about 3:50 p.m. in the 10200 block of King George Boulevard in Surrey. No one was injured, police said. Fong was in jail following convictions this year for a string of property offences in the Ladysmith and Nanaimo areas. He was on the run for 19 days. A prisoner at Vancouver Island Regional Correctional Centre, Fong was brought to Victoria General Hospital's emergency department on Oct. 4 for medical treatment. Fong escaped shortly before 8 p.m. that night from the custody of a provincial correctional officer at the emergency department. Police did not alert the media until the next morning, after they had acquired a warrant for his arrest and approval to release the prisoner's name and photograph. West Shore RCMP received information on Fong's location, co-ordinated its search with Surrey RCMP and its auto crime unit, and executed Fong's capture Wednesday. Fong had a history of escaping from custody, said West Shore RCMP. At the time, Justice Minister Suzanne Anton would not provide details as to how the prisoner - in an emergency room with other patients and staff - was supervised and how he was able to escape. The provincial Justice minister said B.C. Corrections would review the escape. Postmedia News (Province, A9, Times Colonist, A3)

Arrests made in $5-billion fraud scheme

Toronto Police helped the FBI uncover a $5-billion fraud and money-laundering conspiracy in a case they say highlights the need for co-operation to track crime proceeds that cross borders more easily than ever. FBI officers and United States Postal Inspection Service investigators watched Thursday in Toronto police headquarters as Detective Sergeant Ian Nichol traced the evolution of the case, which led to charges against three Toronto-area residents and six south of the border. "We saw significant linkage with what was going on on the U.S. side ... notes were compared, and lo and behold, we were onto something bigger than what we had originally," Det. Sgt. Nichol said. The three charged locally are alleged to have wired funds through accounts in several countries, including the proceeds of "romance scams." They came to police attention through a local case: a 63-yearold Canadian widow who was swindled of her life's savings in 2014. Globe and Mail, A12; Toronto Sun, 4 (Edmonton Sun, 54); * Agence QMI (Journal de Montréal, 27); 1, 2

*** Probe into Quebec police abuse nears end**

Quebec provincial police have nearly completed a five-month internal investigation into eight officers accused of abuses against indigenous people, and say they will soon send the files to the Crown for possible criminal charges.The Sûreté du Québec launched a probe into officers at its Vald'Or detachment in May, after 12 aboriginals - mostly women - came forward with allegations of abuse of power as well as sexual and physical abuse dating to between 2002 and 2015, spokeswoman Sergeant Martine Asselin said. All of the officers, including at least one woman, have been questioned and remain on duty, she said. In the coming weeks, the files will be provided to the Crown for potential prosecution.Several of the aboriginal women gave their accounts to CBC's French service, Radio-Canada, and some went on to file formal complaints. According to the program Enquête, the women alleged a long-standing pattern of officers picking up women, driving them to remote areas and then leaving them there to walk back. Some women alleged physical assault and sexual abuse, with one saying she was paid to perform sex acts - at

times in exchange for cocaine."We went to a road in the woods and that's where they would ask me to perform fellatio," Bianca Moushoun told the program. The officers, whom she said offered her beer from their trunk, would allegedly pay her $100 for the sex act and $100 in hush money. "They were in uniform, with their guns," she said."They have the power. They have the badge."Allegations about aboriginal women being abused and mistreated by police have surfaced across the country over the years. Human Rights Watch released a scathing 2013 report detailing allegations against the RCMP in northern B.C. regarding the abuse of aboriginal women, including rape and an unwarranted attack by a police dog.These kinds of accusations, indigenous leaders say, feed into the historic mistrust of law enforcement and underscore the need for a national inquiry into Canada's more than 1,181 missing and murdered aboriginal women. Prime-minister-designate Justin Trudeau said earlier this week his Liberal government would move forward "quickly" with an inquiry.Dawn Lavell-Harvard, the president of the Native Women's Association of Canada, said she was "disgusted" by the Val-d'Or allegations and not entirely surprised; she has heard similar accusations elsewhere, she said."Until you have an inquiry ... to actually expose how our women are treated, this kind of thing won't change," she said.Police services have been working to rebuild their relationship with the aboriginal community after decades of tension - stemming, in part, from law enforcement's role in forcibly removing indigenous children from their homes and taking them to residential schools, where they were stripped of their culture and abused. Some families of missing or murdered indigenous women continue to express deep mistrust, saying they believe their relatives' case was mishandled due to police bias. Globe and Mail, A7

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Dorchester inmate hospitalized after assault**
An inmate from the Dorchester Penitentiary was sent to the hospital earlier this week after being assaulted in the medium security unit. Correctional Service Canada issued a statement on Thursday saying the inmate was assessed by staff after the assault and then taken to an outside hospital. No staff members or other inmates were injured during the altercation, which happened on Sunday morning. "The assailant has been identified and the appropriate actions have been taken," the statement said. The Correctional Service Canada says it will review the assault and will take the appropriate steps to prevent further incident. CBC News

Dorchester tulip garden honours Second World War veterans
A small group of volunteers braved the rain and cold Thursday to plant hundreds of tulip bulbs in the Dorchester Village Square to commemorate the 70th anniversary of the liberation of the Netherlands during the Second World War. "It's very fitting that we are doing this in Dorchester, right next to the cenotaph that remembers our veterans from the wars," said Susan Spence, co-president of the IODE Shepody Chapter, as she and others knelt on the cold ground to set the bulbs in a freshly-dug trench surrounding the war memorial. "We have a very strong Remembrance Day program here." (...)The volunteers from the IODE had help Thursday from a few inmates from Dorchester Penitentiary, who did the work of digging and refilling the flower bed. The Correctional Service of Canada inmate community work program allows inmates supervised leave from the institution for several hours. In Dorchester, they have done jobs ranging from building maintenance and gardening to painting lamp posts and fire hydrants. Telegraph-Journal, A4 (Times & Transcript)

Deportation awaits killer
After a decade in prison, a 33-year-old man will have to choose between staying in a Canadian jail or applying for his parole and likely being deported to Somalia. Bashir "Donovan" Gaashaan, 33, was sentenced to life in prison with no possibility of parole for 10 years on Thursday in Red Deer Court of Queen's Bench. He pleaded guilty to second degree murder and committing an indignity to human remains on Monday. Jenna Cartwright, 21, was killed on March 30, 2011. Her body was dumped in a treed area east of Olds, about six metres from a rural road. Justice Read said when the body was found more than a month later, it had been scavenged by wild animals. Gaashaan, a Somalian refugee who came to Canada in 1993, faces potential deportation back to Somalia upon his release from jail. "You may deprived of your ability to remain in Canada," said Justice Donna Read. "That's terrible, but that's

what happens." Read imposed the minimum wait of 10 years for a parole application for a second-degree-murder conviction. She said Gaashaan has shown remorse and has made steps to improve his life while in custody at the Edmonton Remand Centre for the last four years. Red Deer Advocate, A1

*** Conviction, sentence appealed**
A Dartmouth man who was shot by police in June 2013 after he pulled a knife on officers is appealing his conviction and sentence. Last month, Christopher James Cockerill, 37, was sentenced to four years five months in prison for the June 27, 2013, incident. However, because he was granted remand credit of about 40 months, he only has 13 months to serve. Cockerill pleaded guilty last year to eight charges in connection with the incident, including three counts of assaulting a police officer with a knife and one count each of possession of weapons (two knives) for a dangerous purpose, uttering threats and resisting arrest. He filed papers with the Nova Scotia Court of Appeal earlier this week. Chronicle-Herald, A6

*** L'ancien père oblat Eric Dejaeger fait appel**
Un ancien père oblat dans l'Arctique déjà en prison pour des dizaines d'infractions à caractère sexuel contre des enfants inuits interjette appel. L'information a été divulguée dans un tribunal du Nunavut à Iqaluit, jeudi, alors qu'Eric Dejaeger s'est vu infliger une peine concernant d'autres agressions sexuelles contre des enfants en Alberta. Des peines de cinq ans ont été ordonnées pour des gestes commis contre trois enfants âgés de six à neuf ans à Edmonton et Grande Cache dans les années 1970. L'une des victimes, alors enfant de choeur âgé de neuf ans, a été agressée sur une période de quatre ans. Les deux autres étaient un frère et une soeur, âgés de huit et six ans, qui ont été agressés sur une période de trois ans. (…)Il purgeait déjà une peine de 19 ans dans une prison du Nunavut avant l'audience de jeudi. Presse canadienne (Voix de l'Est, 9), Canadian Press (National Post, Times Colonist), Radio-Canada

*** The Shop makes cut as prison hangout**
An opinion piece by federal inmate Jose Vivar states, "I haven't cut my hair in close to a year, and I'm starting to look like someone who attended Woodstock or wherever those hippie parties used to happen back in the '70s. But just because I don't get my hair cut doesn't mean I'm not a regular to the **prison** barber shop. There's not a day that I don't visit The Shop. Not only because I have to pass it on the way to the library, chapel or school and might as well drop in to see what's going on, but I visit it because it's the most fascinating place in here." Kingston Whig-Standard, A6

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

End of the road for random street checks
Random and arbitrary carding by police forces across Ontario will be illegal by the end of fall. Yasir Naqvi, minister of community safety and correctional services, made the announcement during a debate Thursday where MPPs from across the province spoke out against carding. At the time they were considering a private member's motion from a New Democrat MPP to ban random and arbitrary carding, also known as street checks. "It's a historic day," said Margaret Parsons, executive director of the African-Canadian Legal Clinic, who watched the debate in the legislature. "This is a monumental shift in our province," said Parsons, who has worked to end carding. She repeatedly paused to compose herself when talking to the Star outside the legislature. "We have been around for 21 years. We have been fighting on this issue since the day our doors opened in July 1994." Earlier in the legislature, Naqvi moved quickly during the debate to address the motion from New Democrat MPP and deputy party leader Jagmeet Singh. "We as a government stand opposed, Speaker, to any arbitrary, random stops by the police simply to collect information when there are no grounds or reason to do so," Naqvi said. "We have heard from the community that street checks, by definition, are arbitrary as well as discriminatory and therefore cannot be regulated; they must simply be ended. The province agrees that these types of stops must end." Toronto Star, A1 (Hamilton Spectator, A1); Waterloo Region Record

*** A useful inquiry into the missing, murdered**

An editorial states, “The timing, it seemed, was worthy of a top-notch Hollywood movie. No sooner had the keys to Parliament been handed to a party that has promised a national inquiry into Canada's missing and murdered indigenous women when news broke Quebec provincial police face allegations they have taken aboriginal women for rides out of town and demanded sex. The aboriginal communities' distrust of police across Canada is like a poison infecting efforts on both sides to battle the violence plaguing indigenous girls and women. Yet, the coincidence is not so remarkable: on any given day, Canadians can hear of yet another tragedy, heinous crime or grave offence against an aboriginal person. This is a sad reflection on the reality in this country. And Justin Trudeau's Liberal government has now assumed the prime responsibility of addressing the historical, complex factors that feed into a shameful state of affairs.” Winnipeg Free Press, A8

*** Inquiry a waste of resources**

An editorial states, “Prime minister-designate Justin Trudeau has promised to quickly launch an inquiry into missing and murdered aboriginal girls and women - an expensive exercise in telling Canadians what they have known for years. An inquiry will generate a thick tome of recommendations and remonstrations that will be consigned to a shelf where, over the coming years, it will be cocooned in a layer of gently accumulating dust. As outgoing Prime Minister Stephen Harper has pointed out, we know the many factors behind these women's tragic fates; this is a matter for law enforcement agencies, not for government rumination on, and review of, what is already known. Unemployment, substance abuse, domestic violence and the other ills that plague many of Canada's reserves and urban aboriginal communities have been extensively documented. Eight years ago, the federal Department of Justice's publication, Victims of Crime Research Digest No. 3, focusing on a summary of the literature on aboriginal victimization in Canada, stated: "Perpetrators of violence against aboriginal people are most often other members of the aboriginal community such as spouses, relatives, or friends of the victim, and as such, victimization among aboriginal people in Canada is often regarded as a mirror image of aboriginal offending."” Calgary Herald, A20

*** Privacy commissioner slams government for deleting emails about Highway of Tears**

In a scathing report that includes evidence of potential crimes in Victoria, B.C.'s privacy commissioner slammed Premier Christy Clark's government for hiding and destroying damaging political information in high-level offices. Commissioner Elizabeth Denham's report examined the record-keeping practices in Clark's own office, the Ministry of Transportation, and the Ministry of Advanced Education. In all three offices Denham found political staffers breached their duty to inform the public. Denham found that staffers did not adequately keep email records under freedom of information law, neglected to respond to information requests, and intentionally destroyed records that were seen by the government as politically sensitive and confidential. "Taken together, these practices threaten the integrity of access to information in British Columbia," Denham said. Denham says she was saddened to have to forward evidence to the RCMP after a Ministry of Transportation political staffer was found to have intentionally deleted emails and lied under oath to Denham's investigators. The RCMP confirmed it is reviewing evidence of "possible offences" submitted by Denham. Denham's investigation was triggered after a whistleblower alleged that in November 2014 George Gretes, a former staffer for Transportation Minister Todd Stone, deleted emails about Victoria's response to Highway of Tears concerns. The whistleblower, 36-year-old Tim Duncan, alleged Gretes directed him to delete the emails and when he hesitated Gretes took his computer keyboard and did it himself. The Province

*** Local artist hopes project will make a national impact**

Eagleclaw Thom knows he has a daunting task ahead of him. But he's looking forward to the challenge of honouring the legacy of women through art. He was one of two artists selected for the University of Regina's new Michele Sereda artistin-residence position. Thom hopes his project, which pays tribute to missing and murdered indigenous women (MMIW), will not only honour the families, but his former colleague as well. Sereda, an alumnus of the theatre department, was one of five people killed in a multi-vehicle crash north of Regina in February. "Michele cared very deeply for the community, so that's why I proposed a project that includes community involvement, and she cared a lot of social justice issues," he said. "I hope it will be responsive to the ways she was involved in the community and contribute in some way that she would be proud of." The issue of MMIW is something that has affected his own life. Leader-Post, A4

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER

U of T throws learning lifeline to those who've faced danger
It was in a public park, of all places, one summer morning in a Tajikistan village that University of Toronto PhD researcher Alex Sodiqov had his freedom snatched away.
The 32-year-old international student had returned to his home country for two weeks last year to do research on conflict resolution. He was meeting an activist when authorities approached to ask for his ID - in broad daylight. Within days he was charged with treason on grounds that were never explained. He spent 40 days in jail. It would be nearly three months before he, his wife and baby daughter were allowed to return to Canada, where they were embraced by a program that supports newcomers who face danger back home.
"When you come out of a hot situation where you've been detained, your finances are stretched because you're hiring lawyers and your family is staying in hotels as they wait for your release," said Sodiqov, now in his second year of support from U of T's Scholars-at-Risk program. Toronto Star, GT1

Don't cosy up to Saudi Arabia
Some experts would have Canadians believe that this country's influence in the world would be enhanced by jettisoning a principled approach to foreign policy in favour of an expanded role at the morally compromised United Nations. Last month, Canadian government documents marked "secret" and "confidential" were leaked to the media during the heat of the recent federal election campaign. The internal documents offered critical analysis of Canadian foreign policy. The leaked documents reportedly lamented the supposed decline of Canada's international status and influence. They made much of Canada's failed bid to secure a temporary seat on the United Nations Security Council in 2010, citing the Harper government's staunch support for Israel as one of the reasons for Canada's international decline. Kingston Whig-Standard, A5

INTERNATIONAL

* **Hurricane Patricia bears down on Mexico**
Residents of a stretch of Mexico's Pacific Coast dotted with resorts and fishing villages boarded up homes and bought supplies ahead of Friday's arrival of Hurricane Patricia, a monster Category 5 storm that forecasters warned could be catastrophic. Officials declared a state of emergency in dozens of municipalities in Colima, Nayarit and Jalisco states that contain the bustling port of Manzanillo and the posh resort of Puerto Vallarta. The governor of Colima ordered schools closed on Friday, when the storm was forecast to make what the U.S. National Hurricane Center called a "potentially catastrophic landfall." Rain pounded Manzanillo late Thursday while people took last-minute measures ahead of Patricia, which quickly grew from a tropical storm into a Category 5 hurricane, leaving authorities scrambling to make people safe. Associated Press (CTV News)

* **'An immense tragedy': Dozens killed in French bus-truck collision**
A truck and a bus transporting retirees on a day trip collided and caught fire Friday in wine country in southwest France, killing 42 people and badly injuring four others, authorities said. It was the nation's deadliest road accident in more than 30 years. An image released by BFM television showed the carcass of the bus -- nothing but a collapsing, charred frame engulfed by smoke. Firefighters fanned out along the narrow country road, between a wooded area and an upward slope near the village of Puisseguin, about 50 kilometres east of Bordeaux. Eight people, including the driver, escaped from the bus after the driver opened the door, but others were trapped as the blaze consumed the vehicles, Puisseguin Mayor Xavier

Sublett said on i-Tele television. The four injured were among those who escaped. French media said the truck driver was killed. Associated Press (CTV News)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
October 27, 2015 / le 27 octobre 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Tory senators could disrupt plan to change anti-terror act
Liberal government changes to the Conservatives' incendiary anti-terrorism law could face a bumpy trip through the Conservative-controlled Senate. "There may be some things that Mr. Trudeau and some of his colleagues are very supportive of, but they may be matters that an overwhelming majority of Canadians are not comfortable with," said Conservative Sen. Bob Runciman, who sponsored the controversial Bill C-51 national security legislation in the upper chamber in May.(…) Requiring government to review all appeals by Canadians whose names are on the no-fly list as potential threats to commercial aviation. Currently, names on the no-fly list have to be reviewed by the **public safety minister** every 90 days. A named individual can apply to the minister to have their name removed. But the minister is not required to reply and, after 90 days, is deemed to have rejected the application. The named individual can appeal to the Federal Court. Postmedia Network (Ottawa Citizen)

Stephen Harper démissionnera en tant que chef du Parti conservateur
Le chef conservateur, qui a déclenché les élections fédérales en août dernier, a donc perdu son pari lundi de remporter un quatrième mandat consécutif au pouvoir. Les électeurs ont opté pour le changement incarné par le chef libéral, Justin Trudeau, qui a balayé plusieurs régions au pays et dans la province. (…)Les conservateurs ont remporté les quatre autres circonscriptions qu'ils détenaient, soit celles de Maxime Bernier en Beauce, de **Steven Blaney** (Bellechasse-Les Etchemins-Lévis), de Jacques Gourde (Lévis-Lotbinière) et du candidat Luc Berthold qui a succédé à l'ex-ministre Christian Paradis dans Mégantic-L'Érable. Ils ont aussi gagné dans Portneuf-Jacques-Cartier, Richmond-Arthabaska, Charlebourg-Haute-Saint-Charles, Beauport-Limoilou et Louis-Saint-Laurent. QMI Agency (Journal de Quebec)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Government announces flood funding
The Alberta government will spend $297 million to build a new reservoir west of Calgary in hopes of preventing a repeat of one of the worst floods in Canadian history. About 120,000 were affected after heavy rains hammered southern Alberta in June 2013. The deluge wiped out roads and bridges and swamped streets, homes, and vehicles. The Springbank Off-Stream Reservoir will provide protection for communities along the Elbow River, including Calgary. "The floods of June 2013 were the largest natural disaster in Alberta's history by almost every measure - the extent of the damage, the number of people affected and the financial cost," Alberta Environment Minister Shannon Phillips said at a Calgary news conference Monday. "We cannot let a disaster of this magnitude happen again." Red Deer Advocate, A3

Tour boat 'must have got swamped by huge wave'
Five British nationals are dead and one person is missing after a whale-watching tour boat sank off Vancouver Island on Sunday afternoon with 27 people on board. Three of the dead were tourists in Canada, while one lived in Ontario and the other in B.C., according to the BC Coroners Service. The victims include four men and one woman between the ages of 18 and 76. "They must have got swamped by a huge wave and it flipped their boat completely," said Alec Dick, one of the first to reach the stricken vessel. "I don't think they had time to do anything. Whatever happened, happened so quick." An official with the Joint Rescue Coordination Centre said 21 people were rescued before the search was called offlate Sunday night. Mounties have taken charge of the search for the one remaining missing passenger, and RCMP crews, along with coast guard and local search and rescue workers, were all out on the water Monday. Postmedia Network (Ottawa Citizen, C1)

Trouble came suddenly for capsizing Leviathan II
The Leviathan II was rolling with the steady swell coming in from the open Pacific when the 27 people on a whale-watching trip from Tofino suddenly realized they were in trouble. Instead of riding up the face of the next wave, the 20-metre boat, with a high, open viewing platform on the upper deck, just flipped over. And investigators and the company don't know why. Five Britons - three tourists and two residents of Canada - died and a sixth person, a 27year-old Australian, was missing after the tour boat operated by Jamie's Whaling Station went down near Plover Reefs, in a rugged wilderness area on the west coast of Vancouver Island. The Sydney man's family said he was on the boat with his girlfriend and her family when it sank, the Australian Associated Press reported. His girlfriend's father was among the five British citizens confirmed dead, it said. It happened so fast there was no time for a mayday call, said officials with Jamie's Whaling Station, who held a news conference Monday afternoon to express their dismay. Globe and Mail, A1

*** 5 Britons killed on whale watching tour**
Five British nationals are dead and one person is missing after a whale-watching tour boat sank off Vancouver Island on Sunday afternoon with 27 people on board. Three of the dead were tourists in Canada, while one lived in Ontario and the other in B.C., according to the BC Coroners Service. The victims include four men and one woman between the ages of 18 and 76. An official with the Joint Rescue Co-ordination Centre said 21 people were rescued before the search was called off late Sunday night. Mounties have taken charge of the search for the one remaining missing passenger, and RCMP crews, along with coast guard and local search and rescue workers, were all out on the water Monday. National Post, A2 (Calgary Herald, Montreal Gazette, StarPhoenix); Vancouver Sun; Times Colonist; Times Colonist; Leader-Post

*** Springbank the 'least-worst' option**
As the province unveiled its plans for flood mitigation on the Elbow River, scientists and environmentalists called the Springbank reservoir the "least-worst" option to protect Calgary. On Monday, the province committed $297 million for a dry dam at Springbank rather than one that was proposed further upstream at McLean Creek. Environment Minister Shannon Phillips said Springbank was chosen for several reasons: lower cost, a shorter timeline to build and fewer environmental impacts. Although scientists and

environmentalists were pleased the province rejected the McLean Creek dam, most said they would have preferred to see the province focus on fixing the river's headwaters upstream of the city rather than building any engineering solutions. Calgary Herald, A3; National Post; Edmonton Sun (Calgary Sun)

*** 80-year-old wreck poses pollution threat**
Authorities continue to monitor a suspected solvent leak in Lake Erie from a barge that sank nearly 80 years ago and a local environmentalist said its contents could have a significant negative impact. Last week, divers were exploring the wreck of the Argo - a tanker barge that sank during a storm in 1937 carrying 4,800 barrels of benzol, a buoyant petroleum distillate, and crude oil - when they noticed an unknown substance that smelled strongly of solvents and reported the discharge to the U.S. Coast Guard. Derek Coronado, co-ordinator of the Citizens Environmental Alliance, said the worst-case scenario is that the oil begins leaking from the barge. Canadian Coast Guard spokeswoman Carol Launderville said both the Coast Guard and Transport Canada are "closely monitoring the situation and are in frequent contact with the (U.S. Coast Guard) on this issue. Windsor Star, A10

*** Body of missing hiker, 49, found near Pemberton**
Search and rescue teams found the body of 49-year-old hiker Michael Charles Low in a crevasse Sunday, Whistler Pemberton RCMP said. Because it was getting dark, recovery of the body was left until Monday, Staff-Sgt. Steve LeClair said. Times Colonist, A10

*** SEARCH CONTINUES**
Search and rescue crews were out on the Yukon River on Friday afternoon, looking for 25-year-old Jeremy Scurvey. The man was first reported missing on Oct. 10. He was last seen in the waters of the Yukon River at the end of Lambert Street. Whitehorse Daily Star, 3

*** Rétablir les faits**
Le choix du thème de la sécurité apparaissait comme une nécessité pour la SODES et les Armateurs du Saint-Laurent, afin de « remettre les pendules à l'heure » et de s'assurer que l'information qui parvient aux représentants de la population au Parlement soit juste et vérifiée. « Il y a un questionnement [sur la sécurité dans les transports] excessivement présent dans la population, dans les municipalités, surtout depuis [la tragédie ferroviaire de] Lac-Mégantic », indique Nicole Trépanier, PDG de la SODES. « C'est un questionnement qui est sain et fondé, mais il y a des faussetés qui se propagent [...] Il y a une tendance à laisser entendre qu'on fait n'importe quoi, n'importe comment », déplore Mme Trépanier, qui insiste sur l'importance de « rétablir les faits ». Le Quotidien, 16

*** New insurance coverage available for weather damage**
Insurance companies are starting to offer additional coverage for severe weather-related property damage. Gordon Murray, Aviva's Atlantic business development vice-president, said it's the first insurance company to offer what it calls 'overland water coverage.' This would cover things such as runoff from snow to heavy rains that result in water-filled basements. The company worked with flood-mapping experts to find 15 risk zones in each province, which can be obtained through an insurance broker, he said. More than 90 per cent of New Brunswick homes fall into zones considered low- to medium-risk. This coverage, he said, is meant for areas that typically don't flood. Flood-prone areas would be excluded from coverage. He said consumers in low- to medium-risk areas will have to weigh the risks of overland water damage created by future severe weather events. Daily Gleaner, A8

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Senate could balk at changes to terrorism law, Tories warn
Liberal government changes to the Conservatives' incendiary antiterrorism law could face a bumpy trip through the Conservativecontrolled Senate. "There may be some things that Mr. Trudeau and some of his colleagues are very supportive of, but they may be matters that an overwhelming majority of Canadians are not comfortable with," said Conservative Sen. Bob Runciman. The senator sponsored the controversial Bill C-51 national security legislation in the upper chamber in May. Overhauling C-51, known as the Anti-terrorism Act of 2015, was a key Liberal pledge when party leader Justin Trudeau and his

caucus voted in support of the Conservative bill in the House in the spring. Now that the Liberals will form government, sources say preliminary drafting of the changes is underway and that these will be tabled early in the new parliamentary session, in concert with public consultations. Other Conservative senators said the Liberal national security legislation will be given the same respect accorded any government legislation, especially from a majority government. "Our position will be reasonable, common sense and in good faith and not on an ideological position," Conservative Senate Leader Claude Carignan said. "We have seen the results of the election and we will play our role as senators and will study very seriously all legislation and we will decide," Carignan said. But he added that final acceptance "depends on the results of our study." Postmedia News (Ottawa Citizen, A1)

Fighter jet politics
Given his busy schedule the past two months, you can forgive prime minister-designate Justin Trudeau for not having had the time to watch the first episode of season 5 of Homeland, the intense television drama about the CIA and the realities of terrorism. He probably also has not had a chance to read Yale University historian Timothy Snyder's new book, Black Earth: The Holocaust as History and Warning. Both should be on his to-do list before he carries through with his decision to withdraw Canadian fighter jets from the mission against the Islamic State. (...)Two months later, during the debate in the House of Commons on extending and expanding the anti-ISIL mission into Syria, Trudeau asserted that "we are all committed to keeping Canadians safe." He argued, as he still does, that Canada "does have a role to play in responding to humanitarian crises and security threats in the world" and "that when we deploy the Canadian Forces - especially into combat operations - there must be a clear mission and a clear role for Canada." Postmedia Network (National Post, A8)

* **C-51, TPP Top List of 'Real Change' Tech Priorities**
Digital policies may not have played a significant role in the just-concluded national election, but the arrival of a majority Liberal government will leave many expecting "real change" on the digital front in the years ahead. Prime Minister-designate Justin Trudeau is likely to focus on key economic promises from his platform once Parliament resumes. However, there will be several digital issues that should command attention during his first 12 months in office. Bill C-51The Liberals voted for the controversial anti-terror law, but the party promised changes to it if elected. In particular, it pledged to establish an all-party review mechanism similar to those found in many other countries that will bring Members of Parliament into the oversight process. TheTyee

* **Des dons de 48 M$ à des groupes islamistes radicaux**
L'organisation Health Partners International of Canada/ Partenaires Canadiens pour la Santé Internationale (HPIC), dont le siège social est à Montréal, aurait fait des dons totalisant près de 48 millions $ à groupes islamistes radicaux, selon des documents obtenus par TVA Nouvelles. L'organisation distribue de l'aide médicale aux pays dans le besoin et lors de crises. Elle se prépare à envoyer de l'aide au Pakistan, qui vient à nouveau d'être ébranlé par un tremblement de terre de forte magnitude, qui a fait plus de 200 morts. De 2004 à 2009, HPIC a donné plus de 17 M$ en aide à IRFAN, aujourd'hui considérée par le Canada comme une organi sation terroriste. En 2003, Mercy International Canada, liée à Al-Qaida, selon le témoignage d'un agent du Service canadien du renseignement de sécurité, a reçu 1,3 M$. La même année, Mercy a versé 1 M$ à IRFAN et a depuis perdu son statut d'organisme de charité. Journal Montreal

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Doer says he'll soon head home from Washington
It's the end of an era for Canada's most important diplomatic post as Gary Doer confirmed Monday that his longer-than-usual stint as ambassador to the United States is about to conclude. The popular former Manitoba premier said he'll help prepare the transition to a new Liberal government and will leave it to the incoming government to pick the specific departure date. (...)The former NDP premier of Manitoba was appointed by Stephen Harper in the hope that his left-of-centre roots and social network might help relations with the then-rookie Obama administration. Much of the media chatter in the last six years has focused on one irritant: the stalled Keystone XL pipeline, which both Harper and Doer have advocated

without success so far. But the era also witnessed a series of major Canadian priorities coming to fruition, including: A sweeping arrangement that would change the way Canadians and Americans cross the border, creating customs points away from the border with the goal of faster crossings.. Canada's entry into the Trans-Pacific Partnership trade negotiations, which happened after considerable lobbying of U.S. politicians and stakeholders. An agreement on a new Detroit-Windsor bridge that bypassed a blockage in the U.S. Congress. Canada will finance the bridge, and also collect tolls on what will become the most important border crossing. Canadian Press (Vancouver Sun, B2, Calgary Herald, Ottawa Sun, London Free Press, Calgary Sun, Winnipeg Sun, Toronto Sun, Edmonton Sun), Canadian Press (Edmonton Sun, Ottawa Citizen, Times Colonist, The Telegram, The Guardian), Presse canadienne (Le Nouvelliste, Acadie nouvelle)

*** Lower loonie hurting cross-border flying, say U.S. airports**

The weak Canadian dollar isn't just hurting cross-border shopping. U.S. airports that enjoyed a surge in the number of Canadian passenger levels when the loonie was valued higher than the American dollar are now seeing the flip side of currency swings. Low ticket prices drew about five million Canadians annually in recent years to fly out of U.S. airports. But the Burlington International Airport in Vermont estimates the number of Montreal passengers is down about 10 per cent so far this year. (...)The number of Canadians travelling south fell by five per cent again in August, marking the 11th monthly decrease in a year. Stateside travelling is 26 per cent lower than a year ago, according to Statistics Canada. Same-day car trips are off 34 per cent while total car trips are down 24 per cent. (...)Canada's airline sector has long called upon Ottawa to lower airport rents, fees and taxes to stem the flow of passengers crossing the border to catch flights. Canadian Press (CTV News, Blackburn News, Cape Breton Post, Daily Courier, Lethbridge Herald, Leader-Post, StarPhoenix, The Province, Montreal Gazette, Chronicle-Journal, Canadian Business, Times Colonist)

Sneaky snowbirds could have financial wings clipped by new security program

Snowbirds beware: The federal government will use its planned border exit-tracking system to avoid paying hundreds of millions of dollars in social benefits now going to people who shouldn't receive them due to absences from Canada. Newly obtained memos say the Canada Revenue Agency and Employment and Social Development Canada expect to save between about $194 million and $319 million over five years once the long-anticipated system is fully in place. Federal officials have been working quietly to satisfy privacy commissioner Daniel Therrien's office that personal information will be properly collected, used and disclosed under the program. Under the 2011 perimeter security pact, Canada and the United States agreed to set up co-ordinated systems to track entry and exit information from travellers. For the moment, the tracking system involves exchanging entry information collected from people at the land border so that data on entry to one country serves as a record of exit from the other. The first two phases of the program have been limited to foreign nationals and permanent residents of Canada and the United States, but not citizens of either country.(...) The initiative's scope prompted the federal privacy commissioner's office to express concern it had expanded "beyond its initial parameters," says one memo. But Canada Border Services Agency officials felt the objectives were "entirely consistent" with the perimeter security pact's commitment, the memo adds. Canadian Press (The Guardian, The Telegram, Daily Courier)

The truth about Brandon's mystery woman uncovered

A mystery woman who lied when she told police she'd been abducted as a child, forced to work in the sex trade and didn't know her true identity has been fined and put on probation for the elaborate story. Before authorities learned the truth - that she'd actually fled Ontario with her daughter in the midst of a custody dispute - the investigation into their identities involved at least four police agencies, the Canada Border Services Agency, Child and Family Services, the Canadian Centre for Child Protection and the Department of Homeland Security in the United States. "This is a highly unusual case," Crown attorney Marnie Evans said in Brandon provincial court on Monday just before the woman was fined $2,000 and put on probation for two years. "It essentially involves a very lengthy investigation which criss-crossed this country and down into the States." The woman can't be named due to a publication ban put in place during Monday's hearing to protect the identity of her daughter who remains in the care of child welfare authorities. Winnipeg Free Press

Belgian leaders tout benefits of EU ties to Canada
Belgium's western Canadian trade mission made an attractive pitch Monday to be Canada's entry point for European free trade, at least for a couple of Vancouver businesses. "I think there are a lot of opportunities (with Canada/European Union free trade) as long as we play nicely together," said Kerry Gibson, president of Vancouverbased EcoCentury Technologies. "That's what I'm doing here (at a morning seminar), checking them out," she said. Selling western Canadian businesses on the idea of using Belgium as a gateway to Europe under the Comprehensive Economic and Trade Agreement, which is expected to be in force as early as 2017, is a significant sub-theme of the Belgian trade mission, which stopped in Vancouver Monday with its delegation of 228, which is being led by royalty. (…)Upon implementation, CETA will mean the elimination of tariffs on more than 90 per cent of goods traded between Canada and the EU zone, as well as the streamlining of many licensing and regulatory regimes (with some exceptions). Vancouver Sun, D2

Hot summer for tourism in Montreal
It was a hot summer for tourism in Montreal. Numbers were up across the board compared to last year, according to Tourisme Montréal. The agency attributed the boost to major events, festivals and attractions, economic conditions and marketing initiatives. Ève Paré, CEO of the Hotel Association of Greater Montreal, said it was a good summer, but not the best ever. (…)Here are some numbers tallied by Tourisme Montréal for June to August or September: 9.8 per cent more American tourists crossed the border. 12.5 per cent more tourists arrived by car. 4.4 per cent more passengers arrived at Dorval airport. Montreal Gazette, B2, Journal de Montréal (Journal de Québec)

Why we shouldn't put provinces in the corner
We think about North America as three sovereign democracies. It's true. But all three nations are also federations, sharing constitutional power with 95 states, provinces and territories. Later this week, Colorado Governor John Hickenlooper will host the first-ever summit of North American governors and premiers in Colorado Springs. Mexican governors will have the best attendance, reflecting that, for now, Mexico is the most enthusiastic about North American collaboration. Yukon Premier Darrell Pasloski and Ambassador Gary Doer will lead the Canadians. (…)As Manitoba premier, Gary Doer included U.S. and Mexican governors at a 2006 Gimli Western Premiers Conference. They joined in the ultimately successful push to use "smart" drivers' licences for cross-border travel. Globe and Mail

Always too soon for a celebratory spliff
An opinion piece states, "I will bet you a sack of weed that Justin Trudeau will not deliver before the next election on his promise to legalize marijuana. This being Canada, we can't just delete marijuana offences from the Criminal Code. That would be too easy. (…)In spite of what some states have done, marijuana remains highly illegal under U.S. federal law, which applies at border crossings. People and products entering the U.S. from Canada would have to be inspected with increased thoroughness, frequency and possibly rubber gloves. Lineups at the Windsor crossing could stretch all the way to back to Toronto. Exports to the U.S. that so many Canadians rely on for their daily bread will be held up for days or weeks." StarPhoenix, A3

*** U.S. Increasing Cross-Border Fees for Some Shipments**
The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS) announced it will publish its final rule on Oct. 29 that adjusts the fees the U.S. government charges to recoup the costs of conducting agricultural quarantine inspections (AQI) at U.S. ports of entry for all modes of transportation and many in Canadian trucking are speaking out against the move. According to the Ontario Trucking Association (OTA), the changes take effect on Dec. 28. In the case of trucking, the fees are applied whether or not a truck crossing the border is carrying agricultural products. The USDA argues the fee adjustment, which it says was subject to an evaluation by "a well-respected" accounting firm, is necessary to align the actual cost of providing the services with what the U.S. government charges. In making its announcement, the USDA also said the "AQI fee adjustments are consistent with the United States' international trade obligations" despite concerns to the contrary from both the Canadian Trucking Alliance (CTA) and the Canadian government. (…)The adjustments to the APHIS fee increases are of little consolation to the trucking industry, according to the president and CEO of the Canadian Trucking Alliance, a federation of the provincial trucking associations representing over 4,500

trucking companies. “This is a cash grab and a tax on trade,” said David Bradley. “We’re still looking at increases of 44 percent for non-transponder trucks and 187 percent for trucks with transponders. That is absurd and a complete contradiction of the principles of the U.S.-Canada Beyond the Border Accord.” Today’s Trucking (2015-10-26)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** CSIS spam scam returns**
T here’s a phone scam trying to convince unsuspecting people that Canada’s spy agency has discovered their computers are being used to pump out spam. I know because I got a call Monday from one of the gang. ITWorldCanada.com

*** SecTor 2015: IT pros — Canada’s spooks want you**
Among the trade show booths at this week’s SecTor security conference in Toronto was one for an organization that hadn’t appeared at previous IT or security shows in the area before: The Canadian Security Intelligence Service (CSIS). Usually recruiting at job fairs and universities, the spy agency sent four staffers (two of them literally men in black) plus a media spokesman to this year’s show to make a pitch for those with infosec skills. According to the agency’s Web site, right now it wants an applications analyst/developer, IT analysts, a programmer analyst, a security assessment analyst and a systems analyst. ITWorldCanada.com

*** NSA warns of growing danger of cyber-attack by nation states**
The deputy director of the US National Security Agency (NSA), Richard Ledgett, has warned of the increasing danger of destructive cyber attacks by states. He told the BBC: "If you are connected to the internet, you are vulnerable to determined nation-state attackers." He said nations would need to identify red lines that should not be crossed. He also said agency targets, numbered in "the high hundreds", had discussed leaks by contractor Edward Snowden, with some changing their behaviour. BBC.com

LAW ENFORCEMENT / APPLICATION DE LA LOI

Email bungle frustrates privacy watchdog
A major failure within the B.C. government's email system left up to 48,000 email accounts without a proper backup, potentially losing thousands of messages and frustrating a recent probe by the privacy commissioner into a deletedemail scandal. The government forgot to turn on automatic monthly backups for its email accounts after it migrated to a new Microsoft Exchange server in June 2014. As a result, up to 48,000 email accounts weren't backed up, as per government policy, until the error was discovered Feb. 5. It was a "serious oversight" of a backup system that's supposed to be used for serious internal government investigations, said Information and Privacy Commissioner Elizabeth Denham in a report this week. "Data has been permanently lost that may be needed for myriad investigative purposes, ranging from financial management matters to employee investigations," Denham wrote. As well, the lack of backup emails hindered Denham's probe into an aide within Transportation Minister Todd Stone's office who was accused of improperly deleting emails related to the Highway of Tears so that they would not become public through a Freedom of Information request. Denham's investigators weren't able to restore the emails from the backup, and so had to resort to other less precise forensic techniques. "It would have assisted this investigation," Denham wrote. Nonetheless, the staffer, George Gretes, resigned from government and is now under RCMP investigation for allegedly lying under oath to Denham's staff. Postmedia Network (Vancouver Sun, A6)

'You can't terrorize your son,' child psychologist told father charged with abuse
An Ottawa man accused of horrific abuse, including starvation and assault, of his son told a child psychologist in 2010 that he feared the boy, just eight-years old at the time, would grow up to be a sexual predator. But child psychologist Xavier Plaus testified on Monday that there were absolutely no signs of it, that the boy was bright, and that his father - then an RCMP anti-terrorism officer - was obsessed with

punishing his son for what he believed was abnormal sexual behaviour. The behaviour, in fact, amounted to nothing more than innocently hugging teachers and, in some cases, fellow students who had been bullied at school. Plaus testified that the boy was extremely intelligent, even though he was living in a chaotic, hostile and poisonous environment. The psychologist said the boy's father interrogated his son about his daily school routine and that even after a battery of tests showing otherwise, he could not persuade the man that the boy showed "absolutely no evidence of sexual pre-occupation." He said the father insisted the boy was manipulating him and telling him what he wanted to hear. During one of several visits to the boy's home, the psychologist said, the father said he punished his son by making him sleep in the basement. The psychologist, hired by the father during a custody battle, told court that he became concerned about the boy's punishments - including pushups and cold showers - and said that if it happened again he'd call child-protection workers. "You can't terrorize your son," the psychologist recalled telling the man in 2010. "The parents saw him as a delinquent. I did not," Plaus told court. The psychologist said he interviewed the boy 14 times and concluded that after years of chaos, conflict and hostility at home, the boy had given up on any expectation that anyone in the world would love him. Three years later, in 2013 and after the punishments intensified, the boy escaped the Kanata basement. Now 13, he has detailed horrifying abuse, including starvation and torture, and told the court he thought he was going to die the day his father pointed his service weapon at his head. The boy's hands were often cuffed behind his back and he was kept naked, and chained to a post in the basement while the rest of his family went about their daily routine upstairs. He recalled that his father once left him with a full jar of peanut butter and some pita bread. "He said, 'This should last you weeks.' " The father, since suspended from the RCMP, has confessed to chaining up his son in the suburban basement, torturing him with a barbecue lighter, and rationing his meals. The boy weighed only 50 pounds when he escaped after slipping out of his shackles. Postmedia News (Ottawa Citizen) (2015-10-26); Le Droit, 7 (2015-10-27)

Concerns raised about CSIS accountability

Internal government notes say the Canadian Security Intelligence Service is likely to team up with "trusted allies," such as the American CIA and Britain's MI6, on overseas operations to derail threats - plans that underscore concerns about CSIS accountability under new security legislation. The omnibus bill known as C-51 allows CSIS to engage in joint "disruption" efforts abroad - including covert actions that break foreign laws - something the spy service previously had no authority to do, according to the government notes. "In the international context, CSIS would likely first seek avenues to work jointly with partners in the local jurisdiction or trusted allies before engaging in independent action," the notes say. "In the past, CSIS has been invited to participate in joint operations abroad to disrupt threats or to provide assistance to allies, but has had no mandate to do so." CSIS's new threat-disruption mandate - perhaps the most contentious element of the legislation that received royal assent in June - could include surreptitious meddling with websites, cancelling airline reservations, disabling a car or myriad other schemes. The spy service would be allowed to engage in disruption activities that violate the Charter of Rights and Freedoms so long as a judge sanctions them, a measure critics say perverts the role of the judiciary. CSIS would co-ordinate threat disruption activity with other agencies such as the RCMP, Canada Border Services Agency and Foreign Affairs, and could use its statutory mandate to enlist the technical expertise of the Communications Security Establishment, Canada's electronic spy agency, the government notes say. Canadian Press (Times Colonist, B5)

RCMP officer charged with sexual assault

A Buffalo Narrows RCMP officer is suspended with pay while facing a sexual assault allegation. RCMP said while the charge is concerning, the officer will get no special treatment as his case moves through the courts. In a news release on Monday, RCMP said the charge was laid against Const. Randy McKay on Oct. 21, in connection with an incident inside a private home in Dillon on May 20. Staff Sgt. Ted Munro, with the North District Management Team, said the complaint was made by an adult woman through "internal channels." While she is not a member of the RCMP, she and McKay are known to each other, Munro said. An internal investigation into the incident is underway, while the criminal investigation has been brought before the courts, he said. "It's just like any other Criminal Code investigation with the general public. That will go before the courts and it will be dealt with and deemed just like any other situation. There's no specialized treatment for any type of police or people within the government." He said McKay was not on duty at the time of the incident. The police force is taking the situation seriously,

and RCMP are working to conclude the matter "as quick as possible," he added. Postmedia News (Leader-Post, A2, StarPhoenix, A4); Radio-Canada

Stolen RCMP gun used to shoot teen
Two men are in custody after a Winnipeg teen was shot with a gun allegedly stolen from an off -duty RCMP officer. Deputy Winnipeg police chief Danny Smyth said investigators believe the gun was stolen Friday evening from a marked RCMP vehicle parked outside the officer's home. "The officer's equipment belt including his firearm had been secured in the vehicle," Smyth said Monday. "Police believe the two accused unlawfully entered the vehicle and stole several items including the firearm from the off -duty officer." Just after midnight later that night, the two suspects exchanged words with a group of young people sitting in a vehicle in a convenience store parking lot. Smyth said one of the suspects allegedly approached the car with a gun and took aim at those inside. A 16-year-old girl was shot once in the upper body and rushed to hospital in critical condition. The shooting was "senseless and reckless" without apparent motive, Smyth said. Canadian Press (Edmonton Sun, 36) National Post, A5, Daily Gleaner, B2, Red Deer Advocate, A6); * La Presse Canadienne (Acadie Nouvelle, 18); * Winnipeg Free Press, A3

*** Mountie given conditional discharge in forgery case**
A Mountie who pleaded guilty to forgery will have a clean record if he follows the conditions of a four-month probation period. On Monday, Const. Jonathan Cormier, 36, of Moncton, was given a conditional discharge in Moncton provincial court for posing as a Crown prosecutor in an email. The forgery was discovered when he inadvertently sent the email to the prosecutor he was impersonating. In making his decision Judge Joseph Michaud reviewed several letters attesting to Cormier's character, performance logs and a psychologist's report. These document showed "without a doubt" that Cormier was a man of "exemplary character," Michaud said, in both his professional and private life. They also showed that at the time of the offence the constable was under severe stress and fatigue because of the events of June 4, 2014, in which three Codiac RCMP officers, his colleagues, were killed. The judge reviewed several examples of case law in which members of the judicial system were given discharges. He said he was convinced giving Cormier a discharge was in the best interest of the accused and not contrary to public interest. Cormier will be on probation for four months, and during that time must donate $1,000 to the Friends of The Moncton Hospital Foundation and continues sessions with a psychologist. The Mountie became emotional when the decision was announced, and after was comforted by friends and family who attended the court appearance. Cormier has been a Mountie for seven years. He was suspended when the RCMP learned of the incident. His defence lawyer Bruce Phillips previously told the court Cormier still has an internal RCMP review pending because of his actions. The Crown, Francois Godin, a Quebec prosecutor brought to Moncton for the officer's case, added that it has not yet been decided if the constable will lose his job. Times & Transcript, A3

*** Mounties hunt prisoner who escaped in cruiser**
Alberta Mounties are searching for a prisoner who escaped by fleeing in a marked cruiser. Police say Jason McGinn, 26, jumped into the driver's seat of a cruiser Monday morning near Thorsby as he was being transferred to the Drayton Valley RCMP. McGinn had been taken into custody Sunday for allegedly being in possession of a stolen vehicle. The RCMP cruiser was found abandoned near Warburg. Police say nothing was taken from the police car. McGinn is white, about 5-foot-10 with dark brown hair, green eyes, a missing tooth and a recent scratch on his face. Canadian Press (Calgary Herald, A7, Red Deer Advocate, A3); Edmonton Sun, 6; Postmedia Network (Edmonton Journal, A2)

Le nombre d'incidents explose
Ils font pester les pilotes, inquiètent les autorités et se jouent de la police. Les individus qui s'amusent à braquer des pointeurs laser sur des avions sont de plus en plus nombreux. Et leurs gestes, potentiellement très dangereux, sont dans la ligne de mire de Transports Canada. Lumière sur un phénomène en pleine explosion. Le 23 septembre 2014. Un Boeing 737 de WestJet en provenance de Vancouver entame son approche pour un atterrissage à l'aéroport d'Ottawa. Soudain, les deux pilotes se retrouvent aveuglés par une intense lumière verte. Quelqu'un, au sol, vient de braquer un laser vers la cabine de pilotage. Les pilotes parviennent à faire atterrir l'avion rempli de passagers. Mais l'un d'eux se plaint d'une sensation de brûlure à l'oeil gauche. Les deux hommes seront admis à l'hôpital. «Par chance,

aucun de nos pilotes n'a subi de dommages sérieux aux yeux, indique le directeur des relations publiques chez WestJet, Robert Palmer. Mais c'est très risqué.» Cet incident est loin d'être unique. Une compilation effectuée par La Presse à partir d'une base de données du ministère des Transports montre que les cas de ce qu'on appelle le «brouillage laser» sont en pleine explosion au pays. En 2002, Transports Canada n'avait signalé qu'un cas de brouillage laser. L'an dernier, le Ministère en avait recensé 502 au pays. Cette année, en date du 20 octobre, déjà 524 incidents avaient été signalés. L'année en cours a déjà fracassé un record et, si l'on se fie à la tendance, au moins une centaine d'incidents devraient s'ajouter d'ici la fin de l'année. Ce type d'incident se produit maintenant près de deux fois par jour à l'échelle du pays. Et selon des gens de l'industrie consultés par La Presse, le nombre de cas réels pourrait être encore plus élevé, les pilotes choisissant parfois de ne pas rapporter les cas afin d'éviter d'avoir à remplir des rapports d'incident. Avec l'Ontario, le Québec est la province la plus touchée... La police est presque systématiquement avisée en cas d'attaque laser. «Ou bien le pilote nous donne des coordonnées GPS, ou il nous donne un endroit d'où il croit que l'attaque provient. Nous envoyons toujours une autopatrouille», explique Marie-Claude Dandenault. Ailleurs au pays, la Gendarmerie royale du Canada envoie même des hélicoptères pour repérer les délinquants. La Presse, A2/Front

*** «Pas brillant comme idée»**

Est-ce qu'un avion pourrait un jour s'écraser à cause d'un brouillage laser? «Si ça arrive dans un moment très critique, très près du sol, ça pourrait sérieusement nuire au pilote et, tout dépendant de ce qui se passe, ça pourrait certainement causer un problème», répond le capitaine Joe DePete, premier vice-président de l'ALPA, qui rappelle toutefois que le transport aérien est le mode de transport le plus sûr et que les pilotes sont entraînés à faire face à ce type d'incidents. Devant l'ampleur du problème, Transports Canada a lancé en juin dernier une campagne de sensibilisation pour le grand public intitulée « Pointer un laser vers un aéronef, pas brillant comme idée ». Pour l'instant, cependant, les chiffres montrent qu'elle n'a pas réussi à freiner le phénomène. Mais qui sont ces individus qui s'amusent à braquer des lasers sur des avions? «Mon impression est qu'une grande partie des gens qui font ça ne sont pas conscients des dangers que ça implique», répond Marie-Claude Dandenault, commandante de l'unité aéroportuaire du Service de police de la Ville de Montréal. Les données compilées par La Presse montrent que les incidents se produisent surtout l'été, et souvent la fin de semaine, au petit matin. La police est presque systématiquement avisée en cas d'attaque laser. «Ou bien le pilote nous donne des coordonnées GPS, ou il nous donne un endroit d'où il croit que l'attaque provient. Nous envoyons toujours une autopatrouille», explique Marie-Claude Dandenault. Ailleurs au pays, la Gendarmerie royale du Canada envoie même des hélicoptères pour repérer les délinquants. La Presse (Le Nouvelliste, 33)

Murder suspect detained in New Brunswick extradited to the U.S.

A North Carolina man has been returned home in custody following his extradition from New Brunswick on charges he fatally shot his uncle in the southern U.S. state in April. James Daniel Ball, 34, was delivered by U.S. marshals from New Brunswick to Raleigh, N.C., last week. From there, Camden sheriff's deputies and State Bureau of Investigation agents transported him to the Camden Sheriff's Office, Sheriff Tony Perry said in a statement Friday. Ball, from Manteo, N.C., is charged with murdering his uncle, 65-year-old William Ball in his home in Shiloh, N.C. After William Ball was found dead April 22, his nephew, who had been staying with him, reported his uncle's death as a suicide, according court documentation filed in New Brunswick in support of James Ball's arrest. Authorities determined that William Ball died from a gunshot wound to the head. After investigators concluded William Ball was the victim of a homicide, U.S. authorities alerted Canadian officials a murder warrant had been issued for James Ball's arrest in Camden and that he might be headed to Canada. The suspect's parents live in Miramichi. The RCMP arrested Ball at the port of entry just across from where Interstate 95 ends at the U.S. and Canadian border near Woodstock. Ball was initially released after Canadian police learned they had no authority to arrest him based on the Camden warrant. Canadian police contacted Ball's parents, who were staying at a hotel on the Canadian side of the border, and he was allowed to stay with them following his release. Daily Gleaner, A8

ASIRT investigating after prisoner dies in police custody in Edmonton

An investigation has been launched after a 46-year-old prisoner died in police custody on Monday. Police say six prisoners from an Edmonton Police Service (EPS) cell block were being transported to the Edmonton Remand Centre at 11:52 a.m. Monday. One of the six prisoners was yelling and kicking while

being placed into the prisoner transport van, said police, but while en route, the man suddenly became silent. The officers stopped the van to check on the prisoner, said police, and discovered he was unresponsive and in medical distress. The officers began performing CPR on the prisoner while EMS crews were dispatched. The prisoner was transported by EMS to hospital, where he died. The Director of Law Enforcement has directed the Alberta Serious Incident Response Team (ASIRT) to investigate. The investigation is said to be in its very early stages, and no further information is being released at this time. This isn't the first time a person died in police custody this year. In April, a 25-year-old man died after being arrested by city police at City Centre Mall. ASIRT said police had taken custody of the man and transported him to EPS headquarters, but as they entered the building, the man went into medical distress and became unresponsive. The man was taken by ambulance to hospital where he died. Results of the ASIRT investigation into the case have not been released. Edmonton Sun (2015-10-26)

*** Naufrage à Tofino**
Des plongeurs de la Gendarmerie canadienne sont arrivés lundi à **Tofino**, sur la côte pacifique, pour rechercher le dernier passager disparu lors du naufrage d'un navire de tourisme, au cours duquel cinq Britanniques sont décédés. Cette équipe spécialisée est arrivée lundi matin au port de cette localité prisée des surfeurs, située à l'ouest de l'île de Vancouver, et a repris les recherches. " Nous gardons espoir [de retrouver vivant le passager disparu], mais nous devons nous préparer au pire ", a déclaré Janelle Shoihet, caporale de la Gendarmerie royale canadienne (GRC). A Londres, le ministère des Affaires étrangères avait annoncé plus tôt que les cinq personnes mortes dans le naufrage de ce bateau d'observation de cétacés étaient de nationalité britannique. Il s'agit de quatre hommes et d'une femme, âgés de 18 à 76 ans, ont précisé les services médico-légaux de la province de Colombie-Britannique. Deux d'entre eux résidaient au Canada, les trois autres au Royaume-Uni, et tous les cinq étaient sur le bateau en tant que touristes. La Presse Canadienne (Le Devoir, A5)

*** RCMP issues Canada-wide warrant for suspect in Sexsmith stabbing spree**
Mounties have issued a Canada-wide warrant for a suspect in a stabbing spree that left one dead and three hospitalized in Sexsmith. Four adults were stabbed, one fatally at the Alamo bar in downtown Sexsmith around 1:13 a.m. on Sunday. One adult was taken to hospital by STARS air ambulance and the other three were taken to hospital by ground ambulance. Jordan Joseph Wendland is wanted by RCMP for one count of second degree murder and three counts of aggravated assault Edmonton Sun; Edmonton Journal; CBC News (2015-10-26)

***Suspicious package causes evacuation**
New Glasgow Regional Police evacuated some businesses and apartments after a suspicious package arrived through the mail Monday afternoon. Police gave the all-clear about six hours later when they realized the package contained an illegal drug. The parcel arrived at a business in the Downtown Mini Mall at about 2:20 p.m., said police spokesman Const. Ken MacDonald. A bank, businesses and several neighbouring apartments on Archimedes Street were quickly evacuated. In addition to police, the New Glasgow Fire Department, the Canadian Red Cross and another hazardous response team responded. Apartment residents were relocated to a firehall or with friends and family. The situation continued that way until about 8:10 p.m. MacDonald said the situation changed shortly after the "RCMP chemical, biological, radiological, nuclear, explosive unit" arrived at the scene. "Investigators have secured the scene to be safe and have determined the substance to be a controlled substance: basically an illegal drug." Chronicle Herald, A5

***Nunavut excessive force investigation done; public disclosure pending**
The Ottawa Police Service has completed its external investigation into a case of alleged excessive use of force by Nunavut RCMP officers against a man in Iqaluit police cells last summer. But the details of that investigation, and whether the two officers involved will be disciplined internally, or charged with offences, are still confidential at this point. RCMP Insp. Don Halina said Oct. 26 that the lead RCMP investigator in the case is away and still has to confer with the complainant, Bernard Naulalik, before disclosing the results of the external investigation. That could take a few weeks, Halina said. "We're just working to finalize next steps and part of that is talking to the complainant," Halina said Oct. 26. For several weeks at least, Nunavut RCMP have had the results of an Ottawa Police Service investigation into the conduct of two officers toward Naulalik on July 19, 2014. We have chosen not to publish their names until they have

been disciplined or charged with offences. The alleged assaults against Naulalik made national headlines when *Nunatsiaq News* broke the story in May 2015. According to court documents and lawyers involved, Naulalik had been picked up by police in Iqaluit on three minor infractions July 18, 2015, and found himself in RCMP cells. While there, he had an altercation with two RCMP officers which was captured on closed-circuit video. Nunatsiaq News

***A new crime trend?**
A Charlottetown man is in jail after a violent event at a motel in Stratford Sunday involving a man brandishing a samurai sword. Queens district and Stratford RCMP were called to the Southport Motel just after 5 p.m. on Sunday after two men were reported to be involved in a heated argument. RCMP Const. Dave Ngo says the accused was upset with his daughter's boyfriend and drove to the motel with the sword. "The individual ... threatened to use the samurai sword on the victim, at which point an altercation did occur," Ngo said. The victim managed to take the sword from the 67-year-old alleged offender during the altercation, just before police arrived on scene. The accused man suffered only minor injuries from the incident, thanks in part to the fact the victim successfully prevented the assailant from exiting his vehicle. Frank Trainor, age 67, of Charlottetown, has been charged with assault with a weapon and uttering threats. Curiously, incidents involving samurai swords appear to be on the rise in Stratford. This marks the third use of the swords leading to arrests in the last two years. John Robert Long was sentenced to 30 months in jail for swinging a samurai sword at two RCMP officers in January 2014. In an unrelated incident in October 2013, Stratford RCMP had to Taser a man who rushed officers while swinging two samurai swords. Jonathan Cantelo was banned from possessing weapons for 10 years and served three months in jail after being sentenced in January last year. Guardian, A3

RCMP heroes treated poorly
An opinion piece states ''As the training ground for Canada's national police force since 1885, it's not too much of a stretch to call Regina the spiritual home of the Royal Canadian Mounted Police. Since the days of the RCMP's forerunner, the North-West Mounted Police, all Mounties have begun their career at Depot Division. It's a tradition this province is proud of, and one reason why we are inclined to consider these men and women "our" Mounties, long after they've completed their basic training in Regina. Thus, the force's missteps in recent years have been keenly felt here, particularly the troubling claims of bullying, harassment and even sexual assault of female members across the country that are the subject of a class-action lawsuit by 375 women. These and other complaints from the rank and file - including men - have created the impression of an out-oftouch senior command downplaying the welfare and concerns of the men and women who serve us. RCMP Commissioner Bob Paulson took over the top job four years ago pledging to tackle "the culture of misuse of authority" raising hope a new era of respect and civility would be established. Paulson has done a lot toward that end, but we are puzzled and disappointed that respect seems absent in the treatment of the four brave Mounties who confronted the gunman who attacked Parliament Hill a year ago. After fatally shooting Cpl. Nathan Cirillo as he stood guard at the National War Memorial, his killer ran into the Parliament building. Former sergeant-at-arms Kevin Vickers got most of the praise for helping kill the gunman, and was rewarded by Prime Minister Stephen Harper with a posting to Ireland as Canada's ambassador. But more than a year later, the four Mounties who helped Vickers subdue the gunman - Const. Curtis Barrett, Const. Martin Fraser, Sgt. Rick Rozon and Cpl. Dany Daigle - have still not received the recognition promised them by the RCMP. Paulson said two weeks ago that the awards are still coming, but had been delayed pending a number of reviews of the incident. Really? Vickers was recognized right away, but it takes a year to determine whether the bravery of these officers is worth a medal? Compounding this woeful inaction is the fact the four officers weren't invited to last week's ceremony in Ottawa to mark the one-year anniversary of the attack. CTV reported that since the shooting, one of the officers was even briefly assigned to RCMP car wash duty. While former RCMP deputy commissioner P.Y. Bourduas told CTV that the failure to include the men in the ceremony was a "regrettable oversight," Paulson said he has publicly thanked the officers, and that a ceremony is being planned for the four Mounties to get commendations and bravery awards.'' Postmedia News (StarPhoenix, A6)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Convicted wife killer seeking an early parole
A 76-year-old Calgary man convicted of strangling his commonlaw wife Joanne Kotyk on July 31, 1995, and sentenced to life with no parole for 25 years, is making another attempt at gaining early freedom. Wilfred Oscar Trohan, whose application was stayed last January in his first bid for early parole under the Criminal Code's so-called faint hope clause, again appeared in Court of Queen's Bench on Monday before Chief Justice Nail Wittmann. This time, his lawyer Kim Ross said they are attempting to revive the application. "Correctional Service Canada says we're out of time to apply. There's a 90-day window you have to make your application," Ross said after the brief appearance. "We're trying to revive it." There was some uncertainty when Trohan first applied in June 2014 whether he was aware of legislation introduced in 2011 that gave prisoners serving a life sentence a 90-day window to file the application to have parole ineligibility reduced once they have served 15 years and become eligible. Once an application is made, Correctional Service Canada would produce a report outlining his behaviour while behind bars, which would then appear before a judge to determine its merit. If the offender passes that hurdle, it is put in front of a jury to consider. However Wittmann stayed it at the first stage. Calgary Herald, A8

$10M settlement reached with Malley clients
A settlement topping $10 million has been reached in the class action lawsuit against a financial advisor in jail for the bombing death of a former client. Currently serving a life sentence for a first-degree murder conviction, Brian Andrew Malley, 58, of Innisfail, was also one of the defendants in an $80 million class action lawsuit from his former clients. Malley, his wife Christine and the two companies they administered and directed - Assante Wealth Management and Assante Capital Management, were all the subject of the lawsuit launched in 2012. A recently reached settlement of $10 million is now open for former clients to apply for a share of the money. Red Deer Advocate, A1

* **Cocaine dealer gets full parole**
Sheer greed and gambling fuelled Justin Alexander Corbett's need for quick money and he became a drug dealer. Corbett, 38, was one of three men charged with possession for the purpose of trafficking after police seized 15 kilograms of cocaine from a Dartmouth post office box over two days in August 2007. On Oct. 22, the Parole Board of Canada granted Corbett full parole from his 10-year sentence in federal prison. Upon release, Corbett is permitted to live with a close friend instead of in a halfway house. The parole board has ordered Corbett avoid any establishments where gambling is the primary source of income and not to gamble or associate with other criminals. While previously on full parole in 2011, Corbett returned to the drug trade, was subsequently convicted and received four years consecutive for the new drug trafficking charge. Chronicle-Herald, A6

* **Lawyer slams 'outrageous' Legal Aid denial**
An Edmonton lawyer is bemoaning the state of Legal Aid Alberta after coverage was denied for an appeal of a murder conviction where the Crown was actually conceding. Defence lawyer Deborah Hatch -- who recently argued the successful appeal pro bono -- said Monday she had to go to Alberta's highest court to get an order appointing her as counsel, which was granted last week and now means the Attorney General will have to pay her fees. Hatch says Legal Aid's decision to deny funding for the appeal, based on there being no merit, is "completely outrageous" in the face of the Crown agreeing to the appeal, which led to the murder conviction being quashed. (...)The appeal stemmed from the second-degree murder conviction of Wendy Scott, a 31-year-old woman with an IQ of 50, in the May 2011 killing of Casey Armstrong, 48. The victim was found in the bathtub of his Medicine Hat trailer home with a knife wound to his neck. Scott, who admitted to police she gone to Armstrong's trailer with Connie Oakes, 51, and watched her kill him, pleaded guilty and was a Crown witness against Oakes, who was also sentenced to life in prison after being convicted by a jury of second-degree murder. (...)After quashing the conviction on Oct. 15, the Court of Appeal ordered that a new trial be held for Scott. She is slated to be back in court in Medicine Hat on Nov. 19. Meanwhile, Oakes has also appealed her conviction. Edmonton Sun, 26

* **All charges in fatal shooting of robber have been resolved**
The final chapter has been written in a killing last year near Baden. Eight people were charged after three robbers were shot - one fatally - by the robbery victim's son, Crawford Lamka. The only outstanding charges in the case were withdrawn this summer, court records show. Claude Ouellette, 53, of Kitchener,

had been charged with being an accessory after the fact to manslaughter and unauthorized possession of a firearm. Ouellette was not one of the robbers. Rather, police had alleged he disposed of the handgun used to kill the robber, Henry Jarsch. (…)In October 2014, Lamka was sent to prison for four years after pleading guilty to manslaughter for using excessive force in self-defence. With credit for time already served, today Lamka has two years in custody remaining Lamka was initially charged with second-degree murder and two counts of attempted murder. Defence lawyer Brennan Smart said Lamka, who has a form of autism and an attention-deficit disorder, may have overreacted in part because he found his father badly beaten after an attack with a baseball bat when he was a boy. Waterloo Region Record, B1

*** 'Sleepwatcher' released from prison, will reside in community**
The man many have called the 'Sleepwatcher' has been granted conditional parole, and will reside in the Community Correctional Centre during statutory release. Barry Edward Sinclair, 52, was sentenced to five years in prison in 2013 for breaking into several apartments where young women lived. Sinclair has a lengthy criminal history, dating back 30-years. He has prior convictions for break and enter, sexual assault, indecent exposure and trespassing at night. Parole documents obtained by Global News say most of Sinclair's crimes are a continuation of '"sexually motivated offences," which date back to 1980, and consist of him entering homes of randomly selected females that are believed to be alone or single. The documents also state Sinclair began "sexually deviant behaviour" as a young teenager. The Parole Board of Canada believes Sinclair is a moderate risk to re-offend in general and a high risk to re-offend in a sexual manner given the lack of progress in his correctional plan. Global News (OR-Politics) (2015-10-26)

*** Courts shouldn't make up facts to kill off new laws**
An opinion piece states, "Section 12 of the Canadian Charter of Rights and Freedoms states: "Everyone has the right not to be subjected to any cruel and unusual treatment or punishment." It's hard to argue against this principle. (…) But I expect judges to make the determination using reasonable criteria, based on the facts before the court. However, the Supreme Court of Canada has given our courts the power to make this determination without any regard to the facts before the court. As a result, courts are considering hypothetical or made-up situations that have never occurred and may never occur when deciding on the issue of cruel and unusual punishment. In an April 2015 decision, the SCC struck down the mandatory minimum three-year sentence for illegal gun possession by a vote of 6-3. But it wasn't that the imposition of minimum sentences on the two people in the case was cruel and unusual. They were, in fact, reasonable sentences. However, the imposition of a mandatory three-year sentence would have been cruel and unusual in a far-fetched hypothetical situation, a made-up situation that had never been before the court. So the Supreme Court justices struck down the mandatory minimum sentence law." The Province

*** Canada-wide warrant**
The Repeat Offender Parole Enforcement (ROPE) Squad is requesting the public's assistance in locating a federal offender known to frequent the Cornwall area, who is wanted on a Canada-wide warrant as result of a breach of parole. Paul Ouderkirk is described as an aboriginal male, 33, 5' 6" (167 cm), 180 lbs (82 kg). He has a tattoos of Tribal Flames and a naked woman with wings on his left arm, buck shot and Tribal Flames on his right forearm. He also has a surgical scar on his upper chest area. Ouderkirk is serving a three-year sentence for Robbery (four counts), Carry a Concealed Weapon, Possession of Weapon for a Dangerous Purpose and Fail to Comply with Probation Order. Cornwall Standard-Freeholder, Seaway News (2015-10-26)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Toutes ces larmes ignores
Un article d'opinion déclare, « Comme bien des gens, j'ai été bouleversée par les témoignages de femmes autochtones de Val-d'Or présentés dans l'excellent reportage d'Enquête, la semaine dernière. J'ai été choquée par les allégations d'abus et d'agressions sexuelles. J'ai aussi été choquée de voir que les autorités, au courant de certaines allégations depuis le mois de mai, aient attendu que le scandale

soit médiatisé pour se réveiller. Fallait-il vraiment cinq mois pour établir que les allégations étaient suffisamment graves pour que les policiers visés soient suspendus le temps de l'enquête? Fallait-il cinq mois pour réaliser qu'il était mal avisé de confier à la Sûreté du Québec une enquête sur la Sûreté du Québec? (...)Avant que la ministre Thériault ne verse une larme, il y a eu des décennies de vies volées, de larmes ignorées et d'histoires étouffées. Des décennies d'impunité et d'indifférence. Et pourtant, on savait. Depuis 15 ans, les rapports au sujet de la discrimination et de la violence contre les femmes autochtones se multiplient. Amnistie internationale, Femmes autochtones du Québec, Association des femmes autochtones du Canada, Human Rights Watch... Tous ces groupes et plusieurs autres encore ont documenté une situation tragique sur laquelle on ferme les yeux depuis trop longtemps. » La Presse, A5/Front

*** Time for inquiry**
An editorial states, "The timing, it seemed, was worthy of a top-notch Hollywood movie. No sooner had the keys to Parliament been handed to a party that has promised a national inquiry into Canada's missing and murdered indigenous women when news broke last week Quebec provincial police face allegations they have taken aboriginal women for rides out of town and demanded sex. The aboriginal communities' distrust of police across Canada is like a poison infecting efforts on both sides to battle the violence plaguing indigenous girls and women. Yet, the coincidence is not so remarkable: on any given day, Canadians can hear of yet another tragedy, heinous crime or grave offence against an aboriginal person. This is a sad reflection on the reality in this country. And Justin Trudeau's Liberal government has now assumed the prime responsibility of addressing the historical, complex factors that feed into a shameful state of affairs." Cape Breton Post, A8, Toronto Star (Hamilton Spectator)

*** How deep is culture of erasing public records?**
An opinion piece states, "Last week's bombshell report on the Christy Clark government's destruction of records related to the Highway of Tears was shocking enough. But here's the question that's even more disturbing: Just how deep does this government's culture of recordshredding and coverup really go? That's what the NDP is trying to find out at the legislature, where more evidence emerged Monday of high-level document destruction in Clark's government. (...)This all follows last week's stunning report from Elizabeth Denham, the independent information and privacy commissioner. Denham found a senior government insider erased emails related to the murders and disappearances of aboriginal women along Highway 16 - the Highway of Tears - in northern B.C., and then lied about it under oath. Denham also found similar email mischief going on in Clark's office and in the office of the Ministry of Advanced Education. So is the record-destruction confined to just three offices?" The Province, A6

Objectif: déstabiliser les autorités
A la fin des années 90, alors que les attentats contre les gardiens de prison secouaient la région de Montréal, les Hells Angels de Sherbrooke ont mené - sans jamais être inquiétés - leur propre entreprise visant à déstabiliser les autorités, révèle le délateur Sylvain Boulanger. Ennuyés par l'attention que la police leur portait, les Hells de Sherbrooke ont commandé une série d'incendies criminels visant des bâtiments de la Ville, allant même jusqu'à mettre le feu à une maison de jeunes, affirme le motard qui a retourné sa veste. Sylvain Boulanger est à l'origine de l'opération SharQc, la plus vaste opération antimotards au Canada. Plus de six ans après le début des procédures judiciaires, la majorité des accusés ont plaidé coupables à une accusation de complot de meurtre en échange de l'abandon par la poursuite des accusations les plus graves. La Presse (La Tribune, 15/Front)

Pour faire bouger les choses
Victime de violence conjugale au point où son ex-conjoint a attenté à sa vie, Roxane Trépanier-De La Bruyère veut faire bouger les choses pour aider non seulement les femmes qui vivent dans ce terrible silence, mais l'ensemble des victimes d'actes criminels. La Sherbrookoise de 29 ans souhaite que les victimes soient représentées par leur propre avocat lorsqu'elles décident de prendre leur courage à deux mains et de dénoncer leur agresseur. Elle vient de lancer une pétition sur Internet pour la défense des droits des victimes d'actes criminels qu'elle veut déposer aux députés de Sherbrooke Luc Fortin et de Richmond Karine Vallières. (...)Dans son cas, l'agresseur c'est Michaël Asselin, le père de son garçon, qui vient d'être condamné à 35 mois de prison à Thetford Mines pour l'avoir braquée, elle et ses enfants,

avec une arme à feu prohibée, chargée. Asselin avait aussi été reconnu coupable de menaces de mort sur ses enfants et de possession d'arme prohibée avec des munitions. La Tribune, 3/Front

Police service looking for budget hike
The Regina Police Service is looking to the city for more money in 2016. Although we know how much RPS wants and what they intend to use it for thanks to documents presented at Monday's city council meeting, no police representatives visited City Hall for additional comment. Council tabled the matter for budget deliberations in December, as is customary. When asked, Mayor Michael Fougere said it is too early to comment on the document. The proposed gross operating budget is 5.1-percent higher, or $3.9 million more, than this year, for a total of $80.8 million. Staffing forms nearly 90 per cent of the gross operating budget, including $2.66-million worth of salary increases planned for 2016. If approved, residents will see eight more patrol officers on the street. RPS is also planning on converting two sworn positions to civilian ones to offset that cost. In addition, the heftier budget covers costs related to a new radio system, improvements to the 9-1-1 call centre, and conducted energy weapon (Taser) cartridges and ammunition. Revenues are expected to increase, too, by 3.2 per cent, or $282,500, to $9.15 million. Leader-Post, A1

* **Ontario police chiefs 'disappointed' with safety minister's stance on carding reforms**
Ontario's police chiefs are "disappointed" with how the province is handling its plans to regulate police street checks and worry officers will be "handcuffed" by new rules expected this fall. J.P. Moczulski for National PostProtesters partially block the intersection of Yonge and Bloor Streets prior to the start of the Ontario Street Checks hearings on carding in Downtown Toronto on Tuesday, September 1, 2015. The comments come days after reports minister of community safety Yasir Naqvi suggested he would ban the practice of "arbitrary carding" with a regulation expected to be released later this fall. Naqvi has maintained since June that the practice of seemingly random, often racially biased stops by police must end. Though the minister hasn't really changed his tone since, his participation in an opposition motion to fully ban carding last week was interpreted by some as a sign he would outright ban street checks, more commonly known as carding. On Monday, Naqvi clarified that he will be regulating, not banning, the controversial practice. "Our principle has been the same all throughout (the consultation process): one there is no room for any discrimination or racial profiling... the second thing we've said and we've been saying it quite consistently, is that any kind of carding or street checks predicated on any race or bias without any reasonable cause for stopping somebody is absolutely unacceptable and we will put an end to that through regulation," Naqvi said. He also said the province is looking at how to handle "other kinds of voluntary interactions with police." National Post

* **Carding ban unhelpful, sensible rules needed**
An opinion piece states, "Police services across Ontario - including in Hamilton - are probably not troubled by the news that the provincial government plans to outlaw arbitrary and random police carding. Can you name one service that will admit it does random and arbitrary carding to begin with? In Hamilton, police refer to "street checks" as opposed to carding, but the difference is semantic. And Hamilton police would vehemently deny they conduct the checks for random or arbitrary reasons, and certainly never because of ethnicity (skin colour) alone. They would argue they only do checks when they have legitimate investigative reasons for doing them. So the province is planning to ban a practice that Hamilton police, and probably all police across the province, insist they don't do anyway. What good is the ban, then? To be fair, the province has only so far announced its intent, and says the rules and regulations that go along with the ban are still in development and should be rolled out by this fall. So maybe there will be adequate substance there by the time implementation rolls around. Let's hope so, because a simplistic ban will not be helpful." Hamilton Spectator

* **Police chiefs unveil how media partners help heal violent extremist tragedies**
At IACP 2015, a distinguished group of police leaders gathered to discuss a wide range of issues related to preparing and responding to violent extremists and their attacks. The panel — consisting of Charleston Police Chief Gregory Mullen, Chattanooga Police Chief Fred Fletcher, Ottawa Police Service Chief Charles Bordeleau, and Jean-Jacques Colombi, the chief of international relations for the French National Police — was moderated by Pierre Thomas, the Senior Justice Correspondent for ABC News. Each of

these law enforcers held key leadership positions during four recent attacks by radicalized individuals. Police One

Netherlands won't pursue international charges
Dutch authorities have dropped international child pornography production charges against Aydin Coban, the Dutch man accused of extorting B.C. teen Amanda Todd, whose 2012 suicide galvanized international efforts to stamp out cyberbullying. In a press release last year, the Dutch Public Prosecution Service accused Mr. Coban of producing and distributing child pornography, with victims in the Netherlands, Canada, Britain and the U.S. One of those alleged victims was Ms. Todd. On Monday, however, Dutch prosecutors told Mr. Coban's lawyer and Dutch media that it would solely pursue child-pornography production charges where there was a Dutch victim. Globe and Mail, A5

*** Human trafficking victim shares story**
Several years ago, Taylor left her homeland and came to Canada with her husband and children looking for a better life. "I had the idea that we were going to start over, maybe go to school, that sort of pretty dream," said Taylor, who didn't use her real name or any identifying details out of concern for her safety. Instead of chasing a dream, she fell into a nightmare of torment and abuse. Her husband physically abused her and eventually started pimping her and two other girls out for sex. "He had always been abusive," the 32-year-old said. "He set me on fire once. The abuse was so terrible that escorting was minor." Eventually, Taylor and the other two victims fled her husband and the city they lived in and headed to Windsor where they heard the rates for sex were higher. Her life took a turn when she "got into issues with the police and they took us to a shelter." Last week, police forces from Windsor, LaSalle and Amherstburg took part in a massive North American investigation into human trafficking. Operation Northern Spotlight resulted in the arrests of 47 people from across the province who are now facing 135 human-trafficking related charges. None of the arrests were made locally but a number of women identified by authorities as sextrade workers were offered safety plans and resources to exit their lifestyle. Taylor's personal journey out of darkness began when she met Shelley Gilbert, the co-ordinator of social work services with Legal Assistance of Windsor. Postmedia News (Windsor Star, A8)

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Gary Doer, Canada's ambassador to U.S., says he's heading home soon
It's the end of an era for Canada's most important diplomatic post as Gary Doer confirmed Monday that his longer-than-usual stint as ambassador to the United States is about to conclude. The popular former premier said he'll help prepare the transition to a new Liberal government and will leave it to the incoming government to pick the specific departure date. CBCNews; Macleans (2015- 10-27)

INTERNATIONAL

*** Canada's climate boy scout**
An opinion piece states, "As the Paris climate summit approaches activists are gearing up for the final push through November and into December, although the movement suffered a bit of a downer over the weekend. Hurricane Patricia, building as a major hurricane of unprecedented proportions, fizzled as a climate mega-disaster into a mere tropical storm, leaving behind no opportunities for media and negotiators to use it as a pre-Paris PR bonanza. As news of Patricia reached Europe at a climate change negotiating session in Bonn on Friday, the head of the Mexico delegation, Roberto Dondisch, said Patricia was evidence the frog was already in the boiling water. A reporter for Climate House quoted

Dondish saying "I don't think I need to say more about the urgency to get this deal done.'" Postmedia Network (National Post, FP, 9)

*** Death toll reaches 311 in quake-hit Pakistani, Afghan areas**

Rescuers were struggling to reach quake-stricken regions in Pakistan and Afghanistan on Tuesday as officials said the combined death toll from the previous day's earthquake rose to 311. According to Afghan and Pakistani officials, 237 people died in Pakistan and 74 in Afghanistan in the magnitude-7.5 quake, which was centered deep beneath the Hindu Kush mountains in Afghanistan's sparsely populated Badakhshan province that borders Pakistan, Tajikistan and China. Afghan authorities were scrambling to access the hardest-hit areas near the epicenter, located 73 kilometers (45 miles) south of Fayzabad, the capital of Badakhshan province. In Pakistan, the Swat Valley and areas around the Dir, Malakand and Shangla towns in the mountains of Khyber Pakhtunkhwa province were also hard-hit in the quake. The Pakistani town closest to the epicenter is Chitral while on the Afghan side it is the Jurm district of Badakhshan. More than 2,000 people were injured in Monday's temblor, which also damaged nearly 2,500 homes in Pakistan, officials said. ChicagoTribune.com; UPI.com

*** Taliban urge rescuers 'not to hold back' on Afghan quake relief**

The Taliban urged aid agencies on Tuesday to push ahead in delivering emergency relief supplies after a major earthquake hit remote mountainous regions of northern Afghanistan and Pakistan, killing at least 300 people. Relief groups' efforts to assess the damage were hindered by an unstable security situation that has left much of the affected areas unsafe for international aid workers and government troops. But the Taliban, which have stepped up their Islamist insurgency against the Western-backed government in Kabul this year, indicated they would not stand in the way of aid efforts. Reuters.com

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Thursday, November 05, 2015 6:37 AM
To: Early Draft DMS / RPQ Édition préliminaire (PS/SP)
Subject: PS Daily Media Summary / Revue de presse quotidienne SP

Follow Up Flag: Follow up
Flag Status: Flagged

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 5, 2015 / 5 novembre 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Goodale eyes C-51 as newly minted public safety minister
Ralph Goodale admits a job as Canada's **public safety minister** was ***"not something (he'd) given a lot of thought about"*** - until he learned he'd be getting it in the new federal government. Now, the veteran Regina MP is ''***impressed by the magnitude in that ministry." "It's a very big file, "*** he said in a wide-ranging interview Wednesday***. "It's the Canadian equivalent of Homeland Security,"*** referring to the massive agency in the U.S. ***"There's nothing more important than it to the proper functioning of the country."*** His ''leading priority'' will be overhauling the Conservatives' controversial Bill C-51, which covered surveillance and counterterrorism work by federal agencies. **Goodale** said the Liberals had been ***"highly critical"*** of C-51 during the election campaign and have already done ***"extensive work***'' on how they'll change it, now plugging into the advice of the public safety ministry itself and the federal department of justice. ***"Canadians repeatedly said that they expect the government to keep them safe - and also expect their***

government to respect civil liberties," he said. **Goodale** specifically mentioned revitalizing the Security Intelligence Review Committee by putting onto it sitting politicians who'd be sworn to lifetime secrecy on security details, but could report the big picture back to Parliament. He acknowledged the reported leaks from parallel bodies in other western countries, but ***said Canada could learn from them what to do and not to do. He said a reinvented SIRC could do two things: Make sure security agencies are doing a "good, competent job" and "appropriately respect civil rights and civil liberties."*** C-51 was passed by Stephen Harper's Conservative government in the wake of two murders of Canadian soldiers last autumn. It was defended by the Tories - and just as determinedly attacked by the NDP and civil libertarians. As Liberal leader, Justin Trudeau steered a middle course, supporting C-51, but also stating he'd quickly change it to reflect concerns about government intrusions into privacy. The appointment of **Goodale**, with 27 years of experience as an MP, illustrates the importance Trudeau attaches to reconciling these opposing views. The Liberal platform also sought a mandatory threeyear review of C-51, balanced by more resources for security work - a reference to the 2014 transfer of 600 RCMP investigators from fraud and drug cases to counterterrorism. Colleen Bell, an assistant professor at the University of Saskatchewan, advised **Goodale** to scrap C-51 entirely and replace it with tighter supervision of security agencies, plus more regard for how Canadian foreign policy might be creating terrorists overseas. Postmedia News (StarPhoenix, A4, Leader-Post, A1)

Trudeau unveils diverse cabinet 'that looks like Canada'

Prime Minister Justin Trudeau and his 30 new ministers started tackling thorny issues within hours of forming government, including two ambitious priorities by year-end: a shift of the tax burden from the middle class to the rich and the resettling of 25,000 Syrian refugees. On a sunny day in Ottawa, Mr. Trudeau and his team walked up to the entrance of Rideau Hall to be sworn in, applauded by thousands of supporters who watched the ceremony on large screens set up outside. Mr. Trudeau promised a government that would "get things done," pointing out his team includes representatives from all provinces and features members from a variety of ethnic origins. "It's an incredible pleasure for me to be here today, before you, to present to Canada a cabinet that looks like Canada," Mr. Trudeau said to cheers from the crowd. All ministers spoke to the media about their new portfolios, quickly setting a different tone than the previous Conservative government. There were few concrete details, but the Minister of Immigration, Refugees and Citizenship vowed to meet the promise to welcome 25,000 asylum seekers displaced by the war in Syria in less than two months. "It remains our firm objective," John McCallum said, vowing to work with other federal departments, the provinces and various NGOs. **Public Safety Minister Ralph Goodale**, whose department will screen the refugee claimants, added: ***"We are going to bend every effort to get this job done, get it done right and properly, and fulfill the commitment the Prime Minister made."*** Globe and Mail, A1

A look at some issues facing Justin Trudeau's first cabinet

The new federal cabinet has a lot of issues to tackle, and not a lot of time to learn their files. Here is an idea of what each new minister faces**: Minister of Public Safety and Emergency Preparedness Ralph Goodale**: The new public safety minister must tackle the reversal of some of the more contentious anti-terrorism provisions contained in Bill C-51, and oversee a promise from the Liberals to have more parliamentary oversight of Canada's national security agencies. Canadian Press (Daily Gleaner, B3, Times & Transcript)

Trudeau sworn in

Justin Trudeau has launched a new Liberal era with a 30-member cabinet that features predominantly fresh faces, an equal number of men and women and probably the most diverse line-up of ministers in Canadian history. The newly minted prime minister emerged Wednesday from the formal swearing-in ceremony boasting that he's put together a cabinet "that looks like Canada." ... The rookies will be backstopped by seven veterans with previous federal or provincial cabinet experience, including: **Ralph Goodale** in **Public Safety**; Stephane Dion in Foreign Affairs; John McCallum in Immigration, Refugees and Citizenship; Carolyn Bennett in Indigenous and Northern Affairs; Canadian Press (Kingston Whig-Standard, B1/Front, Record, Edmonton Journal, Spectator, Windsor Star); Le Devoir, A1; Guardian; Chronicle Herald; Telegram; Sun Media Corporation (London Free Press); Postmedia Network (Vancouver Sun, Ottawa Citizen); Postmedia News (Ottawa Citizen); La Presse, A3

Guards union 'welcomes' new government

The national vice-president of the Union of Canadian Correctional Officers says he's "cautiously optimistic" that relations with the new Liberal government will be better than it was with the previous Conservative government. On Wednesday, Prime Minister Justin Trudeau was sworn in and **Ralph Goodale**, a cabinet minister in previous Liberal governments, was appointed **public safety and emergency preparedness minister**. "Certainly we welcome the new government, welcome the new minister, and we want to sit down with him and certainly talk about correctional issues," said Jason Godin in an interview Wednesday. "Unlike the previous government, we hope this government has an open-door policy and will sit down and have conversations with us." Godin hopes the lines of communication, which were shut down when Vic Toews was the Conservatives' public safety minister, will be open with Goodale. "He brings a lot of experience, obviously, to the government and hopefully he'll sit down with us in the very near future to discuss some of our issues." While the Conservatives were in power, they closed Kingston Penitentiary, shut down the prison farms and came in with anti-labour

and anti-union legislation. The Conservatives changed the definition of danger in the Canada Labour Code, which concerned correctional officers a great deal, Godin said. "There wasn't any warning or consultation when they changed the definition of danger and we're hopeful this government will act fairly expeditiously to bring things back to where they were to resolve our health and safety issues for correctional officers." Osprey Media Group (Whig-Standard, A1)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

TRUDEAU, TEAM OF 30 CABINET MEMBERS SWORN IN TO KICK OFF NEW LIBERAL ERA

Justin Trudeau kicked off a new Liberal era Wednesday with a 30-member cabinet that features predominantly fresh faces, an equal number of men and women and probably the most diverse lineup of ministers in Canadian history. The newly minted prime minister emerged Wednesday from the formal swearing-in ceremony boasting that he's put together a cabinet "that looks like Canada." Fully 18 of the newly minted ministers are rookies who won election for the first time last month, including the all-important finance minister, multimillionaire Toronto businessman Bill Morneau. The cabinet includes two aboriginal ministers, two disabled ministers, one openly gay minister, a refugee from Afghanistan and four Sikhs - one of whom was once wrongly accused of terrorism, tortured and detained without trial for almost two years in India. "The diversity that is reflected around the cabinet table and in the House of Commons is incredibly empowering," said Jody Wilson-Raybould, Canada's first indigenous justice minister. "(It) brings new voices to the table for substantive discussions and debate and dialogue and different perspectives from backgrounds but ultimately working together to move forward in terms of solutions." Wilson-Raybould will be one of the most powerful of Trudeau's ministers, responsible for a raft of priority issues, including the promised legalization of marijuana, a new law governing medically assisted dying, new prostitution legislation and the promised rewrite of controversial anti-terrorism legislation. Canadian Press (Red Deer Advocate, A1, A2)

New justice minister faces some of Canada's biggest legal challenges

British Columbia aboriginal leader Jody Wilson-Raybould is a newcomer to government but not to the law, and as Justin Trudeau's newly named justice minister she faces several of the country's biggest legal challenges ever. Drafting an assisted suicide law to conform to a Supreme Court of Canada ruling last February immediately falls to Wilson-Raybould, a lawyer, former provincial Crown prosecutor and treaty commission adviser. Her other big agenda items include Trudeau's pledge to legalize marijuana, and whether to defend a number of Conservative government laws and policies that face constitutional or legal challenges in the courts. Those include: The niqab ban at citizenship ceremonies. The law that allows terrorists holding dual citizenship to be stripped of their Canadian passport. Mandatory minimum sentences for people convicted of growing small amounts of marijuana Arbitrary curbs on sick leave provisions for public servants. Amending the national security scheme under Bill C-51 to meet the Liberal campaign pledge of more parliamentary oversight and ensuring CSIS respects Charter rights. Wilson-Raybould will doubtless be a key hand on legal issues involving aboriginal communities as well. Toronto Star; 1

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Un ex-prisonnier de Guantanamo interdit d'entrée au pays

Un ex-détenu français à la prison américaine de Guantanamo qui est aujourd'hui un militant pacifiste a été arrêté mardi à sa descente d'avion à Toronto, pour des motifs de sécurité nationale. Il pourrait bien être renvoyé chez lui, selon son avocat. Mourad Benchellali, de Lyon, est connu pour son travail en matière de «déradicalisation» chez les jeunes islamistes et il devait donner une série de conférences sur le sujet au Canada. Il a été détenu dès mardi soir comme un prisonnier à sécurité maximum à l'Aéroport de Toronto après que les agents de l'immigration eurent refusé qu'il puisse retirer sa demande d'entrée au Canada et rentrer volontairement en France. Selon son avocat, Hadayt Nazami, les autorités auraient maintenant changé d'avis et seraient prêtes à le laisser regagner son pays - dès mercredi soir, semble-t-il. L'Agence des services frontaliers du Canada a refusé de commenter. (…). Selon son avocat, M. Benchellali s'est appliqué depuis à combattre la radicalisation des jeunes Français. Me Nazami soutient que le Service canadien du renseignement de sécurité et la Gendarmerie royale du Canada avaient tous deux autorisé sa visite de cinq jours au Canada. M. Benchellali avait gagné le Canada via l'Islande, pour éviter de survoler les États-Unis, où son nom figure toujours sur la liste d'interdiction de vol, selon son avocat français. La Presse Canadienne (Acadie Nouvelle, 17, La Presse, 13); Canadian Press (Red Deer Advocate, C2, Times Colonist); Canadian Press (Times & Transcript, B5); London Free Press, B1/FRONT

Woman involved in murder case denied bid to appeal sentence
A foreign national who pleaded guilty to being an accessory after the fact to a Halifax murder will be deported back to her homeland of Saint Vincent. In a written decision released Wednesday, the Nova Scotia Court of Appeal dismissed Debra Jane Spencer's motion to extend time to file a notice of appeal of her sentence. On March 9, 2014, Bradford Eugene Beals murdered David William Rose, 65, in a south-end Halifax rooming house. Spencer, Beals's girlfriend at the time, was at the scene of the murder. Beals and Spencer were arrested two days later. In May 2014, Spencer pleaded guilty and was sentenced to two years in a federal prison. (…)"Ms. Spencer makes it clear that the only objective of her appeal is to avoid deportation," Justice Joel Fichaud wrote in the decision. "To succeed with her objective, Ms. Spencer would have to persuade a panel of this court to reduce her sentence from two years to six months." In Spencer's case, Fichaud said, such a reduction would drop her sentence "far below the range of sentences for being an accessory to murder." "There is no possibility that a panel of this court would order that reduction," the judge wrote. "In my view, her submission is not an arguable ground of appeal." Fichaud dismissed Spencer's motion. Chronicle-Herald, A7

10 % plus d'Américains à Québec cet été
La dépréciation de la devise canadienne a été bénéfique pour l'industrie touristique dans la région de Québec dont les activités ont progressé de 2,1 % au cours de l'été. L'augmentation des principaux indices a été encore plus significative en septembre avec 11,5 % d'augmentation globale, selon les chiffres dévoilés hier par l'Office du tourisme de Québec. En détail, pour l'été 2015, on note une hausse de 3,4 % de l'achalandage dans les hôtels et de 0,6 % dans les restaurants. En ce qui concerne les attraits et les boutiques, l'achalandage a crû de 2 %. Les données observées en septembre sont encore plus spectaculaires. Selon le directeur général de l'Office, André Roy, il s'agit des meilleurs résultats pour septembre depuis le 400e anniversaire de la ville de Québec, en 2008. (…) Historiquement, le mois de septembre attire principalement des touristes hors Québec. Les entrées en provenance des États-Unis à la frontière sont en nette progression (+9,8 %) pour les mois de juin à août 2015. «C'est sûr qu'il y a une corrélation directe entre la valeur du dollar canadien et le nombre de visiteurs américains.» Journal de Quebec, 19

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

Law prof will oversee Val-d'Or probelt might sound like mission impossible.
On Wednesday Quebec's premier thrust Fanny Lafontaine into the centre of the country's most highly publicized police brutality scandal. Her task is to ensure that Quebecers can trust an investigation in which cops from the Montreal police force delve into claims that their colleagues at the Sûreté du Québec physically and sexually abused aboriginal women while on the job. First Nations leaders have already expressed reservations about Lafontaine's ability to pull it offand the SQ's rank-and-file say there shouldn't be an investigation to begin with. Furthermore, Premier Philippe Couillard says he offered the job to other candidates, who turned it down. But Université Laval professor Lafontaine says she wouldn't have accepted to be named the civilian observer of this controversial police probe if she doubted its mandate. Before her appointment, Lafontaine says she received written assurances from the government that she would have full access to the case's chief investigator, to police files, interview transcripts and receive first-hand knowledge of how interrogations are conducted. If she sees anything remotely off base, Lafontaine has the authority to denounce it to the Minister of Public Security. Gazette, A7

Affaire Michel Vienneau
Annick Basque, la compagne de Michel Vienneau, abattu par un agent de la police municipale de Bathurst, a retiré sa demande en cour visant à recevoir les échanges électroniques d'Échec au crime. Elle garde cependant le cap pour la divulgation de toute la documentation entre les mains de la GRC de la Nouvelle-Écosse et les dossiers du coroner. Dans une communication du 31 octobre, l'avocat de Mme Basque avise le tribunal de Bathurst des changements(…)Ils exigeaient également d'avoir tous les documents en possession de l'organisme de la prévention du crime relatifs à Michel Vienneau. Comme l'Acadie Nouvelle le révélait en primeur, c'est une information anonyme à Échec au crime qui a déclenché la surveillance policière du couple Vienneau-Basque à la gare VIA Rail de Bathurst. Une ou plusieurs balles ont atteint M. Vienneau alors qu'il quittait le stationnement à bord de son véhicule. La source affirmait que le couple aurait un chargement de drogues, des pilules, à son arrivée en train. Il revenait de Montréal. Échec au crime ne révèle jamais l'identité des dénonciateurs, ni toute information qui pourrait les identifier. Cette garantie est protégée par la Cour Suprême. Néanmoins, la compagne de l'homme d'affaires de Tracadie insiste pour que la GRC lui fournisse tous les documents pertinents de son enquête sur les circonstances du drame. Elle veut également les fichiers d'autopsie et de toxicologie du coroner. Acadie Nouvelle, 6

When protecting privacy means protecting scum of society

Toronto police Det. Paul Krawczyk is posing as a pedophile in an online chat forum where anonymous men are sharing some of the most troubling thoughts the mind can fathom - from luring young children for sex to feeding them rape drugs. "This person has told me . . . they're interested sexually in 3-year-olds to 9-year-olds," says Krawczyk, a senior child exploitation investigator, reading a message sent on a "boy love" chat forum. The online posters trade technical tips on how to hide their identities from police throughout. "He's saying to use a particular chatting program that is known for its encryption." A joint Toronto Star/Scripps News investigation has detailed how post-Snowden privacy measures - including highly advanced encryption and added search-warrant requirements - have allowed child molesters, drug dealers and organized crime members to hide their crimes from police. While stronger privacy measures have addressed concerns about authorities snooping into our lives, police say they have had unintended consequences: the likelihood that criminals can evade justice because evidence is unattainable. It raises an unanswered question of the digital age: how do we balance protecting personal privacy with the ability of police to investigate crime? On the one hand, police warn that crimes can now unfold before them as they stand by handcuffed by time-consuming judicial bureaucracy or unbreakable encryption. On the other, privacy advocates say we are all better protected from criminal threats posed by everything from tyrannical governments to sophisticated criminals. "Is the public ready to accept that there is a wall too high and a moat too deep . . . for law enforcement and security agencies in Canada to access information that is a security concern to all of us?" asks Scott Tod, Ontario Provincial Police deputy commissioner. Toronto Star, A1

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Correctional officers assaulted

Two Collins Bay Institution correctional officers were injured after being assaulted in the maximum security unit on Tuesday morning, Correctional Service Canada reports. The assault occurred at approximately 8:45 a.m., and the two male officers were evaluated and treated at an outside hospital. Wayne Buller, assistant warden of management services at Collins Bay, told the Whig-Standard Wednesday that there was only one offender accused of the assault. "It was just during the normal day-to-day activities," Buller said. "(During day-to-day activities), they could be going to programs, they could be going to appointments in health care, so when they are moving they could be moving offthe range, or within the range itself. "In this particular case, it was contained in the range itself." The two living units at Collins Bay are broken up into secured ranges for 96 offenders with 12 cells per range. "(Offenders) move within the range, and outside the range from time to time," Buller said. The institution and the joint forces penitentiary squad are investigating the assault. "There may be more information released possible pending charges," Buller said. The correctional officers were advised to attend the hospital but were not admitted. "Normally that's what we do if any staffare injured, and would need medical attention, we would absolutely send them to hospital," Buller said. Kingston Whig-Standard, A3

Mafioso who died wasn't suicidal: report

A report obtained by the Montreal Gazette through the Access to Information Act reveals Correctional Service Canada staffsaw no signs that Mafioso Giuseppe De Vito was suicidal before he died of cyanide poisoning inside a federal penitentiary. The report, prepared by a committee assembled to examine the 46-year-old's death, on July 8, 2013, is another sign De Vito, one of the leaders behind a failed attempt to replace the Rizzuto organization at the top of the Mafia in Montreal, was murdered. A Quebec coroner who investigated De Vito's death found cyanide in his body. Two months before he died, De Vito told a jury he blamed himself for the death of his two daughters at the hands of their mother, Adele Sorella. The girls - Sabrina, 8, and Amanda, 9 - were murdered in 2009 by Sorella. At the time, Sorella was under a great deal of stress generated, in part, by De Vito's absence. In 2006, De Vito went into hiding to try and avoid arrest in Project Colisée, an investigation into the Mafia in Montreal. De Vito was arrested in 2010 and was later convicted of taking part in a conspiracy to smuggle massive amounts of cocaine into Canada through Pierre Elliott Trudeau International Airport. At the time of his death, De Vito was serving a sentence of 11 years and seven months at the Donnacona Institution, a maximum-security penitentiary near Quebec City. The sentence would have expired on Jan 19, 2024. Sorella was convicted of murdering the couple's daughters just two weeks before De Vito was found dead. Despite the bleak circumstances of his life at the time, the committee assigned by Correctional Service Canada to investigate his death reported there were no signs that he was suicidal. Montreal Gazette, A6

Via terror plotter to appeal

A man accused of plotting to derail a passenger train between Canada and the U.S. intends to appeal his conviction on terrorism charges at Ontario's highest court. Raed Jaser has filed a notice of appeal with the Ontario Court of Appeal in which he indicates he will be asking for a new trial. In the document, which is an initial step in the appeals process, Jaser argues that the judge who presided over his eight-week jury trial made several errors. Jaser and his co-accused, Chiheb Esseghaier, were found guilty in March on a total of eight terror-related charges between them. They were sentenced to life in prison in late September, with no chance of parole until 2023. Canadian Press (The Guardian, B5, Whitehorse Daily Star, Toronto Sun)

Ex-jail guard convicted of sexual assault has day parole extended

Day parole has been extended for three months for a former jail guard who sexually assaulted and severely choked a young woman with his hands. Robin Mitchell Smyth, 44, is serving a 3-year sentence for sexual assault, sexual assault causing bodily harm and careless use of a firearm. Smyth committed the offences in his home over a seven-month period. The Lower Sackville man was granted day parole in April. He previously worked at the Dartmouth jail. On Oct. 20, the Parole Board of Canada extended Smyth's day parole after concluding that he is a low risk to reoffend and his reintegration potential is consistently high. Before his day parole release, Smyth participated in an intensive sex offender program. He also has continued support in the community, the decision said. Chronicle-Herald, A9

Inquest to begin Dec. 7 into disabled man's starvation death
An inquest into the starvation death of an intellectually and physically disabled man will begin in Dec. 7 in Brockville, the province announced Wednesday. Jamie Hawley, 41, weighed just 57 pounds and his body was covered in 33 bed sores when he died at Brockville General Hospital in May 2008. His brother Jerry Hawley is serving a 20-year prison sentence for manslaughter for Jamie's death. Police initially charged Jerry Hawley was with first-degree murder in what they believed was a deliberate attempt to starve Jamie to benefit from his disability cheques without having to provide him with adequate care. That charge was later reduced to second-degree murder. In February 2013, a jury found Jerry Hawley guilty of manslaughter. Ottawa Citizen

Class-action lawsuit seeks end to solitary for juvenile offenders
Seeking an end to solitary confinement for juvenile criminals, lawyers filed a class-action lawsuit Wednesday against the Ontario government, saying the practice is always cruel and harmful. The $125-million lawsuit is the latest in a growing legal fight against the practice of segregation in Canada. It alleges that youth-justice centres regularly violate Ontario policies meant to limit the use and duration of solitary, and advocates to give youths access to legal help to stay out of segregation. It also says children as young as 12 are being placed in solitary. Solitary "will always fly in the face of the purpose of youth justice, which is to rehabilitate children," James Sayce, a Toronto lawyer who is involved in the lawsuit, said in an interview. (…)The case follows a lawsuit brought in January by the B.C. Civil Liberties Association and the John Howard Society alleging that the federal government's use of solitary confinement leads to the deaths of prisoners, discriminates against mentally ill and aboriginal inmates and is unconstitutional. Mr. Sayce filed a separate class-action lawsuit in Ontario in July, saying the federal use of solitary violates the rights of the mentally ill. The federal government has kept the practice in widespread use, with some changes in response to the 2007 death of Ashley Smith, who at age 19 had spent nearly a year in solitary before dying from self-inflicted strangulation. Globe and Mail, A1, Canadian Press (Ottawa Sun)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

Consultations first on refugee promise
Newly-minted Immigration Minister John McCallum says a campaign promise to resettle 25,000 Syrian refugees remains the Liberal government's goal. And McCallum, who served as the Liberals' immigration critic in the last Parliament, says he's not backing away from Jan. 1 as the target date for fulfilling that promise. With only eight weeks remaining, McCallum says he is waiting to be briefed intensely on the file. He says he'll be reaching out quickly to different levels of government, non-governmental organizations and other federal departments, including the federal ministries of Defence, Health and Public Safety, which he says all have a role to play. McCallum's new portfolio, Immigration, Refugees and Citizenship, was announced earlier Wednesday at a colourful swearing-in ceremony for the new Liberal cabinet. Canadian Press (Red Deer Advocate, C2)

Syrian influx key 'objective'
Even before John McCallum was named immigration minister, members of Prime Minister Justin Trudeau's inner circle were working on one of the new government's most time-sensitive promises: to resettle 25,000 Syrian refugees by the end of the year. A former Royal Bank of Canada chief economist who previously served in cabinet under Jean Chrétien and Paul Martin, McCallum was confirmed as Canada's minister of Immigration, Refugees and Citizenship during Wednesday's cabinet swearing-in ceremony at Rideau Hall. His appointment wasn't wholly surprising. With the clock already ticking, it was widely acknowledged that Trudeau would need an experienced hand who knew how government and the bureaucracy worked in order to start moving quickly on the Syrian refugee crisis.(…) Some refugee groups have warned over the past week that the new government won't be able to keep its promise to accept 25,000 Syrians by the end of the year. Asked for an update Wednesday, Trudeau would only say he had taken "a big step toward it by appointing the kind of cabinet that gets things done." (…)Sources said Trudeau's transition team had already met senior officials to discuss a way forward. While no decisions had been made, deploying more immigration officers to screen

asylum seekers and using military aircraft to ferry refugees to Canada were among the options on the table.The Syrian refugee file is one of the government's top priorities and Trudeau is expected to order that no effort be spared to get the refugees to Canada, in part because he doesn't want to start his time in government by breaking a promise. Postmedia News (Ottawa Citizen, A3, Leader-Post)

Afghan vet takes on Defence
In 2009, Jon Vance, then a brigadier general, asked Harjit Singh Sajjan to go to Afghanistan as a special adviser to the Canadian mission in Kandahar. Six years later, Sajjan will be working again with Vance, albeit in a significantly different role. Sajjan, a 44-year-old combat veteran who served in Bosnia and in Afghanistan on three deployments, was named the country's defence minister on Wednesday. The Vancouver South MP takes on one of the most difficult portfolios in the federal government. "The list of issues the new minister will have to grapple with is very extensive," said Martin Shadwick, who teaches strategic studies at York University in Toronto. "And some of the major ones will have to be dealt with almost immediately." (...) At the same time, the Canadian Forces could be called on to provide help in transporting and supporting the 25,000 Syrian refugees the Liberal government wants to bring into Canada by the end of December. Kingston Whig-Standard, B2

Consultations first on refugee promise
Newly-minted Immigration Minister John McCallum says a campaign promise to resettle 25,000 Syrian refugees remains the Liberal government's goal. And McCallum, who served as the Liberals' immigration critic in the last Parliament, says he's not backing away from Jan. 1 as the target date for fulfilling that promise. With only eight weeks remaining, McCallum says he is waiting to be briefed intensely on the file. He says he'll be reaching out quickly to different levels of government, non-governmental organizations and other federal departments, including the federal ministries of Defence, Health and Public Safety, which he says all have a role to play. McCallum's new portfolio, Immigration, Refugees and Citizenship, was announced earlier Wednesday at a colourful swearing-in ceremony for the new Liberal cabinet. Canadian Press (Red Deer Advocate, C2)

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

Canadian anti-ISIL fighter reported killed by suicide bomber
A Canadian volunteering with Kurdish forces in northern Syria was reportedly killed in a suicide bombing on Wednesday, and an Ontario mother said she was trying to verify it was her son, a Canadian Forces veteran. "A Canadian fighter was martyred by a terrorist suicide bomber who detonated an explosives belt during fighting in Hasakeh," Talal Ali Sello, spokesperson for the Syrian Democratic Forces coalition, told Agence France-Presse. Thehead of the Syrian Observatory for Human Rights, meanwhile, said the Canadi-an's passport showed he was a 32-year-old born in Toronto. The name and profilematched a former Canadian infantryman who left for Iraq on April 30. Postmedia News (London Free Press, B1/Front); Postmedia News (Windsor Star, A1); La Presse, A15

Quiet spy inspired Bond
One of the world's greatest spies was an operative for England with an affinity for martinis, a suave rapport with elite power players, and an uncanny ability to infiltrate and eliminate threats. This isn't the fictional James Bond we're talking about, but the real-life Sir William Stephenson - a quiet **Canadian** code-named Intrepid who many believe inspired author Ian Fleming to create his over-the-top British spy hero. "Without doubt, Fleming's idea of James Bond is based on Sir William," says Cord Hart, a former CIA operative and U.S. Army colonel who got to know Stephenson through intelligence circles in the early '80s. With the latest instalment in the bombastic 007 franchise, Spectre, hitting theatres Friday, descendants and admirers of the late Winnipeg-born war hero say Stephenson's impressive exploits are too little known. "I always tell people he's the most famous Winnipegger of all time," says Heartland Travel and Tours owner Don Finkbeiner, whose tours include a stop at a bronze life-size statue of Stephenson near the Manitoba legislature. "Nobody even comes close. And I would suggest he's the most famous Canadian of all time." Canadian Press (Red Deer Advocate, C4)

INTERNATIONAL

Sent to: !DMS - EARLY DRAFT

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
April 6, 2016 / le 6 avril 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Vancouver Island officer killed in crash with pickup
The RCMP has confirmed a police officer with West Shore RCMP was killed in a crash Tuesday morning in Langford on Vancouver Island. **Federal Public Safety Minister Ralph Goodale** relayed his condolences to the family, friends and colleagues of RCMP Const. Sarah Beckett. ***"The death of a police officer is a stark reminder of the sacrifices and bravery of our policewomen and men who put themselves in harm's way each and every day to keep our communities safe,'*** **Goodale** said in a statement Tuesday. In the statement, RCMP commissioner Bob Paulson extended the department's full support to Beckett's family and to personnel of the force as they grieve for their colleague. B.C. solicitor general Mike Morris announced in the legislature that a member of the RCMP had been killed. "The member was on duty at a traffic stop and was unfortunately struck and killed on duty," he said. "She's a mother of two young children and my condolences go out to her, her family, her workmates in the RCMP and the police in general." The crash happened at Goldstream Avenue and Peatt Road at about 3:30 a.m. between a police cruiser and a pickup truck. There is no word on charges, and the incident remains under investigation. BC Ambulance said two people were transported to hospital in serious condition. The

intersection was expected to be closed much of the day and motorists were advised to avoid the area. Vancouver Sun, A9; Canadian Press (Red Deer Advocate, A7, Guardian, Telegram, Chronicle-Herald, Cape Breton Post, Calgary Sun, Edmonton Sun, Province); Times Colonist, A1; CBC; *Press Canadienne (Le Droit, 37); *Global News

How to mourn friends and reassure people
A minister's disaster handbook: **Public safety minister** prepped with talking points on everything from hostage-takings to major terrorist attacks. Bureaucrats have prepped **Public Safety Minister Ralph Goodale** on how to talk to the public after tragedies, even prescribing "no comment" responses to hypothetical scenarios, according to ministerial briefing books. When they take office, Canada's **public safety ministers** are offered a "ministerial handbook for responding to events." Embassy obtained the most recent copy with an access-to-information request, part of a series of briefing books given to **Mr. Goodale** after he was sworn in as **public safety minister** early last November. It's a look at the pragmatism of the department in delivering potentially disastrous news to Canadians. (…) The **public safety minister** is expected to provide "national leadership" across the government and co-ordinate a response to "events in the national interest," in concert with Foreign Minister Stéphane Dion if the events occur outside of Canada. (…) If a terrorist attack happens in Canada, **Mr. Goodale** is advised to tell the public "a tragic event has taken place in [city or town] and our heartfelt sympathies are with those directly affected and their families." He's supposed to reassure the public that he's in close contact with provincial and territorial officials, Royal Canadian Mounted Police and national security partners. (…) 'Very sad day for all Canadians' Incidents involving the agencies that fall under **Public Safety Canada** are also addressed in the handbook. (…) Similar language has already been used by **Mr. Goodale** in responding to terrorist attacks in Brussels and Paris, and the recent death by suicide of an RCMP officer near Parliament Hill. The wording isn't exactly the same. The department does, after all, employ dozens of communications staffers. The tone of statements made by **Mr. Goodale's predecessor, Steven Blaney,** are similar. Embassy; *Hill Times

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** National Energy Board orders pipeline firms to post emergency manuals online**
Canada's energy watchdog is ordering pipeline companies to post their emergency response plans online as part of a broader effort to build public trust. The National Energy Board believes it's the first regulator in North America to have that requirement. Companies must have their emergency procedures manuals available on their websites by the end of September, according to the order issued Tuesday. Some information may be excluded, such as personal information and details that may jeopardize security or harm traditional indigenous sites or at-risk species. Canadian Press (Financial Post, FP4; National Post, Globe and Mail, Red Deer Advocate, Times Colonist, Telegraph-Journal); Calgary Herald

*** Report on avalanche death calls for more training, gear**
A report into the death of a Canadian Forces member who was buried under metres of snow during an exercise is recommending more avalanche training for search-and-rescue technicians. Sgt. Mark Salesse, 44, was swept off a narrow mountain ledge by an avalanche on Feb. 5, 2015, in Banff National Park. His funeral drew hundreds of people to 442 Transport and Rescue Squadron at 19 Wing Comox, where he had become a SAR technician in 2005. The military board of inquiry report also recommends that troops use proper rescue and communications equipment when taking part in ice climbing and backcountry skiing training in terrain with an avalanche hazard. Salesse wasn't wearing an avalanche transceiver, a device that allows rescuers to home in on a signal to locate buried victims. Canadian Press (Times Colonist, A2; Edmonton Journal, Times & Transcript); Calgary Herald; Calgary Sun

*** 3.1 earthquake off Victoria**
Victoria got a light shaking and an emergency-preparedness reminder on Tuesday morning. A magnitude-3.1 earthquake struck just south of Orcas Island, about 36 kilometres from Victoria, at 11:06 a.m., said Taimi Mulder, an earthquake seismologist with Natural Resources Canada. The quake was felt in Victoria, Sidney, the Gulf Islands and the San Juan Islands. No damage was reported. Times Colonist, A4

*** Vancouver sets up disaster support hubs**
Within minutes of city staff announcing a network of disaster support hubs around Vancouver Tuesday, a 3.1-magnitude earthquake rattled nearby Squamish and the Sunshine Coast. The earthquake did no damage, according to Natural Resources Canada, but it was a timely nudge for Vancouver residents to take stock of their emergency plans - in part because the city is looking for residents themselves to play a big role in disaster response. After a 6.3-magnitude earthquake shook Christchurch, New Zealand, flattening buildings and killing scores of people, residents banded together to recover and rebuild. That relief effort all started with citizens connecting on social media and gathering at community sites to see how they could help out. In a bid to enable that type of response when disaster strikes Vancouver, staff have designated 25 locations around the city for residents to gather, Daniel Stevens, Vancouver's director of emergency management, told city councillors. "When we looked at what happens during an earthquake, we realized ... that community - the people around you - are really the people that provide the most support," Stevens said. "Our first responders will be prioritizing response to life saving incidents. The capacity will be stretched." Vancouver Sun

*** First responders will receive PTSD compensation**
Ontario unanimously passed legislation Tuesday recognizing post traumatic stress disorder as work-related illness for police, firefighters and paramedics. Under the old rules, first responders had to prove their PTSD was related to their job to be eligible for coverage under the Workplace Safety and Insurance Act. Labour Minister Kevin Flynn beamed as legislation that assumes PTSD is work-related for first responders passed third and final reading by a vote of 96-to-0. "It was gratifying to look around the House and realize that by an action of this legislature, in a unanimous manner, we're able - I think - to change and affect lives in a really meaningful way," Flynn said. "I think over the years we haven't dealt with those issues properly - and I don't mean us as a government, I mean society just hasn't paid enough attention to mental health issues in general." Flynn said first responders are at least twice as likely as the general population to suffer from PTSD, and that the condition results in more suicide attempts than all other anxiety disorders. Canadian Press (Waterloo Region Record, A5)

*** Tofino whale-watching capsizing: Leviathan II survivors file potential class-action lawsuit**
Two German brothers who survived the capsizing of a whale-watching boat off Tofino, B.C., last fall are suing, claiming the capsizing was "preventable" and alleging negligence by the company, owner and captain. Christian Barchfeld and Dirk Barchfeld were passengers on the Leviathan II, owned by Jamie's Whaling Station Ltd., when it capsized on Oct. 25, killing six of the 27 people on board. They have filed a potential class-action lawsuit, on behalf of all passengers, which details their own physical and psychological trauma, with one brother saying he was tossed from the ship and the other describing being trapped inside. CBC News

*** 36 of 58 cars removed**
Ontario Northland crews are on site tonight responding to this morning's derailment near Peninsula Road. An incident command post has been set up on site with an emergency response team comprised of rail experts, Transport Canada and a dangerous goods expert from the Railway Association of Canada. There were no injuries reported Tuesday morning when 25 tanker cars of the northbound 58-car train derailed. The highway was closed for a few hours after the 5:30 a.m. incident. The cars usually transport sulphuric acid. They were empty at the time of the derailment and there appeared to be no breach of any of the cars, Deputy Fire Chief Greg Saunders reported from the scene. As of Tuesday evening, 36 cars had been removed from the area and equipment had been mobilized to facilitate re-railing of the remaining cars and repair of infrastructure. North Bay Nugget (2016-04-06)

*** Missing man's body found**
Police have recovered the body of a missing man. On Monday, RCMP in Port Alice and Port Hardy received a report that a car was down a steep embankment on a remote logging road outside Port Alice. The steep terrain made it impossible for investigators to get to the car, said Staff Sgt. Gord Brownridge. It was recovered with the assistance of Campbell River Search and Rescue and the LeMare Logging Company. Inside, police found the body of Marc Regimbal. Times Colonist, A4

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Ottawa fines bank $1.1M, but keeps its name secret**

The federal anti-money laundering agency has levied a $1.1-million penalty against an unnamed Canadian bank for failing to report a suspicious transaction and various money transfers. It is the first time the Ottawa-based Financial Transactions and Reports Analysis Centre of Canada, known as Fintrac, has penalized a bank - and it's being billed as a warning to thousands of other businesses. Generally, the centre tracks cash flows linked to terrorism, money laundering and other crimes by sifting through millions of pieces of data annually from banks, insurance companies, securities dealers, money service businesses, real estate brokers, casinos and others. In this case, Fintrac spokesman Darren Gibb said he cannot legally discuss details of the bank's infractions, and the federal agency is keeping secret the identity of the financial institution, which recently paid the penalty of $1,154,670. But Fintrac wants to send a strong message that it will take whatever measures are needed to encourage compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. The agency depends on a steady flow of reports about suspicious dealings, electronic fund transfers and large cash transactions to produce needed intelligence, Gibb said in an interview. "The reporting to us is absolutely critical. Without those reports, Fintrac is out of business," he said Tuesday. "We're going to be extra-diligent to ensure that entities are submitting suspicious transaction reports when they should be." About 31,000 businesses across the country must furnish Fintrac with reports. The agency, in turn, provided 1,260 disclosures of financial intelligence to police and national security partners in 2014-15. Canadian Press (Toronto Star, A1, Guardian, Red Deer Advocate, Telegram, Cape Breton Post, Chronicle Herald, Ottawa Sun, Record, Hamilton Spectator, Times Colonist, National Post, Globe and Mail, Times & Transcript); Globe and Mail, A10

*** Les gouvernements font déjà "tout ce qu'ils peuvent"**

Depuis le début des révélations des Panama Papers, de nombreuses voix s'élèvent pour réclamer des actions plus vigoureuses de la part des gouvernements nationaux dans la lutte contre l'évitement et l'évasion fiscale. Mais selon l'expert en fiscalité internationale Jean-Pierre Vidal, les États impliqués dans cette bataille, y compris le Canada, ont déjà fait ce qui est en leur pouvoir. " Les gouvernements font déjà beaucoup. En fait, je pense qu'ils font déjà tout ce qu'ils peuvent ", affirme le professeur au Département des sciences comptables de HEC Montréal en entrevue au Devoir. " Le défi, c'est surtout d'obtenir les informations pour prendre les gens qui sont en défaut, précise-t-il. Tant que les gens sont capables de cacher ce qu'ils font, on ne peut pas les atteindre. Et même si on engageait des dizaines de milliers de vérificateurs, ça ne changerait rien. " Selon M. Vidal, les gouvernements ont fait des progrès considérables en matière d'échange d'informations depuis le début des années 2000. Sous l'impulsion de l'OCDE, de nombreuses juridictions se sont engagées à échanger des renseignements fiscaux : 132 se sont jusqu'à maintenant dites prêtes à le faire " sur demande " et 96 ont promis d'échanger des informations de manière " automatique ", dans un délai de deux ans... L'Agence du revenu du Canada a réitéré mardi son intention de donner suite aux révélations des Panama Papers. " L'Agence cherche activement la collaboration de ses partenaires signataires de convention et du Consortium international des journalistes d'investigation pour obtenir tous les dossiers divulgués qui concernent des résidents canadiens ", a-t-elle déclaré par voie de communiqué. Dans son dernier budget, le gouvernement Trudeau a consacré 444 millions de dollars sur cinq ans à la lutte contre l'évasion et l'évitement fiscaux. Ce nouvel effort permettrait, selon Ottawa, d'aller chercher 2,6 milliards sur cinq ans. L'agence fédérale de lutte contre le blanchiment d'argent a imposé une pénalité de plus de 1 million de dollars contre une banque canadienne non identifiée pour avoir omis de rendre compte d'une transaction suspecte et de divers transferts d'argent. C'est la première fois que le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), établi à Ottawa, sanctionne une banque. L'agence retrace les fonds liés au terrorisme, au blanchiment d'argent et à d'autres crimes. Le porte-parole du CANAFE a affirmé ne pas pouvoir discuter des détails des infractions, et l'agence exerce son droit discrétionnaire de ne pas divulguer l'identité de l'institution financière, qui a payé récemment la pénalité. La Presse canadienne (Le Devoir, A4)

*** Snowden says Panama Papers show whistleblowers 'vital' to society**
Edward Snowden, the former U.S. National Security Agency contractor responsible for the release of thousands of classified documents detailing the American government's use of mass surveillance, says the Panama Papers show the role of the whistleblower in a free society has become "vital." Mr. Snowden, who is living in Russia under political asylum, made the comments via video link during a sold-out event hosted by Simon Fraser University on Tuesday night. Mr. Snowden said the Panama Papers reveal "the most privileged and the most powerful members of society are operating by a different set of rules."
"I think that this shows, more than ever, the role of the whistleblower in a free society has become not only desirable but vital," he said. (...) At the same time, through programs of mass surveillance revealed in recent years, we, the private citizens, are increasingly transparent to government. The relationship between the governing and the governed has become inverted. And rather than those who represent us in our government being accountable to us, we are now accountable to them." Mr. Snowden, when asked about Canada's new anti-terror legislation, cited its connection to the United States and the Five Eyes intelligence alliance. "You put everything in one big, giant bucket. I would suspect this is what C-51 is really about," he said. "It's about broadening that bucket and making sure we put more Canadian information in that sharing bucket, so that it's more easily shared. Now I don't want to say that it's absolutely what's happening, but ... this is how it works, this is what we do for every other country." Globe and Mail; HuffPost BC

*** Sharing of intelligence required for our safety**
An opinion piece states "Information is vital currency in the war against terrorism. So, too, is the willingness and ability of authorities to act on it. It came to light this past week that the FBI had warned Belgium about two of the men who carried out suicide bombing attacks that killed more than 30 people last month in Brussels. That fact evokes a sad and bloody history in the West, in which terror attacks have repeatedly come on the heels of failures in intelligence sharing. Such failures date back notably to the Sept. 11 terrorism attacks against the United States, as subsequent reviews and 2004's 9/11 Commission's report found. While this latest incident may or may not have been preventable, the fact remains that the sharing of intel in a timely and co-operative manner is the best tool at the disposal of the governments, police and spy agencies working to protect us from a very real threat. It is not just between allies that information should be shared. It must also be co-ordinated inside our own borders. There is a recent report that authorities are bridging divisions between the Canadian Security Intelligence Service and its counterpart, the Communications Security Establishment, which is not permitted itself to spy on Canadians. Their co-operation, including apparently through the CSE-CSIS Collaboration Office, is obviously essential to our security safety network. They need to be working hand in glove." Kingston Whig-Standard, A4

*** Terrorists defile Islam**
A letter to the editor states, "With the rise of recent extremism in the world, critics are continuously pointing fingers at Islam for being the catalyst of much of terrorism by fringe terror groups. At this time it is essential that we remember just like guns don't kill people, people kill people; Islam does not promote violence, people do. They misconstrue the peaceful teachings of Islam to justify their hatred acts. As a young Canadian Muslim, I invite you to reach out to a fellow Muslim and discuss the real teachings of Islam, rather than judging the sensationalized propaganda as your average Muslim belief." Waterloo Regional Record, A6

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

*** CBSA officers kept 36 suspected criminals out of Canada in Feb.**
The Canda Border Services Agency (CBSA) refused entry to 55 foreign nationals in the month of February this year, including 36 who had a criminal history and were attempting to enter Canada. At the Carievale border crossing, officers turned back a United States male who had been convicted of sexual assault of a child, as well as a woman who had been convicted on six counts of conspiracy to distribute methamphetamines. They also arrested a man from North Dakota on grounds of his involvement in organized crime. An immigration and refugee board hearing found the man inadmissible due to his membership in the Varrio Norwalk gang, so a deportation order was issued. At the Northgate border

station, officers refused entry to a North Dakoa man on Feb. 18 after it was learned he had been convicted of making terrorist threats. That same man attempted to seek entry into Canada at the North Portal border crossing station six days later and was again refused entry. North Portal officers also refused entry to a man convicted of sexual assault. On Feb. 23, North Portal officers intercepted and arrested an impaired driver and turned him over to the RCMP. At the Oungre, Sask., crossing, officers refused entry to an American male who had been convicted of conspiracy to distribute methamphetamines. Estevan Mercury

Turtle smuggler slapped with $25,000 fine
A Toronto seafood supplier has been fined $25,000 after he was nabbed smuggling 40 live turtles into Canada at the Queenston-Lewiston Bridge in Niagara-on-the-Lake, Ont. Jie Hua Shen, owner of Marine Seafood Inc., pled guilty March 26 in St. Catharines court to importing Florida soft-shell turtles into Canada illegally. The case stemmed from a joint Environment Canada and U.S. Wildlife Service operation launched in December 2013 focusing on the trade in the turtles. Florida soft-shell turtles are prized for their meat, which has led to a decline in their numbers. In response, Florida has banned the commercial fishing of the turtles. The turtles seized in this case were found to have fish hooks buried in their throats. In May 2015, Shen was found guilty in federal court of contravening the Customs Act. National Post

An 'Unfair And Perverse Legal Restriction'
An opinion piece states, “Canada, the great liberal state, can take in refugees from strange lands by the thousands, spend $1 billion providing them with health care, housing and welfare, put them up in hotels and provide prime ministerial greetings at its airports. Welcome to Canada - land of big hearts and abundant resources. Hell, we' ll even renew the citizenship of a terrorist as a matter of the highest principle. But heaven help the individual or family that might want to quietly settle in Canada, in contravention of some heavy-handed entry barriers embedded in the Immigration and Refugee Protection Act. Indeed, a family of 10 can arrive as a part of mass transfer of 250 refugees on a plane from Jordan, regardless of how much they might cost taxpayers; yet regular immigrants face tougher, sometimes insurmountable, barriers. When Felipe Montoya applied three years ago to become a permanent resident of Canada with his wife and two children, he ran into those barriers. One of Montoya's children, his son Nicolas, has Down syndrome, a condition that prompted Citizenship and Immigration Canada (CIC) to determine that Montoya and family may be inadmissible on health grounds. Montoya, a native of Costa Rica, has been a professor of environmental studies at York University for the past four years. As numerous news stories have reported, on March 3 he received a letter from CIC - signed, "Sincerely, DO877" - saying that "it appears that you or your family member may not meet the requirements for immigration to Canada." (...)The reason: "Your family member, Nicolas Montoya, has the following medical condition: Down's syndrome." (...)Montoya also sees his family's rejection as a breach of the Canadian Charter of Rights and Freedoms. But his only option may be to appeal to the minister.” National Post, A9

'Speed it up,' refugee sponsors tell minister
Responding to public outrage over delays in bringing Syrian refugees to Canada, Immigration Minister John McCallum will meet with private sponsorship groups on Thursday to explore options. "What I can say to you right now is I'm doing everything in my power to speed the process up as much as we can to admit as many Syrian refugees as possible, as quickly as possible," he told dozens of protesters on his way to a luncheon hosted by the C.D. Howe Institute Tuesday. "We have to do it as quickly as possible and I know you want to help. I appreciate that. So many people are out here, saying we want our refugees quickly. I will be meeting with (former Toronto mayor) John Sewell to talk about it in more detail." It was the first faceoff between the embattled McCallum and members of private sponsorship groups since Ottawa quietly stopped making it a priority to process Syrian sponsorship applications, shortly after meeting its goal of bringing in 25,000 Syrian refugees by the end of February. Last week, the government did briefly extend the deadline for community and faith groups to submit new applications, but refugee sponsors were further angered by the 24-hour notice they had to finish incomplete applications. Toronto Star, GT2

*** Worldpac Canada v. CBSA: Blanket B2 authorization requests do not affect time limits to file refund requests under the Customs Act**

In its February 18, 2016 ruling in *Worldpac Canada v. CBSA*[1], the Canadian International Trade Tribunal (the "CITT") clarified several key issues of prescription and recourses to appeal in the context of the *Customs Act* (the "Act"). In particular, the CITT addressed the so-called "blanket authorization" process (or Blanket B2 adjustment), which allows an importer to apply to the Canada Border Services Agency (the "CBSA") for an authorization to file several adjustment or refund requests at once in order to reduce both the paper burden and processing time. The CITT held that this procedure is purely administrative and does not affect the statutory time limits provided for under the Act. In addition, it held that neither the CBSA nor the CITT has jurisdiction to consider refund requests filed outside the statutory time limit. Worldpac Canada is an importer of original equipment and automotive parts. Between 2011 and 2013, the company submitted a total of three blanket authorization requests to the CBSA with respect to refund requests for erroneously classified importations that occurred between March 1, 2008 and December 21, 2009. Between February 28, 2012 and July 12, 2013, the CBSA issued blanket authorization letters with respect to Worldpac's requests (although one authorization was cancelled by the CBSA in March 2013). In its letters, the CBSA clearly informed Worldpac that the blanket authorizations "... in no way remove or extend [...] the four-year time limits to file a refund under section 74 [of the Act]" Lexology (2016-04-05)

Liberal, Tory, NDP MPs pan protectionist talk by Trump, Sanders
MPs from all three major parties say they reject the protectionist positions of leading United States presidential candidates on free trade, warning that a thicker US border would harm businesses and workers in both countries. However, a few NDP and Liberal MPs expressed similar concerns over free trade agreements to those raised by Hillary Clinton, Bernie Sanders and, of course, Donald Trump over the past year. Free trade is a rare subject on which Mr. Sanders, Ms. Clinton and Mr. Trump appear to agree, or at least to hold common concerns. Mr. Trump pledged in September to force a renegotiation of the North American Free Trade Agreement between Canada, the United States and Mexico, or else to "break" it. Mr. Sanders said earlier this year he picketed against the NAFTA while it was under negotiation in the early 1990s. Ms. Clinton has in the past criticized and expressed support for the deal. Both Democratic candidates have said they opposed the Keystone XL pipeline from Alberta's oilsands to the US Gulf Coast, and all three candidates-as well as Republican candidate Ted Cruz-have said they oppose the Trans-Pacific Partnership agreement, which would supercede many parts of the NAFTA if it were ratified. (...)Liberal MP Ken Hardie, another member of the interparliamentary group, warned that a more protectionist United States could put even more pressure on forestry workers in his Fleetwood-Port Kells riding in British Columbia, while former Conservative MP and envoy to the US Congress Rob Merrifield said Canada's energy sector would be particularly vulnerable to a thicker border, given Canada's inability to sell to other markets. Embassy, Edmonton Journal

*** Manifestation contre l'importation de lait diafiltré en Montérégie**
Des producteurs laitiers de la Montérégie réunis à Delson mardi ont lancé un cri d'alarme et demandé à Ottawa de bloquer la route à l'importation de lait diafiltré. Le lait diafiltré, qui provient des États-Unis, est un lait ayant été filtré à plusieurs reprises pour obtenir un produit ultra protéiné. Au Canada, il est utilisé dans la fabrication de yogourt ou de fromage. Les producteurs laitiers qui manifestaient ont soutenu que l'importation du lait diafiltré cause des pertes partout au pays, dont en Montérégie. «Sur ma ferme, je dois perdre environ un 9000 $ à 10 000 $ par mois. Dans le fond, les coûts de production restent les mêmes, le 9000 $ à 10 000 $, c'est le profit qu'on perd», a déploré Mario Parent. Son fils Michel, qui souhaite reprendre l'entreprise familiale, ne voit également pas ces importations d'un bon il. «Si ça continue de même, il va y avoir de plus en plus de lait diafiltré qui va rentrer, alors la marge de manuvre va devenir bien plus mince», a-t-il dit dans le stationnement d'une place d'affaires de Delson, où les producteurs avaient amené des vaches pour marquer le coup. Les Producteurs de lait du Québec ont récemment réclamé une solution «rapide» et définitive au problème d'importation du lait diafiltré et des isolats de protéines laitières (IPL). L'organisation a ainsi dénoncé l'importation au pays d'ingrédients laitiers qui ne sont pas assujettis aux tarifs douaniers en raison de «failles du classement tarifaire» permettant de «contourner les limites d'importation». Agence QMI (Journal de Montréal)

*** The race is on at Cornwall's RAD**
The first couple of hundred local Grade 6 students completed a lap Tuesday of education and awareness at the 19th Racing Against Drugs. "We want the students to know five things after today," said RCMP Const. Jean Juneau, a key organizer of RAD, held at the Cornwall Armoury. "To know what a drug is; the

consequences surrounding drugs; how to say 'no'; healthy alternatives; and what is a healthy lifestyle and why is this important?" Communicating these messages were a number of organizations which staged interactive demonstrations and workshops for eight French-language schools: Cornwall Community Police Service, RCMP, Club Optimiste Club Octogone, Emergency Management Services Cornwall SDG, Canadian National Railway, Partir d'un bon pas, Ministry of Natural Resources, Ontario Provincial Police, Canada Border Services Agency, Centre de sante communautaire de l'Estrie, Eastern Ontario Health Unit and Patenaude Martial Arts. (…)Some other booths concentrated on imparting knowledge of specific participating groups, such as the work of Canada Border Services Agency officers at two separate kiosks. At one, the students learned of the many types of drugs, paraphernalia and weapons that cannot be legally brought across the border in Canada. Cornwall Standard-Freeholder (2016-04-05)

CYBER SECURITY / CYBERSÉCURITÉ

*** WhatsApp adds end-to-end encryption: Why app is showing yellow bubble to tell people information is secure**

WhatsApp has added end-to-end encryption, and announced it with a little yellow pop-up that reads: "Messages you send to this chat and calls are now secured with end-to-end encryption". But it's been much less clear about what exactly that means. The new technology is intended to ensure that messages can't be intercepted, and stay secure. While there are some concerns about exactly how private those messages are, it is a huge new development in the ongoing argument about how private our communications should be (…)The site has had a form of end-to-end encryption since the end of 2014. But it just announced that every message — not just texts, as before, but also voice calls, pictures, videos and other files, on every platform. The company said that it had done so simply to make the site more secure — by forcing itself to be unable to give up information to hackers or to oppressive governments (it didn't say which ones). Independent UK

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Calgary man claims RCMP beat him**

Elbows raining down from the police officer on top of him, Christian Duckchief's orbital bone came apart, along with his cheek and nose, his fiancée says. Chantel Stonechild said Duckchief, 23, was dragged from the house naked except for handcuffs. "They treated him worse than an animal," she said. Duckchief and Stonechild were asleep, in bed in her Siksika Nation home when Gleichen RCMP came for him Friday morning — Stonechild believes their eight-year-old daughter let the Mounties in. Calgary Sun (Canoe News, Edmonton Sun); 660 News; (2016-04-06); Calgary Herald

In mourning, community thanks RCMP

Someone else had already left flowers outside the West Shore RCMP when Bonnie Brannstrom showed up with her bouquet on Tuesday morning. The Langford woman had heard about Const. Sarah Beckett's death and couldn't stop thinking about the 32-year-old mother of two, so she drove to the detachment. "I lost my father at a young age. I know how painful it is to lose a parent," she said after leaving her flowers by the bronze sculpture - a young female Mountie kneeling beside a little girl - outside the police station. Above her, a bitter wind snapped a flag that was already lowered to half-mast. "It's senseless," Brannstrom said, her voice choked with emotion. "These officers do such a wonderful job. They don't get enough credit for what they do. All you see in the headlines is the odd one who makes a mistake." Brannstrom's sorrow was palpable. (…) Such deaths are, thankfully, rare. The last time a police officer died on duty on Vancouver Island was Sept. 28, 1991. RCMP Const. Chris Riglar was directing traffic at the scene of a fatal crash on the Trans-Canada Highway near Thetis Lake when he was struck and killed by a drunk driver. Riglar, a 37-year-old native of Nanaimo, was in full uniform, wearing a reflective vest and carrying a flashlight when he was hit from behind by a car that crossed into his lane. He was from the Colwood RCMP, now known as West Shore - the same detachment as Beckett. Times Colonist, A3

Un employé voit son licenciement annulé
Est-ce le prélude à un changement des mœurs au sein de la police ? Un tribunal du travail fédéral vient d'annuler le licenciement d'un employé civil de la Gendarmerie royale du Canada (GRC) qui s'était vu montrer la porte parce qu'il fumait occasionnellement du cannabis. « Pour être content, je suis content ! J'ai vraiment vécu ça comme si l'employeur voulait juste se débarrasser d'un employé de plus », a commenté David Féthière lorsque joint par La Presse hier. Jusqu'à son licenciement, M. Féthière travaillait comme commis au sein de l'unité d'enquête sur les fraudes par télémarketing de Montréal : son rôle en était un de soutien administratif aux policiers. Il transcrivait leurs entrevues, tenait les dossiers à jour, entrait des données dans le système informatique... Le sergent-major de son équipe, Jacques Rainville, avait organisé une fête chez lui, au bord d'un lac. En plus des employés de la GRC, il avait invité ses voisins ainsi que des policiers de la Sûreté du Québec et du Service de police de la Ville de Montréal (SPVM). David Féthière a trop bu ce jour-là, de l'avis de tous. Ivre, il a demandé à son patron s'il pouvait fumer un joint. Il a évidemment essuyé un refus catégorique et irrité de la part du policier. Le commis s'est ensuite essayé avec une autre policière et a essuyé un nouveau refus. Il est finalement allé fumer seul, à l'écart, mais serait revenu en traînant l'odeur distinctive du cannabis... L'incident est tout de même pris au sérieux. Dès le lundi, le sergent-major de l'équipe rédige un rapport, et deux procédures sont mises en branle : une enquête disciplinaire, qui mènera à une sanction de 10 jours de suspension pour le fonctionnaire, mais aussi une enquête de sécurité, pour déterminer s'il peut conserver sa cote de fiabilité, essentielle pour avoir accès aux locaux et aux informations de la GRC. La Presse, 9

* **Bullet hole found at station**
Police are investigating after a bullet hole was discovered in a window of the Surrey RCMP's Guildford station. According to Cpl. Scotty Schumann, the bullet hole, about the size of a quarter, was discovered Tuesday morning by a maintenance worker. Schumann said the hole does not seem fresh and it's not known exactly when the damage was caused. The discovery follows a recent string of shootings in Surrey. So far this year, there have been 31 shootings in Surrey. Province, A12

* **Variety of topics covered during student research day**
The 14th Annual Student Research Day at St. F.X. took place March 24 at the conference rooms in the Keating Centre and, as has been the case with all previous years, a variety of fascinating topics were explored by students who were on-hand to talk about their work. Amongst the many, Courtney Campbell, a BSc. human nutrition with honours student, displayed a project with the long title of The Lipid Composition of Pastured Eggs from Wild Orchid Farms Versus Conventional Eggs in Antigonish. She noted the local farm (North Grant) contacted the university and that set her research in motion. "We were contacted by the farmer actually and she wanted to know more information about her eggs so she could provide more information for her consumers," Campbell said. "So when people asked what was different about her eggs she could provide more information on that." Campbell talked about a finding. "The eggs from Wild Orchid Farm actually have more oleic acid," she said. "Oleic acid is omega-6 which is something that is always advertised on the market, so I thought it was a very good thing these free range eggs - these pastured eggs - had the more abundant omega-6." Emma van Reekum's research dealt with post-traumatic stress disorder (PTSD) with Canadian veterans and RCMP. She noted the research she was displaying was still a work-in-progress. "I only have pre-intervention data ... my thesis is going to evaluate the ethicacy of interpersonal group process for Canadian veterans and RCMP officers with PTSD," she said. " Chronicle-Herald, L3

* **Advocacy centre will bring people together to combat child abuse**
Former NHLer Sheldon Kennedy plans to help set up a child advocacy centre in Red Deer. Kennedy, lead director of the Calgary-based advocacy centre that bears his name, was in Red Deer on Tuesday to deliver the keynote speech at the Alberta Common Ground Alliance's Dig Safe Conference. Since Kennedy brought to light the sex crimes of former junior hockey coach Graham James, he has become a tireless advocate for children who have suffered abuse or who are at risk. His centre pulls together numerous government agencies, police forces and others in a collaborative model for investigating and treating child abuse. About 125 investigations a month are handled through the centre. Mayor Tara Veer, who joined Kennedy at an event to promote Dig Safe on Tuesday morning, said a group of local concerned citizens have applied for funding to establish a Central Alberta version of the centre. "We're working as an affiliate of the Calgary centre," said Veer, who said more details about the plans are

expected in June. Red Deer city council was joined by Central Alberta mayors and MLAs for a tour of the advocacy centre earlier this year. (...) The centre has been a celebrated success. It has 120 employees, including RCMP, 30 social workers, 25 child psychologists, pediatricians, as well as the entire Calgary Police Service child abuse unit. In his conference address, Kennedy focused on the importance of speaking up - a message that can be applied to victims of abuse, but also in the workplace when unsafe practices may be happening. Red Deer Advocate, A1, A8

* **No ink needed for new fingerprint machine**
The Fredericton Police Force has a new high-tech electronic fingerprint machine and the days of taking old fashioned ink and paper fingerprint records are gone forever. You slide your hand into the machine, it takes a picture of your fingerprints, makes sure the prints are clear, and the results can be sent to the RCMP crime data base in Ottawa at the push of a button. The machine is called LiveScan and it, and the licence to operate it cost Fredericton $36,000, the city's public safety committee was told Tuesday. "We consider this a definite business improvement," April Doyle, assistant manager of administrative support at the Fredericton Police Force, told the committee. "It has quality control, it has time savings and efficiencies for officers." "It actually tells you if you have a good print. There is an opportunity to retake it again if it's not good." The electronic fingerprint system integrates with the city's electronic mug shot system and all the images can be viewed on police desktop computers and the laptops in patrol cars, she said. In 2015 Fredericton police took 552 sets of fingerprints using ink and paper, said Doyle. But those fingerprints use to sit around for a month or two at the police station until they were mailed to the RCMP, she said. Using the new LiveScan machine, the police have already processed 110 sets of fingerprints and sent them to Ottawa in the first two months of 2016, she said. Daily Gleaner, B3

* **Police crack down on fentanyl**
Fentanyl, marijuana, cocaine and a substance believed to be heroin were seized as an RCMP federal investigations unit carried out six drug raids Monday. "It's a significant seizure," said RCMP spokesperson Const. Elenore Sturko in a brief interview Tuesday, adding police were still going through what was seized to calculate total quantities. Police arrested 14 people after carrying out the search warrants in Yellowknife, Ndilo and Dettah. They seized what is described as "a significant quantity of illicit drugs and cash," according to a news release from Sturko. Charges were expected to be laid Tuesday afternoon, Sturko said, but no further information was available at press time. No names have been released so far. The busts came at the end of what Sturko stated was a "lengthy investigation targeted the trafficking of fentanyl and other illicit drugs in Yellowknife and surrounding communities." Approximately 1,000 fentanyl pills were seized. (...) Monday's raids began with a vehicle en route to Yellowknife from B.C. that was stopped near Fort Providence where a man was arrested. The searches at six separate sites in the three communities were then carried out Monday evening. The warrants were carried out concurrently to ensure they could make arrests at the same time. More than 30 RCMP officers were involved in the operation, the news release states. Yellowknifer

* **Man dies after crashing into Rogersville home**
A man is dead after a driver who refused to stop for police crashed into a house in Rogersville Monday night. Sgt. Pat Tardif of Southeast RCMP confirmed Tuesday that a car left Route 126, the main road through the village, shortly after 8 p.m. Monday and crashed into a home that was occupied at the time. No one was in the part of the home that was struck by the car, however. The vehicle caused significant damage, coming to a stop with only a bit of the back end of the car protruding from the building. Tardif identified the victim as a 23-year-old man from Alberta. The officer said a Mountie on patrol tried to pull over the vehicle at approximately 8:15 p.m. on Route 126 in the village but the driver sped away. "The police officer followed the vehicle briefly, but stopped when the suspect's vehicle accelerated to excessive speeds, in the interest of the safety of the public and the police officer," Tardif said in a news release issued Tuesday afternoon. "A few minutes later, police received a report that the suspect's vehicle had collided with a power pole then crashed into a house on Route 126. The driver died at the scene." Telegraph-Journal, A3 (Times & Transcript); Canadian Press (Guardian, A8); Acadie-Nouvelle, 5

* **'They're becoming quite defiant'**
A veteran Yellowknife security contractor, who has been in the business for a quarter-century in the city, said he has recently noticed a dramatic change for the worse in behaviour from the city's downtown

population. Brian Carter said homeless people have become more bold now that it is known RCMP may not arrest them for being intoxicated in public. The change in policy came last fall after police announced it would only take intoxicated people to RCMP cells if there was a public safety threat. RCMP explained at the time that policy change came, in part, as an effort to shift police resources to other areas, such as drunk driving and drug investigations. An access-to-information request later revealed, however, RCMP are also concerned about complaints resulting from picking up intoxicated people that lead to public inquiries and internal investigations. Yellowknifer

Police find duffel bag of weapons, arrest two boys near Sackville school
It may have been "a drug deal gone wrong" that led to a Middle Sackville high school going into lockdown mode Tuesday. That was the suggestion being passed among students via text messages as police investigators scoured classrooms and hallways inside Millwood High School and RCMP patrol cars cruised surrounding neighbourhoods. Nearby Millwood Elementary School was put into "hold and secure" mode during the search. "We started getting texts from my friends saying that it was a drug deal gone wrong," Grade 12 student Alex Billard, 17, said following the lunch hour scare. "A fight, weapons," he said of what students had been hearing. "I don't think there was anyone injured and ... two people are in custody.'" Police responded to the weapons complaint at Millwood High shortly before noon, Halifax RCMP spokeswoman Cpl. Jennifer Clarke confirmed. Cape Breton Post; * Cape Breton Post; * Chronicle-Herald, A1; * Canadian Press (Guardian, A8, Telegram)

*** Nunavut's polar bear problem growing in Hudson Bay communities**
The hamlet of Chesterfield Inlet, Nunavut, says it has a serious polar bear problem and is looking for help by reaching out to other coastal communities along Hudson Bay. Last week representatives from the hamlet attended a workshop in Churchill, Man., to learn from experts on polar-bear human conflicts. This was the first time that people from Nunavut, northern Manitoba and northern Quebec came together to address this issue. Chesterfield Inlet is on the migration route of polar bears who travel along the western coast of Hudson Bay. Barnie Aggark, mayor and the chair of the local hunters and trappers organization, says each day three to five bears are spotted near the community. A few even walk into town. "There was just one three weeks ago that was looking in through the windows of a couple of homes, going into porches, the back of the pick-up trucks," said Aggark. "It's kind of tense, especially at night when the kids are heading home."... Chesterfield Inlet is now hoping to get money for a polar bear patrol and the tools needed for the job. "Right up to ice freeze-up we have quite a few polar bears come by our community and we don't really have paid bear watchers," said Aggark. For now it's up to local hunters, the conservation officer as well as the local RCMP to help keep the bears out of town. CBC News

*** Surrey RCMP investigate fourth shooting in four days**
Surrey RCMP are investigating a targeted shooting that sent one man to hospital Tuesday evening. The shooting happened around 11:10 p.m., near a home in the 7700 block of 155th Street. When officers arrived, they found an injured man who was later transported to hospital in stable condition. This incident marks the fourth shooting in Surrey in just four days. CBC News

*** Man with knife sparks lockdown at Nanaimo school**
Woodlands High School was locked down Tuesday morning while Nanaimo RCMP officers searched for a man armed with a knife. At 9:20 a.m., police received reports that a man was trying to use a stolen credit card at Home Hardware in the Brooks Landing Mall. When employees confronted him, the man pulled out a knife and ran away. Because the incident was so close to the high school, it was locked down. Officers and a police dog tracked the man for 10 minutes. A 32-year-old man was arrested behind a home on Giggleswick Drive. He was bitten several times by the police dog and was taken to hospital for treatment of his bites. The man faces charges of possession of a dangerous weapon, breach of probation and fraudulent use of a credit card. The investigation is continuing, said Nanaimo RCMP Const. Gary O'Brien. Times Colonist (2016-04-05)

Québec élargit le mandat du SPVM à toute la province
Le Service de police de la ville de Montréal (SPVM) pourra désormais enquêter sur toutes les plaintes criminelles de femmes autochtones contre tous les corps policiers du Québec, partout dans la province, a annoncé le gouvernement québécois mardi. L'automne dernier, un reportage troublant de Radio-Canada

avait mis en lumière des allégations graves d'agressions sexuelles et d'abus de pouvoir qui auraient été commis par des policiers de la Sûreté du Québec (SQ) contre des femmes autochtones à Val-d'Or. Québec avait mandaté le SPVM pour mener l'enquête sur la SQ. Mardi, le gouvernement québécois a annoncé qu'il élargit le mandat du SPVM en lui donnant tout le territoire du Québec et les agents de tous les corps policiers, si ceux-ci sont accusés de gestes inadmissibles de nature criminelle envers les femmes autochtones. De plus, toutes les enquêtes actuellement menées par la Sûreté du Québec (SQ) à ce sujet seront transférées au SPVM - sauf lorsque le SPVM est visé, évidemment, a fait savoir en conférence de presse le ministre de la Sécurité publique, Martin Coiteux. Québec ajoute aussi une ressource pour les femmes autochtones qui veulent dénoncer des policiers: une nouvelle ligne téléphonique sera à leur disposition. Elle sera gérée par l'organisme Services parajudiciaires autochtones du Québec qui reçoit aussi pour mandat de les accompagner dans leur processus de dénonciation auprès du SPVM. Des membres de l'organisme les dirigeront ensuite vers le centre d'aide aux victimes d'actes criminels (CAVAC) où elles pourront recevoir des soins et de l'aide. Une ligne téléphonique existait déjà pour elles auprès du SPVM, mais cette «seconde porte d'entrée» peut être nécessaire pour celles qui hésitent à dénoncer un policier à un autre policier, reconnaît M. Coiteux. La Presse Canadienne (Le Droit, 37, Voix de l'Est, Le Devoir); 1

*** Police body cameras show promise, but raise questions**

As Canadian police forces complete pilot projects assessing whether officers will wear video cameras on their uniforms, experts in both civil rights and policing say they see value in the practice but urge proceeding with caution. "The 'how' is extremely important," Laura Berger, acting director of the public safety program at the Canadian Civil Liberties Association, told CBC News. "This an area where the devil is absolutely in the details." The Toronto Police Service wrapped up the 10-month test phase of a pilot project that equipped about 100 officers with body-worn cameras on March 31. The evaluation process is expected to be completed by June 30, police spokesman Mark Pugash said.The idea of using body-worn video cameras gained momentum in the U.S. and Canada over the last few years amid concerns from both the public and the police about use of force and misconduct allegations. In 2014, U.S. President Barack Obama pledged millions of dollars for 50,000 body cameras to be distributed to police departments across the country. In Canada, Calgary is the city closest to outfitting all of its front-line uniformed police officers with the cameras - something the police force has announced it will do by 2017. "This is the future," said Kevin Brookman, spokesman for the Calgary Police Service, told CBC News. "Everybody from, you know, elementary school right up to adults have smartphones or cameras. How is it that a policing agency in the ... 21st century has no capability of recording what we're doing?" CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Dangerous offender won't be released

A serial spouse batterer serving an indeterminate prison sentence isn't ready for release into the community, the Parole Board of Canada has decided. James Richard Standingwater, 43, was declared a dangerous offender and sent to prison indefinitely in 2010, following his latest convictions for beating and confining his wife on the Thunderchild First Nation. An indeterminate sentence still carries with it a chance for parole. However, while Standingwater has made gains during his incarceration, his risk for violent reoffending is too high to make day parole feasible, the parole board found. Standingwater's criminal record includes 10 serious assaults against his common-law wife, including a horrific incident in 2005 when he broke into her home - while on court-ordered conditions to have no contact with her - and "hit and punched her, pushed her head into a wall, pulled her hair, pulled her around, dragged her down wooden steps and outside, kicked her in the chest, head and face with hard boots, and then choked her until she lost consciousness," according to the parole board decision. StarPhoenix, A3

*** Tobby Carrier : pas de décision cette semaine de la Cour suprême**

La Cour suprême ne décidera pas cette semaine si elle entendra l'appel de la Couronne dans l'affaire Tobby Carrier. La décision a été reportée. La Cour suprême devait annoncer jeudi si elle acceptait de revoir la décision de la Cour d'appel qui avait ordonné la tenue d'un nouveau procès en juillet dernier. Tobby Carrier, de Matane, a été reconnu coupable du meurtre non prémédité de son frère, Ismaël, et de tentative de meurtre sur ses parents, Nelson Carrier et Chantal Michaud, en mars 2009. Benjamin d'une

famille de trois garçons, Tobby Carrier avait 19 ans au moment des faits. Il a été condamné à la prison à perpétuité avec un minimum de 14 ans de détention avant une possible libération conditionnelle en février 2013. En juillet dernier, la Cour d'appel du Québec a annulé les verdicts de culpabilité, dont celui de meurtre au deuxième degré, ainsi que la peine d'emprisonnement à perpétuité prononcés à l'endroit du Matanais Tobby Carrier en 2013. (…) Tobby Carrier qui est détenu à la prison de Port-Cartier devait revenir en cour, à Rimouski, le 12 avril prochain, pour connaître, si tel était le cas, la date de son nouveau procès. Radio-Canada

Dennis Oland demeure incarcéré
La Cour d'appel du N.-B. a rejeté pour une deuxième fois la demande de libération sous caution de Dennis Oland, qui contestera en octobre le verdict de culpabilité prononcé contre lui pour le meurtre non prémédité de son père. Dans une décision écrite rendue publique lundi, un comité de trois juges de la Cour d'appel, dont le juge en chef, confirme ainsi la décision d'un juge du même tribunal rendue en février. Dennis Oland, âgé de 48 ans, avait été condamné le 11 février à la prison à perpétuité, sans possibilité de libération conditionnelle avant 10 ans, pour le meurtre de son père, l'homme d'affaires Richard Oland, commis en juillet 2011. Il est extrêmement rare au Canada qu'un condamné pour meurtre - même non prémédité - obtienne sa libération sous caution en attendant l'audition de son appel. Presse canadienne (Acadie Nouvelle, 2)

* **Man who killed Calgary doctor granted day parole**
The man convicted in the shocking murder of a Calgary doctor more than two decades ago has been granted day parole. The silence of a mid-September 1992 night was broken by the sounds of a break-in. It awoke Dr. Geoffrey Cragg, who chased the offender down the stairs. During an ensuing struggle, Sheldon Klatt stabbed the 45-year-old several times, with Cragg's wife and four kids looking on. Klatt was convicted of second-degree murder and sentenced to life in prison. He was granted several unescorted passes in 2014. And in documents obtained by News Talk 770, the Parole Board of Canada granted the now-46-year-old day parole this past March 16th, which will be reviewed in six months. News i880 AM (2016-04-05)

* **25 mois de prison pour avoir publié une image intime de son ex-conjointe**
C'est parce qu'il «voulait récupérer son chien et la bague laissée en héritage par son père» que Shane-Charles Macintosh a publié une image intime de son ancienne conjointe sur les réseaux sociaux, en plus de trouver un moyen particulier pour que cette dernière se fasse harceler. Cela lui a valu une peine d'emprisonnement de 25 mois, de laquelle a été retranchée la période de détention provisoire, ce qui veut dire qu'à compter d'aujourd'hui, il lui reste une peine de 14 mois à purger. Au début de 2015, Macintosh, qui s'est déjà fait «connaître» par le passé pour avoir entretenu une relation amoureuse avec une agente des libérations conditionnelles pendant qu'il était détenu au pénitencier de Donnacona, a rencontré Chantal (prénom fictif), de qui il est tombé amoureux. Radio-Canada (2016-04-05)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

* **The 'inward emptiness' of social media**
An editorial states, "In 1925, English novelist and outcast Virginia Woolf wrote about what happens to a person when she spends her entire life trying to fit in. "Once conform, once do what other people do because they do it," Woolf wrote in The Common Reader, a collection of essays, "and a lethargy steals over all the finer nerves and faculties of the soul. She becomes all outer show and inward emptiness; dull, callous and indifferent." (…) For proof, look no further than the University Of Pittsburgh School Of Medicine, where researchers recently determined via a large study (the first of its kind in the United States) that social media use is "significantly associated with increased depression." The study, conducted in 2014 and published this year, sampled nearly 1,800 American millennials - 19 to 32 years old - and concluded that more than a quarter had high indicators of depression. (…) And what do you know: Those who used social media most frequently were 2.7 times more likely to be depressed than their less-active peers. This result surprised the researchers. "We had expected a U-shaped curve, with a higher risk of depression being correlated with no social media use at all or excessive use," says Dr.

Brian Primack, senior author of the study and director of the University of Pittsburgh Center for Research on Media, Technology and Health. (…) Primack suggests the usual suspects: "Highly idealized representations of peers on social media may elicit feelings of envy and the distorted belief that others lead happier, more successful lives." There's also cyberbullying, he says (though it is much less prevalent among adults), "and other similar negative reactions."" Toronto Star, A7

*** Pas un geste «haineux»**

«Je ne suis pas raciste.» L'un des individus accusés de voies de fait contre un sikh de la région de Toronto en visite à Québec pendant la fin de semaine de Pâques se défend d'avoir commis un geste «haineux». Gabriel Royer Tremblay, 21 ans, n'essaie pas «d'excuser son geste», écrit-il lors d'un échange réalisé mardi avec Le Soleil. «J'ai énormément honte de moi en ce moment, car c'est en voyant la vidéo comme tout le monde que j'ai pris conscience de ce qui s'est passé.» Cependant, il refuse de passer pour raciste. Une étiquette qui «l'écoeure au plus haut point». (…)Les images de la vidéo ont circulé dans tout le pays après la diffusion d'un reportage par CTV News. L'affaire a pris des proportions politiques lorsque le premier ministre du Canada, Justin Trudeau, et la ministre de l'Immigration du Québec, Catherine Weil, eurent dénoncé ce geste «d'intolérance», vendredi, à la lumière des informations disponibles à ce moment. Le plaignant dans cette histoire, Supninder Singh Khehra, a raconté au journaliste de la chaîne anglaise qu'il cherchait un taxi lorsque des individus l'ont attaqué vers 3h45 dans la nuit du 26 mars près du parc de la Francophonie, rue D'Artigny. «C'était surtout des insultes en français, mais ils disaient également certains mots anglais», raconte l'homme lors de l'entrevue. «Ils pointaient ma tête, mon turban.» (…) Mardi après-midi, la police de Québec a corroboré, en partie, les témoignages obtenus par Le Soleil. Par voie de communiqué, elle a dit rejeter l'idée que l'agression sur M. Khehra «ciblait une communauté religieuse spécifiquement». L'enquête de la police démontre «qu'un des suspects avait été impliqué dans deux autres événements auparavant» sans que des accusations ne soient portées, explique l'agente Marie-Eve Painchaud. Question d'enlever un peu de pression médiatique sur la question du crime racial, la police souligne qu'étant donné la «concentration élevée de gens sous l'influence de l'alcool dans ce secteur, un plan d'action en partenariat avec les tenanciers de bars a été mis en place en 2014 pour réduire les incivilités et comportements inappropriés, qui ont chuté de 42 % depuis.» Le Soleil, 3

*** Deux fois plus d'agressions sexuelles rapportées à Gatineau**

L'activité criminelle est demeurée stable en 2015, à Gatineau, si ce n'est qu'une légère hausse de 1% par rapport à l'année passée. Une donnée détonne cependant plus que les autres dans le bilan annuel des activités policières de Gatineau présenté mardi en comité plénier. Le nombre d'agressions sexuelles rapportées a bondi de 40% dans la seule dernière année. Un total de 245 personnes derrière ces statistiques ont choisi de dénoncer leur agresseur à la police de Gatineau. Le chef du Service de police de la Ville de Gatineau (SPVG), Mario Harel, affirme que la situation a même obligé la direction à changer les affectations de certains enquêteurs afin de faire face à cette croissance imprévue. «Il y a eu en 2015 le même nombre de cas d'agression sexuelle qu'habituellement dans une année, par contre plusieurs victimes sont venues pour des cas provenant du passé, précise-t-il. On avait vécu la même chose quand il y avait eu l'histoire de Nathalie Simard. Il y a des phénomènes qui font que les gens viennent dénoncer, même si c'est une vieille histoire et c'est exactement ce qu'on souhaite que les gens fassent.» (…) L'une des grandes préoccupations pour le SPVG dans les années à venir sera la cybercriminalité qui oblige les forces de l'ordre de partout à revoir leurs façons de faire. «On patrouille sur le terrain, mais maintenant nous avons aussi un monde virtuel à patrouiller et où les gens sont aussi victimes d'actes criminels, explique M. Harel. C'est un défi et nous devrons nous organiser pour répondre là aussi aux besoins des gens.» La Presse, Zone 911 (2016-04-05)

*** Surrey violence: NDP MLAs demand "immediate and effective action" from Clark government**

NDP Surrey MLAs Harry Bains, Sue Hammell and Bruce Ralston on Tuesday demanded "immediate and effective action" from the Christy Clark government in light of the escalating violence in Surrey. They said in a statement: "There were too many shootings in Surrey last year, and this year we're seeing more than double the number. In 2015, there were 60 shootings in Surrey, and as of yesterday the 2016 count is at 31, several of which were in broad daylight and near school grounds. "What's even more worrying is the fact that there is currently no effective strategy in place from the Christy Clark government to reduce and eliminate gun violence in Surrey. Children and families are feeling terrorized, and many are too scared to

leave their home in the evening. “People in Surrey deserve to feel safe, they deserve real and immediate solutions to the violence their communities are facing, and they deserve better than the lack of support that they are getting from the Christy Clark government.” Voice Online (2016-04-05)

*** Opioid related deaths on the rise in Ottawa**
Health care professionals are raising the alarm as opioid related deaths continue to rise in Ottawa. Data obtained by the Ontario Coroner's Office shows 26 people died in Ottawa in 2014 due to opioid related deaths compared to 16 in 2012. Two highly addictive prescription painkillers, Fentanyl and Morphine, were the most dangerous drugs in 2014. Both accounted for nine deaths. "We definitely, over the past year have received reports from clients and other harm reduction partners about the increased use of fentanyl in the city," said Kira Mandryk the supervisor of Ottawa Public Health's harm reduction unit. In addition to a rise in fentanyl use Ottawa Public Health is seeing powdered fentanyl on the streets for the first time. It's a more potent and dangerous version of the narcotic. CTV News (2016-04-05)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

*** UNB honours residential school survivors with traditional powwow**
Driving past the large farm field just outside Indian Brook First Nation, Ashley Julian says you'd never know the piece of land was home to Shubenacadie Indian Residential School, where her mother resided for six years. "It's not something many residential school survivors talk about," said Julian, who grew up in the First Nation community in Nova Scotia. (…)To celebrate their lives and what they've been through, Julian will be taking part in the University of New Brunswick's second annual powwow, Dancing Towards Reconciliation, where she will be performing the womens' fancy shawl dance, a modern powwow dance. The powwow aims to emphasize the importance of working towards implementing the Truth and Reconciliation Commission's recommendations and calls to action, a 386-page report that aims to help residential school survivors heal and reconcile. Some residential school survivors are expected to attend this year's event. (…) The event will also honour missing and murdered aboriginal women, another topic that hits close to home for Julian, whose aunt, Anna Mae Pictou Aquash, was killed in 1976 in South Dakota. She was a leader in the American Indian Movement, an advocacy group for Native American civil rights. Daily Gleaner,

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Marijuana**
An opinion piece states, “New Brunswick's acting Chief Medical Officer of Health Dr. Jennifer Russell related in a news story Monday how she is doing necessary research into what sort of regulations ought to be required once Ottawa legalizes marijuana. Her work, which will involve talking to authorities in other jurisdictions where 'pot' is already legal, her counterparts across Canada, and consultation with other relevant groups, reports and studies is necessary if the provincial government is to make wise decisions. It needs the best information it can get. It's also crucial because there are so few places that have legalized marijuana. Experience elsewhere is extremely limited. Canada, including New Brunswick, is blazing new trails. But we're getting hints that pot legalization could become hotly debated, creating political headaches for Ottawa and the provinces. But ironically, such controversy would arise from the devilish details, not legalization itself. The Liberal election promise proved highly popular and remains so. Marijuana is not totally harmless, but it's way down the list and less risky than alcohol. Criminalizing people for use, possession, sale and growing the drug - an effort that costs more than $1 billion annually in Canada - makes no sense. (…) And while Ottawa's legislation hasn't been released yet, New Brunswick just assisted the producer with almost $1 million to enable it to expand. But the same government is showing signs of simultaneously riding off in opposite directions at once. It wants the taxes, profits and jobs but Public Safety Minister Stephen Horsman also says he favours a 'legal age' for marijuana of 21.” Times & Transcript, A8

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Millennials and the PS**
A editorial states, **"**The Treasury Board president wants to hire more millennials, pumping new blood into the public service and ushering in a golden age. But it raises the rather large question: How?Scott Brison argues that hiring millennials is a twofold boon to the public service. First, the greying of the public service presents a long-term logistical problem. The average age of new hires is 37. Second, the government needs people to step up with new approaches as others retire. Millennials would bring in new skills and diverse values. Sounds reasonable. But what do young people actually want from their employer? According to numerous studies and surveys, millennials seek meaningful work, less hierarchy, fewer rules, flexible work schedules, support for risk-taking and so on. Many young people want to make a difference in the world. Brison says government is where people can really move the needle. This can be done, he says, if government gives them the tools to do that. Can he and the public service actually offer this? And if they can, should they? Government is cumbersome to reform. So far, there doesn't seem to be a clear plan to make the public service more millennial-friendly (which can't be a straightforward process). So Brison has a lot of work ahead. It means, fundamentally, making the government as attractive a place to work as tech start-ups or change-the-world NGOs. This is a tall order, especially when briefing documents suggest there are too many decision-making layers and a toxic work environment in the bureaucracy." Vancouver Sun

* **Forging provincial consensus on CPP reform easier said than done**
Unless there is a breakthrough at a June meeting of finance ministers, pension reform may become the biggest Liberal election promise that never comes to pass. On April 19, if the polls can be trusted, Progressive Conservative Leader Brian Pallister will win the Manitoba election, further dimming the Trudeau government's hopes for pension reform. Unless there is a breakthrough at a June meeting of finance ministers - which is possible but shading toward unlikely - pension reform may become the biggest Liberal election promise that never comes to pass - a depressing prospect for those in need of help with their retirement. "Confused," is how Keith Ambachtsheer, director emeritus of the Rotman International Centre for Pension Management at University of Toronto, describes the state of play between Ottawa and the provinces on bolstering the Canada Pension Plan. Although the election platform promised to "work with the provinces and territories, workers, employers and retiree organizations to enhance the Canada Pension Plan," and last month's budget set a "goal of being able to make a collective decision before the end of 2016," getting the required consent of seven provinces representing two-thirds of the population is proving elusive. Globe and Mail

OTHER / AUTRE

* **The first casualty: Iceland's PM resigns after secret offshore firm is exposed by document leak that's igniting a global firestorm**
Within 48 hours, the largest leak of confidential documents in history has shaken the foundations of power around the world, triggering the resignation of Iceland's prime minister and sending political shock waves from Pakistan to Argentina to Ukraine. Prime Minister Sigmundur David Gunnlaugsson relented to withering public pressure Tuesday, stepping down as Iceland's leader one day after thousands gathered outside parliament in protest over revelations he held a secret offshore company. (…) The files contain evidence of offshore companies controlled by the presidents of Argentina and Ukraine, and the King of Saudi Arabia. They also include 128 other politicians and public officials, and at least 33 people and companies blacklisted by the U.S. government because of evidence they've done business with Mexican drug lords, terrorist organizations such as Hezbollah or pariah nations such as North Korea and Iran. (…) The Canada Revenue Agency issued a statement in response to the investigation, saying that it "continues to pursue audits related to offshore tax evasion including some Canadian clients associated with law firm Mossack Fonseca." (…) On Tuesday, information contained in the leak prompted France to put Panama back on its "black list" of tax havens, which puts a withholding tax on financial transactions

between the countries. Panama had been taken off the list in 2012. Here are some leaders whose secret offshore financial dealings have come under scrutiny. Toronto Star, A1

*** Arms deal by Canadian firm raises issues about Ottawa oversight**
A new UN panel report says a shipment of armoured personnel carriers to Libya from a Canadian-owned company's Mideast facilities several years ago violated an international arms embargo - an incident that raises questions about how extensively Ottawa should be policing the defence and military trade conducted by its citizens abroad. The March 2016 report, which flagged a transfer of armoured vehicles produced by Streit Group, a company first established in Ontario in the 1990s, was drawn up by experts monitoring global compliance with the United Nations Security Council arms embargo against Libya in place since 2011. Streit is owned by Guerman Goutorov, a Canadian citizen who lives in the United Arab Emirates. His Canadian-based company is Streit Manufacturing in Innisfil, Ont. The UN panel's reporting on what it calls an "illicit transfer" of armoured personnel carriers comes amid a growing debate in Canada over the military and defence goods that Canadians sell to Mideast countries - including a $15-billion deal with Saudi Arabia - and increasing concern that Ottawa is not doing enough to monitor, control and shine a light on this flourishing business. Libya has been engulfed in civil war since dictator Moammar Gadhafi lost power in 2011. The top U.S. general in Africa last month described Libya as a "failed state." Globe and Mail, A1

*** Canadiens condamnés pour des liens avec le Hezbollah**
Un tribunal des Émirats arabes unis a condamné «un groupe composé d'Arabes et de Canadiens» à six mois de prison pour leurs liens présumés avec le Hezbollah libanais. Selon l'agence de presse officielle du pays, les personnes condamnées lundi seront plus tard déportées. Ni l'identité ni le nombre des inculpés n'a été précisé. Affaires mondiales Canada, à Ottawa, n'avait toujours pas commenté mardi. Ni les autorités libanaises ni le Hezbollah n'ont voulu non plus commenter l'affaire. Le Hezbollah, soutenu par l'Iran (chiite), est de plus en plus contesté dans le golfe Persique, notamment par l'Arabie Saoudite (sunnite wahhabite). Associated Press (le Soleil, 22); Journal de Montreal, 27 (Journal de Quebec)

INTERNATIONAL

*** West should adopt Israeli security systems to stay safe**
An opinion piece states "When it comes to airport security, Israel is regarded as the gold standard. On a daily basis, Israel is forced to deal with strategic, tactical and existential terror threats, while facing constant scrutiny from the international community and our media for efforts that every nation is obligated to take to ensure the safety of its citizenry. Given the tragedies that have taken place in Paris and Brussels, the world searches to find answers as to why individuals would commit such atrocious and ghastly acts of violence against innocents. (…) Cameras with constant surveyors keep a close watch on any suspicious activity. Before entering the terminal, another checkpoint has security guards who analyze and inspect passersby in an attempt to draw any sort of suspicion a terrorist might conceal." Province, A14

*** Kim Jong-il's ex-bodyguard seeks asylum**
For more than a decade, Lee Young-guk was a bodyguard for the man who would go on to become one of the world's most brutal dictators. After a failed attempt to flee North Korea in 1994, when the Communist regime rewarded a smuggler in China for forcibly returning him to Pyongyang, Lee finally escaped to South Korea where he became a citizen - and a vocal critic of his former boss, Kim Jong-il. Now, Lee is on the run again. On March 13, the now-53-year-old arrived in Toronto with his wife and two young children. He once again became an asylum seeker, this time fleeing what he claims are threats and persecution by South Korea for his outspoken criticism of their neighbour to the north. "I was arrested in a demonstration. Police beat me and tortured me. They released me but continued to follow me and threaten me," said Lee, who changed his name to Lee Young-dae after his defection to Seoul. "They are very sensitive to any criticism against the North. I feared they would send me back to Pyongyang," said Lee. Kim Jong-il ruled North Korea with an iron fist, with thousands imprisoned, tortured or dying of starvation during his 17-year reign that ended when he died of an apparent heart attack in 2011. Waterloo Regional Record, B6

*** What would a Syrian peace deal look like?**

After the Syrian army recaptured the city of Palmyra from Islamic State a week ago, United States State Department spokesman John Kirby admitted that the liberation of the ancient city was a "good thing." But he could not resist adding: "We're also mindful, of course, that the best hope for Syria and the Syrian people is not an expansion of [President] Bashar al-Assad's ability to tyrannize the Syrian people." This was entirely in line with the long-standing US policy of seeking to destroy both Islamic State (also known as ISIS, ISIL and Daesh) and the Syrian government (i.e. the Assad regime) at the same time. But that was never more than wishful thinking, especially as the United States was quite sensibly determined not to commit its own ground troops to the conflict. If the Syrian army actually had collapsed (as was looking quite likely before the Russians intervened to save it last September), nothing could have prevented Islamic State and the rival Islamist forces of the Nusra Front from taking the whole country. They might then have fought each other for control, but all of Syria would have ended up under extreme Islamist rule. Hill Times (Embassy)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
April 8, 2016 / le 8 avril 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Oil spill fears remain one year after bunker fuel fouled Vancouver beaches**
When the MV Marathassa leaked at least 2,700 litres of bunker fuel into Vancouver's harbour one year ago, the effects of the spill reached far beyond the city's picturesque waters and beaches. Delays in clean-up and notification of the city sparked public outrage, drew attention to Conservative cuts to the Canadian Coast Guard and prompted a flurry of campaign promises from the New Democrats and Liberals. The miscommunication and uncertainty of roles that caused the delays were revealed months later in an independent report, which made a number of recommendations that the coast guard says it is implementing. But city manager Sadhu Johnston says despite improvements made by the federal government including reopening the Kitsilano coast guard base and working toward a regional response

plan fears about oil spills still loom large. "Not a ton has changed since last year," he said. "There's been planning and engagement together, but we're still not there yet. We're still not ready for a major tanker spill in this region." The spill on April 8, 2015, while relatively small, happened when concerns were running high in Vancouver about increased tanker traffic that would be caused by Kinder Morgan's proposed Trans Mountain pipeline expansion. St. John's Telegram

*** Wildfire hazard high near Rocky**
The wildfire hazard was raised to high in the Rocky Mountain House Forest Area on Thursday. Existing permits have been cancelled and no new fire permits will be issued. Safe campfires are still allowed. A wildfire advisory for the Rocky forest will remain in effect until conditions improve. As of Thursday afternoon, the Rocky forest had three smaller wildfires burning, all under control. The cause of these fires is still under investigation. Across Alberta, in the 24 hours to Thursday afternoon, there were four new wildfires. Red Deer Advocate, A3

*** River 'finds a way' - Renfrew landslide left lasting damage**
The floodwaters and debris have receded in Horton Township near Renfrew, but Steve Osipenko hasn't forgotten the frightening speed of last week's massive landslide, and the flooding it caused. Ten hectares of land slid into the Bonnechere River downstream from Renfrew on the night of March 28 to 29, clogging the fast-running river with trees and clay. With the river blocked by trees and debris, water backed up behind the blockage. It rose more than seven metres near the landslide, and about five to six metres upstream in Renfrew. Osipenko, who heads the Renfrew County Paramedic Service, could only watch and wait. Sooner or later, he said, "the river always finds a way through." But first the muddy floodwaters washed away a cottage, damaged a small hunting camp, poured water seven feet deep into a house, submerged the Renfrew sewage plant and got into the basement of the hydroelectric plant. Then, after seven to eight hours, the blockage finally broke loose, releasing all the debris into the Ottawa River. As long as trees and mud blocked the river, a gauge downstream showed the rate of flow as zero. When the blockage burst, the flow jumped to 250 cubic metres of water per second - two and a half times the normal rate for a spring runoff. The river is flowing almost normally now. Ottawa Sun, A6 (Ottawa Citizen)

*** Nova Scotia Power investigating about 9,000 outages - The utility says high winds and heavy rain are pushing trees onto power lines**
About 9,000 homes and businesses are starting the day without electricity due to power outages stretching from the South Shore to Pictou County. Nova Scotia Power says it is investigating the cause of the outages, which range from Digby and Shelburne to Amherst and Stelllarton. "We have very strong winds across the province and in some areas we also have pockets of very heavy rain. The wind and a number of areas, combined with the rain, is causing trees and branches to come down onto the lines," said spokeswoman Bev Ware. She says crews were working through the night. With winds coming from the west, Ware says parts of the Annapolis Valley and the South Shore have been hardest-hit so far, but outages are starting to pop up in northern parts of the province as well. CBC News

*** Rain, wind warnings for west coast; snow coming to Labrador**
Environment Canada has issued rain and wind warnings for the west coast of Newfoundland, and is forecasting another spring snowfall for parts of Labrador Friday. The west coast of Newfoundland, from Port Saunders and the Labrador Straits down to Burgeo-Ramea should expect rainfall through Friday. In Bay St. George, Burgeo, Port aux Basques and Corner Brook, Environment Canada says rain heavy at times is expected to develop Friday afternoon. That rain will fall ahead of an approaching cold front, and spread northeast Friday night into Saturday. An expected 25 to 35 millimetres of rainfall is expected on the west coast, and Environment Canada warns of up to 70 mm in some coastal areas through Saturday. CBC News

*** Grief continues a year after tragic Makwa Sahgaiehcan First Nation fire left 2 children dead - 2-year-old Harley and 18-month-old Haley died in Feb 2015**
More than a year after the death of their two children, Martin Cheenanow and Hazel Ochuschayoo are still processing their grief. "We've had a lot of heartbreaking moments, as we keep thinking about [the loss]. It never left me. Still today, I still think about it lots. We still get lonely for them," says Cheenanow. On Feb. 17, 2015, the couple's children, two-year-old Harley and 18-month-old Haley, died when their

house on the Makwa Sahgaiehcan First Nation went up in flames. The tragedy in the community, located 300 kilometres northwest of Saskatoon, attracted a lot of attention because the volunteer fire service of the neighbouring village didn't answer the 911 call. The fire service attributed its lack of response to an unpaid bill, saying that its firefighters wouldn't have been insured. The controversy has gone away but the grieving continues. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Secrecy a disservice to banking industry
The federal anti-money laundering watchdog's secrecy over the name of the first bank ever fined for breaching its standards has smeared the reputation of the entire industry, a financial sector advocate said Thursday. Janet Ecker, president of the Toronto Financial Services Alliance, is calling on the Financial Transactions and Reports Analysis Centre of Canada to identify the bank recently fined $1.1 million for failing to report a suspicious transaction and various other transfers. "They should make the name public rather than tarring everyone," she said. "Our industry has an excellent reputation globally," she said. "So clarity is important to ensure we don't suffer needless reputation risk." The failure to name the offending institution is a disservice to the industry because it paints an unfairly dubious picture of all players, said Ecker, who is in China on a trade mission. Ecker also wants the government agency, better known as Fintrac, to release more information about the nature of the breach so the public can judge whether the bank committed a serious infraction or a simple oversight. Fintrac said it exercised discretion in deciding not to release the name of the bank in Tuesday's announcement - though it has for many other businesses - in order to send a message of deterrence swiftly rather than wait out a potentially lengthy appeal process before releasing the name. Hamilton Spectator, A1; Toronto Star, A1; * La Presse, 2

La Cour suprême n'entendra pas l'appel d'Asad Ansari
La Cour suprême du Canada n'entendra pas l'appel de l'un des membres du groupe terroriste surnommé les «18 de Toronto». Asad Ansari cherchait à en appeler de sa condamnation datant de 2010. Il avait été trouvé coupable d'avoir participé ou d'avoir contribué aux activités d'un groupe terroriste. Il avait reçu une peine de six ans et cinq mois de prison, mais avait aussitôt été libéré, parce qu'il avait déjà complété sa peine en détention préventive. Le groupe a été accusé d'avoir comploté pour commettre des actes terroristes, incluant un stratagème pour prendre d'assaut le Parlement et décapiter le premier ministre Stephen Harper. M. Ansari avait aussi participé à un camp organisé par les meneurs du groupe. Comme cela est toujours le cas, la Cour suprême n'a pas donné de raisons pour son refus. La Presse canadienne, 19

*** Big Data, surveillance and Privacy 2.0 after Snowden**
An opinion pieces states “Edward Snowden's analysis of the largest leak yet - the Panama papers - did what Shane Pointe of the Musqueam Nation intended: lift up the heart and minds of very brave truthtellers. While Snowden's public conversation terrified many, he also pointed the way to hope in the era of Big Data and the Internet of Things. When talking about Big Data and Surveillance, focus on the information and knowledge that comes from the data, and the power matrix in which that unfolds. That is the real message from the Snowden event held in Vancouver last Tuesday. Value can be positive or negative: information, knowledge and understanding can be used for good or bad purposes. To make Big Data constructive, we need more than just the technological advances and industrial developments - the key component is keeping sight of the rights to human privacy and personal security. Advances in Big Data offer huge potential benefits and risks when we bring different data resources together. (...) "Big" should be just big enough data collection to serve the intended purpose. Second, reform to Canada's Anti-Terrorist Act (C-51) and the Federal Digital Privacy Act should include stronger parliamentary oversight and further empower the Privacy Commissioner with financial penalties over private-sector security breaches, proportional to risk and consequential harms. There are provincial privacy laws that could also use revision and renewal.” Vancouver Sun

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Child porn seizures up at borders
The number of seizures of suspected child pornography at Saskatchewan border points this year is above recent yearly averages - despite the fact this year has only passed its first quarter. According to information provided last month by the Canada Border Services Agency (CBSA), officers in the province averaged five suspected child porn seizures per year between 2010 and 2015. This year, so far, the number of such seizures sits at six. StaffSgt. Scott Lambie with the Saskatchewan Internet Child Exploitation (ICE) unit said seizures at border points, including airports, are "becoming more regular." "What we're seeing is an increase," he said, although he was unable to say what was leading to that increase. "We get the calls from CBSA and we just attend to verify what they've found." One man, an American resident, was arrested this week at Regina International Airport after suspected child pornography in the form of animation was allegedly found on his iPhone. Carlos Melendez appeared at Regina provincial court the next day, facing charges of possession and importation of child porn. StarPhoenix, A3 (Leader-Post)

First Nations groups criticize tobacco smuggling bust
The Mohawk Council of Kahnawake and the Elected Council of Six Nations of the Grand River say the recent tobacco smuggling bust, Project Mygale, led by the Quebec provincial police is an infringement on aboriginal rights. "It's disheartening to read statements, like the one recently issued in the Mygale project, attempting to criminalize our tobacco industry," Six Nations Chief Ava Hill said in a statement. "Tobacco is a historical trade that supports the growth and economic prosperity of our communities. As sovereign nations, the federal and provincial governments have no jurisdictional right to tax and regulate tobacco on our territories." Hill could not be reached Thursday to elaborate on her comments. A spokesperson for the Sûreté du Québec would not comment on the statement. A 38-year-old Ohsweken man is wanted on fraud-related charges for allegedly being one of 21 main players of a criminal organization with links to biker gangs and organized crime that extended to the United States, South America and Europe. He was on holidays out of the country when the bust took place last week, and remains outside of Canada, a spokesperson for the Sûreté du Québec says. Two million kilograms of tobacco were bought in North Carolina and illegally imported in trucks at the Lacolle, Que., Lansdowne, Ont. and Fort Erie border crossings between August 2014 and March 2016. The tobacco was processed mostly on reserves, police say. The statement from the two First Nations organizations argued that "tobacco is not an illegal activity" and "any attempt to regulate or restrict a First Nation from manufacturing and participating in inter-nation trade within the tobacco industry is an attack on this inherent indigenous right." Hamilton Spectator, A6

Une «brèche» qui coûte cher aux producteurs
Une «brèche» dans le système de l'importation de protéines de lait au Canada prive actuellement les producteurs québécois de 15 000 $ à 16 500 $ par année, affirment des associations de l'industrie, qui déplorent l'inaction du gouvernement fédéral dans le dossier. Considéré comme un ingrédient par l'Agence des services frontaliers lorsqu'il est exporté des États-Unis vers le Canada, le lait diafiltré change de statut dès qu'il traverse les douanes. L'Agence canadienne d'inspection des aliments (ACIA), qui assure le suivi des produits, le considère alors comme du lait. Conséquence? Les transformateurs peuvent utiliser la quantité de lait diafiltré qu'il désire, au détriment du lait frais, dans leur recette de fromage, puisqu'il est considéré comme du lait, explique Richard Bouchard, président des Producteurs de lait de Capitale-Nationale-Côte-Nord. Si le lait diafiltré était considéré comme un ingrédient, les entreprises auraient un maximum de quantité - selon la réglementation en vigueur - qu'elles pourraient utiliser dans leur production de fromage, poursuit-il. Rappelons qu'en 2007, afin de limiter les dommages liés à l'importation de concentrés de protéines laitières (IPL), le gouvernement avait mis en place des normes de composition des fromages. Ces normes limitaient l'ajout d'ingrédients laitiers dans les recettes de fabrication. Afin de maintenir un équilibre dans le marché, l'importation des produits laitiers au Canada est également limitée par des tarifs douaniers. Ayant le statut d'un ingrédient, le lait diafiltré est toutefois exempté de tarifs, ce qui en fait une option alléchante pour les grands transformateurs. Le Soleil, 25, Journal de Québec (Journal de Montréal)

Franchisee suing McDonald's following 'negative publicity'
A former McDonald's franchisee who says he was forced to give up control of three restaurants is suing the fast-food chain's Canadian arm, alleging it cost him millions of dollars even though a government review of his use of temporary foreign workers ultimately cleared him of wrongdoing. Glen Bishop has filed a lawsuit in B.C. Supreme Court against McDonald's Restaurants of Canada Ltd. The company has not yet filed its response. Mr. Bishop's notice of civil claim says an April, 2014, report by CBC's Go Public news segment accused his Victoria restaurants of giving more shifts to temporary foreign workers than Canadian workers. He said he was delivered a letter by McDonald's representatives that same day that said he could not continue as an owner and operator. He said he was told he would not get any compensation if he did not immediately sign a letter agreeing to transfer the restaurants over to McDonald's. Mr. Bishop said a January, 2015, letter from the then-minister of employment Jason Kenney said its review was complete and the suspension against Mr. Bishop and his company, Nasib Services Inc., had been lifted. But he said McDonald's formally terminated its agreements with him in March, 2015, causing him major losses. Globe and Mail, S1

Job vacancy rate highest in B.C.
British Columbia has the highest job-vacancy rate among provinces, a survey of small businesses shows, with smaller employers - particularly restaurants and retail stores - having a harder time filling positions. It is another sign that B.C.'s economy is growing, but a signal that some businesses are hitting limits in their ambitions to expand, said Aaron Aerts, B.C. economist for the Canadian Federation of Independent Business. Aerts said it is smaller businesses, those with fewer than 20 employees, experiencing a harder time finding candidates where "having a vacant position empty for months on end can (put) a real drag on a business' growth." B.C.'s private-sector employers had a three per cent job vacancy rate, generally speaking, according to the federation's latest quarterly Help Wanted report, released Thursday, which translates to 50,000 positions. (…)"That is very consistent with what we're hearing," said Ian Tostenson, CEO of the B.C. Restaurant and Food Service Association, with kitchen jobs among the hardest to fill. (…)Instead, Tostenson thinks that a declining number of young people going into the cooking trades is a bigger factor, along with changes to the federal government's temporary foreign workers program, which eliminated a large pool of unskilled labour for restaurants. Vancouver Sun, C2

Syrian program to get staff boost
Additional staff are being sent back to Canadian visa offices in the Middle East for faster processing of Syrian refugees, part of a Liberal promise to bring 10,000 privately sponsored Syrians to Canada by early next year. Sponsorship groups have given Immigration Minister John McCallum and other Liberal MPs an earful in recent weeks after efforts to resettle Syrians were scaled back following the end of the government's program to get 25,000 to Canada by the end of February. Staffing cuts and limits on applications meant people who had raised money, rented apartments and amassed clothes, furniture and volunteers would likely not meet their refugees until well into next year. McCallum responded to some of those concerns last week, saying the 10,000 people whose applications were in by March 31 would be in Canada by the end of this year or early in 2017. Canadian Press (Waterloo Region Record, A3, Hamilton Spectator), Toronto Star, Globe and Mail

DSW n'est pas pressée d'entrer au Québec
Ceux et celles qui raffolent des chaussures et qui voyagent aux États-Unis connaissent les magasins DSW Designer Shoe Warehouse. Depuis deux ans, ce géant de la vente au détail, coté en Bourse, prend de l'expansion partout au Canada_ sauf au Québec. L'entreprise torontoise Town Shoes, qui exploite l'enseigne DSW au Canada, vient d'annoncer l'ouverture de six magasins l'automne prochain. Ceux-ci s'ajoutent aux quatre autres déjà prévus cette année. Résultat : il y aura 23 DSW d'un bout à l'autre du pays d'ici Noël. Les nouveaux points de vente seront notamment situés en Ontario (Ancaster, Burlington, Vaughan), en Colombie-Britannique (Tsawwassen Mills et Richmond) et à Edmonton. Dans l'est du pays, un magasin s'apprête à ouvrir à Halifax (qui s'ajoute à celui de Moncton). L'entreprise est également présente à Ottawa. Et le Québec dans tout ça ? (…)En raison des tarifs douaniers (18 % au Canada comparativement à 8 % aux États-Unis), les prix ne sont pas les mêmes dans les DSW du Canada qu'au sud de la frontière, convient Bruce Dinan. « Mais nous offrons les meilleurs prix au Canada », jure-t-il. DSW possède aussi un site web canadien. La Presse +

* **Canada faces Tuesday EU visa deadline in long-running Romania, Bulgaria spat**
Canada and the European Union are racing towards a Tuesday deadline to avoid triggering a process that could result in Canadian travellers having to obtain a visa to travel to 26 European countries. It is part of an ongoing dispute in which the EU has pushed Canada to lift its requirement on travellers from its member countries, Romania and Bulgaria. The issue has raised concerns that the dispute could adversely affect the mammoth Canada-EU free trade deal, which still has yet to be ratified. The 28-member bloc says Canada's visa violates the spirit of reciprocity, but the Immigration Department disagrees. Representatives from Canada, the EU, and Bulgaria and Romania have met four times since then including a session this past Wednesday but no progress has been made, said one source familiar with the efforts but not authorized to discuss them publicly. Tuesday's deadline raises the possibility of igniting a nasty public spat in a year when Canada and the EU are celebrating 40 years of relations and hoping to finally ratify their landmark free trade deal. The Telegram

* **Lure Of Canada: Favorable exchange rate brings Americans across the border**
Residents of Detroit and Windsor, its Canadian neighbor to the south, have long enjoyed a close relationship on many levels — entertainment, shopping, dining out. Before the 9-11 terrorist attack, it was common for Downtown Detroit office workers to have lunch in Windsor and suburbanites often visited the Canadian city to shop, eat at an ethnic restaurant or try their luck at the casino. After 9-11, long backups sometimes occurred at the two Detroit-Windsor border crossings as security ratcheted up. Quick, fun trips to Canada were no longer so appealing. "Before 9-11, 30 percent of our customers were from the U.S.; after, it dropped to 10 to 12 percent," said Dan Orman, co-owner of Freed's, a popular clothing store in downtown Windsor for 86 years. But, in recent years, traffic flow has improved, based on reports from individuals who travel to Windsor regularly and official websites that track border crossing times. Orman says he commutes to Windsor from his West Bloomfield home in about 30-35 minutes as long as it's not rush hour. But it's the favorable currency exchange rate that is once again luring more U.S. citizens to Canada. (…)While traffic backups are rare during non-rush-hour border crossings, Allan Gale of West Bloomfield recommends that visitors avoid the trip on Saturday nights when traffic is heavier because American young adults often visit Windsor bars and the casino. Unlike the U.S., Canada's legal drinking and gambling age is 19. For many Detroiters, a trip to Windsor to celebrate a 19th birthday is a rite of passage. Jewish News (2016-04-07)

* **Drug dealers get 17 and 15 years in jail after 112 kilograms of cocaine found in Mississauga**
Two men have been jailed 17 and 15 years respectively for their roles in a cocaine smuggling operation that saw close to $9 million worth of the drug make its way by sea from Guyana to St. John, New Brunswick, and then to a public storage facility in Mississauga. Justice Peter Daley found James Buttazzoni, 45, of Mississauga, and Rampersaud Ramlall, 40, of Whitby, guilty in Brampton court of conspiracy to import cocaine and possession of cocaine for the purpose of trafficking. "The impact of cocaine upon our citizens cannot be underestimated. It is a plague on our community and impacts on all aspects of society by destroying the lives of those involved in its use as well as their families," the judge said in sentencing the pair. Daley acquitted both men however, of importing cocaine, ruling Buttazzoni only became involved with the cocaine when it arrived in Ontario. Evidence showed that Ramlall had communication with people in Guyana, who were involved in the exportation of the cocaine to Canada, but the judge ruled "his conduct, on the evidence, does not constitute importing." (…)Canada Border Services Agency (CBSA) officers opened the container and located 112 kilograms of cocaine with a purity of 74 per cent, which was hidden in the wooden pallets located in the container. The container also held quantities of hot sauce, Chinese sauce, seasonings and noodles, court heard. Mississauga (2016-04-07)

* **$200k in U.S. cash seized from man on river shore**
A police patrol on the St. Lawrence River has netted $200,000 (U.S.) seized from an Akwesasne, N.Y. man. While on patrol during the late evening hours of March 31, members of the Cornwall Regional Task Force (CRTF) observed a vessel with two occupants heading north on the St. Lawrence River to a shoreline dock in the city's east end. Upon arrival at the dock, police a male passenger disembark the vessel, walk up to the roadway and proceed east carrying a black sports bag. CRTF members stopped to question the individual. (…)The CRTF is a joint forces partnership that includes the Royal Canadian Mounted Police, Ontario Provincial Police, Canada Border Services Agency, and the Ontario Ministry of Finance. Cornwall Seaway News (2016-04-07)

*** GOP Congressman Mike Bishop lies about promising vote on bridge to Canada, wants to eliminate the Dept. of Education**
An opinion piece states, "It's well-known that MI-08 Republican Congressman Mike Bishop is a bought-and-paid-for lapdog of the Moroun family. The patriarch of that family, Manuel "Matty" Moroun, is the billionaire owner of the Ambassador Bridge that spans the Detroit River between Detroit and Windsor. Although there is a desperate need for an additional bridge to facilitate truck traffic that now backs up for miles on busy days, Moroun is equally desperate that no additional bridge be built unless he is the one that builds it and profits from it. He went so far as to attempt to get voters to pass a ballot initiative back in 2012 that would assist him in maintaining his monopoly. Voters rebuffed him but he has never given up hope. He has fought another bridge proposal, one that is now a done deal and will be called the Gordie Howe International Bridge, tooth and nail and nobody has been more helpful along the way, exploiting his government position and political connections, than Mike Bishop. (…)Last week, in an interview with WHMI, Bishop suddenly revised history, claiming he never promised a vote on the bridge his benefactor Matty Moroun has spent the past decade trying to stop: (…)What IS clear is that Moroun is still very much politically active and intent on stopping the Gordie Howe International Bridge so he can build one of his own." Eclectablog (2016-04-07)

*** Think tank: Private investment needed to fill infrastructure spending gap locally, nationally**
There are unexplored opportunities for the private sector to invest in the nation's $2 trillion worth of deteriorating infrastructure – and get a return on investment – in coming years via a broad expansion of public-private partnerships. That's the message from a report released Thursday by the Bipartisan Policy Center, a Washington, D.C.-based think tank whose executive council on infrastructure toured Detroit for two hours Thursday morning prior to a meeting and panel event at the Westin Book Cadillac Detroit hotel. Public-private partnerships, in which private companies agree to build and sometimes operate public infrastructure for a fee or other payments, are increasingly common overseas and in Canada (which is using a P3 to building the $2.1 billion Gordie Howe International Bridge between Windsor and Detroit), but the United States has lagged in its implementation. Michigan is allowing more than two dozen states that lack the sort of enabling legislation to more easily allow P3 projects. Crain's Detroit Business (2016-04-07)

CYBER SECURITY / CYBERSÉCURITÉ

*** Adobe issues emergency update to Flash after ransomware attacks**
Adobe Systems Inc issued an emergency update on Thursday to its widely used Flash software for Internet browsers after researchers discovered a security flaw that was being exploited to deliver ransomware to Windows PCs. The software maker urged the more than 1 billion users of Flash on Windows, Mac, Chrome and Linux computers to update the product as quickly as possible after security researchers said the bug was being exploited in "drive-by" attacks that infect computers with ransomware when tainted websites are visited. Ransomware encrypts data, locking up computers, then demands payments that often range from $200 to $600 to unlock each infected PC. Reuters (Yahoo! News)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Motorcade today, candlelight walk Sunday to honour RCMP constable killed in crash
Crowds of people lined the streets to offer their support and condolences as officers from police departments across southern Vancouver Island solemnly escorted the body of one of their own. Const. Sarah Beckett, an 11-year member of the West Shore RCMP, was killed in a two-vehicle crash in Langford early Tuesday. Thursday's motorcade wound its way from the Victoria General Hospital to the Victoria airport, at one point driving beneath a large Canadian flag hung between the extended ladders of two fire trucks. Other emergency personnel were on hand to pay their respects, including representatives from BC Ambulance Service, BC Sheriff Services and various fire departments. RCMP spokeswoman Cpl. Janelle Shoihet says police are conducting a criminal investigation, and Saanich police have confirmed they are responsible for looking into the crash that killed Beckett. The other driver involved in

the collision was taken into custody on Tuesday but was released a day later without charges. A candlelight walk is planned for Sunday. A Facebook page called "Candle light walk to remember Sarah Beckett" says the memorial walk will begin at 8:30 p.m. Sunday and go from Peatt Road to Veterans Memorial park off Aldwynd Road. Vancouver Sun (Toronto Sun, Guardian, Telegram, Ottawa Sun, Edmonton Sun, Calgary Sun, Winnipeg Sun); * Truro Daily News; * Brandon Sun; * Times Colonist, A3)

Dashboard video shows intense police takedown in North Battleford
An intense RCMP takedown at an intersection in North Battleford that was captured video is being shared widely online. The footage, captured by a citizen's dashboard video camera, shows a police takedown of a suspected criminal who was fleeing police on a bicycle. The video shows an unmarked police minivan speeding through an intersection to intercept the suspect on the bike. A plainclothes police officer then jumps out of the van and tackles the suspect on the bike. Soon, a second unmarked police car and another marked RCMP vehicle arrive at the scene. In a news release, RCMP said they were searching for a suspect believed responsible for "numerous complaints" of criminal activity in the North Battleford area. They eventually located the suspect, but he fled police on a bike, the release said. RCMP said the suspect was not injured during the takedown, but one officer sustained a minor injury to his shoulder. RCMP said they are now reviewing the footage for "investigative purposes." Star Phoenix

Accusations contre la GRC
Accusée de violations au Code du travail lors de la fusillade du 4 juin 2014, la GRC a obtenu un nouvel ajournement. La conférence préparatoire de procès est reportée au 12 mai. L'avocat représentant la force policière, Ian Carter, s'est rendu en Cour provinciale jeudi à Moncton, pour répondre aux accusations portées contre le corps policier à la suite de la fusillade. Les deux parties ont indiqué que plus de temps serait nécessaire pour examiner certains éléments. Les plaidoyers sont donc remis au mois prochain. La GRC est accusée de ne pas avoir pris les mesures adéquates pour assurer la sécurité de ses employés et d'avoir commis quatre violations du Code canadien du travail lors des évènements. Les accusations concernent l'équipement, la formation et la supervision des policiers. C'est à la suite d'une enquête de la GRC sur les circonstances entourant la fusillade qu'on a pu constater que les agents sur place avaient alors été confrontés à une série de problèmes dans le cadre de leur intervention, parmi lesquels l'accès à des armes plus sophistiquées, l'utilisation d'équipement de protection adéquat et des problèmes dans leurs communications. En mai 2015, le Service des poursuites pénales du Canada a recommandé d'intenter une poursuite contre la GRC en invoquant des contraventions au Code du travail, plus particulièrement aux clauses touchant la santé et la sécurité au travail. Acadie-Nouvelle, 6

* **New inspector to oversee administration at Kelowna RCMP**
Kelowna RCMP welcomed a new inspector in town this week. Insp. Paul McDougall arrived from the Maritimes with his wife and daughter to become the Kelowna RCMP's corporate and client services officer. "He occupies a newly created administrative position, responsible for looking after a variety of administrative duties for the detachment," said Const. Jesse O'Donaghey. Inspector is the RCMP rank directly below superintendent, the rank held by Nick Romanchuk at the Kelowna detachment. Kelowna Daily Courier

Shining the light on police mental health
On Nov. 8, 2008, Jean-Michel Blais stood in front of a collapsed primary school in Haiti, watching as 93 bodies, most of them children, stacked up in front of him. The United Nations police team bore through the rubble in search of survivors, and found a girl trapped between the bodies of two other children. As deputy commissioner of the UN mission, it was Blais who gave the order to cut one of the bodies in half to pull the surviving girl out safely. More than to serve and protect, Blais says police work is about confronting the problems that people would not, should not and could not deal with. But sometimes, he can't either. Blais, who became Halifax Regional Police Chief in 2012, recently revealed he has post-traumatic stress disorder. It has become a hallmark of his leadership atop the Halifax force, where he has made officers' mental health a priority. By next month, every Halifax cop will complete a half-day Road to Mental Readiness workshop. "Day in, day out, these officers have to show up at the doors and deal with the challenges that are there," Blais said in a recent talk at Mount Saint Vincent University, "Spat upon. Shot at. Cut. Yelled at You think that doesn't leave them with a lasting stress?" Blais wants to start a discussion about mental illness within the force. He says in a "suck-it-up" police culture, officers have

been more likely to grab a 40-ouncer than reach for help. He's trying to change that. "(Officers) have to realize that they have to take care of themselves before they can take care of others," Blais said in an interview. When he talks publicly about his PTSD, Blais makes a point of wearing his uniform, to show that mental illness can happen to anyone. Canadian Press (Chronicle-Herald, A3, Toronto Star, Telegraph-Journal, Times & Transcript)

Inconduites sexuelles - L'ONU fait face à un combat complexe
Les suspensions de cinq et neuf jours imposées à deux policiers du Service de police de la Ville de Montréal (SPVM) pour inconduite sexuelle en Haïti ne font rien pour diminuer l'impression d'un système qui favorise l'impunité devant de tels actes, estime un expert. L'affaire révèle en filigrane la complexité de la lutte contre l'exploitation sexuelle dans les missions de paix. En coulisses, le SPVM reconnaît que les peines imposées aux deux policiers qui ont eu des enfants avec des Haïtiennes ne sont " d'aucune commune mesure " avec le geste posé. Mais il n'y a pas eu de plainte quand les policiers étaient en poste en Haïti, et la seule sanction possible en était une de discipline, dit-on : une manière de ne pas laisser le geste impuni. En vingt ans de collaboration avec Haïti, c'est la première fois que le SPVM fait face à une telle situation. Mais ce n'est pas d'hier que différents cas d'agressions sexuelles touchent les Casques bleus, notamment en Haïti. L'ONU a lancé en 2005 une stratégie pour lutter contre ces agressions... seulement pour constater dix ans plus tard que les cas demeuraient " répandus et pas assez dénoncés ". Dans un rapport interne publié en 2015, l'ONU répertoriait 231 femmes haïtiennes affirmant avoir eu des relations sexuelles avec des Casques bleus, souvent en échange de biens matériels -- chaussures, vêtements --, ou carrément contre des produits de première nécessité et des médicaments. (...) " A titre de policier canadien affecté à une mission de paix internationale, vous occupez un poste qui entraîne une différence quant au pouvoir, à l'autorité et au statut réels ou perçus entre vous et les membres de la collectivité locale ", rappelle la GRC aux policiers. Toute contravention à ces règles sera punie, ajoute le guide. Le Devoir, A5

*** Shooting suspect caught after Portage lockdown**
RCMP have a suspect in custody after two people were shot on a southern Manitoba reserve. Police locked down the Dakota Tipi community near Portage la Prairie for hours Thursday searching for a 31-yearold man. RCMP blocked all roads around the reserve and urged residents to remain indoors. RCMP say Tyson Pashe, who is known to police, was arrested mid-afternoon. A man and a woman were shot in separate homes in the community and were taken to hospital in serious condition. RCMP say officers will remain in the community for "an extended period of time" as the investigation continues. Truck amok Drunk driving charges have been laid against a Winnipeg man after a truck crashed into a house. The wreck occurred just before 10:30 p.m., at a home near the corner of Arlington Street and Sargent Avenue. Police said the truck had been driving south on Arlington when it left the road, went through a fence and continued through two yards before driving off. The home was damaged, said police. When officers arrived, police said bystanders directed them to a nearby business on the 700-block of Sargent Avenue, where the vehicle was located and the alleged driver arrested. Canadian Press (Winnipeg Sun, A10, Times Colonist); Winnipeg Free Press

*** Drug network centered in city: police**
Police are calling Monday's drug bust the largest in a decade as they released the names of 11 people charged Wednesday. Six separate search warrants were carried out Monday, resulting in 14 arrests, including 20-year-old Todd Dube of Yellowknife, who police accuse of being the leader of a drug-dealing criminal network centered in Yellowknife. Two others, Vitaline Lafferty, 76, and Marie-Anne Lafferty, 55, of Ndilo were arrested outside of Fort Providence on March 18. Eleven people have been charged so far with a variety of mainly drug-related offences. Two of them remain on the lam and arrest warrants have been issued. (...) Dube has been in and out of custody over the past year after being charged with other drug-related offences. He was charged last year in another major RCMP drug raid which yielded fentanyl, cocaine and about $200,000 in cash. He is scheduled to be sentenced on charges related to that bust in territorial court May 25. (...) Mayor Mark Heyck said the city is grateful for the work of the RCMP. He noted RCMP in collaboration with the city had made gangs and drugs one of the force's top three policing priorities for the year. LeSage said the ability to closely monitor this drug network provided "incredible insight into the extent of the drug abuse in the community." He said he is extremely proud of the

investigation and thanked officers involved. He added there are still many long hours of police work to prepare the evidence for court. Yellowknifer

*** Man dies in custody**
A 45-year-old man was pronounced dead in hospital Wednesday shortly after being arrested by Chilliwack RCMP. The B.C. Coroners Service said Lindsey Harvey Gauthier went into medical distress after being arrested at a restaurant. He was transported to hospital, but could not be resuscitated. The coroners service and the Independent Investigations Office are investigating. Province, A4; Canadian Press (Times Colonist, A6)

Gun scare suspects in court
Two teens charged in connection with a gun scare and lockdown at Millwood High School will appear in court Friday. The pair, aged 17 and 15, will be in Halifax Provincial Court Friday afternoon for a bail hearing. Tuesday's lockdown ended with the two facing 19 charges, including theft, two counts of possession of a weapon for the purpose of trafficking and several other weapons-related charges. Police believe the two got off the #82 Halifax Transit bus in front of the school dressed in camouflage, one dropping a gun on the ground. Police quickly set up a perimeter around the school and arrested one youth. Another was apprehended offsite. The RCMP seized a small hockey bag containing two long-guns and two BB guns from the woods behind the school. Cpl. Jennifer Clarke says the youth were neither selling guns, nor was this drug-related. Chronicle-Herald, A5

As home burns in early-morning hours, police capture escaped murder suspect Braidy Vermette near P.A
Family members of Troy Napope are finally feeling some relief after his accused murderer, who made a daring escape from jail guards in Prince Albert, is back behind bars. Braidy Chase Vermette and his girlfriend, Tristen Smith, were taken into custody shortly after 1 a.m. Thursday, RCMP said in a release. Vermette, one of the men accused of killing Troy Napope in 2015, had been on the run since March 30, when he escaped - with the help of two people armed with bear spray and a gun - from two jail guards who were escorting him to hospital for treatment of a self-inflicted wound. "I'm feeling relief. My family is feeling relief," said Christie Napope, Troy's sister, shortly after learning of Vermette's arrest. Provincial officials said inmates at the Prince Albert Correctional Centre helped Vermette plan the escape. Police are still searching for the two suspects who allegedly helped him get away. "Our investigation has shown that Mr. Vermette was receiving help from inside his unit (at the jail)," Justice Ministry spokesman Drew Wilby said at a press conference Thursday in Regina. Braidy Chase Vermette, 28, is charged with first-degree murder in the May 2015 death of Troy Napope. The RCMP's emergency response team was called to a home in the RM of Buckland near Redwing after police received a tip about Vermette's location Wednesday around 4:30 p.m. StarPhoenix

VPD say no connection between 4 attacks on women in same East Van neighbourhood
An attack on a woman in East Vancouver Wednesday evening is at least the fourth stranger assault in as many months in a small area of the Hastings Sunrise neighbourhood.In the latest incident, a 41-year-old woman was surprised and grabbed by a man as she sat in her car near Nootka Street and East Broadway. She managed to fight off the attacker and call for help.Less than four block away near East 7th Ave. and Windermere Street, another woman was attacked and sexually assaulted as she was getting into her parked car in January. (…) Burnaby RCMP recently formed a special task force after a fifth sexual assault in just over a month in North Burnaby. Police there say there are some commonalities in all five attacks. Both clusters of attacks - in East Vancouver and in Burnaby - have occurred not far from SkyTrain stations along the Millennium Line. CBC

A request for comment from the Burnaby RCMP was not returned
2 men arrested in Inuvik after firearms incident. Two men have been arrested in Inuvik and are facing charges after police responded to a firearms call Tuesday night. RCMP say the incident continued into Wednesday morning. Police say no one was injured in the incident and both men remain in custody. CBC

*** RCMP recapture escaped suspect**

A man facing charges in connection with the death of Troy Napope has been taken into custody again after escaping on March 30. Braidy Vermette is facing a charge of first-degree murder, and was receiving medical treatment in Prince Albert when he escaped police custody. On Wednesday afternoon, police received a tip about Vermette's location. On Thursday they deployed an emergency response team to a residence in the R.M. of Buckland, where Vermette and a woman wanted by the Prince Albert Police Service were hiding. According to RCMP, both suspects were taken into custody as they exited the building after it caught fire. The incident occurred shortly after 1 p.m. No serious injuries to the suspects, police or the general public were reported. Buckland Fire and Rescue responded to the fire, but were unable to save the building. It is expected to be a total loss. There is currently no risk to public safety, but RCMP say there may be road restrictions in the area for the rest of Thursday. They also ask the public to stay away from the residence while investigators and fire crews work on the scene. At the request of the RCMP, another police service has been asked to conduct an independent external investigation into the matter. RCMP have also asked the provincial government to assign an independent observer to the case. Prince Alberta Daily Herald

*** Woman accused of defrauding family of London-area crash victim found dead in British Columbia**

A woman being investigated for defrauding the grieving family of a London-area man killed in a crash has been identified as the victim of a grisly homicide in British Columbia. Her friends, meanwhile, are outraged by the media's focus on the fraud allegation -- her death made headlines across Canada -- and want her to be remembered as a devoted mother, skilled mechanic and lover of the outdoors. Police say a motorist discovered a burned body by a service road near Mission, B.C., east of Vancouver, on March 29. Homicide investigators haven't released the victim's name, but family and friends identified her as Victoria (Vikki) Heppner. Heppner, 28, made national headlines last fall after more than $24,000 went missing from an online fundraiser she had set up for Roger Belanger, a fellow truck driver killed in a single-vehicle crash south of Woodstock on July 28. More than 170 people donated to the Gofundme account for Belanger's widow and two young sons, but the family said they never received a penny. Belanger, 29, had met Heppner through a Facebook group for truck drivers, his family said. Mounties in Wood Buffalo, near where Heppner had lived in Fort McMurray, launched an ongoing fraud investigation, Cpl. George Cameron said Thursday, adding he hadn't received confirmation of Heppner's death. London Free Press

*** N.S. politician says blackmail letter threatened to reveal call to male escort**

A municipal councillor in Nova Scotia says someone tried to blackmail him into resigning by threatening to reveal a call made from his hotel room to a male escort service. Steve Sampson, a member of Richmond County council, said he received an unmarked envelope in the mail Tuesday at his home containing a photocopy of a hotel bill from February, 2014, incurred while on county business in Seattle, Wash. "The bill included a phone call to a male escort agency," Sampson told a news conference Thursday in Halifax. The anonymous letter-writer told him he would publicize the expense unless Sampson resigned by Friday and agreed never to run for office again, he said. Sampson said he instead decided to take the letter to RCMP, and asked them to investigate "this attempt to blackmail a public official." He said he is disturbed that various scandals that are roiling Richmond County council have produced such a toxic threat. "It has never been my practice to mix private, personal matters with public life. But in these circumstances, I don't believe I have a choice," he said in a statement to reporters. As warden until 2014, Sampson led a successful fight to reduce county council to five seats from 10. "The blackmailer apparently believes I can be embarrassed or shamed into resigning my seat, but I will not be blackmailed into leaving public office. Unlike the blackmailer, I have complete faith in the fairness and good judgment of the people of Richmond County. I trust them to weigh the motives of the blackmailer against my conduct over many years." An RCMP spokesman could not be reached late Thursday to discuss any investigation. Telegram (Guardian, Cape Breton Post, Toronto Sun)

*** Nanaimo police investigating racist graffiti again**

Police are investigating a case of racist graffiti after ads featuring real estate agents of Asian descent were defaced in Nanaimo this week.The graffiti appeared on three bus-stop bench advertisements, according to police. "Just terrible, senseless graffiti," said said Const. Gary O'Brien, with Nanaimo RCMP.

"They have since been cleaned up and we have no idea who is responsible for it." One community organization says it was shocked to see the hateful messages. CBC

*** Surrey mayor calls for new prosecution rules after recent shootings**
A wave of gang-related shootings in Surrey has prompted the city's mayor to propose changing the rules for criminal prosecution to get more accused gunmen before the courts. Linda Hepner's suggestion Thursday came amidst a wave of drug-related shootings in British Columbia's second-largest city - more than 30 for 2016 - that have alarmed the public. At least nine people have been injured in the shootings and one killed, according to media reports. "We have become so overburdened with process requirements," Ms. Hepner said in an interview. Globe and Mail

*** Break-in sexually motivated: RCMP**
A violent home invasion against an elderly Selkirk couple last weekend appears to have been a random, sexually motivated attack, according to court documents. RCMP previously released information an 88-year-old man and his 85-year-old wife were found Sunday evening suffering from serious injuries. Both were taken to hospital, where they remain in stable condition. Police also disclosed earlier this week they had arrested a 22-year-old Selkirk man, whom they found walking in the area shortly after the incident and charged him with multiple counts of assault and break-and-enter. However, the court information sworn out against the accused, Justin Bannab, reveals additional details about what allegedly happened. Bannab is charged with aggravated sexual assault and break-and-enter with the intent of committing aggravated sexual assault against the female victim. He is also charged with aggravated assault and break-and-enter with the intent of committing aggravated assault against her husband. Bannab appeared briefly in a Winnipeg courtroom Thursday, where the Crown obtained an order banning him from having any contact with the two victims. He remains in custody at the Winnipeg Remand Centre and has not yet made a bail application. Winnipeg Free Press, B2

*** Près de 400 arrestations en six mois**
L'opération policière à l'origine des troubles qui secouent de nouveau Montréal-Nord s'inscrivait dans une vaste offensive contre les gangs de rue, frappés par près de 400 arrestations depuis six mois. La recrudescence des meurtres et des crimes violents liés aux gangs d'allégeances rouge et bleue, en 2015, a incité la police de Montréal à accentuer la pression sur cette forme de criminalité avec le «projet Accalmie». Depuis septembre dernier, ce blitz d'opérations a mené à plus de 380 arrestations pour trafic de stupéfiants, crimes violents et possession illégale d'armes à feu. C'est dans ce contexte qu'est survenu le décès de Jean-Pierre Bony, atteint d'une balle de plastique à la tête alors qu'il tentait de fuir les policiers lors d'une rafle au quartier général d'un réseau de trafiquants des Rouges, rue Arthur-Chevrier, le 31 mars. Une douzaine de suspects ont alors été arrêtés, dont Dany Villanueva, frère du jeune Fredy Villanueva, abattu en 2008 lors d'une intervention policière qui avait provoqué des émeutes à Montréal-Nord et dont l'anniversaire de naissance coïncidait avec la manifestation qui a tourné au saccage, mercredi soir. Il faut remonter à 2007 pour trouver pareille offensive à l'encontre des gangs de rue à Montréal. Journal de Montréal, 15 (Journal de Quebec)

*** Per capita costs downin 2015:police board**
The per capita cost of operating the Winnipeg Police Service last year was below the national average for police forces across the country, a Statistics Canada report shows. Don Norquay, executive director of the Winnipeg Police Board, said the service's per capita costs in 2015 were $363.43, while the national average - according to a recent Statistics Canada report - was $391. Norquay told councillors on city council's finance committee Thursday the board is in the process of comparing the WPS per capita costs with those of police forces across the country. In a comparison with three other Prairie cities, Norquay said the WPS's costs were lower than those of police in Calgary and Edmonton but higher than those in Saskatoon. Norquay said the board will be continuing its research and hopes to have a more comprehensive comparison ready at a later date. He said the police service's per capita costs in 2015, when adjusted for inflation, decreased "slightly" from the costs in 2014. While the police board and the WPS were stung by criticism from Mayor Brian Bowman and several councillors over the increase in the police budget for 2016, Norquay said the fourth-quarter financial report for 2015 paints a positive picture of the police service's financial situation. While the police budget overall climbed 6.32 per cent, Norquay said a comparison of actual expenses from 2014 to 2015 showed an increase of 1.87 per cent - and most

of that was driven by salary increases that totalled three per cent. Norquay said the mill rate contribution to the WPS budget - those funds paid for by property taxes - increased 1.98 per cent. "All in all, it's a fairly positive fiscal picture for the police service," he said. Winnipeg Free Press

*** Une tragédie nationale**
La mort de Sandy Michel, survenue mercredi soir à Lac-Simon, en Abitibi, n'est pas qu'un simple fait divers. C'est une catastrophe. Pire : une tragédie nationale. En moins de six mois, c'est la troisième fois que cette communauté algonquine de quelque 2000 habitants, située près de Val-d'Or, est au c_ur d'un drame humain. En octobre 2015, il y a eu des allégations d'agressions sexuelles et d'abus de pouvoir qui auraient été commis par des policiers contre des femmes autochtones. Puis la mort, le 13 février, du policier Thierry LeRoux, tué lors d'une intervention qui a mal tourné dans une résidence de la communauté, suivie du suicide du meurtrier, Anthony Papatie. Et avant-hier, la mort de Sandy Michel, tombé sous les balles d'un policier en pleine rue. L'homme de 25 ans, qui avait consommé de la drogue et était sans doute en proie à une psychose, était armé d'une machette. Il a été happé par une voiture de police avant d'être atteint par balle. Son frère est mort dans des circonstances semblables en 2009, lui aussi abattu par un policier. La mort de Sandy Michel risque d'augmenter d'un cran la tension entre les policiers autochtones et les membres de la communauté. Mais, au-delà des tensions, elle montre à quel point cette communauté autochtone est malade et les problèmes sont criants : pauvreté, violence, chômage, surconsommation, drogue et alcool, problèmes de logement, de santé mentale, décrochage scolaire, agression sexuelle, suicide, etc. La population de Lac-Simon est en explosion. Dans tous les sens du terme. On assiste à un baby-boom. Jusqu'à 60 naissances par année sur un territoire d'un kilomètre carré. Mais le nombre de maisons est nettement insuffisant pour héberger tout le monde. Dans certaines maisons, on retrouve plus de 15 personnes de la même famille. Et la situation s'aggrave d'année en année. Il n'y a pas d'espace, pas d'oxygène. Ça crée des situations propices à la violence. La Presse, 3

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Prison locked down
Bath Institution, a medium-security facility, was locked down at approximately 1 p.m. on Thursday so staff members could conduct an exceptional search. A news release from Correctional Service Canada did not say what type of contraband staff were looking for or for how long they expect the institution to be in lockdown. The search was ordered to ensure the safety and security of the institution, its staff and inmates, said the release. Normal operations will resume as soon as it is considered safe to do so. Regularly scheduled visits may be affected. Visitors who have already planned a visit are asked to contact the institution directly, said the release. Kingston Whig-Standard, A3

Donald Trump 'homosexual' Wikipedia edits made from Corrections Canada computer
Edits to an online page on Donald Trump, calling him transgender and homosexual, were made using a computer with an IP address belonging to the Correctional Service of Canada (CSC). The changes were made Mar. 16 to the Wikipedia page Political Positions of Donald Trump. The page lists his history and his views on everything from trade policy to abortion. (…) A page showing the Wikipedia revisions made by the IP address lists hundreds of edits to pages on a variety of topics including firearms, football, a beer concoction called the michelada, gender dysphoria and the CSC's own page. (…) In January 2015 a warning was posted that the IP address was being watched by the press and the CSC after it had been linked to "homophobic" Wikipedia contributions in an Ottawa Citizen article. CSC officials told the Citizen whoever made the edits could face disciplinary measures for posting "offensive and inappropriate" comments. Global News reached out to the CSC regarding the Trump page changes but did not receive official comment by time of publication. Global News (2016-04-07)

*** Province adds them to the ranks of first responders, recognizes post traumatic stress disorder as a work-related illness**
The national vice-president of the Union of Canadian Correctional Officers is applauding legislation passed at Queen's Park declaring that correctional officers are now considered first responders -- along with police, firefighters and paramedics -- and sees post-traumatic stress disorder as a work-related

illness. Jason Godin said the legislation will allow correctional officers to receive treatment for PTSD much faster. "They categorized in the bill whom they considered first responders and it actually included correctional officers. We've been long arguing and fighting to get governments to recognize us as first responders," Godin said. Bill 163 was passed unanimously in the legislature this week. It covers both federal correctional officers working in Ontario and their provincial counterparts. North Bay Nugget

«Rambo» rattrapé par son passé
Bernard «Rambo» Gauthier se retrouve avec un casier judiciaire pour des gestes posés il y a 18 ans. La Commission des libérations conditionnelles du Canada a révoqué le pardon octroyé au leader syndical de la Côte-Nord en 2007, a appris Le Soleil. En novembre dernier, Bernard Gauthier apprenait que la Commission révisait sa décision d'il y a presque 10 ans évoquant l'article 7 de la Loi sur le casier judiciaire, qui lui permet de révoquer un pardon s'il «existe des preuves convaincantes» que l'individu visé a «cessé de bien [se] conduire». (...) Un représentant de la FTQ-Construction a d'ailleurs confirmé qu'une demande d'appel sera déposée au plus tôt vendredi devant la Cour fédérale pour «contester la décision» rendue le 7 mars.(...) Bernard «Rambo» Gauthier a été au coeur de plusieurs démêlés avec la justice depuis les dernières années. En décembre 2014, le représentant de la section locale 791 de l'Union des opérateurs de machinerie lourde a été reconnu coupable d'intimidation dans un chantier de construction, une condamnation pour laquelle il a été absous conditionnellement. «Les comportements [...] liés à votre condamnation pour intimidation, de même que ceux liés à la profération de menaces en 2009 où vous avez été acquitté et ceux liés à du harcèlement criminel où il y a eu un arrêt des procédures en 2014 [...] sont contraires aux critères légaux de bonne conduite de la Loi sur le casier judiciaire», peut-on lire. (...) En 1998, Bernard Gauthier a été condamné pour avoir proféré des menaces et un an plus tard, en 1999, il était reconnu coupable d'avoir enfreint la Loi réglementant certaines drogues et autres substances. Sans pardon, ces deux infractions figurent maintenant à son casier judiciaire. Le Soleil, 7

Court rejects Tang appeal
The Supreme Court of Canada will not hear an appeal from a selfstyled Chinese Warren Buffett who was convicted in a multimillion-dollar fraud. Weizhen Tang was convicted in 2012, sentenced to six years in jail and ordered to pay a $2.8-million fine within five years of his release. Tang operated an investment fund called the Overseas Chinese Fund, which defrauded investors from Canada, the U.S. and China of millions in a Ponzi scheme. Canadian Press (Times Colonist, B2, Toronto Star, National Post Red Deer Advocate)

*** The six jailed Bandidos hoped the Supreme Court of Canada would let them appeal their eight murder convictions**
It was the bloodiest mass murder in Ontario's modern history, and the horrific crime in London's backyard was revealed to the world a decade ago today. April 8, 2006, has gone down in infamy as the day when the bodies of eight bikers were discovered on a lonely dirt road near Shedden. The slayings would collectively come to be known as the Bandidos Massacre. (...) Eight members of the Bandidos motorcycle club, the "No Surrender Crew" from Toronto, were murdered at Wayne Kellestine's Dutton-Dunwich farm. Kellestine and his Winnipeg crew had been instructed to "pull the patches" of the Toronto bikers, effectively kicking them out of the club. All were shot, their bodies found stuffed in abandoned vehicles dumped a few kilometres away from Kellestine's address. Thursday morning, one day before the 10-year anniversary of the discovery of the bodies, the Supreme Court of Canada said it would not hear the appeals of three of the six men convicted of killing their fellow bikers, bringing the long legal saga to a close. (...)Wayne Kellestine, 65, Frank Mather, 41, Brett Gardiner, 30, Marcelo Aravena, 38, Dwight Mushey, 47, Michael Sandham, 45, convicted on Oct. 29, 2009 after seven-month jury trial in London. Kellestine, Mushey and Sandham each convicted of eight counts of first-degree murder. Mather and Aravena found guilty of one count of manslaughter and seven counts of first-degree murder. Gardiner found guilty of two counts of manslaughter and six counts of first-degree murder. London Free Press (2016-04-07)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Whalen wavers on cyber law

Four months after a judge struck down the pioneering cyberbullying law inspired by the death of teenager Rehtaeh Parsons, Nova Scotia's justice minister confirmed Thursday she has yet to decide whether to rewrite the act or appeal the decision. Diana Whalen said the absence of the law has created a quandary for the justice system because the province's groundbreaking CyberScan unit no longer has the tools it needs to combat cyberbullying. "We're well aware of the need for something to take the place of that act because it has really left a void," the minister said after a cabinet meeting. "We know that the last act was written in haste. It was passed in about three weeks. We need to make sure that what we write this time will withstand a constitutional challenge . . . (But) I haven't committed to a bill yet." Whalen said the five-member CyberScan unit was working with the province's schools to educate students about cyberbullying. However, she said the unit has been stripped of the enforcement tools it used to deal with 800 cyberbullying cases over the past two years. Whalen said the province may turn to other means to deal with online harassment, which could include making amendments to existing acts and introducing new policy tools and training. Canadian Press (Chronicle-Herald, A1, The Guardian, Cape Breton Post, Daily Gleaner, Times & Transcript)

No sanctions issued in first year under Sask. stripper law

The Government of Saskatchewan says it has not issued a single sanction under new legislation prohibiting strip shows in the province. The law is aimed at keeping patrons safe. One bar owner says it has all but bankrupted his business. "They got me pretty well shut down here," said Don Verstraeten, who owns and operates the Codette Hotel, which used to hold weekly strip shows before the law was in place. (...)The province banned strip shows in April 2015, except for events held once a year for charitable causes. The intention was to increase patron safety in bars, deter organized crime and protect people who may be vulnerable to exploitation. (...) David Morris, a spokesman for the Saskatchewan Liquor and Gaming Authority (SLGA), said no sanctions have been issued under provincial legislation specific to strip shows. However, the SGLA has fielded numerous questions, he said. (...)When asked about the challenges faced by the Codette Hotel, Morris said the legislation was meant to help eliminate the potential for establishments to profit from activities that "involve the sexual exploitation of vulnerable individuals," like human trafficking. "For a lot of permittees, they understand that following the rules is within their best interest, especially issues related to public safety," he said. Postmedia Network (StarPhoenix, A1, Leader-Post)

Vigilante 'Creep Catchers' target online predators

Members of a loosely affiliated band of vigilantes who use covert social media accounts to expose and publicly shame alleged online predators have emerged in Medicine Hat. Police in the southern Alberta city said Thursday they recently met two people who called themselves "Creep Catchers" and claimed to have recently met one of their targets. They told officers they baited their target by posing online as a teenage girl to arrange a meeting, which they claimed to have recorded on video and threatened to post it on social media. "Individuals who engage in vigilante activity are putting themselves at considerable risk of defensive or retaliatory harm from the people they are confronting," Medicine Hat police said in a statement. Creep Catchers pose a growing concern for law enforcement across North America, including in Calgary, where Dawson Raymond wages a similar public shaming campaign. Raymond told Postmedia last fall he poses as a young teenage girl on online dating sites, where he claims a surprising number of men request to meet, despite the fact the fictitious girl is a minor. He later confronts these men in person as a friend captures video footage, which he posts to his website. The Calgary man's website says Creep Catchers helps prevent the exploitation of children and young adults. "We are building our presence across Canada to catch and expose online child/teen predators as well as similar topics of interest," the site says. Calgary police say they do not condone Raymond's vigilante tactics, though they are investigating complaints that have emerged from his video-recorded confrontations. Officers warn vigilante acts could interfere with police investigations and the collection of evidence, which could mean suspects are not charged or convicted. Postmedia Network (Calgary Herald, A1, Edmonton Journal)

*** Deadly drug finds market in Sudbury**

Greater Sudbury Police are concerned about the growing problem of fentanyl abuse in the city, but encouraged to know nearly 300 patches won't make it to the city after an alleged trafficking ring was broken up in the York region earlier this week. Two Sudbury residents, 30-year-old Sean Holmes and 26-year-old Alexandra Boudreau, and a Toronto family doctor are among several people who were arrested and charged by York Regional Police following a six-month investigation, during which Greater Sudbury Police played a key role. "Our drug enforcement unit worked collaboratively with the drug enforcement and intelligence officers from the York region on this, so it's a joint partnership," said Staff Sgt. Marc Brunette, from the Greater Sudbury Police. "The drugs in question were in fact fentanyl and they were trafficked from the York region and destined for this area." (...) Opioid abuse accounted for 108 deaths in Greater Sudbury from 2008 to 2014, according to information supplied by Sudbury and District Health Unit. Of those, 23 were fentanyl related. "That's a lot of people, so when these drugs are coming into our community, it does pose a huge public health risk," said Brenda Stankiewicz, a public health nurse at the health unit. "We know folks that are addicted will misuse the drug, and we are aware there are times when people pick up the patch, not knowing its potency, and become ill from that, as well." Greater Sudbury has a community drug strategy, co-chaired by the health unit and local police and endorsed by city council, part of which is a patch-for-patch program, where people who legitimately get a prescription from a physician and have it filled by a pharmacist, must return used patches to the pharmacy in order to get new ones. Sudbury Star

*** Marlies' Bibeau is his own harshest critic**

Toronto Marlies goaltender Antoine Bibeau is too hard on himself, and he knows it. Part curse of his position, part curse of his nature. "Sometimes you have a bad game, you think it's the end of the world," Bibeau said after practice on Thursday. "It doesn't matter what kind of goal I give up, it's always my fault." (...)On his off-day Wednesday, Bibeau spoke to students at Kennedy Public School about bullying and told about his own feelings as an outsider. Knowing no English at all, he was drafted at age 16 into the QMJHL and ended up playing in P.E.I., 10 hours from home. "I was scared at first to talk," he said, "because I felt I was going to say something that's not perfect and they were going to laugh at me." In a warning about cyber bullying, Bibeau relayed a personal story about the negative comments he heard after the Maple Leafs passed him up until the sixth round of the 2013 NHL entry draft, No. 172 overall. Toronto Star, S2

*** Per capita costs down in 2015: police board**

The per capita cost of operating the Winnipeg Police Service last year was below the national average for police forces across the country, a Statistics Canada report shows. Don Norquay, executive director of the Winnipeg Police Board, said the service's per capita costs in 2015 were $363.43, while the national average — according to a recent Statistics Canada report — was $391. Norquay told councillors on city council's finance committee Thursday the board is in the process of comparing the WPS per capita costs with those of police forces across the country. In a comparison with three other Prairie cities, Norquay said the WPS's costs were lower than those of police in Calgary and Edmonton but higher than those in Saskatoon. (...)While the police board and the WPS were stung by criticism from Mayor Brian Bowman and several councillors over the increase in the police budget for 2016, Norquay said the fourth-quarter financial report for 2015 paints a positive picture of the police service's financial situation. While the police budget overall climbed 6.32 per cent, Norquay said a comparison of actual expenses from 2014 to 2015 showed an increase of 1.87 per cent — and most of that was driven by salary increases that totalled three per cent. Norquay said the mill rate contribution to the WPS budget — those funds paid for by property taxes — increased 1.98 per cent. Winnipeg Free Press (2016-04-07)

*** Hamilton Police carding/street checks plummeted to 30 last year**

Hamilton Police say they did just 30 street checks in 2015, compared to nearly 200 in 2014 and thousands in previous years, according to numbers obtained by CBC Hamilton under a Freedom of Information request. It's a stunning near-disappearance of a practice that police have publicly defended as a crucial part of their job, but Thursday just described as part of a "downward trend." Senior police have said limiting the tool will make Hamilton less safe. They stood by that argument in the face of criticism from communities of colour and anti-poverty advocates who say the practice of being stopped and asked for ID even when not under investigation is unconstitutional. The province has come up with

new rules governing when police ask people for ID in street stops. But this sharp decline happened even before these new rules take effect. CBC News (2016-04-07)

*** Ontario's profiling rules hurt small-town policing, chief says**
Ontario's new racial profiling regulations will hinder small-town police forces from doing their job, according to Gananoque Police Chief Garry Hull. Hull said the new regulations are a Toronto-centric response to perceived or real racial profiling issues that don't exist in small-town Ontario. In such communities as Gananoque, Brockville and Smiths Falls, there are no problems with racial profiling nor any complaints from citizens, the chief said. If metro Toronto has problems with profiling, or "carding" as it is sometimes called, then the city and province should take actions there to solve them, he said. Instead, small police forces are being swept "into the vortex that is Toronto" by the government's one-size-fits-all approach to policing. Under the new regulations that are effective on Jan. 1, 2017, police officers must go through a cumbersome protocol before talking to someone on the street. The officer must first inform the citizen that the conversation is voluntary and that they have the right to walk away. The police officer must also provide a reason for the stop, identify themselves, inform the citizen that they are taking notes and let the citizen know how he or she can file a complaint against police for the stop. Hull said the regulations will make conversations between his officers and the public awkward and that the rules will prevent the types of friendly chats common between citizens and small-town cops. Gananoque Reporter (2016-04-07)

*** Could a gun amnesty help curb Surrey's shooting problem?**
Surrey's violent crime rate is continuing to climb with another stabbing overnight, which comes on the heels of a shocking escalation in shooting incidents. And yet ideas on how to solve the crisis continue to be discussed with little success. Conservative MP and former Surrey mayor Dianne Watts says she thinks all option should be on the table, but does appear to be supporting an amnesty model. "There's a multitude of different opportunities. One of those would be having a finite amount of time to return weapons to the police, and move forward from there." But when it comes to the idea of a gun buyback, she expressed less enthusiasm. "I don't necessarily have an issue with it if it's going to get the guns off the street, but again we have to determine what does that look like," The model for gun buy-back scheme usually involves people turning in their guns for money. It's also been announced there'll be more talking from our politicians; BC Public Safety minister Mike Morris and mayor of Surrey Linda Hepner will be making a public statement about gun violence tomorrow. iNews880 (2016-04-07)

*** Police Deny Racism And Demand Data (That They Won't Collect)**
An editorial states, "Want to know what's more offensive than a months-old tweet by a Black Lives Matter Toronto co-founder? How about something even more outrageous than attempts to use that tweet, however ill-advised it was, to discredit an entire social justice movement fighting anti-black racism and police violence? Here you go: Toronto Police Association president Mike McCormack is fiercely attacking Ontario Premier Kathleen Wynne for the crime of acknowledging systemic racism exists. "But what I want to ask the premier is for her to show us the data that she is referring to when she says we still have systematic racism in our society," McCormack told the Toronto Sun. "We want this clarified. If she has data to show there is such a racism problem in policing or any of her departments, then the question I have is what is she doing about it?" "It's not true," he said regarding claims of systemic racism in the police force, despite the lack of data he had literally just mentioned, "and it's not acceptable to suggest it." Why is this demand for data so offensive and outrageous? That's because McCormack is well aware that his police force doesn't collect racial data. (…)That 2012 Toronto Star series Known to Police revealed some shocking data. In the city's Entertainment District, where young people of all races used to gather due to the areas then-prevalent nightclubs, "for young black males, the ratio of individuals documented to the population there is 252:1. For brown young males, it is 65:1. For young white males, 23:1." Across the city as a whole, blacks were three times more likely to be carded than whites. This ratio was later revealed to be mirrored in other Ontario cities like Mississauga, Brampton and London. It was even higher in Ottawa, where blacks made up 20 per cent of people street-checked over the last five years despite being only five per cent of the population." Huffington Post (2016-04-07)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Racism, sexism taint murdered and missing cases, minister says
Federal Indigenous Affairs Minister Carolyn Bennett told a global audience in New York that racism and sexism in Canada have tainted the way some investigators handle homicide and missing-person cases involving indigenous women. On stage Thursday at the Women in the World Summit, Dr. Bennett said there is at times an "uneven application of justice" in cases involving indigenous women. "You end up with people who have been told that it was an overdose, or a suicide or an accident," she said. (…) When confronted by the moderator with the title of the panel, Canada's Shame: The Murdered and Missing, Dr. Bennett said bluntly: "It's the truth. Without the truth we will never fix this problem. ... We've got to deal with the issues around poverty, violence and education, and the racism and sexism that mean that when somebody who happens to be indigenous goes missing or is murdered, [the case] doesn't receive the same treatment as a non-indigenous person." The minister and her three copanelists - relatives of two victims, and a former Vancouver detective who worked on the investigation of serial killer Robert Pickton - laid bare the historic and modern social ills that render indigenous women vulnerable to crime in a country that is often on the international stage espousing human rights elsewhere. In a phone interview with The Globe and Mail shortly before the panel began, the minister said she has little confidence in the RCMP's widely cited finding, released in 2014, that 1,181 indigenous women were killed or went missing across the country between 1980 and 2012. "We don't believe that the data is of a high quality," she said. (…)Dr. Bennett reiterated the government's intent to launch a national inquiry into the violence by the summer, telling The Globe she expects it to be under way before the House of Commons breaks for the summer toward the end of June. Long before then, she said, the cabinet will approve the terms of reference and the choice of commissioner or commissioners. Asked whether the government has a short list, Dr. Bennett said a "very, very long list" emerged from preinquiry consultations that wrapped in mid-February. "We have heard, from coast to coast to coast, that the leadership should be, or should include, indigenous women," she said. Globe and Mail, A1

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Les bonnes raisons de réglementer la marijuana au Canada
Un article d'opinion d'un expert note, « Fort de l'appui de 65% de la population canadienne sur ce plan, le premier ministre Justin Trudeau a confié le dossier de la légalisation de la marijuana à son député Bill Blair, ancien chef de la police de Toronto. Présentement, seul l'usage médical de la marijuana est légal au pays. L'usage récréatif, la vente, la possession, la culture ou le transport de marijuana ne le sont pas - tout comme aux États-Unis, d'ailleurs. On sait cependant que le gouvernement de Barack Obama a laissé les différents États légiférer depuis quelques années, à condition qu'un système de réglementation soit mis en place. Le Colorado, l'Alaska, le District de Columbia, l'État de Washington et l'Oregon ont légalisé la marijuana à des fins récréatives. L'accès est limité aux adultes de 21 ans et plus, et d'ici quelques années, une douzaine d'autres États devraient eux aussi légaliser son utilisation - ou à tout de moins assouplir leurs politiques. Il y a aussi ce petit pays de l'Amérique du Sud, l'Uruguay, qui aura été le premier pays du monde à légaliser la production et la distribution de marijuana, en décembre 2013, dans le but de contrôler le marché et de le soustraire au crime organisé. Après quelques années, la difficile application de cette loi donne des résultats intéressants, mais mitigés, surtout sur le plan de la distribution dans les pharmacies locales, qui collaborent plus difficilement. » La Presse

PUBLIC SERVICE / FONCTION PUBLIQUE

L'AFPC demande de reporter la mise en oeuvre de Phénix
En raison des nombreux problèmes liés à l'implantation du nouveau système de paye Phénix, l'Alliance de la fonction publique du Canada (AFPC) demande au gouvernement fédéral de repousser son déploiement. Au début mars, 124 000 fichiers d'employés avaient été transférés à Phénix, mais les

nombreuses plaintes reçues jusqu'à maintenant ont poussé l'AFPC à intervenir pour demander qu'on reporte la phase deux, et le transfert de 170 000 comptes additionnels prévu le 21 avril. « Nous avons reçu plus d'une centaine de plaintes de nos membres, travaillant dans différents ministères, disant qu'ils n'ont pas été payés correctement depuis la mise en oeuvre du système en mars. Pour nous, la situation sera aggravée si l'on poursuit avec la deuxième phase tel que prévu », a indiqué au Droit Chris Aylward, vice-président exécutif national de l'AFPC. « Le ministère ne semble pas voir les choses de la même façon que nous, et ne voit pas pourquoi il reporterait la phase deux. Tout ce qu'on nous a dit, c'est qu'on ajouterait 40 personnes pour répondre aux appels de plaintes », a indiqué le dirigeant syndical après sa rencontre avec les représentants du ministère des Services publics et de l'Approvisionnement, responsable de Phénix. Le syndicat souligne qu'il a sommé le gouvernement d'embaucher plus de personnel au Centre des services de paye de Miramichi, s'il ne peut retarder le transfert de nouveaux fichiers. Selon M. Aylward, il y aurait présentement un cumul de 120 000 comptes ou fichiers qui n'ont pas encore été traités. Le Droit, 4

The liberals and the PBO

In an irony so sharp it must have been almost physically painful, analysts in the Parliamentary Budget Office laid their hands on federal-budget costing for the next five years - but weren't permitted to share the final three years of that data with the public. Instead, the PBO had to release a report based on only two years' worth of information, ignoring the other numbers in its possession. This is inexcusable behaviour from the Liberal government. Not only was it exercising selective secrecy about the numbers - such costing has routinely been made public by predecessor governments - but it placed the PBO in an untenable position: aware of the full story, but unable to make use of it on behalf of the parliamentarians it supposedly serves. What was the government thinking? Given the PBO's long and frustrating history of trying to pry facts from federal departments under the Conservatives, Liberal ministers would be well aware of the optics if they did not provide data to their budget watchdog. Rather than hold back information, however, they have now made the PBO part of their secrecy. Six months into a government's tenure is early to speak of patterns emerging, but, well, patterns are emerging. Just last week, for instance, Treasury Board President Scott Brison launched an "open by default" government initiative but said an overhaul of the ossified Access to Information Act - legislation many taxpayers depend on to help them obtain key information about the programs they fund - won't take place for another two years. For all of their "sunny ways" rhetoric, the Liberals still reign over a system in which information is hoarded. Some examples: When the government's anti-money-laundering agency, FinTrac, this week fined a Canadian bank $1.1 million, it wouldn't identify the bank. Ottawa Citizen, A10

OTHER / AUTRE

Brussels Airlines launches direct Toronto flights

Belgium's biggest airline launched direct flights to Toronto Thursday, days after resuming operations following the deadly attacks (http://www.thestar.com/news/world/2016/04/07/belgian-police-launch-appeal-to-find-man-in-hat-terror-suspect.html) that killed 32 people. "It was a very important sign for us to show that we are looking ahead, looking at the future," said Kim Daenen, Brussels Airlines spokesperson. The first flight landed in Toronto Thursday afternoon, she said. It will connect the two cities five times a week. The airline announced the service in December and launch March 27, but the airport was closed. It reopened Sunday. The flight is its first connection to Canada and is part of the Brussels Airlines expansion of international flights, Daenen said. It launched flights to New York and Washington in 2011. Most North American flights to Africa stop in Brussels, so the carrier added frequencies to the 18 African countries it flies to as a result, Daenen said. The only other company with flights between Toronto and Brussels was Indian carrier Jet Airways, for which flights then went on to India. But it moved those connections to Amsterdam instead on March 27, as planned before the attacks. Brussels Airlines is part of the Lufthansa group, an Air Canada partner, so passengers will be able to book flights - and connecting flights to several countries - with the Canadian carrier. Toronto Star

INTERNATIONAL

Belgium intensifies bombing suspect hunt
Belgian prosecutors launched a public appeal Thursday seeking any information on the "man in hat" suspect in the Brussels Airport suicide bombings that killed 16 people. Belgian federal prosecutor Eric Van der Sypt said authorities were especially interested in people who might have filmed or photographed the man. He was seen at the airport with two suicide bombers before they died in the March 22 attacks. A subsequent explosion at Brussels' Maelbeek subway station killed another 16 people the same morning. Photos released by prosecutors showed the "man in hat" leaving the airport on foot, walking to the nearby town of Zaventem and then into Brussels, where all traces of him were reportedly lost. The suspect also wore a white jacket but discarded it at some point, prosecutors said. The appeal for public assistance more than two weeks after the suicide bombings indicated that investigators have hit a standstill. Three bombers, two at the airport and one in the subway, also died in the attacks, which were claimed by Daesh, also known as ISIS and ISIL. Associated Press, A14

* **Radicalization of a Belgium Student Turned Bomb Maker Was Invisible**
He attended Catholic school and studied electrical engineering. His immigrant family valued education and discipline. His brother carries the Belgian flag as a national martial arts champion. But none of that stopped Najim Laachraoui from being drawn to the Islamic State, or from turning the technical skills that could have provided a bright future to building the bombs that, the authorities suspect, were used in the recent attacks in Paris and Brussels. Mr. Laachraoui wheeled his handiwork into Brussels Airport on March 22 and, at age 24, blew himself up along with 15 bystanders, the authorities concluded after finding his DNA. Another attacker exploded a bomb nearby, and a third man detonated explosives on a subway, killing 17. The authorities suspect that bomb had also been made by Mr. Laachraoui. Until that day, Mr. Laachraoui was an unseen yet central player and a key link between the cell that carried out the Paris attacks, organized by Abdelhamid Abbaoud, and the bombers in Brussels. New York Times

* **FBI debates sharing hack with Apple**
The FBI has not decided whether to share with Apple Inc. details about how the bureau hacked into an iPhone linked to a California terrorism investigation. FBI Director James Comey discussed the situation during a speech Wednesday at Kenyon College in Ohio. He called it a "technological corner case" and said the flaw the FBI exploited in Apple's software works only on a "narrow slice of phones" - the iPhone 5C, running version 9 of Apple's mobile operating system, not on newer or older models. "If we tell Apple, they're going to fix it and we're back where we started," Comey said. "As silly as it may sound, we may end up there. We just haven't decided yet." Associated Press (Times Colonist, B3)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
January 28, 2015 / le 28 janvier 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

L'opposition rejette la prison à vie sans libération conditionnelle
Le plan du gouvernement fédéral qui viserait à imposer la prison à vie sans possibilité de libération conditionnelle rendrait le milieu carcéral plus dangereux, selon les partis d'opposition à Ottawa. Les porte-paroles du Nouveau Parti démocratique (NPD) et du Parti libéral du Canada (PLC) en matière de sécurité publique ont affirmé mardi qu'une telle mesure aggraverait l'état des criminels, mettant en danger le personnel des prisons. Lors du discours du Trône, en 2013, le gouvernement fédéral s'était engagé à adopter une telle politique, ce qui avait suscité une levée de bouclier chez les criminalistes. Selon eux, les lois actuelles prévoient déjà des mesures spéciales pour les détenus qui ont commis des délits graves - dont les meurtres en série et des agressions sexuelles sur des enfants.Privilégier la réhabilitation
Le NPD et le PLC croient que le gouvernement devrait plutôt se concentrer sur la réhabilitation des détenus. « C'est un gouvernement qui ne fait que punir, punir et punir. L'objectif de notre système correctionnel est pourtant de rendre plus sécuritaires les communautés en réhabilitant les prisonniers », a affirmé le député néo-démocrate Randall Garrison. Il a ajouté que les criminels qui purgeaient une peine de prison à vie seraient surveillés le reste de leur vie, même s'ils réussissent à sortir de prison.[…] Le **ministre de la Sécurité publique Steven Blaney** a indiqué que le projet de loi serait déposé avant la fin de la session parlementaire, au mois de juin. « ***Ceux qui commettent des crimes graves et violents à plusieurs reprises constituent une menace pour le public. Le premier objectif est de protéger le public*** », a expliqué M. **Blaney**, mardi, après la réunion d'un comité de la Chambre des communes. Le Devoir, A6 (Acadie Nouvelle, Le Quotidien)

Opposition MPs slam plan for life sentences

The government's long-promised plan to lock up some criminals and throw away the key will only make prisons more dangerous, opposition MPs say. Denying any chance of parole to the worst violent offenders will increase the chances of prison guards being attacked, the NDP and Liberal public safety critics said Tuesday as the government signalled legislation would come before summer. Opposition MPs want a greater emphasis on rehabilitating inmates. Criminologists denounced the life-behind-bars initiative after it was announced in the October 2013 speech from the throne, saying there are already legal provisions to ensure the most heinous offenders never get out. At the time, the government said those convicted of the worst crimes - such as multiple murders or sex assaults on children - could spend the rest of their lives in prison. **Public Safety Minister Steven Blaney** says legislation will be tabled before Parliament rises in June. "***People who commit serious and violent crimes in a repetitive manner constitute a menace to society***," **Blaney** said Tuesday after a House of Commons committee meeting. "***The premier objective is to protect society***." When the plan was first outlined, Justice Minister Peter MacKay said the provisions would be applied very narrowly. Chronicle Herald, A9 (Cape Breton Post, Hamilton Spectator, Times&Transcript, Times Colonist, Red Deer Advocate, Whitehorse Daily Star)

Prison watchdog pushes Ottawa on plans for solitary confinement
Canada's corrections investigator is pressing Ottawa to detail its plans to address solitary confinement in federal prisons amid growing pressure to place limits on the controversial practice. Howard Sapers says he sent a letter to Correctional Service Canada commissioner Don Head and **Public Safety Minister Steven Blaney** seeking details on more than a dozen initiatives the CSC suggested it would undertake in response to a coroner's inquest on the death of Ashley Smith. Ms. Smith died of self-inflicted strangulation in 2007 after a lengthy period in solitary confinement. A recent Globe and Mail report detailed how another inmate, Eddie Snowshoe, killed himself after spending 162 days in solitary. The CSC's response to a coroner's inquest into Ms. Smith's death included references to an effort to identify offenders at risk of segregation and a pledge to consult on the practice with other jurisdictions. The agency did not offer a detailed response to many of the jury's 104 recommendations, and rejected some, including new limits on solitary. Mr. Sapers said last month's letter requests more information on 13 initiatives that were mentioned as part of the CSC's 26-page response, including several dealing specifically with solitary confinement. Globe and Mail, A1

Feds outline more details of upcoming anti-terror bill
Public Safety Minister Steven Blaney assures the government's new terror bill expected Friday will be in "***full compliance with Canadian law***." The bill is expected to include provisions to allow "***preventative arrests***" and criminalize the "***promotion of terror***" -- measures law enforcement has indicated would help detain potential terrorists before a crime is actually committed. Asked to explain how the government will criminalize the promotion of terrorism, Blaney said the Criminal Code already contains provisions on "supporting hatred or violence." "It is really criminal to incite terror, to support terrorism or to encourage to use violence to achieve your means," Blaney said. Liberal public safety critic Wayne Easter says it's worth examining whether Canada actually needs new laws or whether it could simply make use of what already exists. "One key question is why have current laws not been utilized to the full extent we think they ought to be," Easter told reporters Tuesday, following a meeting of the House public safety committee. QMI Agency, 30 (Edmonton Sun, Calgary Sun, Kingston Whig-Standard, London Free Press); Le Droit (Le Devoir); La Presse

*** Disaster costs to triple after formula change**
The amount of money Manitoba will have to spend on natural disasters before the federal government will come to the table will almost triple next week when Ottawa changes the formula for the first time in more than four decades. **Public Safety Minister Steven Blaney** announced the changes earlier this month, as he promised also to roll out the promised $200-million, five-year flood-mitigation program promised in last year's federal budget. "***To strengthen Canada's emergency-management approach, we are shifting from a reactive model to one that allows us to better identify, plan for, and prevent flood risks and the costs for Canadians that comes with them,***" **Blaney** said in a Jan. 16 news release. However, as part of the program, he is also changing the formula for disaster financial assistance that has the federal government help provinces pay for major disasters. Since 1971, Ottawa's assistance has kicked in when the cost of a disaster reaches the equivalent of $1 per person in a province. In Manitoba, currently, that

would be $1.272 million. As of Feb. 1, the formula is going to be set at $2.92 per person, which Blaney says is equivalent to half the impact of inflation since 1971. In Manitoba, it means the province will have to cover 100 per cent of the costs of disasters up to $3.71 million. After that, Ottawa's share will be up to 90 per cent. Manitoba NDP MP Niki Ashton said Tuesday the government is once again off-loading costs onto the provinces. "This will have a huge impact in Manitoba," said Ashton. "In the last five years, we have had three major floods, as well as other disasters. Under the new rules, the current government is upping the threshold, leaving municipalities and the province with no relief." Winnipeg Free Press, A7

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fierce storm delivers as promised
A blizzard wrapped much of New Brunswick in its icy grip on Tuesday, grounding flights, closing schools and leaving many hunkered down all day long, waiting for the storm to blow away. But if the weather forecast holds true, that's going to take a while. Nearly all of the province was still under a blizzard warning by 6 p.m. on Tuesday, with another five to 15 centimetres set to fall during the night. Periods of falling and blowing snow, caused by wind expected to gust as high as 90 kilometres an hour, was expected to continue into Wednesday afternoon. "We'll still be under very strong winds for the rest of today, tonight and during the overnight period," Environment Canada meteorologist Claude C... told Brunswick News on Tuesday afternoon. "So even by daybreak on Wednesday, we'll still have brisk and strong northerly winds and some flurry activity. So there will still be some reduced visibility, but not to the magnitude of what we're getting right now." That means the drive to work on Wednesday might not be much better than it was on Tuesday. "Although conditions are expected to improve over the next 12 hours, cleanup in the wake of the storm will take some time," the province's Emergency Measures Organization warned in a news release issued late Tuesday afternoon. "Roads will remain hazardous while crews work to clear them." The provincial EMO issued a no-travel advisory for all of southern New Brunswick, including the highways that link the province's major cities, on Tuesday afternoon. The stretch of Trans-Canada Highway linking Moncton and the Nova Scotia Border, along with Route 11 between Shediac and Kouchibouguac, was closed to traffic for part of Tuesday. The Associated Press, (The Daily Gleaner, The Telegraph Journal), Times & Transcript, L'acadie Nouvelle,

*** La tempête effleure New York, frappe les Maritimes**
Des vols ont été annulés et des écoles, des bureaux gouvernementaux et des universités un peu partout dans les Maritimes ont été fermés mardi, alors qu'une violente tempête hivernale a déclenché des vents puissants et apporté de fortes chutes de neige sur la région. La tempête était déjà responsable de la fermeture d'écoles et d'entreprises dans le nord-est des États-Unis, et des milliers de vols y ont été annulés. Environnement Canada a émis un avertissement de blizzard pour l'Ile-du-Prince-Édouard, le sud-est du Nouveau-Brunswick, presque toute la Nouvelle-Écosse et pour le secteur extrême est de la Gaspésie, avec un mélange de pluie verglaçante, de vents et de neige pour Terre-Neuve-et-Labrador. Presse Canadienne (Le Devoir, A2) ; Canadian Press (Red Deer Advocate, A5; The Record, A5; Daily Star, 12; Cape Breton Post, A7; Times Colonist, A7); Associated Press (Windsor Star, A9; Vancouver Sun, B2; Ottawa Citizen, C3; Calgary Herald, D2; Edmonton Journal, A9)

*** La neige qui ne tombe pas**
Dimanche, le maire de New York avait sorti ses trémolos angoissés des grands jours de cataclysme pour annoncer, d'un ton prophétique, la tempête du siècle à venir. Ne manquaient que les trompettes de l'Apocalypse. A l'entendre, cette tempête était possiblement la plus colérique que les États-Unis connaîtraient depuis celle du Créateur qui a chassé du paradis terrestre papi Adam et sa concubine, une dénommée Eve, parce qu'elle refusait de lui donner la recette de sa fameuse tarte aux pommes américaine. Évidemment, devant cette tempête devenue historique avant même d'avoir eu lieu, CNN n'allait pas rater l'occasion d'étaler ses prouesses infographiques et «journalistiques». L'Acadie Nouvelle, 13 ; Agence QMI (Journal de Montréal, 11 ; Journal de Québec, 17) ; La Presse, A2; Associated Press (The Record, A5); QMI Agency (Ottawa Sun, 25; Toronto Sun, 56)

*** Snow on the way Thursday for Waterloo Region**

Keep watch Thursday for something unusual this winter in Waterloo Region: a steady, all-day snowfall. At least five centimetres of snow is expected across southern Ontario, with up to 10 centimetres in some areas, said Geoff Coulson, a meteorologist at Environment Canada. "Any way you slice it, it's a normal January snowfall," he said. The Record, B4

*** Des employés d'Hydro-Québec «au coeur de la tempête»**
Des employés d'Hydro-Québec basés en Estrie ont pris le chemin des États-Unis afin de prêter main-forte aux équipes américaines devant faire face à des pannes causées par l'importante tempête de neige. Une douzaine d'équipes de la région Estrie-Montérégie de la société d'État ont été dépêchées au nord de Boston et attendaient les ordres, mardi matin. « Nos employés sont au coeur de la tempête », reconnait Louis-Olivier Batty, porte-parole d'Hydro-Québec. La Tribune, 4

*** Study finds companies lag in flood preparation**
A Calgary Chamber of Commerce report on the flood of 2013 has found many city businesses remain ill-prepared for future emergencies. Its survey, released Tuesday, says 40 per cent of flood-impacted businesses still do not have off-site storage for critical documents, the ability to operate remotely or an emergency communications strategy. Calgary Herald, D2

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Limits on free speech are risky business
An opinion piece states, "When the Harper Conservative government introduces its anti-terror legislation later this week, it will walk a fine line. The legislation is needed, because the threat of terror, especially homegrown terror, is all too real, as we have seen first hand. Most of the omnibus anti-terror bill builds on existing frameworks, giving police and security officials expanded powers and making it easier to share information - including about all citizens, not just those suspected of terror links. But there is new ground here as well, and that's what we should be watching. A key feature of the new law is a measure that draws a line between free expression and endorsing terrorism. Simply put, people who verbally promote or glorify terrorism could be charged under the act. It's easy to see how this will work in extreme cases, for example, where someone praises terror attacks like the ones that happened in Canada last year. But what about in more subjective cases? Any time we limit free speech, even for a good reason, we need to tread carefully. This is no exception." Hamilton Spectator.com

Let's see the video
It's an old tradition for terrorist groups to retrospectively embrace perpetrators of attacks against innocents as their own. Al-Qaeda and Islamic State both claim involvement in the Paris attacks. Now IS seems - at least tangentially - to be linking itself to the Parliament Hill shooting via comments one militant has made in a new online recording. The RCMP, meanwhile, has a video made by the Ottawa assailant himself before the attack that may outline his motivations. It was always in the public interest for that footage to be released. The IS glorification of the attack adds to the need to do so. In the immediate aftermath of the Ottawa attack, in which Corporal Nathan Cirillo was killed, RCMP Commissioner Bob Paulson indicated the video would be made public. Then he quickly reversed himself. The Mounties contend the video constitutes important evidence. As the months roll by with no arrests of putative accomplices or facilitators, the assertion seems more like a hope than an aspect of an investigation. Globe and Mail, A12

CSE tracks millions of downloads daily: Snowden documents
Canada's electronic spy agency sifts through millions of videos and documents downloaded online every day by people around the world, as part of a sweeping bid to find extremist plots and suspects, CBC News has learned. Details of the Communications Security Establishment project dubbed "Levitation" are revealed in a document obtained by U.S. whistleblower Edward Snowden and recently released to CBC News. Under Levitation, analysts with the electronic eavesdropping service can access information on about 10 to 15 million uploads and downloads of files from free websites each day, the document says. "Every single thing that you do - in this case uploading/downloading files to these sites - that act is being archived, collected and analyzed," says Ron Deibert, director of the University of Toronto-based internet

security think-tank Citizen Lab, who reviewed the document. In the document, a PowerPoint presentation written in 2012, the CSE analyst who wrote it jokes about being overloaded with innocuous files such as episodes of the musical TV series Glee in their hunt for terrorists. CBC analyzed the document in collaboration with the U.S. news website The Intercept, which obtained it from Snowden. The presentation provides a rare glimpse into Canada's cyber-sleuthing capabilities and its use of its spy partners' immense databases to track the online traffic of millions of people around the world, including Canadians. That glimpse may be of even greater interest now that the Harper government plans to introduce new legislation increasing the powers of Canada's security agencies. CBC.ca

*** Lutte au terrorisme: les policiers et les espions n'ont pas assez de ressources, selon le NPD**
Alors que le gouvernement conservateur continue de dire que les policiers et agents du Service canadien du renseignement de sécurité (SCRS) ont besoin de plus de pouvoirs pour stopper les terroristes, l'opposition est d'avis que les policiers et les espions ont seulement besoin de plus de moyens. «On a entendu parler de policiers qui savaient qu'il y avait des individus qui se radicalisaient, mais ils n'avaient pas les ressources nécessaires pour effecteur de la surveillance», a expliqué Rosane Doré-Lefebvre, porte-parole du NPD en matière de sécurité publique. L'opposition demande plus d'argent pour le SCRS et la GRC, au moment où le gouvernement peine à équilibrer son budget. Alors que certains s'inquiètent des ressources allouées aux agents de renseignements, le réseau Global a mis la main sur les frais de déplacement du directeur du SCRS, Michel Coulombe. «Ça n'a pas de bon sens que les voyages du directeur du SCRS coûtent plus cher que ceux du ministre. Une chambre d'hôtel à 750 $ la nuit, c'est un peu exagéré», s'est indignée Mme Doré-Lefebvre en Chambre. Le président du Conseil du trésor, Tony Clement, a déjà demandé une révision des dépenses du directeur du SCRS. Journal de Montréal.com

*** Links probed**
One of the country's largest Muslim organizations gave hundreds of thousands of dollars to a Hamas-linked charity, and vocally supported an Egyptian Islamist group, QMI Agency has learned. The Muslim Association of Canada (MAC), based in the Toronto suburb of Mississauga, Ont., owns or operates at least 20 Islamic schools and 15 mosques in Ontario, Alberta and Quebec. MAC's website says the group is centred around "holistic educational and spiritual development" and "has no organizational link or affiliation with other organizations." However, QMI obtained an RCMP search warrant linking the group to IRFAN-Canada, a banned charity group and a listed terrorist organization also based in Mississauga. The Mounties, citing Canada Revenue Agency disclosure, say: "The Muslim Association of Canada (MAC) provided $296,514 between 2001 and 2010" to IRFAN-Canada. The Conservative government declared IRFAN-Canada a terrorist group on April 29, 2014 -- one day after the Mounties raided the charity. The government said "between 2005 and 2009, IRFAN-Canada transferred approximately $14.6-million worth of resources to various organizations associated with Hamas." Hamas's charter calls for the destruction of Israel. IRFAN-Canada's Ottawabased lawyer, Yavar Hameed, had no comment on Tuesday. The group is fighting its terrorist designation in Federal Court. The Mounties obtained their warrant as part of Project Sapphire, involving surveillance, wiretaps and undercover operatives in the Toronto and Montreal area. The warrant led to a raid on IRFAN's Mississauga headquarters and a Montreal apartment on April 28, 2014. Invest igators seized computer files, donation forms, and promotional videos that "demonize Israel." London Free Press, B2 (Calgary Sun, Edmonton Sun, Kingston Whig-Standard, Toronto Sun, Ottawa Sun)

*** Couillard combattra la radicalisation**
Philippe Couillard ne veut plus parler de lutte contre l'intégrisme, mais bien de lutte contre la radicalisation, axant son discours identitaire sur la sécurité. Au cours de la conférence de presse qui clôturait le caucus présessionnel des députés libéraux, Philippe Couillard a tenu à signifier ce changement de vocabulaire. Ainsi, la ministre de l'Immigration, de la Diversité et de l'Inclusion, Kathleen Weil, qui fut chargée par le premier ministre de définir un plan d'action contre l'intégrisme, s'évertuera plutôt à contrer la radicalisation. Lundi, Philippe Couillard avait affirmé que dans la mesure où les droits sont respectés, l'intégrisme " fait partie des choix personnels de chacun ". Mardi, il a cité l'exemple d'un intégriste catholique qui assiste à la messe deux fois par jour, porte un cilice et respecte toutes les prescriptions des Écritures. " Tant que cette pratique ne met pas en jeu les droits des autres, la sécurité des autres, les principes fondamentaux comme l'égalité hommes-femmes, cette pratique-là, à ce que je sache, personne ne songe à l'interdire. Et ça existe dans toutes les religions, c'est une minorité, mais ça

existe '', a-t-il expliqué. L'intégrisme peut toutefois porter atteinte aux droits, aux libertés et devenir '' de l'extrémisme qui peut mener parfois, malheureusement, à la violence '', a-t-il distingué. '' La radicalisation des jeunes et la menace de la violence terroriste, c'est un enjeu qui est distinct en lui-même et qui a ses propres dynamiques. '' Le Devoir, A3

*** New Conservative anti terror bill needs to walk a fine line, Kenney says**
There's a fine line between legitimate religious expression and inciting terrorism, says Conservative cabinet minister Jason Kenney. It's that line the government will be walking - carefully - in its new anti-terrorism bill, expected to be unveiled Friday. The bill is the government's long-awaited legislative response to two attacks carried out on Canadian soldiers last fall by men believed to have been influenced by radical Islam - attacks the government considers acts of terrorism. Though police already have the power to go after those suspecting of being on the verge of committing terrorist attacks, the new bill is partially aimed at stopping the seeds of those attacks from germinating altogether. "Our objective is not to diminish legitimate expression of political or religious views, but rather incitement to terrorism - and there is a fine line there that the legislation will try to draw," Kenney said in an interview Tuesday. "Obviously there are some malevolent religious influences that can add to the process of radicalization towards violent extremism, and we have to be extremely mindful of that." How to effectively combat radicalization is a struggle facing governments and security agencies the world over. The RCMP is currently rolling out its own strategy, which includes working more closely with community groups in order to identify and divert people who may be susceptible to extreme views that could eventually lead to violence. Ipolitcs.ca

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Fate of Roma family seeking refuge to be decided Wednesday
The fate of a Roma family seeking refuge in Canada will go down to the wire. The judge expected to rule on a stay of deportation will make a decision hours before the deportation is set to happen on Wednesday. After a Federal Court hearing on Tuesday, the judge said he would sleep on it and make a decision the following morning. Anasztazia Szilagyi, her husband and two children fled Hungary in 2011 to seek asylum in Canada. As members of Hungary's Roma minority, they say they face persecution in the country, which has seen a rise in anti-Roma rhetoric in the past years. According to a 2014 report by the Harvard School of Public Health, mainstream politicians and paramilitary groups openly incite hatred against Roma and other minority groups. Despite the dangers faced by Roma groups in Hungary, the country is on Canada's safe list following reforms to asylum rules in 2012. The family's refugee claim was denied in 2013. The Gazette

U.S.-Cuba thaw unlikely to deter defection
The young midfielder talked about it with close friends on Cuba's national soccer team and almost tried his luck on a few occasions, only to let fear deter him. But when he saw his chance - the night before a World Cup qualifying match in Toronto in the fall of 2012 - there was no hesitation, he said. He and two teammates, Odisnel Cooper and Heviel Cordoves, grabbed their passports and belongings while the rest of their group settled into their hotel rooms. They then slipped out through the fire escape and bolted down the street to avoid being spotted by their coaches. U.S. officials later confirmed the three had crossed the border in Niagara Falls, Ont. "We had to do it if we wanted to play professional soccer. We also had to do it when we were still young," Chang, 23, told The Canadian Press in a phone interview from Charleston, S.C., where he, Cooper and Cordoves play for the Charleston Battery in a lower-tier professional league. "We had already played at all levels in the national team and we realized that there was nowhere else to go," he said in Spanish. Dozens of top athletes - including many from Cuba - have defected during international competitions in an effort to escape persecution or to move up to a larger market. It's too early to tell whether the thawing relations between Cuba and the U.S., which will ease travel restrictions and may affect immigration policies, will reduce the incentive for Cuban athletes to defect while playing abroad, experts said as Ontario prepares to welcome thousands of athletes for the Pan Am and Parapan Games this summer. When Canada last hosted the Games in 1999, eight members of the Cuban delegation defected, stirring tensions between the two countries as Cuban officials accused Canadian media of inciting athletes to jump ship. When Winnipeg first staged the

Games in 1967, a Cuban boxer defected shortly after winning a gold medal. Two players from the Cuban women's soccer team defected in 2011 after facing off with the Canadian team in Vancouver in an Olympic qualifying match. They crossed into the U.S., where they were reunited with relatives. "It is fairly common given that these events bring people from different places in the world. ...They may be persecuted due to their sexual orientation, due to their political opinion and other grounds," said Jamie Liew, an Ottawa lawyer specializing in immigration and refugee law. (…)Athletes seeking to stay in Canada rather than head south of the border will have to go through the same process as any other asylum-seekers, Canadian officials said. "Canada's refugee policies are applied consistently regardless of any special event," a spokesman for Citizenship and Immigration Canada said in an email. In the past, there were allegations that Ottawa - or NGOs acting with federal approval - actively encouraged defection, Kidd said, more to embarrass its political rivals than to bolster Canadian teams. More recently, he said, Canada "has not gone out of its way to recruit defectors, it has simply considered and supported those who have asked for refugee status." The Canadian Press (Times & Transcript)

Cross-border shopping drops

The Canadian dollar is down, but a Port Huron official says Canadian visitors haven't disappeared from the community on the Michigan side of the Blue Water Bridge. The loonie traded at 81 cents US Tuesday, according to the Bank of Canada's website, and Statistics Canada says same-day car trips to the U.S. dropped more than 2% in November." People tend to come over here and shop from Canada for a number of different things," said Thelma Castillo, president of the Blue Water Area Chamber of Commerce in Port Huron. "They come over here for gas; they come over here for entertainment. "They come over here just to come over here, so I don't really think the dollar really impacts their spending habits. "John Elliott, chief executive of the Canadian side of the Blue Water Bridge, said overall traffic on the crossing tends to be consistent year to year, but car traffic into Michigan has been down about 3% recently, and dropped 6% in December. "That has to do with the exchange rate, to one degree or another," he said. The London Free Press

Canadians can sort out CETA

In the early 1980s, Canadians witnessed the sorry spectacle of provinces roaming around Westminster, cap in hand, lobbying British politicians to save them from their own federal government in its move to patriate the Constitution. It was a sad chapter in Canadian political history, provinces invoking Britain's role as colonial master, asking Britain to save them from their own federal government because the provinces couldn't settle internal differences with Ottawa by their own means. This time, it's Newfoundland and Labrador complaining about a fisheries compensation deal with Ottawa that's supposed to help ease adjustment once the Canada-EU trade agreement (CETA) comes into effect. (…)The CETA, of course, provides tariff-free access to the huge EU market and many other benefits for exports of Canadian goods and services. This includes seafood and other exports from Newfoundland. So in the end, Newfoundland would be the big loser. Globe and Mail

Wine retail policy changes violate NAFTA, California vintners say

Some of British Columbia's liquor policy changes violate Canada's international trade obligations, such as the North American free-trade agreement, says a U.S. wine industry group. The Wine Institute, which represents more than 1,000 California wineries and associated businesses, has sent a letter to B.C. Premier Christy Clark requesting that the revisions be withdrawn or modified. The institute says the changes, announced last month, will further disadvantage imported wines. (…) Max Cameron, a political science professor at the University of British Columbia who has also written a book on NAFTA, said in an interview that the Wine Institute appears to have a point. "This looks like a classic example of a non-tariff barrier that would essentially discriminate against a product from another NAFTA member. And, I think on the face of it, it looks to me like they've got a pretty compelling case," said Prof. Cameron, author of The Making of NAFTA: How the Deal Was Done. Globe and Mail

$35 million tunnel plaza upgrades unveiled in Windsor

It's been fully serviceable since November, but federal and provincial government officials on Tuesday unveiled the $35-million tunnel plaza improvements in downtown Windsor. "This is going to be a real asset for Windsor and Detroit," said Neal Belitsky, CEO of the Detroit-Windsor tunnel. "It's important in terms of esthetics, efficiency, convenience and security. "This should be the model for all border

crossings between Canada and the U.S." The tunnel improvement effort has been in the works for several years and includes a new commercial customs and bus inspection building, improved employee parking and an expanded footprint to help take traffic lineups off city streets. Funding for the project came out of the $300-million Lets Get Windsor-Essex Moving commitment made by the federal and provincial governments over a decade ago. The Windsor Star

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Small businesses must address privacy**
Imagine finding out that a stranger has received highly sensitive information about you because a company has sent your mail to the wrong person. Or asking to look at your own personal information for the sake of fixing a suspected error, only to be denied access to it by the company that collected it. As privacy commissioner of Canada, it's these kinds of things I want to draw attention to on this Data Privacy Day. About a third of private-sector privacy complaints to my office under the Personal Information Protection and Electronic Documents Act, Canada's federal private-sector privacy law, involve smaller businesses that employ fewer than 100 people. Winnipeg Free Press, A9

*** Kenya's Christian-owned Hope FM radio hijacked**
Suspected hackers briefly hijacked a popular Christian radio station in Kenya, and played Islamic verses before it went off air. Hope FM said on its Facebook account that a "foreign signal" had interfered with its broadcast on Tuesday night. It resumed transmission about three hours later. BBC News

*** Taylor Swift se moque de son hacker**
La chanteuse Taylor Swift s'est moquée hier du hacker qui a brièvement pris possession de ses comptes sur les réseaux sociaux et menacé de publier des photos de la star nue, affirmant qu'elles n'existent pas. Les comptes Twitter et Instagram de Taylor Swift avaient été piratés par au moins un hacker qui a menacé de publier des photos nues d'elle si ses fans ne le payaient pas avec suffisamment de bitcoins, une monnaie virtuelle. «Un hacker qui dit avoir des photos de moi nue"?» a écrit la star lorsqu'elle a pu reprendre le contrôle de son compte Twitter. «Pfff tu aimerais bien mais tu ne peux pas! Amuse-toi bien sur Photoshop parce que tu n'as RIEN.» Taylor Swift, très active sur les réseaux sociaux, est l'une des quatre seules célébrités à être suivie par plus de 50 millions d'utilisateurs sur Twitter. Associated Press (Le Soleil, 36)

*** Facebook paralysé**
Facebook est tombé en panne pendant une cinquantaine de minutes tôt, hier, dans plusieurs pays. La panne a notamment affecté les abonnés du Canada, des États-Unis, du Royaume-Uni, de l'Australie et de pays d'Asie. Peu après la reprise des activités, une multitude d'abonnés asiatiques ont rapporté que les fonctions étaient lentes et incomplètes. Le réseau Instagram a aussi été affecté. Facebook a publié un communiqué assurant que la panne s'était produite lors de mises à niveau techniques, non pas à cause d'une cyberattaque. Cette panne a été la plus longue à toucher Facebook depuis celle du 24 septembre 2010 qui avait duré 90 minutes. Associated Press (Le Soleil, 19 ; The Record, E3)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Police probe shooting in Langford
West Shore RCMP were investigating after reports of a shooting in Langford on Tuesday night. There are reports a man was shot and that police are looking for the shooter, but RCMP have not yet confirmed that information. The condition of the victim was unknown. Sooke Road between Jacklin and Anders roads was blocked off as police investigated. Times Colonist, A1; 1 ; Postmedia News (The Province)

Painkiller linked to rising number of Alberta deaths
highly potent drug often fashioned to appear like a prescription painkiller has caused a big spike in fatal overdoses in Alberta - with dozens of deaths in the past two years - as emergency rooms grapple with an influx of affected patients. Authorities believe this rise in abuse of fentanyl, a potentially lethal narcotic, is

linked to the release of a prescribed painkiller designed to deter illegal abuse. OxyNeo was introduced to the Canadian market in 2012 as a new version of OxyContin, pills that addicts crushed, injected and snorted, leading to a spate of overdoses and deaths. OxyNeo pills contain the same painkilling drug, oxycodone, but they are designed to be more difficult to abuse: they squish when pressed and turn to gel when dissolved in water. The move may have served as a deterrent, but it also led to the spread of replacement drugs such as fentanyl. Fentanyl is often sold to drug users as oxycodone, according to medical and law enforcement authorities... Investigators with the Alberta Law Enforcement Response Teams (ALERT), a provincial umbrella organization, believe organized crime is responsible for bringing fake OxyContin tablets containing fentanyl into the province. Since April 2014, ALERT has seized nearly 3,200 of these pills across Alberta, including more than 2,000 in Grande Prairie, 800 in Medicine Hat, more than 100 in Calgary, about 90 in Edmonton and roughly 35 in Red Deer. ALERT investigators believe the pills are made in clandestine labs, but they don't know where, said Staff. Sgt. Rod Klassen. A separate investigation by RCMP and Saskatoon police led to a series of raids in Saskatchewan and Alberta earlier this month that yielded more than $8 million worth of drugs. The seizures included more than 3,000 fentanyl pills with the same chemical composition as narcotics linked to three overdose deaths in Saskatoon. Thirteen of the 14 people charged in the bust are members of the Hells Angels or the Fallen Saints, another motorcycle gang, police say. Postmedia News (Edmonton Journal, A1, Calgary Herald, A1))

Shot RCMP officer recovering, wife says

It's been almost two months since an RCMP officer was shot during a traffic stop in Kamloops and now his wife says they're confident he will overcome his substantial injuries. Colleen Michaud says her husband, Cpl. Jean-Rene Michaud, was shot several times and critically wounded in a senseless and unforgivable act of violence. She says her family has suffered a great deal and she is deeply saddened and angry that two more RCMP families are experiencing similar pain after two Mounties were shot in Alberta. Michaud says her husband has endured many surgeries, countless complications and setbacks and has a long road to recovery, but he has shown courage and strength at every step. She says she, their two young children and the rest of their family has received overwhelming support from across the country and that she's thankful for the encouragement and thoughtfulness. Postmedia News (Vancouver Sun); Canadian Press (Times Colonist, Daily Gleaner)

Eight banks robbed in eight weeks, three provinces

Mounties are searching for a man who they say has leapfrogged between British Columbia, Alberta and Saskatchewan robbing banks at gunpoint. At a news conference in Kelowna on Tuesday, Mounties said the man has robbed eight banks over an eight-week period. The first robbery police recorded was Dec. 1 in Princeton, B.C. Eight days later the same man was 200 kilometres to the north where he held up a Vernon financial institution. Between Dec. 19 and Jan. 21, the same suspect jumped between the three provinces, holding up banks in High River, Alta.; Merritt; Swift Current, Sask.; Lethbridge, Alta.; Claresholm, Alta., and finally Langley. RCMP Const. Kris Clark said the sheer number of robberies by the same suspect concerns police. "We have a series in the past, but nothing necessarily to this extent, with the number of robberies that have occurred and crossing multiple jurisdictions and multiple provinces." No one has been hurt in the robberies, Clark said. "It's also very concerning that a firearm has been involved in all incidents either the mention [of a weapon] or produced and obviously we're concerned for public safety." Canadian Press (Times Colonist); Postmedia News (StarPhoenix, Leader-Post, Calgary Herald); QMI Agency (Edmonton Sun, Calgary Sun)

'We're no good to anybody if we don't arrive safely,' says RCMP officer

Emergency response officials say they were prepared to answer the call during Tuesday's blizzard. Insp. Dan Goodwin, West District operations officer for the RCMP in New Brunswick, said the challenge on such days is being able to get to a call in a timely manner. Goodwin said the force has a fleet of four-wheel drive vehicles and the patrol cars have all-wheel drive. "We can respond; we're prepared to respond," Goodwin said. District wide, Goodwin said members told him that the roads are bad and visibility is terrible. "It's the blowing snow and there's going to be drifting involved so just take precautions," he said. "Our members, we are talking to them and they're urging people to make sure they have their headlights on and their full headlights. "Sometimes the running lights are on and the taillights don't come on unless you activate the full headlight." As of mid-morning, Goodwin said the force hadn't

responded to many accidents, as motorists were apparently heeding warnings to stay off the roads. On days like this, Goodwin said, the RCMP will look at the nature of a particular situation and react accordingly. Daily Gleaner, A3

Moncton shootings RCMP bill nearing $4M, says city councilor
The provincial government, the federal public safety department and the RCMP all deny they are in negotiations with the Codiac Regional Policing Authority to cover the extra costs related to RCMP operations following last June's murder of three constables in Moncton. The authority functions as a police commission and its role is to set the budget for the communities of Moncton, Dieppe and Riverview - communities that are patrolled by the Codiac RCMP detachment. In October, chairperson Nick LeBlanc wrote a letter to the provincial public safety department asking it to cover 100 per cent of the cost of bringing in hundreds of officers from across the country for several weeks. In the letter, he noted the provincial government had declared this event a provincial emergency. LeBlanc isn't saying much about where things stand now. "I won't discuss the negotiations until it is settled," he said. Public Safety Minister Stephen Horsman said in December that any other municipalities in the province would have had its costs covered by the province. However, that rule did not apply to the Codiac detachment. Horsman says that's because the Codiac policing contract was signed with the federal government. "The responsibility for Codiac's costs incurred during the the emergency is a matter for discussion between the parties," he wrote. CBC.ca

10 arrested as RCMP bust grow-op in 'very large' Langley barn
Several thousand marijuana plants were seized and more than 10 arrests made during a massive grow-op bust in Langley Tuesday. The investigation began four weeks ago, centring on a sevenacre rural property in Langley on Zero Avenue and 264th Street, according to Sgt. Laurie White of the RCMP's federal serious and organized crime unit. "The focus is on a very large barn - and by large, I mean it's 51,000 square feet," White said. The property features many access points and is located close to the Aldergrove border crossing. White said the barn posed a "huge safety risk" because the electrical system was wired improperly to allow for extra lights. Many rooms held what was estimated to be several thousand marijuana plants. Postmedia News (The Province, A13)

Mountie killer proves legal system broken
An editorial states, "Canada's legal system has lost its way and now a good man is dead. Enough is enough. The more we learn about Shawn Matthew Rehn, the more we're in disbelief that the system let this man walk the streets. He should have never had the chance to be in that Alberta casino last Saturday, where he shot two RCMP officers. One of them, Const. David Wynn, died in hospital. He leaves behind a wife and three children. If you look at the facts, Rehn was clearly a danger to society. He had 98 convictions and outstanding charges against him. The list runs the gamut: domestic violence, home invasion, armed robberies, drug offences. Sure, he'd never been imprisoned for murder before. But to say this guy was an accident waiting to happen is an understatement. His offences included violating parole conditions and skipping bail. What judge would release someone after he's proven that he not only has total disregard for the laws of the land, but that he's not even going to follow his bail conditions? Yet judges continued to let him out. He was before a judge in December 2013 for multiple offences including resisting a peace officer. Then, just this past September, he faced eight charges. In October he was taken in again for driving without a licence and evading an officer, among other charges. RCMP Assistant Commissioner Marlin Degrand told the media: "We're very concerned about the fact that an individual with his criminal history came into contact with our officers." You don't say..." Sun Media (London Free Press)

System is detached from society
An editorial states, " On Monday, the RCMP family and the community of St. Albert laid to rest Const. David Wynn (42), a husband and father of three. Wynn, of course, died from a gunshot wound to the head inflicted by serial criminal Shawn Rehn while Wynn was investigating a stolen vehicle at a casino in suburban Edmonton in the early morning hours of Sat., Jan 17. Thousands of police officers from across the country gathered in St. Albert to honour Const. Wynn. Thousands more attended services across the country to remember their colleague. It was truly moving. But one thing kept coming to mind during the regimental funeral: Const. Wynn didn't have to die. No justice system will ever be perfect. There is no

guarantee that even if Canada's criminal justice system was tougher that Shawn Rehn would have been behind bars on Jan. 17 rather than roaming free to kill Dave Wynn. But making it harder for repeat offenders to get bail couldn't hurt. That would better protect frontline police officers and the public from sociopaths like Rehn. The numbers in Rehn's rap sheet bear repeating. He had 98 convictions or outstanding charges against him. And yet, somehow he kept being released on bail... Let's just admit it. In important ways our justice system is broken. It has become detached from the society it is supposed to protect. And Const. Wynn is a victim of that disconnect. Stop studying the system and start tightening it up." QMI Agency (Edmonton Sun, Kingston Whig Standard, Winnipeg Sun, Toronto Sun, Ottawa Sun, Calgary Sun, London Free Press)

Wynn's death must lead to change

An opinion piece by Howard Burns, president of the Calgary Police Assoc. states, Re: "Final farewell to fallen Alberta Mountie," Jan. 27. RCMP Const. David Wynn is the latest Canadian police officer to be gunned down in the line of duty by a career criminal whose history causes us to question why he was free to commit this horrendous act. Justice Minister Jonathan Denis has ordered a full review into the matter. That is a good start, but a review with no meaningful change is futile. Federal Justice Minister Peter MacKay has rejected a full-blown examination into Wynn's death. With an election on the horizon, MacKay may be reluctant to direct public attention to Canada's failing justice system. In 2005, James Roszko murdered four RCMP officers in Mayerthorpe. The justice minister ordered a full review of his criminal prosecutions. Before Mayerthorpe, there was the 1990 murder of Edmonton police Const. Ezio Faraone. He was viciously mowed down with a sawed-offshotgun after cornering career criminals Albert Foulston and Jerry Crews, after a bank robbery. Foulston received a statutory release from prison in 2009 and has been in and out of jail ever since. Time will tell on that one, but our justice system seems bent on providing the opportunity. Canada's justice system is in desperate need of significant parole and bail reform. The Alberta Federation of Police Associations and the Canadian Police Association have lobbied for meaningful changes for several years now, such as making parole something that is earned and increasingly more difficult to achieve for those who demonstrate a disregard for the law. How many more lives need to be lost before significant changes are made? We are playing Russian roulette with Canadian lives and it is more difficult to act surprised when the gun goes off. " Calgary Herald, B5

*** Drunk driving message slow to sink in, says Prince District RCMP**

Statistics from all three RCMP districts in Prince Edward Island show that there continues to be problems with impaired drivers in every county of the province, say Prince District RCMP, which released its 2014 numbers recently. As was the case in both Kings and Queens districts, Prince District RCMP laid a number of charges for impaired driving-related offences. Prince County laid 57 charges relating to impaired driving, compared with 44 in Kings District and 60 charges in Queens. Queens and Prince district numbers do not include charges laid by Charlottetown, Kensington and Summerside police. The Prince District statistics present a fairly even distribution across the age groups: 33 of 57 charges were laid on drivers 31 and older, while the remaining 24 were 30 and younger. "It's hard to imagine that adults are unable to grasp the simple 'don't drink and drive' philosophy," the RCMP said in a statement. "Sadly, many are hurt, killed or hurt and kill others before the message sinks in." Prince District also handed out 15 roadside suspensions in 2014. The Guardian, A4

*** Judge decides RCMP justified in shooting**

An Alberta judge has concluded RCMP officers reacted as they were trained in the shooting death of a man in Sherwood Park in 2011. The fatality inquiry, held in November 2013, into the death of William Francis McCoy, 56, made no recommendations for the prevention of similar deaths. Provincial Court Judge Bruce Garriock concluded the actions of McCoy left the RCMP with no other choice, but to use lethal force. McCoy phoned the RCMP the morning of Jan. 16, 2011, saying he was on the road outside his home in Sherwood Park and was going to shoot himself. Police established a perimeter around McCoy, who was discovered carrying a shotgun. Police asked some nearby residents to leave their homes for their own safety. In total, 37 RCMP personnel, two Edmonton police and three emergency medical staff spent eight hours trying to negotiate with McCoy to put his weapon down. RCMP officers testified McCoy was "very distraught, verbally abusive, highly agitated and very angry," and made repeated threats to kill himself and anyone he saw. He did not respond rationally to RCMP efforts to assist him and it appears he "intended to engage the police in a confrontation to end his life." McCoy

refused repeated requests to drop his weapon. One of the RCMP officers said McCoy began raising the barrel of his gun toward officers. It was at that point that four RCMP members shot McCoy. "I am satisfied that the RCMP members and the ERT (emergency response team) members who were involved did all that was reasonably possible to achieve their goal ... to contain, isolate and encourage McCoy to arrive at a peaceful resolution through negotiation," Garriock wrote. Edmonton Journal, A5

*** UFC's Sheldon Westcott puts fight thoughts aside, focuses on fundraiser for slain RCMP officer**
While Sheldon Westcott has begun preparing for his next Ultimate Fighting Championship bout, one that will take place halfway around the world in April, much of his immediate focus is on a tragedy that hit close to home. The UFC prospect is pitching in to contribute to a fundraiser in memory of Const. David Wynn, the 42-year-old RCMP officer, husband and father of three, who died Jan. 21, four days after he was shot while checking on a stolen vehicle at the Apex Casino in St. Albert. Money raised through a silent and live auction, donations and more will go to Wynn's family and to help support Aux. Const. Derek Bond, who was injured during the shooting. Westcott, a 30-year-old native of St. Albert, said it is a privilege to have any role - big or small - in an event honouring the slain officer and his partner. Star Phoenix

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Corrections workers made 'offensive' edits
Federal correctional workers who have been using government computers to make Wikipedia edits may face disciplinary measures for posting "offensive and inappropriate" comments on the site, an agency spokesperson says. The edits range from homophobic remarks to commentary about Correctional Service Canada to apparent inside jokes between employees. In some instances, names of current correctional officers were also posted on the online encyclopedia. "CSC employees are expected to act according to the highest legal and ethical standards," spokeswoman Veronique Rioux said in an email. "The content (the Citizen) highlighted is indeed offensive and inappropriate. CSC is examining this matter and disciplinary measures will be taken as appropriate." In January 2014, someone using the CSC network wrote that Fenbrook Institution in Gravenhurst, Ont. - now amalgamated with Beaver Creek Institution, a medium-and minimum-security prison - "operates quite differently than other institutions" by allowing "protective custody" inmates to "operate as if they were 'Free Men,' allowing them to shop, cook and court as if they were in Canadian Society." The editor cited "Facebook" as the reference. The edit goes on to say: "While the Correctional Service of Canada does not have an official position or statement, Fenbrook is known to house the largest concentration of Homosexual Inmates in the entire Ontario Region." Ottawa Citizen, A1

Parole board puts restrictions on violent offender
A man who stabbed and bit one man and kicked another in the head 10 times will be under several restrictions when he is released from prison next month. Mathieu Terrence Myers has been serving two years, four months and 17 days in prison on several charges, including uttering threats, aggravated assault and assault causing bodily harm. Myers broke into his former girlfriend's apartment, stabbed a man who was with her, bit him and accidentally cut her. While in jail he assaulted another inmate, kicking him in the head 10 times. The victim was unconscious after the first blow. Myers is eligible for statutory release on Feb. 14 and in its report, the parole board imposed eight conditions, including that he not have any contact with the victims or their family members. (...) The report said Correctional Service Canada was of the opinion some of Myers' behaviour was the result of "grandstanding" and trying to impress other offenders. The Guardian, A1

Opposition rejects life-in-prison plan
The government's long-promised plan to lock up some criminals and throw away the key will only make prisons more dangerous, opposition MPs say. Denying any chance of parole to the worst violent offenders will increase the chances of prison guards being attacked, the NDP and Liberal public safety critics said Tuesday as the government signalled legislation would come before summer. Opposition MPs want a greater emphasis on rehabilitating inmates. Canadian Press (The Guardian, A5, Waterloo Region

Record); * Presse canadienne (Le Quotidien, Le Droit, La Tribune), * QMI Agency (London Free Press, Kingston Whig-Standard, Calgary Sun, Edmonton Sun)

Solitary confinement legal challenge filed
The federal government is facing a second court challenge to the use of solitary confinement in prisons. The Canadian Civil Liberties Association and Canadian Association of Elizabeth Fry Societies have filed a petition in Ontario Superior Court. The petition seeks to challenge the constitutionality of isolation, which the groups call cruel and inhumane. Last week, the B.C. Civil Liberties Association began a similar action in British Columbia. Toronto Star, A6

*** Murderer found dead in his cell**
A man serving an indeterminate sentence for the 1986 slaying of his brother's estranged wife and her pregnant friend was found dead in his cell at the Drumheller Institution. Earl William Davenport, 56, was discovered unresponsive Monday in the medium security unit northeast of Calgary. "Inmates are counted several times during the course of the day. It was slightly before noon when staffwere doing their count and noticed him," said JeffCampbell, regional communications manager with Correctional Service Canada. "He was in his cell and he was unresponsive at that time, so they made efforts to resuscitate him. But unfortunately, they were unsuccessful." The cause of death has yet to be determined, but there is no indication of foul play, Campbell added. Davenport had been at the Drumheller Institution since Nov. 27, 1987, for the first-degree murder of Laura Ann Davenport, 31, and the second-degree murder of Susan Joy Hornbeck, 30, in Hamilton, Ont. (...) The police and coroner have also been called, a standard procedure in all cases involving the death of an inmate, and Correctional Service Canada has launched a review. "This is something we take very seriously, when there's a death in custody," Campbell said. "Certainly, we want to determine all the circumstances around his death." Calgary Herald, A13, Calgary Sun

*** Cruel and unusual**
An editorial states, “For three-and-a-half years - over half the time she spent behind bars - Bobby Lee Worm lived in a woodshedsized cell for 23 hours a day. Some days, the only human contact she would have was when a small slot in the door opened and a guard passed her a tray of food. "Being locked up like that you start to feel like you're losing your mind. The only contact with another human is through a food slot. Days turn into nights turn into days - and you have no idea whether you will ever get out," Ms. Worm told the Vancouver Sun in 2013. "If you're not broken when they put you into a hole, you're broken when they take you out." Ms. Worm was not incarcerated in some benighted country with no respect for human rights; she was a ward of the Canadian state. Luckily for her, the B.C. Civil Liberties Association (BCCLA) took up her cause and got her released from solitary confinement. But unfortunately, her experience is all too common: One quarter of prisoners in Canadian jails have spent time in solitary. At any given time, approximately 1,850 prisoners are being held in segregation in federal and provincial prisons across the country. Many of them are not told when they can be expected to be released from solitary, or what they need to do to get out, the BCCLA points out. Nor do prisoners have access to any administrative procedure to try to contest their confinement before a third party. The results of this system of administrative segregation, as it is known in the prison system, are less than favourable. Numerous studies have shown that solitary confinement can exacerbate or even cause mental health issues, including psychosis, hallucinations and insomnia. And as the case of Ashley Smith - who spent more than 1,000 days in solitary before taking her own life - highlighted, it also increases the risk of suicide, which is seven times higher in the penal system than it is for the country as a whole, with close to half of deaths occurring in solitary confinement. Following Ms. Smith's tragic death, a coroner's inquest recommended that "indefinite solitary confinement ... be abolished," and that the use of administrative segregation be limited to a maximum of 15 days. In December, Corrections Service Canada dismissed the coroner's recommendations outright. This was not the first time the government has ignored calls for reform: Previous reports written by former Supreme Court justice Louise Arbour (who called for limits on the amount of time prisoners can spend in solitary) and Canada's prison watchdog (who called for a prohibition on putting mentally ill inmates in solitary confinement) were also ignored. In fact, while other Western countries are reducing their reliance on solitary confinement, Canada has increased its use by 6% over the past five years.” National Post, A8

*** Murrell's death a mystery**
An autopsy on the body of John Murrell did not disclose a cause of death, his aunt said Tuesday. 'They don't know why he died, said Vera Stortz, saying the medical examiner's office is now "waiting for (toxicology) tests.' Murrell, 37, was found dead early Sunday in his room at an Edmonton halfway house apartment he shared with other parolees. Murrell was released about a month ago from a B.C. prison after spending most of his adult life in prison. He told the Sun just days before he died that he was working full-time and was trying to make a fresh start. Murrell was five-years-old when his sister, Tania, 6, vanished without a trace while walking the two-blocks home from a city school on Jan. 20, 1983. Edmonton Sun, 8

*** Parole must stay**
An editorial states, "One of the most distinctive things that sets Canada apart, for the better, from the U.S. is its far more humane attitude toward incarceration, as manifested by the provision for parole for even the most heinous crimes. We need to keep it that way. That's why news that the federal government is planning legislation that would deny some killers any chance of parole is both alarming and disheartening. The justice system must not lose its inherent belief in human redemption. Some criminals, deservedly, will never be paroled. Paul Bernardo is one. And Clifford Olson was in prison for life. We're pretty sure ex-Col. Russell Williams isn't ever getting out either. The new law, however, would mean that people with first-degree murder convictions who have killed prison guards or police officers, along with anyone who commits murder while sexually assaulting their victim, and anyone convicted of kidnapping, terrorism, or other as yet undefined vicious murders, will never be eligible for a parole review. Sentencing right now for first-degree murder is life, with the chance of parole after 25 years. That doesn't mean everyone automatically gets parole, and it shouldn't mean that, of course. However, to take away an offender's access to parole forever, from Day 1, is to ignore the fact that people change, that they can be rehabilitated, that they can redeem themselves, and that a 30-year-old who has murdered someone is not necessarily that same individual 25 years later at age 55. Removing any possibility of parole also removes any hope and any incentive for an offender to walk down that path to rehabilitation. There can be no possible motivation for change when one is sentenced to spend the rest of one's life behind bars with no chance of getting out." Calgary Herald, B4, Globe and Mail

*** De la poudre... de lait dans les prisons**
Fini le lait frais dans les pénitenciers fédéraux. Les prisonniers passent à la poudre. Afin d'économiser, le Service correctionnel du Canada a décidé de moderniser ses services d'alimentation, notamment en centralisant ses achats. Ainsi, depuis août, les établissements de l'Ontario, du Québec et des Maritimes passent au lait en poudre, comme cela prévalait déjà dans l'Ouest. Mais le Bloc québécois considère que cela conduit à des incohérences. Ainsi, les pénitenciers de Cowansville et de Drummondville, situés près de fermes laitières, reçoivent désormais de la poudre provenant... de Winnipeg. " La Laiterie Chagnon livrait depuis des décennies 12 000 berlingots de lait par semaine " à ces deux endroits, a rappelé le député Louis Plamondon. Il a demandé au gouvernement de revoir cette " décision aberrante " qui entraînera des pertes d'emplois au Québec. Le Devoir, A2, La Presse (Voix de l'Est)

*** Why the prison farm issue won't go away**
An opinion piece states, "During a day of protest on Parliament Hill in 2010, farmer Jeff Peters -- along with Pauline Lally of the Sisters of Providence -- spoke alongside a donkey bearing a sandwich board that read, "Conservative Prison Farm Consultant." The government's decision to shutter prison farms had provoked the rally. Later, Peters got a call from CBC Radio's The House, a show on Canadian politics hosted by Evan Solomon. "We want the farmer, the nun and the donkey," the Ottawa producer said. Somehow the farmer coaxed Stormy the donkey up the stairs at the Sparks Street broadcast centre, across a wide expanse of carpeting, into the studio and down the stairs again without, um, incident. Peter, who farms near Kingston, got a good laugh telling that story at a recent showing in The Screening Room of Til the Cows Come Home, a gripping, one-hour documentary film about the controversial decision to close two prison farms in Kingston (and four others across Canada). Peters is seen in the film being arrested by Kingston Police during a two-day-long sit-down protest in August 2010 aimed at blocking cattle trucks from carting away 150 dairy cows that, along with some 2,000 chickens, were the mainstay of the farm at Frontenac Institution (beside Collins Bay Institution). When arrested, Peters was wearing his trademark tan ball cap and green T-shirt with white lettering that read, "Save Our Prison Farms." The

one he wore to the screening read, "Restore Our Prison Farms," and on the back, "Your Vote Matters." (…)Two aspects of the prison farm story are remarkable: its location and its longevity. The blockade drew 200 people and saw 24 arrested for civil disobedience -- the youngest a 14-year-old girl, the oldest an 87-year-old woman. Margaret Atwood had earlier led more than 1,000 Kingstonians in an unprecedented march on the regional headquarters of the Correctional Service Canada. All this in a conservative bastion where John A. Macdonald practised law and is buried." Kingston Whig-Standard, B5

* **Criminal psychopaths don't understand punishment**
The worst criminals, from serial murderer and rapist Ted Bundy to fictional characters such as the cannibalistic serial killer Hannibal Lecter, share distinct personality traits: they're callous and glib; manipulative and cold; pathological liars yet quite charming. Not only do their brains appear to function differently from run-of-the-mill violent criminals, but they may also be resistant to punishment, new research suggests. "This is the first information we have that shows they don't understand the consequences of punishment. And like most of us, they are driven by reward," said Université de Montréal professor Sheilagh Hodgins, who led the study at King's College London with a local team of researchers. According to data, one in five jailed violent criminals is a psychopath, compared with about one per cent in the general population. What the study set out to do was to understand the difference between the usual anti-social, aggressive criminal and the psychopath. (…) Called Punishment and the Psychopath, the study, to be published Wednesday in the journal Lancet Psychiatry, could help inform intervention programs for violent offenders who do not benefit from rehabilitation programs. Also, the study's findings could help in the development of prevention programs for children with "conduct problems" who repeatedly break the rules despite sanctions from parents and teachers and incarcerations in youth protection. Postmedia News (StarPhoenix, A7, Leader-Post, National Post, Calgary Herald, Montreal Gazette)

* **Giant Mine bomber's parole conditions changed**
The Parole Board of Canada has changed Roger Warren's parole conditions so that he can spend an extended period away from his halfway house for medical treatment. Warren, 71, was sentenced to life in prison in 1995 after confessing to planting a bomb that killed nine men during a bitter labour dispute at Giant Mine in 1992. An e-mail from the parole board, dated Jan. 13, indicates it authorized the leave because Warren was in hospital being treated for pneumonia and his file indicates more hospitalization will be needed for further testing. Yellowknifer

* **Ex-prison guard guilty of smuggling contraband**
A former correctional officer accused of smuggling contraband into a medium security prison in Ontario has pleaded guilty to a breach of trust charge. Darrell Fairman, 54, of Trenton entered the guilty plea during a court hearing in Cobourg, Ont., on Monday. He did not enter a plea for a second charge of possession of contraband. Fairman was working as a correctional officer at Warkworth Institution, near Campbellford, Ont., when police conducted a search following suspicions that a staff worker was smuggling items into the facility. The OPP said that during the search they discovered unidentified contraband in Fairman's possession. Metroland Media (Mississauga News) (2015-01-27)

Cruel and unusual: why 'tough on crime' agenda may cost Canadians
When he looked out his window in January 2010, Jeffrey George Ewert claims he thought the nation must be at war. Men holding automatic weapons patrolled the halls. He was forced from his room at gunpoint, strip-searched and denied a shower, a phone call and fresh air in the days that followed The twist in the 52-year-old's claim — his room was a cell and his hallway a corridor in B.C.'s Kent Institution. But Ewert says the prison is his home nonetheless. "I was denied basic human rights," he claims in a BC Supreme Court affidavit. "I could not get my mind off the thought that at any moment, amidst all this tension, yelling of orders and aggression, that something was going to go terribly wrong and my head would get blown off." The tension between incarceration and human rights is at the centre of a precedent-setting proposed class action lawsuit related to a violent lockdown at Kent. Ewert is the lead plaintiff, and his lawyer will make final arguments for certification on Friday. By any stretch of the imagination, the 220 potential complainants make for unsympathetic plaintiffs: violent men, sex offenders and murderers scattered in institutions across Canada. But they're the same type of inmates the BC Civil Liberties Association and John Howard Society seek to represent in another lawsuit launched last week against Canada's attorney

general. They claim the government's use of solitary confinement amounts to cruel and unusual punishment. (...) Ewert's lawsuit followed a scathing report on the Kent lockdown by federal Correctional Investigator Howard Sapers. CBC News (2015-01-27)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Grieving Vancouver mothers speak out about gang life**
Two Metro Vancouver mothers who lost their children to gang violence six years ago say they hope a new anti-gang video campaign will help steer youth away from the deadly lifestyle. Carol Kinnear, who's featured in six videos created by the Combined Forces Special Enforcement Unit and Odd Squad Productions, says she wants to spare other parents from the devastating pain that has rocked her family. Kinnear's daughter Brianna - who had been dating gangster Jesse Margison - was shot to death in Coquitlam on Feb. 3, 2009. No one has been charged in her death. She was 22. "We live with this tragedy every single day and it is just a heartache that I don't really want any other parent to go through," Kinnear said in an interview. "I don't want any other child to put their parents through it. So I thought maybe it's time for me to try to put a message out there." Postmedia News (The Vancouver Sun, A5)

*** Big bucks going to fight gangs**
The city is poised to add $250,000-$350,000 to its fight against gangs, specifically to help extract gangsters from the criminal underworld, the Sun has learned. The 2015 draft budget will be tabled next week with an anticipated cash injection for programs reintegrating former gang members into society. It's the so-called "exit strategy" needed to complement police enforcement. Nothing would be final until council votes on the budget in March after a month of public consultation. Stittsville Coun. Shad Qadri, the chairman of Crime Prevention Ottawa, didn't want to say how much more he thinks council should spend on gang programs, even though the draft budget is a week away. QMI Agency (Ottawa Sun, 4, 1)

*** Ne pas faire bande(s) à part**
Un article éditorial déclare, « Répression, arrestations, concertation, interventions et prévention: la crainte d'une balle perdue lors d'une fusillade entre bandes de rue rivales à Ottawa est enfin parvenue à convaincre les divers intervenants de faire rimer leurs intentions. Les souliers en grappe sur les fils électriques pour marquer les territoires d'un gang ou d'un autre, dans différents quartiers de la capitale, ne sont pas apparus hier. L'Unité des bandes de rue du Service de police d'Ottawa (SPO) est en place depuis 2001. Son Équipe d'intervention directe existe depuis 2007. Le phénomène, loin d'être nouveau, est documenté, suivi de près. Les plus récents chiffres rendus publics par la police font état d'une quinzaine de gangs répertoriés sur le territoire de la Ville. Ils réunissent entre 400 et 500 membres ou associés. Si les Crips et les Bloods s'affrontaient à une certaine époque, les groupes d'aujourd'hui sont plus éclatés, indépendants, nombreux et mouvants, y compris jusque du côté de Gatineau. Ils ont aussi plus facilement accès aux armes de poing de contrebande (qui représentent plus de 50% de la cinquantaine d'armes à feu liées à un crime saisies par le SPO en 2014), et sont plus décidés à en faire usage pour régler leurs comptes. L'explosion du nombre de fusillades liées aux bandes de rue d'Ottawa, passé de 30 en 2013 à 49 l'an dernier, a donc de quoi inquiéter. D'autant que cette augmentation notable pourrait notamment refléter les aspirations de quelques «alphas» d'ici d'établir leur réputation à l'approche de la remise en liberté de membres des **Hells Angels** incarcérés à la suite de l'opération SharQc. » Le Droit, 16

*** Young honour lost women**
New artwork on permanent display at Sir John Franklin High School encourages students, staff and visitors to reflect on the unfinished lives of missing and murdered indigenous women and children in Canada. A team of nine young women in grades 10 through 12 sewed two pairs of beaded moccasin uppers to memorialize the women's lives and to represent the children who never returned home from Canadian residential schools. "It hits me hard because I'm aboriginal and I'm a woman so I wanted to make it known to more people," said Grade 12 student Kyla LeSage. "It meant a lot that I could have a part in something like that." Yellowknifer

*** Waking up to cyber abuse**

Other than online, the dark underbelly of the internet is perhaps nowhere better exposed than in the eye-opening pages of Extreme Mean: Trolls, Bullies and Predators Online. Paula Todd's far-reaching investigation into cyber abuse takes us inside the stories of victims and the minds of cyber bullies. An investigative journalist for over 20 years, Todd tells it like it is. This so-called interpersonal terrorism is more disturbing than we imagined. Online luring, extortion, cyber mobbing, tormenting, grief tourism and revenge porn are everyday occurrences. Anonymity and a lack of consequences create a fertile playing field for bullies looking to get a high from the control they exert. The resulting mental anguish has in some cases led to suicide. When did it become okay to tell someone, "Go kill yourself?" "The motivations behind cyber abuse include such things as immaturity and copycatting, especially for young people, mental illness, drug and alcohol use, frustration, anger and something called strain," says Todd. The 'strain' theory holds that those under pressure, struggling at work or school, in a failed relationship, experiencing economic difficulty, and other strains of living are more likely to act out. Some bullies are sadistic: they enjoy causing pain. Other tormentors insist they're just joking, trying to get a reaction. Young people are easy targets. Like Amanda Todd, disenfranchised youth are looking for affirmation online. Other targets can include people who are grieving, good Samaritans, children targeted by other parents, people with a vindictive "ex," and more. Sexual cyber abuse reflects a different dynamic. StarPhoenix, N18

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

*** Canada has moral obligation to the Badawis**

An opinion piece by Liberal MP Marc Garneau states, "While Stephen Harper's government is lauding its zero tolerance for barbaric cultural practices bill, Saudi Arabian free speech advocate Raif Badawi was given on Jan. 9 the first 50 of the 1,000 lashes that he has been sentenced to receive over 20 weeks. Badawi, whose family has found refuge in Sherbrooke, has been in a Saudi jail since June 2012. He was fined $300,000 and sentenced to 10 years in prison by the Criminal Court in Jeddah on charges of "blasphemy" and of "adopting liberal thoughts." The Liberal Party of Canada strongly condemns this inhumane sentence and urges the Saudi Arabian government to reconsider its stance on Badawi, whose only crime was to peacefully exercise his freedom of speech and his support for freedom of religion. As the Liberal foreign affairs critic, I wrote to Saudi Arabia's ambassador in Ottawa in early January to request a meeting with him so I could express my party's concerns regarding Badawi's sentence. I am disappointed that the ambassador has not yet followed up on my request. Canada has political, economic and social relations with many countries, including Saudi Arabia. When disagreements occasionally arise between our country and others on certain issues, our government has an obligation to speak up. Canada has always promoted human rights and voiced its concerns about humanrights violations through respectful and open dialogue. Montreal Gazette, A17, Le Devoir

INTERNATIONAL / INTERNATIONAL

*** Anti-terror chief urges rehabilitation**

The European Union's anti-terror chief called Tuesday for countries to rehabilitate rather than punish returning jihadists with no blood on their hands, saying that some prisons have become "incubators of radicalization." EU counter-terrorism co-ordinator Gilles de Kerchove said in an interview that "if we can avoid prison, let's avoid prison." At a time when EU nations are still shocked by the attacks in France earlier this month, many are pushing for swift, repressive measures for anyone who has gone offto join the jihad in Syria or Iraq. And even if true criminals among the returnees need to be punished with jail time, "I don't advise to bring them all to court because it would be a mistake," de Kerchove said. Since the

Jan. 7 to 9 Paris attacks that killed 20 people, including the three gunmen, dozens of people have been charged in France with defending terrorism. Inciting terrorism can bring a five-year prison term - or up to seven years for inciting terrorism online. "We know how much jails are major incubators of radicalization. Much better, provided they accept to do that, they undertake major rehabilitation," de Kerchove said. France recently expanded prison terms for terrorism-related offences, but the country was still caught off-guard when a member of a jihadist network worked in tandem with his brother and a former jailhouse acquaintance during three days of attacks in the Paris region. Calgary Herald, B2 (Ottawa Citizen, Montreal Gazette, Edmonton Journal, StarPhoenix, Vancouver Sun, Windsor Star)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
January 29, 2015 / le 29 janvier 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Secrecy surrounds attack that fuelled anti-terror bill
An opinion piece states, "Was Michael Zehaf-Bibeau a terrorist? Canadians still don't really know. In the three months since the attack on the National War Memorial and Parliament Hill, government leaders have repeatedly declared Zehaf-Bibeau to be a violent jihadist. Prime Minister Stephen Harper mentioned it again during a campaign-style speech in Orléans on Sunday. "Jihadist terrorism is not a future possibility, it is a present reality," he said, referring to October's attacks in Ottawa and Saint-Jean-sur-Richelieu, Que. "Violent jihadism is not simply a danger somewhere else. It seeks to harm us here, through horrific acts like .... shooting a soldier from behind as he stands guard at a war memorial." Yet politicians and police have tendered no clear evidence to underpin their claims. On Friday, the question becomes more important. The Conservatives are set to table anti-terrorism legislation directly inspired by the events of Oct. 22. Harper has said the new laws will increase the state's powers to monitor, arrest and detain suspected terrorists. Knowing whether Zehaf-Bibeau, 32, was a terrorist driven by Islamist rage would help in understanding whether the proposed laws are necessary or wise - or, as the opposition NDP charges, whether the legislation is more about political opportunism in an election year. Q What have authorities said about Zehaf-Bibeau and terrorism? On the afternoon of Oct. 22, in the first public briefing on the attack, RCMP Assistant Commissioner Gilles Michaud, commanding officer of the RCMP National Division, said the investigation into the day's events was "dynamic and unfolding" and that it was "way too early to be able to determine motive." Hours later, in a televised speech to the nation, Prime Minister Stephen Harper linked the assault to international terrorism. [...] In the three months since, the prime minister, **Public Safety Minister Steven Blaney** and other Conservative politicians have repeatedly cast Zehaf-Bibeau as a terrorist." Ottawa Citizen, A1 (Leader-Post, Edmonton Journal)

Le projet conservateur divise
Les chefs de l'opposition à Ottawa ne sont pas sur la même longueur d'onde en ce qui a trait au projet d'instaurer la peine de prison à vie sans possibilité de libération conditionnelle : tandis que Justin Trudeau se montre intéressé, Thomas Mulcair y voit une vaine aventure politique.En point de presse au parlement, hier, le chef du Parti libéral du Canada a déclaré que la population canadienne s'attendait à ce que « quelqu'un qui est condamné pour un crime sérieux ait des conséquences sérieuses ». M. Trudeau a précisé que des criminels comme Paul Bernardo, qui a écopé en 1995 d'une peine d'emprisonnement à perpétuité pour une série de crimes sordides, ne devraient être libérés « sous aucune condition ».
De son côté, le chef du Nouveau Parti démocratique (NPD), Thomas Mulcair, fait remarquer qu'il existe déjà, dans le Code criminel, des dispositions concernant les délinquants dangereux, lesquelles permettent à un juge de conclure si un détenu devrait être libéré ou pas. Il accuse ainsi les conservateurs d'inventer un problème qui n'existe pas dans la réalité. « Trop souvent, depuis qu'ils sont là, les conservateurs ont eu tendance, pour des raisons purement politiques, à inventer un problème », a laissé tomber M. Mulcair dans le foyer des Communes. « Ils sont dans leur dixième année au pouvoir. Si c'était si grave que ça, ils n'ont qu'eux-mêmes à blâmer », a-t-il ajouté. Le premier ministre Stephen Harper avait promis dans son discours du Trône, en octobre 2013, qu'Ottawa modifierait la loi « afin qu'une sentence à vie soit bel et bien un emprisonnement à vie ». Le projet est revenu à l'ordre du jour. Le **ministre de la Sécurité publique**, **Steven Blaney**, a d'ailleurs signalé mardi qu'un projet de loi en ce sens serait déposé d'ici le mois de juin. Il a fait valoir que l'objectif des conservateurs était de protéger la société « ***des individus qui commettent des crimes graves et violents de manière répétitive*** ». La Voix de l'Est, 20 (L'Acadie Nouvelle)

Tories to tighten rules for statutory release
The Conservative government is set to announce that it will make violent, repeat criminals wait longer to get the near-automatic ticket out of jail known as "statutory release." Few prisoners in Canada serve their full sentence. Most, if they do not receive parole, are set free with conditions at the twothirds mark under statutory release. But the government intends to keep offenders with a violent history behind bars until they have just six months left in their sentence. The government will bring those changes to Parliament next month, a source said. They will be introduced around the time the Conservatives table a new law, revealed in The Globe and Mail this week, that would end the possibility of parole for some convicted killers. The two proposed changes would reinvigorate the government's tough-on-crime agenda as an election approaches next fall. Both plans focus on a public perception that sentences judges impose do not do what they say they do: life does not mean life, and a nine-year term means three years (with parole) or six years (with statutory release). [...] Jason Tamming, a spokesman for **Public Safety Minister Steven Blaney**, declined to answer specific questions about the new rules, but said in an e-mail: "***Our Conservative Government is keeping dangerous criminals behind bars where they belong. We are always interested in new ideas to keep our communities safe***." Globe and Mail, A1

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Manque de surveillance d'Ottawa, selon le BST**
Malgré les mesures mises en place par le gouvernement fédéral à la suite de la tragédie de Lac-Mégantic, d'importantes lacunes demeurent pour s'assurer qu'Ottawa ait véritablement à l'oeil les compagnies ferroviaires, signale le Bureau de la sécurité des transports (BST). Le Bureau, chargé d'enquêter sur l'accident survenu le 6 juillet 2013, s'est dit préoccupé hier que Transports Canada n'ait pas encore mis en place un programme de "surveillance efficace" garantissant que toutes les sociétés ferroviaires feront l'objet de vérification d'envergure et de fréquence suffisantes pour que les problèmes de sécurité soient corrigés à temps. Le BST a fait valoir que jusqu'à ce que les systèmes de gestion de la sécurité (SGS) fassent partie de la culture des sociétés ferroviaires du Canada et que Transports Canada s'assure qu'ils ont été mis en oeuvre de manière efficace, "les avantages en matière de sécurité escomptés des SGS ne seront pas entièrement réalisés". Le BST recommande donc au ministère d'effectuer des vérifications des SGS des sociétés ferroviaires assez poussées et suffisamment fréquentes pour confirmer que les processus nécessaires sont efficaces et que des mesures correctives

sont mises en oeuvre pour améliorer la sécurité. Journal de Montréal, 24 (Journal de Québec); QMI Agency (Edmonton Sun; Toronto Sun; Kingston Whig-Standard; London Free Press; Calgary Sun)

*** Les citoyens de Lac-Mégantic plus dépressifs**
Un an et demi après la tragédie ferroviaire de Lac-Mégantic, la population est encore très affectée au niveau psychologique, révèle une nouvelle étude dévoilée hier. Selon cette étude, pas moins de 50 % des gens de la MRC du Granit qui ont été exposés à la tragédie ont souffert de symptômes dépressifs depuis 12 mois, contre 23 % pour les gens qui n'ont pas été touchés par le drame qui a fait 47 victimes en juillet 2013. Les gens qui ont été exposés de près ont aussi une consommation excessive d'alcool quatre fois plus grande que ceux qui ne l'ont pas été. L'enquête démontre aussi plus de symptômes anxieux et une consommation plus grande de médicaments tels les sédatifs et les tranquillisants chez la population de la MRC du Granit qu'ailleurs en Estrie. Journal de Montréal, 24 (Journal de Québec); Presse canadienne (Le Droit); La Tribune (La Voix de L'Est; Le Soleil); La Presse; Le Devoir

*** Indemnisation des victimes - une séance d'informations**
La population de Lac-Mégantic sera informée des développements dans le dossier de la Montreal, Maine et Atlantic (MMA) et du plan d'indemnisation des victimes à la suite de la tragédie ferroviaire du 6 juillet 2013. Le contrôleur Richter organisera des séances d'information qui se dérouleront entre le 1er février et le 31 mars 2015. Le plan d'arrangement avec les créanciers qui doit être déposé à la Cour supérieure au cours des prochaines semaines prévoit un fonds d'indemnisation qui s'élève présentement à 207,8 millions $. Les victimes, qui font partie des créanciers de la MMA, seront appelées à se prononcer sur l'acceptation ou le rejet lors de l'assemblée des créanciers de la MMA qui devrait se dérouler en mars ou avril 2015. La Tribune, 5

*** CLEAN BILL OF HEALTH - City water tests negative for E. coli; officials hope boil advisory will be lifted today**
Winnipeg remained under a boil-water advisory Wednesday, but city officials were hopeful it could be lifted by Thursday afternoon. The advisory was issued late Tuesday after E. coli and coliform bacteria were found in samples during routine testing of the city's water. By Wednesday, extensive retesting was done and Mayor Brian Bowman announced it had all come back negative. However, the advisory remains in effect until further tests are complete. "I am pleased to advise that the testing that we've conducted over the last 24 hours has come back negative, which means according to our experts ... they were false positives," said Bowman. "Ultimately we have to respect the fact this is a provincial decision, as soon as we receive the green light, believe me, we want to give you the news we were hoping to give you today." The decision to lift the advisory is in the hands of the province and under Health Canada guidelines, the tests must come back negative twice in 24 hours before the city gets the all-clear. Winnipeg Sun, 3; Canadian Press (CTV News)

*** Winnipeg power outage adds insult to injury on day 2 of boil water-advisory - Nearly 9,000 in Winnipeg's Garden City and River East neighbourhoods affect by outage, says hydro**
Not only is the entire city slick after freezing rain and still without drinkable tap water, but thousands were also left without power after an outage swept through Winnipeg's Garden City and River East neighbourhoods Wednesday night. On the second night of the citywide boil water-advisory, many households like Doug Palmer's were suddenly unable to follow the advisory. "It feels like you're going back maybe 40, 50 years where there's no running water," said Doug Palmer. He and his wife Barb lost power Wednesday night. Luckily, they had pre-boiled water before the outage. "I was lying in bed and then all of a sudden I saw a flash," said Barb Palmer. "Then after that the power went off. I went, 'great, no roads, no water, no power." The pair are among 9,000 hydro customers who were left in the dark for hours Wednesday night. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Standing with Israel, again
Once again Israel is under attack. Last summer it was from Hamas. This time it's Hezbollah. On Wednesday the Islamist terrorist group fired missiles at an Israeli military convoy that was near the Israel-

Lebanon border. The missiles killed two Israeli soldiers and a Spanish United Nations peacekeeper. Israel has so far responded with artillery fire and airstrikes. Hezbollah would like you to believe this is all tit-for-tat. Their PR campaign will tell you that this is a game of equals and they're just firing back. Their excuse for this is that the attack is in retaliation for a Jan. 18 airstrike Israel conducted in southern Syria that saw several Hezbollah members die. But it's important to put all of this into context. When we describe Hezbollah as an Islamist terrorist group, that's not spin. We're just plainly echoing how many governments describe the Lebanese militant and political group. Canada has officially labelled Hezbollah a terrorist group since 2002. Here's how the Public Safety Canada website describes it: "One of the most technically capable terrorist groups in the world, Hezbollah is a radical Shia group ideologically inspired by the Iranian revolution. Its goals are the liberation of Jerusalem, the destruction of Israel, and, ultimately, the establishment of a revolutionary Shia Islamic state in Lebanon, modelled after Iran." In other words, whenever they act against Israel, it's not about being tit-for-tat. It's about utterly annihilating the Jewish state. They have the same modus operandi as Hamas." QMI Agency, 8 (Winnipeg Sun, Ottawa Sun, Toronto Sun, Edmonton Sun, Calgary Sun)

Federal bill expected to criminalize act of encouraging a terrorist attack

The Conservative government wants to make it a criminal offence to encourage someone to carry out a terrorist attack. The Canadian Press has learned that legislation to be tabled Friday is expected to create a new Criminal Code provision against advocating an act of terrorism. A government source says an internal federal review of fatal assaults on Canadian soldiers last October identified the absence of a measure to prosecute extremists who encourage others to wage terrorism. The provision would stop short of criminalizing the glorification of terrorism for instance simply posting an Internet video of a bomb going off. But if the video also called for a similar attack on Canadians, that would fall under the planned new measure. "This is not a glorification offence. This is about encouraging those kinds of terrorist acts," said the source, who spoke on condition of anonymity because they were not authorized to discuss the federal review. "The test that is applied is, is this advocating or promoting terrorism or a terrorist act?" On Oct. 22, a rifle-wielding Michael Zehaf Bibeau shot Cpl. Nathan Cirillo, an honour guard at the National War Memorial, before he died in a hail of gunfire inside Parliament's Centre Block. Charlottetown Guardian.ca (Hamilton Spectator); * The Province

Spies zero in on file sharing services as part of terrorist hunt

A new report says Canada's electronic spy agency sifts through millions of videos and documents downloaded every day through file-sharing services as part of its bid to find terrorists. CBC News says details of the Communications Security Establishment project, called Levitation, are revealed in a 2012 PowerPoint presentation obtained by former U.S. intelligence contractor Edward Snowden. The document says that under Levitation, CSE analysts can access information on about 10 to 15 million uploads and downloads of files from free websites each day. CSE says it takes strict measures to protect the privacy of Canadians. Whitehorse Daily Star, 10

New anti-terror bill could put chill on freedom of speech

Prime Minister Stephen Harper said last weekend that new anti-terror legislation to be introduced on Friday will, among other things, "criminalize the promotion of terrorism." Such a move, however, could have a chilling effect on freedom of expression in Canada and would not necessarily contribute to effectively fighting domestic extremism, according to legal experts. The new bill aimed at combating domestic threats was promised by the federal government in the weeks following the October attacks in Quebec and Ottawa that left two members of the Canadian Forces dead. Justice Minister Peter MacKay suggested that the measures would, among a host of other consequences, allow authorities to target materials that may be contributing to the radicalization of Canadians, particularly online. The new bill, however, is largely a knee-jerk response to October's attacks and Canada already has the necessary laws on the books to pursue and prosecute people promoting hatred or inciting violence, says Kent Roach, a professor at the University of Toronto who specializes in constitutional and terrorism law. "The government has the burden before they introduce new laws to demonstrate why it's not possible to prosecute these kinds of offences under existing Canadian law," he says. "There's a real danger when we make laws in reaction to events with the assumption that those laws will help prevent tragedies from happening again." CBC.ca; * Globe and Mail

*** Loi pour contrer le terrorisme: les vidéos menaçantes contre le Canada deviendront criminelles**
Le gouvernement Harper déposera vendredi un projet de loi qui criminalisera la diffusion de vidéos menaçantes incitant à perpétrer des attaques contre le Canada. Une vidéo comme celle où l'on voit le djihadiste canadien John Maguire en appeler aux armes contre le Canada, sera maintenant spécifiquement visée par le droit criminel. Une source conservatrice a indiqué qu'en vertu des mesures actuelles, il est impossible d'accuser un individu si la nature des attaques n'est pas précisée. «La loi actuelle prévoit une infraction de terrorisme dans des cas précis, par exemple lorsqu'on suggère à quelqu'un de tuer une autre personne dans un but politique, religieux ou idéologique.» Déjà, au lendemain des attentats à Ottawa, le ministre de la Justice faisait part de son intention de criminaliser les individus qui faisaient l'apologie du terrorisme. Journal de Montréal.com (Journal de Québec, L'Acadie Nouvelle, Le Soleil)

*** Police to be briefed on anti-terror legislation**
Canada's privacy watchdog is expressing early concerns about information sharing provisions expected in the Conservatives' new anti-terror laws, as Prime Minister Stephen Harper meets with Toronto police chiefs to win support for the new measures. Daniel Therrien said he's been briefed on the government's new anti-terror bill, to be tabled in Parliament on Friday, and will be closely watching the wording of provisions aimed at increasing information sharing among government agencies. "Information sharing regarding whom? Regarding people who are suspected of terrorist activities, or the sharing of information about other Canadians who are not suspected of anything in order to identify a national security threat?" Therrien asked. "Travellers crossing the border, ordinary Canadians crossing the border. Will there be greater information sharing about them from the border agency to the secret service?" The anti-terror measures are expected to improve the ability of security agencies to share information and allow security officials to take "proactive measures" much earlier in a terror investigation - if they perceive a threat. As well, amendments are coming to the Criminal Code to deter the promotion to terrorism and make it easier for law enforcement officials to get peace bonds. It is expected there will also be changes to "enhance" no-fly rules. The government has expressed concern about Canadians travelling abroad to fight with extremists. The measures will likely provoke backlash from civil libertarians and privacy advocates. Harper is scheduled to meet with police leaders from across the Greater Toronto Area on Thursday to brief them on the new anti-terror laws, and to seek their support for the measures. Toronto Star, A6

*** Conservatives defend spy agency's actions**
The Conservatives defended Ottawa's electronic spy agency Wednesday in the wake of revelations of a massive surveillance program targeting file-sharing websites. Working with the journalist in possession of a cache of documents from whistleblower Edward Snowden, the CBC reported Wednesday that the Communications Security Establishment was running a massive surveillance program tracing traffic on file-hosting websites. The program, dubbed Levitation, tracked between 10 million and 15 million downloads and uploads to file-sharing websites. According to documents, the search was meant to flag access to suspicious files, and turned up around 350 "interesting download events" each month. The revelations brought renewed questions from opposition critics about the legality of CSE's operations, and whether or not the secretive spy agency is picking up Canadian citizens' private information. "No one is questioning the need to go after those who download terrorism-related material," NDP defence critic Jack Harris said in the House of Commons. "However, what we are concerned about is the potential that the Communications Security Establishment may again be going beyond its mandate and monitoring Canadians." Associate defence minister Julian Fantino defended the agency, but did not address the specifics of the program. Toronto Star, A6 (Waterloo Region Record)

*** Canadian spy program raises Internet anonymity concerns**
Revelations about a Canadian spy program that can sift through 15 million downloaded files a day are raising concerns that Ottawa's fight against terrorism is eroding Internet anonymity. But Canadian spies claim to have used this technique to unearth a specific intelligence lead - the "hostage strategy" of an al-Qaeda offshoot, before passing it along to U.S. intelligence. A top-secret Communications Security Establishment document about its "Levitation" program was leaked by U.S. contractor Edward Snowden and published by the CBC and online publication The Intercept on Tuesday. Some of the spying described in the document closely matches what a federal official has suggested is one of Canada's most valued spying stratagems. "Let's imagine there is a hostage situation unfolding," the CSE's signals-

intelligence director said in a 2013 interview with The Globe. Drawing a diagram of three terrorist hostage takers talking on their phones, he said that "the solution to this, for us, is metadata." Metadata is information about an electronic communication excluding the spoken or typed words. Leaders of electroniceavesdropping agencies, such as CSE, have convinced the executive branches of government that they need an unfettered ability to collect, log and search this material - in bulk. Past leaks have shown that CSE analysts have a continually collected trove of metadata at their fingertips, through a database known as "Olympia," which allows Ottawa to scour all manner of covertly collected telecommunications traffic. Globe and Mail, A12

*** Sécurité nationale - Les espions en ligne du gouvernement inquiètent les Canadiens**
Alors qu'Ottawa se prépare à modifier certaines lois au nom de la sécurité nationale et de la lutte contre les extrémismes, une majorité de Canadiens envoie un message clair au gouvernement : la quête de la loi et de l'ordre ne doit pas se faire au mépris de la vie privée des citoyens, indique un sondage national mené à la fin de l'année dernière pour le compte du Commissariat à la protection de la vie privée du Canada. Sondage qui, plus d'un an après les révélations de l'ex-espion de la NSA Edward Snowden, met en lumière des préoccupations croissantes au pays face aux intrusions de toutes sortes dans l'intimité des gens. Le document a été dévoilé mercredi, à l'occasion de la Journée de la protection des données. En substance, 57 % des répondants y font part de leur inconfort face à la collecte de renseignements personnels par des ministères et organismes gouvernementaux auprès de compagnies de télécommunication, et ce, sans mandat judiciaire. Pis, 78 % des 1520 personnes passées à la question, entre le 21 octobre et 10 novembre derniers, d'un océan à l'autre, se disent également très inquiets par l'utilisation par le gouvernement, à des fins de surveillance, de données personnelles en ligne les concernant. Ce niveau de préoccupation est en croissance au pays depuis 2012, soulignent les auteurs du sondage. Le Devoir, A5; Le Devoir

*** Hot property**
A Muslim umbrella organization that allegedly funnelled money to a Hamaslinked charity is buying up property from Quebec to Alberta. QMI Agency conducted land-register searches that show the Muslim Association of Canada (MAC), based in the Toronto suburb of Mississauga, has bought at least 11 buildings in Ontario, Quebec and Alberta since 2006. They're being converted into mosques, community centres and schools as the group's financial dealings catch the attention of the RCMP. The group was named in a search warrant related to Project Sapphire, a probe into terrorist financing. Warrants indicates MAC sent nearly $300,000 in the 2000s to IRFAN-Canada, a group that raised millions for Hamas. The Canadian government considers both IRFAN-Canada and Hamas to be terrorist organizations. The Muslim Association of Canada remained a registered charity as of this week, having reported $16.1 million in revenues, and a nearly $5.8 million payroll, in 2013. The group says its mission is to "establish an Islamic presence in Canada that is balanced, constructive, and integrated, though distinct." Establishing that presence has included buying up more than $30 million of land and buildings across the country. Two mosques in north-end Montreal were donated for free. The MAC Islamic Centre of Cold Lake, Alta., was purchased in November 2013 and assessed the following year at $220,900. QMI Agency, 9 (Calgary Sun, Ottawa Sun, Winnipeg Sun, London Free Press, Kingston Whig-Standard, Edmonton Sun, Toronto Sun)

*** Un adolescent pourrait écoper d'une peine pour adulte**
S'il est reconnu coupable, l'adolescent montréalais de 15 ans qui est devenu en décembre le premier Canadien accusé d'avoir tenté de quitter le pays pour participer à une activité terroriste en vertu de la nouvelle Loi sur la lutte contre le terrorisme pourrait écoper d'une peine pour adulte. Lors du passage du jeune homme au Tribunal de la jeunesse, ce matin, la procureure de la Couronne fédérale a annoncé au juge qu'elle «considérait faire une demande» à la cour pour que l'accusé, que la loi nous interdit d'identifier parce qu'il est mineur, soit assujetti à une peine pour adulte. Rappelons que le garçon est détenu dans un centre jeunesse depuis qu'il a été arrêté au mois d'octobre après avoir volé 2000$ dans un dépanneur de L'Ouest-de-l'Ile armé d'un couteau et le visage couvert d'un foulard. Inquiet de son comportement de plus en plus radical, c'est son père qui l'avait dénoncé. La police lui a mis la main au collet alors qu'il était à son école, un prestigieux collège privé de Montréal. La Presse, A8

*** Don't curtail freedoms the jihadists hate**

An opinion piece states, "Any society that would give up a little liberty to gain a little security will deserve neither and lose both"--Benjamin Franklin. We live in frightening times. Terrorists gun down cartoonists in Paris for the imaginary crime of blasphemy. A solider is murdered in Ottawa by a domestic jihadist while merely standing on guard at a war memorial. ISIS. Boko Haram. Al-Qaida. The list goes on. Islamic terrorism is real. We have to deal with it both at home and abroad. But in doing so we cannot let fear override our reason and sacrifice our freedoms in the name of security. Prime Minister Stephen Harper has now revealed some details of a new antiterrorism bill he intends to introduce in Parliament. He talked about enacting a law that would make illegal speech that promotes terrorism. We sort of knew this was coming. After the Ottawa shooting, Justice Minister Peter MacKay mused about giving police the power to remove Internet posts that authorities deem could be "poisoning young minds". Both Harper and MacKay would benefit by reading a little Ben Franklin. The rationale is that given the rare, but real phenomenon of "home-grown" terrorism, if you limit speech that promotes terrorism, it's harder for terrorists to recruit." QMI Agency, 17; ipolitics.ca (Hamilton Spectator)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Human trafficking awareness should live on

Too often, what happens in January stays in January. Just think of our New Year's resolutions. On Jan. 1, we implement them with such excitement and alacrity, but as the month whittles away, so do our resolutions. This cannot and should not be the fate of human trafficking awareness. Human trafficking is indeed a global problem with international victims, but we Windsorites need to understand that human trafficking is also a Windsor problem with victims right here in our own backyard. Legal Assistance of Windsor is the lead organization in assisting survivors of human trafficking in Windsor and Essex County. Shelley Gilbert, social work services co-ordinator at LAW and chair of Windsor-Essex Fights the International Growth of Human Trafficking, known as WEFiGHT, says Windsor is indicative of other cities across Canada.There is sex trafficking, forced marriage and forced labour. Often, victims of human trafficking are threatened with deportation and experience physical and sexual violence. The Windsor Star

5 charged after drugs, gun turn up in raid

Ottawa police have charged five people - including two Bloodsrelated shooting victims in December - after a raid on a Draper Avenue apartment Friday turned up a loaded handgun and crack cocaine. Officers executed a search warrant at a highrise at 2600 Draper Ave., near Pinecrest and Baseline roads, around 11:30 p.m. Friday. (...) Grace M'Pemo, 18, charged by police with drug-and firearms-related offences as a result of the raid, was driving a white sedan near Bloomsbury Crescent and Regency Terrace in the final days of 2014 when he was shot at repeatedly in a driveby shooting. M'Pemo was hit once in the arm, abandoned his vehicle, which was crashed into a Dumpster, and took a taxi to the hospital. (...) In the raid, police seized a Turkish-made Girsan Yavuz 9-mm handgun - one of four crime guns seized by police so far in 2015 - 10 rounds of ammunition, 45.6 grams of crack cocaine, four grams of cocaine and 10.5 grams of marijuana. Nearly $3,200 in cash was also seized. (...) M'Pemo, Affat, Richard Wallace, 31, James Gerrior, 46, and his sister Margaret Gerrior, 45, were all charged with drug possession and possession for the purposes of trafficking, along with various weapons charges Wallace was charged with possession of marijuana and violating undertakings. Police said Wallace is in Canada illegally and was placed on an immigration hold for the Canadian Border Services Agency. The Ottawa Citizen

YVR heroin seizure sparks B.C. probe that leads police to drugs and guns

Mounties say the seizure of heroin at Vancouver's airport has sparked an investigation that led to weapons and drug charges against a 31-year-old man from the Okanagan. Vernon RCMP spokesman Gord Molendyk says the Canadian Border Services Agency intercepted a large quantity of heroin from Thailand at the airport Jan. 8. He says border agents alerted police who obtained a warrant and searched a Vernon home on Jan. 13. Molendyk says police seized four loaded handguns, more than $10,000 in cash and prescription and non-prescription drugs. Ronald Learning is facing 17 charges related to weapons offences, possession of stolen property and breaches of court orders. Molendyk says the police

recently warned local drug users about overdoses and the city is safer now that illicit drugs have been taken off the streets. (CKFR, CHNL) The Vancouver Sun

Deportation stay denied for Roma family
The last hope of a Hungarian Roma family seeking refuge in Canada was dashed when a Federal Court justice denied a stay of deportation on Wednesday morning. They were deported in the evening. Anasztazia Szilagyi, husband Deszo Nemeth and their two children fled Hungary in 2011 to seek asylum in Canada. As members of Hungary's Roma minority, they say they face persecution in the country, which has seen a rise in anti-Roma rhetoric in the recent years. The Gazette

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Privacy watchdog seeks reports of major breaches**
B.C.'s independent privacy watchdog called on the provincial government Wednesday to start reporting all major privacy breaches to her office. Elizabeth Denham issued a 60-page report showing that the government investigated more than 3,700 suspected privacy breaches and confirmed 2,700 between April 2010 and December 2013. Yet, she said, fewer than 45 of those cases were reported to her office. "I'm concerned that we only heard about one per cent of the breaches that the government investigated over a four-year period," she said. Denham said the government is not even telling her about confirmed breaches caused by malicious viruses, hacking or phishing. There were seven such breaches from 2010 to 2013, her report says. "We're not hearing about some of the cyberattacks," she said. "We're not hearing about the numbers of people that were affected. Times-Colonist, A5

LAW ENFORCEMENT / APPLICATION DE LA LOI

Mom wants serial killer Robert Pickton charged with killing daughter
The mother of a woman whose DNA and bones were found on Robert Pickton's property says her daughter's remains should result in another murder charge for the convicted serial killer. In January 1997, Michele Pineault's daughter Stephanie Lane disappeared. It would be many years later when her family learned some of her skeletal remains were found on Pickton's Port Coquitlam, B.C., pig farm. Pickton was first charged with killing 26 women, but later convicted of six while 20 charges were stayed and an additional six cases, including Lane's, never resulted in charges. In 2003, Pineault was told her daughter's DNA, from bodily fluid, was found on the Pickton farm in a deep freezer, and if more of her daughter's remains were found, Pickton would face a murder charge. But it wasn't until last August when the BC Coroners Service informed Pineault they had Lane's partial skeletal remains, which had been kept in storage. The RCMP had them until 2010, when they were turned over to the coroner's office. Pineault got the remains last September. "I was told that they found two pieces of my daughter's vertebrae on the farm," she said. "It remained in a storage locker and the only explanation was -- none. "The only thing they could say was, 'It was an oversight.'" Pineault is calling on the B.C. Coroners Service to re-examine the remains to confirm the identity of the bones, and wants police and Crown prosecutors to reopen the case and charge Pickton with her daughter's death. QMI Agency (Edmonton Sun, Calgary Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun); Canadian Press (The Telegram, B3)

Barton case goes to appeal
An appeal court was described as Gerald Barton's last chance at justice Wednesday by a lawyer who argued RCMP negligence contributed to his client's wrongful conviction on a statutory rape charge 45 years ago. "This is probably Gerry Barton's final stop on his quest for justice and I hope you will entertain arguments on his behalf," Dale Dunlop told the five-judge panel of the Nova Scotia Court of Appeal. Dunlop argued that a Nova Scotia Supreme Court judge erred last April when he cleared the RCMP of wrongdoing and ruled there was nothing wrong with the way police investigated the case against Barton, who is now 64. Justice James Chipman should have found Barton's confession in 1969 was false and caused by some form of police coercion when the then 19-year-old gave a statement in Digby, he said. Since the woman recanted her story in 2008 and blamed her brother for causing her pregnancy, Dunlop said the confession must be both false and improperly obtained. "Why did Gerry Barton say he had sex

with someone when he didn't? There was no sex," he said. "The onus is on the other side to explain how they got this through correct police methods." He urged the judges to award Barton significant damages in his lawsuit against the Mounties. Canadian Press (Chronicle Herald, A6, Whitehorse Star, Times & Transcript, Cape Breton Post)

Missing mental patients pose 'threat'

Police in North Bay, Ont., say they believe a man and a woman missing from a local mental health facility are believed to be in New Brunswick and pose a "significant threat to public safety." In a news release on Wednesday, the North Bay police say that Cara Duval - who also goes by the last name Donnelly - and Joseph Pepin did not return to the North Bay Regional Health Centre's Mental Health and the Law program on Thursday of last week. The police release states that the two patients were believed to be in Hanwell earlier this week, on Tuesday. The RCMP released photos of the duo from an in-store camera at a convenience store and gas station on the Hanwell Road. The photos of the woman, man and the Volkswagen Jetta car they are travelling in were taken at 2:30 p.m. on Tuesday. "Concern for their well-being and safety continues," the North Bay police say in the release. "Without ongoing monitoring and supervision, both pose a significant threat to public safety." Daily Gleaner, A1

Stolen goods seized from notorious residence

A man faces additional charges after police seized drugs, weapons and stolen tools and equipment from a notorious Penhold residence. Innisfail RCMP Staff Sgt. Chris Matechuk said a search warrant on Saturday netted the stolen goods, including a replica firearm and rifle reported stolen from Three Hills. The charges came after a two-week investigation. Since July, police received 70 complaints about suspicious people, vehicles and incidents at the residence. Police say the suspect is linked to 40 of those complaints. "The community is very frustrated," said Matechuk. "They are seeing all this activity. ... We have received a lot of positive comments from the community and relief that we were able to make an arrest." Police will continue to keep an eye on the property. Matechuk told reporters that the suspect has been arrested four times and charged five times since July. The most recent warrant was issued for his arrest on Jan. 5. His charges related to stolen property, failure to comply, driving without a valid licence and other offences. Matechuk said the criminal activity at the home was not limited to Penhold. The investigation was conducted by the newly-formed regional Property Crimes Tasks Force and the Safer Communities and Neighbourhoods Act, a division of ALERT. Red Deer Advocate, A1

Police were at house before man was shot

Two hours before a 38-year-old man was shot several times in a house in Langford Tuesday night, West Shore RCMP were there responding to a disturbance. One man was told to leave but no arrests were made. By 8:30 p.m., officers were back at the white bungalow at 2639 Sooke Rd. after the shooting. Debbie England, who grew up in the bungalow and whose nephew now owns the property, said her husband went to the house about 6 p.m. because he had keys to let police into the rental suite. "[Police] removed someone," she said. "And two hours later that person came back and shot [the tenant's] boyfriend or ex-boyfriend." After a 13-hour manhunt, a 22-year-old Victoria man was arrested Wednesday at a home in the 3200 block of Quadra Street. Acting on a tip, Saanich police entered the home about 10 a.m. and took the suspected gunman into custody without incident. Saanich police also arrested the 21-year-old resident of the Quadra Street home, who faces charges of accessory after the fact for allegedly helping the wanted man hide from police. Police were waiting to obtain a search warrant for the Saanich residence to look for a handgun. Both men were being held at West Shore RCMP detachment. Their names have not been released pending charge approval. West Shore RCMP has recommended charges of attempted murder against the 22-year-old. Times Colonist, A1

Officer arrested

An off-duty Vancouver police offi cer has been arrested following allegations of domestic assault and unlawful confinement. The Vancouver Police Department says the member with 10 years' experience was arrested Friday night by Mounties in Maple Ridge. They say a woman went to the Ridge Meadows detachment earlier that day and reported the allegations. Vancouver police say they were advised and the office of the Police Complaint Commission informed. The officer has been removed from front-line duties. His identity has not been released, and Vancouver police say the RCMP is in charge of the investigation. Postmedia News (Vancouver Sun, A2, The Province)

City council split on $5M handout for new police building
Hamilton police are banking on the city to pony up $5 million for a new investigative services building they say will alleviate a space crunch. But with the city facing a $3-billion infrastructure backlog, there's no consensus among councillors that the project should make the cut in this year's municipal budget. "It's hard to say this one goes ahead of everything else without knowing what the list looks like in its entirety," Coun. Chad Collins said after Wednesday's general issues committee meeting. But police officials say provincial and federal funds for the $15-million project, which includes a cutting-edge forensics lab, hinge on the city's commitment. "In the 2015 capital for this facility, I would like to see approval of the $5 million so that we can continue to advance our planning and our work," police Chief Glenn De Caire said after his budget presentation at City Hall. Dan Bowman, assets manager for the police, told councillors the service is short 53,000 square feet of space. This has put evidence at risk of cross-contamination in a cramped and outmoded forensics lab, and split investigators among four sites. Hamilton Spectator

Placentia stabbing prompts 'precautionary' school lockdowns
The victim of a reported stabbing in St. Bride's Wednesday morning is in the Health Sciences Centre with serious injuries, and the 46-year-old suspect in in police custody. According to a news release from the RCMP sent Wednesday night, police eventually caught up with the suspect and arrested him. They expect to lay several charges, including aggravated assault, assault with a weapon, driving while prohibited and breaches of court orders. The RCMP alerted the Royal Newfoundland Constabulary to lock down two schools in Mount Pearl after the stabbing. Fatima Academy implemented a secure-school protocol as well, a school board spokesman said. The lockdowns ended when the suspect was arrested. Both St. Peter's Junior High and O'Donel Junior High in Mount Pearl were locked down for about an hour and a half Wednesday morning. It caused some tense moments for students at St. Peter's Junior High, who had to get on the floor for close to half an hour during the lockdown before things were cleared. The Telegram

Surrey RCMP search for 'high-risk' missing woman
Surrey RCMP are asking the public to help track down a "high-risk" missing woman. Chelsea Hagen was reported missing on Jan. 24, and has not been heard from since. Her last known residence was in Surrey's Newton neighbourhood. "Family and police are concerned about her current well-being as she lives a high-risk lifestyle," read a police statement. Hagen is a 21-year-old white woman, about 5-foot-8 tall, about 135 pounds. Hagen has brown hair and hazel eyes, and has tattoos on her left wrist and right forearm. There is no information about what she was wearing at the time of her disappearance. Postmedia News (The Province)

RCMP cleared of wrongdoing in Tofield-area shooting
Mounties who opened fire on a wanted man during a Tofield-area confrontation that left two officers injured have been cleared by the province's cop watchdog. The Alberta Serious Incident Response Team (ASIRT) was directed by the Director of Law Enforcement to investigate the Jan. 6, 2014, RCMP officer-involved shooting near Township Road 524 and Range Road 192. Earlier that day, two rural homes were broken into and guns were stolen. The investigation led five Mounties to the rural home of a man associated with the suspect. Edmonton Sun ; Edmonton Journal

Retention pay, banked sick days first targets in curbing police cost
A long-standing perk that allows Toronto police employees to bank up to 18 sick days a year and potentially collect a payout of tens of thousands of dollars will be a key issue in looming contract negotiations. So, too, will lucrative "retention pay" bonuses that have been in place for more than a decade and reward officers for not quitting their jobs. On Thursday, the budget committee takes its first detailed look at the proposed 2015 police budget. Toronto Star, GT2

Halifax passes $77m police budget
Halifax councillors signed off Wednesday on a $77-million regional police budget. But while the 2015-16 budget is only a slight increase over last year, it doesn't include wage increases for some unionized workers - one of the biggest single cost pressures for the force. The current collective agreement with Halifax Regional Police Association, the union that represents sworn officers and some civilian staffers, is

set to expire March 31. "One of the things that you will not see (in the budget) is the additional pressures from wages," Police Chief Jean-Michel Blais said during a presentation to committee of the whole. "The amount proposed does not include any wage increases for the collective bargaining unit that is represented by the (association)," he said, adding that it would be "premature to even speculate how much that number will be." Wages for both the union's sworn officers and civilian staffers is set at $65.14 million for 2015-16, about 85 per cent of the total police budget. The Chronicle-Herald, A6

A dozen arrested, 116 charges in illegal tobacco case in metro
A five-month investigation into illegal cigarette sales in the Halifax area led to 116 charges against 12 people, Halifax RCMP and Service Nova Scotia said Wednesday. Police allege the cigarettes were first purchased, legally, by the owner and another person from Bridgeview Grocery on the Bedford Highway but were then illegally resold to 11 local convenience stores, which sold them to the public. The couple from Bridgeview Grocery face 47 charges, mostly for selling contraband cigarettes. If convicted, they could face several fines that go as high as $100,000, but no jail time. The other people face charges of purchasing, possessing or transporting contraband tobacco. "We had retailers that were not buying tobacco from a licensed wholesaler," said Bernie Meagher, director of audit and enforcement at Service Nova Scotia. "There's only licensed wholesalers that are responsible for collecting the taxes." The Chronicle-Herald, A4

Windsor, LaSalle police chiefs to meet
The next step in talks over regional policing will be a future meeting between Windsor and LaSalle's police chiefs, according to Windsor Mayor Drew Dilkens. Dilkens said Wednesday morning's "very hearty twohour meeting" with Amherstburg Mayor Aldo DiCarlo and LaSalle Mayor Ken Antaya focused mainly on LaSalle's concerns about blending their municipal police forces into a regional service. Now, it's about crunching the numbers. "Where we ended up at the end of the day was the mayor of LaSalle said 'have your chief meet with our chief, figure out what the level of service being provided is so that we can do an apples-to-apples comparison,"' Dilkens said. "And then provide us with a costing." Dilkens said it will take months to provide information to both Amherstburg and La-Salle on what police services could cost if a regional service was formed - either between Windsor and Amherstburg or Windsor, Amherstburg and La-Salle. Amherstburg is looking to reduce costs and is also seeking an OPP costing but the OPP have placed a moratorium on providing costings until the fall. The Windsor Star, A3

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Ottawa gruge 6,3 M$ dans l'assiette des détenus
Les criminels détenus dans les pénitenciers devront se serrer la ceinture. Ottawa ne leur servira plus que des menus congelés et le lait frais sera remplacé par du lait en poudre. Au total, Ottawa compte épargner plus de 6,3 M$ grâce à ces nouvelles mesures. Les repas seront dorénavant préparés dans un centre de production avant d'être congelés et transportés dans les pénitenciers où ils seront réchauffés et servis aux détenus. Ottawa prévoit ainsi épargner 3,2 M$ par année en ne préparant plus les repas directement dans les prisons. Certains établissements à sécurité minimum où les détenus préparent eux-mêmes leur repas ne sont pas touchés par ces mesures. Les services correctionnels ont aussi l'intention de revoir le menu des détenus en centralisant les achats et en choisissant des produits à faible coût. Par exemple, le lait frais sera remplacé par le lait en poudre, comme c'est déjà le cas dans plusieurs prisons aux États-Unis et dans l'Ouest canadien. "L'utilisation du lait en poudre est plus rentable que le lait liquide et répond également aux exigences du Guide alimentaire canadien", a indiqué la porte-parole des services correctionnels, Véronique Rioux. Journal de Montréal, 10 (Journal de Québec), 1

1,9 million$ pour une maison de transition vide
Une maison de transition construite à grands frais sur la Côte-Nord accueille un seul prisonnier. D'une capacité de 20 lits, le centre Kapatakan Gilles-Jourdain, situé sur la réserve innue de Mani-Utenam, n'a toutefois qu'un seul «client», a appris Le Journal. Le centre, bâti en 2012 pour 1,9million$, coûte malgré tout 680000$ en frais annuels. Le centre transitoire, qui accueille les «adultes innus et les autres

membres des Premières Nations» en processus de libération conditionnelle, offre des «services diversifiés et adaptés selon les valeurs et les traditions des peuples autochtones.» «Pour l'instant, notre mission est d'accueillir des personnes autochtones. Les besoins sont là. Mais on n'est pas assez connus», es-time le directeur général du centre, Robert St-Onge. Pour remplir ses lits, le directeur général doit trouver des prisonniers autochtones qui purgent des peines dans des établissements provinciaux. Lorsqu'ils reçoivent la bénédiction de la Commission des libérations conditionnelles, ils peuvent suivre un «programme de rétablissement avec la guérison autochtone pour inspirer un nouveau mode de vie et pour la consolidation de l'identité et des valeurs autochtones. » Le «stage» dure 12 semaines. Pour l'instant, l'option n'est pas très populaire puisque 12 personnes seulement sont passées par le Centre depuis son ouverture, en mars 2013. Journal de Québec, 5 (Journal de Montréal)

Quand la prison rend fou
Un article d'opinion déclare, « Au début du XIXe siècle, les quakers ont développé la détention en isolement. Seuls dans le silence, les prisonniers devaient cheminer vers Dieu et la réhabilitation. Mais la plupart n'y ont trouvé que l'enfer. Comme plusieurs États américains ont commencé à le faire, le Canada devrait restreindre cette pratique. Le gouvernement conservateur est resté insensible aux rapports critiques de l'enquêteur correctionnel, du vérificateur général et de l'ONU. Le seul espoir qui reste : que les deux poursuites intentées dans les dernières semaines forcent une réforme. Selon la bureaucratie carcérale, il existe deux motifs pour l'isolement : disciplinaire ou « administratif ». La première catégorie vise les détenus qui violent certains règlements (drogue, bataille, etc.). Ce volet ne compte que pour 2 % des cas d'isolement. La punition est limitée à un mois et un système indépendant révise les décisions. C'est dans le volet « administratif » que se trouve le problème. Les gardiens peuvent isoler les détenus s'ils font l'objet d'une enquête ou s'ils posent un danger pour eux-mêmes ou les autres (pédophile menacé, caïd qui complote un meurtre, etc.). La durée de la réclusion n'est pas limitée. Il faut toutefois prouver qu'il n'existe pas d'autre solution. L'isolement doit donc, en théorie, servir de dernier recours. Mais il est devenu un simple outil de gestion pour régler les troubles quotidiens causés par le surpeuplement carcéral et la désinstitutionnalisation en santé mentale. Plusieurs études ont démontré que quelques semaines d'isolement suffisent pour exacerber une maladie mentale ou en causer une nouvelle. Lorsqu'on est enfermé dans une cellule 23 heures sur 24, les murs se rapprochent, et la paranoïa s'installe. » La Presse

Home invaders leave lasting scars
Ante Maglic knew the death threat wasn't idle - he'd been beaten, stabbed and tortured with a cordless drill - but he didn't have what the home invaders wanted. When four men started torturing Maglic for drugs and money, before realizing they burst into the wrong Ellrose Avenue home, his first instinct was to fight back. "I threw one of them off me," Maglic recalled Wednesday. "That's when they put the gun to my head. I didn't do anything except take a beating." Maglic and his girlfriend, Sheri Meloche, received a total of $26,525 in compensation Wednesday for physical and mental suffering after enduring a night of terror at the hands of intruders. Basil Percy Scott, 37, Maurice Geramine Heptbourne, 24, and William Charles Langdon, 21, were each sentenced to nine years in prison for the February 2013 attack. Jalen Lloyd Elliott-Strain, 22, was sentenced to five years after testifying against the others. Maglic and Meloche told of how the attack has affected their lives during separate hearings before Ontario's Criminal Injury Compensation Board. Maglic was awarded $12,000 for pain and suffering, $1,900 for loss of income and $1,200 for more counselling. Meloche received $9,000 for pain and suffering, $25 for half a day of lost pay and $2,400 for counselling. Windsor Star, A1

*** Life behind bars: the politics of despair**
An opinion piece states, "Stephen Harper wants to bring back the death penalty. Not the quick kind, by poison or electrocution. The slow kind - life imprisonment without parole. A *living* death. The proposed legislation - news of which was opportunistically leaked on the day slain RCMP officer Const. David Wynn was buried - would remove any possibility of parole for the killing of a police officer or jail guard, for a murder that occurred during a kidnapping, a sexual assault or "terrorist" act, and for especially brutal homicides. It's the apotheosis of the Conservatives approach to criminal law: simplistic, short-sighted, vengeful and purely political. Probably doomed, too. Some history: In 1967 the death penalty was temporarily suspended under Prime Minister Lester B. Pearson for all homicides apart from those involving the deaths of police officers and prison guards. During this trial period, all death sentences for

murder were automatically commuted. In 1976, Pierre Trudeau's government introduced Bill C-84, abolishing the death penalty. The noose was replaced with a life sentence accompanied by a period of parole ineligibility (and the "faint hope" of an even earlier release - a safety valve that later would be abolished by the Harper government). A life sentence is just that - a life sentence. A conviction for first degree murder carries an automatic 25 year sentence of incarceration. Only after a quarter century has passed can a first degree killer apply for full parole. Release from prison is only granted when a federally-appointed parole board determines that the public's safety will not be placed at risk. It's not automatic. It's not a revolving door. After release from prison the sentence continues; any breach of parole, any offence - no matter how small - results in an immediate return to prison. The supervision is intense. And the system *works*. The rate of recidivism for those released on parole is low (despite the fact that the government axed effective reintegration programs)." iPolitics

*** Still fighting shadows**

An editorial states, "There he goes again. Prime Minister Stephen Harper has never met a criminal law he didn't want to torque, and he's planning to tighten the screws again ... just in time to burnish his tough-on-crime credentials for the federal election. His latest targets are reportedly some of Canada's most notorious: Multiple murderers, cop-killers, jail guard killers and those who kill during a terrorist attack, sex assault or kidnapping. Under legislation the government plans to bring in they would face an automatic sentence of life without parole, meaning they'd die in prison. Currently the maximum is a life sentence without parole eligibility for 25 years, then possible release under supervision for life. The Tories are banking, rightly, that few Canadians will lose sleep over the fate of the very worst. Even so, this is the latest instance of Harper cynically pandering to his right-wing base by passing "tough" laws that have driven up the criminal justice system's cost by $5 billion and jammed the federal prisons with 15,000 inmates, a 25-per-cent increase - without making the country any safer. The need for harsh new laws is far from apparent. As Statistics Canada reported this week, crime is at its lowest point in 45 years. Homicide rates peaked in 1975 and have steadily if unevenly declined ever since; they're now at 1966 levels. That's nearly a half-century low. Attempted murder is down to the 1971 level. And this trend began long before Harper's first crime bill. As the Star has written before, the Conservatives are wringing their hands over a crime wave that isn't sweeping the country. They're tilting at shadows for political gain, posturing as defenders of law-abiding folks and victims. On Harper's watch they have sought repeatedly to tie judges' hands and to stiffen sanctions by bringing in more mandatory minimum sentences, reducing conditional sentencing (house arrest) options, curbing credit for pre-sentence custody, curbing parole eligibility and making pardons harder to get. Their latest fixation - throwing away the key - is yet another solution to a problem that doesn't exist." Toronto Star, A14

*** Certains criminels méritent une vie en prison, juge Trudeau**

Le chef libéral Justin Trudeau ne s'insurge pas contre la volonté du gouvernement conservateur de retirer aux personnes condamnées pour meurtre la possibilité d'un jour sortir de prison. A son avis, les crimes les plus odieux devraient être punis d'une peine proportionnelle. " Le Parti libéral et les Canadiens s'attendent à ce que quelqu'un qui est condamné pour un crime sérieux ait des conséquences sérieuses. Nous allons regarder le projet de loi quand il sera déposé, mais les gens s'attendent à ce que des gens comme Clifford Olson et Paul Bernardo ne soient libérés sous aucune condition ",a déclaré M. Trudeau. Le gouvernement avait indiqué, dans le dernier discours du Trône, son intention de faire en sorte que l'emprisonnement à perpétuité signifie rester en prison jusqu'à ce que mort s'ensuive. Le premier ministre est revenu à la charge avec cette promesse dimanche. Tout indique qu'un projet de loi sera déposé d'ici juin, juste à temps pour les élections. Les cas Olson et Bernardo cités par Justin Trudeau sont mal choisis, car tous deux ont été déclarés " délinquants dangereux ". Cette étiquette permet d'imposer une peine à durée indéterminée. Le tueur en série Clifford Olson est mort derrière les barreaux en 2011, après 30 ans d'incarcération. Ses deux demandes de libération conditionnelle lui avaient été refusées. Le violeur et assassin Bernardo est en prison depuis 20 ans. Le chef du Nouveau Parti démocratique, Thomas Mulcair, a évoqué cette disposition pour expliquer sa tiédeur devant l'initiative à venir. " Je vais attendre de voir le texte de leur loi, mais les dispositions existent déjà. Trop souvent, depuis qu'ils sont là, les conservateurs ont eu tendance, pour des raisons purement politiques, à ériger un homme de paille qu'ils vont faire tomber eux-mêmes. " (...) Une étude de 2012 du Service correctionnel du Canada, menée auprès de 1129 condamnés à perpétuité et remis en liberté entre 1995 et 2005, a démontré que seulement 3,5 % d'entre eux ont commis une nouvelle infraction. Le Devoir, A2

*** What about public safety?**
A letter to the editor states, "Re: Cruel And Unusual, editorial, Jan. 28. I read with interest your editorial on solitary confinement of prisoners and believe I have the solution: capital punishment. I do not say this in jest. I truly believe if people have trouble envisioning prisoners being in solitary confinement for whatever heinous crime they have committed, it would be much easier for all involved if the prisoners no longer existed. If someone has been tried and convicted of a serious crime such as murder, the public should not have to worry about them being paroled early for good behaviour or convincing some weak-kneed judge they have found religion and therefore are no longer a threat to anyone. How many people do you think would mourn Paul Bernardo if he were to be executed? People just want guarantees that dangerous criminals have no chance of being released and ever threatening anyone again." National Post, A9

*** Paroled too soon**
A letter to the editor states, "The article Tories Seek Tougher Penalties For Killers (Jan. 27) led me to reflect again on the recent passing of Francis Simard, an admitted kidnapper and murderer of Pierre Laporte in 1970. He was sentenced to life imprisonment but was paroled after only 11 years. Such an early parole can certainly be seen as a solid argument to legislate a stricter system. While a total end to parole for capital crimes may be excessive for Canada, the family of the victim - and indeed society at large - has a right to know that convicted killers will be held to serve a term of long duration." Globe and Mail, A14

*** Life with no parole**
A letter to the editor states, "The number of Mounties Canada has lost recently is appalling and our government of any stripe can do better in helping to strengthen our laws. I do not believe a prison term without parole is applicable in all situations except for the killing of law enforcement officers. They are entitled to have the best protection the government can bring. They take on dangerous careers to keep our communities safe. We owe them a certain duty of assurance." Edmonton Journal, A16

*** Powdered milk is good enough**
An opinion piece states, "Powdered milk will soon be served to prisoners in all federal institutions. The savings, however, estimated at $3.1 million by Correctional Service Canada, does not impress the official opposition in Ottawa. New Democratic Party MP Rejean Genest was quoted in the latest edition of La Terre de Chez Nous as saying he hates the taste of dried milk so much he doesn't even put it in his coffee. He finds it lacks "decency" to serve it to criminals. How can he be sorry or even care that a pedophile, a murderer or a crook doesn't like the taste of his milk? Contrary to Thomas Mulcair's party, what I find lacks decency is that as taxpayers we pay more, per meal, to feed prisoners than patients in hospitals or residents in senior housing. Genest adds that fresh milk is not a luxury but a basic product on anyone's table. What does the NDP say to a 15-year-old or his single mom earning minimum wage who has never been able to afford more than dried milk for her family? Criminals certainly don't deserve better than that mother and her kids." QMI Agency (Winnipeg Sun, 9, Toronto Sun, Ottawa Sun, Edmonton Sun, Calgary Sun)

*** Notorious Ottawa killer found dead in Alberta prison**
Ottawa's gas bar killer, Martin Pinkus, was found dead in his Drumheller jail cell on Wednesday. Drumheller Institution staff members discovered Pinkus unresponsive in his medium-security cell, immediately tried to perform CPR and then called 911. He was taken to the Drumheller Health Centre where he was later pronounced dead. Pinkus, 47, had been serving an indeterminate sentence since Dec. 20, 1999, for the shotgun slaying of Ottawa's Danny Jones outside Namers Convenience Store, a Gloucester gas bar. (...) Local police and a coroner have been notified, while Correctional Service Canada are reviewing the circumstances of the incident. Pinkus' death marks the second in three days at the Drumheller jail. Ottawa Sun, 9, QMI Agency (Edmonton Sun, Calgary Sun)

*** Double murderer Earl Davenport dies in prison**
Hamilton man who committed a 1986 double murder that a judge described as "barbaric" and "savage" has been found dead in an Alberta prison. Earl William Davenport, 56, was found unresponsive in his cell

at Drumheller Institution, 110 kilometres northeast of Calgary. Correctional Service Canada reported he was found Monday during a regular check at about noon in his cell in the medium-security unit. Staff members performed CPR and emergency services were called, but Davenport could not be resuscitated. Davenport was convicted on Nov. 27, 1987, of stabbing to death his sister-in-law Laura Ann Davenport, 31, and her friend Susan Joy Hornbeck, 30, who was seven months pregnant. He was sentenced to life in prison with no eligibility for parole for 25 years. The Crown said the Aug. 23, 1986 killings were based on Davenport's "intense hatred" for his sister-in-law. He was the brother of her estranged husband, David Davenport. The couple separated in 1985 and had two daughters. Correctional Service spokesperson Jeff Campbell told The Calgary Herald there is no indication of foul play in the death of Davenport. The police and coroner were called and Correctional Service will conduct a review. Hamilton Spectator, A6

*** Inmate charged after prison rampage**

A federal inmate is accused of causing thousands of dollars in damage while running amok with a metal pipe. Terrance Joseph Keleher, 28, was supposed to appear in Moncton provincial court Wednesday morning, but his case was set over until the afternoon. Because of the weather, no prisoners were transported to court in the morning, but they were expected to be brought to the Moncton Law Courts Wednesday afternoon. But when his case was called in the afternoon, there was confusion over whether or not he's still in custody. The judge adjourned the matter for a couple of weeks. Keleher is charged in relation to incidents that occurred at medium-security Dorchester Penitentiary on Aug. 23. He's accused of uttering threats to cause bodily harm to guard Timothy Wellman, interfering with property by causing a false alarm of fire and doing more than $5,000 worth of damage to the prison. The RCMP allege guards responded to an inmate's cell on the day in question and encountered an intoxicated inmate armed with a shank and a needle. The emergency response team was called in but before they arrived, the inmate got out of his cell. Police allege the inmate used a metal pipe to smash eight cell-door windows, four other windows, a toilet, a sink and a camera, and also tried to incite a riot. The damage was estimated at more than $5,900. The inmate finally surrendered and was handcuffed and taken to segregation. Times & Transcript, A4

*** Return of daughter's remains triggers call for Pickton trial**

The mother of a woman whose DNA was found on Robert Pickton's property says the serial killer should be charged with murder, arguing human remains returned to her represent new evidence. Michele Pineault said an official with the B.C. Coroners Service met with her last September and gave her fragments from two vertebrae belonging to her daughter, Stephanie Lane, who was 20 when she vanished in January 1997. Lane is among six women whose DNA was found on Pickton's farm but whose cases did not result in charges. Pineault said prosecutors told her at the time that Lane's DNA was found in a freezer, which wasn't enough to proceed with charges. She said she was never told about the bone fragments' existence. "I was told that ... if there had been more [than DNA], it would have been enough to charge him," Pineault hold a news conference in Vancouver, holding a pair of small plastic bags containing her daughter's remains. "I want Robert Pickton charged with my daughter's murder." The B.C. Coroners Service said in a statement that the remains were known to police during the original investigation and "do not represent new evidence." Crown spokesman Neil MacKenzie said prosecutors also knew about Lane's remains when they made their decisions about charges. He repeated the criminal justice branch's long-standing position that Pickton will not be prosecuted for additional murder charges. Canadian Press (Times Colonist, A7, Whitehorse Daily Star, Waterloo Region Record, The Province, The Telegram, 24Hrs Vancouver), Globe and Mail, Postmedia News (Vancouver Sun, National Post)

*** Sentence too light**

If it were up to Alberta's top court, drunk driver Ryan Jordan Gibson would have been handed a prison term of at least four years. But in rejecting Gibson's appeal of his 32-month sentence on Wednesday, a three-m ember Alberta Court of Appeal panel said they were bound by the punishment imposed. "A fit sentence here would be no less than four years," the judges said, noting the Crown had not given notice of and intention to contend the original sentence. "Recent authorities from other jurisdictions have seen fit to impose four-and-a-half or five years imprisonment where less egregious driving patterns were present," they said in a written ruling. Because the Crown did not give such notice, it cannot now seek to appeal the sentence to the Supreme Court, despite the judges' comments a greater punishment would have been appropriate. Gibson had appealed the 32-month sentence imposed by provincial court Judge Karim Jivraj

who rejected a Crown and defence joint submission for a two-year term. The appeal court judges said Jivraj was correct to find the two-year sentence proposed was outside the proper range considering Gibson's conduct in killing Cochrane teen Brandon Thomas. Calgary Sun, 7, Calgary Herald

*** Some of the others charged in Project Axe**

EMMANUEL ZÃPHIR, 42, MONTREAL Pasquale Mangiola drew the attention of police when ZÃ©phir, considered a leader among Montreal street gangs for nearly two decades, agreed to buy a kilogram of cocaine from him. Project Axe was centred on ZÃ©phir and many members of the Syndicate, a street gang ZÃ©phir took control of early in 2006, when he left a federal penitentiary after having serving an eight-year prison term for having killed a rival gang member who stabbed him first, in 1999, during a party in Montreal. In December 2010, ZÃ©phir pleaded guilty to several charges related to Project Axe - notably drug trafficking, conspiracy to traffic drugs and gangsterism. He was sentenced to an overall seven-anda-half-year prison term. He was left with 34 months to serve when his case came to an end.(…) CURTIS RODNEY, 41, POINTE-CLAIRE A longtime friend of Mangiola's who delivered the kilogram of cocaine Mangiola sold to ZÃ©phir. He was also convicted of possessing 600 Cialis pills, designed to treat erectile dysfunction, with intent to traffic. He is currently serving a sentence of 40 months, which he received in November. Montreal Gazette, A3

*** Inquest to be held into death by starvation**

A 41-year-old man, abused as an infant into physical and intellectual disability and starved to death by his brother, will be the subject of a coroner's inquest, the province announced Wednesday. Jamie Hawley weighed just 57 pounds and his frail body was covered in 33 bedsores when he died at Brockville General Hospital in May 2008. (…) Hawley's official cause of death was listed as starvation, pneumonia and infected bedsore. Experts testified at trial that these were preventable ailments that could have been treated before they became fatal. Ontario Superior Court Justice Lynn Ratushny sentenced Jerry Hawley to 20 years in prison for circumstances she said were "nearmurder" carried out by a man "primarily interested in working, partying, beer and drugs" and not the responsibility of caring for his brother. "It is a tale of a young man with serious physical and mental disabilities who was taken in by his brother for his disability benefits and who ended up being ignored, neglected, degraded, tortured and starved," Ratushny said in her decision. "It is a harrowing account of extreme neglect that should never have happened." The inquest will attempt to determine how exactly it did happen and a jury will be tasked with making recommendations to prevent similar deaths. Inquests do not lay blame or find fault. Inquests are not typically called until all criminal charges have been resolved. Jerry Hawley had filed a notice for leave to appeal both his conviction and his sentence but has since abandoned the conviction appeal, his lawyer Sam Scratch confirmed to the Citizen. A date to appeal his sentence has not been set but will not run counter to the inquest. Ottawa Citizen, A6

*** Psychopathic criminals learn differently from punishment cues**

Criminal psychopaths learn to respond differently to punishment cues than others in jail and may need more reward-focused treatments, new research suggests. Criminals such as Paul Bernardo, Ted Bundy and Clifford Olson, who scored high on psychopathy checklists, were known to be callous and unemotional. Psychopaths derive pleasure from being manipulative and use premeditated aggression to get what they want with no regard for those who are hurt. The search for what makes them tick has shown some physical differences in their brains such as reductions in grey matter. (…)The findings could have implications both for treating incarcerated psychopaths and to prevent children showing callous tendencies from progressing to psychopathy. In Canada, psychopathy occurs in about one per cent of the population. In federal prisons, it's about 25 per cent, said Michael Woodworth, a psychologist at the University of British Columbia Okanagan, who has worked on research projects with Correctional Service Canada. CBC News, Le Devoir

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Strip-search challenge to proceed**

A charter legal challenge alleging that level-three strip searches by Toronto police discriminate against aboriginal people is going ahead, after a judge denied an attempt by the Toronto Police Services Board and four officers to dismiss portions of the claim. In a decision released Monday, Judge Paul Perell rejected the defendants' argument that claims of discrimination by Toronto resident Megan Anoquot should be excluded because the allegations are "a disguised class action." And Perell dismissed the notion that previous searches conducted on Anoquot - who has been arrested several times for petty theft - aren't relevant to the case. Natalie Kolos, the lawyer for the board and police, had argued they should be excluded because officers conduct the searches on a "case-by-case basis." "With respect, the Defendants seem oblivious to the nature of the claim that Ms. Anoquot is making, which is that the Defendants employ a stereotypical approach and systemically strip search Aboriginals rather than engaging in a case-by-case basis," wrote Perell in his ruling. Toronto police conducted invasive strip searches in 60 per cent of all arrests, according to statistics from 2010 that were quoted in the ruling. Toronto Star, GT1

*** Sex ed called out of step in digital age**

While the province works on a new curriculum, schools in Ontario are teaching sex education based on guidelines developed in the digital dark ages - or at least a time before sexting was part of the vocabulary. Not only is the 15-year-old sexeducation curriculum out of step with technology, said Sara Mison, of Ophea, a lobby group that advises the Ontario government on physical and health education, it hasn't kept up with physical changes in children. A few decades ago, the average age of puberty was 10 or 11. Now, many girls and boys go through puberty at nine or 10, a trend not recognized in the way sex education is currently taught. Educators and others say teachers should talk to students about puberty in Grade 4 - a year earlier than they do now. That change was included in curriculum introduced by the Ontario government in 2010, but it was later scrapped amid criticism. Since then, Ontario schools have continued to teach sex education based on curriculum developed in 1998. Proposed changes are, once again, proving controversial in Ontario. Ottawa Citizen, A12

*** Battling gangs through city budget**

There's a chance antigang funding will become a fixture in the city budget. "We'll see how that first year goes and then if there's a requirement for additional funds, which I suspect there will be, then we'll look at that in context of the 2016 budget," Mayor Jim Watson said Wednesday. As reported first by the Sun, the city is looking to spend $250,000-$350,000 on an exit strategy for gangsters in the 2015 budget. Watson wouldn't discuss the numbers, saying they will be revealed when the draft budget is released next week. The money would eventually go to Crime Prevention Ottawa via the social services department. In other words, the city would have control over releasing the funds to CPO each year. There are questions about whether a quarter-million dollars is enough money to help mostly young men leave gangs. The city money would be spent on working with outside agencies that have expertise in getting criminals to turn their lives around. QMI Agency (Ottawa Sun, 5)

PUBLIC SERVICE / FONCTION PUBLIQUE

Les dirigeants syndicaux du secteur public fédéral sont inquiets

Plus que les chiffres, l'incertitude entourant le prochain budget fédéral et l'intransigeance manifestée par le premier ministre Harper n'ont rien pour apaiser les craintes des dirigeants syndicaux du secteur public fédéral. «Nous sommes très nerveux. Nous sommes comme dans une tempête, alors que le vent tourne continuellement», observe le vice-président exécutif de l'Alliance de la fonction publique du Canada (AFPC) pour la capitale nationale, Larry Rousseau. Selon lui, l'analyse du directeur parlementaire du budget de l'impact de la baisse des prix du pétrole a peut-être réussi à mettre les pendules à l'heure au niveau budgétaire. Mais il reste encore trop d'inconnus pour savoir comment le gouvernement réagira à ces turbulences, alors qu'il est déjà en pleine ronde de négociations avec l'ensemble des employés du secteur public fédéral. «C'est comme si on nous avait dit que les freins de notre char étaient très usés, illustre M. Rousseau. Nous roulions à 40km/h pour éviter le pire. Mais là, c'est comme si on était obligé de passer à 100km/h et qu'on ne sait pas si on va pouvoir éviter l'obstacle en avant.» A l'Institut professionnel de la fonction publique du Canada (IPFPC), la présidente Debi Daviau déplore que le

gouvernement ait des services publics «pour appliquer le programme de réduction d'impôt tordu». Le Droit, 9

Parliament watchdogs fear disclosure bill could trigger 'witch hunt' among staff
Parliament's watchdogs used terms like "witch hunt," and "metaphorical tattoo" to argue against a bill that would require their employees and potential hires to disclose any past political positions. Four agents of Parliament who appeared before a Senate committee Wednesday night said that Bill C-520 appears to be trying to fix a problem that doesn't exist, but could create new ones. "Candidates for positions in the offices of agents of Parliament must declare their past political activities, but what are agents to do with this information?" said Privacy Commissioner Daniel Therrien, who said political preference is considered by law sensitive personal information. "Or put another way, it is not clear for what specific problem is this legislation a remedy?" Conservative MP Mark Adler's private member's bill obliges anybody applying for a job with an agent of Parliament to declare prior political work. Current and future employees would have to post their political histories for the decade before their hire on the Internet. Canadian Press (CTV News)

OTHER / AUTRE

*** France wants Canada on UN Security Council**
Canada should try again for a seat on the United Nations Security Council despite its historic loss in 2010, because it is a "global player," says the French ambassador to Canada. Envoy Philippe Zeller said he's noticed that the Harper government has drifted away from engagement with the UN, but as one of the permanent five on the Security Council, France would value having Canada back at the table. In October 2010, Canada lost to Portugal in a bid for a two-year council term. The defeat came after six successful campaigns for a seat over the previous six decades. Analysts have variously attributed the defeat to the Harper government's controversial foreign policies in the Middle East and Africa, or to Europe closing ranks to support one of its own. Zeller, who leaves Ottawa next week after a three and half years in Ottawa, said Canada and France see eye-to-eye on 90 per cent of issues, but on UN relations it has noticed that Canada under the Conservatives seems to have less time for the institution. He cited Canada's withdrawal from the Kyoto Protocol and the Convention to Combat Desertification. Zeller said all countries have to regularly review their foreign policies. "But when it's such a question as to how to deal with desertification, well it's difficult to accept, to see a leader like Canada, countries that are known for having developed aid policy since the 1960s, to decide to go out. But we have to respect that." Daily Gleaner, B1

INTERNATIONAL / INTERNATIONAL

*** The (good) problem with Ebola - Just a few months after the epidemic in West Africa peaked, doctors worry a dramatic reduction in cases could imperil hopes of having vaccines and treatments ready for the future. 'It is a concern,' one public health official says, 'but it's a good concern to have'**
Earlier this week, Medécins Sans Frontières (Doctors Without Borders) reported something that might have seemed unimaginable at the zenith of the Ebola epidemic, when the aid agency had to turn dying patients away from its teeming treatment facilities. Only 50 or so of the 650 isolation beds at MSF's eight Ebola treatment centres in West Africa are now occupied. The empty beds are a tangible sign of the steep decline in new cases in Guinea, Sierra Leone and Liberia, a development that is being greeted with cautious optimism - and warnings against complacency - in the international public health community. Beneath the optimism is a growing acknowledgment that what is undoubtedly good for the people of West Africa is very likely bad for the quest to bring Ebola vaccines and treatments to market. Case counts are plummeting just as the first large-scale trial of experimental Ebola vaccines is about to get under way in Liberia, where only 29 new cases have been confirmed in the past four weeks, down from a high of 367 in a single week in September. The phase three trial of two vaccine candidates, including one made in

Canada, needs to have enough Liberians at risk of Ebola exposure to determine if either shot shields people from the virus. Globe and Mail, A10

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
January 30, 2015 / le 30 janvier 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

The language of terrorism
Following the terrorist attacks in Paris earlier this month, Prime Minister Stephen Harper cranked up his rhetoric. "We will not be intimated by jihadist terrorists," said Harper during an appearance in a Vancouver suburb, adding that "the international jihadist movement has declared war" on Canada and its allies. Now, just a few weeks later, the term "jihad," or "jihadi" has become a routine part of the government's speaking notes. This vocabulary - along with terms such as "Islamist" which the prime minister has also used, and even "war" - is one method politicians use to try to frame the often-complex debate around terrorism policy. "I'm guessing it's a way that they want to simply capture that very broad, very diff use set of actors," says Jeremy Littlewood, a senior research affi liate with the Canadian Network for Research on Terrorism, Security and Society, and a Carleton University international aff airs professor. Groups such as al-Qaida now have multiple spinoffs or rivals, such as the Islamic State (ISIL), and it's easier for politicians to lump them together than to focus on their diff erences. [...] And while recent internal CSIS documents identified suspects in recent terrorist plots as "Islamist extremists," the agency has stopped using the term in its public annual reports. Similarly, Public Safety's annual terror threat reports have avoided all terms relating to jihad and Islam, though the agency's minister, **Steven Blaney**, uses terminology similar to that now employed by Harper. Conservative Sen. Lynn Beyak took the agency to task for its selective wording last fall when officials testified at the national defence committee. Ottawa Citizen, A9

Terrorism bill worries privacy experts
The Conservative government will redefine free speech Friday as it tables a new bill to criminalize the promotion of terrorism. The bill was drawn up after the attacks against soldiers in Quebec and Ottawa last

fall. It is widely expected to grant police new powers to arrest people who are suspected of supporting terrorist organizations but have not made explicit threats. Prime Minister Stephen Harper said Sunday the bill will "criminalize the promotion of terrorism and prevent terrorists from travelling and recruiting others." This has privacy experts worried. Police can already arrest people for planning a crime, so these new arrest powers could extend to people who have committed no wrongdoing, said Josh Paterson, executive director of British Columbia Civil Liberties Association. Criminalizing the mere expression of support for a terrorist group is likely unconstitutional, Paterson said. "Expanding the government's power to detain people without any charge, without having committed any crime, is a very serious matter and really runs against the principles of fundamental justice." Harper is scheduled to publicly unveil the bill early Friday afternoon in Richmond Hill, Ont., with Justice Minister Peter MacKay and **Public Safety Minister Steven Blaney**. The government hasn't revealed the details of what is in the bill, but there are signs it will include broad changes. The tentative title of the bill shows it will make changes to Canada's spy agency, immigration rules and to who is allowed on a plane. Chronicle Herald, A10

Sweeping new powers on the way for spy agencies
Minister Stephen Harper will unveil Friday details of an omnibus public safety bill to bring in a raft of new anti-terror powers, including authority to knock terrorist propaganda offline and new protections for secret evidence gathered by spies. Broader powers for CSIS to disrupt terror activities, such as air travel or bank transactions by suspects, are among some of the details reported by media outlets Thursday evening - a big expansion of the agency's role that was strictly limited to intelligence gathering since its creation of 30 years ago. The bill will enact two new laws and make amendments to the Criminal Code, the CSIS Act, the Immigration and Refugee Protection Act among a host of others. It's not clear whether the Conservatives are prepared to boost the budgets of national security agencies, a key focus of opposition criticism. The government put the Commons on notice that funding will attach to the measures, but a senior government official said it shouldn't be interpreted as new funding, rather is intended to provide authority to spend for a new purpose. However, the official Opposition NDP insists the question of resources is the main one and is skeptical of the need for new laws it fears will further erode civil liberties and privacy rights. Harper has chosen the riding of Richmond Hill to make the long-awaited announcement, flanked by **Public Safety Minister Steven Blaney** and Justice Minister Peter MacKay at the same time the bill itself is tabled in Parliament. Toronto Star, A4

Premiers to debate disaster funding - Federal-aid changes top meeting agenda
It's unfair of Ottawa to unilaterally tell the provinces they have to shoulder millions more of the cost when a natural disaster strikes, Premier Greg Selinger said Thursday. "It's a fairly significant download," said Selinger, who arrived in Ottawa Thursday for a premiers' meeting where disaster-aid changes will be a prominent item on the agenda. "It's a concern to all the premiers." Until this weekend, Ottawa's aid following a disaster kicked in after costs hit the equivalent of $1 per capita in a province. In Manitoba, the threshold for Ottawa's help starts at about $1.3 million, Selinger said, and Ottawa would begin paying 90 per cent of the costs when the bills exceeded $6.5 million. The new formula, which kicks in Feb. 1, means Ottawa won't start paying until the costs hit $3.9 million, and won't begin covering 90 per cent until the bills exceed $20 million. Selinger said many smaller emergencies may never qualify for federal aid now, and added the formula will be indexed to inflation so the provinces will continue to share larger portions of the bills in years to come. He said he was first told there was a change coming to the formula a couple of weeks ago. Federal **Public Safety Minister Steven Blaney** put out a release Jan. 16, and the formula will change this Sunday. "It was a unilateral decision, and it's come fairly rapidly," said Selinger. "It puts a lot more pressure on the provinces." In 2013-14, a briefing package from the Department of Public Safety identified the rising costs associated with the disaster financial assistance program as the biggest risk facing the department and noted it was being reviewed for sustainability. Winnipeg Free Press, A10

Gouvernement Harper - Punir, punir, punir
Un éditorial déclare, “Il y a des indices qui ne trompent pas. La multiplication des lois par le gouvernement de Stephen Harper pour resserrer les conditions de détention des prisonniers nous confirme que nous serons bientôt en élections. Qu'il s'agisse de terrorisme ou de criminalité, les conservateurs s'assurent de faire comprendre aux électeurs qu'avec eux la loi et l'ordre régneront au Canada.\r\nLe premier ministre Harper en avait fait la promesse dans le dernier discours du trône. " Trop longtemps, la voix des victimes a été réduite au silence, pendant que le système dorlotait les criminels ",

avait-il dit en octobre 2013. Il ne l'a pas oublié. D'ici la fin de la session, des projets de loi seront adoptés, d'une part pour rendre caduque la pratique de mise en liberté anticipée et automatique aux deux tiers de la peine dans le cas des multirécidivistes, d'autre part pour faire en sorte qu'une sentence à vie soit bel et bien un emprisonnement à vie. [...] Ces mesures ont eu pour effet d'augmenter la population carcérale et le temps passé en prison où, à en croire les préjugés courants, ce serait un peu la vie d'hôtel. Pour s'assurer qu'il n'en est plus ainsi, les détenus sont désormais souvent deux par cellule (comme les étudiants au collège, a déjà fait valoir le **ministre Steven Blaney**), le service des aumôniers a été réduit, tout comme l'accès à des cours de formation. Puis, on apprenait cette semaine que désormais il n'y aura plus de cuisine en prison : on servira des plats congelés. Quant au verre de lait frais, il sera remplacé par du lait en poudre. Il n'y a pas de petites économies, comme il n'y a pas de petites peines de prison." Le Devoir, A8

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Second Lower Mainland bird-flu case confirmed**
A Lower Mainland man has been confirmed as Canada's second case of H7N9 bird flu. The unidentified man and his wife are believed to have contracted the virus during a recent trip to China. They are the first North Americans known to have been infected with this virus. Bonnie Henry, B.C.'s deputy provincial health officer, said the positive test result was confirmed late Thursday by the National Microbiology Laboratory in Winnipeg. Both patients have recovered, and no other cases have been reported. Canadian Press (Times-Colonist, A6; VancouverProvince.com; CTV News)

*** Flu vaccine a bust this year: study - Shot offers little protection against most common strain in Canada**
This year's flu vaccine offers little or no protection in Canada against becoming sick enough to require medical care, a study published Thursday suggests. The research, based on data from British Columbia, Alberta, Ontario and Quebec, found the vaccine offers most people virtually no protection against the strain that's causing the lion's share of the illness this year, H3N2. There weren't enough cases of flu caused by H1N1 or influenza B viruses to assess whether the vaccine would have been more protective against them. That may change as the flu season progresses - it is not uncommon to see late-season surges of influenza B illness. But for now, this year's shot's performance looks pretty dismal. Canadian Press (Times-Colonist, C11); Edmonton Sun; Edmonton Journal

*** Winter storm could blanket New Brunswick with 35 cm of snow**
Another winter storm is heading toward New Brunswick and could dump 35 centimetres of snow on parts of the province by Saturday. Environment Canada has issued a winter storm warning for most of the province and a winter storm watch for the northwest parts of New Brunswick. Snow is expected to start on Friday afternoon and up to 35 cm is expected to fall by the end of Saturday, according to Environment Canada. The agency is advising people to consider postponing non-essential travel and to take extra care when walking or driving in affected areas. CBC News; Radio-Canada; Times and Transcript

*** Group uses Winnipeg boil water advisory to highlight First Nation water woes**
A group is using Winnipeg's boil-water advisory to highlight the ongoing struggles of the First Nation that supplies the city with its drinking water. Shoal Lake 40 First Nation, which provides Winnipeg with water through an aqueduct, has been under a boil-water advisory for 17 years. Chuck Wright said it's time Winnipeg residents learned more about the cost of their drinking water. "I really hope that the inconvenience of only a day and a half of an E. coli scare that it will create more empathy for the many, many First Nations, not just Shoal Lake 40, that have been under boil-water advisories and without adequate drinking water for so many years, sometimes decades," he said. Wright and a few others handed out bottled water Thursday in downtown Winnipeg, plastered with the label "Boil Water Advisory Day Count - Winnipeg: 1.5, Shoal Lake 40: 6,205+" to raise awareness about the reserve. Canadian Press (Cape Breton Post, A9; Charlottetown Guardian)

*** La ligne comptable Lac-Mégantic**

Autant de dévastation ne pouvait pas faire autrement que de causer de sévères dommages aux citoyens de Lac-Mégantic. Encaisser un pareil choc, ça fait aussi dérailler des vies! Au-delà des 48 pertes de vie (un suicide est recensé avec les 47 victimes déclarées), les blessures psychologiques sont profondes et il faudra des années pour les guérir, a dépeint mercredi la Direction de la santé publique de l'Estrie. On n'a pas lésiné sur les moyens pour décontaminer les sols souillés par le pétrole. On a calculé les volumes de terre à déplacer et à traiter, une première estimation de 200 M$ a été avancée, et on est parti avec ça. Advienne que pourra. Même chose pour le nettoyage des cours d'eau. Il faut ce qu'il faut. Le premier politicien qui agira en trésorier plutôt qu'en gardien de l'environnement finira dans le goudron et les plumes. Combien de temps et d'argent faudra-t-il encore pour faire disparaître toute trace de « contamination » chez les humains? Selon les données compilées par l'Agence de la santé et des services sociaux, les services de santé associés à la tragédie de Lac-Mégantic se chiffraient à 4,5 M$ à la mi-décembre. De cette somme, 1,8 M$ sont imputés au Centre des services sociaux de la MRC du Granit, dont le personnel a évidemment été le plus sollicité. Québec a compensé 100 pour cent de la facture de 2,8 M$ présentée pour les services rendus au cours des sept mois et demi ayant suivi le déraillement, durant l'exercice financier 2013-2014. La Tribune, 6

*** SaskAlert to spread word in emergencies**

Saskatchewan finally has its own emergency alert system. The testing phase for SaskAlert will begin on Feb. 1 in the western part of the province, through the Weather Network's smartphone app, website, Twitter feed and TV station. By the time it's fully online - emergency management commissioner Duane McKay hopes within about a month - it will disseminate emergency information through smartphone apps and the media. Saskatchewan has seen "a significant increase in emergency events" over the past several years, and SaskAlert will plug a good chunk of the communication gap when danger approaches, McKay said. Alerts will be split into Level 1 and Level 2, depending on the immediate threat to lives and property. A tornado, destructive storm cell or train derailment in which an entire community needs to be evacuated, for example, would be a Level 1 warning. Leader-Post (Star-Phoenix, A6)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

The dark sophistry of CSEC

'Levitation" might suggest a matter of levity, but the project of the Communications Security Establishment Canada that goes by that name is another unsettling example of "tradecraft" disclosed by Edward Snowden. The objective of the program is detecting terrorists, but Levitation appears to do this by broadly surveilling Canadians - just what CSEC is not allowed to do. Mr. Snowden found a deck of CSEC slides explaining how Levitation sweeps up vast quantities of files from upload sites, searching for suspicious videos or other electronic documents that, for example, provide instructions to terrorists on how to make a gas bomb. The Levitation presentation uncovered by Mr. Snowden is businesslike, and has a relaxed and often jocular language. For example, it explains how, in searching through millions of uploaded files, Levitation is able to filter out episodes of the musical-comedy television show Glee. If uploaded episodes of TV programs and enormous quantities of other data are being searched and accessed, it suggests that CSEC is collecting huge libraries of files and signals from millions of Canadians. Which, again, is not what CSEC is supposed to be doing. The CSEC presentation says that it sees 10 to 15 million free file uploads (FFU) per day from around the world. The presentation says that out of all of this trawling, CSEC is "finding about 350 interesting download events" a month. One example of success was finding a hostage-taking strategy for al-Qaeda in the Islamic Maghreb, which the CIA and other agencies then shared. Globe and Mail, A10

Canada needs to watch the watchers

An opinion piece in the Times Colonist states…."Quis custodiet ipsos custodes? While Latin might have gone the way of the dinosaurs, the meaning behind that ancient Roman phrase couldn't be more relevant: Who watches the watchers? A peculiar situation has emerged in this country since 9/11: Intelligence gathering has become more important while the review process for these activities has been diminished. Our security officials haven't had as free a hand to carry out their business since the cavalier days of the RCMP Security Service, which was found to have been involved in barnburning and other illegal activities in the 1970s. Once almost the exclusive turf of the Mounties, intelligence gathering is now conducted by

14 different federal agencies, including the Canadian Security Intelligence Service, the Department of National Defence, Canada Border Services Agency and the Communications Security Establishment. There are numerous ways to hold these agencies accountable. The most far-reaching is an oversight system, where an independent body is granted leverage over an agency's management, such as by holding some purse strings. Another option is to have a review process, where the agency is examined after the fact to ensure they have behaved in a legal manner. Canada has generally followed the latter approach with respect to CSIS and CSE, but has no review system in place for any of the other agencies. Times Colonist, Hamilton Spectator, The Guardian, Postmedia News (Vancouver Sun)

Stephen Harper expected to unveil new anti-terror bill, with expanded powers for CSIS, on Friday
Prime Minister Stephen Harper is expected to unveil on Friday details of a bill that would provide Canada's government with new powers to fight terrorism, according to several news reports. The powers will include protections for evidence gathered through espionage, and the ability to remove terrorist propaganda from the Internet, according to a report in the Toronto Star. As part of the legislation, the Canadian Security and Intelligence Service - Canada's spy agency - would get new powers to help prevent radicalized Canadians from travelling overseas or funding suspected terrorist activity, according to a CBC News report, citing sources familiar with the legislation. The Toronto Star reported that the Conservative omnibus safety bill would include amendments to the Criminal Code, CSIS Act and the Immigration and Refugee Protection Act. Related Conservatives will introduce new security legislation aimed at stopping lone-wolf terrorist attacks: Harper. Give all-party watchdog the power to oversee Canada's new anti-terror measures, Justin Trudeau urges PM. National Post.com (Ottawa Citizen, Edmonton Journal, Calgary Herald, Leader-Post, StarPhoenix, Windsor Star, Vancouver Sun)

*** The critical tool of skepticism**
An opinion piece states, "Canada's recent experience with terrorism is not unique. Nor is its government alone in seeking to introduce fresh counterterrorism laws and powers. Across the Atlantic, Britain is debating new legislation that would, among a range of changes, allow the government to block the return of Britons suspected of involvement in terrorism while abroad, require Internet providers to keep records of IP addresses so computer users could be identified, and legally require a variety of state institutions, including universities, to "prevent individuals being drawn into terrorism." As such, there are cautionary aspects of the British experience, both with the current legislation and with past efforts at reform, that should inform debate over the Canadian government bill being tabled Friday. Top among the lessons is that skepticism about the need for new powers or laws should be the default reaction from parliamentarians, news media and the wider public. Over the past decade, and across seven significant counterterrorism bills introduced since Sept. 11, 2001, various British governments have preached that the counterterrorist sky would come crashing down without the introduction of new, supposedly essential measures. Mandatory identity cards were needed to prevent terrorism, Tony Blair's government warned. David Cameron's government killed off this proposal in 2010." Globe and Mail, A11

*** CSIS to be given new anti-terror powers**
Canada's spy agency will be granted the authority to intervene and disrupt threats to national security in a massive expansion of its powers as the federal government tries to make it easier to thwart terror plots at home and abroad, sources say. The Canadian Security Intelligence Service's role is currently restricted to collecting intelligence, analyzing and reporting on dangers to Canada, but new anti-terror legislation to be unveiled Friday is expected to rewrite its mandate to allow CSIS agents to take action to foil security threats. The new role for CSIS is one of a series of measures in the legislation promised after deadly attacks on Canadian soldiers last October that also saw a gunman storm Parliament Hill. Ottawa is building in judicial oversight for this new CSIS power, however, and will require the agency to obtain a court warrant to flex its new muscles. As long as a judge approves, CSIS agents would be able to cancel someone's travel reservations, for instance, or disrupt a banking transaction or electronic communications. The new power would lift a fundamental restriction on CSIS's activities and gives the agency a measure of authority that's currently reserved for police forces. CSIS, a civilian agency, was created in the early 1980s after an inquiry into the RCMP security service's illegal activities and civil-rights abuses recommended that policing be separated from intelligence gathering. Globe and Mail.com

Analyst: Schools present a problem

Islamist ideology that's taught in Canadian mosques and Islamic schools is the biggest challenge facing investigators, a security expert tells QMI Agency. Former CSIS manager Michel Juneau-Katsuya said police don't have resources to deal with "the sheer number of young minds being radicalized." He was reacting to QMI Agency's investigation into the expanding national real-estate footprint of the Muslim Association of Canada (MAC). QMI obtained an RCMP document indicating MAC donated nearly $300,000 to a Hamas-linked group before the federal government revoked its charity status. Juneau-Katsuya, without naming any specific groups, says law enforcement must always remain vigilant, adding that such organizations "capable of deploying a phenomenal amount of resources and influence, need to demonstrate to the authorities that they do not represent a risk." He said anti-terror investigators need help from Muslim leaders, such as the unnamed Toronto imam who reportedly tipped off police in 2013 to an alleged Via Rail bombing plot that led to two arrests. A noted critic of Islamic extremism says not everyone is so willing co-operate. QMI Agency, 30 (Edmonton Sun, Toronto Sun, Calgary Sun, Kingston Whig-Standard, Ottawa Sun)

Group denies funding

The Muslim Association of Canada (MAC), accused of funnel-ling money to a Hamas-linked charity, said it hasn't supported the group since IRFAN-Canada's charity status was revoked in 2011. A QMI Agency investigation found the Toronto-area-based Muslim nonprofit was named in an RCMP probe into terrorist financing. Warrants indicate the association sent nearly $300,000 in the 2000s to IRFAN-Canada, a group that raised millions for Hamas, a listed terror group. The RCMP raided IRFAN locations in Montreal and Mississauga last April 28 and declared it a terrorist organization on the following day. RCMP documents obtained by QMI Agency suggest the force might still be investigating possible ongoing links between MAC and IRFAN. MAC said in a statement it is "opposed to ter rorist activity of any kind" and hasn't supported IRFAN since 2011. "When specific allegations of IRFAN's relationship with groups that are inconsistent with MAC's values arose, we immediately stopped all donations to that group." QMI Agency, 30 (Edmonton Sun, Calgary Sun, Toronto Sun, Ottawa Sun)

Djemila Benhabib est troublée par des propos de Philippe Couillard

L'ex-candidate péquiste et militante pour la laïcité Djemila Benhabib se dit troublée de voir que le premier ministre Philippe Couillard tolère l'intégrisme religieux. Mme Benhabib a affirmé hier que le terrorisme est un produit de l'intégrisme, qui est par essence antidémocratique. « Montrez-moi un intégrisme qui respecte le droit des femmes, ça n'existe pas, a-t-elle dit hier. [...] L'intégrisme est une idéologie abjecte qui porte en soi la discrimination, la haine de l'autre et la détestation. » Lors d'une conférence en compagnie d'une journaliste de Charlie Hebdo, Zineb El Rhazoui, Mme Benhabib a réagi à de récents commentaires de M. Couillard. « Un premier ministre qui considère qu'il n'est pas de son devoir de combattre l'intégrisme religieux, je trouve ça quand même troublant », a-t-elle dit. Plus tôt cette semaine, M. Couillard a affirmé que l'intégrisme doit être considéré comme un choix personnel qui peut être toléré tant qu'il ne s'attaque pas aux droits de la personne. La Presse.ca (La Tribune)

*** ISIS sympathizer's road to jihad - from Canada to Syria to Iraq - tracked one Tweet at a time**

The Toronto woman who Tweeted so sympathetically about ISIS probably had no idea that, when she left Canada late last year, she was being tracked by researchers following her movements using geocoding. But every time she posted a Tweet, she was inadvertently giving away her location, allowing the researchers to map her as she travelled from the ISIS capital in Raqqah, Syria to the front lines in Kobani and Mosul. "I did not see in their actions anything but the utmost of respect for me as a sister," she wrote in Arabic from Kobani on Dec. 25. In another Tweet, she wrote: "God bless those who live on His path and who die on His path." By failing to turn off the locator on her cellphone, she not only left an incriminating electronic trail, she also highlighted a disturbing trend: Canadian women are increasingly involved in supporting the Islamic State of Iraq and al-Sham. While most of the Canadians who have either left to join ISIS or who have been stopped by police en route are men, some are women. ISIS prohibits women from taking part in combat, so their roles are limited to serving as "jihadi brides." .Every time a Toronto woman who Tweeted sympathetically about ISIS posted a Tweet, she was inadvertently giving away her location. A report released Wednesday by the London-based Institute for Strategic Dialogue said that about 550 of the 3,000 Western citizens in ISIS territory are women. The study looked at the social-media profiles of several women in ISIS, one of them a Canadian. Edmonton Journal, A16

(Nationol Post, Ottawa Citizen, Calgary Herald, Montreal Gazette, Leader-Post, StarPhoenix, Vancouver Sun, Windsor Star)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Ruling cuts sentences for date-rape drug smugglers
The B.C. Court of Appeal has reduced the sentences of three men convicted of trying to traffic more than 1,000 kilograms of the date-rape drug ketamine that had been smuggled into Canada. The province's highest court ruled the trial judge was wrong to find the three men - Yiu Tim Kwok, 62, Hin Cheung Lau, 46, and Wing Kee Ng, 62 - belonged to a criminal organization, earning them a longer sentence. The appeal court reduced Kwok and Ng's sentence to 12 years from 16 years for smuggling the ketamine into Canada with the intention of trafficking it. And the three appeal judges cut Lau's term from 10 years to six years for his conviction for possession for the purpose of trafficking. All three also got extra credit for the time they served in pre-trial custody. Appeal Court Judge Elizabeth Bennett said "the Crown did not prove beyond a reasonable doubt that they formed a criminal organization." "In my respectful view, the sentencing judge erred when she found as an aggravating factor that these appellants fit into the definition of criminal organization," said Bennett in her reasons, released Thursday. Judges David Frankel and Edward Chiasson concurred. In December 2010, the Canada Border Services Agency intercepted the ketamine - worth up to $50 million. Border agents were suspicious of Kwok when he entered Canada that month with "documents relating to the shipment of coffee mugs," Bennett noted. "As a result, the shipment was intercepted, the drugs were found and sugar was substituted for the ketamine. A controlled delivery was performed, and the shipment of coffee mugs was delivered." Postmedia (The Vancouver Sun, The Province)

Boarding with bullets
Machetes and maple syrup, police batons, bullets (real and fake) and peanut butter: these items don't fly at Toronto's largest airport. But that doesn't mean some people don't try, which is why they're among the objects recently confiscated from Pearson International Airport's nine security checkpoints. Anything brass-knuckle-related - the latest trend in phone cases and purse handles - is taken away. Finding the weapon itself merits a call to the Peel Regional Police airport division; so does the seizure of illegal throwing knives, another treasure in the chest. Have you heard of a stun gun concealed in a cellphone case? Mathieu Larocque, spokesperson for the Canadian Air Transport Security Authority (CATSA), has. They're not found at security ever day, but he's seen a few. Lately, Larocque said, blenders are growing in popularity as a carry-on item. The blender jar, he said, can go through. The blades are a no-go. A normal bin of seized items brims with scissors, lighters and small knives, said Larocque; security checks at Terminal 1 on Monday and Tuesday filled two of them. The bins don't include liquids, aerosols or gels, which get tossed right away. "Water bottles are by far the most popular interception, but they're just thrown away," Larocque said. He's not exaggerating; at least a dozen people threw out water bottles at one of Pearson's designated pitching stations in less than an hour Wednesday. A third-party waste management company is in charge of gathering and disposing of the seized objects. The Toronto Star

Tannous to lead border logistics hub at airport
Local lawyer and former border customs officer Laurie Tannous has been appointed CEO of the Institute for Border Logistics at Windsor's Airport. Her mandate will be to help business better navigate trade through the border and attract greater economic investment to the Windsor area.
"It feels like my life's work has culminated with this job," Tannous said. "I'm looking forward to working with the business community to expand trade for this region." The IBLS is a partnership that was formed between the University of Windsor and City of Windsor to create a facility to respond to the needs of companies involved in logistics and movement of trade in both directions across the Windsor-Detroit border. Funding of $20 million for the initiative was supplied by Federal Economic Development Agency for Southern Ontario with another $3 million coming from the city. The plan includes the opening of a FedEx facility at the airport. The university will be part of the operation where training will be made available on logistics for local businesses and students are to be involved conducting research. "The

hope is for Windsor and Essex County is to be known as world-class leaders as it relates to customs and border issues," said Tannous, who will retain her role as vice-president of government relations at Farrow. The biggest winners are likely to be local small-and medium-sized business owners who have no idea how to export goods outside the region, she said. "We will provide education and training at no cost," she said. "We will connect them with individuals outside Canada and make connections happen." The Windsor Star

***Canadians still went south in 2014 despite drop in dollar**

More Canadians crossed at southern Saskatchewan border crossings in 2014 than in 2013, even as gas prices and the Canadian dollar dropped late in the year. "This is a sign of our wealth. We can afford to go on holidays a lot more than we used to," said Doug Elliott, publisher of Sask Trends Monitor, on Thursday. Last year, according to the Canadian Border Services Agency, a total of 388,170 returning Canadians crossed Southern Saskatchewan borders, up more than 60,000 from 2013's totals. Elliott said the high number of Canadians shopping and vacationing south of the border over the past few years can be attributed to the high value of the loonie. In December, the Canadian dollar dropped to 86 cents US. "There's no doubt this will slow with 80-cent dollars," Elliott said. He projected the number of Canadians heading to the U.S. will drop this year. "If you own a condo in Arizona, an 80-cent dollar isn't going to change anything. You're still going to go there, but some of the trips to Mexico may get curtailed. People may decide to go to B.C. or someplace instead," Elliott said. From December 2013 to December 2014, B.C. bordercrossing numbers at one location dropped 7.6 per cent and another border location saw a decline of 11 per cent. "If you think B.C., I usually think of Vancouver and it's right on the border there so that probably is a whole bunch of people going into Seattle to shop. So, it will have been hit harder by the dollar than we are. We mostly go to escape the weather; I think they go to shop," Elliott said. Leader Post

***New Nexus card processing facility opens in Blaine, Washington**

A new Nexus card facility opening just south of the U.S. border crossing from B.C. is expected to drastically speed up the process of getting that coveted card.The card is designed to expedite the border clearance process for low-risk travellers into Canada and the U.S. once they go through a screening interview process. But it can be a lengthy process.But the new Trusted Traveller Enrollment Center in Blaine, Wash. will be able to handle more than 300 Nexus interviews a day — more than double of what was processed at the old building at Peace Arch. "We can process the applications faster, interview the individuals so that we can approve the application at a faster rate than we used to in the past," said Michele James, director of field operations at U.S. customs and border protection. It is the biggest facility of its kind. Ironically, the facility's grand opening comes as new Canada Border Services Agency statistics show a 12.5 per cent drop in Canadians crossing over to the U.S. from this time last year — thanks in large part to the falling loonie. But officials say the demand for Nexus cards is still high."The thing about the falling dollar one way or another, whether it's Canadian or American, is these things are cyclical," said Lynne Platt, the U.S. Consul General Vancouver. "It may feel like, from the Canadian side, the dollar doesn't go as far down here. But on the other hand, it attracts more Americans to go the other direction." CBC (2015-01-29)

***Border hassles can't stop young bluesman**

The way our border cops treat Taylor Scott and his band, it's a marvel he keeps coming back to play Edmonton."It was our worst experience yet," says the 21-year-old frontman. "They literally tore our van apart," adds keyboardist Jon Wirtz. They're talking after a set at Blues on Whyte this week – the band's third appearance at the club since the band formed just a year ago.For any US band subjected to Canadian border crossings, having your van torn apart is no surprise. What's a bigger shock is that the Denver-based quartet has spent a significant amount of their touring time playing in Canada, away from home. Following his last tour dates here in June 2014, supporting their full-length album Lonelier With You, Scott put the band on hiatus to tour overseas as lead guitarist in Chicago great Otis Taylor's band, touring four months throughout virtually every country in Western and Northern Europe. The audiences may be different, he says, but it's the same warm reception they get in North America. Gigcity.ca

***Trade tribunal slaps duties on cheap foreign steel**

British Columbia supports helping to build the national Canadian economy in theory, but apparently not if it means driving up construction costs in B.C. by treating companies in other provinces fairly.Headed into

this week's meeting of Canadian premiers and territorial leaders in Ottawa, B.C. Premier Christy Clark was quoted by The Canadian Press stressing the importance of internal trade: "We should be trading freely between our own provinces. That's the best way, the quickest way to be able to strengthen the national economy. "But those words seem to be at odds with a position the province took this week when it attacked a Canadian International Trade Tribunal ruling aimed at levelling the playing field for manufacturers of steel rebar in Alberta, Ontario and Quebec. Rebar is used to reinforce concrete in construction projects. The case began last April with a complaint from three steel manufacturing companies -- ArcelorMittal LCNA in Quebec, Gerdau Long Steel North America in Ontario and AltaSteel Ltd. in Alberta -- to the Canada Border Services Agency about cheap or subsidized rebar from China, South Korea and Turkey being dumped in Canada. Dumping refers to a predatory pricing practice where a good is sold in a foreign market at a price that is either below what it would be in the home market or lower than what it costs to produce.The CBSA initiated an investigation that led to preliminary duties and an inquiry by the CITT. The tribunal found evidence that the Chinese goods were subsidized at home and that the cheaper rebar from all three countries was being dumped in Canada, threatening to harm the Canadian rebar industry. The Tyee

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Pierre Karl Péladeau victime d'une cyberattaque**
Des pirates informatiques se sont attaqués au site Internet de Pierre Karl Péladeau, le député de Saint-Jérôme et favori dans la course à la direction au PQ. Les agressions virtuelles ont rendu inaccessible «pkp2015.quebec». Elles ont débuté mardi soir, vers 20 h, confirme l'entourage de l'élu du Parti québécois. Elles se poursuivent depuis, en provenance du Québec, mais en grand nombre aussi de pays européens, principalement de l'Allemagne. Jusqu'à hier soir, les conseillers politiques de M. Péladeau n'excluaient pas que celui-ci soit une victime collatérale. Les manoeuvres virtuelles ne le visaient peut-être pas directement, a évoqué pendant la journée l'attaché de presse Marc-André de Blois. C'est tout le serveur Internet, hébergeant celui du politicien, mais également ceux de 29 autres clients, qui était alors paralysé. En début de soirée, «pkp2015.quebec», «pkp» pour les initiales du politicien et actionnaire de contrôle de Québecor, a été transféré vers un nouveau refuge virtuel ne comprenant qu'une seule adresse «IP», donc réservée à Pierre Karl Péladeau. Le Nouvelliste, 24 (Le Soleil); Agence QMI (Journal de Montréal)

*** Global DDoS attacks increase 90 percent on last year**
The increase of distributed denial-of-service attacks during Q4 2014 was driven by the rise of the Internet of Things, and the increasing exploitation of web vulnerabilities and botnet building. Yahoo! News

LAW ENFORCEMENT / APPLICATION DE LA LOI

'Blooding' stirs civil rights concerns
Police in Windsor, Ont., have ordered hundreds of DNA testing kits and are going door to door in a residential neighbourhood asking everyone to provide a blood sample to rule themselves out as a suspect in the murder of a pregnant woman. The unusual mass request for a blood sample prompted more than 500 residents to agree and a "handful" to refuse. It also has stirred warnings from civil libertarians about a police technique increasingly turned to when murder probes falter. "The extraction of a DNA sample without a warrant is concerning. It is inherently coercive," said Sukanya Pillay, executive director and general counsel of the Canadian Civil Liberties Association. "There is no guarantee that doing wide sweeps of DNA collection is going to produce the killer, but there is a guarantee it will create potential privacy violation and erosion of standards." On Dec. 11, Cassandra Kaake, 31, seven months pregnant, was found dead in her home on Benjamin Avenue after firefighters extinguished a blaze. An autopsy found she died of blood loss - not the fire - and a veteran police investigator described it as "the most disturbing" crime scene he had seen. Postmedia News (Vancouver Sun, A1 National Post, A1, Edmonton Journal)

Health Canada puts medical marijuana firm under further RCMP review
Health Minister Rona Ambrose is concerned about the controversy surrounding CEN Biotech, and the company's application to become Canada's largest medical marijuana producer is being sent back to the RCMP for further investigation, her office said. "The allegations against this company are deeply concerning," Ms. Ambrose's spokesman Michael Bolkenius said in an e-mailed statement to The Globe and Mail on Thursday. "This application is with the RCMP," he added. "And it won't be going anywhere until all these issues are addressed." The statement comes on the heels of a Globe investigation that revealed the Ontario company had misrepresented itself to the public, the government and shareholders on numerous occasions and - in an unusual twist - was caught inventing a fake employee to dispute the allegations. All applicants are vetted by the RCMP initially. But the pattern of false claims by CEN Biotech over the past 14 months has called for further investigation. The concerns include misleading investors about its licence status with Health Canada and suggestions that CEN was being favoured by the government. Some of these claims helped push the company's shares up more than 2,000 per cent in the loosely regulated penny stock market. Meanwhile, its chief executive officer, Bill Chaaban, was selling off millions of shares for more than $4.6-million. Globe and Mail, A1

On Patrol
Shawn Schofield and Trevor MacKinnon are bringing an extra level of security to P.E.I.'s Confederation Trail this winter. The two conservation officers with the Department of Environment, Labour and Justice will be assisted by RCMP and members of the P.E.I. Snowmobile Association to conduct safety stops at various locations along the 400-plus kilometres of the trail. The association is the leaseholder of the Confederation Trail during the winter months, which allows permit holders access to the trail from one tip of P.E.I. to the other. Schofield and MacKinnon won't be advertising where they're going to be but promise to do their best to make their presence known. "We pick our spots," Schofield told The Guardian on Thursday. "If there's going to be a lot of people around we'd make sure that we were there to show our presence."... RCMP Sgt. Leanne Butler said Schofield and MacKinnon will be checking for the proper permits but also for any signs of impairment of drivers, noting that the same rules apply on the trail as they do on the province's highways. "Snowmobiles are no different than a car," Butler said, adding that the presence of the two conservation officers will strengthen the enforcement effort and make the whole trail system safer and more enjoyable for all users. The Guardian, A1

Police use Taser to arrest man holding knife to own neck
Regina Police used a conducted energy weapon (CEW), commonly called a Taser, to arrest a man in a downtown business Wednesday night. Police said a 27-year-old male will face charges following an incident in the 2100 block of Albert Street. Around 8:50 p.m. that night, police went to the business over a report of a male exhibiting signs of intoxication by drugs and behaving irrationally. Officers found the man, who'd locked himself in a bathroom stall, and attempted to negotiate with him. "After repeatedly stating he would not co-operate with police, the suspect opened the stall door, holding a knife to his own neck. He ignored police demands to drop the weapon," said a police news release. It added that an officer discharged her CEW and the suspect was taken into custody without further incident. Under the police service's policy, EMS went to the scene and took the suspect to hospital for assessment. "Further investigation found the suspect to be in breach of a court-ordered condition of no contact with (not to attend the workplace of) his former partner," it said, adding the male has been medically cleared and criminal charges will follow. Postmedia News (Leader-Post, A3, Leader Post)

Bank robber strikes again
A serial bank robber has struck again, this time in northeastern B.C. Police and RCMP issued a warning on Tuesday, saying that the man had robbed eight banks over an eight-week period in Alberta, Saskatchewan and Manitoba. On Thursday, RCMP in Dawson Creek said a man fitting the description walked into a bank on Wednesday, produced a firearm and demanded money. He left with an undisclosed amount of cash. The first robbery police recorded was on Dec. 1 in Princeton. Eight days later, the man was 200 kilometres to the north, where he held up a Vernon financial institution. Between Dec. 19 and Jan. 21, the same suspect is believed to have held up banks in High River, Alta., Swift Current, Sask., Lethbridge, Alta., Claresholm, Alta., Merritt and Langley. RCMP have released photos of the man entering the banks he robbed and in every one, he's dressed in black, wears dark glasses and either a hoodie or a tuque. Canadian Press (Times Colonist); QMI Agency (Calgary Sun, Ottawa Sun,

London Free Press, Toronto Sun, Edmonton Sun, Kingston Whig Standard, Winnipeg Sun)

Police seize firearms
Five Red Deer residents were arrested and face more than 200 criminal charges following the police seizure of 16 firearms in the city. A variety of rifles and a couple of handguns believed to be stolen from area homes were found in two locations: in a vehicle pulled over by police in north Red Deer; and during a Jan. 23 search of a downtown Red Deer residence that's close to Central Middle School and the temporary location of Annie L. Gaetz School. "We consider this a significant seizure," said acting Insp. Chad Coles, of the Alberta Law Enforcement Response Team (ALERT), on Thursday. He believes that police diverted the guns from being used to commit crimes. "It's important to get them off the street," added Coles, who noted the trade in stolen firearms is increasing in the province and "it's a concern for law enforcement and public safety." Acting on a tip, a dozen officers from Red Deer City RCMP, K-Division and ALERT obtained a search warrant for a residence. They found a stash of weapons in the home, as well as ammunition, 28 grams of methamphetamine and other stolen property. Red Deer Advocate

Member of Bountiful community asks court for passport to shop in the U.S
One of four B.C. residents accused of polygamyrelated charges is asking a court to return her passport so she can travel to the United States. Emily Crossfield is accused along with two others of unlawfully removing a child from Canada with the intent that an offence of a sexual nature would be committed. She asked provincial court Judge Ron Webb on Thursday to have her passport returned so she can shop in the U.S. Crossfield said she has taken a herbal practitioner course at a local college and would be buying mostly herbs. Crown lawyer Tom Arbogast opposed return of her passport, telling the court the RCMP believes she is a flight risk. Crossfield, her husband Brandon Blackmore and James Oler all face the same charges, Arbogast noted. It is believed they have an "extensive network of contacts in Utah and Arizona," he told the court. Crossfield replied that she has responsibilities in Canada, adding: "I'll return." Postmedia News (The Province); Canadian Press (Times Colonist); Globe and Mail

East Hants RCMP leader hails opening of detachment
The RCMP presence in the western part of the Municipality of the District of East Hants is official and permanent. "This brings a smile to my face," Staff Sgt. Joe Marando, district commander for East Hants RCMP, said Thursday after the ribbon cutting to open the Upper Rawdon detachment, which has been operational since earlier this month. "Really happy that we had this day today and that this detachment is now open." Marando, who took over command in November, said the new detachment will have six officers and a detachment assistant. Warden Jim Smith described a "long, hard journey" for East Hants to acquire the new detachment. "I don't know how many meetings I've been to, but we pushed the boulder uphill," said Smith, adding that the idea for a new detachment had been kicking around for more than six years. Years of stops, starts and long location debates later, the detachment is a reality. The Chronicle-Herald, A8

Cop, force sued for rape in custody
There was plenty of drinking in Tasiujaq that weekend in 2011, just as there was whenever a shipment of alcohol arrived in the isolated village in Quebec's far north. The lone police officer on duty on the night of Sept. 19 had her hands full. Fresh out of police school, she had been on the job less than a month and was not even authorized to carry a sidearm. But as she apprehended a 17-year-old girl who had become heavily intoxicated, Const. Danielle Gallant made a decision that would come back to haunt her. According to court documents, she handcuffed the girl and placed her in the back of her Kativik Regional Police Force vehicle. Already in the back seat for having caused a disturbance - but not handcuffed - was Joe Kritik, who at age 24 already had four convictions for sexual assault and was listed on the national sex offender registry. As the officer made a third stop, she left the two detainees alone, and Kritik pounced on the girl. "When Constable Gallant came back to her vehicle after a short period of time, she observed Mr. Kritik with his pants down while on top of the plaintiff," a statement of claim filed by the victim states. "The plaintiff was unable to defend herself, being handcuffed in her back and unable to leave the vehicle, the doors being locked." Despite the assault, the girl was kept in a police cell overnight and was not given medical attention, the lawsuit says. Her parents were not contacted. Kritik pleaded guilty to sexually assaulting the girl in 2012 and was sentenced to 39 months in prison. A lawsuit filed last

year in Quebec Superior Court against Gallant, the Kativik Regional Police Force (KRPF) and the Kativik Regional Government is seeking $400,000 in damages for the victim, who cannot be identified. Postmedia News (Leader-Post, A7, Star Phoenix, Vancouver Sun, Edmonton Journal, Montreal Gazette, National Post)

Police budget may creep up
Toronto Police Services are proposing a 0% budget increase for 2015 but that may not last. In an appearance before the city budget committee Thursday, TPS board chairman Alok Mukherjee said the service is currently in negotiations with its officers and any increase in police compensation costs would be added directly to the budget. The rising cost of policing is becoming unsustainable for taxpayers, he said, so the board is looking at how services are delivered to control the budget. QMI Agency (Toronto Sun, 8); Toronto Star

Costs of June 4 manhunt and aftermath still being discussed
New Brunswick's minister of public safety, Stephen Horsman, says the door is certainly still open for the province to help the Codiac Regional Policing Authority with extraordinary costs incurred in Moncton last June. Sheila Lagace, a department spokeswoman, clarified the matter after media reports appeared this week suggesting otherwise. The murder of three RCMP members and wounding of two other Mounties in north end Moncton resulted in one of the largest police operations in Canadian history to capture the killer, investigate the crimes and police the tri-community while many local RCMP members were stood down for mandatory counselling and debriefings. Local constables Fabrice Gevaudan, Dave Ross and Douglas Larche were killed, and constables Darlene Goguen and Eric Dubois were wounded. Justin Bourque was given five life sentences with no chance of parole for 75 years for his crimes at the end of October. As reported in the Times & Transcript in November, how much the federal government would pay to help the Codiac Regional Policing Authority is largely set through existing contract agreements and commitments already made. Canadian Press (Telegraph-Journal, A3)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Got milk? Only the powdered kind in prison
Inmates at all of Canada's federal institutions will have access to only powdered milk as part of the government's cost-cutting efforts, officials confirmed Thursday. Phasing out fresh milk in prisons will save an estimated $3.1 million a year, Veronique Rioux, a spokeswoman for the Correctional Service of Canada, said. Powdered milk has been used for a few years in prisons in Western Canada, Rioux said. Now, prisons in Ontario, Quebec and the Atlantic region are making the transition. Laiterie Chagnon, a Waterloo, Que., dairy company, had been delivering milk to institutions in Drummondville and Cowansville for the past 10 to 15 years, sales director Jean Robidoux said. The last delivery to Drummondville was Jan. 12 and the last delivery to Cowansville is Feb. 2. The contracts brought the company about $275,000 annually. "For a small business like us, $275,000 is a lot of money. We have to get on and find new customers," he said. Robidoux said he was told the powdered milk would be shipped to the province from a supplier in Winnipeg. Francois Dumontier, spokesman for the Federation of Milk Producers of Quebec, said he found this choice strange. (…)The correctional service said all prison menus are reviewed and approved by registered dietitians and must meet appropriate nutrition standards. "The use of powdered milk is more cost-effective than the use of liquid milk and meets nutritional requirements in accordance with Canada's Food Guide," Rioux said. Postmedia News (Vancouver Sun, Canada.com, StarPhoenix, Ottawa Citizen, Leader-Post, Edmonton Journal, National Post)

Mort d'un détenu de Port-Cartier à Québec
Un détenu de l'Établissement de Port-Cartier est décédé jeudi à l'hôpital de l'Enfant-Jésus à Québec, a fait savoir Service correctionnel Canada. Sylvain Hamel était âgé de 44 ans. Il purgeait une peine de prison de 8 ans pour vols qualifiés et évasion de garde légale depuis le 25 juin 2008. La police et le coroner ont été prévenus et une enquête sera menée pour comprendre les circonstances de la mort du prisonnier, a souligné Service correctionnel Canada. Agence QMI (Journal de Montréal, Journal de Québec)

*** Second inmate dies at Drumheller Institution**
For the second time this week, an inmate has died at a southern Alberta prison. The Correctional Service of Canada says Martin Pinkus was discovered unresponsive in his cell Wednesday at Drumheller Institution. Staff tried to resuscitate the 47-year-old man and emergency services were called, but he was pronounced dead at the local health centre around noon. Pinkus had been serving time since December 1999 for seconddegree murder, aggravated assault and assault causing bodily harm. There was no immediate word on the cause of death. On Monday, Drumheller staff found a convicted murderer, Earl William Davenport, unresponsive in his cell and could not revive him. A Correctional Service spokesman says foul play is not suspected in Davenport's death. Edmonton Journal, A6, CBC News

*** 81-year-old inmate dies in Kingston, Ont., hospital**
Officials say an inmate who spent the last several decades in prison has died in a Kingston, Ont., hospital. A spokeswoman for Warkworth Institution, a medium-security facility in Campbellford, Ont., says 81-year-old James Butt died Wednesday. Assistant warden Cindy Herrington says Butt had been serving "an indeterminate sentence" for second-degree murder since 1988. His next of kin have been notified. The Correctional Service of Canada says it will look into the circumstances of his death. Canadian Press (CTV News, My Kawartha) (2015-01-29)

N'abolissez pas la liberation
Un article d'opinion déclare, « Comme souvent quand ce gouvernement parle de criminalité, ça commence par un mensonge. «Les Canadiens ne comprennent pas pourquoi les criminels les plus dangereux pourraient être libérés un jour», disait le ministre de la Justice Peter Mackay en 2013. Lundi, le leader conservateur en Chambre, Peter Van Loan, a annoncé qu'une loi serait bientôt déposée pour faire en sorte qu'une peine d'emprisonnement à perpétuité «soit juste ça: une peine à perpétuité». Le mensonge, c'est que les criminels «les plus dangereux» recouvrent la liberté. Des meurtriers obtiennent parfois une libération conditionnelle. Mais seulement s'ils ont démontré qu'ils ne sont plus dangereux. Une condamnation pour meurtre entraîne une peine automatique d'emprisonnement à vie. S'il s'agit d'un meurtre au deuxième degré (non prémédité), le juge fixe entre 10 et 25 ans le nombre d'années pendant lesquelles le délinquant n'aura pas droit à une libération conditionnelle. S'il s'agit d'un meurtre au premier degré, le meurtrier est inadmissible à la libération pendant 25 ans. Le meurtre au premier degré recouvre les meurtres prémédités, les meurtres de policiers et de gardiens de prison, les meurtres commis pendant un kidnapping ou une agression sexuelle et les meurtres commis lors d'un acte terroriste. On n'a pas encore le projet de loi, mais il semble que ce soit pour cette catégorie que la libération conditionnelle pourrait être abolie. » La Presse, A5/Front (Le Quotidien)

Life without parole is a solution without a problem
An opinion piece states, "Canada's criminal justice system faces many challenges. For example, provincial prisons contain more people who are legally innocent while awaiting trial than they do offenders who are serving prison sentences. Our sentencing structures are becoming more and more incoherent with each passing bill, such that it is becoming increasingly impossible for judges to follow a simple and almost universally accepted principle: that the sentence should be proportionate to the gravity of the offence and the degree of responsibility of the offender. We faces other challenges - economic and international ones, for example. But instead of addressing these difficult problems, Prime Minister Stephen Harper's government has picked an easy target. The Conservatives are promising to create a new sentence of "life without parole" for certain categories of people found guilty of first-degree murder. The question is "Why?" As Globe and Mail justice reporter Sean Fine pointed out this week, it's not because of crime - the homicide rate has been decreasing for decades. Contrary to recent statements by Mr. Harper, the decreases have nothing whatsoever to do with his crime policies. And the life-without-parole proposal has nothing to do with current sentencing laws. First-degree murderers get automatic life sentences. E ven if paroled - after a minimum of 25 years - they are supervised for life. Canada's parole boards are already tough on offenders. If all parole boards stopped granting full parole to those serving sentences other than life, the prison population would increase by just 2.7 per cent. And offenders on parole commit very few offences. About 150,000 adults a year are charged with violent offences, but just 16 federal parolees are convicted of such offences each year. The government's view is that some murderers should never be released, and most people would probably agree. The question is when that decision should be made: right after someone is convicted, or decades later, when the parole board can

see whether they have changed and whether the public interest is served by releasing them? The Harper government opposes policies based on the assumption that people can change." Globe and Mail, A11

*** Don't remove hope for parole**
An editorial states, "The Harper government is considering making a life sentence without parole automatic for certain crimes. While that is consistent with the Conservatives' get-tough-on-crime agenda, it is not consistent with a fair and effective justice system. The government should not take away from judges and parole boards the flexibility to examine each case on its merits. The ability to make decisions based on humaneness and common sense should not be removed from the justice system. The Conservative government plans to introduce legislation that would make a life sentence without parole automatic for killers of police officers and jail guards, as well as anyone who kills during a kidnapping, terrorist act or sexual assault. It could apply to other particularly brutal killings, if a judge so decides. "Canadians do not understand why the most dangerous criminals would ever be released from prison," Gov.-Gen. David Johnston said in the speech from the throne in October. "For them, our government will change the law so that a life sentence means a sentence for life." First-and second-degree murder convictions in Canada already automatically result in life sentences, but with the possibility of parole after 25 years in the case of firstdegree murder. Minimum parole eligibility for seconddegree murder convictions is 10 years. This isn't a plea to go soft on killers. While convictions are based on guilt being proved beyond reasonable doubt, those who have murdered should prove to a parole board, beyond any doubt at all, that they can be safely released. While one of the aims of the justice system should be rehabilitation, it's a distant second to public safety." Times Colonist, A11

*** Life, no parole**
A letter to the editor states, "Re We Don't Need Life Without Parole (editorial, Jan. 28): First, the Harper government implemented a series of amendments to the Criminal Code imposing mandatory minimum sentences. It appeared that they didn't trust the discretion of judges, many of whom they appointed. Now they want to take away the discretion of the federally appointed National Parole Board to determine whether an offender serving a life sentence for firstdegree murder may be released on parole after having served 25 years in the penitentiary. Don't they trust anybody?" Globe and Mail, A10

*** How Pierre Poilievre is keeping me safe from bad people**
An opinion piece states, "A few days ago, I opened up my mailbox to find a householder pamphlet from my MP, Pierre Poilievre. Normally, I do my part for the environment and chuck these things straight into the blue box - but this one caught my eye. In big, bold letters, it read, "What's being done to help keep my family safe?" Good question. Poilievre's probably the least-qualified guy on the planet to answer it. Remember what he had to say in the immediate wake of the Boston Marathon bombing? "The root cause of terrorism is terrorists." Brilliant. In other news, scientists now say the root cause of rain is water. Only Poilievre could make his boss, Stephen "Let's Not Commit Sociology" Harper, look thoughtful. (…)There's nothing in the bill that does anything to enhance public safety - but it does make for good headlines. If the Conservatives were truly interested in the threat posed by mentally ill offenders, they'd begin to properly fund mental health services in federal prisons for offenders who will soon be released into the community. (…)There was no third option - so I decided to add one: "None of the above. I *do* want the federal government to protect my family by doing what makes actually makes us safe, not what makes us feel safe. I want the government to fund things like restorative justice programs that have been shown to reduce the risk of high-risk sex offenders re-offending, to invest in preparing offenders to return to my community. I am worried about politicians with simple solutions to complex problems who want to exploit my desire to protect my family and my fear that something bad may happen to them.'" iPolitics

*** Abusive segregation of inmates**
An opinion piece states, "Edward Snowshoe was a 24-year-old prisoner at Edmonton's maxiumum security prison when he hanged himself. He had been at Stony Mountain Institution first and then was transferred. His time behind bars included 162 days in segregation; 134 of them at Stony. The reason? He threatened guards with a juice box. Mr. Snowshoe had also repeatedly attempted suicide, and he was described as paranoid and vulnerable by staff. Mr. Snowshoe fits the profile of many dumped into solitary confinement in Canada's federal prisons. There is a high rate of mental illness among prisoners. Prisons have a much higher rate of suicides than the general population, and half occur in segregation units. Mr.

Snowshoe's story is reminiscent of that of New Brunswick teenager Ashley Smith, who killed herself after more than 1,000 days in segregation. Their sad odysseys have triggered a rising demand for major reform of how Canada uses segregation." Brandon Sun

"On ne peut pas continuer avec ces dépenses"
La maison de transition qui accueille un seul prisonnier sur la Côte-Nord est un "éléphant blanc", estime l'opposition officielle, qui exige un plan d'action. "Dans le contexte d'austérité, on ne peut pas continuer avec ces dépenses. La ministre Lise Thériault doit présenter un plan d'action pour attirer davantage de prisonniers ou carrément fermer l'établissement", croit Pascal Bérubé, porte-parole péquiste en matière de sécurité publique. D'une capacité de 20 lits, le centre Kapatakan Gilles Jourdain, situé sur la réserve innue de Mani-Utenam, n'a toutefois qu'un seul "client". Le centre, bâti en 2012 pour 1,9 M$, coûte 680 000 $ en frais annuels. Le centre transitoire accueille les "adultes innus et les autres membres des Premières Nations" en processus de libération conditionnelle et offre des "services diversifiés et adaptés selon les valeurs et les traditions des peuples autochtones." Journal de Montréal, 20 (Journal de Québec)

Un ex-bras droit de Rizzuto demande sa libération
Un criminel notoire au parcours tumultueux, ancien associé du parrain de la mafia Vito Rizzuto, se bat pour obtenir sa libération conditionnelle, dans le but, assure-t-il, de mener une vie rangée et honnête. D'emblée, le nom de Christian Deschenes ne dit peut-être rien aux lecteurs, mais il a été l'un des acteurs majeurs de la plus importante tentative d'importation de cocaïne par voie aérienne de l'histoire du Canada. C'est en effet lui et ses hommes qui, le matin du 18 novembre 1992, ont quitté trop tôt la piste de Casey, laissant en plan le pilote de brousse Raymond Boulanger et les 4000 kg de cocaïne qu'il transportait. Au fil des ans, Deschenes a gravi les échelons du crime organisé, si bien qu'on le retrouvait à la droite de Vito Rizzuto. A la fin des années 80, il a été arrêté pour importation de 14 tonnes de haschisch. C'est lui qui était responsable du transport. «Si un camion ne s'était pas renversé, je n'aurais jamais été pris», analyse-t-il. En juillet 2001, il a été de nouveau appréhendé pour avoir comploté l'enlèvement de lieutenants de la mafia et le meurtre de Vito Rizzuto, après que l'un de ses complices eut éventé le projet et fut devenu un agent source de la police. Les enquêteurs ont saisi un véritable arsenal dans cette sordide affaire. Tous ces crimes commis alors qu'il était en libération conditionnelle font que Deschenes purge une peine accumulée de 45 ans de pénitencier. Aujourd'hui, il en a assez, dit-il, et jure qu'il n'a plus de liens avec le crime organisé et qu'il veut tourner la page. La Presse, A6

* **Day passes granted to paraplegic's killer**
Nearly 15 years removed from the "crackhead mode" that prompted him to choke, stab and then drown a paraplegic family friend who refused to lend him $10, a former Calgary resident will take his first steps toward freedom with day passes from prison. The Parole Board of Canada granted Tyler Preston Agate's application for escorted temporary absences, which will allow him to leave Bowden Institution for community service outings under the supervision of a prison guard. Agate, who is in his mid-40s, is serving a life sentence for killing Douglas Arthur Klein in the victim's southwest Calgary home in July 2000. Calgary Herald, A11

* **Parole board denies passes for man who killed stepsister**
Blacking out from alcohol and pills may have prevented Nathan Pelletier from remembering how he killed his 12-year-old stepsister in 1998, but the Parole Board of Canada said his own lack of insight is keeping him from explaining why he did it. For that reason, the parole board rejected Pelletier's application Thursday for unescorted temporary passes from prison to visit his father, saying he poses too much of a risk to be in the community without the presence of a prison guard. "You have had a long time to think about it," said parole board member Ron Kuban, who delivered the two-member panel's decision following a hearing at Bowden Institution in central Alberta. "You need to understand ... what was going on inside you and in your environment so you don't repeat it." Calgary Herald, A6

* **Appeal denied for convicted murderer in cousin's death**
A man found guilty of first-degree murder in the 2009 death of his 16-year-old cousin has had the appeal of his conviction dismissed by the New Brunswick Court of Appeal. Curtis Bonnell asked the court to overturn the conviction and order a new trial after he was sentenced to life in prison with no parole eligibility for 25 years in the death of Hilary Bonnell. Defence lawyer Peter Corey argued last April that

the trial judge in his instructions to the jury should have related the evidence they heard to a possible finding of manslaughter. Corey also said the trial judge erred by allowing text messages Hilary Bonnell sent before she died to be entered as evidence. The jury was shown two text messages that she sent to Haylie Bonnell, the accused's sister, on the morning she disappeared. They read, "Please answer me I'm scared," and "OMF text me I'm scared." Corey argued there was nothing in the messages to identify who she was with or what scared her. In a written decision released Thursday, the court dismissed the argument. Telegraph-Journal, A3 (Times & Transcript)

* **Suspect from Guelph asks for adjournment**
The suspect in an early morning police chase that ended with a crash at Reversing Falls Bridge on Jan. 7 was back in court on Thursday morning. Michael Samuel French, 28, of Guelph, Ont., was to set a trial date on a charge of failing to stop his vehicle in attempt to evade a police officer, but instead he requested an adjournment of one week. French said he wanted to talk to his family, "and then I'll plead," he said from the prisoner's dock wearing the same Roots hoodie he was wearing during his first appearance. At the time of his arrest, police said French was wanted on a Canada-wide warrant. His parole has since been revoked for the unrelated matter, and he's now being held at Atlantic Institution in Renous. French will return to set a trial date on Feb. 5. Telegraph-Journal, B2

* **Men charged with more robberies after they were sentenced**
Two men who were handed stiff sentences for an armed robbery are facing additional 2013 robbery charges that weren't dealt with when they were sentenced. Eric Douglas Squires appeared in provincial court in St. John's Thursday, while William Peter Edwards'case was called Wednesday. They've been charged with three counts each of armed robbery, having their faces masked, possessing a weapon dangerous to the public and breaching probation. The charges stem from robberies that happened in October 2013 at an Ultramar gas station, a Marie's Mini Mart and an Orange Store. They were laid Wednesday, the day after Squires was sentenced to 5 1/2 years in prison in Newfoundland Supreme Court. Edwards was sentenced to three years in jail last year after he pleaded guilty. Both were sentenced in connection with an armed robbery at a Marie's Mini Mart store on Elizabeth Avenue in October 2013. The men will have their cases called in provincial court again Feb. 11 to deal with the new charges. The Telegram, A3

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

An appeal to Facebook, a jail term cut short
Call it trial by Facebook. When justice wasn't served inside a Sarnia courtroom this month, an unconventional appeal was spontaneously mounted in a much less hallowed hall: an online comment thread. On Jan. 15, James Trevor Munroe, 23, was slapped with a year in jail after pleading guilty to possessing just over three ounces of marijuana for trafficking, a relatively small amount that typically garners a 30- or 60-day sentence. But the federal prosecutor, Munroe's lawyer and even the judge, who called the sentence "extremely harsh," said their hands were tied: Canada's new mandatory minimum sentencing laws dictated the penalty must be one year in jail. "This is mandatory. Not much I can do," the Sarnia Observer quoted Munroe saying afterwards. But within days, a ragtag team of Toronto lawyers and prosecutors serendipitously assembled on Facebook, at first decrying the steep penalty before discovering the amount of marijuana did not even qualify for mandatory minimum sentencing. After the mistake was brought to the attention of a federal prosecutor in charge of Ontario's criminal appeals unit - again on Facebook - Munroe was released on bail, just over a week into his year-long stint. Toronto Star, A1

Leniency on leases proposed for victims of domestic violence
Victims of family violence will be better equipped to protect themselves from debt if proposed changes to the territory's Residential Tenancies Act pass. Bill 42, which is currently being reviewed by a standing committee, includes a provision that would allow a victim of physical or psychological abuse at the hands of someone who is sharing a lease with them to cancel their tenancy agreement without facing a financial penalty. "It's just an additional avenue for safety once a person has been assaulted or family violence has

been acted upon them," said Lorraine Phaneuf, executive director of the Status of Women Council of NWT, which supports the amendments to the act. The Protection Against Family Violence Act already provides significant protection to victims of domestic violence, including a provision that allows them to take over a lease from an abusive partner, according to Mark Aitken, assistant deputy minister for the attorney general's branch of the Department of Justice. Aitken said the proposed amendments in the Residential Tenancies Act provide a companion to existing legislation by allowing victims the opportunity to get out of tenancy agreements that may cease to be affordable. Yellowknifer

*** Exposure to violence increases PTSD risk**

An Ottawa psychiatrist who developed post-traumatic stress disorder after watching videos of sex killer Russell Williams assaulting two women is warning that members of the public are increasingly vulnerable to emotional harm from exposure to graphic video. In a digital age, when disturbing video images are just a mouse-click away and nearly everyone has a video camera on their smartphone, members of the public risk developing vicarious trauma or the more serious PTSD from exposure, said Dr. John Bradford, a renowned forensic psychiatrist and an Order of Canada recipient. His concerns come at a time when ISIL has been posting videos of beheadings and other graphic video imagery is readily available online. "There is clearly significant risk with exposure to graphic video such as beheadings," said Bradford. A former skeptic, Bradford was diagnosed with acute, chronic PTSD after working on the Williams case, in which the evidence included high-quality, graphic videos. Williams, a disgraced former colonel in the armed forces, was sentenced to life behind bars in 2010 after pleading guilty to the murder of the two women, other sexual assaults and a series of break-ins in Ottawa involving women's lingerie. Bradford, who has spent a career studying the kind of evidence that many would find disturbing, said it never bothered him until he was exposed to high-quality video. He had earlier suffered similar symptoms after watching video from the Paul Bernardo trial. For months after working on the Bernardo case, Bradford was unable to shake certain images and sounds from his head, he said. That eventually faded, but after watching video from the Williams case in 2009, Bradford was hit with an "emotional storm" that spiralled into severe depression, personality changes and suicidal thoughts until he received treatment and began taking medication. Ottawa Citizen, A7

*** Manitoba 'one of worst places for natives'**

Federal government documents show Manitoba is one of the worst places for First Nations people to live in Canada. Internal reports from Aboriginal Affairs and Northern Development show Manitoba natives are more likely to grow up in poverty, drop out of school, live off social assistance in dilapidated housing and suffer family violence. Their life expectancy is also eight years shorter than that of other Manitobans. The 10 regional updates spanning 2012 to 2014 lay out the poor living conditions on Manitoba reserves but offer little concrete action on the part of the government. Canadian Press (The Daily Gleaner, B1)

*** Hate mail highlights Winnipeg's racism**

Inside a card decorated in a field of flowers and trees, Thelma Favel - the great-aunt of slain aboriginal teenager Tina Fontaine - received a seething message of hate: "You guys are nothing but a bunch of drunken Indians." The handwritten, unsigned note, delivered Wednesday to her rural Manitoba home, is an anomaly among the hundreds of letters of support and prayer she has received since Tina's lifeless body was pulled from Winnipeg's Red River in August. But the note is piercing, going on to allege that 15-year-old Tina was not a nice person, got drunk in back alleys and was following in her dead father's footsteps. Her father was beaten to death in 2011. "This is not right what they did," Ms. Favel said of the card after relaying its contents over the phone Thursday. "All the hatred seems to go to the First Nations people," she added. "I know the truth. I know Tina and they didn't." Although the card is an aberration in Ms. Favel's pile of condolences and well wishes, its sentiment is not incongruous with comments and behaviour that Ms. Favel and other indigenous people have encountered in Canada. Last week, Maclean's magazine branded Manitoba's capital as the nation's most racist city. Winnipeg's mayor and other community leaders responded in an unexpected address. The Globe and Mail, A5

*** RCMP report fewer crimes**

The final RCMP statistics for 2014 show an overall decline in crime in the city, with 16,940 complaints reported, down from 18,176 in 2013. RCMP Cpl. Donnie Duplissea presented the report to council Monday, adding that while crime has decreased over all, the last few months of the year were busy for

the detachment. "As a man who works in uniform, policing Yellowknife was pretty colourful," Duplissea said, giving as an example, the recent standoff at the Northern Lites Motel. Assaults of all kinds dropped to 853 reports, down from 1,254 last year, as did break-and-enters, of which 98 were reported, down from 172 in 2013. "It is striking, the difference between this year and last," said Coun. Adrian Bell. "Is there anything we can draw from this?" One possible explanation Duplissea gave for the general decrease in crime was the increase in the number of people jailed, keeping offenders off the street. In 2014, 6,034 prisoners were reported, up from 5,450. As well as imprisonment, Duplissea said the fully-staffed detachment, assistance of municipal enforcement and enhanced patrols could also be the reason. He said it could "also just be dumb luck." There were some increases in crime reported, including motor vehicle theft, which rose to 84 from 71. Mischief, including public intoxication, also saw a steep increase to 5,393 occurrences in 2014, up from 4,055 the previous year. Yellowknifer

PUBLIC SERVICE / FONCTION PUBLIQUE

Consultants brought in to screen FOI requests

The federal government has spent about $57 million on outside consultants over the past nine years to help decide which government records Canadians are allowed to obtain. About 60 per cent of that spending, to handle what are called "access to information" requests, have occurred during the last four years of Conservative rule. The spending is above and beyond that allocated to full-time staffwho handle such requests in each department. The spending figures are contained in an order paper question from NDP MP Charlie Angus, although the data are not complete. Some agencies and Crown corporations, such as the CBC and the Public Service Commission, didn't provide numbers in the response, instead directing recipients to the annual reports each files on access to information spending. Under the access to information regime, Canadians can request federal government records and information - which their taxes pay for - although the law allows some information to be withheld, such as data that could compromise national security or breach someone's privacy. "This is extremely sensitive information," Angus said. "You need specialists in your department to handle this. You don't ... put an ad in the paper. We don't know who is doing the review." Ottawa Citizen, A10

OTHER / AUTRE

Wife of Saudi blogger asks for Harper's help

The wife of the imprisoned Saudi blogger Raif Badawi says her husband can't endure another flogging. Ensaf Haidar, now a refugee living in Quebec, joined an all-party coalition of MPs on Parliament Hill on Thursday urging Prime Minister Stephen Harper to intervene personally with the Saudis. They want the prime minister to push for the release of Badawi, who is set to receive 50 more lashes on Friday. It is part of Badawi's ongoing punishment of 1,000 lashes, a 10-year prison sentence and heavy fines for criticizing Saudi clerics on a blog he founded. The 32-year-old father of three was lashed 50 times on Jan. 9, but his second scheduled beating was postponed last week for medical reasons. "Raif's health condition is getting worse and worse," Haidar said through a translator during a press conference on Parliament Hill. She said that was the conclusion of several doctors who examined her husband in the last week. "I am very concerned about him. It is impossible for a human being to be able to withstand 50 lashes weekly." Liberal MP Irwin Cotler, a long-time human rights advocate, said Saudi Arabia must live up to its international obligations as signatory to the United Nations convention banning torture. Canadian Press (Cape Breton Post, Montreal Gazette, The Guardian, Whitehorse Daily Star, Times Colonist, Telegraph-Journal, Times & Transcript, Daily Gleaner, Vancouver Sun, The Telegram), * Globe and Mail, * Presse canadienne (Voix de l'Est, La Presse, La Tribune, Le Droit, Le Soleil)

INTERNATIONAL / INTERNATIONAL

*** Canada to maintain pressure on Ebola**

The Ebola treatment centre where Canada's military medics are working is now nearly empty, but Canada has no immediate plans to scale back its mission to Sierra Leone in response to the steep decline in cases. Lieutenant-Colonel Gary O'Neil, the task-force commander for Canada's deployment to the Ebola zone, said Thursday that just one suspected Ebola patient was at the British-run Kerry Town Treatment Unit, where 37 Canadian military health-care workers and support staff have been on the ground since December. More patients were en route to the centre on Thursday night, he added. The unit has treated 36 confirmed and suspected Ebola patients since the Canadians arrived. Globe and Mail, A8

* **Ebola - L'épidémie ralentit dans les pays les plus touché - Moins de 100 nouveaux cas ont été recensés en une semaine, une première depuis juin**

Le nombre de contaminations hebdomadaires par le virus Ebola est passé sous le cap de 100 pour la première fois depuis sept mois, signe que l'épidémie ralentit, mais elle " n'est pas encore endiguée ", a averti jeudi l'ONU. L'Organisation mondiale de la santé (OMS) a fait état jeudi d'un " ralentissement " de l'épidémie dans les trois pays les plus touchés par la fièvre hémorragique -- Guinée, Liberia, Sierra Leone -- où, pour la première fois depuis fin juin 2014, moins de 100 nouveaux cas au total ont été recensés en une semaine. Cette baisse est particulièrement marquée au Liberia, qui n'a rapporté que quatre nouveaux cas dans la semaine du 25 janvier (contre huit la semaine précédente), et en Sierra Leone, qui a recensé 65 nouveaux cas (contre 117). En Guinée, le nombre de contaminations, qui baissait jusqu'ici, est resté stable dans la même semaine, avec 30 nouveaux cas contre 20 la semaine précédente. Depuis son apparition en décembre 2013 en Afrique de l'Ouest, l'épidémie de fièvre hémorragique a fait au moins 8810 morts, essentiellement dans ces trois pays, et contaminé plus de 22 000 personnes, selon l'OMS. " La réponse à l'épidémie d'Ebola est actuellement entrée dans une deuxième phase, mettant l'accent non plus sur le ralentissement, mais sur la fin de l'épidémie ", a expliqué l'OMS, qui avait averti le 23 janvier que la situation restait néanmoins " extrêmement préoccupante " et qu'une recrudescence de l'épidémie ne pouvait être exclue. Le Devoir, A4

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
February 25, 2015 / le 25 février 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Tories move to limit study of terror bill
The Conservatives are seeking to limit testimony on their wide-ranging terrorism bill to just four days, sources say, with Prime Minister Stephen Harper urging MPs to pass the bill "as quickly as possible." The parliamentary committee studying Bill C-51 met for several hours behind closed doors Tuesday to discuss potential witnesses and schedule meetings. Because the discussion was held in secret, MPs are prohibited from speaking publicly about the debate. But several sources told the Star the government wants only three meetings to hear expert witnesses, plus one appearance from **Public Safety Minister Steven Blane**y and Justice Minister Peter MacKay. That would amount to only four days to study the most dramatic changes to Canada's security legislation since 2001. No decisions were made on Tuesday, and Blaney's office said it's up to the committee - on which the government enjoys a majority - to determine how many meetings they'll hold. In the House of Commons, NDP Leader Thomas Mulcair demanded that the bill be given a full study. "Ramming C-51 through without improved oversight is reckless," Mulcair said, urging the government to listen to human rights and security experts. Harper dismissed Mulcair's criticisms as "ridiculous" and argued the measures have the support of the majority of the Canadin public. "The bill is before committee and I would urge the committee to study this bill as quickly as possible in order to ensure the adoption of these measures to ensure the security and safety of Canadians," Harper told the House. The Conservatives introduced Bill C-51 in January, suggesting the Canadian Security Intelligence Service needs expanded powers to combat terrorist threats to Canada. Toronto Star, A1 (Globe and Mail); Ottawa Citizen; La Presse (Le Quotidien, La Tribune, La Voix de l'Est)

Leader's words should strengthen, not scare, the nation

An opinion piece states, "A new catchphrase is spreading through the rhetoric of Stephen Harper and his ministers. It is only four words - they hate our values - but it packs an emotional wallop. The prime minister road-tested it on an audience in Richmond Hill in January. "Canadians are targeted by jihadi terrorists for no other reason than that we are Canadians," he warned. "They hate our society and the values it represents." He used it in a different context in Quebec City 10 days ago. This time, he lashed out at employees of Radio-Canada. "I remain convinced that Quebecers are not leftists, contrary to the image conveyed by some media or the opposition parties," he said. "I understand that there are many at Radio-Canada who hate these values but I think that these values are the true values of a large percentage of Quebecers." **Public Safety Minister Steven Blaney** echoed the mantra as he headed to an international security summit in Washington last week. "***Canadians are being targeted by jihadi terrorists simply because these terrorists hate our society and the values it represents***." In some ways this epithet is like previous Tory terms: soft on crime, Taliban sympathizer, defender of child pornography. It is simple, spiteful and calculated to whip up strong feelings." Toronto Star, A13

La guerre, yes sir
Un article d'opinion déclare, "Henri Bourassa doit se retourner dans sa tombe. Les Québécois, dit un récent sondage, sont à 60 % favorables à la mission en Irak. De tout temps, les Québécois se sont farouchement opposés aux expéditions militaires canadiennes outre-mer. A la toute première excursion, en 1899, au moment de la guerre des Boers, pourfendue avec ardeur par Bourassa, à la conscription en 1917 et encore en 1944, et jusqu'à la guerre en Afghanistan en 2001. La supposée tradition pacifiste du Québec vient d'en prendre pour son rhume. Pour la première fois depuis longtemps, Québécois et Canadiens se retrouvent sur la même longueur d'onde. Et Jean-François Lisée qui croyait le fossé entre les deux solitudes désormais infranchissable... Ah, niqab, quand tu nous tiens ! Ou devrais-je dire, nous étouffes ? [...] Qui sont parfois bien méchants, bien sûr, mais quel rebond quand même ! Quelle habileté pour l'amalgame dont nous mettait en garde François Hollande à la suite des attentats à Charlie Hebdo. Le ministre Jason Kenney qui, hier encore, s'en prenait au projet québécois d'interdiction des signes religieux, aujourd'hui retourne sa veste en promettant de porter en appel la décision permettant à une musulmane de prêter serment et de porter un niqab en même temps. **Steven Blaney**, lui, ne rate pas une occasion de brandir la " ***menace islamique*** " tout en gardant secrète la vidéo trouvée chez Michael Zehaf-Bibeau, responsable de l'attentat à Ottawa. La vidéo devait fournir une preuve de plus du danger qui nous guette, mais curieusement, on n'en entend plus parler." Le Devoir, A7

*** Le terrorisme et le «gros bon sens»**
Un article d'opinion déclare, « Jean Leclair Professeur titulaire à la Faculté de droit, Université de Montréal Une majorité de Québécois, à l'instar d'une majorité de Canadiens, se réjouit à l'idée du renforcement éventuel des pouvoirs policiers destinés à contrer les «menaces à la sécurité du Canada», sans trop se soucier de la nature ou de l'étendue de ces pouvoirs. Les politiciens, quant à eux, font dire au projet de loi C-51 ce qu'il ne dit pas (Mulcair), mentent (Kenney), taisent et dissimulent ce qu'il dit effectivement (**Blaney** et Harper) ou encore préfèrent reconnaître ses lacunes tout en promettant toutefois de l'approuver (Trudeau). En outre, tout argument un tant soit peu rationnel en défaveur du projet de loi est immédiatement associé par le gouvernement à une manifestation de poltronnerie. Le «gros bon sens» triomphe de tout. Tout cela dans un contexte où le débat démocratique sera malheureusement presque impossible, puisque le projet de loi ne fera pas l'objet d'une étude circonstanciée, étant donné que, quoi qu'il arrive, le PLC appuiera le PC, déjà majoritaire en chambre. Il faut bien admettre que quand la population elle-même s'enthousiasme pour la répression, les politiciens pusillanimes trouvent peu d'intérêt à s'y opposer et ceux qui ont le courage de le faire risquent gros. A quel endroit pourra-t-on alors exiger du gouvernement qu'il fasse la démonstration rationnelle de la pertinence, de l'urgence, et du caractère mesuré de son intervention? Devant les tribunaux, ces assassins de la démocratie - aux dires de plusieurs -, ces censeurs du «gros bon sens.» La Presse, A17

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Production d'anticorps contre l'Ebola à Québec**
Medicago, une société de biotechnologie implantée à Québec, vient de décrocher un contrat pour la production d'anticorps destinés à lutter contre le virus Ebola. « Nous sommes ravis de contribuer aux

efforts internationaux contre le virus Ebola. Notre but est d'améliorer la capacité mondiale de production de traitements. Nous travaillons depuis plusieurs mois déjà sur Ebola et la fabrication d'anticorps », signale le président et chef de la direction de Medicago, Andy Sheldon. Journal de Québec, 18 (Journal de Montréal); Le Soleil; Cape Breton Post

*** Rail safety rules still don't go far enough**
Even with rail safety a priority for Ottawa, two reports into train derailments by the Transportation Safety Board this week suggest the new standards still aren't high enough. The TSB said Tuesday that its investigation found numerous rail fractures and undetected defects led to a fiery train wreck west of Edmonton in October 2013, a day after it reported a derailment and fire in northern Ontario last week revealed flaws with supposedly upgraded tanker cars. The unsettling reports came just days after federal Transport Minister Lisa Raitt introduced the third tranche of legislation to bolster rail safety in Canada since the deadly crash of a train carrying crude oil at Lac-Megantic in eastern Quebec in July 2013. A series of spectacular derailments in North America have coincided with a surge in crude oil moving by train in Canada and the United States in recent years and raised public concern over the capacity of an aging rail system to safely handle large volumes of dangerous goods. The Lac-Megantic crash killed 47 people. The TSB said last week's derailment "demonstrates the inadequacy" of the new rules. Any confidence that might have been inspired by Ottawa's most recent announcement on enhancing rail safety was quickly undone by the facts on the ground revealed by the TSB. Calgary Herald, D1

*** La Cour supérieure suspend le jugement en recours collectif**
La Montreal, Maine & Atlantic (MMA), avec l'accord du contrôleur au dossier ainsi que les avocats des victimes, ont obtenu hier une ordonnance visant à retarder le jugement dans le dossier du recours collectif de la tragédie de Lac-Mégantic. Cette ordonnance permettra à MMA de compléter son plan d'arrangement avec ses créanciers ainsi que la constitution d'un fonds d'indemnisation pour les victimes qui pourrait atteindre près de 500 M$ US, selon certaines sources. Hier, le juge Gaétan Dumas de la Cour supérieure a émis l'ordonnance demandée par la MMA, ce qui a pour effet de suspendre le prononcé du jugement en autorisation de recours collectif que devait prononcer son collègue Martin Bureau. Les parties opposées à cette requête en suspension de jugement avaient jusqu'à midi hier pour manifester leur opposition. L'ordonnance du juge Dumas s'étend jusqu'au 20 mars. D'ici là, la MMA et ses représentants poursuivront leurs démarches auprès des compagnies tiers qui n'ont pas encore manifesté leur intention de contribuer au fonds d'indemnisation. La Tribune, 38

*** Fake quake tests local response team**
The fake earthquake hit just outside of Windsor around 12:30 a.m. on Tuesday, creating chaos throughout the region. Imagine the quake, registering at 6.5 on the Richter scale, knocking out power to thousands of homes and toppled buildings. The city's hospitals are running on backup generators and the integrity of the Ambassador Bridge is questionable. The majority of residents no longer have Internet and cellular phone connections. It's a disaster like the city has never seen and, hopefully, never will, said fire prevention officer John Lee, who hosted a news conference at the Windsor Public Library. The emergency simulation brings together a host of emergency responders, including the province's Heavy Urban Search and Rescue Team, as all groups update plans for dealing with such a disaster. The scenario will play out over multiple days before wrapping up on Thursday. Windsor Star, A2

*** Emergency response tested with 'disaster' - Simulation will be largest and most complex conducted in the province**
Alberta's emergency response is being tested this week in a mock disaster exercise to rescue civilians trapped in a collapsed building. The test - simulating the collapse of a mall in Elliot Lake, Ont., - will be the largest and most complex conducted in the province, according to Shane Schreiber, director of Alberta's Emergency Management Agency (AEMA). "It's important for us to set the bar high so that Albertans know that we're ready to respond," he said. "Exercises like the one we're conducting over the next three days are critical to ensuring Alberta, its communities and its government are well prepared for future emergencies." Calgary Herald, A7; Edmonton Sun

*** Pas d'autres Lac-Mégantic**

Un éditorial dit «Il va falloir faire mieux, beaucoup mieux pour que le transport ferroviaire devienne vraiment sécuritaire et réponde aux attentes légitimes de la population nord-américaine. Deux déraillements majeurs survenus coup sur coup dans le nord de l'Ontario et en Virginie-Occidentale il y a quelques jours démontrent qu'un autre Lac-Mégantic demeure une trop forte probabilité pour ne pas exiger un nouveau resserrement des règles pour le transport de produits dangereux. Il y a eu un bon premier pas de la part du gouvernement fédéral à la suite de la tragédie survenue au Québec en juillet 2013. L'ajout d'un deuxième employé pour accompagner les convois de matières dangereuses, la limitation de vitesse des trains à risque et une sécurité accrue autour des trains laissés en attente allaient de soi. Évidemment, la décision la plus importante était celle d'interdire, dans le cas des matières inflammables, l'utilisation des wagons trop fragiles devenus bombes incendiaires au coeur de la ville estrienne. Malheureusement, le remplacement de ces DOT-111 par des CPC-1232 au revêtement d'acier plus épais et comportant des caissons pour protéger les valves n'a nullement empêché la déflagration dans les deux nouveaux cas évoqués ci-dessus. Heureusement, cette fois, il n'y a pas eu de victimes. Mais qui peut être rassuré, sachant que quelque 140 000 wagons-citernes transportant du pétrole brut devraient circuler sur les rails du pays cette année? En 2009, il y en avait 500... » Le Soleil, 24

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Mysterious tunnel eyed with caution

"There's no criminal offence for digging a hole," Toronto's Deputy Police Chief Mark Saunders told a packed news conference Tuesday morning. That 10-metre hole - tunnel, bunker, call it what you will - dug apparently by hand near a venue for this summer's Pan Am Games is getting international attention at a time when the public is jittery with repeated terror warnings. But there's no indication of terrorism. Or drug operations. Or a smuggling ring. If there was some nefarious purpose suspected, police aren't saying. Saunders did indicate that certain items found in the bunker were held back so that if anyone came forward, police would be able to verify their claims. And there was evidence of people eating, drinking and recently spending time in the bunker, so perhaps they have DNA - should that matter. The most intriguing detail released Tuesday was the discovery of a rosary and Remembrance Day poppy. "This was found inside the actual tunnel itself and it was nailed on the wall," Saunders said holding up a large photo of the poppy and rosary, sparking a cacophony of camera shutters... Reports stated that the case was referred to the national security agencies, and sources said both the RCMP and CSIS were briefed on the case. But that is standard, given the location and mysterious nature of the tunnel, and no alarm bells went off in either agency, nor were formal investigations launched, which means unless more evidence comes to light following Tuesday's news conference - as police hope - this is not the #TerrorTunnel that was trending on Twitter. Waterloo Record, A1 (Hamilton Spectator, A1)

RCMP red-flagged Almalki after 9/11, despite doubts

Newly released documents show that an RCMP national security team described Ottawa's Abdullah Almalki as an imminent threat and an "important member" of al-Qaida to foreign agencies even as investigators expressed serious doubts about the veracity of those claims. Other documents reveal that the RCMP team, despite its misgivings, shared details of Almalki's international travel plans with the U.S. Central Intelligence Agency in December 2001, during the highly charged aftermath of 9/11. "The available information clearly confirms the intent of Canadian investigators in sharing the travel information was, if possible, to arrange for or assist in his detention before he could return to Canada," Almalki's lawyers charge in a written submission to the Federal Court of Canada. The new documents have been released to Almalki's legal team as part of the disclosure process in his $100-million civil suit against federal officials for his detention and torture in Syria. Almalki, a Carleton University graduate and father of six, spent 22 months in Syrian custody after his arrest at the Damascus airport in May 2002. He has never been charged with a crime in Canada. A federal inquiry has already found that Almalki was inaccurately labelled by the RCMP in letters to foreign intelligence agencies. The new documents disclosed by the government suggest that RCMP officers, in labelling Almalki an imminent threat, also ignored evidence to the contrary. Postmedia News (Ottawa Citizen, A1, Edmonton Journal)

*** Crainte d'acte terroriste d'un Montréalais, selon la GRC**

Bien qu'aucune accusation criminelle ne pèse contre lui, Merouane Ghalmi, 22 ans, pourrait ainsi devenir le premier Québécois à se voir imposer des conditions spéciales par le tribunal, à la suite d'une enquête de la GRC en matière de sécurité nationale. Ni la Couronne ni la GRC n'ont voulu révéler le moindre détail au sujet de ce dossier. La Couronne cherche à obtenir l'émission d'un mandat de paix à l'endroit du jeune homme, selon un document judiciaire signé lundi par le juge Louis A. Legault et dont Le Journal a obtenu copie. Merouane Ghalmi devrait alors s'engager à garder la paix et à ne pas commettre d'infraction criminelle pendant un an. «C'est arrivé à moins d'une dizaine de reprises ailleurs au pays qu'on obtienne une telle ordonnance pour des motifs liés au terrorisme. Mais ce serait un précédent au Québec», a mentionné Daniel Brien, porte-parole du Service des poursuites fédérales du Canada.
De plus, le tribunal pourrait ordonner à Ghalmi de respecter des conditions, telle l'interdiction de communiquer avec certaines personnes et de posséder des armes ou explosifs. «C'est l'un des outils mis à la disposition de la GRC pour tenter d'éviter des atrocités comme celle survenue à Saint-Jean-sur-Richelieu, le 20 octobre dernier», a fait remarquer Pierre-Yves Bourduas, l'ex-commandant de la GRC au Québec. L'aspirant djihadiste Martin «Ahmad» Rouleau avait alors happé deux militaires avec sa voiture, causant la mort du caporal Patrice Vincent. L'ancien haut gradé de la police fédérale a rappelé qu'une telle mesure judiciaire aurait pu être prise à l'endroit de Rouleau, avant qu'il ne passe aux actes. Journal de Québec.com (Journal de Montréal)

Made here?
An inquest into the attack on an Algerian gas plant, set to release its findings Thursday, has painted a chilling picture of two young terrorists from London. The inquest also sends a clear message to this city and the rest of the country: the terrorism was born here. Xristos Katsiroubas and Ali Medlej met in London and "both were introduced to a radical form of Sunni Islam through associates in the community," concludes a British police counterterrorism unit, based in part on an RCMP investigation, quoted at the inquest. Katsiroubas became a leader of the attack and the main negotiator to the outside world, pleading for a peaceful solution and perhaps saving some hostages, but threatening violence, perhaps making a list of those to kill, and ending communications with a prophetic threat: "You need to stop the Algerians so we can deal with this or everybody's going to be dead, we're going to blow up the factory." The inquest into the 2013 terrorist attack on a gas plant near In Amenas, Algeria, has received little media attention in Canada. Muslim leaders in London said they were unaware of the inquest, but have been working to prevent radicalization of their youths. London Free Press, A1

Little new money for agencies that fight terrorism: main estimates
While Prime Minister Stephen Harper says Canada is at war with violent jihadism, his government's spending estimates for the coming year show little increase in the amount of money going to some of the key organizations responsible for fighting terrorism. Main estimates tabled Tuesday by Treasury Board Minister Tony Clement show that many of those organizations, such as the Canadian Security Intelligence Service (CSIS) and the Canada Border Services Agency are slated to receive only small increases in their budgets to keep Canada safe. Others, like the RCMP, the Public Safety Department and National Defence are being asked in the main estimates to spend less in the coming year than Parliament gave them to spend last year. The main estimates call for the Communications Security Establishment - which got a very large increase in its budget last year to fund its new, state of the art headquarters - to spend 35 per cent less than it got last year. That is still 21 per cent more than it received in 2013/14. While the budgets provided for each department can be increased through the budget tabled by the finance minister or supplementary estimates voted by Parliament, government officials did not respond Tuesday when asked whether they plan to inject more money into the government effort to battle terrorism. Ipolitics.ca

Small spending increases for security, even less for security watchdogs
The government plans only modest spending increases for key national security agencies in the coming year despite proposed legislation to dramatically expand their powers and scope, according to federal spending estimates released Tuesday. What's more, as the Conservatives continued their weeklong defence of anti-terror Bill C-51 in the Commons Tuesday by insisting that rights and freedoms will be protected by robust, independent oversight, Treasury Board revealed that Canada's two national security oversight agencies are to receive a combined total of just $16,358 in additional funding in the next fiscal year. By comparison, Canada's "human" spy agency, the Canadian Security Intelligence Service (CSIS),

and the electronic spy agency, the Communications Security Establishment (CSE), are to get a combined total of almost $37 million more in annual net spending for 2015-16. CSIS is to see a net $20.8 million, or 3.8 per cent, boost, bringing planned spending to $537 million for 2015-16. The CSE is to get $16.1 million, or 3 per cent more, for total spending of $538.2 million. The Canada Border Services Agency's (CBSA) net spending is to rise $37 million, or 2.2 per cent, to $1.78 billion. The RCMP, which has responsibility for criminal national security investigations, is to see a $4.1-million, or 0.2 per cent, spending increase. The limited increases are surprising, given the government's relentless warnings since October that Islamic extremists now threaten Canada like never before. Ottawa Citizen.com

Harper urges swift passage of terror bill

Prime Minister Stephen Harper is urging a House of Commons committee to study the government's anti-terror bill as quickly as possible, in spite of accusations the Conservatives are using their majority to rush the legislation onto the books. NDP Leader Tom Mulcair told the Commons on Tuesday it is essential to scrutinize the bill, and asked Harper to ensure that security and human rights experts are not only heard, but also heeded. The Conservatives brought in the bill - which would significantly expand the powers of Canada's spy agency - following the murders of two Canadian soldiers last October. The bill would also make it easier for authorities to control the movements of terror suspects, expand no-fly list powers, crack down on extremist propaganda and outlaw encouraging someone to commit a terrorist act. The NDP opposes the legislation, saying it threatens civil liberties and fails to make Canadians safer. Harper dismissed Mulcair's criticisms and said the public strongly supports the proposals. Waterloo Region Record, A3

*** Senate grills Muslim leader over alleged radical ties**

A Muslim social services leader made an anti-radicalization submission to a Senate committee then faced tough questions about her own alleged association with radicals. Shahina Siddiqui, of the Winnipeg-based Islamic Social Services Association, appeared before the Senate committee on national security and defence in Ottawa on Monday. She called on Muslims and non-Muslims to work together to combat ISIS and al-Qaida but also cautioned against "religious bigotry by Islamophobes." Committee chairman Sen. Daniel Lang and member Sen. Lynn Beyak questioned Siddiqui about her work as a board member with the National Council of Canadian Muslims (NCCM), formerly known as CAIR-CAN. Senator Beyak asked Siddiqui about the connections between CAIRCAN and CAIR-USA. The U.S. group is an unindicted co-conspirator in a US$12-million Hamas financing trial that led to guilty verdicts in Texas in 2008. "How can we trust community organizations to help us develop a counter-radicalization narrative when they themselves are affiliated with organizations with known ties to terrorism?" Beyak asked. Siddiqui told senators that CAIR-USA and CAIR-CAN/ NCCM are not related. But, in fact, Canada's trademarks database indicates CAIR-USA applied for, and was granted, the trademark on the CAIR name in Canada in 2005. QMI Agency, 32 (Edmonton Sun, Ottawa Sun, Winnipeg Sun)

*** FINTRAC looks to banks to monitor clients' social media activities**

The federal agency responsible for monitoring potential money laundering and terrorist financing is encouraging financial institutions to go as far as analyzing their clients' public social media activity when investigating suspicious transactions. A 2014 presentation prepared by FINTRAC for financial institutions contains a hypothetical scenario in which a bank examines the social media activity of its own client to assess a potential case of terrorist financing. "We are disclosing a [suspicious transaction report] relating to Heinrich TRAVELLER and based on adverse information revealed through our open-source research and activity in his account that does not correspond to his profile," reads a fictional bank report to FINTRAC. The scenario is part of a presentation titled "Financial Intelligence and Counter Terrorism in Canada," obtained by Embassy through an Access to Information request. "Mr. TRAVELLER has been one of our clients since June 20, 2012," the mock correspondence goes on to state. "He is a 25-year-old retail sales clerk. At the time of this statement, the balance of his portfolio was $9,356.53. An online search using the client's name revealed adverse information about the client pertaining to the promotion of terrorism, anti-Semitism and acts of martyrdom." Financial institutions are required to report any suspicious client activity to FINTRAC under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, but the guidelines for determining suspicious activities are open-ended. Institutions are to report any activities that they have "reasonable grounds to suspect" are money laundering or terrorist

financing offences. The legislation applies to a range of financial players, including life insurance companies, accountants, real estate dealers, casinos and money transfer agents. Embassy

*** Britain's intelligence committee controversy backs Ottawa's system**
In Canada, the opposition is holding up the British Intelligence and Security Committee (ISC) as a model for increased parliamentary oversight of the country's security agencies, especially given the proposal to beef up anti-terrorism legislation. Critics rail that Canada's current oversight agency – the Security Intelligence Review Committee (SIRC) – has been filled with patronage appointees, including former chair Arthur Porter who is currently fighting against extradition to Canada in a Panamanian cell. Mr. Porter, a former hospital administrator in Montreal, has been at the heart of a massive RCMP probe into allegations of kickbacks involving engineering firm SNC-Lavalin. He was active in Conservative circles when he was approached by the PMO to sit on SIRC in 2008. In his recent autobiography, he said he underwent a minimal security check before joining the body where he was given access to classified intelligence. He left in a storm of controversy in 2011. The ongoing controversy in Britain involving former ISC chair Malcolm Rifkind plays to Ottawa's argument that it's better to have a non-political oversight system. The government has defended SIRC as a made-in-Canada success, arguing that oversight bodies such as the ISC open the door to political interference in national-security matters. Globe and Mail.com

*** Don't sacrifice liberty for security**
An opinion piece states, "Four former Canadian prime ministers (including a Conservative) and five former Supreme Court justices have warned Conservative Prime Minister Stephen Harper that protecting the security of Canadians and their most important freedoms is not a zero-sum game. In their own words criticizing his anti-terrorism legislation, Bill C-51, they warn: "Protecting human rights and protecting public safety are complementary objectives, but experience has shown that serious human rights abuses can occur in the name of maintaining national security." Harper has already said he will ignore this historically unprecedented collective advice, even though it warns that key security agency review bodies will not have enough power to provide critical oversight of new government security activities. (Contrast that with the views of our closest allies in the U.S., U.K., Australia and New Zealand who have established that democratic oversight is a key aspect of national security.) The reason for the prime minister's refusal to listen can be found in the fact that he announced his sweeping anti-terrorism legislation not in Parliament, but in an election campaign-style presentation in an Ontario riding. Ignoring the most effective way to protect both our security and liberties to win the fear vote on terror is a Faustian bargain of selling the soul of your democratic principles for power. Could it be that his refusal is also based on the need for maximum opposition to the legislation so those who disagree with the bill can be slammed as "soft on terror"?" Toronto Star, A13

*** Leak reveals spies chase more activists than terrorists**
Despite popular belief that they are chasing terrorists and master criminals, the world's spy agencies spend much of their time pursuing environmentalists, opposition leaders, dissidents and even airline staff, leaked documents show. The intelligence agencies, including Canadian spies, are interested in civilian targets that go far beyond terrorism, according to the latest batch of South African intelligence agency reports, leaked to Al Jazeera. Many spy agencies are more preoccupied with political activists than with terrorism, the reports show. One document revealed that the Canadian Security Intelligence Service (CSIS) was strongly interested in whether the Israeli airline, El Al, might have any guntoting Israeli spies among its staff in international airports. It questioned whether El Al staff might have illegally obtained firearms. South Korea's spy agency wanted a "specific security assessment" of Greenpeace International's director, Kumi Naidoo, before the G20 summit in Seoul in 2010, while Cameroon's espionage agency sought an intelligence report on an opposition politician before an election in 2011. The Rwandan government wanted the authority to spy on "negationists" - anyone who questioned its version of the Rwandan genocide. And Sri Lanka wanted information on Tamils from Canada and elsewhere who were allegedly attending "military training" in South Africa. South Africa rejected the requests from Cameroon, Rwanda and Sri Lanka, and it is unclear whether it spied on Mr. Naidoo. Globe and Mail, A17

*** La peur et la réplique**

Un éditorial déclare, "Que quatre Canadiens sur cinq soient d'accord avec le projet de loi antiterroriste du gouvernement Harper ne surprend pas. Dans le climat international actuel et sa forte médiatisation, avec les décapitations du mouvement État islamique qui sèment la terreur, les attentats perpétrés chez nous l'automne dernier, les menaces diffusées sur Internet, le récent complot terroriste déjoué par la police concernant un déraillement de train passager de Via Rail sur la ligne Toronto-New York qui aurait fait un lot de victimes, et puis la découverte inquiétante d'un mystérieux tunnel à Toronto, pas étonnant, donc, que le public applaudisse à une démarche du gouvernement qui promet de lutter encore plus efficacement contre le terrorisme. Évidemment, on ne peut pas présumer du fait que tous ceux qui ont répondu au récent sondage avaient lu de A à Z le projet de loi C-51 et étaient donc parfaitement informés de ses tenants et aboutissants. Mais il y a des spécialistes, des juristes, d'anciens ministres de la Sécurité publique et quatre ex-premiers ministres canadiens qui l'ont lu. Et bien qu'ils soient d'accord avec les objectifs poursuivis et le resserrement des mesures de contrôle qu'il prévoit, n'en sont pas moins inquiets du manque de balises qui pourrait, selon eux, mener à un abus de pouvoir et à une violation des droits de la personne. Leurs préoccupations méritent qu'on s'y arrête." Le Nouvelliste, 14

*** Edmonton mall terror threat must be heeded**
An opinion piece states, "Of course a mall is a good terror target. It's so open to the public that it's hard to secure perfectly. It's also a goal of terrorists to make ordinary people feel unsafe in their daily lives. So what better place to carry out an attack than where we buy our clothes or groceries, get our hair done or go to a movie? On top of that, the al-Qaida affiliate from Somalia -- al Shabaab -- which called on supporters to attack malls in Canada, the U.S. and Britain (including West Edmonton Mall) has a history of attacking malls near its base in Africa. They carried out the September 2013 attack on the Westgate Mall in Nairobi, Kenya in which Islamic extremists sealed off the mall then spent three days executing ordinary shoppers who were unable to recite basic Muslim prayers. Of course an Edmonton mall is also a terror target. Even though the war with terrorists seems far away (and it is, for the most part), the Edmonton Garrison sent more soldiers to Afghanistan than any other base in the country. We may see Edmonton as a sleepy little oil-service burg on the northern fringes of the Prairies with a hardworking population and pro hockey team, but terrorists see it as home to an army of crusaders who have invaded Islam's homelands. They would be happy for some retribution." Kingston Whig-Standard, A4 (London Free Press, Toronto Sun, Calgary Sun, Ottawa Sun, Edmonton Sun, Winnipeg Sun)

*** ISIS recruited Canadian woman to join fight in Syria**
The family of a young Canadian woman who travelled to Syria after being radicalized say losing her was the most "shocking thing in the world" and that they wish CSIS had done more to prevent the 23-year-old's departure. The woman, whom CBC News is calling Aisha to protect her identity, made the journey to Syria to join up with ISIS last summer, after taking an online course to study the Qur'an taught by a woman based in Edmonton, says her older sister Rabia (whose name has also been changed). "We all went to work, came home, all her stuff was gone. She had packed all her winter clothes, took her computer and left," Rabia says. "It was the most devastating, most scary, most shocking thing in the world." Over the past several months, Rabia has been speaking to CBC News about her family's ordeal. Some details, such as names and the family's location, are being withheld for security reasons. The Canadian Security Intelligence Service declined to comment on the specific case, but said in an emailed statement that terrorism "including radicalization of Canadians and terrorist travel remains the most prominent threat to Canadian interests and our national security." CBC News

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Moncton couple accused of conspiring to import cocaine
A Metro Moncton couple has been charged in relation to a massive cocaine seizure at the U.S.-Mexico border two years ago. Luc LeBlanc, 42, and Michelle LeBlanc, 37, were charged in late January with conspiring with others to import cocaine into Canada. Times & Transcript, A3

Fighting for medical care as deportation looms

An Ottawa-born man ordered deported to India after a stint behind bars is now fighting for access to OHIP. In September 2014, Deepan Budlakoti, 25, lost a bid to have a federal court judge declare him a Canadian citizen which he vowed to appeal. In addition, the man's legal woes have denied him access to provincially-funded health care. QMI Agency (Ottawa Sun, 4)

Chris Brown barred at Canadian border
R&B singer Chris Brown says he's been barred from entering Canada. The "Forever" singer tweeted Tuesday that the "good people of the Canadian government" wouldn't let him into the country for shows in Montreal and Toronto. Canadian Press (Toronto Star, A3, Cape Breton Post)

*** CBSA finds 162 ammunition magazines on Kentucky man**
The Canada Border Services Agency (CBSA) released the first report of 2015 from Saskatchewan's port of entries in the southern part of the province. On January 18, officers at North Portal seized a record 162 magazines from a Kentucky man en route to Alaska. He declared five firearms and 15 magazines, which were overcapacity rifle clips. Upon closer examination, officers noted one of the guns was a restricted assault rifle that wouldn't be allowed to cross the border. When officers began the vehicle search, they found more than what they were looking for: 162 military-grade magazines (including 147 prohibited) valued at over $5,000. The man was issued a $1,000 penalty and returned to the U.S. In the beginning of January, officers in southern Saskatchewan made several seizures of prohibited weapons and devices. Estevan Mercury

*** Drugs, weapons, cash and child porn seized at Niagara border crossings**
Border agents in Niagara seized a cache of weapons, drugs, cash and child porn over the last four months. They also reunited two missing children with their families and arrested a woman who opted to cross the border using a raft instead of a bridge. The Canada Border Services Agency on Tuesday released information on enforcement highlights at Niagara border crossings between Oct. 1, 2014 and Jan. 31. Niagara Falls Review

*** American gets 90 days in jail for smuggling child porn into Halifax, arrested on boat**
An American citizen has been sentenced to jail time for smuggling child pornography after he was arrested in December on a boat in Eastern Passage. The Canada Border Services Agency (CBSA) announced Tuesday that Brian Scott Long, 51, of Washington pleaded guilty to smuggling child pornography in Dartmouth provincial court on Monday. The release said Long was sentenced to 90 days in jail. Cape Breton Post

*** Will Matt DeHart be the next victim of the war on leaks?**
A blog post states, "The case of Matt DeHart, a former U.S. drone pilot turned hacktivist, is as strange as it is disturbing. The 29-year-old was recently denied asylum in Canada, having fled there with his family after — he claims — he was drugged and tortured by agents of the FBI, who accused him of espionage and child pornography. Last week the Canadian Border Services Agency said he will be deported to the U.S. to stand trial "in very short order," after a Canadian Immigration and Refugee Board ruling earlier this month denying his request for refugee status. He is being denied access to two thumb drives that he says contain evidence of illegal acts perpetrated by a U.S. government agency. Now after three unsuccessful attempts to gain political asylum, he fears that he and the files will be delivered to the very government he sought to escape." Aljazeera

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** CSE monitors millions of Canadian emails to government - Critics question how long data is stored and what it's used for**
Canada's electronic spy agency collects millions of emails from Canadians and stores them for "days to months" while trying to filter out malware and other attacks on government computer networks, CBC News has learned. A top-secret document written by Communications Security Establishment (CSE) analysts sheds new light on the scope of the agency's domestic email collection as part of its mandate to protect government computers. CBC analyzed the document in collaboration with U.S. news site The

Intercept, which obtained them from U.S. National Security Agency whistleblower Edward Snowden. Canada's electronic spy agency watched visits to government websites and collected about 400,000 emails to the government every day, storing some of the data for years, according to the 2010 document. Today's volume is likely much higher given online traffic growth. CBC News

*** Government computers subject to 'millions' of 'probing attempts' daily: Fantino**
Junior defence minister calls out "foreign countries or companies" as well as "criminal organizations," "activists with political or social agendas" and "terrorists" as possible cyber threats. Cyber security concerns were top of mind at this year's Ottawa defence conference, as revelations continue to come out about the extent of international electronic eavesdropping by allied nations and Canada.United States National Security Agency director Admiral Michael S. Rogers spoke at the Ottawa Conference on Security and Defence, lamenting the loss of public trust exacted by the exposure of top secret files gathered by former US security contractor-turned-whistleblower Edward Snowden. Associate Minister of National Defence Julian Fantino also chose to spend half his Feb. 20 speech at the event talking about cyber security, suggesting that "millions of Canadians" will "fall victim to cybercrime," and "millions of probing attempts are detected daily of government systems." Some of those Canadians are inside Mr. Fantino's own government. A financial update tabled in Parliament on Feb. 19 showed the "unauthorized cyber intrusion" on the computer systems of a national research organization last year will cost the government $32.5 million. Hackers broke into the National Research Council's computers in July 2014, and Canada's chief information officer, Corinne Charette, blamed a "highly sophisticated Chinese state-sponsored actor"-an allegation a spokesperson for the Chinese Embassy called "groundless" on CBC News. In his speech, Mr. Fantino called out "foreign countries or companies" as well as "criminal organizations," "activists with political or social agendas" and "terrorists" as possible cyber threats. Embassy

*** U.K.-U.S. spy hacking 'probably happened,' SIM card maker admits**
Gemalto, the world's largest maker of mobile SIM cards, said a preliminary company probe of sophisticated attacks against it in 2010 and 2011 showed British and U.S. intelligence services "probably" hacked into its office networks. Gemalto said the suspected attacks by the U.S. National Security Agency and Britain's Government Communications Headquarters "probably happened," but said the intrusions "only breached its office networks" and "could not have resulted in a massive theft of SIM encryption keys." The Franco-Dutch company was responding to a report by investigative news site The Intercept, which last week published documents it said showed that U.S. and British spies hacked into Gemalto, potentially allowing them to monitor the calls, texts and emails of billions of mobile users around the world. Reuters (Globe and Mail)

*** Companies unprepared for cyberattacks, report finds**
Organizations that oversee sensitive information remain woefully unprepared to fend off increasingly clever and sophisticated data raiders, according to a sobering new study. Nearly 70 per cent of those hit by data breaches in 2014 found out about the infractions from outsiders such as police or customers, according to a report issued Tuesday by Silicon Valley security software firm FireEye Inc. Data breach victims took a median of 205 days - almost seven months - to realize they had been hit, giving "attackers ... a free rein in breached environments far too long before being detected," the report said, while "run-of-the-mill cyber criminals" out to steal creditcard data are becoming harder to distinguish from state-sponsored attackers due to advanced camouflaging tools and tactics. Despite increasing awareness of cyberthreats and investments to protect sensitive data, including personal customer information and corporate secrets, corporations appear to be falling behind in their efforts to counter hackers. Many companies are better prepared for fires, floods and ice storms than data breaches, which "are more likely, and likelier to have a more significant business impact" than other emergencies, said John Proctor, vice-president of global cybersecurity with Montreal information technology services firm CGI Group Inc. Globe and Mail

*** US announces $3 million reward for accused prolific cyber criminal believed to be in Russia**
The U.S. government has announced a $3 million reward for information leading to the arrest of a man American authorities call one of the world's most prolific computer hackers. Evgeniy Bogachev, who is believed to be in Russia, was indicted in Pittsburgh last year on charges including bank fraud and conspiracy. His picture has been plastered on "Wanted" signs distributed by the FBI. Bogachev is

accused of acting as ringleader for a massive hacking operation in Russia and Ukraine that installed malicious software on victims' computers to capture bank account numbers, passwords and other sensitive information. CharlottetownGuardian.ca

*** Anthem says hack may affect more than 8.8 million other BCBS members**
Health insurer Anthem Inc, which earlier this month reported that it was hit by a massive cyberbreach, said on Tuesday that 8.8 million to 18.8 million people who were members of other Blue Cross Blue Shield plans could be victims in the attack. Anthem, the second-largest U.S. health insurer, is part of a national network of independently run Blue Cross Blue Shield plans through which BCBS customers can receive medical services when they are in an area where BCBS is operated by a different company. It is those Blue Cross Blue Shield customers who were potentially affected because their records may be included in the database that was hacked, the company said. Anthem does not know the exact number of Anthem versus non-Anthem customers affected by the breach because of those incomplete records, which prevent it from linking all members with their plan, Anthem spokeswoman Kristin Binns said. Yahoo! News

LAW ENFORCEMENT / APPLICATION DE LA LOI

SIU refuses to name man shot by police
The name of a 49-year-old man who was shot dead by Toronto police a week ago remains secret, though the province's police watchdog knows who he is. Due to a fairly recent policy change at the Special Investigations Unit, the public may never know the man's identity - a troubling thought, say observers, who point out that the name is crucial to scrutinizing a shooting by police and ensuring transparency. The SIU, which investigates all police-related deaths, decided in 2012 to release names of people killed by officers only with the consent of the family. The new policy stands in contrast to police force practice, which is to routinely release the names of homicide victims regardless of the family's wishes. In the case of last Wednesday's police shooting near Dupont St. and Spadina Rd., "investigators are continuing to work diligently to locate next of kin," SIU spokeswoman Jasbir Dhillon said. Toronto Star, A1

House blast sends six to hospital
An explosion that destroyed a house in Nova Scotia's Annapolis Valley was caused by a combination oil and wood-burning furnace that overheated and ruptured, the provincial fire marshal says. The explosion was originally thought to be gas related, but Harold Pothier ruled that out after completing his assessment of the explosion that happened shortly after 1 a.m. Tuesday in Westville. Six people were taken to hospital and all but one of them has been released, the provincial government said in a news release. RCMP Const. Kelli Gaudet said a 63-year-old man remained in hospital with non-life-threatening injuries. Canadian Press (The Guardian, A1, Daily Gleaner)

Sûreté du Québec: des coupures de 30 millions $ annoncées
Exceptionnellement, tous les cadres de la SQ dans la province ont été conviés à se rendre à l'École nationale de police du Québec (ENPQ), à Nicolet, pour assister en personne à l'annonce de leur directeur général. De plus, la direction leur a demandé de faire leur trajet aller-retour en covoiturage, à trois policiers par véhicule, afin d'économiser sur les frais de transport. Autant de mesures symboliques pour contribuer à la cure minceur imposée à la SQ par le gouvernement Couillard et dont la mise en uvre reviendra à cet ancien sous-ministre associé à la Sécurité publique. Nommé à la tête de la SQ en octobre dernier pour remplacer Mario Laprise, Martin Prud'homme devrait notamment confirmer l'abolition de 150 de ses 400 postes d'officiers. Une telle réduction des postes de cadres se concrétisera par une vague de départs à la retraite que l'organisation ne comblera pas. Martin Prud'homme entend également soumettre la police provinciale à une restructuration majeure. On promet une refonte des 10 districts administratifs actuels de la SQ, de sorte que le territoire desservi par les policiers de la SQ serait dorénavant réparti en quatre ou cinq régions élargies. Le nombre d'escouades régionales mixtes de lutte au crime organisé, qui est présentement de huit, sera lui aussi réduit, selon nos sources. Agence QMI (Journal de Quebec, Journal de Montreal)

Police watchdog 'limited' by hiring policy
The head of the Independent Investigations Office said having more freedom to hire former police officers who have worked in B.C. in the past five years would allow the office to attract more highly skilled investigators who can pass their expertise to civilian employees. Richard Rosenthal said hiring former police officers doesn't affect the long-term goal of having the organization, which investigates serious injuries or deaths involving police officers, fully staffed by civilians. "It's a one step back, three steps forward [strategy] and ... it gives us the opportunity to have people with current major crime experience in policing in B.C. who can train our people and make sure that we're operating according to best current practices," Rosenthal said Tuesday. The IIO's chief civilian director was responding to one of the key recommendations in a report released Monday by a special legislative committee. The committee looked into the organization and the feasibility of having it staffed fully by civilians by 2017. The hiring rule was a key recommendation laid out by retired judge Thomas Braidwood, who led the inquiry into the RCMP investigation into the 2007 death of Tasered Polish immigrant Robert Dziekanski at the Vancouver airport. His report led to the creation of the civilian-led oversight body in September 2012. The IIO can hire former police officers from outside the province regardless of when they retired. Times Colonist, A3

Four Mounties face assault charges
Four Mounties on Vancouver Island face assault-related charges in connection with alleged jail-cell incidents at two RCMP detachments. The charges come after investigations into two separate incidents by the Independent Investigations O ce. The Criminal Justice Branch says one alleged incident occurred last June at the Nanaimo RCMP detachment and resulted in Const. Tim Bedard facing one charge of assault causing bodily harm. In the second case, three Mounties are charged with assault with a weapon after the alleged use of pepper spray at the Parksville detachment in June 2013. Constables Scott Jones, and Mick White, and Cpl. Michelle Lebrun, are to appear in court in Nanaimo on March 17. Postmedia News (Vancouver Sun, A2); Canadian Press (The Province, , Times Colonist)

Woman assaulted on UBC campus
Police are warning the public to be vigilant after an 18-year-old was assaulted on campus at the University of B.C. Mounties say the woman was walking alone on Sunday night when a man grabbed her from behind. RCMP say the woman was not hurt and was able to break free from the man's grip, who then ran away. The suspect is described as an 18-to 20-year-old man with olive skin, spiky short black hair, and a medium build. Police say the incident is probably isolated and not related to a string of on-campus assaults in 2013. But Cpl. Brenda Winpenny says the public should stay aware of their surroundings, especially while walking alone late at night or early in the morning. Postmedia News (Vancouver Sun, A2)

*** Senate committee will ask RCMP to show Michael Zehaf-Bibeau video**
The Senate's national security committee is asking the RCMP to make public a video that Michael Zehaf-Bibeau reportedly recorded before the Oct. 22 shootings in Ottawa. Committee chairman Sen. Daniel Lang told senators this week he will draft a letter to RCMP commissioner Bob Paulson, asking the top Mountie to release the video Zehaf-Bibeau made before he killed Cpl. Nathan Cirillo at the National War Memorial, then died in a shootout inside the Centre Block. MPs on the House of Commons' public safety committee made the same request on Feb. 17. The Commons committee also wants Paulson to release the video at his "earliest convenience," and speak to the committee about the investigation. Lang is asking for the video to be released when the RCMP investigation into Zehaf-Bibeau was over. "Mr. Zehaf-Bibeau applied for a visa to go to Libya just weeks before and was denied. Mr. Zehaf-Bibeau had taken a tour of Parliament Hill prior to the attack, and he also went out to obtain a rifle just days before the attack. His name was also found on a computer of a known terrorist," Lang said Monday. "Given what we know, I would like to advise the committee that I'll be writing to the commissioner to have the video released as soon as the investigation by the RCMP has concluded." Postmedia News (Ottawa Citizen)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Don't interview Khadr**

A letter to the editor states, “Let us interview Khadr: media outlets - Feb. 10 The problem with letting the media and the public get hold of Omar Khadr before he is released from prison is that they will put him in a place where he feels he is not welcome in Canada. Many people from other countries already feel they are not welcome here and get looked at differently then the average Caucasian male or female. Of course Canada should have the "right to understand" what this man is capable of, but they cannot do anything about him being released. Therefore, putting Khadr through an interview and asking him questions where half the nation will not believe his answers seems unfair.” Waterloo Region Record, A6

*** Man on federal parole charged with attempted bank robbery**
A 34-year-old man appeared in provincial court Tuesday charged with attempting to rob the Royal Bank on Lansdowne Avenue Monday around 10:30 a.m. Marc LeBlanc was asked if he wished to have a judge and jury trial or deal with the charge in provincial court. Duty counsel Margaret Gallagher said LeBlanc did not wish to choose at this time. Prosecutor Kelly Winchester objected to his release and Gallagher said LeBlanc is a federal inmate on parole who wants to serve his remand time in a federal penitentiary rather than a provincial jail. Winchester said that would be up to the correction system, but said she has no reason to keep LeBlanc in jail in Saint John. Provincial court Judge Andrew LeMesurier asked LeBlanc where he thought he would go. "Renous," Leblanc replied. Telegraph-Journal, B2

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Looking for some solutions
How can violence against indigenous women and girls be eliminated? That is the question First Nations leaders and community organizations are hoping Saskatchewan citizens can answer. On Tuesday, a forum hosted by the Federation of Saskatchewan Indian Nations (FSIN) in partnership with Regina Treaty Status Indian Services (RT SIS) was held at the First Nations University of Canada (FNUniv). "We are going around the province right now in order to get as many viewpoints as we can," said Erica Beaudin, manager of RT SIS. "We have been in Saskatoon and next month we hope to be in Prince Albert and other areas. We feel that every voice counts and every voice matters." During the event, participants were asked to discuss and complete a survey about violence and what needs to be done to address it from the community level all the way up to the national level. "The way toward a solution is to get as many people discussing and ready to move on the issue of eliminating violence in our lives," said Beaudin. FSIN plans to take the community suggestions and present them at the roundtable on missing and murdered indigenous women happening in Ottawa on Friday. "We have collected data from over 100 people, thus far, and that includes men, women, children and elders," said Beaudin. "What we are seeing is that the solution is one the family and strengthening the family, supporting the family, prevention rather than intervention and when intervention is needed then the necessary supports are there and they are adequate and they are relevant." Beaudin has been working in the area of missing and murdered women for years and said it's great to see others like Mayor Michael Fougere and his councilmen standing up and supporting a call for a national inquiry. Leader-Post, A1

Student cyberbullying on rise as teachers, police work to keep up
Cyber-bullying is growing exponentially in schools as teachers and police work to keep up with the massive proliferation of social media sites and the anonymity that youth believe they offer. "We're at the point where the way that kids communicate with each other now, it's electronically," said Const. Brad Bulman, a student resource officer at Centennial High School who is dealing with a cyberbullying incident at least once every two weeks at the school. "We're seeing boys organizing fights after school, we're seeing kids sharing photos that they really shouldn't be. "But there's a lot going on that we don't know about, that the kids probably aren't even telling us. That's the scary part." More than 1,500 students gathered at Centennial High School Tuesday for the Who's Frank event, on the eve of Pink Shirt Day, to raise awareness around bullying. Frank, a life-size pink elephant at the centre of the campaign partnering Calgary high schools with Mount Royal University, is meant to kick-start the discussion around bullying as the "elephant" in the room. Students and teachers at Tuesday's event said that cyber-bullying is a large elephant, a monster of sorts in the lives of many young teens, particularly those in the 13 to 15 year age group who are still discovering social media yet are most vulnerable to it. "It's a bit of an ogre really," said

Matt Christison, principal at Centennial High School. '"We're seeing females versus females, or males versus males, most often, or those who are in a relationship and then break up. There are a lot of terrible words, it can be relentless, very harmful, and for some individuals who are susceptible, the pain can go very deep." Calgary Herald, A1

*** So many victims, so little change**

An editorial states, "Given the tragic shadow cast over Saskatchewan by the murders of dozens of aboriginal women and the disappearance of many others, it is good to see this province speaking with a strong, united voice for a national inquiry into what's become a shameful issue across the country. On Monday, Regina city councillors added their unanimous call for "an inquiry or round table into missing and murdered indigenous women" to similar declarations by Saskatoon city council, the Saskatchewan Urban Muncipalities Association and numerous aboriginal groups. Saskatchewan Justice Minister Gord Wyant heads to Ottawa Friday for a meeting of First Nations leaders and federal and provincial politicians to discuss the issue. Canada's premiers and territorial leaders all support an inquiry and Wyant says the Conservative government should drop its resistance to the idea and take a leadership role in addressing "why there is so much violence against aboriginal women and girls." An RCMP report last year identified 1,017 female aboriginal victims of homicide in Canada between 1980 and 2012. It said an additional 164 were "missing". The RCMP said the numbers exceeded previous public estimates and added that aboriginal women were almost three times more likely to be victims of violence than non-aboriginal women. Saskatchewan had the highest proportion of female aboriginal homicide victims - 55 per cent - among the provinces during the studied period, despite aboriginal women comprising just 15 per cent of our population. Between 1980 and 2012, 153 aboriginal women were murdered in this province, compared with 116 non-aboriginal women. Manitoba (49 per cent female aboriginal victims) and Alberta (28 per cent) were the next-highest provinces." Leader-Post, A8

*** 'Every voice counts and every voice matters,' say native groups**

First Nations leaders and community organizations hope Saskatchewan citizens can help answer the question of how to eliminate violence against indigenous women and girls. The Federation of Saskatchewan Indian Nations (FSIN) and Regina Treaty Status Indian Services (RTSIS) hosted a forum Tuesday on the subject at the First Nations University of Canada (FNUC). "We are going around the province right now in order to get as many viewpoints as we can," said Erica Beaudin, manager of RTSIS. "We have been in Saskatoon and next month we hope to be in Prince Albert and other areas. We feel that every voice counts and every voice matters." Participants at Tuesday's event were asked to discuss and complete a survey about violence and what needs to be done to address it from the community level to the national level. The FSIN plans to present their suggestions at the roundtable on missing and murdered indigenous women in Ottawa on Friday. StarPhoenix, A9

*** Mettre fin au massacre**

Des millions de civils se font tuer, amputer, blesser, torturer, déplacer sous les yeux d'une communauté internationale qui n'intervient pas pour mettre fin à la boucherie. C'est ce dur constat qui ressort du nouveau rapport annuel d'Amnistie internationale, rendu public aujourd'hui partout dans le monde. «La réponse internationale est une honte. Pourtant, nous ne sommes pas impuissants», dit le secrétaire général de l'organisation, Salil Shetty. Résumé des points saillants de ce document de plus de 500 pages en sept recommandations. (…)Le rapport d'Amnistie n'épargne pas le Canada, notamment à l'égard des droits des autochtones. «Il faudrait écouter ce que le rapporteur spécial des Nations unies a à dire là-dessus. Il parle d'une crise. Il faut mettre en place une commission d'enquête sur les disparitions de femmes autochtones. Il y a un vrai problème de violence contre les femmes autochtones. On leur doit au moins de les écouter !», fait valoir Béatrice Vaugrante. La Presse (Le Quotidien, 40, Le Soleil)

*** The power of pink**

Feb. 25 is Pink Shirt Day, a day when everyone is encouraged to wear something pink to show a united front against bullying. Pink Shirt Day originated with Nova Scotia high school students, who organized a protest to wear pink in sympathy with a Grade 9 boy who was being bullied for wearing a pink shirt. At least 1 in 3 adolescent students in Canada have reported being bullied recently. 47% of Canadian parents report having a child who is a victim of bullying. 7% of adult (18+) Internet users report they have

experienced cyber-bullying at some point in their life. QMI Agency (Winnipeg Sun, 25, Calgary Sun, Edmonton Sun, Kingston Whig-Standard)

*** Premier Greg Selinger gets earful from First Nations leaders**
Manitoba Premier Greg Selinger faced sharp criticism on Tuesday at the Assembly of Manitoba Chiefs' annual general assembly of chiefs at Brokenhead Ojibway First Nation. Selinger was there for three hours to talk about the province's progress implementing the recommendations from the Phoenix Sinclair inquiry and to take questions from the First Nations leaders. But some chiefs were unhappy Selinger limited the number of questions chiefs could ask. ?O-Pipon-Na-Piwin Cree Nation Chief Chris Baker of South Indian Lake said he was not happy the premier was there for such a short period of time. He said he would have liked Selinger to hear more of what the chiefs had to say at the general assembly, but he also wanted a separate meeting over a full day or two with the premier and his cabinet to discuss poverty, social issues, and Manitoba Hydro concerns. "The resources that are being extracted and taken away from us, and the opportunities, the training and the education that we talk about - why can't we sit down and get a commitment from the province?" Baker said at the meeting. Selinger agreed to further meetings with the chiefs involving his cabinet. Manto Sipi Cree Nation Chief Michael Yellowback voiced his concerns about the province taking over the band constable program. Federal funding for the program runs out in April. CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

Canadian military trainers ordered to leave region threatened by Boko Haram
Canadian special-forces soldiers providing counterterrorism training in Niger have been forced to pack up from a border region and relocate to another part of the African country in order to stay out of the way of fighting between Boko Haram extremists and government troops. At the same time, the Canadian military says it stands ready to step up its role in Niger if Ottawa decides to send aid. The government of Niger, a poor desert country, recently declared a state of emergency in the border region of Diffa after a number of attacks by Boko Haram, an Islamist terror group. Troops from Canada are training African counterparts in shooting, communications and mission planning - skills they could use in order to combat groups such as Boko Haram, which controls more than 50,000 square kilometres of territory in western Africa and is destabilizing the region. The operations are being conducted as part of an annual U.S.sponsored military exercise called Flintlock, which this year began in February and runs until March 9. Globe and Mail, A3

INTERNATIONAL / INTERNATIONAL

Extremists kidnap at least 70 Christians in Syria
The Islamic State militants struck before dawn, staging house-to-house raids in a cluster of villages nestled along the Khabur River in northeastern Syria. They abducted at least 70 Christians - many of them women and children - while thousands of others fled to safer areas. The captives' fate was unclear Tuesday, a day after they were seized, and relatives said mobile phone service was cut off and land lines also were not going through, adding to the fear and uncertainty about their loved ones. Heavy fighting was reported in the area. The Islamic State group has a history of killing captives, including foreign journalists, Syrian soldiers and Kurdish militiamen. Most recently, militants in Libya affiliated with the extremist group released a video showing the beheading of 21 Egyptian Christians. The group's bloody campaign in Syria and Iraq, where it seeks to form a self-styled caliphate, has repeatedly targeted religious minorities since it took control of a third of both countries. The United States and a coalition of regional partners are conducting airstrikes against the group. Associated Press (Chronicle-Herald, A14,

Red Deer Advocate, Whitehorse Daily Star, Times & Transcript, Telegraph-Journal, Edmonton Journal, Vancouver Sun, Montreal Gazette, StarPhoenix, Acadie nouvelle, Waterloo Region Record)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
April 16, 2015 / le 16 avril 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Debate urged on changes to secretive 'no-fly list'
Much of the recent analysis of the Conservative government's controversial anti-terror legislation has focused on extending investigative powers to Canada's spy agency. But critics say there's another part of Bill C-51 that has been largely overlooked, though equally troubling: the overhaul of the secretive "nofly list." Here's a look at how someone gets flagged under the Passenger Protect Program, how the process would change under Bill C-51, and why some observers are sounding the alarm. Q: How does someone get on the list now? A: A person is added to the list if there are "reasonable grounds to suspect" they pose a threat to aviation security. According to internal guidelines, this could include someone who is believed to be involved in a terrorist group that has threatened aviation security in the past or may do so in the future, as well as someone who is believed to be capable of violence and may have a motive to harm people on a plane. Senior police, intelligence, border and transportation officials meet every 30 days to review names and make recommendations to the **public safety minister**, who has the final say over the list. The list is passed on to air carriers. If someone on the list tries to board a plane, the transport minister (or designate) is notified. If the person is deemed to pose an "immediate threat," the minister can issue an emergency direction to stop that person from boarding. That person can challenge the decision by writing to the Office of Reconsideration, which will review the case and make a recommendation to the **public safety minister**. Q: What would change under Bill C-51? A: People don't necessarily have to pose a threat to the plane itself. They can be added to the list if there are reasonable grounds to suspect they are travelling to commit a terrorist act abroad. (This criterion was likely added in response to the many Canadians who have gone overseas to join ISIL militants). If they show up at the airport, it now falls on the **public safety minister** (or designate) to decide whether to stop them from boarding or have them

undergo extra screening. There is no mention of having to determine whether they pose an "immediate threat." Postmedia News, A15 (Edmonton Journal, National Post, Leader-Post, Windsor Star, Montreal Gazette, The Province, Vancouver Sun)

Ottawa seeking new prison watchdog
Ottawa is searching for a new prison ombudsman after refusing to extend the contract for the current Correctional Investigator for Canada beyond one year. Howard Sapers, who has held the position for eleven years and been a vocal critic of the Harper government's treatment of mentally ill and Aboriginal inmates, as well as the use of solitary confinement, was recently told he would remain on the job only until a replacement was found. Sapers had told **Public Safety Minister Stephen Blaney** over a year ago that he would like to remain in his role for another term, which is typically three or four years. Canada's prior ombudsman held the position for 25 years. But Sapers' fate was unknown with just hours to go before his term expired on March 31, when **Blaney** made a recommendation that he would stay on - but only temporarily. "Reappointing me for up to one year without giving me, or my organization, any certainty about the length of the term is a little destabilizing," Sapers said in an interview with the Toronto Star. "It's very hard to be a small, independent agency trying to hold a large government department to account. The role of this agency should be nurtured and supported and this is not the way to support that role." Liberal Public Safety Critic Wayne Easter said keeping Sapers "in limbo" will impact the work of his department and accused the Harper government of playing politics with a vital oversight role. "He's absolutely right. When your chief executive officer, so to speak if you're talking about a business, is in limbo, it doesn't only effect the person, it effects your whole establishment," Easter said. Toronto Star, A6

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Lac-Mégantic revit à La petite séduction**
Lac-Mégantic a vécu pire que l'enfer le 6 juillet 2013. L'émission La petite séduction qui y a été tournée l'automne dernier pour ouvrir la 10e saison n'est pourtant pas la plus larmoyante que j'ai vue de cette série. On ne se remet pas aussi vite d'une telle tragédie, mais on sent un tel sentiment de reconnaissance et ce besoin de revivre chez les citoyens. C'est d'ailleurs pour remercier le Québec tout entier que les Méganticois ont voulu recevoir l'équipe de Dany Turcotte, dans cette émission diffusée mercredi à 20h sur ICI Radio-Canada Télé, mais déjà accessible dans une version allongée sur ICI Tou.tv. A cette occasion, on a ramené cinq invités vedettes, accompagnés de citoyens des villes et des villages qui les avaient reçus lors de précédentes émissions de La petite séduction. «Je ne peux même pas m'imaginer qu'il y avait là un centre-ville», affirme Pénélope McQuade en marchant le long de l'immense trou où se trouvait le coeur de Lac-Mégantic, il y a à peine deux ans. Guylaine Tremblay, Anne Casabonne, Rémy Girard et Vincent Vallières ont aussi voulu apporter leur appui à la population. Le Soleil, 32

*** L'assemblée des créanciers remise**
L'assemblée des créanciers pour la faillite de la Montreal, Maine & Atlantic (MMA) sera retardée. Initialement prévue pour le 27 mai prochain dans la requête qui avait été déposée au dossier de la cour, cette assemblée cruciale pour la mise en place du plan de dédommagement de 293 millions $ des victimes du déraillement du 6 juillet 2013 à Lac-Mégantic sera remise à plus tard. « La date du 27 mai prochain devient très difficile pour la tenue de l'assemblée avec les créanciers. Les réunions d'information seront aussi retardées. Nous espérons que le débat supplémentaire ne retardera pas le processus de plus de deux semaines », explique l'avocat de la MMA, Me Patrice Benoit qui tient à ce que l'assemblée des créanciers de la MMA se déroule avant les vacances estivales. Les avocats du recours collectif, qui font partie des créanciers de la MMA, se sont opposés hier au palais de justice de Sherbrooke au plan d'arrangement avec les créanciers déposé par le contrôleur de la faillite Richter. Les représentants des victimes du 6 juillet veulent déposer un plan d'arrangement avec les créanciers alternatif à l'offre faite par le contrôleur de la faillite de la MMA. La Tribune, 5

*** Grosse foule pour le recours collectif**
Il aurait fallu une salle deux fois plus grande que celle du Pavillon Fernand-Grenier, du parc de l'OTJ de Lac-Mégantic, où avait lieu, mardi soir, la réunion d'information sur l'état de situation du recours collectif

des victimes de la tragédie du 6 juillet 2013. Les 150 chaises prévues ont en effet été occupées très rapidement et à peu près le même nombre de personnes ont dû rester debout ou n'ont pu pénétrer dans la salle bondée. L'avocat Daniel Larochelle a animé la rencontre, à l'aide d'un montage PowerPoint, flanqué de ses avocats associés au recours collectif, Joel Rochon et Jeff Orenstein. Il a commencé par l'énumération des démarches effectuées depuis septembre 2013, soit les recherches pour identifier une quarantaine de compagnies parties prenantes à la poursuite, l'entente avec une majorité de ces compagnies qui ont décidé de contribuer dès maintenant dans le cadre du plan d'arrangement de la MMA, plutôt que d'être poursuivies au Canada et aux États-Unis ultérieurement, puis les comparutions à la Cour supérieure du Québec, à Sherbrooke. La Tribune, 4

*** Des Méganticois encore affectés**

Les avocats responsables du recours collectif ne veulent pas minimiser les dommages psychosociaux subis par les citoyens de Lac-Mégantic et encore ressentis, plus de 21 mois après la tragédie de juillet 2013. « J'émets certaines réserves concernant le plan d'arrangement proposé : les sommes allouées pour les personnes souffrant de troubles psychologiques sont limitées et ma crainte est que le plan sous-estime grandement l'ampleur des dommages de ce groupe très vulnérable », a déclaré Me Daniel Larochelle lors de la réunion d'information. D'ailleurs, à la période de questions, un pompier de Lac-Mégantic a témoigné de son besoin récent de consulter l'Équipe psychosociale de rétablissement, sur le tard, et se questionnait sur la possibilité d'une réévaluation de son état de santé, car il n'avait pas présenté de demande de dédommagement plus tôt après la tragédie. « On travaille encore régulièrement dans la zone rouge, nous avons encore les images de la tragédie dans la tête, je la vis encore à tous les jours », a-t-il avoué. La Tribune, 4

*** Surveillance du fleuve - l'OMU sur un pied d'alerte**

L'Organisation des mesures d'urgence du Nouveau-Brunswick (OMU) a haussé d'un cran la surveillance des différents cours d'eau de la province en raison des températures chaudes et des averses enregistrées à travers la province au cours des derniers jours. Selon l'OMU, les températures prévues, combinées aux récentes précipitations, demeurent propices à la fonte de la neige accumulée et à une détérioration des glaces dans toutes les régions. Les débits et les niveaux d'eau devraient augmenter dans l'ensemble du bassin, et les risques de mouvement des glaces seront élevés le long du fleuve Saint-Jean, et dans les autres réseaux au cours des prochains jours, indique l'OMU. Toujours selon l'organisation, le mouvement des glaces pourrait provoquer des embâcles et ainsi causer des inondations. «On vient de franchir une autre étape dans la saison de surveillance du fleuve», admet Sheila Lagacé, porte-parole de l'organisation des mesures d'urgence. L'Acadie nouvelle, 8; Telegraph-Journal; CBC News

*** Resident fights to save home from flooding**

Of all the properties in the RM of Cupar dealing with spring flooding, Bill McCallum's has been hit the hardest. McCallum, who has lived in the area for 21 years, is now doing everything he can to keep the water from reaching his house alongside Highway 6 just south of the town of Southey. Clay has been brought in to build berms all around the home, and an additional line of sandbags has been put in place - but some of the damage has already been done, and the water is four feet deep in one area outside the temporary wall surrounding his home. "I own out to that north tree line," McCallum said, pointing to a group of trees a few feet away from his house. "We're going to wind up, I suspect, with that entire tree line gone ... It's kind of devastating, actually." Around him, bulldozers moved dirt and clay to increase the height of the berms surrounding his land from five feet to seven feet. "Hopefully it will remain safe, but we don't know at this point," he said. Most of the flooding is occurring along a 50-kilometre stretch of Highway 22 from Earl Grey to Dysart. Star-Phoenix, B6

*** Spill response not 'world class'**

An opinion piece states "When is an oil spill not merely an oil spill? When it happens in English Bay, that's when. The debacle last week in Vancouver's harbour, caused by a foreign grain carrier, will have huge implications for billions of dollars in proposed pipeline investments as well as Ottawa's strategy for exporting the country's energy resources. The future of the Northern Gateway pipeline and expansion of the Trans Mountain line depend on their respective sponsoring companies gaining social licence for such infrastructure, which was elusive even before the MV Marathassa spewed bunker fuel into the waters

around Vancouver. The mishap occurred next to an urban area that is action central for this country's environmental movement. B.C. is home base for a huge posse of environmental activists and the only province that has elected Green party politicians. It is a place where seabirds and wildlife have exalted status, and where livability is king... With so much riding on British Columbians having confidence in both industry and government to be prepared and fully equipped for an oil spill, it is unfortunate that last week's accident caught all parties with their pants down. The public, for the most part, has no idea about respectable emergency response times and practices for an oil spill, so it was left to authorities to put on a competent, co-ordinated and reassuring display. Everyone has known for some time how much is riding on such a professional response. And while it might be a challenge to demonstrate alacrity and efficiency on a remote stretch of B.C. coastline, a quick and able response would be absolutely expected right in Vancouver's harbour. Yet the feds, the province and the city of Vancouver blew it, in unison." Vancouver Sun (Calgary Herald, C4)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Deux jeunes arrêtés

Deux jeunes ont été arrêtés à Montréal par la police canadienne qui craignait qu'ils ne commettent une infraction liée au "terrorisme", a annoncé mercredi la chaîne publique Radio-Canada. El Mahdi Jamali, jeune homme de 18 ans, et Sabrine Djaermane, elle aussi du même âge, ont été incarcérés à la suite de l'opposition du ministère public à leur remise en liberté. La Gendarmerie royale du Canada n'a pas dévoilé les motifs de leur arrestation, mais l'enquête se poursuit et pourrait mener à leur inculpation. La GRC "craint qu'ils ne commettent une infraction liée au terrorisme", a rapporté la radio-TV publique canadienne sur son site. Selon la chaîne, El Mahdi Jamali et Sabrine Djaermane étudient au Collège de Maisonneuve à Montréal. C'est ce même lycée que fréquentaient cinq des sept jeunes, issus de la seconde génération de l'immigration, qui ont embarqué ces derniers mois pour Istanbul afin de rallier les combattants du groupe État islamique en Syrie, selon les témoignages de certains parents. Une responsable de l'institution scolaire n'a pas été en mesure de confirmer si les jeunes se connaissaient. Le Quotidien, 36; La Presse (Le Soleil, Le Nouvelliste, La Voix de l'Est, Le Devoir); Journal de Montréal (Journal de Québec) Toronto Star

Slamming the door on the snoopers

The first thing revealed by U.S. National Security Agency (NSA) contractor-turned-whistle blower Edward Snowden was a government program that collects records of every single phone call made in the United States. That program could soon come to an end, unless both houses of Congress vote to reauthorize Section 215 of the Patriot Act before the June 1 deadline. But given that we now know the U.S. government, and its "Five Eyes" allies (including Canada), have also been vacuuming up just about every piece of information that's sent over the Internet, allowing Sec. 215 to expire will barely make a dent in the massive surveillance state that Snowden revealed. Interestingly, recent polling data suggests that people have changed their online behaviour after learning that Big Brother is watching everything they do. Y et most people have still not adopted the technologies that would actually prevent governments from spying on them. According to a recent poll conducted by Amnesty International, 19 per cent of Canadians, and 21 per cent of Americans, say they are less likely to search for "personally sensitive or confidential information" online, since they learned about the surveillance programs. Another poll conducted by the Pew Research Center in the U.S. reveals that 25 per cent of those who were aware of the surveillance programs had changed the way they use computers and mobile phones. Others have taken some steps to increase the security of their online communications, such as using more secure passwords. National Post, A12

'Terrorism has no borders'

India's prime minister says last October's attack on Parliament Hill was a violation of a "temple" of democracy that was felt by free countries around the world. Narendra Modi made an impassioned plea for greater international co-operation in the fight against terrorism, standing next to Prime Minister Stephen Harper not far from the corridor where the attack took place. Modi called on the United Nations to use its 70th anniversary this year to adopt a draft treaty, several years in the works, which would formally criminalize terrorism, and deny access to money and weapons. Harper says Canada and India will

continue to deepen their partnership on matters of national security. Remarks about the Oct. 22 attack are becoming a regular feature for visiting foreign leaders after they and Harper stroll the Hall of Honour, where gunman Michael Zehaf Bibeau died in a hail of gunfire. The pair addressed the media in the grand Reading Room, the spot where the prime minister and his Conservative caucus took refuge while the gunfight raged outside the door. "We have been victims of this, and now the whole world is undergoing this, and everyone feels now that terrorism has no borders, it has no form," Modi said. "This attack on the temple of democracy was not just against Canada, it was an attack on human values. We have to come together, and we have to fight against terrorism." Cape Breton Post, A9 (Charlottetown Guardian, Times Colonist)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

American man to be deported again
An American man who has repeatedly snuck across the border into Canada is to be deported once again after being sentenced Wednesday in an Edmonton court. Giovanni Stoll, 33, was handed a nine month jail term, which was deemed already served by time spent in pre-trial custody, after pleading guilty to two offences under the Immigration and Refugee Protection Act (IRPA). Provincial Court Judge Donna Groves said it is frustrating that Stoll keeps sneaking across the Canadian border and she joked "tongue-in-cheek" that maybe a tracking chip should be implanted inside his body. Federal prosecutor Moira Vane told court that Stoll was nabbed by the RCMP while driving a stolen car in Evansburg, 100 km west of Edmonton, on Sept. 27, 2014. Court heard the Mounties contacted the Canada Border Services Agency (CBSA) and learned Stoll had actually been deported back to the U.S. from Quebec 11 days earlier and he was here yet again without being granted entry. Vane said Stoll's fourth deportation order was issued on Sept. 30, 2014, and the CBSA have been waiting for his court case to end so they can remove him back to the U.S. QMI Agency (Edmonton Sun, Calgary Sun)

Online pharmacy firm targeted by U.S. prosecutors
A mysterious RCMP raid, a secret court file and the latest in a string of multimillion-dollar convictions against U.S. doctors for buying its drugs have thrust a Canadian cross-border pharmacy back into the legal spotlight. The Mounties' recent search of Canada Drugs Ltd. offices comes two years after U.S. authorities accused the Winnipeg firm of organizing a shipment of fake cancer drugs south of the border. The bogus Avastin affair continues to reverberate, as the latest in a string of physicians prosecuted for buying it and other "misbranded" products from Canada Drugs was convicted this month. Robert Walker, a Joplin, Mo., oncologist paid $2 million in fines and restitution. Earlier, U.S. regulators prosecuted one of Canada Drugs' American associates for his part, seizing $4.5 million in land, cash and an Aston Martin sports car, calling the Montana resident a "predatory opportunist." U.S. authorities have never taken legal action against the Canadian company or its lowprofile owner, Kris Thorkelson. But it is almost certain the raid on Canada Drugs' premises last month stemmed from the cancer-drug affair, said Jim Dahl, a retired assistant director of the U.S. Food and Drug Administration (FDA) criminal investigations unit. "I don't think there's any question about it," said Dahl, a director of the pharmaceutical industry-funded Partnership for Safe Medicines. "Their entire business model ... is in violation of U.S. law." It wouldn't be the first time American officials have pursued a Manitoba-based Internet pharmacist, he noted. Andrew Strempler, who sold his RxNorth to Thorkelson, was jailed in 2013 for four years for marketing unapproved and allegedly counterfeit drugs to Americans. A Canada Drugs spokesman could not be reached for comment. The RCMP investigation is the latest twist for a surprising boom-and-bust industry that emerged on the Prairies in the early 2000s. By the middle of the past decade, Internet pharmacies based largely in Manitoba earned hundreds of millions a year, selling cheaper products to Americans, who face the world's highest prices for prescription drugs. The boom eventually waned, partly because of supply problems. Postmedia (Vancouver Sun, B2, Windsor Star, Leader-Post, Montreal Gazette, Calgary Herald, Ottawa Citizen, Edmonton Journal, National Post, The Province)

Accused fraudster denied bail
A man accused of defrauding a Regina business of more than $800,000 has been denied bail. Richard Dale Johnston launched a bail application at Regina Provincial Court last week. Judge Anna Crugnale-Reid reserved her decision until Wednesday, when she ordered the 55-year-old held in custody until his

charges are dealt with. Details of evidence heard at the hearing, as well as the reasons for the judge's decision, can't be reported because of a publication ban, which is routinely imposed at bail hearings. Johnston faces charges of fraud over $5,000, theft over $5,000 and laundering proceeds of crime. (…)Charges were officially laid last April, although Johnston was not immediately arrested since he was reportedly living in the Dominican Republic. An arrest warrant was issued and by working with Interpol, RCMP were able to obtain authorization that allows authorities to locate an accused person and secure an arrest for the purposes of extradition. Johnston was subsequently arrested by members of Interpol last month in the Puerto Plata area and deported back to Canada. Postmedia (Star Phoenix A7, Leader-Post)

U.S. officials, Royal Canadian Navy to announce details of record drug seizures from recent operation

A news conference is planned for Thursday morning in San Diego, California to outline the amount of drugs seized by U.S. Navy and Coast Guard vessels and Royal Canadian Navy ships. (…)Coast Guardsmen operating from cutters, U.S. Navy ships and Royal Canadian Navy coastal defence vessels have seized more than 56,000 pounds of cocaine worth over $848 million wholesale and apprehended more than 101 suspected smugglers making this the most successful fiscal year for counter drug operations in the Eastern Pacific since 2009. (The U.S. government's fiscal year runs from Oct. 1 to Sept. 30.) Numerous U.S. agencies from the Departments of Defense, Justice and Homeland Security are involved in the effort to combat transnational organized crime including the Coast Guard, U.S. Navy, Customs and Border Protection, FBI, DEA, ICE, U.S. Attorney's Offices in California, Florida and Puerto Rico, and U.S. intelligence agencies. The Royal Canadian Navy also continues to play an important role in counter drug operations. The fight against transnational organized crime networks in the Eastern Pacific requires interagency and international unity of effort in all phases from intelligence to detection and monitoring to interdiction and to prosecution. Ottawa Citizen

40 years since end of Vietnam War, U.S. draft dodgers left their mark in Canada

When 22-year-old Bill King returned home to Indiana in 1968 to visit his parents after a stint as Janis Joplin's music director, the FBI was there waiting for him. King's father, a Second World War veteran who landed at Normandy, helped negotiate a deal with the agents, who had been travelling around the United States looking for Vietnam War draft dodgers. "If I agreed to go in the military, (the FBI) agreed to drop the charges of draft evasion," King, 68, said in an interview from Toronto ahead of the 40th anniversary of the end of the war on April 30. King spent the next 10 months at two army bases before fleeing the night before he was to be sent off to Vietnam. He then hitchhiked to Canada, joining thousands of other draft dodgers between 1965 and 1975 who made the journey north of the border. While it is still unclear how many men and women sought sanctuary in Canada the country labelled draft dodgers as immigrants, as opposed to refugees the federal government estimates up to 40,000 made the journey. Most stayed after the war, "making up the largest, best-educated group this country ever received," says an archived report on the Citizenship and Immigration website. The Guardian

*** Teen forced into sex trade**

Two men are facing a string of charges following a human trafficking investigation in which police continue to look for a third suspect. Police say that a 17-yearold girl was allegedly forced into the sex trade and taken to hotels throughout the Greater Toronto Area where she was forced to work in the sex trade over about three months. Police say when the girl tried to dissociate herself from those people, they threatened her family's safety. Deshawn Holmes, 19, has been arrested and faces six charges that include trafficking in persons under 18 by exercising control, and criminal harassment. Nathan Turnbull, 19, has been arrested and faces four charges that include procuring a person under 18 years and uttering threats. Postmedia (Vancouver Sun, B7)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Cyberattaque au Conseil de recherches**

Le temps ne s'arrête pour personne, mais des pirates informatiques ont tenté mettre en panne le service du Conseil national de recherches (CNRC) qui synchronise les horloges des ordinateurs. Le service NTP, pour Network Time Protocol, ou protocole de diffusion du temps en réseau, du conseil fédéral a été visé

par deux attaques par déni de service distribué l'an dernier, révèlent des documents obtenus en vertu de la Loi sur l'accès à l'information. Une note interne blâme «les Chinois» pour au moins une des tentatives d'attaque. Ces attaques ont été révélées moins d'un an après que le CNRC a été victime d'une cyberintrusion qui a paralysé durant des mois le système de technologie de l'information principal de l'agence. Le Canada avait alors, pour une rare fois, blâmé un groupe hautement sophistiqué soutenu par l'État chinois d'avoir perpétré cette attaque en juillet 2014. Pékin a nié toute implication et reproché au Canada de faire des accusations irresponsables. Malgré cela, le Conseil national de recherches a tout de même relié l'attaque informatique de son horloge à la Chine. Presse canadienne (Le Droit, 16)

*** Governments must join fight against digital spying, think tank says**
An elite international group dedicated to preserving the Internet's free and unfettered qualities is calling for "a new global social compact" to counter the growing threats of digital spying and large-scale data theft. "It is now essential that governments, collaborating with all other stakeholders, take steps to build confidence that the right to privacy of all people is respected on the Internet," said a report released Wednesday by the Global Commission on Internet Governance, an independent body led by former Swedish prime minister Carl Bildt and whose members include former U.S. Homeland Security secretary Michael Chertoff and Angel Gurria, secretarygeneral of the Organization for Economic Co-operation and Development. The report by the commission - formed a year ago by two independent think tanks, Chatham House of Britain and Waterloo, Ont.-based Centre for International Governance Innovation - is intended to influence an ongoing global debate about how to counter the threats of an increasingly interconnected world. Data thieves have consistently kept ahead of companies and governments in fettering out confidential data, while government-sponsored cyberspying has been exposed as a widespread practice. Meanwhile, many individuals are still not heeding basic warnings for how to protect themselves online from data raiders. A report this week by Verizon Enterprise Solutions found nearly one in four people open "phishing" messages intended to trick them into revealing confidential information such as their passwords, while one in nine click on attachments inside the e-mails that can wreak havoc on their computer systems. Globe and Mail, B6

LAW ENFORCEMENT / APPLICATION DE LA LOI

Metro police swamped by gun calls
Several times each month, Codiac Regional RCMP respond in a "robust manner" to calls where someone thinks someone else is carrying a gun and a grudge. The spike in gun calls and the extraordinary police responses took root in the days following the murders of three Codiac members and the wounding of two others last June. And as long as the calls continue, a senior officer said Wednesday, police will respond to them in great numbers and with all of the resources at their disposal. "We have had, I would estimate, about 15 calls in the last three or four months where young people are walking the streets with either real guns or imitation guns," Insp. Jamie George told the monthly meeting of the Codiac Regional Policing Authority. The Mounties' responses to these calls have attracted a lot of attention in Metro Moncton, with neighbourhoods blockaded, police dogs brought in, most if not all officers on duty rushing to the scene clad in superior body armour and toting rifles or shotguns, all followed by a meticulous operation to bring the person of interest under police control until officers can sort out the situation. Only sometimes is a real firearm is involved, but as authority chairman Nick LeBlanc pointed out in an interview outside the meeting, that's never obvious to officers until after the fact. "So you have to (properly) answer every one of those calls," LeBlanc, a retired career officer, explained. The consequences of not doing so could prove ominous, he said, should the call turn out to be a disturbed individual with an agenda to create mayhem. Times & Transcript, A1

Ex-Saskatchewan police chief in running for Toronto's top job
A trailblazing former police chief from Saskatchewan is the wildcard contender to become Toronto's next chief, The Globe and Mail has learned. Dale McFee may not be a household name in Canada's largest city, but he is nationally recognized and respected in law enforcement. Four years ago, Mr. McFee transplanted a community-based policing model from Glasgow, Scotland, to his force in Prince Albert, Sask. The results have been dramatic, and the program is being replicated across the country - including in Toronto. A source with knowledge of the process said Mr. McFee is being offered as a viable

alternative to the current front-runners, Toronto's Deputy Chief Peter Sloly and Deputy Chief Mark Saunders. Mr. McFee retired from the Prince Albert force to become Saskatchewan's deputy minister of corrections and policing in 2012. He is a past president of the Canadian Association of Chiefs of Police, president of a WHL team and a Métis with strong support in the aboriginal community. That backstory has intrigued Toronto's seven-member civilian oversight board. Chief Bill Blair's contract is up at the end of next week. About half a dozen contenders have been interviewed, and the board hopes to name a successor before the chief's departure. Globe and Mail, A1

NDP wants Dunphy inquiry

Don Dunphy's daughter supports a call for a commission of inquiry into the death of her father, lawyer Erin Breen said Wednesday afternoon. Breen has been representing the Dunphy family after the 59-year-old Mitchells Brook resident was shot in his home by an RNC officer on Easter Sunday. The officer was investigating a perceived threat based on something Dunphy posted on Twitter two days earlier. According to the RCMP, which is investigating the matter, after the RNC officer was invited into the home, Dunphy became agitated and pointed a rifle at the officer, and the RNC officer shot and killed Dunphy. In the 10 days since the shooting, calls for some sort of inquiry have been mounting, and on Wednesday afternoon NDP Leader Earle McCurdy told reporters his party is calling on the government to initiate a commission of inquiry. Breen said Dunphy's daughter is generally supportive of that call, although up until now they're primarily focused on the criminal investigation being conducted by the RCMP. McCurdy said there are questions the police investigation simply cannot answer. "Among other things, it would need to look into the protocols and decision-making processes of the protective security unit, and the relationship between and among that unit, the premier's office, the RNC, the RCMP and the general public," McCurdy said. The Telegram, A1

11 charged in alleged Richmond dial-a-dope ring

Three men are being sought by Richmond RCMP under arrest warrants for their part in a 'dial-a-dope' drug distribution group busted by the detachment's organized crime unit. A total of 11 people were charged with multiple offences, including possession of a controlled substance for the purpose of trafficking and trafficking in a controlled substance. But still at large are: Andrew Weir, 30, of Surrey; Jason Requena-Hurlburt, 21, of Vancouver; and Geoffrey Ambridge, 30, of Calgary. Others charged as members of a drug line that operated in Richmond and Surrey, allegedly selling cocaine, heroin and methamphetamine, are: Patrick Befus, 39, of Victoria; Clay Sidney Crawford, 35, and Jo-Ann Spencer, 51, of Delta; Catherine Jane Pepper, 37, and Travis Pete, 24, of Richmond; and Surrey residents Ashneel Prasad, 30, Alvin Kumar Sharma, 37, and Christopher Lance Silva, 32. The eight-month investigation of the group began in June 2014. Police said deliveries of drugs were made throughout Richmond and Surrey, at locations ranging from residential neighbourhoods to shopping malls and other public venues. Search warrants were executed Jan. at two locations in Richmond and one in Surrey, with officers making eight arrests and seizing drugs packaged for street sale, a single-barrelled shotgun, about $56,000 in Canadian currency and three vehicles, one of which was equipped with a hidden compartment. Postmedia News (the Province)

Four arrested in drug bust near Markerville

Three men and a woman were arrested on Wednesday after police descended on a rural property near Markerville as part of a month-long drug operation. Led by the Priority Crimes Task Force, RCMP from Red Deer, Sylvan Lake and Innisfail detachments and other specialized units executed a search warrant at a property six km north of Markerville about 9 a.m. Police seized undisclosed quantities of drugs, firearms and stolen property during a search of the 130-acre property and various out buildings. RCMP officers remain on scene cataloguing and analyzing seized items. A witness said about 20 police vehicles, including an armoured vehicle, gathered early in the morning and tactical team officers wearing camouflage could be seen going into the property. "They were armed for bear these guys. There's no kidding about that." The property is a quarter section with a large house and several quonset buildings. It has been the scene of numerous suspicious comings and goings over the last couple of years, especially in the last few months. Police said more details on what and how much was seized and the scope of the investigation are expected to be released this afternoon. The names of the suspects and their charges have not yet been released. Priority Crimes Task Force includes officers from Red Deer RCMP general investigative section and Innisfail and Sylvan Lake detachments. Red Deer Advocate, A2

Man accused of posting child porn on Twitter
An 18-year-old Windsor male is facing multiple charges for allegedly uploading child pornography images to his Twitter account. Najm Najm has been charged with eight counts of unlawfully possessing child pornography, eight counts of making child pornography available, and eight counts of unlawfully accessing child pornography. Windsor police said their Internet Child Exploitation unit has been investigating Najm since February, after they were contacted by the RCMP's national co-ordination centre on child exploitation. The RCMP informed ICE members that someone in Windsor was allegedly posting child pornography images on a Twitter account. The ICE unit were eventually able to identify a suspect. The Windsor Star, A2

Tweet results in charge
Andrew Abbass says he is being charged with uttering threats by the RCMP. Abbass met with officers on Tuesday in relation to a post on his Twitter account last week that was seen as a potential threat. The post made on April 6, which was directed at Premier Paul Davis, said, "I'm going to bring down Confederation and have politicians executed. Ready to have me shot, coward?" The next day, he was visited by members of the Royal Newfoundland Constabulary (RNC) and subsequently detained at Western Memorial Regional Hospital under the Mental Health Care and Treatment Act. He was released on Monday, but maintains the detention was unlawful. The Telegram, A5

Man arrested in chase faces list of charges
A 24-year-old man accused of stealing a vehicle and leading police on a lengthy chase through Highlands and the Saanich Peninsula is facing a host of charges, including resisting arrest, assaulting a police officer and carrying a concealed weapon. Kenneth Johannes Donald Brens was arrested Tuesday after he allegedly stole a bright green Jeep Cherokee from a home on York Ridge Place in Highlands, then escaped as police tried to stop him. Four police departments - West Shore RCMP, Sidney/North Saanich RCMP and Saanich and Central Saanich police - were involved in the chase around Willis Point and Ross Durrance roads. Times Colonist, A4

Lacombe adds $400,000 to police station project
Lacombe city council has dipped into last year's surplus to cover a nearly $400,000 increase in cost of building a new police station. The city had set aside $8 million in its budget for the new facility. But after detailed design work was done, the bill came in at about $8.9 million. About $537,000 was trimmed by the police facility design committee and its architectural and cost consultants to leave $391,600 unfunded. On Monday night, city council approved transferring that amount from the surplus and to go ahead with tendering the station. Red Deer Advocate, C2

*** Yellowknife RCMP officer touts benefits of out-of-court system**
A Yellowknife RCMP member is touring various detachments in the N.W.T. to encourage other members to use an alternative method of policing, one designed to keep certain cases out of the court system and keep people from getting criminal records. "Charging offenders is not the only option out there," says Cpl. Jason Doucet, a restorative justice officer with the RCMP. "We should also be about second chances." Doucet is a practitioner of alternative justice, a system in which, in lieu of court proceedings, an offender meets a justice committee made up of residents from the offender's community. The committee members, as well as the victim, speak out about how the offender's crime has affected the community. Then the committee recommends a remedy for the offender, which can range from a letter of apology to community service. "Let them deal with the problems and some of the offences and try to find a result so that it doesn't happen anymore - that's the road we're onto," says Doucet. It's a system that Doucet admits has been met with some skepticism from other officers who fear offenders are being let off easy, and is not as well known among senior officers. But the method does not override the usual investigative process, Doucet stresses. "We have to investigate the matter right to the end, need to have enough information to take it to court before we can do a diversion," he says. "And the offender has to agree to the diversion process." CBC News

*** RCMP needs to be more visible, Codiac policing authority told**
A retired member of the the Codiac RCMP thinks more needs to be done to improve police visibility,

staffing, and transparency in the region. Terry McKee appeared in front of a monthly meeting of the Codiac Regional Policing Authority, which oversees policing in Moncton, Dieppe and Riverview. McKee used the five minutes allotted to him as a member of the public to detail issues he has with policing in the Codiac region. A lack of police visibility in the region is one of his concerns. "No one sees a patrol car in their neighbourhood, unless the police are tending to a call," said McKee, pointing out many people he knows have echoed his concerns. McKee said he thinks the lack of visibility is a result of inadequate staffing and that it gives people more opportunities to commit crimes. However, Moncton Coun. Charles Leger, who is a member of the policing authority, said that just because someone isn't seeing RCMP patrols, it doesn't mean they're not there. "I do believe there is a difference too as I mentioned between visually seeing something, versus not knowing whether or not a police vehicle for example was in my community," said Leger. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Coroner's inquest makes recommendations to Correctional Services Canada**
Nearly two years after an in-mate committed suicide at a BC prison, we're learning more about how his death may have been prevented. Jesse Lahn was serving time for kidnapping and armed robbery when he hanged himself in May of 2013. The 33-year old was only a few months shy of completing his sentence at Agassiz's Kent Institution. A three-day inquest in Burnaby has wrapped up with the coroner's jury making four non-binding recommendations to Correctional Services Canada. They include more frequent checks on prisoners, better designing cells to prevent hangings, improving mental health support and increased video surveillance. CKNW

Pointe-Claire pedophile has parole revoked
A Pointe-Claire man who was recently released to a halfway house while he continues to serve a 10-year sentence for sexually assaulting a young girl and posting images of the abuse on the Internet has been returned behind bars, in part because he corresponded with other pedophiles during his parole.
The Parole Board of Canada revoked Richard Reber's day parole after a recent hearing. According to a written summary of the decision, Reber was given warnings to be more transparent with his parole officers and to find a more positive social network before being returned to a penitentiary. (...) Within three weeks of his release, Reber visited a relative's home and three girls happened to be present at the same time. Nothing happened but one of the conditions Reber was ordered to follow required that he not be in the presence of minors unless they were accompanied by an adult aware of his criminal record and authorized by Correctional Service Canada. Montreal Gazette, A5

Cuts hurt victims and offenders
An editorial states, "When it comes to crime, the federal Conservatives have tried to carve out a moral high ground. Victims and public safety must be defended at all costs, they insist. Conservatives have championed mandatory minimums and made dozens of changes to the Criminal Code. Life should mean life, they've insisted, ignoring experts who worry about an inflexible, retributive justice system. That's why it's frustrating the feds quietly withdrew funding last month for Circles of Support and Accountability, a volunteer program targeting high-risk sex offenders released after their sentences expire. Studies have shown the model is remarkably effective. The latest federally commissioned evaluation estimates CoSA reduces rates of sexual offences by 92.8 per cent in the first three years, 74.5 per cent over five and 67 over 10 years. For every tax dollar invested, roughly $4.60 is saved in costs to emergency services and justice." Vancouver Sun, B8

Crash sends paroled murderer back to jail
A man sentenced to life in jail for shooting dead the flamboyant owner of the Penthouse strip club 32 years ago in one of Vancouver's most sensational murder cases has been sent back to jail after drinking alcohol and driving while impaired. Scott Forsyth, 56, was convicted of firstdegree murder and jailed in 1984 for shooting Joe Phillipponi, 70, in the head after drinking with him at the nightclub's Seymour Street office on Sept. 18, 1983. Forsyth had stolen $1,084 from the club's safe. At trial, he confessed and testified that Sid Morrisroe, a Burnaby plumber and close friend of Phillipponi, had hatched the murder and robbery plot and supplied the gun. The safe was supposed to contain $1 million. Morrisroe, now 80, who

has always maintained his innocence, was also convicted of first-degree murder and sentenced to life. He was released on full parole in 2002 after serving 19 years. The Province, A12

The Supremes got it right
A letter to the editor states, "Re: Supreme Court's Cunning Rejection, John Ivison, April 15. Yes, mandatory minimums are dumb because they don't deter crime but swell prison populations, especially for youth and minority groups. Our Supremes did the right thing, but unfortunately, the hypothetical example they used was weak. After all, Prime Minister Stephen Harper has granted repeated amnesties to long-gun owners who failed to renew their licences or to register all their weapons, even the owners of semi-automatic rifles, and advised such remiss gun owners to graduate up to restricted gun licences." National Post, A11

* **The Supremes got it right**
A letter to the editor from former MP Inky Mark states, "I've been preaching the same sermon for many years - C-68 criminalizes the lawful gun owner. Harper has broken his election promise to repeal this law many times. Therefore, he sees lawful gun owners as criminals in waiting, and refuses to change the breach of law from felon to misdemeanour. It is cruel and unusual punishment to treat law-abiding gun owners as criminals. Under Section 92 of the Criminal Code, if your paper possession licence is not valid and you are in possession of a gun of any type, you are deemed a felon and have broken the law. The penalty for such a breach could land you in jail for up to 10 years. Lawful gun owners pose zero danger to the public. If this isn't cruel and unusual, then what is?" National Post, A11

Gun ruling misses mark
An editorial states, "Once again, when it comes to gun issues, it feels like the good guys are the villains and the bad guys are the victims. Responsible gun owners are getting sick of it. Heck, average Canadians in general are sick of it. On Tuesday the Supreme Court of Canada ruled that mandatory minimum sentences for gun possession are unconstitutional. The Conservatives instituted a new law that provides a three-year sentence for anyone convicted of unlawfully possessing a prohibited or restricted gun that's loaded or for which ammunition is lying around nearby. That rolls up to a five-year sentence for repeat offenders. Basically, it's a way to lock up the thugs who keep illegal guns handy. Aren't those the people we want to target?" QMI Agency (Ottawa Sun, 14, Toronto Sun, Winnipeg Sun, Calgary Sun)

* **'Judicial activism' isn't killing Harper's crime agenda - Harper is**
An opinion piece states, "If a foolish consistency is the hobgoblin of small minds, the Harper government has been very, very consistent - at least when it comes to crime. The federal Conservatives have reduced criminal justice policy to a simple flow chart. Step one: Promise 'tough on crime' legislation that's easy to sell to the Conservative base. Step two: Table the bill while ignoring the advice of experts (both inside and outside the Justice department) arguing the new law would be both ineffectual *and* unconstitutional. Step three: Cling like grim death to the talking points, at least until step four - when the Supreme Court strikes the law down. Step five: Cry 'judicial activism', then refer to step one. The pattern is always the same; only the bills change. The results speak for themselves - for the Harper government, one defeat after another in the nation's highest court. They've been in power since 2006. They really should be getting better at this by now. This week, the SCC struck down a 2008 law that imposed mandatory minimum sentences for the unlicensed possession of prohibited or restricted firearms." iPolitics

* **Targeting gun law**
A letter to the editor states, "When clearing my late mother's house, I came across an army officer's 45-calibre six-shooter revolver, complete with ammunition, from the Second World War. When I told our daughter, a Crown prosecutor, that I planned to take it to our local police station for disposal, she insisted that I not dare exit the house with it, but instead immediately tell the police and ask them to collect it. She explained that carrying the unlicensed gun in public could well result in a lengthy visit to a prison. After a call to the police, two very polite officers very promptly arrived at our front door and departed with the gun and bullets, leaving me behind I'm pleased to say. So I was relieved our Supreme Court has struck down mandatory minimum sentences for gun possession, such that carrying an army six-shooter to the police for disposal would no longer risk an automatic jail term." Globe and Mail, A16

*** Supreme Court did its job killing a sloppy law**
A letter to the editor states, "In typical fashion, some Canadians are reacting with outrage to the Supreme Court's decision striking down the Harper government's mandatory minimum sentencing law relating to gun crimes. The critics should be thanking the top court. Left alone, the badly crafted legislation could ensnare lawful gun owners or those who commit minor infractions such as allowing a licence to lapse. They may have broken the law but they're not armed robbers, gangsters or drug dealers. This legislation was sloppy and deserved to be shot down." Hamilton Spectator, A12

*** Time to concede to charter's trump**
An editorial states, "In yet another monumental slap-down to the Harper government's law-and-order agenda, the Supreme Court has ruled the government's mandatory minimum sentences for gun crimes are unconstitutional. Slapping three- or five-year terms on anyone who transgresses firearm laws risks unfairly, cruelly penalizing some, the court said. It was a clear message to the Tories, who have a penchant for minimum sentences, it's time to curb the enthusiasm for laws that trample core rights in this country." Winnipeg Free Press

*** Unconstitutional mandatory minimums and the role of pandering progressive politicians**
An opinion piece states, "In the wake of the great news that the Supreme Court had ruled that the gun related mandatory minimum sentencing provisions of the Tackling Violent Crime Act were unconstitutional, the decision was widely heralded as a blow to the Harper government's reactionary "get-tough-on-crime": agenda by both the media and progressives. And it is. But it is also a lesson in how reactionary agendas are often built with the aid of pandering "progressives" who capitulate to these narratives out of what are purely cynical and crass electoral considerations." Rabble.ca

Inmate dies at Stony Mountain Institution
A 32-year-old inmate serving time at Stony Mountain Institution for sexual assault and sexual interference has died. Prison officials said Dwayne Mervin Flett was found unresponsive in a living unit at the medium-security jail. Prison staff immediately began performing CPR on Flett upon his discovery and emergency services were called, but prison officials said he could not be resuscitated. Flett had been servince a nearly five-year sentence since May 31, 2011, for sexual assault and sexual interference. Prison officials did not release the cause of death. Winnipeg Sun

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Valley police appeal to community leaders to help quell violence
Police are appealing to Fraser Valley ethnic community leaders and families in an attempt to deal with a new wave of criminalized youth committing acts of violence and turning to the drug trade. Both Surrey RCMP and Abbotsford police have taken the unusual step of issuing public warnings and releasing photographs of some of those involved in an effort to stem the violence. There was more gunfire in Surrey early Wednesday that RCMP believe may be part of the conflict between two groups of young drug dealers of South Asian and Somali descent who have been involved in 20 shootings in the past six weeks. And Abbotsford police are concerned that local gangsters have recruited young men involved in a petty dispute which over several months has escalated to a more serious level of criminality. Abbotsford police co-hosted a forum with the local school board Wednesday night for Punjabi-speaking parents to warn of the risk of gang recruitment in the city. Const. Ian MacDonald said the problem has grown since police first intervened last year between two feuding groups of youth. "It started pretty low-end with property damage, mischief, that sort of thing and then has been escalating to the point where we've got shots fired, stabbings, pretty serious incidents," Mac-Donald said Wednesday. "And now what we've seen over the last few months - which is what we feared - is recruitment of young South Asian men, in particular, into gang lifestyle." ... The Abbotsford forum came a day after Surrey RCMP and Delta police released another eight photographs of young men involved in the conflict who are refusing to cooperate with police even after they've been shot. One of those men contacted The Sun Wednesday, claiming he was being unfairly treated by police and wanted to be interviewed. But he failed to show up at the scheduled meeting. Postmedia News (Vancouver Sun, A1, Edmonton Journal)

Shooting in Surrey fits pattern
Police say public safety is their top concern after another shooting in Surrey, hours after officers revealed that gang rivalry prompted similar incidents. Surrey RCMP received several calls about 1 a.m. Wednesday from witnesses who saw occupants of a red pickup and a grey SUV shooting at each other while driving westbound near a secondary school. Cpl. Bert Paquet said it's too early to say whether the shooting is linked to a recent spate of gunfire in Surrey and nearby Delta, but it's certainly along the same lines. "It's very fortunate that there have been no injuries suffered by innocent bystanders," he said. Mounties said a turf war between groups of people of South Asian and Somali descent is responsible for 11 of the 19 shootings that have unleashed bullets into homes and vehicles in the region east of Vancouver. No one has died in the shootings. Paquet said there were no reports of injuries from the latest round of gunfire and officers are still looking for the vehicles involved. About 12 hours before Wednesday's shooting, Surrey RCMP released the names and photos of victims in some of the shootings. None of the victims is co-operating with police. Police have arrested one person, Delta resident Arman Dhatt, and charged him with 12 firearms and drug trafficking offences. Canadian Press (Times Colonist, A7, The Province, National Post)

Youth, Police hash it out
Students from all across Regina gathered Wednesday to find solutions for some of the issues they're facing every day. Chelsea Almojuela, a Grade 12 student, was one of the 80 attending the Speak Out Regina youth forum at the Campus Regina Public. She said she was excited to be there and share her ideas on how to make schools in the city better. "The school is a really safe place," she said. "It's actually fun and more studying and pursuing your goals or dreams in your life." Still, she admits she has seen bullying take place at her school and it isn't always a stress-free place. "Right now I'm experiencing pressure because I'm going to university (and applying)," she said. Students were given an opportunity to ask questions to representatives from the city, province, school boards and police. Students bravely approached a microphone in a room full of their peers to ask questions such as: "How are schools planning to explore self-identity and help students feel more comfortable with themselves?" and "How are schools dealing with gangs?" Some students raised concerns over how some schools had better reputations than others, while others wanted to know what was being done to help students with mental illnesses. Postmedia News (Calgary Herald, A16, Leader-Post)

*** True crimes, faulty statistics and Aboriginal women**
An opinion piece states, "How the heck did Bernard Valcourt get himself into a fix like this? In a March 20 closed-door meeting with a group of western First Nations band and region chiefs, the federal Aboriginal affairs minister apparently got defensive when the issue of missing and murdered Aboriginal women came up. Valcourt pointed out that an estimated 70 per cent of murders of indigenous women are perpetrated by indigenous men. The chiefs knew that there was no such finding in the RCMP's "operational overview" of the topic issued last year. It was, indeed, a noticeable gap in the report. The RCMP had strongly disavowed any ability or desire to make factual assertions about the racial demographics of a subset of murderers. So the chiefs very understandably asked Valcourt where this number had come from, and the minister was left babbling that he would come up with something. Whatever goodwill had been present in the room was gone. A cynic would say Valcourt had committed a breach of the delicate manners that prevail in face-to-face talks between a minister and the leadership of his clientele. It would be equally valid to say he had failed to show sufficient respect." Maclean's

*** 'Relationships' program for new arrivals could include all NBers**
Let`s talk about healthy relationships and avoid abusive ones. I recently had the opportunity to learn more about a project led by Centre d'accueil et d'accompagnement francophone des immigrants du sud-est (CAFi). This is the 'immigrant settling' service for francophone immigrants arriving in South-East New Brunswick. It's called 'engager les hommes et les garçons à la promotion des relations saines,' or in English 'involving men and boys in the promotion of healthy relationships.' This initiative, which began in February 2013 and was funded by Status of Women Canada, aims to educate and involve men and boys in promoting healthy relationships dynamics between men and women as well as between boys and girls. This project recognizes and tries to address some of the root causes of unhealthy gender dynamics in

relationships that can lead to violence. It makes men and boys part of the solution, discussing, debating and mentoring other men towards healthier relationships. Times & Transcript, A11

*** Crimes decrease in Chatham-Kent**
Chatham-Kent's crime statistics are experiencing a downward trend overall, the police board has been told. Among the numbers for 2014, there were zero murders; one attempted murder, which is up from zero in 2013; 59 sexual assaults, down from 65; 374 assaults, down from 403; 19 robberies, down from 26; 24 weapons cases, down from 37. Criminal harassment cases dropped to 52 from 135. London Free Press, A6

PUBLIC SERVICE / FONCTION PUBLIQUE

L'AFPC lance un message en prévision des élections fédérales de 2015
L'Alliance de la fonction publique du Canada (AFPC) vient de publier une liste de huit enjeux qui devraient influencer le vote de ses 175000 membres, leur rappelant que les élections fédérales de 2015 donnent «une excellente occasion de remettre le pays sur la bonne voie». «Lorsque vous irez voter cette année, n'oubliez pas les compressions imposées par le gouvernement conservateur à nos précieux services publics», lit-on sur le site de l'AFPC. «Il y a eu tellement d'attaques, qu'on ne pourrait pas toutes les nommer. Mais il y a un consensus au niveau syndical à travers le pays. Il n'est pas question de maintenir la tendance» explique Larry Rousseau, vice-président exécutif de l'AFPC pour la région de la capitale nationale. Son syndicat n'a pas l'intention de dire à ses membres comment voter. «Nos membres sont assez intelligents pour tirer la bonne conclusion. On entend ad nauseam que les syndicats disent à leurs membres quoi faire. Mais ce que nous faisons, c'est informer nos membres», a nuancé le dirigeant syndical. Les huit enjeux touchent l'abolition d'emplois et les compressions dans les services publics, les services de garde d'enfants, les modifications à l'assurance emploi, la sécurité de la retraite, les soins de santé, les droits de la personne, l'environnement et les anciens combattants. Le Droit, 31

*** The public's right to know more**
When Canada's Information Commissioner Suzanne Legault tabled her most recent report in Parliament, she must have figured it would be unlikely to be acted upon in the final run of this government. That's in part because we're at a point in the life of this government where it's now a near certainty that no new legislation or law amendment is likely to progress through Parliament that hasn't been promised by the Stephen Harper Conservatives. It's also because this government has demonstrated a lack of commitment to broadening Canada's Access to Information Laws, which Legault was recommending in her latest report, issued last month. In fact, the Harper government's track record on even fostering a greater spirit of access to government information has been awful. This is a government, after all, that pulls things like no-questions-permitted media events such as the one this week in which it disclosed that Canada would be sending military trainers into Ukraine. It's a government that refers Canadians seeking information to try to obtain it through Access to Information requests - seemingly as a matter of policy. Then, it handles those requests in such a way that sees sky-high rates of formal complaints being filed. The complaints are over such things as delays in releasing materials, fees being charged, purportedly unreasonable requests for time extensions and alleged abuse of the exclusion granted to materials deemed "confidential advice to cabinet." Finally, it has impaired the Information Commissioner's ability to handle these complaints by reducing that person's budget by more than 10 per cent. Waterloo Region Record, A12

OTHER / AUTRE

*** Canadian detained at Cairo airport**
After 558 days in a Cairo jail and three months anxiously awaiting papers that would allow his exit from Egypt, Canadian resident Khaled Al -Qazzaz thought he was flying home to Toronto Thursday. "We have our passports, our clearances and we're trying not to look back, only forward. We want to get our lives

back together," his wife, Sarah Attia, said in a phone interview from Cairo Wednesday. Instead, the family's dream of going home turned into an airport nightmare. When Al-Qazzaz, his wife Sarah Attia and four children aged 4 to 8 arrived at the Cairo airport later in the day, they were stopped by the airport security services, barred from leaving the country, and held without explanation. Toronto Star, A18

INTERNATIONAL / INTERNATIONAL

NIL

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
January 27, 2015 / le 27 janvier 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Did Stephen Harper just find his Falklands moment?
An opinion piece statess, "In 1982, the Conservative government of British Prime Minister Margaret Thatcher was in trouble. Three million Britons - one in every eight workers - were out of work. Manufacturing firms shut their doors and the economy slid into a deep recession. Trade unions demanded wage increases and engaged in acts of violence. Critics, including members of Thatcher's own party, accused the PM of being obsessed with cutting public spending instead of supporting ailing industries. Her party was trailing in the polls, an election was looming, and most pundits predicted Thatcher and the Tories would be out of government before long. [...] In response, the office of **Public Safety Minister Stephen Blaney** issued this statement: "***The international jihadist movement has declared war on Canada and our Allies ... No Canadian government should ever stand on the sidelines while our Allies act to deny terrorists a safe haven - an international base - from which they would plot violence against us.***" The remarks echo those issued by Harper after the terrorist attacks on Charlie Hebdo in Paris: "The international jihadist movement has declared war. They have declared war on anybody who does not think and act exactly as they wish they would think and act ... They have declared war on any country like ourselves that values freedom, openness and tolerance." Ipolitics.ca

' Alberta Mountie's sister urges mourners to live life to fullest
The sister of an Alberta Mountie told mourners at his funeral Monday that he would want them to live life the way he did - with joy, with passion and with every effort to make the world a better place. "Over the past 10 days, there has been such an outpouring of stories about Dave and obvious love for him from the

people that he has touched that I have realized he was far more than I ever imagined," Mona Wynn said in her eulogy before thousands at a recreation centre in St. Albert, Alta. "Dave was an ordinary man with an extraordinary capacity to make the world a better place for everyone around him." Const. David Wynn, 42, died last Wednesday, four days after he and auxiliary Const. Derek Bond were shot during a struggle with a suspected car thief at a casino in St. Albert. He was shot in the head and never regained consciousness before he died. An RCMP officer lays the hat of slain RCMP Constable David Wynn, on his casket during his funeral in St. Albert. The shooter, career criminal Shawn Rehn, killed himself hours later. Prime Minister Stephen Harper, left to right, Public Safety Minister Steven Blaney and Health Minister Rona Ambrose attend the funeral for slain RCMP Constable David Wynn, in St. Albert, Alta. Canada.com

Militant calls for attacks on Canadians
Three months after attackers espousing Islamist extremist beliefs killed two Canadian Forces members, Islamic State held them up as role models on Monday in a speech that called for more killings in western countries. In a nine-minute audio clip distributed on Twitter, Islamic State spokesman Abu Muhammad al-Adnani once again urged his followers to attack Canadians over the government's decision to join the anti-Islamic State military coalition. The release came shortly before the Armed Forces acknowledged that Canadian special forces had engaged in two more gun battles against Islamic State. Canadian CF-18s also destroyed Islamic State "fighting positions" on Saturday and Sunday. An apparent attempt to rally his fighters and weaken western resolve, Adnani's speech referred to attacks in Canada, including the Oct. 22 shootings on Parliament Hill, and warned that "what lies ahead will be worse - with Allah's permission." He encouraged extremists in Europe and other "disbelieving" western countries to "target the crusaders in their own lands and wherever they are found." He said to use explosives, guns, knives, cars, rocks "or even a boot or a fist." [...] Asked about Adnani's threat, **Public Safety Minister Steven Blaney** confirmed the government would put legislation before Parliament on Friday that would, among other things, criminalize the promotion of terrorism. "***The international jihadist movement has declared war on Canada and our allies***," said **Blaney**. Postmedia News, A1 (National Post, Calgary Herald, Edmonton Journal, Leader-Post, Vancouver Sun, Montreal Gazette, StarPhoenix, The Province)

Le tireur d'Ottawa glorifié par les djihadistes dans un enregistrement
Un porte-parole du groupe armé État islamique (EI) a glorifié le tireur qui a tué un soldat au Monument commémoratif de guerre du Canada, à Ottawa, en octobre dernier. Dans un enregistrement audio d'une durée de neuf minutes publié hier, Abou Mohammed Al-Adnani a couvert d'éloges les auteurs des récentes attaques en Australie, en Belgique, en France et au Canada. Michael Zehaf Bibeau avait abattu un soldat, avant de se rendre à l'édifice du Centre du Parlement, où il était tombé sous les balles des forces de sécurité. Le porte-parole du groupe extrémiste a encouragé ses auditeurs à prendre exemple sur celui qui s'est attaqué à ce «parlement infidèle», selon lui. Les événements d'Ottawa étaient survenus seulement deux jours après qu'un autre homme ayant des liens avec les djihadistes, Martin Rouleau-Couture, eut tué l'adjudant Patrick Vincent, à Saint-Jean-sur-Richelieu. [...] Réagissant à ce message du groupe EI, le **ministre de la Sécurité publique**, **Steven Blaney**, a affirmé que le mouvement djihadiste international avait déclaré la guerre au Canada et à ses alliés, et que c'est pourquoi le gouvernement avait décidé de participer à la coalition aérienne. Le ministre a aussi mentionné les projets de loi du gouvernement contre «***la promotion du terrorisme***». Le Soleil, 18 (Le Nouvelliste, La Voix de l'Est, La Tribune)

Blaney condamne Les nouvelles menaces de l'ei
Le **ministre de la Sécurité publique**, **Steven Blaney**, a condamné hier les nouvelles menaces du groupe armé État islamique proférées contre l'Occident. Dans un message audio mis en ligne hier, les djihadistes de l'EI appellent leurs partisans en Europe et en Occident à cibler des Occidentaux en se servant de n'importe quelle arme, "que ce soit une bombe artisanale, des balles, un couteau, une voiture piégée, ou le poing", a rapporté l'agence Reuters. Ils ont aussi salué les attentats perpétrés au Canada, en France, en Australie et en Belgique. "Vous n'avez encore rien vu", a prévenu Abou Mohammad al-Adnani, porte-parole de l'EI, dans le message audio, a indiqué l'AFP. Le gouvernement conservateur déposera vendredi aux Communes un projet de loi visant à accroître les pouvoirs des autorités en leur offrant de meilleurs outils pour traquer et stopper les terroristes. Journal de Montréal, 22

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** PREMIER CAS CONFIRMÉ EN COLOMBIE-BRITANNIQUE**
Une femme de Colombie-Britannique a reçu un diagnostic de grippe aviaire H7N9. Elle aurait contracté le virus lors d'un séjour en Chine, dont elle est revenue le 12 janvier dernier, a fait savoir la ministre de la Santé, Rona Ambrose, par voie de communiqué hier. La femme serait hors de danger et récupérerait chez elle, en isolement volontaire. Il n'a pas été nécessaire de l'hospitaliser. Les contacts étroits de la personne ont été identifiés, et leur santé est suivie par les autorités provinciales de santé publique. C'est le premier cas de virus de grippe aviaire de ce type recensé en Amérique du Nord. Selon l'Agence de la santé publique du Canada, le virus H7N9 ne se transmet pas entre humains. Une personne peut cependant le contracter lorsqu'elle entre en contact avec des volailles d'élevage ou sauvages. Journal de Québec, 22 ; Agence France-Presse (Le Nouvelliste, 23) ; Presse Canadienne (La Presse, A10; Voix de l'Est, 20) ; Canadian Press (Hamilton Spectator, A8; Red Deer Advocate, A6; Charlottetown Guardian, A5); Postmedia News (National Post, A5; StarPhoenix, C8; Ottawa Citizen, C1); QMI Agency (Edmonton Sun, 22; Ottawa Sun, 10)

*** « Ce n'est pas une tempête typique »**
Vols suspendus, spectacles annulés, transports en commun arrêtés au moins pour la nuit, New York tournait au ralenti hier soir, frappée par une tempête de neige accompagnée de vents violents affectant des millions d'Américains dans le nord-est des États-Unis.La neige tombait dru hier soir à New York où des centaines de chasse-neige étaient mobilisés contre le blizzard. Le maire Bill de Blasio a appelé la population à sortir le moins possible, et a interdit la circulation de tous les véhicules - sauf véhicules d'urgence - à partir de 23 h, une mesure rarissime. Selon la météo nationale, on prévoyait que la neige tombe durant la nuit au rythme de 5 à 10 cm par heure, avec une accumulation attendue de 60 cm à New York, voire plus en certains endroits, et des bourrasques de 72 à 88 km/heure. « La tempête va s'aggraver durant la nuit », avait annoncé en fin d'après-midi le gouverneur de l'État de New York Andrew Cuomo. Il a annoncé la fermeture du métro, qui fonctionne à New York 24 heures sur 24, à partir de 23 h, pour une durée indéterminée. Agence France-Presse (Voix de l'Est, 2 ; Le Nouvelliste, 10) ; Associated Press (Le Droit, 5 ; Charlottetown Guardian, B4; Chronicle Herald, A14; Hamilton Spectator, A1; National Post, A14; Red Deer Advocate, D3)

*** L'Acadie se prépare à affronter le blizzard**
Une combinaison d'abondantes chutes de neige, de vents de 70 à 90 km/h et une visibilité réduite vont compliquer la vie des Néo-Brunswickois au cours des prochains jours alors qu'une importante tempête hivernale devrait frapper le Nouveau-Brunswick mardi. Selon les avis de blizzard émis lundi matin par Environnement Canada, des accumulations de 15 à 30 centimètres de neige sont attendues sur une large partie de la province. Le tout sera accompagné de forts vents. Ces avis épargnent, pour l'heure, le Nord-Ouest et le Restigouche. L'Acadie Nouvelle, 3

*** Two Vancouver flights cancelled due to eastern storm**
Just two flights from Vancouver were cancelled Monday due to a winter storm that is walloping cities in the Maritimes as well as U.S. cities such as New York, Boston and Philadelphia. Chou said that on Monday, two flights were cancelled out of YVR: an Air Canada flight to Newark, N.J., Monday morning, and a Cathay Pacific flight Monday evening from Vancouver to New York. Vancouver Sun, A6

*** Des répercussions à l'aéroport d'Ottawa**
Une dizaine de vols en provenance ou à destination de New York et de Boston ont été annulés ou retardés à l'aéroport d'Ottawa, en raison d'une tempête de neige qui s'annonçait historique, hier, dans le nord-est des États-Unis. L'Outaouais et l'Est ontarien seront épargnés par ce système météorologique, alors que la région sera toujours frigorifiée, avec des températures atteignant les -27°C, avec le facteur éolien. Selon Environnement Canada, cette tempête ne touchera que les provinces maritimes. La Nouvelle-Écosse, le Nouveau-Brunswick et l'Ile-du-Prince-Édouard s'attendent à recevoir de 15 à 30cm avant que la neige se transforme en pluie dans certains secteurs, en soirée. Le Droit, 5 ; Ottawa Citizen, A3

*** Déneigement «made in USA»**
Des camions à ordures pour déneiger, des citoyens forcés de pelleter les trottoirs: les pratiques de déneigement diffèrent grandement aux États-Unis. Et si les tempêtes de neige y sont moins fréquentes qu'au nord de la frontière, elles sont aussi beaucoup moins coûteuses. Alors qu'une tempête s'annonçant historique souffle sur la côte est américaine, La Presse en profite pour dresser un portrait du déneigement «made in USA». Le déneigement pèse peu sur le budget des villes américaines. La Ville de New York dépense en moyenne à peine 7$ par habitant chaque hiver pour déneiger ses rues. La métropole américaine reçoit toutefois beaucoup moins de neige que Montréal, qui en reçoit près de quatre fois plus. Les quantités de neige tombant sur New York varient énormément d'une année à l'autre. En 2012, la Grosse Pomme avait reçu à peine 25 cm de neige. L'année précédente avait pourtant marqué un record avec des précipitations totalisant 152 cm. A Montréal, il tombe rarement moins de 150 cm. La Presse, A3

*** Island in store for 'long, painful' blizzard**
It was inevitable. A blizzard warning is in effect for Prince Edward Island today as Islanders get set for the first real big blast of winter. Environment Canada's Linda Libby said Monday the system was moving in the Maritimes a lot faster than they thought it would. "It's going to be a long, slow, painful kind of storm," Libby said. Snow is expected to be heavy at times, beginning between 4 a.m. and 6 a.m. today. Charlottetown Guardian, A1; Daily Gleaner, A1; Telegraph-Journal, A1

*** Hydro-Québec envoie 180 employés à Boston**
Hydro-Québec a envoyé près de 180 employés dans la région de Boston afin de donner un coup de main aux équipes américaines qui se préparent à affronter une tempête hivernale possiblement historique. La société d'État a indiqué que la demande était venue de la société américaine National Grid. Les 150 monteurs ainsi que des membres du personnel logistique et technique sont en route vers la grande région de Boston, où les équipes et les véhicules seront déployés. L'aide accordée est prévue par le North Atlantic Mutual Assistance Group, un groupe de collaboration dont fait partie Hydro-Québec. La société d'État avait également envoyé des équipes aux États-Unis en novembre 2014, lors d'une autre importante tempête sur la côte Est. Un avertissement de blizzard a été lancé pour une section d'environ 400 kilomètres du nord-est des États-Unis, et les météorologues affirment que la tempête pourrait laisser de 60 à 90 centimètres de neige dans la région allant du New Jersey au Connecticut. Presse Canadienne (Voix de l'Est, 2)

*** Des pertes de 250 M$ par jour**
Les tempêtes de neige ne font pas qu'entraîner la grogne. Elles coûtent 250 millions $ us à l'économie locale. Dans une étude sur l'impact économique d'un phénomène météo, la société de recherche IHS Global Insight a compilé des données sur la côte est américaine en incluant le Québec et l'Ontario, en raison de leur climat. Le Québec voit ainsi un 250 millions $ d'activité économique directe et indirecte disparaître lors d'une tempête, en raison des déplacements limités et des fermetures temporaires. Agence QMI (Journal de Québec, 51 ; Journal de Montréal, 35)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

ISIL praises attack on Parliament Hill
The spokesperson for the Islamic State group has praised the man who killed a Canadian soldier at the National War Memorial in October and is calling on Muslims living in western countries to carry out attacks. The spokesperson says any loyalist who has the opportunity to "shed a drop of blood" should do so. Abu Mohammed al-Adnani, in a nine-minute audio recording released Monday, praised recent attacks in Australia, Belgium and France - where 12 people were shot and killed in the Paris office of Charlie Hebdo magazine. He also praised the man who killed an unarmed sentry at the War Memorial in Ottawa on Oct. 22 and then stormed the Parliament Hill's Centre Block before being killed by security forces, saying: "You all saw what one Muslim did in Canada and its infidel parliament." Michael Zehaf Bibeau's killing of Cpl. Nathan Cirillo came just two days after another attack by a man with known jihadist sympathies who ran down a soldier in Quebec, Warrant Officer Patrice Vincent. The attacks ignited a debate on homegrown terrorism in Canada. The Canadian government is expected to introduce

legislation soon to crack down on suspected terrorists and those who openly encourage them. Waterloo Region Record.com (Charlottetown Guardian, Toronto Star, Times&Transcript, Times Colonist)

Canadians urged to join fight against fundamentalism
When she heard there had been a shooting at the satirical French magazine Charlie Hebdo, journalist Zineb El-Rhazoui imagined a gunshot and maybe some broken glass - so inured were she and her colleagues to the risks on the front lines of the free-speech fight. They had grown used to threats and lawsuits after publishing a controversial caricature of the Prophet Muhammad in 2006. Their offices had been firebombed in 2011. Editor-in-chief Stéphane Charbonnier, or Charb, was on the Al Qaeda terror group's most wanted list. But she had not envisioned the massacre carried out on Jan. 7 by French-born brothers Saïd and Chérif Kouachi, apparently acting on orders from Al Qaeda in Yemen. Twelve people were dead. Nine were El-Rhazoui's colleagues at the magazine. There was a stunned silence as she watched the news reports from her native Morocco, where she was vacationing. Grief was followed by anger. Now the 33-year-old has found resolve. Under the watchful eye of two strapping bodyguards, El-Rhazoui has brought that determination to Quebec in a tour that is a fundraiser and show of solidarity for her cash-strapped magazine. Her tour is also an activist campaign that touches on a raging debate in this province, and throughout Canada, about how to tackle radical Islam. In Ottawa this week, Prime Minister Stephen Harper is to introduce legislation to crack down on terrorism and give authorities greater powers to track radicalized Canadians who may be plotting attacks at home or trying to join the fight abroad. Toronto Star, A8

Proposed anti-terror bills' legality questioned
With the government's latest in a long string of anti-terror bills expected this Friday and slated to include such measures as allowing "preventative arrests" and outlawing the "promotion of terror," security and legal experts are expressing concerns about the bill's constitutionality. Though the details of the proposed law have yet to be seen, information leaked to media indicates it would make it easier for law enforcement to detain without arrest and is expected to outlaw the nebulously phrased "promotion of terror." Asked about that fine line between charter-guaranteed freedoms and national security, Justice Minister Peter MacKay was vague Monday, saying only the government had "examined this." "But we believe, given concerns and elevated threat assessment, this is something we have to do," MacKay said. National security expert and former CSIS operative, Mubin Shaikh would like to see more nuance in the feds' view of terrorism, domestic and international. "Will we use the label of terrorism given by despot regimes to their opposition? What about groups like the PKK (Kurdish Workers Party) in Syria who are a terrorist organization but whose interests in fighting ISIS join with our own? Shaikh asked. University of Ottawa security law Prof. Craig Forcese said that while the devil will be in the details, laws don't solve problems. Edmonton Sun, 22 (Kingston Whig-Standard)

*** Jihadists seek 'to harm us here:' PM**
Warning that Canada faces real threats from "violent jihadism," Prime Minister Stephen Harper says his government will move this week to introduce new legislation to help halt attacks and bar terrorists from travelling and recruiting. Spurred by the October attacks in 2014 here in Canada, as well as attacks abroad, Harper said the threat facing Canada is real. "Jihadist terrorism is not a future possibility, it is a present reality. Violent jihadism is not simply a danger somewhere else. It seeks to harm us here," Harper said in a speech Sunday. Harper used a speech to party loyalists to signal that security and the economy will be the priorities as Parliament returns for what's expected to be the final session before Canadians go to the polls in October. Harper said the legislation, expected Friday, would have measures to ensure police and security agencies "have the tools they need to meet evolving threats." "These measures are designed to help authorities stop planned attacks, get threats off our streets, criminalize the promotion of terrorism and prevent terrorists from travelling and recruiting others," the prime minister said. Harper said the legislation would respect rights of free speech, freedom of association, religion "and all the rest." "Notwithstanding the threats, we will not overreact. But neither will we underreact, because the big picture ... is very worrisome," Harper told the crowd in a high school gym in suburban Ottawa. Waterloo Region Record, A5

*** Time-consuming war on terror**

An opinion piece states, "We all knew this would be coming. After years of predictions about how Canada would succumb to so-called lone-wolf terrorist attacks, we were struck with two shocking incidents within days in October, killing two Canadian soldiers in Saint-Jean-sur-Richelieu, Que., and Ottawa. Meanwhile, we appear to be observing a stream of radicalized young adults spirited away from across Canada by the so-called Islamic State, whose violence, rooted in religion-inspired hate, has been repeatedly referred to as a "death cult" by world leaders. Late last week, QMI Agency reported two Montreal women declared missing by their families in November are believed to have gone to Syria to join ISIS. This follows the reported death of a former Ottawa man who fought with Islamic State. Earlier in January, three Ottawa men were arrested on terrorism-related charges, one among them stopped as he tried to fly out of the country. Before that, we learned three men from Edmonton were killed last fall while fighting for Islamic State. And previously, an apartment complex in downtown Calgary came under heavy scrutiny after several of its inhabitants ended up travelling to the Middle East to join jihadist fighting factions. It's therefore no surprise the federal government would move to strengthen Canada's laws in an attempt to stop this sort of activity. After the October attacks, the feds moved to give more muscle to Canada's spy agency, CSIS. It signalled at the time more change would be coming." Calgary Sun, 15

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Duo fined in tunnel incident

Two Michigan men have pleaded guilty to possession of prohibited weapons and set free after they prompted a dramatic three-hour shutdown of the Windsor-Detroit tunnel. Kyle Martens, 29, pleaded guilty to possession of brass knuckles. He received three years probation and a $100 victim find surcharge. Ernest Edwards, 18, pleaded guilty to possession of brass knuckles and two butterfly knives. He received three years probation and a $500 fine plus a 30 per cent victim find surcharge. The men, who initially faced multiple weapons charges, spent two days in pre-trial custody. They were arrested around 5 p.m. Jan. 20 after officers with Canada Border Services Agency found two knives, brass knuckles and a smoke bomb in the sport utility vehicle they were driving into Canada from Detroit. The officers called for an immediate evacuation of the Windsor-Detroit Tunnel and the border crossing complex after finding the weapons inside the 2004 Dodge Durango. When officers looked into a bag and found a cardboard cylinder with a fuse attached, they didn't initially realize it was a smoke bomb. After the area was evacuated and the two men were arrested, the Windsor police bomb squad went in to inspect the device. The tunnel was reopened shortly before 9 p.m. The Windsor Star, A5

Ontario changes policies on transgender inmates

Transgender inmates in Ontario will now be dealt with based on their own gender identity, not their physical sexual traits, a policy Ontario's corrections minister is calling the most progressive of its kind in North America. Previously, inmates were put in institutions based on a person's "primary sexual characteristics." Now, they will be housed according to their self-identified gender and referred to by their chosen name rather than their legal name and their preferred pronoun. "This is the most progressive policy on the treatment of trans inmates in North America," Correctional Services Minister Yasir Naqvi said Monday. "No other jurisdiction in Canada has such policy." Last year there were 25 inmates that self-identified as transgender in provincial correctional facilities, the ministry says. The policy builds on interim guidelines that were put in place last April, Naqvi said. The case of a trans woman from England who was detained by the Canada Border Services Agency last February pushed the issue to the forefront as she tweeted her experiences before being detained in a men's facility, despite travelling on a passport identifying her as female. Avery Edison was eventually transferred to a women's facility, but filed a human rights complaint about her treatment. The Canadian Press, (The Record, A3 National Post, Hamilton Spectator),Red Deer Advocate, The Toronto Star (2015-01-26)

Sex doll case due back in court in February

The case of a man suspected of sending a child-like sex doll in the mail was called in provincial court in St. John's Monday. Kenneth Harrison, who is not in custody, was not in court. St John's defence lawyer Bob Buckingham appeared in court via teleconference. Buckingham requested a postponement until next month, at which time, he said, he would be in a better position to advise the court whether or not colleague Kier O'Flaherty will stay on as Harrison's lawyer. He and prosecutors Natalie Payne (provincial

Crown) and Bill Howse (federal Crown) agreed to reschedule the case for Feb. 19. Harrison faces four counts, including two criminal charges - possessing child pornography and mailing obscene matter - including a sex doll depicted as a child. Two charges of smuggling and possession of prohibited goods contrary to sections 159 and 155 of the Customs Act were laid by Canada Border Services Agency (CBSA). The 49-year-old made his first appearance in court April 23, 2013. He was arrested in relation to a child pornography investigation. On Jan. 30, 2013, CBSA officers at the International Mail Centre in Toronto intercepted a package that was found to contain suspected child pornography. On March 12, 2013, members of the RNC criminal investigation division and the CBSA's criminal investigations division searched a home in St. John's and arrested Harrison. The Telegram, A3

A risques élevés, paies augmentées
Des camionneurs qui ont passé à répétition la frontière américaine avec des centaines de kilos de cocaïne au début des années 2010 n'ont pas hésité à demander de fortes «augmentations de salaire» à leurs patrons, en raison des risques subis. L'appât du gain est l'un des facteurs qui ont joué contre Serge Étienne Boyer la semaine dernière, alors que l'homme de 29 ans, qui avait été arrêté au cours de l'importante opération Loquace en novembre 2012, a été condamné à une peine de huit ans et demi de pénitencier. L'enquête Loquace, menée par la Sûreté du Québec, a visé un consortium composé d'individus liés notamment au crime organisé irlandais et aux Hells Angels, qui auraient tenté de prendre le monopole de l'importation et de la distribution de cocaïne au Canada. Boyer travaillait pour le propriétaire d'une entreprise de transport, Éric Brochu, déjà condamné à 11 ans de pénitencier dans cette affaire. L'entreprise de Brochu était spécialisée dans le transport de roulottes fabriquées aux États-Unis et vendues au Canada. Ses camionnettes, qui franchissaient continuellement la frontière, avaient été modifiées et équipées d'une cache dans laquelle les suspects pouvaient importer jusqu'à 100 kg de cocaïne chaque fois. La Presse

Not knowing import rules comes with steep price
As the world becomes a smaller place and commerce becomes more global, more and more businesses are sourcing products outside of Canada. Whenever a business starts importing goods, it needs to be aware of and keep an eye on import duty issues. While it might not seem urgent to a company just starting to import products, the cost of incorrectly classifying goods brought into Canada can compound as the stream of imports grows and, if not spotted in time, end up costing them in overpaid duty they can't recover or penalties for underpaid duty. (...)Problems also can arise when importers don't question ruling classifications by U.S. Customs. Canada Customs does not accept these classification rulings, although they can still be useful to help determine the correct tariff classification. For example, one Canadian company relied on a U.S. ruling that classified parts for a coffee maker as duty free. When Canada Customs examined the transaction, they changed the classification, resulting in a rate of 6.5 per cent being applied to four years of imports, resulting in duty owing of more $300,000 plus interest. (...) Documenting your procedures with respect to classification and valuation of imported goods is essential so you're ready to show the Customs authorities you're fulfilling your obligations, especially if you import certain targeted goods. Each year, the Canada Border Services Agency singles out specific imported products for audits to verify compliance with tariff classification, valuation and other rules. These audits can result in re-assessments going back four years. For 2014, these targeted products include batteries, footwear, machinery for public works, special purpose motor vehicles, bedding and related party transactions. With all your procedures in place, you may want to consider opportunities to reduce the import duty you pay. For example, do your imported goods originate in a country that has a free-trade agreement with Canada, such as NAFTA? Canada also has free-trade agreements with Chile, Costa Rica, Colombia, Israel, the European Free Trade Association and several others and is negotiating agreements with many more. You can often import goods duty-free from these countries, but you'll need the appropriate documentation to prove where they originated. Incorrect or false country of origin claims can result in Canada Customs denying the preferential duty treatment and penalties being assessed. Telegraph Journal, D1

Delray wrestles with uncertainty
Residents in Delray, Mich., remain worried that those in charge of the planned Windsor-Detroit bridge will do little to help mitigate damage to their community or provide jobs during the massive construction effort. The $2.1-billion Detroit River International Crossing project is in the planning phase with property

acquisition already underway in the southwest Detroit industrial community to make room for the bridge, plaza and feeder roads. But community leaders are frustrated because nobody overseeing the project is providing guarantees the community's concerns will be addressed, that people will simply be displaced and their neighbourhoods turned into a giant trucking plaza. "There have been hundreds of meetings, a lot of talk, but nothing in writing on community benefits," said former state Rep. Rashida Tlaib, a leader in the fight to ensure Delray's residents are treated fairly during bridge construction. "The constant pushing back has people starting to distrust the process." Nobody from Detroit has a seat at the table with the Windsor-Detroit Bridge Authority, which will oversee construction, or the six-member International Authority it reports to on the project. "It sends a message to the community that no one wants to hear from them," said Tlaib, who herself has reached out several times and been unable to get direct answers. She wants to see in writing some form of job guarantees, community greening plans and how exactly residents are to be treated in regards to relocation. "We are eager to see this move forward, but in a way where the community is at the table," Tlaib said. "This community has learned so much from dealing with the Ambassador Bridge and Matty Moroun that it's critical to have promises in writing." WDBA officials indicated Monday they are paying attention to the community concerns being expressed in Delray. The Windsor Star

Pour un équilibre budgétaire durable
Le problème des finances publiques du Québec ne réside pas dans le salaire de ses employés. Les Québécois sont les plus taxés au Canada et le Québec reçoit près de 10 milliards en péréquation du fédéral. En plus, le Québec est la province la plus endettée. En retour de leurs taxes et impôts, les Québécois ont des systèmes de santé et d'éducation qui ne répondent pas aux attentes et des infrastructures qui ne sont pas à niveau.Cette politique de petits salaires n'incite pas l'État du Québec à vraiment faire le ménage dans les finances publiques. Ce ménage viserait notamment les subventions à l'agriculture - les producteurs d'ici sont déjà largement subventionnés par les consommateurs à l'aide de tarifs douaniers variant de 175 à près de 300 % qui les mettent à l'abri de toute concurrence, à l'exception d'une petite quantité que l'on peut importer sans payer le tarif douanier. La Presse

Oberlander prosecution enters third decade
Retired developer Helmut Oberlander plans another court appeal, 20 years to the day after Canada began prosecuting him for serving as a low-ranking interpreter with a Nazi death squad. The government launched its case on Jan. 27, 1995, aiming to strip Oberlander of his citizenship and then deport him, without presenting evidence that he personally committed a war crime. Since then, lawyers have retired or moved on. A judge who delivered a key ruling has died. Governments have changed. Court decisions have piled up, with 13 rulings archived at the Federal Court of Canada or the Supreme Court of Canada. What hasn't changed is that Oberlander, 90, is still in Canada and still fending off deportation, while the government is still making mistakes in its case against him, according to the latest court ruling made this month. As the battle enters its third decade, frustration is mounting among organizations demanding that Oberlander face justice. "The system (in Canada) makes it very difficult," historian Efraim Zuroff said, from Jerusalem in Israel. He's the chief Nazi hunter for the Simon Wiesenthal Center, a Jewish human rights organization. Zuroff has asked the German government to seek Oberlander's extradition, so that he may be tried in Germany as an accessory to war crimes. The Record

*** B.C. could pick up business from backed-up ports on U.S. west coast**
Transportation analysts believe B.C. ports such as Prince Rupert stand to benefit from chronic congestion plaguing the U.S. west coast, as shippers begin looking for alternative routes to get their goods to market. A prolonged labour dispute coupled with structural and resource considerations related to accommodating larger container ships have resulted in months of gridlock at two of the U.S. west coast's busiest ports, Los Angeles and Long Beach, which account for an estimated 40 per cent the country's trade with Asia. The delays have prompted calls for the White House to get involved, reported the Financial Times, as retailers fight to get their goods off-loaded and other key sectors of the economy, such as agriculture, begin to feel the pinch. Some shippers, meantime, are posting loses in the millions of dollars, according to other reports. "It's a mess, to be honest with you," said Cathy Roberson, a senior analyst at Transport Intelligence Ltd. "There is one issue after another, it just keeps building. At last count, I think there were ... 25 ships waiting to dock at the port of L.A." The gridlock, however, could be a boon for B.C., said Roberson, who will be one of several speakers at an upcoming conference at the

Vancouver Convention Centre on global trade trends. Some freight already has been diverted north of the border to B.C., she said, while other container ships have headed to Mexico to off-load. "Your ports are noting some nice increases," she said. "Canadian west coast ports are very highly competitive and very friendly." While acknowledging the labour unrest south of the border has caused changes to the supply chain, a spokesman for the Vancouver Port Authority noted there are other factors behind the recent bump in container traffic Vancouver has experienced. While at least some of the recent increase in traffic can be attributed to the natural peak in the shipping season - back to school, Thanksgiving and Christmas - Vancouver is also experiencing an ongoing surge in shipping volume, said John Parker-Jervis, the media and government affairs adviser for Port Metro Vancouver. Last year traffic increased by an estimated four per cent, and overall volume is expected to double within the next 10 to 15 years, he said. The Province

* **Thumbs down, boss**

Airports are highly secured environments; there are ample reasons why Big Brother ought to look over various shoulders. However, in requiring baggage handlers in Montreal, Toronto and Halifax to use fingerprints to clock in and out of work, Air Canada is treading on treacherous privacy terrain. Employees with access to "air-side" areas should be subjected to stringent security controls, if only to police would-be smugglers. But workers in this case claim fingerprinting was introduced primarily to address so-called "buddy-stamping" of time cards. The policy is heavy-handed, even if you believe clock-punching chicanery amounts to theft. The union representing the employees has filed a grievance and a raft of privacy complaints; the matter has yet to be adjudicated. It's not clear if others in the company will be affected. Union officials say members don't object to giving their fingerprints to the RCMP or Transport Canada. They contend having an employer demand it - and then threatening disciplinary measures up to and including dismissal, as company-issued letters obtained by Montreal's La Presse appear to do - is a bridge too far. We agree. An Air Canada spokeswoman told La Presse the technology is widely used in the industry and simply aims to bolster security and replace obsolete equipment. It's not clear the airline is doing anything illegal. In 2008, Alberta's privacy commissioner concluded fingerprint-based attendance controls can be a reasonable intrusion, although employee privacy rights there are limited by provincial statute (and airlines generally fall under federal law).The federal privacy commissioner set out broad criteria for biometric workplace measures a decade ago in rulings on voiceprint and GPS tracking technology. An employer must demonstrate necessity; it must collect the minimum information required; data cannot be used for any other purpose and must be carefully safeguarded. Employees should be notified and allowed access to their data. In other words, biometrics should be used sparingly. Some might argue fingerprinting is relatively non-intrusive. It's also used by police to keep track of criminals. But companies have less invasive options to track employees' comings and goings and audit their hours. Privacy rights matter, even in a dysfunctional workplace. The Globe and Mail

* **Police say 400 – 500 gang members in Ottawa**

The numbers don't lie. According to the Ottawa Police Guns and Gangs Unit, there are between 400 and 500 gang members in the capital. Staff Sgt. Ken Bryden revealed the numbers in a presentation to the Police Services Board on Monday night (...) Hundreds of charges were also laid in the past 12 months, most of them drug related." By far the drug trade, in particular cocaine in both powder and rock form, is the driving factor behind...the criminality," says Bryden. Guns are the other main issue. Bryden refused to even guess the number of firearms on the streets of the capital. But he did say that 60% of them are smuggled into the country, mostly from the United States. They're hoping to shrink that number. "In 2014, two arrested members involving gang activities were deported out of Canada," says police chief Charles Bordeleau. "That's why it's important we continue to work with CBSA (Canada Border Services Agency) on that work."That work has also led to the police seizing four guns since the beginning of January. CTV News (2015-01-26)

* **Drummon Island Ice Bridge to open**

It is that time of year again when the "Ice Bridge" forms between Canada and the United States.The ice bridge is scheduled to be marked with signs and the tree line on Saturday, January 24, 2015. Once the ice bridge is established, CBP will begin staffing the reporting station on Friday, January 30, 2015. The opening and closure of this reporting station is subject to change contingent on weather and ice conditions. Travelers entering from Canada must report directly to the reporting station on Drummond

Island during the established hours of 2 p.m. to 10 p.m. Friday through Sunday. The number of days that the reporting station is open has been reduced due to the low volume of people using the ice bridge. The Drummond Island reporting station will be closed this year Monday through Thursday.The official CBP Reporting Station is located at the Drummond Island Yacht Haven Dock. Entering at any other location or outside of these hours is prohibited and violators could be assessed a $5,000 fine. SooToday.com (2015-01-26)

* **CBSA Celebrates International Customs Day**
Today, the Canada Border Services Agency (CBSA) joins counterparts around the world in celebrating International Customs Day. This year's theme is Co-ordinated Border Management - an inclusive approach for connecting stakeholders. The CBSA supports the World Customs Organization (WCO)'s decision to highlight the importance of partnerships in meeting the trade and border security demands of the 21st century.Border management is a shared international responsibility, and threats and opportunities arising from global migration and trade are dealt with most effectively by working together. The CBSA is considered a leader in global border management and currently chairs the "Border Five," an informal group of representatives from Australia, Canada, New Zealand, the United Kingdom and the United States. Recognizing the importance of strong partnerships with stakeholders, the CBSA maintains a robust international network. Currently, the Agency has over 60 employees working in 47 locations around the world. The CBSA has also signed Customs Mutual Assistance Agreements with 10 international partners to date.In 2015, the CBSA will continue to work collaboratively with external partners to support our common goals of international security, public safety and the facilitated flow of legitimate people and goods. Likewise, the Agency will continue to share best practices and lessons learned with other customs organizations, as well as enforcement partners around the world. Market Wired. (2015-01-26)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

* **Hacker group claims it is behind outages at Facebook, other sites**
Internet sites including Facebook, the world's largest social network, Instagram and other popular sites suffered temporary outages on Tuesday and a hacker group associated with other recent high-profile attacks claimed it caused the outages. Reuters (Yahoo! News)

* **Des Idées en revues - L'exigence de transparence et le "contrôle social 2.0"**
Quiconque utilise Internet aujourd'hui doit s'attendre à ce que ses moindres faits et gestes puissent faire l'objet d'une surveillance continue et en temps réel. Si nous pouvions déjà le soupçonner, les troublantes révélations d'Edward Snowden sur l'étendue de la surveillance menée sur le Web par la National Security Agency (NSA) nous l'ont confirmé. Le Devoir, A7

* **Facebook's outage exposes our digital fragility**
OMG Facebook is down! Down too went Instagram. It was just for an hour this morning, but the tweets screamed "Do I have to talk to someone real?" In a manner of speaking, yes. Despite the hackers of Lizard Squad claiming credit, it is now clear that an outage at Facebook's HQ was responsible. But the confusion was understandable after Lizard Squad had in recent weeks variously hit Sony executives and Microsoft products. It brought down PlayStation and Xbox platforms over Christmas. Guardian UK

* **Un "méga-hacker" sera extradé vers les USA**
La justice néerlandaise a autorisé aujourd'hui l'extradition vers les Etats-Unis d'un hacker russe soupçonné d'avoir dérobé plus de 160 millions de numéros de cartes de crédit en pénétrant les systèmes de sociétés américaines et européennes. Ce piratage informatique est un des plus importants jamais réalisés contre des sociétés américaines et européennes. Le Figaro

* **Apple preparing fix for Thunderstrike malware in upcoming OS X 10.10.2 release**
It's long been said, both by Apple and independent security experts, that Apple's computers are more secure than those running Windows. That does not mean, however, that Macs are invulnerable to malware threats. One particularly terrifying example is called Thunderstrike. It allows a malicious actor to

replace the firmware in Macs with something much more nefarious. The firmware controls extremely low-level functions of the computer, everything that happens from the moment the power button is pressed. Yahoo! News

LAW ENFORCEMENT / APPLICATION DE LA LOI

Thousands attend funeral for Mountie slain during struggle
The sister of an Alberta Mountie told mourners at his funeral Monday that he would want them to live life the way he did - with joy, with passion and with every effort to make the world a better place. "Over the past 10 days, there has been such an outpouring of stories about Dave and obvious love for him from the people that he has touched that I have realized he was far more than I ever imagined," Mona Wynn said in her eulogy before thousands at a recreation centre in St. Albert. "Dave was an ordinary man with an extraordinary capacity to make the world a better place for everyone around him." Const. David Wynn, 42, died last Wednesday, four days after he and auxiliary Const. Derek Bond were shot during a struggle with a suspected car thief at a casino in St. Albert. He was shot in the head and never regained consciousness before he died... RCMP Insp. Kevin Murray called him "the finest example of a front-line police officer." Deputy Commissioner Marianne Ryan, responsible for the Alberta RCMP, addressed Wynn directly: "Constable David Matthew Wynn, you have served this province and your country well. It is soon time for you to grab your fishing rod and head for the Miramichi, where I know your father will be waiting for you once more. We wish you Godspeed and tight lines." It was standing room only as more than 7,000 people came to pay their respects. The mourners included more than 2,100 Mounties, police officers, military members and first responders from communities across Canada. Canadian Press (Red Deer Advocate, A1, Chronicle Herald , A1); Postmedia News (Edmonton Journal, A1, Vancouver Sun, A1, Calgary Herald, A1)

High-risk takedown at Schlumberger site ends peacefully
A man caught up in a police incident just south of Red Deer on Monday afternoon said it began for him when he was told to stay indoors. "I says, 'What's going on? ' and I looked out in the front lot there was a half dozen RCMP vehicles, the officers were vesting up, they were getting out their high-powered rifles." The incident occurred outside at Schlumberger Ltd.'s pressure pumping base in McKenzie Industrial Park, located on McKenzie Road between 30th and 40th Avenues. Blackfalds RCMP responded to a call of an attempted truck theft and firearm complaint. It ultimately ended peacefully with the arrest of one 17-year-old male suspect. Blackfalds and Innisfail RCMP, ALERT, Police Dog Services and the RCMP helicopter were involved. RCMP said the firearm turned out to be a replica pistol. The man who was there when it happened, and whom the Advocate is not identifying, said a lockdown for safety purposes quickly began at about 2 p.m., when about 75 people who were working outside in the yard were told through company loudspeaker to come inside. A suspect was sitting in a large black crewcab truck in the parking lot on the east side of the Schlumberger facility. Red Deer Advocate, A1

Police use 'blooding' to hunt killer
Last week police detectives went door to door in a Windsor neighbourhood asking individuals to voluntarily provide a DNA sample in an effort to find the killer of Cassandra Kaake, who was brutally murdered in December. It is the first DNA sweep on record in Windsor. DNA sweeps, or blooding, as it is provocatively called, are more common than you might think. The practice dates back to 1987 when English police decided to find the killer of two young women using a new technology of genetic, or DNA, fingerprinting. Thousands of men had blood drawn using syringes, hence the term blooding. None, however, turned out to be the killer. The real killer was a local baker, Colin Pitchfork. He had briefly evaded detection by paying a co-worker to give his blood pretending to be Pitchfork. The police eventually found out and Pitchfork became the first person to be convicted using DNA evidence. The case led to the novel The Blooding by Joseph Wambaugh. Not long after DNA technology made its way to Canada in the 1990s, there were reported instances of blooding across Canada, including a sweep of 300 men in Vermilion, Alta., in search of a serial rapist. Windsor Star, A6

Prince George police say case of missing man is homicide
There is no body, but RCMP in Prince George, say they're treating the disappearance of a 24-year-old

man as a homicide. Jordan McLeod was reported missing a week ago and was last seen in Prince George and Vanderhoof three days earlier. RCMP issued a news release last week saying they believe McLeod's disappearance may have been linked to a report of shots fired near Highway 16 and Upper Fraser Road in Prince George. Police say their investigation into McLeod's case involved more than 100 officers from three different communities. Investigators are looking for his burgundy 2006 Chevrolet Malibu with the licence plate 163 RNA. Mounties believe the vehicle he was driving is an important piece of evidence and they are asking anyone who spots the car to call police. Canadian Press (Vancouver Sun)

Moncton suspect toujours recherché

Les policiers sont toujours à la recherche d'un jeune homme qui aurait été aperçu marchant dans les rues de Moncton dimanche et possiblement armé. Après une imposante opération policière qui aura tenu en haleine pendant plusieurs heures les résidents d'un grand quartier résidentiel au coeur de Moncton, la GRC poursuit son enquête. Le suspect recherché par la GRC, un jeune homme aux cheveux foncés et de taille moyenne, aurait été vu une seule fois sur la rue Katherine. Il portait un pantalon foncé, un manteau gris avec des barres rouges sur les manches, ainsi qu'une tuque foncée en tricot. Après avoir établi un périmètre de sécurité, passé au peigne fin les voisinages ciblés et cogné aux portes de nombreux résidants, les policiers n'ont pas trouvé l'arme ni le suspect. Le périmètre a été levé vers 20 h 30. Néanmoins, la GRC poursuit son enquête et demande à quiconque possédant de l'information sur cette affaire de communiquer avec la police au 506-857-7400. L'Acadie Nouvelle; Postmedia News (Telegraph-Journal, A3, Times & Transcript)

Mounties set in Upper Rawdon

It has been a long and sometimes bumpy ride, but the RCMP have arrived in Upper Rawdon. "Officers will work out of that detachment seven days a week," said Const. Tammy Lobb, an RCMP spokeswoman. Officers have been working out of the new sub-detachment at 2945 Highway 14 for the past few weeks, but the grand opening, originally set for Tuesday, has been rescheduled for Thursday at 11 a.m. The initial plan was to have the building open last summer, but delays pushed the opening to 2015. A revamped East Hants policing model had been designed to bring all of the municipality's officers within the borders of the Municipality of the District of East Hants. In the past, the municipality shared several officers who were stationed in West Hants. East Hants council decided on an Upper Rawdon detachment to serve the rural, western side of the municipality, but the provincial Justice Department recommended in 2011 that a Mount Uniacke office would better suit the municipality's needs because of the area's growing population. Council requested another meeting with the RCMP and the province and was pleasantly surprised to see that the police and the Justice Department had done an about-face by the summer of 2012 and agreed to the Upper Rawdon location. Chronicle Herald, A5

RCMP seek man who exposed himself

Police are looking for a man who exposed himself to four eight-year-old girls while they were playing outside in a Red Deer neighbourhood Saturday afternoon. Red Deer RCMP say the girls were in the front yard of a home on Northey Avenue when the incident occurred shortly before 2 p.m. When one of the girls walked away from her friends to go inside to get a drink, a man appeared in the yard, picked her up and took her toward a shed in the backyard. The other three girls followed their friend and the man directed them to the shed. He blocked their exit and then exposed himself to them. He began to touch himself, refusing to allow the girls to leave, police said in a news release. He left a short time later and was last seen running south down the alley behind Northey Avenue. The girls were not physically harmed, police said. RCMP officers and police dog services swept the area but were unable to locate the suspect. Edmonton Journal, A2 (Red Deer Advocate)

Police officers fired after two prisoners escape cells

Several Edmonton police officers were fired after two separate jail breaks proved the cells were more sieve than se cure. Two of those escapers were re captured only to be involved in a second break out the same week from RCMP barracks. It's not known if the Mountie involved in that incident lost his job too. City Const. Sylvester was let go after an internal investigation found his carelessness was to blame for the escape of Fred Palmer and Ed Young. Sgt. Lang, the officer in charge at the time, also lost his job.

Palmer and Young were facing charges for the separate thefts of fur coats and were awaiting trials. Edmonton Journal, A2

Deadly pills still out there
The potentially lethal pills that killed three young people in Saskatoon are still on the street. In two separate cases, police arrested three people - all of them accused of selling fentanyl. "As long as the pills are there and people are buying them there is a potential for another tragedy," said Staff Sgt. Donovan Fisher Monday. Police say two men from British Columbia turned themselves in to Saskatchewan authorities after they were charged as part of a large scale investigation into guns and drugs targeting two local biker clubs. The pair - 29-year-old Ruslan Jamal Bakuridze and 30-year-old Adam Harada - are also charged with dealing cocaine, heroin and methamphetamine in addition to the lethal fentanyl pills. They are the latest of more than a dozen people charged in the wake of police raids targeting the Hells Angels and the Fallen Saints as a result of an investigation known as Project Forseti. The Jan. 15 raids in several Saskatchewan and Alberta cities, uncovered more than 3,000 fentanyl pills and large amounts of cash and guns. Officers also seized over $8 million of cocaine, methamphetamine and heroin. Saskatoon police said fentanyl pills are responsible for one overdose death earlier this month and two in September. Postmedia News (Leader-Post, A4)

* **Alleged Regina identity fraudsters face similar charges in Alberta**
An apparent victim of identity fraud in Regina wonders why the man charged, with a long history of fraud, was released on bail just two weeks before the Regina incidents began. Marino Vecchioli is one of 23 alleged victims of James Donald Provost, of no fixed address, who is facing 58 charges related to mail theft, forgery, impersonation and identity fraud. Vecchioli said in mid-November he was buying a car which required him to get a credit check… The former director of the RCMP's proceeds of crime unit, Garry Clement, said this story highlights a problem with the way Canada treats fraud. "Canada has to start treating white collar criminals with some severity because the unfortunate part is there isn't any respect of the damage they are doing to these individuals (victims) and in some cases it's life changing for some of these people," he said. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Tories seek tougher penalties for killers
The Conservative government is developing legislation that would mean some murderers will have no hope of release from prison. The new penalty would apply to several categories of those convicted of first-degree murder: killers of police and jail guards, anyone who kills during a sexual assault, kidnapping or act of terrorism and for especially brutal murders. The current penalty for first-degree murder is an automatic life sentence with the first chance for a parole review after 25 years, and the supervision of parole authorities for life. The planned legislation has yet to be approved by cabinet, a source said. The departments of Public Safety and Justice, which are working together on the new bill, were told to speed up their work after a man shot two Mounties in St. Albert, Alta., on Jan. 17, killing one. The bill is expected to be introduced within a couple of weeks of a new terrorism bill coming on Friday, the source said. The change would reshape the Canadian legal landscape in an area seen as distinguishing this country from the United States. It sets the stage for the government's tough-on-crime policies to be a centrepiece of the federal election campaign expected next fall. A spokesperson for Justice Minister Peter MacKay declined to comment directly on the categories outlined by The Globe, but quoted the Throne Speech of October, 2013, saying: "Canadians do not understand why the most dangerous criminals would ever be released from prison. We are currently reviewing options to ensure that a life sentence actually means life." (…) In recent years, the website of Correctional Service Canada has described those serving life sentences as "the most likely to succeed on parole." A spokesperson said on Monday the agency could not identify, for privacy reasons, the last first-degree murderer released on parole who killed again, nor how many have done so since 1976. Globe and Mail, A1

Du lait en poudre pour les prisonniers
Du lait en poudre sera désormais servi dans les prisons fédérales. Une mesure administrative qui représente des économies de l'ordre de 3,1 M$, a-t-on confirmé de la part du Service correctionnel du

Canada. L'entreprise laitière Chagnon, implantée à Waterloo depuis 60 ans, écope de cette directive. « Je viens d'apprendre la nouvelle. On est devant le fait accompli. Le 12 janvier dernier, j'ai fait ma dernière livraison de lait au pénitencier de Drummondville », explique le président Denis Chagnon à *La Terre de chez nous*. Depuis 10 ans, l'entreprise livrait 6 000 berlingots de lait par semaine destinés à la prison de Drummondville qui compte 415 détenus. La laiterie Chagnon dessert aussi la même quantité depuis 15 ans aux 666 détenus du pénitencier de Cowansville. « À cet endroit, durant la même période, on a perdu une seule fois l'appel d'offres », précise M. Chagnon. Dorénavant, une compagnie de Winnipeg va transporter la poudre par camion en direction des établissements du Québec. Les pénitenciers doivent s'équiper d'un appareil servant à la fabrication du lait à base de poudre. « Quand les fonctionnaires font leurs calculs, tiennent-ils compte de l'impact régional? » s'interroge M. Chagnon qui perd ainsi un contrat de 275 000 $. (...) Le Service correctionnel du Canada (SCC) a refusé notre demande d'entrevue. Toutefois, on nous a fait parvenir par courriel une note explicative. « Le 1er novembre 2012, le SCC s'est engagé à moderniser son modèle de prestations des services d'alimentation aux détenus. Cette initiative s'inscrit dans les efforts consacrés au gouvernement afin d'améliorer l'efficacité des services et de réduire le déficit », précise Julie O'Brien, conseillère en relations avec les médias au SCC. La Terre (2015-01-26)

Leave extended for mine bomber
A man granted day parole two decades after being convicted of planting a bomb that killed nine miners in Yellowknife will be getting extended leave privileges. Roger Warren has been granted permission by the national parole board to spend more time away from his halfway house for medical treatment. The board says its decision was made after 71-year-old Warren was hospitalized for pneumonia and doctors said he needed to stay longer for tests. Warren was imprisoned for setting off an explosion deep inside the Giant Mine during a bitter strike in 1992, when nine replacement workers were killed as their ore car went over a trip wire. Documents from the board say Warren must follow a series of conditions and a parole supervisor may revoke his release if there's a risk to the public. Warren was being held at the Mission Minimum Institute, east of Vancouver, when he was granted day parole last June, when he was transferred to a halfway house at an undisclosed location. Canadian Press (Times & Transcript, A4, The Province, Winnipeg Free Press, Metro News, Revelstoke Times Review, Vancouver Sun, Kelowna Daily Courier, Medicine Hat News, Victoria News), Resource Clips

* **Solitary confinement creates problems for the community, says John Howard Society of Canada**
Prison isolation up to 23 hours per day for weeks at a time is cruel and unusual punishment, says the John Howard Society of Canada. The society, along with the B.C. Civil Liberties Association, started a lawsuit against the federal government's use of solitary confinement in prisons. The two human rights groups said they want reforms around the use of segregation in prisons and don't see it as suitable for individuals with mental health issues. Solitary confinement is increasingly being used to house prisoners with mental health issues, even though studies have shown that isolation worsens mental illness, the John Howard Society said. Catherine Latimer, a spokeswoman for the organization, said the John Howard Society of New Brunswick proposed a resolution at the national annual general meeting last fall that a stand be taken against solitary confinement. "New Brunswick was the home of Ashley Smith, so it understands the harms caused by solitary confinement." Smith committed suicide while in isolated confinement in 2007. Latimer said had the federal government responded to the coroner's report in the Smith case by limiting solitary confinement in a manner that was consistent with the John Howard Society's resolution, it wouldn't have needed to take the matter before the courts. Daily Gleaner, A5

* **In the courts, Kingston**
A compilation of offences from Kingston's Ontario Court of Justice for the period of Jan. 12 to 15, 2015. Only sentences that involved a large fine, probation or incarceration are included. (...)Destiney J. Meyler, 22, was convicted on three counts of possessing drugs for the purpose of trafficking. He had two years added to the federal penitentiary sentence he's already serving. Kingston Whig-Standard

* **Religion et philo en maison de transition**
Converti à la religion et à la philosophie, un membre influent des Hells Angels récemment libéré du pénitencier devra approfondir ses nouvelles valeurs en maison de transition. La Commission des libérations conditionnelles du Canada (CLCC) vient de confirmer que Richard "Dick" Mayrand devra résider dans une maison de transition, où il sera sous surveillance jusqu'à nouvel ordre, plutôt que dans

un appartement. Le motard de 51 ans contestait cette condition spéciale imposée il y a deux mois, en affirmant qu'il ne fait plus par-tie des Hells Angels et qu'il ne désire plus avoir de contacts avec des membres de cette organisation criminelle. Membre du défunt chapitre d'élite "Nomads" des Hells, Mayrand dit vouloir "poursuivre (son) implication dans la religion et la philosophie". Mais son souhait d'aller vivre dans un logement voisin d'un bar appartenant à un autre membre des Hells mettrait en péril les progrès qu'il a réalisés au cours de ses deux dernières années de bagne, d'après la CLCC. Journal de Montréal, 10

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Cyberbullying policy a bust with kids

Zero-tolerance cyberbullying policies have made kids less likely to go to adults for help for fear that police will become involved, a survey of Canadian children's lives online suggests. Parents and teachers need to act less like online cops and more like mentors, found the survey by MediaSmarts, Canada's think-tank for digital and media literacy. "We don't believe that surveillance, in particular covert surveillance, is particularly effective. We all know teens are masters of avoiding surveillance," said Matthew Johnson, director of education at MediaSmarts. "Teens feel like they're guilty until proven innocent and they're more covert about what they're doing and less likely to seek help if something goes wrong." MediaSmarts spoke to 5,400 students from grades 4 to 11 in every Canadian province and territory, and had four focus groups with different age groups and with parents, between 2012 and 2013. Many of the children and teens feel adults overreact to conflict online, the survey found. London Free Press, A1

Joint policing isn't easy

Windsor and Amherstburg are so enthusiastic about maybe saving money by combining **police** forces that LaSalle has been reluctantly drawn into the discussions this week. You can't blame LaSalle Mayor Ken Antaya for being independently minded. He knows his town and says the residents don't want to be covered by somebody else's police department. He's probably right. But Antaya pretty much has to be at the table with Windsor and A'burg anyway for appearances - and just in case there is real money to be saved. Creating a regional police force is inevitable for Windsor and some of its suburbs. Eventually. But there are a few things all the parties need to know before any rush to the altar: sometimes arranged marriages don't work. Also, there are some downright stupid provincial regulations governing such departmental marriages. After all, this is Ontario. Take the City of Peterborough and the former Village of Lakefield northeast of Toronto. Their arrangement ended in bitter acrimony on Dec. 31 after years of fighting and public hearings. Their saga has played out in hundreds of stories in the Peterborough Examiner newspaper since the 1990s. Like Windsor and Amherstburg, Peterborough and Lakefield don't share a border. There is a gap of about 20 kilometres between them. The city and the village decided to amalgamate their police departments during the 1990s. By Ontario statute, they first had to disband their own forces, then incorporate a new one. They did so in 1998. Windsor Star, A3

Still have lots of questions

Worried about the marked increase in guns and gangs in Ottawa, city councillors arrived at Monday night's police board meeting looking for answers. But hard and fast answers on the city's strategy still appear somewhat illusive. How many officers have been reallocated? What is this costing the city? And how long will resources for guns and gangs be diverted from other police departments? No definitive answers. That doesn't mean of course that the police are being evasive. In fact, it is as Staff Sgt. Ken Bryden told the board -- and many of the city councillors on hand -- it's a very fluid situation. "I came to get some answers, some of what I heard was a little bit vague. There's still a little bit of vagueness with the allocation of resources. That's what concerns us, we want to ensure we're properly staffing the police to do their job," said Gloucester-Southgate Coun. Diane Deans, whose ward has had problems with guns and gangs. "We heard from Chief (Chuck Bordeleau) that they're moving resources around, that's it's a fluid situation. I was looking for some firm answers on whether there was a permanent allocation of resources. He didn't give a lot of details about where exactly those resources are coming from," Deans said following the presentation. Despite those concerns, Deans said in her ward, she believes the police

have worked pro-actively in keeping pressure on the problem along with community partners. QMI Agency (Ottawa Sun, 3);* Ottawa Citizen; CTV News

International commission puts the Oppal Inquiry in context
The report of the Inter-American Commission on Human Rights, which was released earlier this month, puts the Oppal Inquiry into its proper context, by clarifying what the Oppal Inquiry did and did not do. The Inter-American Commission calls for the full implementation of the Oppal recommendations, but says that this will be a starting point for reforms in one area only. The Inter-American Commission on Human Rights, which is an arm of the Organization of American States, launched an investigation into the murders and disappearances of indigenous women and girls in B.C. in 2012. This investigation was requested by the Native Women's Association of Canada and the Canadian Feminist Alliance for International Action. In its groundbreaking report, the commission states clearly that Canada has an obligation under international human rights law to ensure that the response of the police, prosecutors and judges to the murders and disappearances of indigenous women and girls is swift, diligent, effective and unbiased - which it has not been so far. But the commission is also clear that the scope of Canada's obligations is broader. Governments must address the risk factors that cause and perpetuate the violence. Specifically, the commission tells Canada that it must combat the poverty of indigenous women, improve education and employment, guarantee adequate housing and address the disproportionate application of the criminal law. Postmedia News (The Vancouver Sun, B4)

* **Report on murdered girl may bring more transparency**
The Manitoba government will this week release a much-anticipated independent report on how to implement the remaining recommendations from an inquiry into the 2005 murder of Phoenix Sinclair, a five-year-old aboriginal girl who died in provincial care. The roughly 200-page report, which could be released online as early as Tuesday, is expected to propose legislative changes that may lead to greater transparency at the Office of the Children's Advocate, an independent body tasked with protecting children and youth in Child and Family Services (CFS) care. The report comes at a time when the province's child-welfare system is under intense scrutiny after the August killing of Tina Fontaine, a native teen who died after going missing from her foster-care placement at a downtown Winnipeg hotel. Her death has also reignited calls for a national inquiry into Canada's more than 1,180 murdered and missing aboriginal women. The Globe and Mail, A5

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

NIL

INTERNATIONAL / INTERNATIONAL

NIL

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
January 19, 2015 / le 19 janvier 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

The threat behind our bars
An opinion piece states, "As France mourns the recent attacks, another conversation is taking place. We now know one of the brothers involved in the terrorist attack spent some time in a French prison for a terrorism-related crime. Media reports suggest incarceration contributed to his further radicalization. Many Muslims are incarcerated in France. It is a fact of life that this population is at risk of being radicalized while incarcerated. In Canada we also have men incarcerated for terrorism-related offences. In addition, there are a significant number of inmates, Muslim or otherwise, who could potentially be radicalized. What is the Correctional Service of Canada (CSC) doing about it? Well, according to a recent CBC story by reporter Kathleen Harris, the spokeswomen suggests CSC is hard at work. The piece was prompted after an access to information request that revealed a briefing note from the CSC Commissioner, Don Head, to the **Minister of Public Safety, Steven Blaney**. In the May 2014 note, the commissioner requests funding ($63,000) to fly experts in from around the world for a roundtable. The minister agreed with the allocation. In the story, a CSC spokeswoman stated, "CSC is reviewing the most effective interventions and management practices for radicalized offenders that are used nationally and internationally." National Post, A10

* **Keeping Canadian Families and Communities Safe**
A blog post states, The **Honourable Steven Blaney, Canada's Minister of Public Safety and Emergency Preparedness**, recently highlighted two outstanding successes by the Canada Border Services Agency (CBSA) that will help keep Canadian families and communities safe. The Harper

Government has reached a major program milestone with successful removals of more than 50 individuals on the CBSA Wanted List; many with criminal activities that have been linked to drugs and organized crime. Additionally, Canadian border authorities have reached a new intelligence milestone with more than 150 convicted U.S. sex offenders denied entry to Canada. Together, these milestones reflect the important work our Government is undertaking to help keep our streets and communities safe by ensuring that foreign criminals are turned away from our borders, and removed once found by authorities." My Steinbach (2015-01-18)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

* **Kinder Morgan wins battle to keep emergency plans secret**
The full details of Kinder Morgan's emergency management plans for the Trans Mountain pipeline will remain secret. The National Energy Board (NEB) has rejected a demand from the B.C. government for Kinder Morgan to fully disclose the plans. The province had argued they needed to see the entire plan to determine if the company could adequately respond to a spill for its proposed $6.5-billion expansion of the pipeline. The expansion project will twin the pipeline and triple capacity to open access to new Asian markets for bitumen from the oilsands in northern Alberta. Vancouver Sun, A1

* **$1-M dike gives peace of mind to residents of 30 Reston homes**
In 2013, Dallas Williamson had two metres of water in his basement after a torrential downpour hammered Reston in western Manitoba. Today, provincial Municipal Government Minister Drew Caldwell and Brandon-Souris Conservative MP Larry Maguire will announce funding for a dike that will protect 30 Reston homes, including Williamson's. The project, which will cost about $1 million, is being shared by the three levels of government: the RM of Pipestone will pay 10 per cent and the remaining 90 per cent being will be shared by the federal and provincial governments. Winnipeg Free Press, A5

* **Campobello mayor hopeful after province asks for details on cellphone service issue**
A decision could possibly come soon from Fredericton bringing Canadian cellphone service a step closer to Campobello Island. The provincial government asked for "as much information as possible" by the end of business hours on Thursday, Mayor Stephen Smart said in an interview on Friday. He hopes this means the cabinet will decide in favour of expanding the Public Safety Radio Network, which would lower the cost of extending cellphone service to this Canadian island off the coast of Maine. Expanding the PSRN, allowing emergency communications when telephone service goes down, would roughly double the number of towers to about 70 including one on Campobello Island. Telegraph-Journal, B4

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Oversight of military intelligence limited
National Defence has been looking at ways to introduce more stringent oversight of its intelligence operations, but "fiscal restraint" may prevent the department from implementing the preferred option. A series of internal documents and slide presentations, obtained by The Canadian Press under access-to-information legislation, show the head of defence intelligence ordered the exhaustive, independent review - which was conducted in the wake of the scandal involving navy sub-Lt. Jeffery Delisle, who was convicted of spying for the Russians. Unlike the Canadian Security Intelligence Service and the Communications Security Establishment, there is no direct civilian oversight body to review the actions and operations of military agents, who conduct investigations into possible threats against the Forces both overseas and on Canadian soil. The powers of intelligence services have come under the microscope following allegations of National Security Agency eavesdropping in the U.S., and the bombshell revelations of former contractor Edward Snowden. Canadian Press (The Chronicle-Herald, A8, Cape Breton Post, The Gazette, Ottawa Citizen, Times & Transcript)

* **What is the public entitled to know about threats?**
The more security agencies grapple with terrorist threats, the less they appear to be telling Canadians. Focusing on current examples of secrecy, Postmedia News reporter Dylan Robertson spoke with experts

about what the public should be entitled to know. Postmedia News (Leader-Post, A5, The Province, Vancouver Sun, Star Phoenix)

*** Canada's anti-radicalization programs lacking against domestic terror recruitment**
St. Jean-sur-Richelieu, Ottawa, Sydney, Paris — cities under siege by attackers on killing sprees. The killers weren't sophisticated soldiers sent from terrorist networks abroad, but emerged from within the same country, in Canada, Australia and France. The attacks have created a heightened urgency for governments to combat the threat of homegrown terrorism and radicalization. In Canada, the federal government is set to table new anti-terror legislation by the end of the month, which is expected to strengthen the country's intelligence and surveillance programs. It includes giving CSIS new powers to track homegrown extremists abroad and the ability to share information with other spy and enforcement agencies. But some say these proposed measures, which will be unveiled when MPs return to Parliament, don't get to the heart of dealing with the radicalization that leads to terror attacks, especially as ISIS and other groups grow more sophisticated with their recruitment campaigns. Michael Zekulin, a researcher with the Centre for Military and Strategic Studies at the University of Calgary, says the legislation might even be playing into the hands of jihadist groups. CBC News

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Federal government defends move to deport Hamilton man to Zimbabwe
Ottawa is defending its decision to deport a 21-year-old man to Zimbabwe who came to Canada to be reunited with his mother and ran afoul of the law. Family, friends and supporters of Farai Chigogora say he is a bright, young man who was a victim of circumstances and should not have been returned to the country he left when he was 14. Chigogora said he pleaded guilty in 2012 to theft under $5,000 in connection with a Cayuga home invasion because of the financial and emotional strain the case put on his family. (…) Anna Pape of the Canada Border Services Agency (CBSA) said the decision to remove someone from Canada is not taken lightly, but that Chigogora had been issued a deportation order for "serious criminality" on July 3, 2014 by the Immigration and Refugee Board. "Protecting the safety and security of Canadians is a priority for the CBSA," Pape said in a statement to The Spectator. "The CBSA places highest priority on removal cases involving national security, organized crime, crimes against humanity and criminals." The Hamilton Spectator

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Wounded Mountie not expected to survive
An Alberta Mountie severely wounded on Saturday was not expected to live, the RCMP said Sunday as the force's commissioner expressed dismay over the criminal background of the man police believe responsible for the shooting. Const. David Wynn had not regained consciousness more than a day after the shooting, Asst. Commissioner Marianne Ryan, in charge of the RCMP in Alberta, told a news conference in Edmonton. "He sustained a life threatening injury to the head at close range, we do not expect him to survive," said Ryan, who visited Wynn's bedside on the weekend. "He is being treated and looked after in the hospital, but it is not optimistic he'll survive," added Ryan, who was joined by RCMP Commissioner Bob Paulson. Wynn, 42, and Derek Walter Bond, an auxiliary constable, were shot in a casino northwest of Edmonton while investigating a suspicious vehicle. Bond was shot in the arm and torso, but was released from hospital on Saturday. Mounties in Alberta identified a suspect on Sunday who was found dead in the hours following the shooting. Police said that Shawn Maxwell Rehn, 34, was the person whose body they found in a home, not far from the Apex Casino in St. Albert where the two officers were shot. Paulson said Rehn had an "incredibly complex criminal history" that included

overlapping firearms bans. Paulson and other officials declined to go into detail about that criminal history, but Paulson noted it may provoke an examination of the police and justice system that allowed Rehn to be free. "I've been policing for 30 years and I've never seen anything the likes of this," Paulson said. Canadian Press (Red Deer Advocate, A1, Leader-Post, A1, Toronto Star, The Guardian, Times & Transcript, MacLean's); Chronicle Herald, A1; Postmedia News (Calgary Herald, A1, Edmonton Journal, A1, StarPhoenix, A1); Globe and Mail, A1; Postmedia News (Edmonton Journal, A1); QMI Agency (Calgary Sun, Edmonton Sun, Winnipeg Sun); Daily Gleaner (Telegraph-Journal); QMI Agency (Toronto Sun, Winnipeg Sun, Ottawa Sun, London Free Press, Kingston Whig Standard, Edmonton Sun, Calgary Sun, Ottawa Sun); * L'Acadie Nouvelle; * Presse Canadienne (La Presse); * QMI Agency (London Free Press);* Agence QMI (Journal de Quebec, Journal de Montreal)

Shooter 'very well known to police'

RCMP say the man who shot two Mounties in St. Albert on Saturday morning was "very, very well known to police". On Sunday, RCMP identified Shawn Maxwell Rehn, 34, a resident of the greater Edmonton area, as the deceased gunman who left two RCMP officers in hospital -- one of whom is not expected to survive. Prior to Saturday's shootings, RCMP say Rehn had an extensive history of firearms related offences and was prohibited from possessing firearms for life. "Rehn represents a significant accumulation of criminality and behaviours that I think will require the RCMP and other stakeholders in the criminal justice system to examine very closely as to how it is this person was walking amongst us," said RCMP Commissioner Bob Paulson. "I think many of us would be surprised to have an individual facing the accusations that he was facing, having the criminal record that he did have, having the unresolved issues that he did have in the community. "There will be a direct and in depth analysis of how it is this individual came to be free." Paulson said the injured officers -- Aux. Const. Derek Walter Bond, 49, and Const. David Matthew Wynn, 42 -- were not aware of the possible danger they faced by confronting Rehn inside the Apex Casino, 24 Boudreau Rd., just outside St. Albert. " They were doing what officers in what every other police force in this country do 24 hours a day -- they investigate suspicious occurrences," said Paulson. "They had no idea who this person was, none whatsoever. There's no way you could expect these officers would know the kind of threat that was going around inside that casino." QMI Agency (Calgary Sun, Edmonton Sun)

'They love' Const. Wynn

Elementary students at a St. Albert school will resume classes Monday without their beloved RCMP liaison officer, after Const. David Wynn was shot in the head Saturday. Wynn, 42, has worked with Keenooshayo elementary school for more than five years, where he delivers the Drug Abuse Resistance Education (DARE) program among other duties. "They love him. He's got a great rapport with the students and he's just a great presence in the school," said St. Albert Public Schools spokesperson Paula Power. "They really all look up to him." Wynn is currently in hospital on life support after a gunman opened fire on him and Const. Derek Walter Bond, 49, at Apex Casino early Saturday morning. Bond was shot in the arm and has been released from hospital. Counselling services will be made available for students and staff on Monday. Power said the district's throughts are with Wynn's family and colleagues. "It's going to be a difficult day tomorrow and a difficult week, for sure. Not only with the students but with the staff too," Power said. "He's part of their school family." QMI Agency (Edmonton Sun, Calgary Sun, Ottawa Sun)

Shooting of auxiliary officer raises safety concerns

The shooting of an auxiliary RCMP officer in Alberta on Saturday is raising questions about whether more could be done to protect the safety of such officers who don't carry firearms. Auxiliary Const. Derek Walter Bond, 49, was shot in the arm and torso when he and a regular RCMP officer - Const. David Matthew Wynn - walked into a casino just north of Edmonton while on a routine investigation. Bond was released from hospital on Saturday evening, while Wynn remains in grave condition and police said he was not expected to survive a gunshot wound to the head. As an auxiliary officer, Bond did not carry a gun though normally auxiliary officers carry pepper spray and a baton. The dramatic events that unfolded in the community of St. Albert on Saturday are thrusting the role of such officers into the spotlight. Rob Creasser, spokesman for the Mounted Police Professional Association of Canada, said there's good reason why auxiliary officers do not carry guns. "They don't have near the training that a regular member does," he said. "They're really not trained in situational use of guns, like when do you pull it and when do

you shoot." He said auxiliary officers are civilians who volunteer part-time to do jobs that free up regular police officers, such as traffic control. They also ride along with officers, as long as they're under the direct supervision of a regular member of the RCMP. There are over 2,000 auxiliary constables in the RCMP across the country. Creasser said they typically wear a RCMP uniform with a small patch on the shoulder that distinguishes them as an auxiliary officer. Canadian Press (Red Deer Advocate, A3)

Police and terror

The more security agencies grapple with terrorist treats, the less they appear to be telling Canadians. Focusing on four current examples of secrecy, the Citizen spoke with security experts about what the public should be entitled to know. The RCMP held a detailed press conference after arresting suspects in an April 2013 plot to derail a Via Rail train. The force did the same on Oct. 20, when a radicalized man killed a soldier in Quebec. It also held an initial press conference after Michael Zehaf-Bibeau attacked in downtown Ottawa Oct. 22. But the force has released only the names and charges in the recent arrest of two twin brothers and a third man, providing no details of what they are alleged to have done. The RCMP said last Wednesday it had no current plans to update the public. Why the secrecy on an issue of such public importance? "The fact that they arrested a third person that was linked to the two brothers could mean their investigation isn't over and they could want to arrest more people," said Michel Juneau-Katsuya, a former senior intelligence officer at the spy agency Canadian Security Intelligence Service (CSIS). But former RCMP superintendent Garry Clement says the public ought to understand what the men are accused of doing. "The one thing I find with the RCMP is, I don't think they do a good job of handling media and they never have," he said, adding that the national capital division tends to be "a lot more conservative" than other divisions, such as the one covering Toronto. Postmedia News (Ottawa Citizen, A1, Windsor Star, StarPhoenix, Leader-Post, Montreal Gazette, The Province, Edmonton Journal)

Bizarre attack lands suspect in lockup

A bizarre series of events left a resident of Happy Valley-Goose Bay scratching his head Friday night. Not only did the man have to deal with an allegedly unprovoked attack by a man he knows, he later had to watch as the Happy-Valley Goose Bay fire department extinguish a blaze at his home. Around midnight, a resident said he was bear-sprayed outside his home by a man he knows. He went inside, and moments later, the man allegedly broke into his home. The resident managed to get him out, according to a news release from the RCMP, but soon he saw the same man lighting his house on fire before running away. The home was left with significant damage. Nobody was injured in the fire. The RCMP says the suspect was found quickly and arrested with no incident. He was charged with arson and assault with a weapon among other offences. The Telegram, A1

Trappers continue to decry exploration

A handful of First Nations trappers continue to camp along a highway in northeast Saskatchewan to protest oil and mineral exploration in the north. "The land is very important to us. It's our store and our drugstore, it's the water that we drink and we're trying to protect that," said Nancy Scanie, an elder from Cold Lake who travelled seven hours to join her colleagues at the camp site over the weekend. The group, dubbed the Northern Trappers Alliance by members, set up a blockade on Highway 955 north of La Loche in late November. Bobby Montgrand, a spokesman for the group, said the RCMP asked them to dismantle the roadblock last month, but that trappers remain in the area. Instead of blocking the road, they're now camping alongside it and waving signs at the trucks that pass by on their way to work sites. "Save the wildlife," reads one. "Save our water," says another. The camp has been manned continuously by about a dozen people for the last two months and Montgrand said no one has any plans to leave. "We're not really worried about the cold because we've got enough work, we've got a fire, we've been living off the land," he said. Clearwater First Nation Chief Ted Clark, who owns a contracting company that's doing exploration work in northern Saskatchewan that was blocked from using Highway 955 in November before the blockade was lifted, said the trappers "are going to be there for a long time." StarPhoenix, A1

RCMP needs three years to implement all changes

The RCMP has accepted all recommendations from an independent review into the police response to the June 4 shootings. But how long it will take to implement each recommendation varies greatly. "There

are 64 recommendations, many of which can be adopted in the short term," said RCMP Commissioner Bob Paulson in the RCMP's response to the MacNeil Report. "Some recommendations have already been implemented, and work is being done on many others. A few of the recommendations will require a more complex response and substantial followup." Paulson said they have prepared an action plan that lays out the response to each recommendation and they will track progress towards implementation. The RCMP's written response to the MacNeil Report contains a response and target date for each of the 64 recommendations, though four of the recommendations have been redacted from the public document because they relate to officer safety equipment. A couple of the recommendations have already been acted upon are listed as complete, while some will be done within three months. Most are targeted to be completed in 2015 and 2016, with a small handful to be completed in 2017. Only one is targeted for completion in 2018. Telegraph-Journal, A1; Times & Transcript, A1

Night of shootings described as 'chaotic'

RCMP Const. Darlene Goguen's experience the evening of June 4 illustrates the chaos that engulfed the police response to an active shooter in Moncton's north end. Goguen, of the Southeast RCMP District, was racing to the scene of the shooting to offer aid to her Codiac RCMP colleagues, according to the independent review of that night prepared by retired RCMP assistant commissioner Alphonse MacNeil. She knew shots were being fired but didn't have a full understanding of the situation. Southeast RCMP uses a different radio frequency than Codiac, so those officers weren't getting the same information. They are also dispatched through Fredericton, so the Operational Communications Centre in Metro Moncton didn't realize she was on her way to the Hildegard Fire Station to offer assistance. "Const. Goguen unknowingly drove directly to the shooter's location as (Justin) Bourque was in the process of firing multiple rounds at police vehicles parked at the intersection of Hildegard and Mailhot," said MacNeil in his report. She heard the shots, started to turn her car around and was hit several times. MacNeil said her quick reaction to reposition her vehicle was a factor in saving her life. She was injured but drove a few blocks to Penrose Street, and another officer eventually got her to hospital. But as MacNeil learned in preparing his report, no one on Codiac's radio channel knew she'd been shot because of the different radio frequency. "Codiac's OCC only learned she had been under fire when someone found her bullet riddled car," says the report. "They mistakenly believed and shared that she had been shot on Penrose Street where her car was parked, adding to the confusion regarding the gunman's movements." Times & Transcript, A1

*** Bourque a 'lone wolf' extremist, says report**

Mountie killer Justin Bourque was a "lone wolf" extremist whose lack of planning made his shooting spree impossible to detect in advance. His actions on the night of June 4 were also looked at as a possible terrorist act but eventually treated as a multiple homicide. That information about the shooting investigation is contained in the independent review into the RCMP response to the June 4 murders of three police officers and shooting of two others, which was released on Friday. The report's author, retired RCMP assistant commissioner Alphonse MacNeil, looked at potential indicators that might have tipped police off to the fact Bourque planned to go on a killing spree. In the end, he determined there was little advance notice of what the killer was going to do. "There was no indication of Bourque planning anything specific until late on the afternoon of June 4; therefore, there was no planning to detect," wrote MacNeil. Bourque is described as a "lone wolf," a term defined as a person who engages in criminal activity who does not belong to an organized terrorist group, acts without the influence of a leader or hierarchy and uses tactics conceived by him or herself. MacNeil said that definition is accepted by several institutions and is used within the RCMP's National Security program. Daily Gleaner, B1

*** Sadly outgunned**

An editorial states, "Justin Bourque outgunned every one of the 24 Mounties who first confronted him when he terrorized Moncton last year. He was hunting for cops with a high-powered M305 Winchester .308 semi-automatic rifle with 20-round magazines. The Mounties had only their handguns, and three shotguns. Moreover, front-line RCMP supervisors didn't have an overall grasp of events on June 4, there were communications breakdowns, and there was no coherent plan to deal with the emergency. What emerges is a picture of chaos in the opening hours of a crisis that dragged on for more than a day. Amid the confusion three brave Mounties were killed that day and two were wounded. It's a credit to their grit that officers went up against Bourque with just their service pistols, given the risk, and a credit to their

restraint that he was finally taken alive to be tried for murder and jailed for 75 years. This tragedy should spur RCMP Commissioner Bob Paulson to rethink the force's crisis training. And Prime Minister Stephen Harper's government should spare no cost equipping the RCMP with high-powered, rapid-fire Colt C8 patrol carbines - short-barrelled assault rifles, essentially. This has been a pressing issue ever since the slayings in Mayerthorpe, Alta., in 2005 of four heavily outgunned Mounties... While the RCMP has been quick to endorse MacNeil's findings, and his many recommendations, this report is a stinging rebuke. Canada deserves better than a national police force that fields poorly supervised, ill-armed, undertrained officers. It has taken a decade to learn Mayerthorpe's lessons. We can only wonder why." Toronto Star, A10

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Solitary confinement faces test**

The first comprehensive legal challenge to Canada's use of solitary confinement in federal prisons will be launched by the British Columbia Civil Liberties Association and John Howard Society of Canada Monday. Even as many countries, including the United States, rein in use of segregation in prisons, Canada's Correctional Investigator says this country has ramped up solitary confinement by 6% in the past five years. The legal challenge to be filed Monday with the Supreme Court of British Columbia argues that administrative segregation is unconstitutional, amounting to "cruel and unusual punishment" that discriminates in particular against mentally ill and aboriginal inmates. The suit comes a month after Correctional Services Canada published its response to the inquest into the death of teenage prisoner Ashley Smith, who spent more than 1,000 days in solitary confinement before killing herself in 2007. In its response, CSC rejected any new limits on the use of administrative segregation and said it could not support the changes "without causing undue risk to the safe management of the federal correctional system." CSC claims segregation is used in limited circumstances when there are no reasonable alternatives and for the shortest time necessary. Critics suggest that is not the case, that on any given day 1,800 prisoners in the federal and provincial system are in solitary confinement; that one in four prisoners spends some time being segregated; and that 16% of inmates are in solitary for more than four months. Carmen Cheung, senior counsel for the BCCLA, said the organization has been calling for reforms since former Supreme Court justice Louise Arbour released a report on Kingston's women's prison nearly 20 years ago that recommended prisoners not spent more than 30 consecutive days in solitary and not more than twice a year. "We hope this lawsuit will force a change where no political change has happened," said Ms. Cheung. Canada has been under increasing pressure at home and abroad over its use of solitary confinement. A UN Special Rapporteur has said being placed in segregation for more than 15 days amounts to torture. Postmedia News (National Post, A4)

Final resolution to triple homicide

A Cambridge Bay man who has spent eight years in custody in different prisons across Canada pleaded guilty to three counts of manslaughter and two counts of attempted murder Jan. 14 at the Nunavut Court of Justice in Iqaluit. The years of incarceration came as a result of earlier convictions, which were overturned on appeal. Chris Bishop's guilty pleas come as a result of a plea bargain between the Crown and defence counsel, accepted by Justice Robert Kilpatrick, who is expected to render a written sentencing decision in a few weeks, completing a dark chapter that has traumatized the community of Cambridge Bay. (...) Bishop was convicted of three counts of second degree murder and two counts of attempted murder in a trial by jury in 2010, and sentenced to life imprisonment. The decision was overturned in the Nunavut Court of Appeal in January 2013 and a new trial was ordered. The plea bargain presented Jan. 14 means a new trial is not necessary but allowed the opportunity for victim impact statements to be made toward sentencing. NWT News/North

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

À quand un programme de déradicalisation chez nous?

"Le Canada est en retard et il doit se doter d'un programme de déradicalisation, c'est la clé du succès", affirme Jocelyn Bélanger, qui s'interroge sur l'absence de mesures chez nous pour réhabiliter les jeunes radicaux. Le professeur au département de psychologie de l'UQAM a fait partie d'un groupe de chercheurs financé par le Département de la défense américaine pour comprendre les processus de radicalisation et de déradicalisation sur plusieurs années et dans plusieurs pays. Selon lui, les programmes de déradicalisation présents aux États- Unis, au Royaume-Uni, dans certains pays du Moyen-Orient et de l'Asie représentent une stratégie très efficace de lutte contre le terrorisme. Le Journal de Montreal, 35

* **IACHR report echoes need for federal inquiry into missing and murdered indigenous women**
Last week the Inter-American Commission on Human Rights (IACHR), an international body and an arm of the Organization of American States, released a report highlighting the grim reality in Canada for many indigenous women and called for a national inquiry or action plan into missing and murdered aboriginal women and girls in Canada, echoing what many domestic and international bodies have been calling for. Being noted on the international stage as a country with a continuing human rights issue is not something the Canadian government should dismiss as not being on its "radar," as Prime Minister Stephen Harper put it in his year-end interview with the CBC's Peter Mansbridge: "You know, our ministers will continue to dialogue with those who are concerned about this. They're studying it. But we have an awful lot of studies and information on the phenomenon and an awful good indication of what the record is in terms of investigation and prevention of these sorts of things." The report issued in Washington, D.C. Jan. 12 rebuts the well-trodden government sentiment that further study isn't needed. It says that to get to the root of the problem there is still "much more to understand and to acknowledge in relation to the missing and murdered indigenous women." The IACHR reiterates that Canada still needs to address the root causes and history of violence against women and systemic racial discrimination as seen through the Indian Act and residential schools, which has made generations of indigenous women more vulnerable to high levels of violence. It points to the lack of due diligence on the part of the police and the state in cases of violence against indigenous women in implementing measures to address the social and economic inequalities that perpetuate it. Hill Times

* **Canada's gang hotspots - are you in one?**
In Atlantic Canada, the Bacchus outlaw motorcycle club runs the drug trade, according to police biker crime specialists. In oil-rich Alberta, bullets fly when the Red Scorpions clash with the United Nations crew. In the Prairies, the White Boy Posse's migration east from Edmonton has spilled blood in Saskatchewan. Gang activity even blights Ottawa, one of the world's safest cities. The capital logged a record 49 shootings in 2014, prompting police to address concerns about gangland disputes. Among those incidents was a targeted Boxing Day shooting that wounded one man during what investigators called "infighting" between members of the Crips. Although Canada's crime rate is trending down, organized crime hotspots still seethe - often outside the urban hubs of Toronto, Montreal and Vancouver. Saskatoon averaged two gang-related homicides a year between 2003 and 2012, according to Statistics Canada. Its annual average rate of 0.89 gang-related murders per 100,000 population more than doubles the per capita rates in Montreal, Toronto and Calgary. "Let's not put blinders on and think this isn't happening in our smaller cities," said Toronto author Jeff Pearce, whose 2009 book Gangs in Canada is used as a textbook in B.C. criminology courses. Whether it's Alberta's oil or Saskatchewan's potash, boomtowns are not immune. (...)The latest national figures cited by **Public Safety Canada** date back to 2002. They put the number of "youth gangs" at 434, representing some 7,000 members. Ontario harboured the most youth gangsters with 3,320; Saskatchewan followed with 1,315 gang members. Abbotsford-Mission in B.C.'s Fraser Valley takes the title of gangland murder capital of Canada. It averaged 1.02 gang-related slayings per 100,000 population between 2003 and 2012, a figure likely elevated by 11 mostly gang-related murders in 2009. CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

Sick females a PS 'crisis'
Women in the public service go on disability leave at almost twice the rate of men, a problem some experts say should be addressed as part of the government's new disability management scheme. The

federal disability insurance plan, managed by Sun Life Financial, is the biggest in Canada. A Sun Life report obtained by the Citizen shows women have ended up on long-term disability at rates vastly disproportionate to their numbers in the public service for more than a decade, especially for mental health conditions. "It's a crisis, a toxic mix of gender, age and work strata ... and it can no longer go unnoticed. The government has an obligation and duty to care," said Joseph Ricciuti, president of SEB Benefits and HR Consulting. "In the meantime, the poor disability-claims numbers speak for themselves and will continue to impact women in the workforce, who are the hardest-hit and paying the socio-economic price." Ottawa Citizen, A1

Ex-PS worker wins battle for back pay
Doug Nicol's six-year battle with the federal government cost him his livelihood, his health and his marriage. The 55-year-old former public servant in Edmonton was forced to rely on food banks and scrounge for empty bottles for cash. Twice he almost lost his house. Last month, Nicol got his best Christmas present ever: An adjudicator awarded him three years' pay and $38,000 in damages after finding that his employer, Service Canada, made no real effort to accommodate his disabilities and engaged in discriminatory practices "wilfully and recklessly." The Public Service Labour Relations and Employment Board upheld a June 2008 grievance by Nicol, a former EI claims assessor with Service Canada who took medical retirement in December 2011. Nicol alleged that Service Canada denied him accommodation for physical and mental disabilities, causing him "serious financial, physical and psychological damages." He also alleged his employer discriminated against him on the basis of his disability. Ottawa Citizen, A7

OTHER

MacIntosh arrested on child sex charges
A former Cape Breton businessman has been arrested in Nepal on charges he lured a nine-year-old boy to his hotel room and had sex with him, a police official said Saturday. Ernest Fenwick MacIntosh, 71, was arrested at a hotel in Lalitpur, a suburb south of the capital, Kathmandu. He was ordered detained by the district court until the charges could be further investigated, Lalitpur's police chief Pushpa Ranjit said. MacIntosh arrived in Nepal on a tourist visa in August 2014, and was a frequent visitor to the children's shelter where the boy lived, and they met there, police said. They also said that Macintosh has been accused of threatening the boy. The Himalayan Times quoted a spokesperson with the Metropolitan Police Range in Jawalakhel as saying the alleged incident at the hotel occurred on Dec. 13. The newspaper report said police received a complaint from the family of the alleged victim on Dec. 19 that a Canadian tourist lured him into a room at a guest house. Police declined to provide further details because the case involves a minor, however, they said they were trying to determine whether there might be other alleged victims. Cape Breton Post, A1

Canada must aid flogged prisoner
An opinion piece states, “There are many reasons the Canadian government should condemn Saudi Arabia more strongly than it has for torturing a blogger (issuing only a "concerned" public request for clemency), and many reasons it should have condemned the torture much sooner than it did (making its request five days after the first 50 lashes of 1,000, and only after the Globe and Mail pressed it about apparent trade meetings with Saudi royals). But three reasons are so compelling that they deserve emphasis, although they're so obvious that they shouldn't need it. First, the Canadian government has a stronger relationship with liberal blogger Raif Badawi - and a greater responsibility to convince Saudi Arabia to stop torturing him - than any other government. But because the blogger isn't Canadian, the Canadian government claims it can't do much. That's transparently craven wishful thinking. While Badawi can't assert the consular rights of a Canadian citizen, his wife and children live in Canada.” Ottawa Citizen, C4, Le Devoir

*** Baird's moral laryngitis**
A letter to the editor states, “Fahmy remains in jail despite Baird's visit, Jan. 16 Foreign Affairs Minister John Baird's "very long and in-depth discussion" was "constructive and fruitful." I suspect this is "diplomat-speak" for a nice lunch where nothing meaningful was said or heard. But then, why should we expect

Egypt to hear complaints from a country that rounds up protesters and bystanders like cattle (dip-speak, "kettles"), that detains foreigners for years without charge or trial (dip-speak, "security certificate") and that keeps the mentally ill in solitary confinement for months on end (sorry, no euphemism available). Our government has contracted moral laryngitis and can no longer speak for our citizens at home or abroad. Perhaps Mr. Fahmy remains in jail because, not in spite, of this intervention." Toronto Star, A10

INTERNATIONAL

France releases three terror suspects

French police have released three female suspects from questioning, but will keep nine other people in custody as part of an anti-terror investigation connected to last week's attacks in Paris that have put Europe on high alert, officials said Sunday. Amid the heightened European vigilance, a far-right rally in Germany planned for Monday was cancelled over a terrorism threat, Italy said it had expelled nine suspected jihadis since late December and Britain's home secretary called for new action to fight anti-Semitism in the wake of the Paris attacks. AP (The Guardian, The Chronicle-Herald, Toronto Star, Cape Breton Post, The Province, Leader-Post, The Gazette, Windsor Star, Calgary Herald, Ottawa Citizen, Vancouver Sun, Edmonton Journal)

Islamic State frees hundreds of captives

The Islamic State group released about 200 Yazidis held for five months in Iraq, mostly elderly, infirm captives who likely slowed the extremists down, Kurdish military officials said Sunday. Almost all of the freed prisoners are in poor health and bore signs of abuse and neglect. General Shirko Fatih, commander of Kurdish peshmerga forces in the northern Iraqi city of Kirkuk, said it appears the militants released the prisoners because they were too much of a burden. "It probably became too expensive to feed them and care for them," he said. Tens of thousands of Yazidis fled in August when the IS group captured the northern Iraqi town of Sinjar. Hundreds were taken captive by the group. Globe and Mail, A5 (Chronicle-Herald), * Associated Press (Acadie nouvelle, Le Devoir, National Post, Waterloo Region Record, Toronto Star, Canada.com)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
March 3, 2015 / le 3 mars 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Ontario revamps efforts to name unidentified dead
When the federal government created a national missing-persons centre in 2011, the presumption was it would supplant siloed provincial and territorial online efforts and serve as a better tool for matching the vanished with the anonymous dead. But the RCMP-led National Centre for Missing Persons and Unidentified Remains (NCMPUR) hasn't progressed fast enough for Ontario, the province with the most anonymous dead. A Globe and Mail investigation has found that Canada's strategy falls far short of the U.S. model, considered the gold standard. The Ontario chief coroner's office and forensic pathology service are now working with the provincial police to revamp their digital outreach to help identify the nameless and bring some closure to families of the disappeared. In some cases, identifications could breathe new life into stalled police investigations and help bring killers to justice. (…) Jean-Christophe de Le Rue, a spokesman for **Public Safety Minister Steven Blaney,** said the government is committed to ensuring the data bank is effective. He said DNA analysis will be consistent with international practices. There are 697 anonymous dead in Canada, according to a Globe survey of the country's coroners and medical examiners. One third of those remains are in Ontario. Globe and Mail A1

Chill sets in over anti-terror laws - Filmmaker concerned he'll be labelled terrorist
Winnipeg filmmaker says he fears the government's anti-terror legislation could ensnare him as he works to produce and promote a miniseries based on a book about an attack on Canada by indigenous fighters. Jeremy Torrie, president and head of distribution for Bandwidth Digital Releasing and High Definition Pictures, said he is working on an eight-part miniseries based on Douglas Bland's book Uprising. The

novel, published in 2009, is a fictional account of the attacks on Canada's military bases and power stations by disgruntled indigenous youth who have found a modern-day revolutionary leader. He hopes to establish a social media campaign when the miniseries is released to foster a real discussion of the issues facing aboriginal youth and why the book and miniseries are not farfetched. Torrie fears provisions in Bill C-51, which makes it a crime to knowingly advocate or promote terrorist offences, could make him a target. "Just me posting some of my ideas for this drama series would be enough for them to throw me in jail and not charge me until they determine they've taught me a lesson, and perhaps even try to dissuade me from producing the series," Torrie said. "Literally freedom of speech, of expression is at stake here." The new law says it can apply to someone who purposely tells someone else to commit terrorism but also to someone whose comments might lead someone to do so, regardless of whether that was the intention, and regardless of whether the comments result in a terrorist activity. It is punishable by up to five years in prison. Jean-Christophe de Le Rue, director of communications for **Public Safety Minister Steven Blaney**, said the bill is clear. "It does not include lawful advocacy, protest, dissent and artistic expression," said de Le Rue. "This bill targets those who advocate, promote or would commit acts of terrorism against Canadians." Winnipeg Free Press, A2

Leader's words should strengthen, not scare, nation
A new catchphrase is spreading through the rhetoric of Stephen Harper and his ministers. It is only four words - they hate our values - but it packs an emotional wallop. The prime minister road-tested it on an audience in Richmond Hill in January. "Canadians are targeted by jihadi terrorists for no other reason than that we are Canadians," he warned. "They hate our society and the values it represents." He used it in a different context in Quebec City two weeks ago. This time, he lashed out at employees of Radio-Canada. "I remain convinced that Quebecers are not leftists, contrary to the image conveyed by some media or the opposition parties," he said. "I understand that there are many at Radio-Canada who hate these values but I think that these values are the true values of a large percentage of Quebecers." **Public Safety Minister Steven Blaney** echoed the mantra as he headed to an international security summit in Washington last week. **"Canadians are being targeted by jihadi terrorists simply because these terrorists hate our society and the values it represents."** In some ways this epithet is like previous Tory terms: soft on crime, Taliban sympathizer, defender of child pornography. It is simple, spiteful and calculated to whip up strong feelings. The Guardian, A7

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Winter not ready to relinquish icy grip, says meteorologist**
The eye of the snowy storm is passing the city, but now Saint John will have to deal with colder-than-average temperatures. Last month, the province experienced some of the coldest temperatures on record. Environment Canada... said the city was unusually chilly in February. And colder temperatures mean more snow... [I]t's likely the city will be hit with at least one late winter storm, although any system tracks are as yet undetermined. An early-March sprinkling of snow has already caused minor issues in the city, with a handful of collisions due to slippery road conditions, including one that closed a highway on Monday morning. Telegraph-Journal, B3

*** Emergency response could improve, report says**
The ice storm of 2013 saw two years worth of freezing rain fall in two days, the weight of which snapped off branches and toppled trees. Power lines were brought down in their wake with the result that more than 400,000 Toronto Hydro customers - at least a million people - went without electricity and heat, some for days and weeks. The province jumped in to offer support to municipalities across Ontario and a new report by the Office of the Fire Marshal and Emergency Management has given the government's response a passing grade. The review, called the 2013 Southern Ontario Ice Storm report, also contains two dozen recommendations to improve communications and co-ordination efforts when future emergencies occur. Toronto Star, GT2

*** Power outages in Sydenham District**
Kingston Hydro will be conducting repairs to the underground electric lines in the Sydenham District that will require some planned power outages on Wednesday. Customers in the Sydenham District areas

listed below will experience power outages ranging from 15 minutes to two hours. Kingston Whig-Standard, A6

*** City studying ways to help frozen pipe victims**
The city will study the prospect of compassionate grants and other aid for homeowners struggling to repair frozen water lines after a record February deep freeze. The coldest February in Hamilton's history was mostly to blame for a record 700 calls to the city about frozen water lines this winter. That exceeds last year's record of around 570 in what had been considered a winter anomaly. But the city can't afford to ignore the possibility of a troubling new trend, councillors said at a public works meeting Monday. Hamilton Spectator, A6

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Disclosing dangerous goods risks terror: CP
Terrorism poses a greater risk to railways and the communities they pass through than derailments do, and notifying public officials of dangerous-goods shipments may actually increase the risk of attacks, says the CEO of Canadian Pacific Railway Ltd. "I will notify every public official every day of what's on that train if they want to know it," Hunter Harrison said Monday in a speech to the Canadian Club of Toronto. "But if you want to give someone the opportunity to break that custody chain and look at the list and say, 'Here's what that car's got in it and here's the location and here's all the bad things I could do' - I don't think we want that." Mr. Harrison told reporters after his speech that he fears terrorism more than derailments "because it can be planned to do the worst possible damage." Following the Lac-Megantic disaster in 2013, Transport Canada introduced new regulations that require Class 1 railways, including CP and Canadian National Railway Co., to provide a quarterly breakdown of the nature and volume of dangerous goods they transport through each municipality. Some critics have called for even more disclosure. Postmedia (National Post FP1/ Front, Calgary Herald Ci/ Front, Vancouver Sun, Ottawa Citizen, Star Phoenix, Montreal Gazette, Edmonton Journal, Financial Post), Globe and Mail; * Canadian Press (The Chronicle-Herald, La Tribune, Times Colonist); Le Devoir

Kenney soldier tweet upset guards
Internal emails show a minister's tweet sparked confusion, frustration and anger as Cpl. Nathan Cirillo's comrades learned about the Canadian soldier's death on Oct. 22 from news reports rather than through official military channels. Cirillo was standing guard with another soldier in front of the National War Memorial shortly before 10 a.m. that morning when a lone gunman shot him in the back. The gunman then drove to Parliament Hill and rushed through the main doors of the Centre Block, where he was killed in a shootout with RCMP officers and Hill security staff. The unprecedented attack prompted an immediate lockdown of military and federal institutions across Canada, amid fears of a coordinated assault on Ottawa and an absence of concrete information. At 1:24 p.m., nearly four hours after Cirillo was shot, a message went out to military commanders across the country providing a brief update on the situation. "There will be no public release of his name or condition until it is certain all information is accurate and the family has agreed to do so," the message added. But 15 minutes later, at 1:40 p.m., then-employment minister Jason Kenney became the first to confirm that the 24-year-old reservist had died, tweeting: "Condolences to family of the soldier killed, prayers for the Parliamentary guard wounded." Kenney has since been named defence minister. The minister's comment sparked a flurry of news reports. In response, Sgt. Tim Perry of the Canadian Forces' Ceremonial Guards emailed his commanding officer, Maj. Michel Lavigne, at 1:53 p.m., saying: "I need a padre and confirmation if Cpl. (Cirillo) is dead or not. My guys are learning from CBC on his status." Postmedia (Ottawa Citizen A1/ Front)

Islamic researcher delves conversion ties to terror
Converts are overrepresented among those few western Muslims who have committed acts of terror. Dr. Scott Flower, an Australian researcher completing a federally funded study of Canadian converts, tells the Ottawa Citizen's Dylan Robertson why we know so little about converts. Q. Imams are concerned by a spike of coverts to Islam after the attacks last October in Ottawa and St-Jeansur-Richelieu, Que. Have you seen spikes in converts? A. For sure, and the Sept. 11, 2001, terror attacks are probably the biggest

example. A lot of the converts I've talked to said that before 9/11, people hadn't really heard of Islam or knew what Muslims believe, and it sent them on a quest for knowledge. Some of the people on that quest eventually convert. I wouldn't say it's necessarily causal, but certainly there's a relation between these big events and increases in conversion. And we likely see that with the onset of ISIL (Islamic State) on the world stage in the last 10 months. Obviously there's also a much, much smaller group of people who are drawn for other reasons. Like, they might have a mental-health problem and have been looking for some ideology to mobilize their grievance. Those individuals seek a more extremist form of Islam, but they're very much a black swan. The statistics on conversion in most western countries are very poor, even non-existent, and that's what our project is trying to do, get some hard statistics. Edmonton Journal, C11

If you're so sure of C-51, debate it
An opinion piece by Tom Mulclair states..."Justice Minister Peter MacKay is out of touch with reality when he pretends the official Opposition is on "the sidelines" of Bill C-51 ('Freedom and security, hand in hand,' Feb. 28). In fact, New Democrats have been on the front line - leading the charge - opposing Conservative schemes to ram it through Parliament at all costs. If the minister and his government were really serious about security, they wouldn't shy away from meaningful study and debate of this sweeping new bill. (...) As New Democrats oppose C-51 and the Liberals vote for it, more than a hundred of Canada's brightest legal experts from institutions across the country sent an open letter to all members of Parliament expressing their "deep concern" about C-51. They call the Conservative bill a "dangerous piece of legislation in terms of its potential impacts on the rule of law, on constitutionally and internationally protected rights, and on the health of Canada's democracy." The NDP believes we need responsible approaches to protecting Canadian values and freedoms, as well as our personal safety." National Post, A9

*** Nuttall was obsessed about leaving DNA evidence, trial hears**
In surveillance video shown to a jury Monday, an agitated-looking John Nuttall is seen pacing around a motel room, giving orders to his wife, Amanda Korody, and obsessing about not leaving traces of DNA for police. Nuttall and Korody have pleaded not guilty to four terrorism-related charges alleging they conspired to explode bombs at the B.C. legislature in Victoria on Canada Day 2013. Monday's video showed the Surrey couple back at a Delta motel room where they have assembled items to build the pressure-cooker bombs they plan to use in the terror attack. Postmedia (The Province, A9, Vancouver Sun); Canadian Press (National Post A6); Times Colonist, A2

*** Muslim group aims to create 'united front' against terrorism**
Hundreds of Muslim families across Canada are opening their doors to their neighbours in an effort to "dispel myths" and "stand united" against terrorism. The program, called Meet A Muslim Family, is spearheaded by Ahmadiyya Muslim Jama mosques from coast to coast. "This campaign comes at a unique time, especially here in Canada given everything we've seen in the past few months, the various terrorist-related activities and various international headlines that have turned a lot of heads towards the Muslim community," spokesman Safwan Choudhry said. "Surely, our fellow Canadians must be scratching their heads and saying, 'What exactly is going on and where is this sudden rise in radicalization coming from?' "Choudhry said terrorist organizations of all stripes have "one thing in common, which is to create fear, which leads to division." QMI Agency (Kingston-Whig Standard B2, Ottawa Sun, Calgary Sun, Edmonton Sun, Toronto Sun, Winnipeg Sun)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

The spies next door
New figures show Canada has turfed out five spies in the past decade from a surprising source country - its best friend and ally, the United States. From 2004 to 2014 Ottawa sent back to the U.S. five of a total of 21 of those barred from Canada "on security grounds for engaging in an act of espionage that is against Canada or that is contrary to Canada's interests," according to a document produced by Canada Border Services Agency. It's not clear if the espionage was by foreign government agents or if it was industrial espionage - that is, spying to obtain state secrets, intellectual property or corporate secrets. A document released under access to information laws shows the suspected spies were permanent

residents or foreign nationals deemed inadmissible on security grounds, but doesn't break down them down by citizenship. Rather, it indicates the country the spies were sent back to. Still, the fact that the U.S. is the origin of the most espionage cases is surprising, especially given the emphasis put by federal politicians - including two former CSIS directors, one of whom is now national security adviser to Prime Minister Stephen Harper - on China as a suspected source of espionage. Toronto Star, A1, La Presse, A2/ Front (Le Quotidien 14/ Front, * Le Soleil, La Voix de l'Est)

Canada's DeHart decision 'shameful'

While Matt DeHart appeared briefly inside a Buffalo courtroom after his deportation from Canada where he had sought political asylum, outside, a prominent international whistleblower support group hailed him for his courage. Mr. DeHart, 30, was turned over to U.S. authorities by Canada Border Services Agency on Sunday and on Monday he was named the third beneficiary of the Courage Foundation, an international organization. Mr. DeHart joins two previous beneficiaries, both wellknown newsmakers: Edward Snowden, the former National Security Agency analyst who leaked documents revealing large-scale global surveillance, and Jeremy Hammond, serving 10 years in a U.S. prison after hacked email from security think-tank Stratfor was published through WikiLeaks, the whistle-blowing organization. "Canada's actions are shameful. It may as well not have a border," said WikiLeaks founder Julian Assange in a statement. (WikiLeaks is linked to the Courage Foundation through its founder, Sarah Harrison, who is a WikiLeaks editor.) "The abuse of the law in DeHart's case is obvious, shocking and wrong," said Mr. Assange. In a tweet, WikiLeaks referred to Mr. DeHart as an "alleged WikiLeaks middleman." Mr. Assange remains in exile in Ecuador's London embassy where he took refuge against extradition to Sweden where he is wanted for questioning on sex-crime allegations. Questions about Mr. DeHart's treatment were revealed in a long investigation by the National Post in May. National Post, A6

Child porn smuggler has prison sentence reduced

Border officials hailed it as one of the harshest sentences ever of its kind. Now a truck driver convicted of smuggling child pornography across the border has won a court fight to reduce his 30-month prison sentence. In a decision released last week, the Manitoba Court of Appeal ruled the sentence unfit and replaced it with a sentence of 20 months. Denys Valeriyovych Basov, 38, was arrested May 7, 2013 in Emerson after border officials found over 300 images and six videos depicting child pornography on his laptop computer. Didn't consider record Vasov argued on appeal the sentencing judge placed undue weight on the number of images found on his computer and failed to take into account that he was a first-time offender. The appeal court ruled the sentencing judge was entitled to consider the number of images as an aggravating factor, but erred in not properly considering Basov's clean prior record. "Generally speaking, the presence or absence of a criminal record is a significant factor in determining an appropriate sentence," Justice Holly Beard wrote. Winnipeg Sun, 4

Dead man believed to be drug trafficker's brother

A man found dead in a vehicle in Surrey on Friday is believed to be the brother of a convicted B.C. drug trafficker. Surrey RCMP were called just after 10 a.m. to the 9500-block 139th Street, where the dead man was found. The death was deemed suspicious and the Integrated Homicide Investigation Team joined the investigation. Police sources say the victim, who is believed to have been shot, is Mike Russell, brother of Edward "Skeeter" Russell. Using social media, Edward Russell wrote that his brother had passed away. Integrated Homicide Investigation Team spokeswoman Sgt. Stephanie Ashton was unable to confirm the dead man's identity, however she said an update on the investigation is expected in the next day or two. In 2011 Edward Russell was sentenced in U.S. District Court in Seattle to four-and-a-half years in prison after pleading guilty to charges related to the operation of a Hells Angelsconnected drug smuggling ring that was busted in 2008. Marijuana, cocaine and cash crossed the border in hollow logs, wood chips and secret compartments in tractor-trailers. Russell admitted to helping arrange for marijuana to be smuggled across the border. Edward Russell's name also came up in testimony during the Surrey Six trial. The Province, A3

Lawyer admits to negligence

A Toronto lawyer who represented hundreds of Roma Hungarian refugees has admitted to professional misconduct for failing to adequately prepare some of his clients' claims for asylum. At a disciplinary hearing Monday, Viktor Hohots filed an agreed statement of facts with a Law Society of Upper Canada

panel relating to allegations made by 13 complainants, all Roma refugees from Hungary, between August 2009 and February 2012. In his submission, Hohots said he "failed to assume complete professional responsibility for his practice and that he failed to directly and effectively supervise the non-lawyer staff of his law office to whom he delegated the preparation of refugee claims." Supporters of the complainants - most of whom were denied asylum and have been deported - hope Immigration Minister Chris Alexander can reopen their files, given Hohots's admission. They include a Roma family who sought sanctuary in a Toronto church for three years, hoping their claim would finally be accepted. Both Hohots and Mitchell Worsoff, his lawyer, said they would reserve their comments until his penalty hearing on May 11. Hohots could face suspension, supervised practice or lose his licence. Refugee lawyers and advocates hailed Hohots's admission of misconduct, saying it exonerates people who had claimed substandard work on his part had led to their asylum - and justice - being denied. Toronto Star, GT1

BSE case prompts U.S. calls for COOL

A handful of U.S. farm groups are using Canada's newest BSE case to prop up arguments in favour of mandatory country-of-origin labelling, or COOL. Among the organizations attempting to draw a link between the labelling law and the latest infected cow is R-CALF - the Ranchers-Cattlemen Action Legal Fund - the same U.S. lobby group that became the bane of the Canadian beef industry during the height of this country's BSE crisis more than a decade ago. But John Masswohl, director of government and international relations for the Canadian Cattlemen's Association, said he doesn't expect the rumblings of a few extreme protectionists to have an impact on Canada's efforts to get the controversial U.S. labelling law repealed. "We always expect the usual suspects to provide the usual spin. We're pretty confident that nobody in the States really pays attention to R-CALF, a Montana-based cattle producers' lobby group, became infamous in Canada in 2004 when it successfully obtained a court injunction blocking the planned reopening of the U.S. border to Canadian beef products. The ensuing legal wrangling lasted more than a year and was one of the reasons bovine spongiform encephalopathy became such a costly and difficult episode in Canadian agriculture history. Now, R-CALF is again raising alarm bells about Canada's food safety system. Last week, the organization's CEO Bill Bullard said the discovery of a new case near Spruce Grove is proof the U.S. Congress should not repeal COOL - even though the law has been successfully challenged at the World Trade Organization by Canada and Mexico for being discriminatory and violating trade agreements. Calgary Herald, C1; Edmonton Journal

Whale meat shipped through port

Canada is opposed to the hunting of the endangered fin whale, but apparently can't do anything about being used as a conduit for the animal's meat. NDP MP Don Davies on Monday used the fact World Wildlife Day is Tuesday to highlight that Canada is being used to facilitate trade in whale meat. Canada is part of an agreement, the Convention on International Trade in Endangered Species of Wild Fauna and Flora, that bans commercial hunting of endangered species. The fin whale, which is the second-largest creature, after the blue whale, remains at risk. But one shipment of fin whale meat from Iceland was sent to Halifax in January 2014 and shipped by rail to Vancouver for export to Japan. Another shipment of an unknown type of whale meat was sent from Nova Scotia in March 2014 to Iceland, according to export data from Statistics Canada. "Canada's marine mammal regulations prohibit the commercial export of any cetacean species," said Davies. "I'm calling on the government to take their international obligations seriously, to quit breaking the law and to protect endangered species." Davies asked Canada Border Services Agency why they allowed shipment of an illegal substance. "They felt they couldn't intercept this shipment because it was in 'bond'," said Davis. "What if we found there were narcotics involved - heroin, cocaine? I don't think any federal government department would be saying they couldn't do anything." The CBSA passed responsibility for the whale meat shipment to Environment Canada, which did not provide a response by press time Monday. The Province, A7

Canada customs launches tool to fight counterfeit

Many U.S. brand owners already work with U.S. Customs and Border Protection (CBP), a division of the U.S. Department of Homeland Security, to keep counterfeit products out of the U.S. CBP examines cargo at more than 300 ports of entry into the U.S., and seizes goods that appear to infringe registered trademarks and copyrights on record with CBP. CBP also has the authority to seize any goods entering the United States, even if the goods are not intended for the U.S. market and the shipment is simply passing through the United States to another country. CBP can also issue monetary fines, request that

the U.S. Attorney's Office criminally prosecute the offenders, and/or coordinate and participate in raids on international counterfeit production facilities. Customs Today.com

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** 'Human error' blamed for Rogers breach**
Rogers Communications Inc. says that a security breach it is attributing to "human error" has resulted in outsiders gaining access to information associated with dozens of its medium-size business accounts. The intruders appear to have used a technique known as "social engineering" - which relies on manipulating people into volunteering confidential information - to trick an IT support agent into handing over an employee's confidential details that were then used to gain access to Rogers's internal records. Globe and Mail, B3; Windsor Star (Edmonton Journal); Canadian Press (National Post, Toronto Star)

*** Canada Revenue Agency warns of email and phone scams**
The Canada Revenue Agency is warning Canadians to beware of telephone calls or emails that claim to be from the CRA but are not. In a media release, the national agency explained that these are phishing and other fraudulent scams that could result in identity and financial theft. Some of these scams ask for personal information directly, and others - such as the email scams - refer to a website resembling the CRA's, where visitors are asked to confirm their identity by entering personal information. People are strongly advised not to click on the links to these websites if they receive such an email. Email scams may also contain malicious software that can harm your computer and put your personal information at risk. Daily Gleaner, A8

*** Shared Services Canada plans data centre expansion in Ottawa**
The federal government is moving ahead with plans to refurbish a data centre in Ottawa — a project that could take years to complete, and possibly cost more than $100 million. The plan is to refurbish an existing data centre by the airport to be a second "development" data centre, which is essentially a space to test programs before they go live, making it one of the seven data centres the government wanted to keep open as part of a massive IT overhaul that the government is undertaking to reduce costs, tighten cyber-security, and help make the public service more nimble. When work to consolidate 485 data centres into seven is complete — sometime around 2020 — the government expects to save about $100 million a year in operating costs. OttawaCitizen.com

*** Computer expert warns Canadians: Watch out for 'Superfish'**
A Whitehorse computer expert is warning Canadians about a computer vulnerability — and he's mentioning one computer brand by name. Martin Lehner is a security expert at Orange Technology in Whitehorse. He says users of Lenovo computers should get their computers checked for pre-installed software. Lehner says many Lenovo computers have software called, "Superfish", which is installed at the factory. The software is designed to wedge sponsored advertising into web sites, but in doing so opens a door to hackers. CBC.ca

LAW ENFORCEMENT / APPLICATION DE LA LOI

Candlelight vigil to mark 'horrible day'
A candlelight vigil will be held in Mayerthorpe today to commemorate the fallen four RCMP officers on the 10th anniversary of their deaths. In Red Deer, Keith and Colleen Myrol will gather with friends and family to remember their son Brock Myrol, 29, who was slain along with Constables Anthony Gordon, Leo Johnston and Peter Schiemann. "It's a strange day because it's not a celebration," said Keith. "It's the marking of a day that actually was a horrible day. "So we'll just work our way through the day." Myrol said their daughter and her husband and grandchildren all live in town and some friends are also stopping by. "We won't be alone. That's the main thing." There have been many events over the years to remember

the sacrifices of the four young RCMP officers and the Myrols are grateful for the thoughts and messages from other Canadians. Red Deer Advocate, A1

'I put my forehead against his ... It was just me and him'
When RCMP Const. Leo Johnston was shot dead in Mayerthorpe 10 years ago, Lee Johnston lost half of himself. That's how the identical twin, also an RCMP officer, describes the murder of his brother, killed alongside three other RCMP officers in an ambush at a Mayerthorpe farm. Lee Johnston is now a corporal in Ottawa, working in tactical training. Ten years ago, he was a constable in Surrey, B.C.; Leo a constable in Mayerthorpe. The brothers were born nine minutes apart - Leo first, then Lee - and had always been close, growing up on a farm near Lac La Biche. The night before Leo died, he and Lee had written back and forth on MSN Messenger, as they often did, chatting until after midnight. On the morning of March 3, 2005, around the time of the killings in Alberta, Lee woke suddenly from a deep sleep. He soon dozed off, unsure what had woken him. Around 11:30 a.m., as he was driving to work, his mom called, wondering if he had heard what was going on in Mayerthorpe. "I just started crying," Lee remembers. "I couldn't help it. I almost never cry. But I just had a feeling." Confirmation that Leo had been killed didn't come for hours. But by then, shock had settled in. Postmedia News (Edmonton Journal, A1)

From Devastation to Forgiveness
A decade ago, Rev. Don Schiemann felt like his arm was ripped off. It's the starkest way the 63-yearold can describe the 10 years since his son, Const. Peter Schiemann, was killed in the line of duty. His grief began with the shock and pain of a sudden, vicious wound, followed by rough years of scars and scabs. He's lived through months of pain and recovery. "Over time, the wound heals, but you always miss that arm," Schiemann says. "It gets better, to a point, but that arm never comes back." In March 2005, RCMP Const. Peter Schiemann - just two months shy of his 26th birthday - was killed with three fellow officers on James Roszko's farm north of Mayerthorpe. The enraged Roszko, known as the town bully and a renowned police-hater, ambushed Schiemann and constables Leo Johnston, Anthony Gordon and Brock Myrol during an investigation at his property. Roszko then shot himself. Since then, Don Schiemann has lived in a world of emotional triggers. Violent news reports - including the June 2014 shooting of RCMP officers in Moncton and the January murder of St. Albert Const. David Wynn - bring pain, as do the holidays and birthdays other families take for granted. Schiemann, a Lutheran minister, cherishes the memory of his son's surprise Sunday morning visits at church in Stony Plain during his drives between Edmonton and Mayerthorpe. The smiling officer would slide into a seat beside his family before anyone knew he was there. "That was Peter," Schiemann remembers fondly. Sitting near an empty pew on a recent Sunday, just for a moment, Schiemann still expected his son to pop by. Postmedia News (Edmonton Journal, Calgary Herald)

* **Fallen 4 Marathon gives back**
A memorial marathon set up after four Mounties were slain in Mayerthorpe on March 3, 2005, continues to improve lives in the community. Since it was created six years ago, the Fallen 4 Marathon Society has raised $178,000 for Whitecourt and Mayerthorpe -- with $29,000 handed out in 2014 from the 1,400 who participated in the two-day event. The four constables -- Anthony Gordon, Lionide Johnston, Brock Myrol and Peter Schiemann -- were gunned down by cop-hater James Roszko, who then turned a gun on himself, at his farm near Mayerthorpe. Tina Prodaniuk, Whitecourt Crime Prevention Coordinator and chairwoman of the Fallen 4 Memorial Society, says the marathon has been a chance to pay homage to the constables. EMS and most of the RCMP, peace officers and fire department are volunteers. "They come out because they want to help with the event," she said. The Fallen Four Marathon starts at the Mayerthorpe Fallen Four Memorial Park and ends up in Whitecourt, connecting the communities where the officers were from. Part of the proceeds also go towards the Fallen Four Memorial Society. QMI Agency (Calgary Sun, Edmonton Sun)

* **Town rises above its grim legacy**
In a once-vacant lot on the south edge of Mayerthorpe stand four life-size bronze statues of constables Brock Myrol, Anthony Gordon, Leo Johnston and Peter Schiemann. The solemn figures surround a monument topped with skyward doves, honouring all Canadians who have died while wearing a uniform. Each officer stands on guard in a different position according to his length of service and faces a different direction, toward his hometown or his first posting. The Fallen Four Memorial Park commemorates the

RCMP officers shot dead on March 3, 2005, on James Roszko's farm north of Rochfort Bridge, a tiny community about 130 kilometres northwest of Edmonton. For 10 years, the shooting has cast a shadow on nearby Mayerthorpe, where three of the four officers were based. The town of 1,500 people has become synonymous with one horrible act. "I feel bad for the town of Mayerthorpe, but you say the word Mayerthorpe and the RCMP and it only means one thing," said Deputy Commissioner Marianne Ryan, the head of Alberta's Mounties. "It means tragedy." In the years since the massacre, the Fallen Four Memorial Park has become Mayerthorpe's reminder of what happened, and its way to redefine the legacy, says Albert Schalm, who was the mayor of Mayerthorpe in March 2005. Postmedia News (Montreal Gazette, StarPhoenix, Leader-Post, Calgary Herald, Edmonton Journal)

Buchanan urges city council to revisit crime map debate

Red Deer city Coun. Buck Buchanan is not giving up the fight to have the city's crimes plotted on a map. Buchanan filed a second notice of motion asking for the city to collaborate with the RCMP to explore the concept of crime mapping as a tool in the overall safety strategy on Monday. His initial motion died on the floor on Jan. 19 because there was no seconder. Buchanan initially proposed working with the Central Alberta Crime Prevention Centre but city administration recommended changing the motion to working with the RCMP. "It's about awareness," said Buchanan. "It's not like it isn't being done in other places or other jurisdictions with the RCMP (such as Kelowna and St. Albert)." He said it is just a matter of releasing the information and the RCMP are not going to release the information unless they are advised by the city. "The Crime Prevention Centre is going out in the communities and the things that are constantly coming up is 'Can you tell us what is happening in our neighbourhood?'" he said. "And unfortunately we can't." Buchanan was not part of the Jan. 19 discussion because there was a perceived conflict of interest. Buchanan said, in fact, some paperwork was mistakenly filed that put him on the Central Alberta Crime Prevention Centre board. Red Deer Advocate, A1

Doctor's findings not vital to case: RCMP

When The Telegram published a set of articles on the Dana Bradley murder investigation in March 2014, much of the information centred around the recovered memories of a man The Telegram referred to as "Robert" - a pseudonym used to protect his identity. Was the incredible story he told of witnessing the December 1981 murder based on real memories or false memories? If real, how can they be corroborated? If false, how did they develop? Robert claims he was in the back seat of the car when 14-year-old Dana was picked up hitchhiking in the west end of St. John's. He describes the murder in graphic detail. The man who committed the murder, Robert alleged, had also sexually abused him as a young boy. The RCMP investigated his claims and say things did not match up. In fact, as reported in Part 1 on Saturday, the RCMP says there are vast differences between the known, hard facts of the case and Robert's account, and Robert's story changed over time. After the RCMP made its determination on Robert's account of the murder, they asked Robert if he would like to meet with Dr. Peter Collins, an expert in forensic psychiatry. Collins believed Robert was suffering from false memories, and the term "false memory syndrome" was noted. According to a police document, Collins advised Robert he was not suffering from post-traumatic stress disorder (PTSD), but was experiencing false memory syndrome. The Telegram, A3 Front

Destruction et poursuite policière à Moncton

Un individu est accusé d'avoir causé plus de 60 000 $ de dégât chez un concessionnaire de voitures Mitsubishi dans la nuit de dimanche à Moncton. Après avoir foncé à vive allure avec un camion dans des véhicules stationnés sur la rue Main, l'homme de 33 ans a poursuivi sa course folle jusqu'à la route Salisbury, où il a finalement été intercepté par les policiers. Pare-chocs arrachés, débris de verre et de métal parsemés sur le trottoir enneigé, Mike Raby a eu une bien mauvaise surprise en rentrant au travail lundi matin. Cinq véhicules neufs du concessionnaire, tous des années 2014 et 2015, ont été fortement endommagés par un chauffard dimanche soir. Selon des informations de la GRC, Christopher Lambke circulait à bord de son camion en direction ouest sur la rue Main quand il aurait mal négocié un virage peu après 20 h. Il aurait ensuite violemment percuté cinq véhicules détruisant les pare-chocs des deux premiers et entassant les trois autres. L'homme fait maintenant face à quatre accusations, dont conduite avec facultés affaiblies. «A regarder les traces dans la neige et l'étendue des dégâts, il devait rouler assez vite, merci. Il a tout fait ça sans même s'arrêter», explique M. Raby, directeur des ventes au concessionnaire. L'Acadie Nouvelle, 4 Front

RCMP respond to another toy gun false alarm

As they battle what seems to be a local trend of terrible judgment, the Codiac Regional RCMP is urging the public to take proper precautions when carrying replica guns or toy guns that may be mistaken for real weapons. Codiac is speaking out after yet another in what has been a long string of frightening incidents in the city since a real gunman rampaged through northwest Moncton last June 4. And most disturbing of all, the incident police responded to on Sunday night involved a young man carrying a replica weapon on Mailhot Avenue, where three local RCMP constables were murdered and two were wounded last June. Just before 11 p.m. on Sunday, police officers were dispatched to Mailhot Avenue. A man with his face covered had been seen waving what appeared to be a toy gun at vehicles passing by and at residences. The street was closed off while police searched the area. The suspect, a 19-year-old man from Moncton, was located at around 11:30 p.m. at a residence on McCoy Street, just metres from where two police officers died last summer. The gun was determined to be a toy. "We take these calls very seriously," said Staff-Sgt. Maurice Comeau in a statement issued Monday afternoon. "All types of firearm calls are treated as if it is a real firearm. Anyone with these types of guns need to understand how important it is to take proper precaution and carry these types of weapons in a case and not to display or use them in public places. We don't want to see anyone hurt, including the public, police officers or the person carrying the gun." Comeau said police officers have only seconds to determine whether or not a weapon is real. He also said the RCMP also urges the public to always follow the commands of police should they be approached by an officer. Times & Transcript, A1

RCMP investigate fatal house fire near Hartland

A fatal structure fire between Hartland and Florenceville-Bristol on Monday is being treated as a crime scene by police. Const. Derek Black, a spokesman for the RCMP, confirmed members of the Woodstock detachment are investigating after the body of a person was found inside a residence in Peel, north of Hartland. He said emergency crews were called to the scene at approximately 4:45 a.m. Monday. He said the house was completely engulfed in flames when crews arrived. "Police are currently working at trying to identify the victim, and the investigation is continuing," Black said. Hartland fire Chief Mike Walton told the Bugle-Observer on Monday morning that the department had been at the scene since shortly after 4 a.m. He said the homeowners are Joseph and Phyllis Roy. Daily Gleaner, A1

Mountie cleared in case involving tot

An unidentified Mountie has been cleared after an investigation of alleged sexual touching involving a three-year-old girl. Nova Scotia's Serious Incident Response Team handled the file from October and released its findings in a written decision Monday. In July, the girl was said to have made two comments to her parents that suggested an officer allowed her to touch his genitals. The officer's wife worked as a caretaker inside their home and watched the girl for a few days a week between September 2013 and July 2014. The mother watched additional children at times. According to the decision, the girl was playing with her father at home when she touched him in the genital area. He told her not to do so, but she said the officer had let her do that. She repeated the statement when her mother entered the room. The girls' parents asked her for more information but did not get any more details. As well, the release said her comments could have had another interpretation. The RCMP contacted the team about the matter in October, when it began the investigation. Chronicle Herald, A5

Police arrest eight in dial-a-dope bust

Eight men face 30 drug charges after police dismantled a Saskatoon dial-adope operation. Officers seized 208.5 grams of hard cocaine, 5.6 grams of soft cocaine, and $70,000 in cash after searching four Saskatoon homes on the weekend, police stated in a news release. The men, who range in age from 20 to 36, are charged with possession for the purposes of trafficking and possession of the proceeds of crime. Two are also charged with breaching court-ordered conditions from Alberta. Police described the Saskatoon Integrated Drug Enforcement Street Team's investigation as "lengthy." Integrated Organized Crime North, which includes city police and RCMP, along with several other city police units, helped with the investigation. The raided houses were in the 900 block of 15th Street East, the 100 block of St. Lawrence Court, the 700 block of Hart Road, and the 300 block of Pendygrasse Road. All eight men were scheduled to appear in court Monday. Postmedia News (StarPhoenix, A7)

RCMP financial crime unit moving in with Ontario Securities Commission
A Toronto-based RCMP contingent of white collar crime investigators is moving in to the offices of the Ontario Securities Commission, a move intended to help the two agencies to work together more closely. The Integrated Market Enforcement Team was launched by the RCMP in 2003 to investigate major fraud cases and protect the integrity of the country's stock markets. The unit consists of teams in Toronto, Montreal, Vancouver and Calgary. The Toronto branch of the Integrated Market Enforcement Team already works with the OSC, but moving the two agencies under one roof is expected to strengthen that partnership. "The goal is to bring all of our collective resources, skills and expertise together in one location," RCMP assistant commissioner Stephen White told reporters Monday. All 28 of the Toronto unit's fulltime staff are expected to be moved in to the OSC's headquarters by April 1. Having both organizations working in the same building will make it easier for them to review cases together to determine whether they fall within the RCMP's mandate, the OSC's mandate or require a joint investigation, said White. In Quebec, the RCMP's team of financial crime investigators already shares an office with the province's securities regulator. White said he is unsure whether IMET's teams in Alberta and British Columbia have plans to move in to their provincial regulators' offices. Canadian Press (The Guardian, B14) ; Toronto Star

Senators call for unedited terror vids
Two influential senators have joined the growing chorus of federal politicians calling on the RCMP to release the unedited video recorded by gunman Michael Zehaf- Bibeau before he killed a soldier at the National War Memorial then stormed Parliament last October. Zehaf-Bibeau, 32, made the video to explain his motives for his Oct. 22 rampage. The RCMP seized the shooter's video as part of its criminal investigation but have kept the recording under wraps, saying its release would interfere with their ongoing criminal probe. During a closed session last month, the Commons public safety and national security committee voted to invite RCMP Commissioner Bob Paulson to screen the video publicly "at his convenience and as soon as possible." The motion emphasized the independence of the commissioner, who will decide whether to accept the invitation. QMI Agency (Winnipeg Sun, 6, Edmonton Sun, Calgary Sun)

Accused killer re-arrested
Travis Vader -- accused of killing two St. Albert seniors who vanished nearly five years ago -- is back in custody after breaching conditions for the second time in less than a month. Vader, 42, was arrested after a call to a rural Edson home around 10:30 p.m. on Feb. 28. RCMP Cpl. Sharon Franks, spokeswoman for K-Division in Edmonton, says a resident of Carrot Creek was at home when a truck pulled into his driveway and stayed in the yard for an extended period of time. "He didn't know who it was; he didn't recognize the vehicle," Franks said. Vader is now charged with six counts of breach of recognizance and one count of dangerous operation of a motor vehicle in that case. After a bail hearing he was remanded into custody. The Edson arrest comes not even a month after St. Albert RCMP arrested Vader Feb. 12 at his residence in the community. He was charged in that case with assault and failing to comply with a condition on his recognizance to keep to peace and be of good behaviour. QMI Agency (Calgary Sun, Kingston Whig Standard, Edmonton Sun, Ottawa Sun, Winnipeg Sun, Toronto Sun, London Free Press); * Postmedia News (Edmonton Journal, A3)

* **Drugs, cash seized by Grande Prairie RCMP**
Grande Prairie RCMP charged two men with a variety of drug offences following a nine-month investigation. Police said search warrants were executed at two apartments. In addition, police searched two motor vehicles. RCMP seized more than $412,000 in Canadian currency, 915 grams of cocaine, 507 fentanyl pills, 10 ounces of crystal methamphetamine and two ounces of heroin. Police have arrested and charged 36-year-old Abdikarim Farha of Grande Prairie with possession of proceeds of crime over $5,000 and breach of a recognizance. An arrest warrant has been issued for 35-year-old Arte Abdillie Jama of Grande Prairie. Jama, who goes by the street name Fresh, has been charged with possession of a controlled substance for the purpose of trafficking and possession of proceeds of crime over $5,000. Edmonton Journal; Edmonton Sun

* **Man in stolen pickup faces 36 charges**
An Alberta man who rammed three unoccupied police vehicles with a stolen pickup truck while trying to

escape Whitecourt RCMP last week faces 36 charges. No one was injured in the incident. "Our officers' assessment of the situation, coupled with a swift and measured response, protected them from a potentially fatal situation," Chief Superintendent Brenda Lucki, district commander for the western Alberta district, said in a news release Monday. The incident began about 6:20 a.m. Feb. 26, when RCMP were dispatched to a call about a possible impaired driver. Officers located the vehicle, a pickup truck later determined to be stolen, with a snowmobile in the back, also stolen, and the truck's lone occupant, a 29-year-old wanted man from the Grande Prairie area. An altercation ensued and the man sped away, RCMP said. The truck and driver were later located in a remote area. Whitecourt RCMP officers set up a perimeter, with help from the police helicopter and canine unit. Postmedia News (Edmonton Journal, A8); QMI Agency (Edmonton Sun, Ottawa Sun, Toronto Sun, Kingston Whig Standard, Calgary Sun, London Free Press)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Accused CSC employees married

The two Correctional Service Canada employees from Kingston charged with offences related to Project Batlow are married to each other, the Whig-Standard has learned. Andrea De Laat, 33, was charged by the Ontario Provincial Police with conspiracy to traffic marijuana and conspiracy to traffic hashish, while Christopher D'Cunha, 44, was charged with possession of marijuana for the purpose of trafficking. The couple, who have two children, live on a quiet residential street in Kingston's west end. Sources have told the Whig-Standard that De Laat is a clerk at the Regional Treatment Centre at Millhaven Institution. De Laat's mother, Janet De Laat, now retired, is the former deputy warden at the Prison for Women, Pittsburgh and Frontenac Institutions. D'Cunha is currently an acting staff training officer at the regional staff college in Kingston. In his current role, D'Cunha trains officers in firearms, self-defence, how to use breathing apparatus and how to deal with chemical agents. (...) Kyle Lawlor, media relations and outreach officer for the CSC, couldn't confirm if the couple have been suspended due to its own internal investigation, which is underway. "It would be inappropriate for the Correctional Service of Canada to comment on matters under investigation," he said. "Due to the Privacy Act, the Correctional Service of Canada cannot comment on specific cases of staff misconduct." According to CSC's code of discipline, If the couple are convicted criminally, it appears there are grounds for disciplinary sanctions against De Laat and D'Cunha. Under conduct and appear-a nce, the code states: "An employee has committed an infraction, if he/she commits an indictable offence or an offence punishable on summary conviction under any statute of Canada or of any province or territory, which may bring discredit to the service or affect his/her continued performance with the service." Lawlor said the employment status of De Laat and D'Cunha may be released once the internal investigation is complete. "CSC does not tolerate any breach of its policies, and all allegations, regardless of the source, are thoroughly investigated by CSC," Lawlor added. Kingston Whig-Standard, A1

Queen of the North navigator seeks review of criminal conviction

A former ferry navigator who was convicted of criminal negligence in a fatal sinking off the B.C. coast is asking the Supreme Court of Canada to review his case. Karl Lilgert was convicted of two counts of criminal negligence causing death and sentenced to four years for his role in the 2006 sinking of the Queen of the North. He is currently in prison, serving his sentence. The ferry struck Gil Island in Wright Sound and sank during an overnight voyage from northern B.C. to Vancouver Island, killing passengers Gerald Foisy and Shirley Rosette. Lilgert asked the B.C. Court of Appeal to overturn his conviction because of alleged errors in the judge's instructions to the jury, but the province's highest court rejected his appeal. Canadian Press (Times Colonist, A5, The Guardian)

*** Killer who sparked faint-hope debate denied full parole**

The man who touched offnational debate on Canada's faint-hope clause - when he reoffended more than a decade ago while out on early parole despite having killed a police officer - recently saw his day parole extended as he again struggles with life on the outside. The Parole Board of Canada recently decided that Randall Tabah, 67, a man who killed a Longueuil police officer during a bank robbery in 1981, is still not ready for full parole as he continues to serve the life sentence he received in 1983. The board decided Tabah should instead continue residing at a halfway house as he has for most of the past five

years. In 2002, Tabah generated headlines across Canada when he was arrested for a break-in in an apartment in Victoria, B.C., and police there learned he was out on full parole despite having been convicted of killing Constable Michel Vincent during the bank robbery in Longueuil. The conviction came with an automatic life sentence and, initially, Tabah was not supposed to be eligible for full parole until 2006. But Tabah's parole eligibility date was reduced to 17 years through the so-called fainthope clause, a part of Canada's Criminal Code from 1976 until the Conservative government had it repealed in 2011. Through it, offenders who had served 15 years of a life sentence could apply to have a jury hear arguments that they were rehabilitated enough to merit an earlier release. Less than a week after news of Tabah's arrest in 2002 spread, the Canadian Police Association began a petition calling for the faint-hope clause to be repealed. The federal Conservatives, who were in opposition at the time, made it part of their election platform while promising tough-on-crime legislation before winning the 2006 election and forming a minority government. Following his arrest, Tabah spent seven more years behind bars before the Parole Board of Canada granted him day parole in 2009. An addiction to gambling and a lack of transparency has prevented the board from granting Tabah a full release since then. His day parole has been suspended three times and was even revoked once, prompting a brief return to a penitentiary in 2013. Montreal Gazette, A6

*** Wiretaps reveal banality of life**

The wiretaps thus far played for the jury in the Mark Moore multiple homicide trial may shed some light on Mr. Moore's reaction to a Toronto Police "stimulation" plan to flush him out of the weeds, and even more on how the prison system runs, but what they really speak to is human nature. Mr. Moore is pleading not guilty to four counts of firstdegree murder in the 2010 slayings of Jahmeel Spence, Courthney Facey, Mike James and Carl Cole. All were gunned down in different parts of Toronto within a 75-day period that fall. Police didn't link the four killings until early 2011, Detective Sergeant Hank Idsinga, the officer in charge of what became one large investigation, told Ontario Superior Court Justice Michael Dambrot and the jurors Monday. Mr. Moore was identified as a "prime suspect" in all the slayings, and by August that year, when police got judicial authorization to tap his phone, he was in custody at the Toronto (Don) Jail on an unidentified matter. (The jurors haven't been told why he was in jail, but on one of the wires, Mr. Moore himself suggested it was a drug charge.) The range in the jail where he was being held had only four phones, so police tapped those and the visitor phones. By Sept. 30, or just 56 days later, Mr. Moore had made 7,500 calls on just two of the prison phones. Postmedia News (National Post, A2, Ottawa Citizen, Montreal Gazette, Vancouver Sun, Leader-Post, StarPhoenix, Calgary Herald, Edmonton Journal, Windsor Star)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Crime of passion**

It's a scam that invokes intense emotional pain in addition to a heavy financial loss. A heartless criminal posts a photo of an attractive person on an online dating site and pretends to be that person. Once they have a target, they'll say and become whatever it takes to draw their victim in, building a relationship or eventually professing love. The next step is to ask for money -- a plane ticket for a visit, help a struggling loved one, or a loan to help resolve some financial problems. The trap's been set and the unsuspecting victim is now ensnared. "These perpetrators are criminals," said Edmonton city police Insp. Mark Neufeld. "Edmontonians have lost hundreds of thousands of dollars to such criminals. Entire life savings have been wiped out and lives have been ruined." Edmonton police and partners in government, law enforcement and business kicked off Fraud Prevention Month on Monday with advice to help citizens avoid becoming victims of eco-nomic crimes, Throughout the month, police will highlight common frauds such as romance and grandparent scams, homeowner, renovation and mortgage swindles, identity and payment card thefts, business and charity deceits, as well as email and online schemes. And Neufeld says that overall fraud is on the rise in Edmonton. Last year, the economic crimes section reviewed more than 3,000 frauds compared to 2,600 the previous year, for an increase of 16%. General frauds are on the rise by about 9%, and cheque frauds are up 20%. Identity theft had the biggest increase at 86% and identity fraud was up 26%. Edmonton Sun, 2, Calgary Herald

*** Roundtable included many emotional moments**

Kwanlin Dun Chief Doris Bill said she was "disappointed" with the federal response to Friday's first-ever roundtable on missing and murdered indigenous women, and called for more leadership and financial commitment from Ottawa. The meeting, which saw premiers, aboriginal leaders and two federal cabinet ministers convene in the nation's capital, aimed to find solutions to grossly disproportionate levels of violence against First Nations women and girls. "Overall, I think the federal government should be right in the lead on this," Bill told the Star this morning. "I think they should be right up there with the Assembly of First Nations and the Native Women's Association and the Sisters in Spirit. They should be helping the families of the missing and murdered women and girls." Bill highlighted the government's longstanding resistance to a national inquiry into the issue, returned to the fore with Prime Minister Stephen Harper's denial of the problem as a "sociological phenomenon" in Whitehorse last August. "The fact that it took the provinces to take the lead on this says volumes about the federal government," Bill said. The government has pledged $25 million over five years as part of a federal action plan. Whitehorse Daily Star, 3

*** The solutions at hand for aboriginal women**

An editorial states, "The common knock against the Conservatives' position on missing and murdered aboriginal women is that they don't see the problem as "a sociological phenomenon" - as Stephen Harper put it in August - but as "crime." Conservative ministers' engagement with the issue does not reflect this simplistic approach, however. Last week, in advance of Friday's National Roundtable on Missing and Murdered Indigenous Women and Girls in Ottawa, Status of Women Minister Kellie Leitch highlighted several measures her government had taken or proposed: Money for shelters, "preventative actions, particularly focused on men and boys," and "empowering" aboriginal women by making them "economically independent," including through matrimonial property rights. At the roundtable itself, Aboriginal Affairs Minister Bernard Valcourt mentioned "community-driven projects to engage men and boys" in an "effort to denounce and prevent violence." Few reasonable people would find fault with these ideas with respect to any non-aboriginal community. Yet the ministers took heavy fire for them last week. Linking violence against women to male attitudes is 110% politically correct. But here it is verboten because it reflects a "racist" assumption that perpetrators of domestic violence against aboriginal women must be aboriginal men, according to Dawn Harvard, interim president of the Native Women's Association of Canada. The government was accused of "victim-blaming." It's proof of how unhelpfully muddled the thinking at work here is that women's rights activists actually seem willing to view the perpetrators of violence as victims. They might well be: Violent childhoods often beget violent adulthoods. But generally speaking, men are not afforded such sympathy." National Post, A8

*** Premiers, PM missing in action**

An editorial states, "What is to be said of premiers who demand a national inquiry into the abhorrent levels of violence suffered by aboriginal women in Canada, but then do not show up at a one-day meeting to talk about solutions? Dereliction of duty tops the list. With Prime Minister Stephen Harper also absent, it's not surprising that Friday's roundtable on missing and murdered indigenous women and girls produced little. Cabinet ministers and bureaucrats do not have the political clout to sign up for projects that cost money. So what did we get? Premier Greg Selinger promised to bring the families of Manitoba victims together with police and justice officials. Not a bad idea, given this is one of the top complaints from relatives. Many have stated police leave them out of the loop, investigations move too slowly and police don't seem committed to their cases. Ontario Premier Kathleen Wynne called for an ambitious to-do list, a national effort that, conveniently, would fall primarily on the federal government's tab. Her "socio-economic action plan" to improve housing, child care and education for aboriginal women, would be a multi-billion dollar (federal) effort. No wonder the two ministers Mr. Harper sent to the roundtable refused to join in the premiers at a press conference Friday. The roundtable was not entirely useless. It was a small step forward in the work that must be done in this country to cut the rate at which aboriginal women are victims of violence. And Perry Bellegarde, national chief of the Assembly of First Nations, took some hope in the fact pledges were made to focus on prevention, and improving the response of police and justice officials to crimes against aboriginal women and girls." Winnipeg Free Press, A6

*** Undelivered justice**

A letter to the editor states, "Re Missing And Murdered (March 2): Stephen Harper boasts that "Our government has made standing up for victims of crime a priority." But based on his government's refusal

to cover the costs associated with DNA testing of missing persons and unidentified remains, we can only conclude that the pledge comes with a qualification. If you're a living victim of crime, you're a priority. If you're a missing or dead victim of crime, your family must lower its expectations of the government and its near-endless promises of justice for the innocent." Globe and Mail, A10

*** Making women's equality a reality**
An opinion piece states, "International Women's Day is a time for celebration, reflection, and action. Since the day was first observed on March 8, 1909, progress and achievements toward women's economic, political, and social equality have undoubtedly been made - this we must celebrate. However, significant barriers still remain in almost every country, and for that we must continue to reflect and urge our governments and communities to act. Even in wealthy countries like Canada, violence against women continues, equal pay is elusive, and women are significantly under-represented in positions of decision making and leadership. When you look closer at the progress of aboriginal women, women with disabilities and racialized women the picture becomes even less rosy. So when will this change? Apparently by 2030." The Guardian, A7

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Parliament lost in a fog of spending**
The Magna Carta will visit Canada this year as part of the 800th anniversary celebrations of the charter that provided the foundation for individual freedom against arbitrary despotism. Parliaments have used the Great Charter as a guide for their role, chief among which has been the task of reviewing and authorizing government expenditure of public funds. Yet scrutiny of public spending is slipping away from Canada's parliament. The average MP's ignorance of how governments spend taxpayers' money is encyclopedic. This is not surprising. The system is stacked against any meaningful review of spending, at least until the Public Accounts of Canada are tabled, 200 days after the fiscal year they cover. MPs are left like the proverbial bald men fighting over a comb - inconsequential jousts over trivia in the House of Commons - while the real business of government is carried out elsewhere. One recent case reveals how Parliament is little more than a ceremonial rubber-stamp. The recent supplementary spending estimates for 2014-15 revealed the federal government is writing off $295 million in uncollected Canada Student Loans. This was no doubt news to MPs who, in all likelihood, were never asked to authorize the loans in the first place. National Post, A4

*** Shared Services to refurbish data centre**
The federal government is moving ahead with plans to refurbish a data centre in Ottawa - a project that could take years to complete, and possibly cost more than $100 million. The plan is to refurbish an existing data centre by the airport to be a second "development" data centre, which is essentially a space to test programs before they go live, making it one of the seven data centres the government wanted to keep open as part of a massive IT overhaul that the government is undertaking to reduce costs, tighten cybersecurity, and help make the public service more nimble. When work to consolidate 485 data centres into seven is complete - sometime around 2020 - the government expects to save about $100 million a year in operating costs. Ottawa Citizen, A6

OTHER

*** Canada hints at Iraq mission extension**
Foreign Affairs Minister Rob Nicholson has given France every indication the Conservative government will move to extend the current Canadian military mission against Islamic State, also known as ISIL, in Iraq. Nicholson, on his first trip abroad since taking over his new portfolio, discussed the fighting in Iraq against ISIL extremists with his French counterpart, Laurent Fabius, in Paris on Monday. "I indicated that we are examining all our options but that we are committed to degrading ISIL, and I made that very clear to my French counterpart and indicated to him that the government would be making a decision on this in the next few weeks," Nicholson told the Star in an interview from France, which is among the allies

fighting ISIL. "We recognize that ISIL is a threat in this part of the world," Nicholson said. "But we believe it is a direct threat to Canada." Toronto Star, A6

*** Lack of diplomatic ties snarls search for Toronto pastor missing in North Korea**
Some time in the last two days of January, Hyeon-soo Lim crossed the land border from China into the north-eastern corner of North Korea. This was nothing particularly special for Mr. Lim, the senior pastor of one of Canada's largest Korean churches. He had been to the Hermit Kingdom more than 100 times before. He was expected to call home on Feb. 4. When he did not, the church initially did not panic: North Korea has in recent months quarantined visitors for up to 21 days to ensure they do not have the Ebola virus. But more than a month has passed with no word, and his church is worried Mr. Lim has been detained in a country that has jailed several foreign Christians in recent years. "There has never been this length of delay before," said Lisa Pak, a pastor at Toronto's Light Presbyterian Church, where Mr. Lim is a senior pastor. From the perspective of the church, he has vanished, and has been reported missing to Canadian Foreign Affairs officials. "We have no information," she said. "He's not a tourist that wandered off. He knows the language, he knows how to behave in a way that's not offensive to the government." Canada and North Korea have no obvious current tiffs, meaning Pyongyang would have little to gain diplomatically by taking a Canadian. It is possible the bureaucracy of a secretive state has magnified something trivial. Globe and Mail, A9

*** Family says Badawi may face death penalty**
The family of imprisoned blogger Raif Badawi says the 31-year-old is facing a major setback in his legal fight - one that could eventually lead to the death penalty. Badawi's wife, who was granted political asylum and has been living in Sherbrooke with the couple's three children since 2013, sent out a desperate plea over the weekend after she was informed by "reliable sources that there are attempts within the Penal Court to retry (Badawi) on apostasy charges again." Charges of apostasy - or renouncing Islam - carry the death penalty in Saudi Arabia, where Badawi is being held. The execution is usually carried out by beheading. Ensaf Haidar has been fighting for her husband's release for months. In her statement, she called on the public and government officials to step in, saying that she fears Badawi will be "dragged" to his death by "bigots." Badawi's situation has received international attention, with hundreds of thousands of people signing various online petitions demanding his release. Montreal Mayor Denis Coderre recently called on Prime Minister Stephen Harper to lobby Saudi officials to free the imprisoned blogger. Harper has said there is little that can done beyond applying diplomatic pressure, as Badawi is not a Canadian citizen. Montreal Gazette, A3

*** Raif Badawi: l'ambassadeur du Canada est intervenu**
L'ambassadeur du Canada à Riyad a récemment discuté du cas de Raif Badawi avec le ministre saoudien des Affaires étrangères, a appris La Presse, alors que les proches du blogueur condamné à 1000 coups de fouet s'inquiètent de la possibilité qu'il soit à nouveau accusé d'apostasie, un crime passible de la peine de mort par décapitation en Arabie saoudite. La rencontre entre l'ambassadeur Tom McDonald et le prince Saoud al-Fayçal, ministre des Affaires étrangères de l'Arabie saoudite, a eu lieu «à la fin du mois de février», a indiqué sans plus de précision une porte-parole du ministère canadien des Affaires étrangères, Amy Mills. La porte-parole n'a pas précisé combien de temps la rencontre a duré ni quel accueil a reçu l'ambassadeur McDonald, venu «réitérer encore une fois [les] préoccupations [du Canada]» à l'égard de Raif Badawi. C'est la première fois qu'un représentant canadien s'entretient avec un membre du gouvernement saoudien au sujet de Raif Badawi, condamné à 1000 coups de fouet, 10 ans de prison et plus de 300 000 $ d'amende pour insulte à l'islam et violation de la loi sur la cybercriminalité. La Presse (Le Nouvelliste, 24, Le Soleil, La Tribune)

INTERNATIONAL

Obama, Netanyahu clash on Iran
A mid rising U.S.-Israeli tensions, a defiant Prime Minister Benjamin Netanyahu said Monday he will not back down from a planned speech to the U.S. Congress the White House says is a deliberate attempt to scuttle a nuclear deal with Iran. Addressing members of the American Israel Public Affairs Committee, the most powerful Israeli lobby group in the U.S., Netanyahu said he intends to deploy technical arguments

Tuesday to persuade U.S. lawmakers negotiations are fruitless because Iran cannot be trusted. Iran is "threatening to destroy Israel, devouring country after country in the Middle East, exporting terrorism and developing capacity to make nuclear weapons - lots of them," he said. As the "prime minister of the one and only Jewish state, I plan to use that voice," he continued to substantial applause. In a sort of pre-emptive strike, U.S. President Barack Obama chastised Netanyahu and Israel in an interview with Reuters Monday, saying they were detouring around accepted protocol in an attempt to reshape U.S. foreign policy. "Ultimately the interaction with foreign governments runs through the executive branch," he said. "That's true whether it's a Democratic president or a Republican president, and that's true regardless of how close the ally is." The White House was furious Republican House Speaker John Boehner did not consult the president before inviting Netanyahu, thereby breaking protocol. Canadian Press (Vancouver Sun B1/ Front, Montreal Gazette A1/ Front, Ottawa Citizen, C1/ Front, Calgary Herald B1/ Front, Edmonton Journal, Montreal Gazette A1/ Front, Windsor Star) Postmedia (National Post A1/ Front), Globe and Mail A1; * Canadian Press (Red Deer Advocate, Ottawa Citizen, Times & Transcript, Cape Breton Post)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
March 5, 2015 / le 5 mars 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Right-wing groups take root
An ugly confrontation unfolded on the streets of Newcastle, England, last weekend. On one side were approximately 2,000 people of all colours and creeds who had assembled under the banner of Newcastle Unites. On the other, a group of just under 400 people who came together to protest what they perceive as the Islamization of the western world; a "Muslim tide" they claim threatens the fabric of British society and its traditional values. The latter group was an apparent offshoot of the far-right organization Pegida - or Patriotic Europeans Against the Islamization of the West. Since its formation in Germany last year, the group has managed to draw thousands into the streets in various European cities with what many perceive as a divisive and racist message. In January, with little fanfare and even less media coverage, Pegida landed in Quebec. A Facebook page set up by the group, featuring photos from Pegida demonstrations around the world, had attracted just under 600 "likes" as of Wednesday, and their first official rally is set to take place on March 28 in St-Leonard. The Montreal Gazette reached out to the organizers behind the page on Wednesday, but they did not respond to a request for comment. (…) The Canadian Press reported on Tuesday that Canada's spy agency (CSIS) recently advised the office of **Public Safety Minister Steven Blaney** of its concerns during a secret September briefing, noting that Canada's burgeoning anti-Islam movement poses an "ongoing risk, particularly as its proponents advocate violence." Postmedia (Montreal Gazette, A1/ Front, Ottawa Citizen C1/ Front, Star Phoenix, Vancouver Sun, Edmonton Journal, Calgary Herald)

Tories to table life-without-parole bill

The Conservative government will introduce life without parole for some killers, in what would be the biggest change to the Criminal Code since the abolition of capital punishment in 1976. Prime Minister Stephen Harper said that, because of constitutional concerns, those sentenced to life without parole would have the right to petition the **public safety minister**, but not before 35 years have elapsed. The policy would revive a routine role for cabinet in release decisions that had ended in 1959 with the creation of the National Parole Board. (…) Rick Sauvé, a lifer in Ontario who has been on parole since 1995, and who works with other lifers for the St. Leonard's Society, said he doubts inmates will receive a fair shake when they petition the **public safety minister** for release. "They would just act on emotion," he said of the minister. And "if you take all sense of hope, people can become desperate. It could create more violence in the prisons." Legal observers called the 35year review by the **public safety minister** a new "faint-hope clause" - an ironic reference to the 1976 law that gave convicted killers a chance after 15 years to apply to a jury for a chance at early parole. The Conservative government killed the 15-year review in 2011. Several lawyers and academics interviewed said the 35-year review at the political level may not be enough to make life without parole pass muster with the courts. Globe and Mail, A1, Toronto Star, A1; Presse Canadienne (Le Quotidien 22, La Tribune, L'Acadie Nouvelle)

The problem with life sentences

An opinion piece states, "On past form, the Conservatives' latest piece of tough-oncrime legislation will come with some sort of folksy name attached, of a kind suitable for use in Tory ad campaigns. The Life Means Life Act, perhaps? The Throw Away the Key Act? The Hanging's Too Good For Them (And What If It Wasn't) Act? Under the legislation, to be introduced in Parliament next week - Wednesday's announcement, as usual, took place hundreds of miles away - would raise the maximum penalty in Canadian law from the current 25 years without eligibility for parole, to a sentence that is often referred to as "life" but is in fact rather closer to "death." Prisoners convicted of particularly "heinous" crimes - for example, murders involving sexual assault, or kidnapping, or the killing of police officers or prison guards, or terrorism (high treason is also on the list) - would be obliged to serve, as a government background document put it, "the rest of their natural lives" in prison, with no possibility of parole, ever. They would be kept locked up until their bodies were actually discovered in their cells. There would be one, grudging exception. After 35 years, prisoners could apply, not for parole, but for "exceptional release," and not to some dogooding parole board, but directly to the **Minister of Public Safety**. This is intended to allay, as the background paper puts it, "legitimate constitutional concerns," what might be called the Keeping The Supreme Court Off Our Backs provision. So life would not quite mean life. It would mean life or the readiness of an elected politician to personally authorize the release of one of Canada's "most heinous criminals." If there were any likelihood of that you may be sure the Conservatives would not have included it in the legislation." Postmedia News (National Post, A1, Ottawa Citizen, Leader-Post, StarPhoenix, Montreal Gazette, Calgary Herald, Edmonton Journal, Vancouver Sun, Windsor Star)

Public safety vs. the politics of payback

An opinion piece states, "These days, if Stephen Harper isn't warning people about the terrorists lurking around every street corner, he's stoking fears about violent crime and child sex predators. For the PM, fear is the object, not the effect; statistics show Canada is getting safer, so you know this isn't about keeping people safe. If it were, Harper wouldn't be allowing funding to lapse for one of the most successful community-based sex offender prevention programs in the world. Harper and **Public Safety Minister Steven Blaney** like to talk about keeping bad people locked up. Which works fine … as long as the bad people stay locked up. Once they're released - as the vast majority of them are, eventually - all bets are off. **Blaney** knows this. He knows that Circles of Support and Accountability (COSA) works, because his government's own research tells him so. He knows that COSA - which uses trained volunteers to re-integrate sex offenders back into the community - reduces their risk of re-offending. He knows that every dollar invested in COSA saves taxpayers more than $4 in policing and prison costs. Blaney knows COSA can and has prevented men from hurting children. But he's going to let its funding expire at the end of the month anyway." iPolitics; Edmonton Journal

Parliament shooter's video to be released

A video made by gunman Michael Zehaf-Bibeau that explains his motives for killing a soldier at the National War Memorial and storming Parliament in October will be released Friday, RCMP confirm.

Commissioner Bob Paulson will appear before the Commons public safety and national security committee (SECU) to show and discuss the video. "At that time, committee members will be provided an update on the investigation arising from the events of Oct 22, 2014, in Ottawa," RCMP spokesman Sgt. Greg Cox said via e-mail Wednesday. (…) **Public Safety Minister Steven Blaney** is "pleased" with the decision, according to ministry spokesman Jean-Christophe de Le Rue."This terror attack remains a significant example of why we need to pass our Anti-Terrorism Act -- to ensure police and our national security agencies have the tools they need to keep Canadians safe," said de Le Rue. QMI Agency (Toronto Sun 8, London Free Press, Kingston Whig-Standard, Edmonton Sun, Calgary Sun, Ottawa Sun), Presse Canadienne (Le Quotidien, Le Devoir, La Voix de l'Est, La Tribune, Acadie Nouvelle, Whitehorse Daily Star), Toronto Star, A3

Ottawa police won't get more than $10M
Ottawa's police force is likely to receive $10 million in federal funding to help cover the costs of policing the capital, but an additional request to pay the costs of policing downtown on Oct. 22, 2014, is likely to fall by the wayside. When the city sent its recent letter to **Public Safety Minister Steven Blaney** asking for the funding to be renewed, it cited the costs to police events such as Canada Day, demonstrations, protests, and visits from foreign leaders, as well as keeping an eye on 118 embassies. In all, there are about 700 events directly related to the federal government that Ottawa police must keep an eye on annually, with the costs borne by municipal taxpayers. "It should be a no-brainer," said local NDP MP Paul Dewar. **Blaney**'s office wouldn't put a timeline on when a decision will be made. Jordan Press (Ottawa Citizen, A7)

La loi C-51 n'enchante pas le PQ
(…) De passage en banlieue de Toronto, hier, le premier ministre Stephen Harper s'est montré peu ouvert à amender le projet de loi, dont l'étude en comité parlementaire débutera la semaine prochaine. «Évidemment, on va écouter, mais le gouvernement a fait beaucoup de délibérations sur le contenu de ce projet de loi et nous sommes tout à fait déterminés à l'adopter», a-t-il déclaré. Face aux craintes que suscite C-51, le **ministre fédéral de la Sécurité publique, Steven Blaney**, a pour sa part assuré que «les activités pacifiques de protestation ne sont pas incluses» dans le projet de loi. Le Journal de Quebec, 20

*** Popular security bill could put lid on voices of dissent**
An opinion piece states, "On Wednesday, I joined a small group of Canadians who have actually read Bill C-51, the Conservatives' bill designed to toughen up Canada's terrorism laws. The merits, or lack thereof, of Bill C-51 have consumed lots of attention in Ottawa, with **Public Safety Minister Steven Blaney** saying (over and over) that Canadians want more protection from terrorists, Opposition Leader Thomas Mulcair arguing the bill goes too far and has inadequate oversight of security agencies, and Liberal Leader Justin Trudeau saying he'll support the bill, but wants better oversight and a mandatory review of C-51 in future. The bill forbids "changing or unduly influencing a government in Canada by force or unlawful means" and prohibits "interference with critical infrastructure." Democratically elected governments shouldn't be changed or influenced "by force," but how can protests or civil disobedience campaigns change laws if they can't "influence" the government? That's the whole point. And who gets to decide when such influence is undue? That section is likely to raise flags among groups like First Nations, student and labour activists and environmentalists, who sometimes break the law (i.e., block roads, stage sit-ins, etc.) in order to try to change policy." The Chronicle-Herald, A13

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE
NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Canadian Pacific weighs shift away from crude by rail**
Canadian Pacific Railway Ltd. wants the power to refuse to haul dangerous goods, a signal it has grown weary of the risks and regulations that accompany the business of hauling oil. Globe and Mail, B1

*** Canada's railways are committed to safety**
Re: "Federal rail-safety measures remain inadequate" (Opinion, Feb. 25)

A letter to the editor states, “Mark Winfield's article suggests Canada's railways are "self-regulated." Railways have to comply with dozens of regulations and hundreds of rules, in addition to the Railway Safety Act - a modern piece of legislation that has been regularly reviewed and updated. By law, each federally regulated railway must also have a Safety Management System (SMS) in place that is approved by Transport Canada. SMS frameworks have not replaced regulation. These safety systems serve as an additional layer of oversight and best practices on top of Canada's robust regulatory regime for rail safety...” The Gazette, A14

* **Cumberland House to get flood protection**
Saskatchewan's government is spending close to $1 million to avoid the muchhigher costs connected to flooding in the northern village of Cumberland House and Cumberland House Cree Nation. StarPhoenix, A4

* **Toronto Hydro says 500 homes still without power after storm**
Toronto Hydro said around 500 homes were still cut off from power on Thursday, more than 24 hours after a weather system did serious damage to power infrastructure in the city. The power company’s online outage map shows several neighbourhoods are still in the dark, with Etobicoke and North York appearing to be hardest-hit. CBCNews.ca

* **Rogers expands wireless coverage across Sask**
Rogers has expanded its wireless coverage in Saskatchewan. Rogers said it is also rolling out LTE for faster speeds and giving more people in Saskatchewan access to 700 MHz spectrum for improved signal quality in basements, elevators and buildings with thick concrete walls. StarPhoenix, D1

NATIONAL SECURITY / SÉCURITÉ NATIONALE

RCMP to show Oct. 22 shooter's video Friday
After weeks of speculation, members of Parliament will get a chance Friday to see the video Michael Zehaf Bibeau made last October before he killed a Canadian soldier and stormed Parliament Hill. RCMP Commissioner Bob Paulson will use an open meeting of the House of Commons public safety committee to provide a 'detailed update' of the investigation into Zehaf Bibeau's deadly attack on Cpl. Nathan Cirillo, said a source familiar with the matter. The source, who wasn't authorized to discuss the issue publicly and therefore spoke on condition of anonymity, confirmed the video would be shown to the committee. Pressure has been mounting on the RCMP - and the Conservative government - to release the video to give people a first-hand glimpse into Zehaf Bibeau's state of mind on the eve of his assault. Last month, the public safety committee, while affirming the RCMP's operational independence, invited Paulson to appear at his earliest convenience to display and discuss the video. Asked about the matter on Wednesday, Prime Minister Stephen Harper said it's up to the RCMP whether to release the video, since it's part of an ongoing police investigation. "It's not my decision one way or the other," Harper told a news conference in Toronto. In the days following the attack, Paulson said he wanted people to see what he described as footage of Zehaf Bibeau explaining his actions in a deliberate and lucid manner, which were rooted in his religious beliefs and opinion of Canada's foreign policy. Canadian Press (Red Deer Advocate, Whitehorse Star, The Guardian, Times Transcript, Telegraph-Journal, Chronicle Herald ,Waterloo Record, Hamilton Spectator, iPolitics, Cape Breton Post); QMI Agency (Toronto Sun, London Free Press, Kingston Whig Standard, Edmonton Sun, Calgary Sun); Presse Canadienne (Le Quotidien, Le Droit, La Voix de L’Est, La Tribune, Le Soleil); * Le Devoir; * La Presse; * Globe and Mail; * Toronto Star; * Agence QMI (Journal de Montreal, Journal de Quebec)

Hill gunman's video invokes jihad, slams foreign policy
Michael Zehaf-Bibeau sat in the front seat of his car minutes before his shooting rampage on Oct. 22, 2014, and spoke to the camera. He spoke just long enough to talk about the actions he was soon to take, and put them into the context of "jihad," the Arabic word for struggle that is associated - moderate Muslims argue wrongly - with a struggle against non-believers. He took aim at Canada's foreign policy, threatened the Canadian military and invoked "Allah." Those words, captured on a cellphone video less than a minute long, have been in the hands of the RCMP since the day of the shooting, and every frame

of the short video has been examined as part of a criminal investigation... The details of how the video came to be, and how it fell into the hands of the RCMP, have been largely shrouded in mystery. The Citizen has pieced together the details from multiple sources with knowledge of the video that has yet to be shown publicly. On Friday, a more than fourmonth wait to see the video will come to an end when RCMP Commissioner Bob Paulson walks into a House of Commons committee room and briefs MPs and Canadians about Zehaf-Bibeau's final message, and the Mounties' criminal investigation into the Oct. 22 shootings in Ottawa. The video could answer lingering questions about Zehaf-Bibeau's actions that day - when he killed Cpl. Nathan Cirillo at the National War Memorial, then stormed Parliament Hill before dying in a shootout inside the Centre Block - including whether he acted alone, or had any help planning or carrying out the shootings... The RCMP declined Wednesday to say whether it has shown the video, or described it in any way, to Zehaf-Bibeau's mother, Susan Bibeau or other members of his family. However, the Citizen confirmed that Susan Bibeau had not seen the video or been contacted by the RCMP as of Wednesday morning. Postmedia News (Ottawa Citizen, A1)

RCMP briefing on Zehaf-Bibeau video raises questions, say opposition
RCMP Commissioner Bob Paulson's decision to comply with a government-worded committee motion to release a video recorded by the gunman who shot a Canadian reserve soldier and attacked Parliament last Oct. 22 has sparked speculation and questions about Conservative motives with a general election on the horizon. Mr. Paulson, in response to a motion passed unanimously on Feb. 17 at the Public Safety and National Security Committee, has agreed to air the video in a public meeting Conservative chair Daryl Kramp (Prince Edward-Hastings, Ont.) scheduled for Friday at 11 a.m.-the last day of a Commons March recess before Parliament resumes next Monday. The video could be crucial to longstanding opposition claims that Prime Minister Stephen Harper (Calgary Southwest, Alta.) branded the attack and shooting death of Cpl. Nathan Cirillo, as well as the murder of a Canadian soldier in Saint-Jean Sur Richelieu only a few days earlier, as an organized terrorist attack against Canada before he had the evidence. The long delay in releasing the cell phone video Mr. Zehaf-Bibeau recorded shortly before his attacks has puzzled MPs since Mr. Paulson first disclosed its existence shortly after the day of the attack. "The RCMP has identified persuasive evidence that Michael Zehaf-Bibeau's attack was driven by ideological and political motives," Mr. Paulson said in a statement, referring to terms in the Criminal Code that in part define terrorism, as distinct from other criminal offences. "Zehaf-Bibeau had prepared a video recording of himself just prior to conducting this attack," Mr. Paulson said. "The RCMP is conducting a detailed analysis of the video for evidence and intelligence. You must understand that we cannot release this video at this time and I would ask for your patience in this regard." Hill Times

* **Parliament Hill security incidents few and tame before Oct. 22 shooting**
A nonsense letter. A wayward cube van. A threatening voicemail. A tractor with the key left in the ignition. These were the infrequent and minor incidents recorded by the RCMP's parliamentary detachment as threats to the security of VIPs during the two years leading up to the tragic shooting on Oct. 22. Through the Access to Information Act, CBC News obtained a dozen "occurrence reports" documenting these relatively tame security challenges on Parliament Hill — tame, that is, until gunfire erupted inside the Centre Block last fall, putting the prime minister and many MPs in real and imminent danger. The mundane incidents in the months leading to the tragedy provide context to last fall's attack in which a lone gunman surprised RCMP officers as he ran, drove and darted up steps with a loaded rifle in hand. Since the traumatic episode, the Harper government has warned of future threats in the capital and across Canada, and introduced legislation to give security agencies more power. CBC News

* **Bill C-51 could violate rights, lawyers say**
The federal government's anti-terrorism bill gives government agencies too much unchecked power, say Saskatoon legal scholars who added their signatures to an open letter to parliamentarians, urging them to vote against the controversial law. "This new legislation will not make Canadians safer, but rather gives government agencies many new and unchecked powers to intrude on the rights of Canadians who are not at all involved in terrorist activities," said Sarah Buhler, an assistant professor at the University of Saskatchewan's college of law. Powers granted under the proposed legislation could be used by the Canadian Security Intelligence Service (CSIS) against groups such as environmental groups and First Nations, Buhler said. "The wording is so broad that it could potentially threaten to criminalize legitimate dissent," she said. Her colleague, assistant professor Clayton Bangsund, noted the Criminal Code

already contains terrorismrelated offences, which leads him to wonder what purpose the new law would serve. Bangsund said wording in the bill is "broad and ambiguous." The bill would authorize CSIS to "engage in intervention activities and disruptive measures," such as "wiping information from a target's computer or fabricating information to discredit a target," Bangsund said. It would also allow CSIS to ask a judge for a warrant to pre-authorize actions that contravene the charter, he said. Postmedia (Star Phoenix, A4)

* **Ex-Tory senator questions spy powers**
A former Tory senator says the new powers proposed for Canada's spies under the Conservatives' new terror law are "unprecedented" in peace time. But Hugh Segal wonders if what Canadians are living through can properly be called "peace time." "I think the question is what we now face with ISIS, and what we face with networked, digital recruitment ... whether this is a different threat than what we faced 10 or 15 years ago," Segal said in an interview earlier this week. "And I would argue that it is." Bill C-51 would give the Canadian Security Intelligence Service police-like powers to "disrupt" threats to Canada. CSIS would be able to use those powers to address terrorist threats, but also threats to Canada's infrastructure or economic stability. Both opposition parties and security experts have criticized the Conservatives for drastically expanding CSIS's powers, while declining to include more independent oversight over Canada's spies. Segal, who retired from the Senate last year and currently holds the post of master at Massey College, has long championed increased oversight for Canada's intelligence agencies. Unlike our closest security partners, Canada has no parliamentary oversight of the country's various spy agencies. The review bodies Canada does have are dwarfed by the agencies they're supposed to monitor. For instance, the Security Intelligence Review Committee - with 17 employees and a budget of under $3 million - is tasked with reviewing the operations of CSIS, with a projected budget of $537 million. The Communications Security Establishment - Canada's answer to the NSA, employing more than 2,000 - has a review body with an annual budget of around $2 million. Toronto Star, A8

* **Tories under fire for using terrorist propaganda to promote C-51**
An Edmonton MLA is blasting the federal Conservatives for an "irresponsible" social media post about terrorist threats to West Edmonton Mall. On Monday, the federal Conservative Party of Canada shared a screengrab on Facebook from a video by al-Shabaab, a Somalia-based terror group that attacked Kenya's Westgate Mall in September 2013, killing 67 people and wounding more than 175 others. A portion of the video encourages attacks on several other malls, including West Edmonton Mall. "Jihadi terrorists are threatening Canada -- we need to give our police and security forces the tools they need to protect us from the threat of terrorism. Add your name if you agree," read the post from the Conservatives, linking to a petition supporting the federal government's Anti-Terrorism Act (Bill C-51). The post didn't sit well with Edmonton-Castle Downs MLA Thomas Lukaszuk, who said the message runs contrary to police assertions that the threat isn't imminent and politicizes national security issues better handled by the federal government. "As an elected official, I don't want Edmontonians to live with some undue fear and avoid public venues like West Edmointon Mall," he said, adding the post suggests that Canada's law enforcement agencies are under-resourced. "Oddly enough, they're asking us to petition the very same government of that same party to give more money to police. I would ask them to petition themselves...It tells Edmontonians to 'nevermind what the police say, they're underfunded. There is a threat and they're not in a position to protect you' and that's just irresponsible." QMI Agency (Edmonton Sun, London Free Press B2, Edmonton Sun, Calgary Sun)

* **Muslim library in hot water over books**
Concordia's dean of students will meet with leaders of the university's Muslim Students Association regarding a television report that suggested the association's library contains books and videos by "extremist preachers." The library "is in a modest setting but nonetheless has cutting-edge software that allows users to consult online books, (among which) TVA news found dozens of works by radical imams," said the report which aired last Friday. In related news, Premier Philippe Couillard said Wednesday a Quebec Liberal member of the legislature should not have advertised on an Islamic community centre website that includes texts extolling violence against women. Postmedia (Leader-Post, C10, Edmonton Journal, Star Phoenix, Calgary Herald)

The spies next door

New figures show Canada has turfed out five spies in the past decade from a surprising source country - its best friend and ally, the United States. From 2004 to 2014 Ottawa sent back to the U.S. five of a total of 21 of those barred from Canada "on security grounds for engaging in an act of espionage that is against Canada or that is contrary to Canada's interests," according to a document produced by Canada Border Services Agency. It's not clear if the espionage was by foreign government agents or if it was industrial espionage - that is, spying to obtain state secrets, intellectual property or corporate secrets. A document released under access to information laws shows the suspected spies were permanent residents or foreign nationals deemed inadmissible on security grounds, but doesn't break down them down by citizenship. Rather, it indicates the country the spies were sent back to. Still, the fact that the U.S. is the origin of the most espionage cases is surprising, especially given the emphasis put by federal politicians - including two former CSIS directors, one of whom is now national security adviser to Prime Minister Stephen Harper - on China as a suspected source of espionage. The U.S. actually tops this list, followed by China, India and Sweden with two expulsions each in 10 years. The only two ousters of suspected spies to China are listed in 2014, with no earlier expulsion for the nine years prior. Russia accounts for just one expulsion - in 2004 - in the decade covered by the search. In a joint project, the Toronto Star and La Presse sought further information from CBSA, the U.S. embassy, former American ambassadors, former diplomats and Canadian officials, but none shed any light on the specifics of any case. Wendy Atkin, a media spokeswoman for Canada's border agency, declined to provide any details on specific cases but in a written statement clarified that Canada may not have been the sole target of the espionage. Toronto Star, A1; Le Journal de Quebec

*** Evidence is overwhelming' in terror plot to derail train**

A Crown lawyer is telling a jury "the evidence is overwhelming" in the case of two men accused of plotting to derail a passenger train between Canada and the U.S. Raed Jaser and Chiheb Esseghaier face multiple terror-related charges in connection with their alleged plot to target a Via Rail train travelling from New York to Toronto. Neither men called evidence or witnesses in their defence. Jaser pleaded not-guilty and Esseghaier, who is self-represented and does not want to participate in his trial, had a not-guilty plea entered for him by the judge presiding over the case. Canadian Press (Guardian, B5, Whitehorse Daily Star, Times & Transcript), Toronto Star, Presse Canadienne (Le Quotidien 16), QMI Agency (Edmonton Sun, Winnipeg Sun, Calgary Sun, Kingston Whig Standard, London Free Press, Toronto Sun, Ottawa Sun, Journal de Montreal, Journal de Quebec); Postmedia (Windsor Star A7, Leader-Post, Star Phoenix, Montreal Gazette, Ottawa Citizen, National Post, Edmonton Journal, Calgary Herald)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Human smuggling ship to be scrapped

Almost five years after a derelict cargo ship with 492 Sri Lankan migrants arrived off the B.C. coast, prompting a change in Canada's immigration laws, the government has failed to find a buyer for the vessel. Now, the MV Sun Sea, on which Ottawa has spent at least $600,000 to store and maintain, is headed for the scrap heap. "Because a buyer did not come forward, the CBSA will commence a judicial process to obtain the legal authority for its disposal," Stefanie Wudel, a spokeswoman for the Canada Border Services Agency, the ship's custodian, said Wednesday. Just two months ago, CBSA awarded a $157,697 contract to a Victoria company to carry out extensive work to remove potential environmental hazards and ensure the stability of the rusting ship, which is parked at a Fisheries and Oceans dock on the tip of Annacis Island, southeast of Vancouver. The work included: a "hot water wash" to remove oil and other pollutants from engine-room bilges; repairs to the hull; testing surface paint for lead; and removing from tanks all "deleterious material" or "fluids that could harm the environment." The agency said Wednesday the "necessity" of the repairs delayed the disposal process. There have been no reports of spillage of any pollutants, Wudel said, nor has any lead over the specified limit been detected. Representatives of Intercon Marine, which carried out the cleanup, declined to comment. After the Sun Sea's arrival in August 2010, the ship spent two years docked at a private shipyard in Nanaimo, before being towed to its current home in the lower arm of the Fraser River. A CBSA official previously told CTV News about $400,000 had been spent on moorage, security and towing during those first two years. Postmedia News (National Post, A1, Edmonton Journal, Calgary Herald, Leader-Post, Windsor Star, Vancouver Sun, The Province); National Post

Quebec man charged for not giving up phone password at border
A law professor in Halifax says the case of a Quebec man charged with obstructing border officials raises a new legal question in Canada. The accused, 38-year-old Alain Philippon of St. Anne-des-Plaines, Quebec, refused to divulge his smart phone password to Canada Border Services Agency during a customs search. Philippon arrived in Halifax Monday night on a flight from Puerto Plata in the Dominican Republic. Rob Currie is the director of the Law and Technology Institute at the Schulich School of Law. He says under the law, travellers crossing the Canadian border have a reduced expectation of privacy. He says border officials have wide-ranging powers to search travellers and their belongings. "Under the Customs Act, customs officers are allowed to inspect things that you have, that you're bringing into the country," he said. "The term used in the Act is 'goods', but that certainly extends to your cellphone, to your tablet, to your computer, pretty much anything you have." Currie says the issue of whether a traveller must reveal a password to an electronic device at the border hasn't been tested by a court. "This is a question that has not been litigated in Canada, whether they can actually demand you to hand over your password to allow them to unlock the device," he said. "One thing for them to inspect it, another thing for them to compel you to help them." Currie says the obstruction case hinges on that distinction. CBC.ca

Un médecin radié 18 mois
Le Dr Jean-François Coupal, qui exerçait la médecine familiale dans la région de Gatineau, voit son droit de pratique suspendu 18 mois pour avoir été reconnu coupable de possession de pornographie juvénile. Le médecin de 53 ans ne pourra également plus soigner de patients de moins de 18 ans, ne pourra plus utiliser l'internet pendant cinq ans et devra constamment se trouver en présence d'un autre membre du personnel sur son lieu de travail, a tranché le conseil de discipline du Collège des médecins, le 26 février. Le Dr Coupal avait été arrêté en 2011 alors qu'il revenait d'un voyage en Thaïlande. Les douaniers avaient trouvé sur une clé USB 200 photos et 195 vidéos de jeunes enfants ou d'adolescents impliqués dans des actes sexuels. Le Dr Coupal a été reconnu coupable de possession de pornographie juvénile en avril 2014. Radié depuis l'été de façon préventive, il devra purger 12 mois supplémentaires de radiation. La Presse, A12

Le «citoyen souverain» livré à la police de Québec
Le «citoyen souverain» Alain Painchaud a finalement été livré au Service de police de la Ville de Québec (SPVQ) hier par la Gendarmerie royale du Canada, a appris Le Soleil. Il fera face à un juge aujourd'hui au palais de justice de Québec. Il a passé la nuit dernière au poste de police du parc Victoria. «L'individu a effectivement été arrêté ce soir [hier]», confirme le porte-parole du SPVQ, Pierre Poirier. «Il va comparaître demain pour divers mandats d'arrestation.» Au mois de décembre, un mandat d'arrestation contre l'ingénieur avait été lancé par le tribunal, puisqu'il n'avait pas été en mesure de se présenter au palais de justice de Québec, étant détenu aux États-Unis. Le juge Michel Babin, qui préside le procès de l'accusé, devait alors rendre les résultats de l'évaluation psychiatrique de M. Painchaud. Le «citoyen souverain» a été arrêté aux États-Unis au mois de novembre en tentant d'entrer à l'aéroport O'Hare de Chicago sans passeport valide, afin de trouver l'asile politique. L'homme de 45 ans, qui a fondé sa propre république rue Sasseville dans Sainte-Foy en 2013, se disait entre autres persécuté par les autorités canadiennes. Il est notamment accusé d'importation illégale de médicaments, d'avoir eu des armes mal entreposées et d'entrave au travail des agents frontaliers qui ont procédé à son arrestation à l'Aéroport international Jean-Lesage, en mars 2014. Le Soleil, 15

Child exposed to bedbug pesticide improving
A child in hospital after being exposed to a pesticide his parents used to kill bedbugs has been taken off a ventilator and moved to a recovery room. Family spokesman Taj Mohammed said the boy, Zain Hasan, is expected to be discharged from an Edmonton hospital later this month. "It is good news," said Mohammed, the principal of Fort McMurray Islamic School where Zain attends kindergarten. "He is offof the ventilator. He is in the recover section of the hospital and he will be two to three weeks before he is discharged." Funerals for Zain's two-year-old brother, Zia, and eight-month-old sister, Zara, were held in Edmonton last week. Mohammed said Wednesday that it is too soon to know whether Zain suffered any permanent injuries. Aluminum phosphide can emit phosphine gas, which can cause long-term damage to a body's liver, heart and kidneys. The family had recently brought a type of aluminum phosphide back from a trip to Pakistan to kill bedbugs in their apartment in Fort McMurray. Two other children, aged four

and seven, were released from a hospital in Fort McMurray last month. The father, Syed Habib and the mother, Nida Habib, remain in Edmonton. It is not clear how the family managed to bring the pesticide into Canada. The Canada Border Services Agency and RCMP have said they are investigating. Calgary Herald, A10 (Red Deer Advocate)

Libyan national to stay in jail
A Libyan national is in custody while he awaits trial in Halifax on immigration charges. Mohamed Zagruba was living on Chelmsford Place in Halifax when he was arrested last month for allegedly giving misleading information in immigration documents. Zagruba, 33, faces three charges of misrepresentation under the Immigration and Refugee Protection Act. The Canada Border Services Agency alleges that Zagruba failed to disclose in visa applications in November 2013 and September 2014 that he had belonged to a militia in Libya. He's also accused of failing to mention in the 2014 application that he and his wife had separated. Lawyer Kai Glasgow appeared in Halifax provincial court Wednesday on behalf of Zagruba, who chose to stay in a holding cell. Glasgow said his client was consenting to remain behind bars for another three weeks while a release plan is formulated. Judge Michael Sherar scheduled the case to return to court March 25 for a bail hearing. He remanded Zagruba back to the Central Nova Scotia Correctional Facility in Dartmouth. The Crown proceeded by indictment, so each charge carries a maximum penalty of a $100,000 fine and five years in prison. Chronicle Herald, A6

Has Detroit's mayor worked out deal with Moroun?
Political leaders are questioning whether Detroit Mayor Mike Duggan has agreed to a deal with Ambassador Bridge owner Matty Moroun over a vital piece of city-owned land needed for Moroun's twin-span proposal. Riverside Park, which sits on the riverfront underneath the bridge in Detroit, is needed by Moroun before he can get U.S. environmental approvals for his "enhancement project" - a new six-lane cable-stayed bridge to Windsor that would run parallel to the existing bridge. Former Michigan state representative and community leader Rashida Tlaib is concerned Moroun has convinced Duggan to either agree to a deal that gives the park to Moroun or at least provide air rights over the park. She's concerned the cash-strapped city may be looking to profit from the asset. Detroit Mayor Mike Duggan speaks with the media at the North American International Auto Show in Detroit, Michigan on Thursday, January 8, 2015. Duggan's office told The Star Wednesday it would be "several weeks" before the mayor's office would respond to questions of a possible Moroun deal. "This is something we hope to arrange soon, but unfortunately right now the mayor's schedule doesn't allow for it for the next several weeks," an official with the mayor's office said in an email. "He is booked." Any potential deal would still need approval from Detroit's city council. Bridge company president Dan Stamper did not respond Wednesday to a message from The Star. Ambassador Bridge president Dan Stamper appears Thursday, Mar. 22, 2012, in the Wayne County Circuit court in Detroit, MI. Windsor Star, A5

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Nil

LAW ENFORCEMENT / APPLICATION DE LA LOI

OPP confirms Ferguson investigation
Coun. Lloyd Ferguson said he expects a "second vindication" from an Ontario Provincial Police investigation into an alleged assault on a journalist at city hall last year. The OPP was contacted by Hamilton police at the end of February, requesting they investigate a complaint of a historic assault, Sgt. David Rektor confirmed Wednesday. The news came shortly after Ferguson publicly announced he would "penalize" himself over an integrity commissioner report that found he violated council's code of conduct by grabbing and pushing journalist Joey Coleman. Ferguson said he would donate $1,000 to an Ancaster charity and step down from a council committee to recruit a new integrity commissioner. Coleman, who accepted an apology from the Ancaster councillor last year, posted a statement online Wednesday indicating the OPP were investigating. He didn't respond to questions from the Spectator Wednesday.

Ferguson said he was "puzzled" by the investigation and hadn't been contacted by police, but added he welcomes the opportunity to end the controversy. Hamilton Spectator, A1

Ministry calls off RCMP probe into researchers

Wrongly fired Health Ministry employees who have had the threat of an RCMP investigation hanging over them since 2012 have been told the ministry is not pursuing a police investigation. B.C. Health Minister Terry Lake directed his deputy to write to six employees with whom the government has settled wrongful dismissal cases and grievances to say the Health Ministry is not pursuing an investigation by the RCMP. On Sept. 6, 2012, Margaret MacDiarmid, then the minister of health, said the government had asked the RCMP to investigate allegations of inappropriate conduct, contracting and datamanagement practices involving ministry employees and drug researchers. The alleged privacy breach involved large amounts of health data downloaded onto unencrypted flash drives and shared with unauthorized people. MacDiarmid said the ministry provided the RCMP with interim results of its investigation. Seven drug researchers were eventually fired and one contractor lost his job. The government has since settled with six employees and apologized for its "heavy-handed" approach, but had left the threat of an RCMP investigation dangling. "I've asked my deputy to write a letter to the employees with whom we have settled, and to the family of Mr. MacIsaac, to let them know that the ministry is not pursuing any action by the RCMP," Lake said. Times Colonist, S1 Front

Langford attacker hunted by police

West Shore RCMP are looking for a man who attacked a woman, knocked her out and took her cellphone and money while she was jogging on a trail near Glen Lake Beach Park in Langford. The 23-year-old woman was jogging near Shoreview Drive about 7 p.m. Tuesday, when a man asked her for the time. She was then knocked unconscious and robbed. The woman regained consciousness and ran for help to a house where she called 911. West Shore RCMP rushed to the area. The attacker was described as wearing black gloves with thick wristbands and a dark-coloured windbreaker with a patch of red under the arm. The trail was cordoned off by police tape Wednesday. West Shore RCMP major crime investigators and the Vancouver Island district forensic identification section continue to investigate. Times Colonist, A1

Man charged after sex attacks

RCMP say DNA evidence has led to criminal charges, including sexual assault, against a 22-year-old Langley man. Kevin Adelmo Sharp is charged with break and enter, two counts of sexual assault with a weapon, theft of a motor vehicle and assault causing bodily harm. In the first of two similar incidents, a woman told Langley RCMP on Oct. 3 that she had been sexually assaulted. She said she was picked up by a man and they agreed to have sex in exchange for money. After a payment dispute, he then he sexually assaulted her. A second allegation refers to a Surrey incident where a man assaulted and robbed a Langley woman on Oct. 7. Then in May, a woman was grabbed by the neck and sexually assaulted in her home by a man who then stole personal items before fleeing. Postmedia News (Vancouver Sun, The Province); Canadian Press (Times Colonist)

Tip alerted police to potential mall threat

Halifax police say their decision to warn a local shopping mall about a potential threat and the later arrest of three people were based on an anonymous Crime Stoppers tip. Const. Pierre Bourdages said Wednesday that one of those arrested learned he was with the subject of the tip because one of the officers making the arrests at a Halifax apartment inadvertently left behind details from Crime Stoppers. Bourdages declined to say what was in the document, except that it included a photo of the suspect and was part of the search warrant that was supposed to be left behind at the residence. He said anyone offering a tip to Crime Stoppers is guaranteed anonymity, which is why the document contained no information about who alerted police. Police would not identify any of those involved because no charges were laid against the two men and one woman who were arrested on Tuesday and released a few hours later. The investigation at the Mic Mac Mall comes a little more than two weeks after two people were charged with conspiracy to commit murder at the Halifax Shopping Centre in an alleged Valentine's Day plot that police say could have resulted in mass casualties. RCMP have said their investigation and the arrests in that case were prompted by a Crime Stoppers tip. Canadian Press (Waterloo Record, Times Transcript)

Sex trafficking will be part of Pan Am Games, says church officer
Cities that host international sporting events put on their best face for the world to see, but they ignore an ugly reality behind the spectacle: the exploitation of women and children shipped in to cater to the sexual proclivities of spectators, says the general secretary for the Canadian Council of Churches. "Human sex trafficking goes with national and international sporting events," Rev. Karen Hamilton said Wednesday in one in the series of Stuart Ivison Memorial Lectures sponsored by Ottawa's First Baptist Church on Elgin Street. "And it will be coming to my city, because Toronto is hosting the Pan Am Games this summer." Canadians - and the politicians and government agencies who serve them - need to face the reality of both human trafficking and sex trafficking, Hamilton said, suggesting that many of those who attend will be as interested in illicit sex as in the athletes, if not more so. Hamilton said she has drawn the attention of David Peterson, chairman the board organizing the games, to the issue, but to date isn't satisfied it is being taken seriously... Within Canada, the RCMP estimate 600 women and children are trafficked into this country each year for sexual exploitation, and at least 800 are trafficked into Canada for all domestic markets, including the drug trade, domestic work, or labour for garment and other industries. Another 1,500 to 2,000 are trafficked through Canada into the United States. Ottawa Citizen, A5

RCMP assessment ideological
An editorial states, "The RCMP's recently disclosed Critical Infrastructure Intelligence Assessment of Criminal Threats to the Canadian Petroleum Industry might be dismissed as a joke if its implications weren't so disturbing. Given the sweeping nature of proposed antiterror legislation, what does this assessment reveal of attitudes about the environmental movement inside government? The RCMP assessment lists several incidents of criminal activity directed at the petroleum industry. Fair enough. We all likely agree those involved in actual crimes, such as bombings and threats of violence, should be prosecuted. But the police force then launches into a propetroleum polemic that tars the "broadly based anti-petroleum opposition" - hundreds of thousands, if not millions of Canadians - with the same brush as it does a handful of violent criminals. The RCMP's assumption that it's somehow "anti-Canadian" to oppose the expansion of fossil fuel infrastructure is simply wrong. It is also wrong that Canada's police force should indulge in an ideologically based critique of a legitimate social movement. Its job is to enforce laws, not take ideological positions... We actually pay people to churn out this nonsense? If using social media is a sin, I guess the propetroleum movement will be cast into hell along with the greens. Any university instructor who receives a paper of this quality would give it a failing grade. Let's hope this nonsense is not used as justification to impose Canada's growing security apparatus on a legitimate environmental movement. If this is what passes for intelligence, Canada is in danger." Postmedia News (StarPhoenix)

*** Police argue their case in ads**
The Winnipeg Police Association has purchased television advertising to make sure everyone knows its officers are nice people who care about the community and risk their lives every day. Why would the police union spend money on such a campaign, and why now? Two reasons: Crime is trending downward; and, cities are looking for ways to cut costs. The new realities have forced police forces everywhere to defend their salaries and benefits and their staffing levels. The advertising campaign, called Protecting What Matters, is what the military might call shaping the battlefield. The police union wants the public on its side at a time when hard questions are being asked about whether the city has too many police officers, many of whom are drawing six-figure salaries and large pensions. With cities struggling to contain costs, police budgets are a natural target, since they represent the largest single expense for any municipality. Even former public safety minister Vic Toews, now a Court of Queen's Bench judge, said there was a need to curb police costs or eventually face sudden and drastic cuts. Winnipeg Free Press

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Tories seek 'a sentence for life'
The Tory government's latest tough-on-crime initiative to make a life sentence a sentence for life without parole appears to be aimed at scoring political points rather than protecting the public, some critics and

legal experts said Wednesday. Prime Minister Stephen Harper told a Toronto crowd his government will introduce new legislation next week to ensure that what he called the country's "most dangerous, violent offenders," could not be allowed back on the streets. The new bill will "ensure that for the most heinous offenders and the most horrific crimes a life sentence in Canada will henceforth mean exactly that - a sentence for life," Harper announced in front of a crowd that included families of murder victims. The legislation would apply to those convicted of first-degree murder involving: the killing of police officers or correctional officers; terrorism; kidnapping or sexual assault; and crimes "of a particularly brutal nature." It would also apply to those who commit high treason. While hesitant to judge the proposed changes until the bill is tabled, some critics and legal experts said the announcement raises several red flags. "Most dangerous killers are already denied parole and held for life," NDP justice critic Françoise Boivin said in a statement. "Sentencing reform should be focused on improving public safety, not on scoring political points. Decisions about who is released should be based on the risk an individual poses to the community and how to best protect public safety," she said. Benjamin Berger, a criminal law expert at York University's Osgoode Hall law school, said the announcement comes across as "political sleight of hand." (...) According to the latest Correctional Service of Canada data on recidivism available, 658 convicted murderers were released on full parole between January 1975 and the end of March 1990. Of those, five were convicted of committing a second murder - three of first-degree and two of second. Canadian Press (Vancouver Sun, B1/Front, Hamilton Spectator, A1, Red Deer Advocate, Chronicle-Herald, The Province, Windsor Star, StarPhoenix, Leader-Post, Calgary Herald, Montreal Gazette, Ottawa Citizen, Edmonton Journal, Whitehorse Daily Star, Times Colonist, Maclean's, Times & Transcript, Telegraph-Journal, The Telegram, The Guardian, Waterloo Region Record, Cape Breton Post), * Presse canadienne (Le Droit, Voix de l'Est, La Tribune, Acadie nouvelle), * Winnipeg Free Press, * La Presse (Le Nouvelliste, 31), Journal de Québec (Journal de Montréal),

En prison jusqu'à ce que mort s'ensuive

La mesure annoncée pourrait s'avérer inconstitutionnelle, selon un juriste. Le gouvernement fédéral veut qu'une peine d'emprisonnement à perpétuité en soit réellement une. Le premier ministre Stephen Harper a annoncé mercredi que son gouvernement ira de l'avant son projet de loi controversé et présentera dès la semaine prochaine une mesure législative pour que de telles peines n'incluent pas de possibilité de libération conditionnelle. Le projet de loi va s'appliquer à ceux qui sont condamnés pour meurtre prémédité d'un policier ou d'un agent correctionnel, condamnés pour terrorisme, kidnapping ou agression sexuelle ainsi que pour des crimes " d'une nature particulièrement violente ". Il concerne aussi les personnes condamnées pour haute trahison. " Notre gouvernement déposera un projet de loi pour s'assurer que pour les criminels les plus haineux et pour les crimes les plus horribles, une peine de prison à vie au Canada va vouloir dire exactement cela -- une peine à vie ", a annoncé le premier ministre devant une foule qui incluait les familles de victimes de meurtre réunies à Toronto. Actuellement, ceux qui sont condamnés pour meurtre prémédité se voient infliger automatiquement une peine de prison à perpétuité sans possibilité de libération avant 25 ans. Considérations constitutionnelles Pour Hugo Cyr, professeur de sciences juridiques à l'Université du Québec à Montréal et spécialiste en droit constitutionnel, cette nouvelle mesure législative est " une solution qui cherche un problème ". " Il ne faut pas croire qu'il est facile de sortir de prison après 25 ans. Présentement, c'est difficile d'obtenir une libération conditionnelle. Cette annonce semble être davantage une mesure pour plaire à un certain électorat que la réponse à un problème réel ", estime-t-il. Le Devoir, A1; * National Post

*** Life sentence will mean life**

In a few weeks the Conservatives are going to table a bill to make a life sentence be what it actually sounds like. This measure will seal the deal on the 2013 throne speech commitment that the "government will change the law so that a life sentence means a sentence for life." Currently, a life sentence in Canada means no eligibility for parole until 25 years is served. But on Wednesday, speaking at an event in Scarborough, Ont., Prime Minister Stephen Harper announced that some categories of individuals convicted of first-degree murder will receive life with no parole. The PM said that while "we want rehabilitation for all criminals," there are certain criminals who should never be allowed to walk the streets. These include first-degree murders that involve terrorism, kidnapping or forced confinement, sexual assault and the killing of police or corrections officers. Also added to the list is "any first-degree murders that are found to be of a particularly brutal nature." It will be interesting to see how the proposed legislation outlines what brutal nature means and how much judicial discretion is granted. Not only was

this legislation expected, but it's also not a huge change. (...)Also, it's not like true life in prison isn't possible right now. The corrections system already has the ability to keep someone locked up forever. Many of "the most heinous offenders," as the PM refers to them, would likely face a true life sentence regardless. For instance, while Paul Bernardo is eligible for full parole beginning in 2018, most legal observers don't think he'll ever receive it. Eligibility does not guarantee freedom. QMI Agency (Kingston Whig-Standard, B1, London Free Press, Winnipeg Sun, Toronto Sun, Edmonton Sun, Calgary Sun, Ottawa Sun)

Convicted murderers who have gained some form of freedom
Four murderers who might still be in prison if convicted under the 'life without parole' measures: Harold Smeltzer Convicted in 1980 of abducting and drowning five-year-old Kimberly Thompson in the bathtub of his parents' Calgary home. Admitted to attacking and raping at least 40 more women and girls upon his arrest. He received day parole in 2008 and a recent Parole Board report confirmed he was spotted lurking around playgrounds as recently as last summer. Steven LeClair In 1980, LeClair shot and killed three random patrons at a Vancouver bar, then drove to Richmond RCMP headquarters to murder the front desk officer. Last year, he began receiving unescorted absences from prison. Craig Munro Monro shot and killed 30-yearold Toronto police Const. Michael Sweet during a botched robbery in 1980. He was granted unescorted leaves from prison in 2010 despite the protests of then-OPP commissioner Julian Fantino. Bill Nichols At the peak of a lengthy 1976 crime spree, Nichols murdered Calgary police officer Staff. Sgt. Keith Harrison in a shootout before taking four hostages at a Calgary home. Despite public protests, he was freed 17 years later under the faint hope clause. Postmedia News (Vancouver Sun, B1/Front, Leader-Post, StarPhoenix, Montreal Gazette, Calgary Herald, Edmonton Journal)

* **Harper's found his own wedge issue**
An opinion piece states, “Life means life. Vote Conservative. On Wednesday, Prime Minister Stephen Harper announced that the government will introduce legislation to keep criminals "too cruel and dangerous to be put back into freedom" locked up permanently, with no possibility of parole. "Our Government believes in standing up for victims of crime and their families, putting their rights and interests ahead of those of criminals, and that a prison sentence should mean what it says. ... [A] life sentence in Canada will mean exactly that: a sentence for life." Politically, the announcement's optics were picture-perfect. Harper delivered his message at a Chinese cultural centre in Scarborough, a part of Toronto that sees more than its share of crime. Six Toronto-area MPs were in attendance, including Citizenship and Immigration Minister Chris Alexander and the PM's Parliamentary Secretary, Paul Calandra, as well as Justice Minister Peter MacKay, whom Harper pointedly credited with helping craft the legislation. The enthusiastic crowd reflected the diversity of Canada's biggest city, and the votes the Tories hope to get there in the upcoming election. But Harper's message wasn't just intended for Toronto, or its ethnic communities. It was intended for Edmonton, a city reeling from the killing in January of policeman Matthew Wynn by Shawn Rehn, an offender with a lengthy criminal record and a history of domestic violence. And for Vancouver, where a parole board is weighing whether killer Allan Schoenborn, found "not criminally responsible" for stabbing and smothering his three children in 2008, should be granted supervised day passes, despite posing "a significant risk of causing physical or psychological harm." And for Winnipeg, where just days ago, it was announced that Vince Li, a schizophrenic who gruesomely beheaded and cannibalized fellow passenger Tim McLean on a Greyhound bus in 2008, will be getting unsupervised day passes, to the horror of Mc-Lean's mother and many citizens in the community.” National Post, A11

* **Canada doesn't need a 'life-means-life' law**
An opinion piece states, “Canada does not need a so-called "life-means-life" law. But we're getting one anyway, courtesy of the always-ideological Harper Conservative government. This law, mandating sentences of life in prison with no parole, will target those who murder police or prison officers, commit terrorist acts, carry out kidnapping or sexual assault resulting in murder, or commit crimes that are "of a particularly brutal nature." Canada's most dangerous killers - the Paul Bernardos - are never getting out of prison. They won't be granted parole. They are not a threat. And this law won't deter the next heinous criminal. There's no difference in that sort of mind between no parole for 25 years and no parole ever. The death sentence isn't a deterrent, and neither is life in prison without parole. Here's another reality: This law will be challenged under the Constitution and will probably be struck down. And another: The

country's violent crime rate is low and dropping. And another: Housing the few inmates this will affect will simply cost more and not result in better or different outcomes. This is all about optics and partisanship in an election year. Period." Hamilton Spectator, A12

*** Throwing away the key just throws away justice**
An opinion piece states, "Prime Minister Stephen Harper is most definitely a man of his word. Even if keeping that word will have the effect of setting back Canada's justice system decades, if not centuries. On Wednesday, the prime minister kept a 2013 promise to eliminate parole for murderers who employ sexual assault, kidnapping and confinement, terrorism, the killing of police or corrections officers in their crimes, and first-degree murders found to be "of a particularly brutal nature." Harper had been warned by federal lawyers last year taking away any hope of parole would be constitutionally untenable. So, the Conservative government will give those sentenced to life in prison a chance to apply for clemency after serving 35 years. Harper argued Wednesday the responsibility to assess the parole eligibility of convicted murders should not rest with an appointed board. Instead, it will rest with "the federal cabinet; men and women fully accountable to their fellow citizens and to the families of the victims of these crimes." This one aspect, in and of itself, is particularly troublesome. It has been nearly 40 years since federal politicians had the power to make decisions on who was paroled or, in the period before 1972, sentenced to death. Politicizing that process again, and trying to dress it up as accountable government, is a long bow for the Tories to draw. For much of the time since, we have allowed the Parole Board of Canada to assess the suitability of parole candidates, and on the whole the system has worked well. Recidivism rates among offenders of all violent crimes are low; among murderers, they are even lower. Just a fraction of one per cent." Winnipeg Free Press

*** La prison à vie a peu d'effet sur le taux d'homicides**
Épreuve des faits - Le premier ministre Stephen Harper fait fi des critiques et va de l'avant avec son projet d'imposer l'emprisonnement à vie à certains meurtriers, sans possibilité de libération. Il promet qu'un projet de loi en ce sens sera déposé aux Communes la semaine prochaine. Pour lui, plus question d'obtenir de libération conditionnelle après 25 ans, comme c'est le cas présentement. Mais cette mesure va-t-elle vraiment faire réduire le taux d'homicides au Canada? Vérification faite : c'est difficile à dire. Les données de Statistique Canada sur les homicides démontrent que le taux d'homicides au pays est en nette régression depuis 1983. Le taux le plus récent disponible est celui de 2013 à 1,44 meurtre par 100 000 habitants. C'est le taux le plus faible depuis 1966. La pire année, en 1983, ce taux atteignait 2,69. Des experts consultés attribuent en grande partie cette baisse au vieillissement de la population, et non à la nature des peines imposées. Selon eux, le groupe le plus susceptible de commettre des meurtres est celui des hommes de 18 à 40 ans, dont la proportion diminue depuis 1983. D'autres l'attribuent aux actions policières ciblant le crime organisé, y compris les bandes de motards criminels, mais préviennent qu'il ne s'agit que d'un cycle. Radio-Canada

« Mom » serait actif en prison
Maurice «Mom» Boucher ne semble pas avoir pris sa retraite du milieu criminel même s'il purge une peine d'incarcération à perpétuité et qu'il a été expulsé des Hells Angels. Le Journal a appris que le nom de l'ancien chef du gang de motards a refait surface du-rant une enquête policière menée à l'encontre d'un réseau de trafic de stupéfiants, dans la grande région de Montréal. Selon nos sources, l'homme de 61 ans tirerait encore des ficelles dans le monde interlope, à partir du pénitencier à sécurité maximum de Sainte-Anne-des-Plaines où il est gardé soit dans l'Unité spéciale de détention (USD). Les policiers soupçonnent l'ex-Nomads d'avoir obtenu l'aide d'un membre de sa famille pour mener ses affaires à l'extérieur des barreaux de sa cellule. Aucune accusation n'a encore été portée relativement à cette enquête. «Mom» a été condamné à la prison à vie, en 2002, pour avoir commandé les meurtres des gardiens de prison Diane Lavigne et Pierre Rondeau. Il ne pourra faire sa première demande de libération conditionnelle qu'en 2022. Depuis sa condamnation, il est incarcéré à l'USD, comme 70 codétenus nécessitant des mesures de sécurité accrues. Plus de 50 caméras permettent aux gardiens d'assurer «une surveillance complète» des lieux, selon le Service correctionnel du Canada. Journal de Québec, 5 (Journal de Montréal)

Ernest Fenwick Macintosh and justice

It was just a matter of time and opportunity before Ernest Fenwick MacIntosh sexually abused another boy, says Bob Martin, one of his victims from more than 40 years ago. "What upset me was when Dr. Angela Connors got on the stand and said there was less than a 20 per cent chance that Mr. MacIntosh would reoffend," said Martin, who was sexually abused by MacIntosh in the early 1970s. "We were going, 'Hell no. He's serial. He needs this.' We were always concerned that he would go out there and do it again." When MacIntosh, who turns 72 this month, did it again, Martin, a photographer now living and working in Port Hood, was watching from afar. During two 2010 trials, MacIntosh was convicted on 18 charges of gross indecency and indecent assault against Martin and five other boys in the Port Hawkesbury area in the '70s. He was sentenced to 5 years in prison. But those convictions were later overturned by the Nova Scotia Court of Appeal because it took too long to bring MacIntosh to trial. Since MacIntosh won his appeal in 2013, Martin has been keeping tabs on him through Google and any other means available. MacIntosh posted a video of his affiliation with a spice company in Sri Lanka and then moved on to Nepal. "You see this guy all the time, the smirks," Martin said. "I'm not a pedophile vigilante. I'm not this guy that wants to harm this man, but I just don't want him to harm other people." But it seems that Martin was right. MacIntosh could not stop harming others, specifically prepubescent boys. (...) Correctional Service Canada regulations make it unlikely that MacIntosh will be transferred to Canada to serve his time. Veronique Rioux, with Correctional Service, said in an email Wednesday she couldn't comment on a specific case, but she added that all transfers from other countries are done under the International Transfer of Offenders Act and are carried out only between Canada and countries with which it has a valid transfer agreement. Nepal is not on that list of countries. Chronicle-Herald, A4

Scumbag on the loose

A violent sex offender who was just freed from Grande Cache Institution and planned to call Edmonton home is already wanted on a Canada wide warrant. Ashton Dennis Natomagan -- born Nov. 21, 1981 -- is serving a five-year sentence for sexual assault causing bodily harm. He was freed from the medium-security prison 435 km west of Edmonton on March 2 and was to live in Edmonton but failed to report to authorities as required and is now wanted on the warrant. Even if Natomagan had reported to authorities, Edmonton city police were prompted to issue a warning to the public about his release. Edmonton police said Wednesday that Natomagan is considered to be a sexual offender who poses a risk of significant harm to the community and that he was to be closely monitored by Correctional Services Canada. Natomagan's rap sheet also includes 46 criminal convictions, including multiple cases of failing to report/comply with conditions, break and enters, property related offences, driving offences, five counts of escaping lawful custody, being unlawfully at large, thefts, drug related offences, and an additional sexual assault causing bodily harm conviction. Edmonton Sun, 3; * Edmonton Journal, * CBC News

*** Violent offender released**

City police are issuing an alert after a violent offender who plans to live in the Edmonton area was freed from Grande Cache Institution. In the interest of public safety, police say that Michael Wayne Beauchamp was released Tuesday from the medium-security prison 435 km west of Edmonton after completing a six-year sentence for robbery, overcome resistance by attempting to choke, suffocate or strangle another person, and failure to comply with recognizance. Beauchamp is considered by police to be a violent offender who poses a risk of significant harm to the community. He will be living in the Edmonton area and will be closely monitored by the Edmonton Police Service Behavioural Assessment Unit. Edmonton Sun, 3, Edmonton Journal

Sarah Cousineau Denis fait appel

Près d'un mois après avoir été condamnée à passer deux ans et demi derrière les barreaux, Sarah Cousineau Denis interjette appel de sa sentence. « Sarah n'a pas demandé de remise en liberté [d'ici à ce que la Cour d'appel rende sa décision], a indiqué hier à La Voix de l'Est sa mère, Josée Denis. On souhaite juste que le jugement corresponde à la fourchette normalement consentie pour ce genre de cause. » La dame, elle-même avocate, n'a toutefois pas voulu commenter au sujet de la durée d'une peine « convenable », s'en remettant uniquement à l'avis d'appel déposé le 20 février par le procureur qui représente de la jeune détenue, Me Pierre Poupart. La femme de 21 ans a écopé de 30 mois d'incarcération, le 4 février, au palais de justice de Granby. A cela s'ajoute une interdiction de conduire de cinq ans à sa sortie de prison. Rappelons que la Mercedes de Sarah Cousineau Denis a fait une violente embardée, le 12 novembre 2012 dans le chemin Bondville à Lac-Brome, après qu'elle en a perdu la

maîtrise en roulant à plus du double de la vitesse maximale permise dans une zone de 50 km/h. Voix de l'Est, 5/Front

*** Federal offender unlawfully at large**
The OPP Repeat Offender Parole Enforcement (ROPE) Squad is asking for the public's assistance locating a federal offender. Jamaal Jackson, 30, is serving a seven-year, seven-month sentence for several robbery related offences, and now has a Canada-wide warrant for breaching parole. "Robbery is a theft with violence," det.-Sgt. Brett Anderson, from the ROPE Squad, said. "Could have been an assault or weapon involved. There are several robbery offences he is serving time for." Anderson said Jackson is not at his hal fway house in Toronto. "He's unlawfully at large, so he would have failed to return," Anderson said. "It's either a fail to show up at the halfway house or a fail to return by curfew." Kingston Whig-Standard, A6

*** High court upholds killers' first-degree murder terms**
Manitoba's highest court has ruled a deadly ambush inside an Elmwood house was a cold-blooded act and not something less. Blake Whiteway and Tyler Sutherland were each convicted of two counts of first-degree murder and one count of attempted murder for the December 2009 attack that left two teens dead and another seriously injured. The men, just 16 and 17 at the time, were given adult sentences of life in prison with no chance of parole for at least 10 years. Whiteway and Sutherland both appealed the verdicts, saying they were "unreasonable" and should be overturned. Whiteway was seeking a second-degree murder conviction, while Sutherland wanted a new trial. As well, Sutherland claimed he should not have received an adult penalty. The Court of Appeal, in a decision released this week, dismissed all grounds of appeal. Winnipeg Free Press, A8

*** Court upholds sentence for church counsellor**
The province's highest court has upheld a 14-year prison sentence for a man who used his position as a counsellor for two church youth groups to sexually abuse six boys and amass one of the largest collections of child pornography ever found in Canada. The Alberta Court of Appeal also dismissed the appeal by Roderick Kyle Janssen to overturn the subsequent 10-year period of community supervision as a long-term offender. Calgary Herald, A9

*** La famille d'une victime se dit abandonnée par le système**
Les parents d'une jeune femme tuée par une chauffarde déplorent que les commissaires n'aient pas tenu compte de leurs craintes en libérant celle qui a embouti la voiture de leur fille. Condamnée à 50 mois de pénitencier en mai 2013, Irina Mysliakovskaia n'aura passé qu'un an derrière les barreaux et huit mois en maison de transition. Elle a causé la mort de Katherine Beaulieu, 21 ans, en conduisant en état d'ébriété en sens inverse sur l'autoroute 55, près de Trois-Rivières, en mai 2010. Hier, la Commission des libérations conditionnelles du Canada lui a accordé une libération totale. "C'est aberrant, tonne la mère de la victime, Lise Lebel. Elle a quand même enlevé la vie de quelqu'un, pas volé un fromage dans une épicerie." Journal de Montréal, 11

*** Un rabais de 50% la renvoie en prison**
Poser un autocollant de rabais de 50% sur un article qui n'était pas en réduction a coûté cher à Stivia Clermont. Celle qui avait été condamnée à la prison à vie pour meurtre, en 1998, a vu sa libération conditionnelle suspendue pour ce larcin. L'incident s'est produit dans un commerce de la région de Québec, le 6 novembre dernier. Mme Clermont, maintenant âgée de 50 ans, a été interceptée à la caisse. Elle a été arrêtée et s'est avouée coupable de fraude dès sa comparution, le lendemain. Elle a reçu une peine de 15 jours, à purger concurremment à sa peine de prison à vie. Mme Clermont purgeait sa peine à l'établissement carcéral pour femmes de Joliette. Mme Clermont avait fait plus de trois mois de prison quand, le 19 février dernier, au terme d'une audience, la Commission des libérations conditionnelles a accepté d'annuler la suspension de sa libération conditionnelle. La Commission a considéré que le «geste malhonnête de faible envergure» était un incident de parcours irréfléchi, dans un cheminement jusque-là très positif. Mme Clermont devra cependant rencontrer son équipe de gestion de cas plus souvent. Une libération conditionnelle totale signifie que la personne purge le reste de sa peine sous surveillance dans la collectivité. «Vous avez compris que vous devrez, en raison de votre statut, maintenir un comportement sans reproche», lit-on dans la récente décision de la Commission des

libérations conditionnelles. Mme Clermont avait été condamnée à la perpétuité, pour le meurtre prémédité de Rocco Racaniello, assassiné à coups de couteau, dans son abri Tempo, en janvier 1995. La Presse, A12

*** Supreme Court to rule on conviction in Candace Derksen slaying**
The Supreme Court of Canada will rule today in the case of Mark Edward Grant, whose conviction in the 1984 abduction and murder of Winnipeg teenager Candace Derksen was overturned. The country's highest court must decide whether to reinstate Grant's murder conviction or side with the Manitoba Court of Appeal, which ordered a new trial for him in 2013. The provincial appeal court said the original trial judge did not consider some evidence that could have cast doubt on Grant's guilt. Manitoba prosecutors appealed the decision to the Supreme Court, which heard arguments in November and will issue its ruling on Thursday morning. Derksen was 13 years old when she disappeared on her way home from school on Nov. 30, 1984. Her body was found six weeks later, bound and frozen, in a storage shed not far from her family's home in Winnipeg's East Kildonan neighbourhood. Grant was not charged until 2007, after numerous tests on a piece of twine used to bind the teen. A jury found him guilty of second-degree murder in February 2011, and he was sentenced to life in prison with no parole eligibility for at least 25 years. Grant has repeatedly denied killing Derksen. CBC News

*** Nova Scotia Court of Appeal rejects application for government-funded lawyer**
The Nova Scotia Court of Appeal has denied a request for legal assistance to a 31-year-old New Glasgow man convicted in connection with a brutal sexual assault in Port Hawkesbury. Justin Christopher Miller was sentenced to 12 years in prison in 2012 after pleading guilty to aggravated sexual assault that occurred Aug. 28, 2010, in Port Hawkesbury. After credit for time served, Miller's sentence equalled nine years, seven months and four days. In a decision released Tuesday, Justice Joel E. Fichaud ruled he was not satisfied it was in the interest of justice that Miller be provided with government-funded counsel for his appeal and was dismissing Miller's application. Miller appealed his sentence, contending the amount of time imposed exceeded the upper limit of the appropriate range for such a crime. He applied for legal aid to represent him at an appeal but after a review his request was denied. He then appealed to the appeal committee of Nova Scotia Legal Aid, which also dismissed his application. He then applied for an order under a section of the Criminal Code that provides for government funding of an appeal, which Fichaud dismissed. At the time of sentencing, the court was told that Miller and the female victim were at a friend's home, and after the victim left, Miller followed her and then attacked her near the courthouse in Port Hawkesbury. Cape Breton Post, A3

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** University, premier deal with Muslim controversies**
Concordia's dean of students will meet with leaders of the university's Muslim Students Association regarding a television report that suggested the association's library contains books and videos by "extremist preachers." The library "is in a modest setting, but nonetheless has cutting edge software that allows users to consult online books, (among which) TVA news found dozens of works by radical imams," said the report, which aired Friday. In related news, Premier Philippe Couillard said Wednesday a Quebec Liberal member of the legislature should not have advertised on an Islamic community centre website that includes texts extolling violence against women. A photo of Marc Tanguay, his contact information and the logo of the national assembly appeared on the FATH community centre website. Couillard called for the ad to be withdrawn and Tanguay complied. "It's not a question of freedom of expression," Couillard said. "Freedom of expression allows people to say stupidities and that's why it exists." But the premier said public funds should not be used to help spread such opinions. Postmedia News (Vancouver Sun, B3, Montreal Gazette, Edmonton Journal, StarPhoenix, Windsor Star, Ottawa Citizen, Calgary Herald), Canadian Press (The Guardian, National Post, Chronicle-Herald, Toronto Star, Globe and Mail), Presse canadienne (Le Quotidien, La Tribune, Le Devoir, Le Nouvelliste, Le Droit, Montreal Gazette, Mississauga News), Journal de Québec (Journal de Montréal)

*** Focus on schools**

A letter to the editor states, "Re: 'Money alone won't solve First Nations' problems,' Susan Martinuk, Opinion, Feb. 27. With the debate around the need for an inquiry into missing and murdered aboriginal women, we should keep in mind that murder statistics for aboriginal men are worse. While only three to four per cent of the population is aboriginal, 17 per cent of murdered men in Canada in 2010-2011 were aboriginals. This is not a gender issue, it is a broader issue affecting all First Nation peoples. With or without an inquiry, all sides must agree that some necessary actions are apparent, such as reforms to funding of First Nations' education. Both sides should get back to the table to negotiate changes that get Bill C-33 passed. A First Nations' education bill that establishes adequate and sustained funding, appropriate quality standards and First Nations control, would do more to address systemic issues than inquiries and political rhetoric." Calgary Herald, A22

*** Why Harper will never call an inquiry into missing/murdered women**
An opinion piece states, "Last week, indigenous leaders and families, together with representatives from all provinces, territories and the federal government, met to draft an action plan to address the issue of missing and murdered indigenous women. When the talking was over, two groups formed behind two podiums in two separate locations and gave two very different versions of events. Both groups heard the same heart-wrenching accounts of murdered and missing women and girls, the same calls for action - yet came to very different conclusions about the nature of the problem. At one podium, presenters voiced their frustration over Ottawa's refusal to call a national inquiry. Across the street, Minister of Aboriginal Affairs Bernard Valcourt and Kellie Leitch, minister for Status of Women, put their emphasis on the criminal aspects of the issue - making it clear that a national inquiry is still off the table. Prime Minister Stephen Harper began defining his government's position on missing and murdered indigenous women some time ago while discussing the murder of 15-year-old Tina Fontaine. He dismissed the sociological aspects of these deaths and insisted his government views them as crimes, plain and simple - a position that has kept them in conflict with indigenous communities ever since. Why have Harper and his ministers stuck so tenaciously to the idea that these deaths and disappearances are crimes without social elements? Because it keeps things simple and takes a potential political liability and forces it to contribute to the government's tough-on-crime narrative. By pushing the discussion into a law-and-order setting it shifts the burden of responsibility from the federal government to local communities and law enforcement. At the same time, it strengthens their argument against a national inquiry." iPolitics

*** Hells ontariens et mafia montréalaise font équipe**
Les Hells Angels ontariens de la section Nomads et la mafia montréalaise ont formé une alliance pour combler le vide causé par l'incarcération d'une centaine de Hells au Québec depuis six ans, constatent les policiers. Selon nos sources, Gregory Wooley, chef du gang Syndicates, aurait joué un rôle clé dans ce partenariat d'affaires, ayant lui-même orchestré une alliance entre les gangs de rue Bleus et Rouges, à Montréal, depuis 2012. Wooley, un ex-membre des Rockers, le défunt club-école des Hells, a déjà compté parmi les hommes de confiance de Maurice «Mom» Boucher avant de devenir un allié du clan Rizzuto. Lui et le nouveau chef présumé des Hells, Salvatore Cazzetta, ont été vus aux funérailles du parrain Vito Rizzuto, mort en décembre 2013. Les policiers constatent présentement une «forte présence» au Québec des Hells Angels de la section Nomads de l'Ontario. Plusieurs de leurs membres sont originaires du Québec et certains y sont toujours établis. Journal de Québec, 5 (Journal de Montréal)

PUBLIC SERVICE / FONCTION PUBLIQUE

Nil

OTHER

*** Online database of leaked Edward Snowden documents now available in Canada**
The first online database of classified documents leaked by former U.S. National Security Agency contractor Edward Snowden has been created in Canada. The Snowden Archive is a joint project between Canadian Journalists for Free Expression and the Politics of Surveillance Project at the Faculty of Information at the University of Toronto. It is the first time hundreds of leaked documents have been

indexed and made fully searchable online. It is the first time hundreds of leaked documents have been indexed and made fully searchable online. CJFE says the archive is a resource for journalists, researchers and concerned citizens to learn more about government surveillance practices. The database will be unveiled at Ryerson University in Toronto on today after a live video discussion with Snowden, followed by a panel discussion. Canadian Press (Whitehorse Daily Star, 10, Telegraph Journal, Times & Transcript)

* **Snowden warns of anti-terror law perils**
Free countries should not pass laws that limit liberties because they are afraid of terrorist threats, warned U.S. whistleblower Edward Snowden on Wednesday during a live web chat. In a sobering online talk sponsored by Canadian Journalists for Free Expression at Ryerson University, Snowden spoke briefly about Ottawa's controversial new anti-terror law, Bill C-51, and the erosion of public rights. The former National Security Agency employee said only Canadians can decide on whether C-51 is a good or bad bill, but "Canadian intelligence has one of the weakest oversight frameworks out of any western intelligence agency." In Canada, terrorism kills fewer people than lightning strikes and it is extraordinarily rare, Snowden said. "No matter what we do, no matter what laws we pass, we cannot throw away all of our rights, all of our liberties, all of our traditional freedoms because we are afraid of rare instances of criminal activity," he said. Toronto Star, A16, QMI Agency (Toronto Sun, Edmonton Sun, Winnipeg Sun, Calgary Sun, Ottawa Sun), Canadian Press (The Record A5, Ottawa Citizen, Hamilton Spectator, Chronicle Herald)

INTERNATIONAL

* **The Globe adopts encrypted technology in effort to protect whistle-blowers**
In a bid to create a safe and secure way for sources and whistle-blowers to communicate with us, The Globe and Mail has become the first Canadian media organization to launch a system known as SecureDrop. Already used by The New Yorker, The Guardian, The Washington Post and more than a dozen other publications, SecureDrop creates a channel for anonymous and encrypted Internet communications that can link potential sources with investigative journalists. Globe and Mail, A4

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
March 10, 2015 / le 10 mars 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Des canadiens sous surveillance
Le SCRS pouvait déjà mener des activités à l'étranger afin de contrer les menaces terroristes au pays, mais les nouvelles dispositions faciliteraient l'obtention de mandats pour mener de telles enquêtes. Le **ministre de la Sécurité publique, Steven Blaney**, a indiqué lundi, devant un comité sénatorial, que le projet de loi permettrait de suivre à la trace plus efficacement les Canadiens partis à l'étranger pour suivre un entraînement ou combattre aux côtés d'organisations terroristes. Selon un rapport fédéral publié l'an dernier, le gouvernement savait que 130 personnes ayant un lien avec le Canada se trouveraient à l'étranger pour soutenir une activité terroriste, et que 80 d'entre elles seraient depuis rentrées au pays. Même s'il l'avait déjà fait dans le passé, le directeur du SCRS, Michel Coulombe, a refusé lundi de mettre à jour ces chiffres, pour ne pas dévoiler d'informations sur le déploiement de ses agents. Il s'est contenté de dire que le nombre de Canadiens qui tentent de joindre les groupes terroristes à l'étranger augmente progressivement. «On ne parle pas de milliers», a-t-il simplement admis. Le **ministre Blaney** a abondé dans le même sens, indiquant qu'une telle divulgation exigerait que l'on détermine si ces personnes se trouvent à l'étranger ou s'ils sont au pays. Presse Canadienne (L'Acadie Nouvelle, 18)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

River-watch season underway

The threat of floodwaters has Dan Dionne up at night. In the wake of unparallelled St. John River levels in recent past, the chief administrative officer of Perth-Andover now receives an email alert from a gauge at the water's edge if there's a noticeable rise. "In the middle of the night, if you're wondering what the water levels is, it's easy to monitor," Dionne said. "I'm the one waking up to check it normally." It's river-watch season, and those that line the province's tributaries are back on edge. The Daily Gleaner, A1 (Telegraph-Journal, A1)

* **Long-term effects feared after CN derailment - Groups say it will take time to reveal environmental impact of crude oil spill**

It could take weeks or even months to understand the real environmental impact of the crude oil spill from a derailed CN train near the town of Gogama, Ont., on Saturday, activists say. "Everything goes somewhere ... The vast majority of what has already leaked or burned will never be recovered," said Keith Stewart of Greenpeace Canada. The crude oil will end up in the environment around Gogama, a tiny town about 100 kilometres south of Timmins, and "will affect that area for a long time to come," Stewart said. "Long after this initial spotlight fades away, we'll still see impacts in the local ecosystems." Some crude will end up in the soil, some in the water and the crude that burned "will deposit toxins in the area which will eventually get into the ecosystem," he added. Thirty-eight cars of a 94-car train derailed near Gogama at 2:42 a.m. on Saturday, triggering a massive blaze that burned furiously until it was extinguished Monday evening. Two cars plunged into the Matagami River. At least one ruptured and leaked crude into the water. The two rail cars were removed from the river on Monday evening. The train was carrying synthetic crude oil, an intermediate product produced when bitumen is upgraded to make it transportable. It is then shipped to a refinery where it is turned into a finished product. It's not yet known how much crude was spilled or how the train derailed, in part because it has been impossible for its investigators to get close to the actual site, a spokesperson for the Transportation Safety Board of Canada said. Toronto Star, A8; Le Devoir

* **Ottawa defends rail-safety efforts after another derailment in Ontario**

The federal government on Monday defended its efforts to boost rail safety in the wake of a fiery derailment in northern Ontario that has stoked concerns over the transportation of crude oil by train. Saturday's derailment of a CN train near Gogama was the second such incident near the community about 80 kilometres south of Timmins in less than a month, and the local member of provincial parliament said it left residents on edge. "For the people of Gogama, it was a very close one," said NDP MPP France Gelinas, who represents the Nickel Belt area. "They all said, 'What if it had been two kilometres this way, we wouldn't be there [anymore],' " she said. "This is a what-if that will be hard for a lot of people to forget and we need to have substantive changes so that people in Gogama and throughout the northeast can feel safe again." Federal Transportation Minister Lisa Raitt said the government has already made several changes to improve rail safety in the two years since the deadly derailment in Lac-MÃ©gantic, Que., including upgrading standards for the tanker cars involved in that incident. The government is also working to replace the Class 111 cars in the next few years, Raitt said during question period. "We are working with the United States on what a new system will be in terms of a new tank car standard," she said. Canadian Press (Times Colonist, B5; Daily Gleaner)

* **Transport ferroviaire - Un moratoire s'impose**

Quatre nouveaux déraillements impliquant des dizaines de wagons-citernes remplis de pétrole explosif se sont produits depuis moins d'un mois dans l'est du continent. Le temps est venu d'exiger un moratoire sur le transport de pétrole brut par rail dans les zones habitées du Canada. Au moment d'écrire ces lignes, lundi, le pétrole brûlait toujours à Galena, en Illinois, et à Gogama, dans le nord de l'Ontario. Dans ce dernier cas, le convoi du CN qui provenait d'Alberta se dirigeait vers Lévis, au Québec. C'est le quatrième incident du genre à survenir en un mois, dont deux dans la même région de Timmins, en Ontario. Les employés du CN étaient d'ailleurs toujours sur place, à Gogama, pour poursuivre les travaux de nettoyage rendus nécessaires par l'accident du 14 février. Selon les premières constatations, le train du CN ne transportait pas du pétrole de schiste de la formation de Bakken reconnu pour être très explosif, mais du pétrole conventionnel. Voilà qui rend cet accident encore plus inquiétant. On ne connaît pas la cause de chacun de ces déraillements, mais on ne peut que constater l'incapacité des autorités et des compagnies ferroviaires à empêcher qu'ils ne se reproduisent à un rythme alarmant. Dans tous les cas récents, les wagons éventrés sous le choc de l'impact étaient du modèle CPC-1232, que l'on disait plus

solide que les tristement célèbres DOT-111 impliqués dans la catastrophe de Lac-Mégantic. Le Devoir, A6; Financial Post (Vancouver Sun; Leader-Post; Calgary Herald)

*** Mégantic: Not the last such explosion**
An editorial states "When the federal government announced bulked-up rail-safety measures last fall, Transport Minister Lisa Raitt said, 'Canadians are never going to forget what happened in Lac-Mégantic.' The oil-fuelled fireball that claimed 47 lives in 2013 scarred our national consciousness, but Ms. Raitt's words would carry more heft if oil-ferrying trains didn't keep exploding on her watch. On Monday, firefighters wrestled with burning cars after a derailment near Gogama, Ont., about 600 kilometres north of Toronto. The rest of us are grappling with questions, such as: Weren't updated safety requirements for tanker cars and a stouter inspections regime supposed to make the booming oil-by-rail trade vastly safer for Canadian communities? They haven't, apparently. The weekend accident is the second major derailment in the Gogama area in three weeks. It adds to harrowing post-Mégantic conflagrations in Plaster Rock, N.B., and Gainford, Alta., and a slew of other calamities all over North America. Ms. Raitt said she's very concerned by the latest mishap; perhaps she'll heed the appeals from the Ontario government, among others, to move more boldly. The federal government can't be charged with inaction - Ms. Raitt and her department have worked diligently - but that doesn't mean there has been sufficient action." Globe and Mail, A10

*** Inondations - les mesures d'urgence en mode «attente»**
A l'approche du printemps, le gouvernement du Nouveau-Brunswick procédera sous peu au lancement de son programme annuel de surveillance du fleuve. Comme à l'habitude, le mouvement des glaces sera scruté à la loupe par les autorités provinciales qui évalueront les risques d'inondations à partir du 16 mars. «La date du 9 mars avait été évoquée pour procéder au lancement du programme de surveillance du fleuve, mais les températures froides ont fait en sorte de le reporter d'une semaine», a indiqué Paul Bradley, porte-parole de l'Organisation des mesures d'urgence du Nouveau-Brunswick. Difficile pour l'instant de prédire les impacts qu'auront eus les températures froides qui ont touché cet hiver le nord de la province et les importantes chutes de neige enregistrées dans les régions du sud de la province. L'Acadie Nouvelle, 13; Telegraph-Journal

*** Extra run-off not seen as major flood risk**
The Saskatchewan Water Security Agency is projecting above-normal spring run-off for central and east parts of the province, including Regina and Saskatoon. But that doesn't mean this area should expect to see any major flooding events from the run-off. "Even though it's above-normal, we're not saying it's high or extreme or anything like that," John Fahlman, associate executive director of hydrology and groundwater services, said Monday. "We're not expecting it to be as bad as the past few years. There is still a chance that we can get some pretty big rains. Again, this is just the snowmelt aspect of it." A forecast last month projected the spring run-off in the southcentral area ranging from Meadow Lake and Prince Albert to Weyburn as near-normal. But Fahlman explained the revised rating to above-normal is due to the amount of snow that fell in February. The recent snow survey also found more water in the snowpack than previously believed. Leader-Post, A5 (Star-Phoenix)

*** Officials mum on user-pay flood model**
Alberta is borrowing an Ohio conservancy district's engineering innovations to protect Calgary's flood vulnerable communities, but so far it has not adopted the organization's financing model that requires landowners who benefit from massive mitigation projects to bear most of the cost. As the province grapples with declining revenues, Finance Minister Robin Campbell has said new roads may be financed by tolls. But the minister's press secretary would not confirm Monday whether they are also considering a levy on the thousands of homeowners and businesses that would be protected by a planned $310-million Springbank off-stream storage project upstream of the city on the Elbow River. "Many revenue options have been considered and suggested," Kevin Zahara said. "Details on what has been decided in regards to (this project) will be provided when budget 2015 is tabled." In the aftermath of the 2013 floods, provincial officials and their consulting engineers visited the Miami Conservancy District where a series of dry dams and levees was constructed nearly a century ago by the people of the Dayton area in the wake of floods that caused the current equivalent of $2 billion in damages. Calgary Herald, A3

*** Study of aftershocks sheds light on temblor - Hydraulic fracturing suspected as cause of quake near Fox Creek**
University of Calgary researchers have determined they recorded four small aftershocks at the epicentre of a magnitude 4.4 earthquake near Fox Creek that is believed to have been triggered by hydraulic fracturing. The largest aftershock they measured was at a depth that would indicate the Jan. 22 earthquake was induced by human activity, U of C geophysicist David Eaton said Monday. Following the earthquake 33 kilometres west of Fox Creek, Eaton and two other researchers measured four aftershocks with estimated magnitudes ranging between 1.4 and 2.3 on the Richter scale. Such aftershocks are expected following a moderate earthquake, whether induced or naturally occurring, Eaton said Monday. Edmonton Journal, B2 (Calgary Herald)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Terror bill could target activists
A prominent human-rights group says the Conservative government's anti-terrorism bill could be used to target environmental activists and aboriginal protesters. In a brief made public Monday, Amnesty International Canada adds its voice to those who say the bill would go beyond genuine security threats to ensnare those who mount demonstrations that fall outside the strict letter of the law. The Conservatives brought in the bill - which would significantly expand the Canadian Security Intelligence Service's mandate - following the murders of two Canadian soldiers last October. Canadian Press (Cape Breton Post, A9/ Front, Times & Transcript, Telegraph-Journal); Le Devoir; * Toronto Star; * Presse Canadienne (La Voix de l'Est, L'Acadie Nouvelle)

Funding fears cited for CSIS watchdog
Without additional money, the watchdog for Canada's spy service questioned on Monday whether it would be able to sustain its current purview under looming legislation to expand and strengthen the reach of the Canadian Security Intelligence Service. "We would be seeing over time a smaller slice of their activities on a yearly basis," Michael Doucet, executive director of the Security Intelligence Review Committee (SIRC), testified before the Senate's national security committee. The panel is studying the government's proposed Bill C-44, which would amend the 31-year-old CSIS Act by confirming the Federal Court of Canada has jurisdiction to grant surveillance warrants to the agency that have effect outside Canada. That would clarify contradictory Federal Court rulings related to spying by CSIS on Canadians overseas suspected of terrorist activities. It also would give greater protection to CSIS informants. In addition to C-44, the government's contentious Bill C-51 is also moving through Parliament. It would, among other measures, give CSIS power to actively disrupt threats to national security, a significant expansion from its current chief mandate of producing security intelligence for government. Ottawa Citizen, A6

City targets radicalization
It'll be tough for Mayor Denis Coderre to prove that he isn't targeting Muslims with his announcement on Monday that the city will create a "radicalization prevention" centre, a race-relations expert and representatives of Muslim groups said. The city and the Montreal police have created a committee that will set up the centre, the mayor announced at a news conference at city hall with Montreal police chief Marc Parent and representatives of CEGEPs and public schools. The centre, which they called a first in North America, will aim to prevent violence and to develop expertise on the phenomenon of radicalization, notably among youth, Coderre and Parent said. The Gazette, A1; * La Presse (Le Quotidien); Toronto Star; Canadian Press (National Post)

Islamic group claims credit for hacking Bloc website
A group calling itself the United Islamic Cyber Force took credit for a cyber-attack on the Bloc Quebecois website and many other sites Monday. The Bloc's home page was replaced with a paragraph in a red font on a black background under the heading "United Islamic Cyber Force, Salami Ala Aqsha." The message describes an invasion of the Arabian Peninsula and Rome, among other things. "For now there is nothing confirming that it's the Bloc specifically that was targeted," said the Bloc's director of communications, Simon Charbonneau. He added that the Bloc didn't receive any threats that would suggest that the party's

staff members are at risk. The party's IT team replaced the black page with a "site under construction" message shortly after noon. Postmedia News (Ottawa Citizen, C1)

*** Tories stoking fear, prejudice against Muslims, says Trudeau**
Justin Trudeau is accusing the Harper government of deliberately stoking fear and prejudice against Muslim Canadians - employing the same kind of rhetoric that led to some of Canada's most shameful displays of racism in the past. The Liberal leader drew a parallel Monday between the current government's rhetoric about Muslims and other "dark episodes" in Canada's history: the internment of Ukrainian, Japanese and Italian Canadians during the two world wars, the turning away of boatloads of Jewish and Punjabi refugees and the imposition of residential schools for aboriginal children. Since two Canadian soldiers were murdered by men with radical Islamist sympathies last October, Trudeau said the government has been blurring the line between the genuine threat terrorism posed to national security and "simple prejudice." Canadian Press (The Record, A3, Hamilton Spectator, Times Colonist); The Globe and Mail

*** Tories getting bad rap with Muslims**
A senior Conservative senator says the heat her government is getting over its messaging around Islam isn't justified. But Sen. Marjory LeBreton says she does regret the fact it's creating a view among Muslim Canadians that they aren't welcome in the country. LeBreton was placed in the hot seat over the issue by Sheema Khan, one of many women who gathered today at an event to honour the three women running the election campaigns for the federal parties this year. Khan said encouraging her daughters to be involved in politics is difficult when they feel their religion is suspect and their presence not fully welcome. She asked LeBreton whether the government would consider changing its tone. Canadian Press (Cape Breton Post, A9, Times & Transcript); Winnipeg Free Press

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Man may be deported over alleged terror links
Federal immigration officials arrested a Pakistani man in the Toronto area on Monday and are attempting to deport him for alleged connections to terrorism, a government source confirmed. Jhanzab Malik was being held at a local detention centre while the Canada Border Services Agency took steps to have him declared inadmissible to Canada on terrorism-related grounds. His lawyer, Anser Farooq, confirmed Malik had contacted him following his arrest but he had no details. He said Malik had been questioned by the Canadian Security Intelligence Service in the past. He was expected to appear before the Immigration and Refugee Board, possibly on Wednesday, to determine whether he should remain in custody pending his inadmissibility hearing. The CBSA declined to comment. The arrest comes almost five months after another landed immigrant from Pakistan, Mohammed Aqeeq Ansari, was picked up in Toronto following an RCMP investigation called Project Seashell. A hearing to decide whether to deport Ansari concluded last week with Ansari insisting he was innocent and the CBSA claiming he had "long-standing involvement" in terror group Sipah-e Sahaba Pakistan. Postmedia (Ottawa Citizen C1/ Front, Gazette, Vancouver Sun, Windsor Star, Leader-Post, National Post, Star Phoenix,)

Local imam wanted in U.S. on sexual assault charges
A lawyer representing a Calgary imam facing outstanding criminal charges in the United States says there has been a "rush to judgment" against his client that is based on stale, years old warrants. Imam Abdi Hersy, 46, is wanted in connection to sexual assault allegations that surfaced in 2006 when he worked as a respiratory therapist at Woodwinds Health Campus in Woodbury, Minn. Hersy was accused of fondling the breasts of two female patients recovering at the hospital. He subsequently lost his licence and lost his job. Prosecutors in Washington County charged Hersy with six counts of criminal sexual conduct. Hersy claims he was unaware of the allegations until 2009, three years after he arrived in Canada, where he sought refugee status. Hersy claimed his life would be at risk in his home country of Somalia because of his minority status there. His claim was approved by the Refugee Board of Canada in 2008, a decision it tried to repeal five years later. Postmedia (Calgary Herald, A6)

Refugee settles long-running lawsuit against Ottawa

An Algerian refugee who was shipped to the United States one day after the 9/11 terrorist attacks has settled his long-standing lawsuit against the Canadian government. Benamar Benatta fought to be compensated for spending almost five years in U.S. custody in grim conditions and allegedly being beaten by guards. Benatta's lawyer, Paul Champ, says terms of the "mutually satisfactory" settlement are confidential. The arrangement appears to close a little-noted chapter in the story of the Sept. 11, 2001, attacks on New York and Washington. Benatta defected from the Algerian military while on training in the United States. In early September 2001, he made his way to the Canadian border at Fort Erie, Ont., where he told officials he intended to claim refugee status. Canadian Press (Times & Transcript), La Presse Canadienne (La Voix de l'Est 33), Globe and Mail

City cop faces new drug charge

A Windsor police officer previously accused by U.S. authorities of drug smuggling is facing a new drug trafficking charge - this time on the Canadian side of the border. Const. David Bshouty, 32, was arrested by the Windsor Police Service on Monday on a charge of trafficking a controlled substance. The arrest is the latest result of an ongoing internal investigation by WPS into Bshouty. At the time of the arrest on Monday, Bshouty was already on paid suspension stemming from a previous charge of possession of a controlled substance. Police haven't named the substance that Bshouty is now accused of trafficking. On April 12, 2014, Bshouty was arrested by U.S. Homeland Security for allegedly carrying crack cocaine as he attempted to cross the Ambassador Bridge and enter Detroit. U. S. authorities were acting on information provided by Windsor police. However, the stop at the border only turned up three grams of "questionable material" in Bshouty's vehicle. The U.S. charges against Bshouty were eventually dropped when it was determined that the material was, in fact, not cocaine. Postmedia (Windsor Star A2)

Un remboursement de la TPS proposé

Le nombre de touristes états-uniens au Canada continue de chuter, selon le Frontier Duty Free Association. Pour les encourager à remettre le cap au nord, l'organisme propose qu'on leur rembourse le 5 % de taxe sur les produits et services qu'ils se procurent. Depuis 2002, le Canada a vu le nombre de visiteurs provenant des États-Unis diminuer de 23,9 %, d'après les données du FDFA. L'Association calcule que le nombre d'excursionnistes d'un jour au pays est en baisse de 55,9 % et qu'il a reculé de 26 % pour ceux qui passent au moins une nuit au Canada. La force du dollar canadien ces dernières années est au coeur de la réticence de nos voisins du sud à venir visiter le Canada, estime le maire de Cowansville, Arthur Fauteux. Il a constaté lui-même que les Américains sont moins nombreux qu'avant. «On le voit. Ils venaient ici quand notre dollar était en bas de 90 ¢. Ils allaient au Canadian Tire, au Walmart. Ces magasins sont de bons indicateurs parce que les Américains les connaissent bien ; ils achètent des pneus et toutes sortes d'affaires. Mais on ne les voit plus tellement.» La Voix de l'Est, 4/ Front.

Temporary foreign workers cap will hurt B.C.

B.C. will be one of the hardest-hit provinces as a result of the Harper government's reforms to the controversial temporary foreign workers program, says the Canada West Foundation. But the loss of access to lowwage overseas workers will be partly offset for B.C. employers because returning workers from the Alberta oil and gas industry can help fill the void, the thinktank said Monday in a report. The release of the report, which lends weight to Premier Christy Clark's argument that the federal reforms are "tragically misdirected," coincided with the political fallout of a comment by Conservative MP John Williamson. The New Brunswick MP, a former media spokesman for Prime Minister Stephen Harper, apologized after telling a gathering of conservatives that it makes no sense for "whities" to be displaced 3 with "brown people" coming in under the foreign workers program. B.C. New Democratic Party MP Jinny Sims rose in the House of Commons to call the comment "disgusting." The report said B.C. and especially Alberta have been among the heaviest users of the program, mainly to feed the needs of the resource and service sectors, while Ontario and Quebec employers have been least likely to use the program. The report's conclusions are expected to be raised March 26 to 28 by the Canada West Foundation at the Metropolis conference in Vancouver. Postmedia (Vancouver Sun, A5)

Temporary Foreign Worker program changes will hit Sask. Hard

It is a report confirming exactly what the provincial government said last year when the federal government changed the temporary foreign worker program - the new rules won't work for Saskatchewan. Authored by Farahnaz Bandali of the Canada West Foundation, Work interrupted: How federal foreign worker rule changes hurt the West paints a gloomy picture, warning that "the impact of the changes could be severe." "Without enough workers, businesses could be forced to have shorter hours, service will suffer, workers will be stressed and businesses could shrink. Some may be forced out of business altogether," Bandali wrote. In a bitter twist of irony, it's Saskatchewan's exceptionally low unemployment rate - lowest in the country at 4.1 per cent in 2013 - which puts the Land of the Living Skies right in the firing line.During some "boom periods," Bandali told the Leader-Post Monday, temporary foreign workers "became a lifeline for some employers." Without them, "there's not a lot of alternative labour supply, not a lot of other options for employers," so a reduction in those workers will hurt the province. Postmedia (Leader-Post)

Welcome stance on BSE case

In May 2003, the first reported case of mad cow disease in an Alberta-born animal set in motion events that devastated Canada's beef industry. Canadian exports were banned almost immediately in 40 countries, including the U.S. The American response was most crippling, given that 70 per cent of Canada's exported beef lands there. Bovine spongiform encephalopathy (BSE) surfaced again in 2010, 2011 and last month, when a beef cow on a Spruce Grove farm tested positive. So far, the U.S. border has remained open to Canadian beef shipments, and rightly so, since no part of the infected cow reached either the human food chain or animal feed system. Over time, the U.S. government's reaction to outbreaks of BSE in Canada - the latest case is the 19th overall - has been tempered by common sense, research and belief in the industry safeguards that were instituted in the wake of the 2003 disaster. In 2007, Canada imposed new rules on cattle feed formulas to prohibit ingredients that may have transmitted BSE. The government also bolstered tracing mechanisms. Postmedia (Star Phoenix)

Get the state out of my smartphone

An editorial by the executive director of the Canadian Constitutional Foundation states... "While I was shuffling along in an airport security line last week, I had my phone out and was reading about the case of a Quebec man who refused to give his Blackberry password to border agents in Halifax. The traveller, 38-year-old Alain Philippon, was coming home from a trip to the Dominican Republic at the time. He has since been charged with hindering a customs official. And if he is found guilty of the offence, he could spend a year in jail and be fined $25,000. (...)I'm (reluctantly) willing to concede to border agents the ability to rifle through my underwear to make sure I haven't smuggled in an illegal substance, but I'm not willing to allow them the ability to check whether the last thing I Googled before approaching them was a strident libertarian manifesto or cute Tom Hiddleston photos. Or both. Nor do I think Section 8 of the Canadian Charter of Rights and Freedoms is ready to grant border agents that ability either. Section 8 states: "Everyone has the right to be secure against unreasonable search or seizure." When parsing what that means, courts have explained that Canadians have a reasonable expectation of privacy in information that tends to reveal intimate details of their lifestyles and personal choices". Postmedia (National Post)

MP slams colleague for racist comment

A veteran Conservative MP who spent years in outreach with cultural communities is accusing one of his colleagues of undoing the party's gains with "racebased comments." Deepak Obhrai, parliamentary secretary to the foreign affairs minister, lashed out at John Williamson on Twitter. Obhrai, an Indo-Canadian born in Tanzania, was once a key figure in the party's quest to make links with Canada's various cultural communities. "Very disturbed by Williamson's race-based comments," wrote Obhrai, a Calgaryarea MP. "Foolish statement damages all of us. Years of hard work down the drain." Canadian Press (Times Colonist)

*** Feds got the foreign-worker situation wrong**

An editorial by a professor of food distribution and policy at the university of Guelph states... "Rural Canada is expecting a massive exodus of foreign workers, which can potentially become a losing situation for everyone. As of April 1, temporary foreign workers who have been in Canada at least four

years will be forced to leave the country. Since Canadian agriculture employs more than 50,000 foreign workers to support farming and processing facilities across the country, losses to this labour force will be considerable and are really coming at the wrong time. For many commodities, current high prices are making market conditions favourable to more supply. So in essence, agriculture could face a severe, sudden labour shortage. ome groups are pushing for a moratorium and a reprieve. In the past, before rules changed in 2011, foreign workers could simply reapply to continue working in Canada for their employer. The new rule limits working-permit durations to four years. Workers now have to wait four years after their working permit expires to reapply. A number of workers are at risk of leaving Canada after working in the country for more than a decade. Some might suggest that the current situation stems from poor strategic planning. Perhaps, but human capital is a very thorny issue in the agrifood sector. It has always been challenging to attract and retain local talent in agriculture due to seasonality and working conditions. Some have been attracted to agriculture, but regrettably, it is more an exception than the norm." Times Colonist

*** Zeyha sentenced on possession charge**

A Grande Prairie man will serve 18 months of probation and pay a $1,000 fine following a joint submission sentence on a single charge of possessing a substance banned by the Controlled Drugs and Substances Act. The possession charge was in replacement of two CDSA charges originally laid: Importing a banned substance into Canada and possession of a banned substance for the purpose of trafficking. On July 23, 2014, Trenton William Zeyha was arrested by local RCMP in relation to a package containing Oxycodone pills, which were seized by the Canadian Border Services Agency at the Edmonton International Airport. On Monday morning, Grande Prairie Provincial court heard that Zeyha, who turns 40 this month, had fallen into a 'significant addiction issue' and the drugs were solely intended for his own use. The 275 pills were concealed in a package labelled as five 'cross-stitch patterns' and had originated in China. Zeyha was the package's intended recipient. Daily Herald Tribune

*** Stewart, B.C./Hyder, Alaska border closure puts security at risk, says border guard union**

The president of the union representing Canada's border guards says reducing the hours at the Stewart, B.C./Hyder, AK border is a hypocritical move for a federal government that says it places a priority on national security."The government right now is about to pass a bill, C-51, in regards of the concerns that the government has with the terrorists and the people who are going off-seas to get training, and meanwhile they're reducing the hours at the border," said Jean-Pierre Fortin, president of the customs and immigration union. He's been told the reduction in hours at the northwestern B.C. border crossing is one of several such moves being undertaken by the Canadian Border Services Agency (CBSA) in other parts of the country. "There are concerns we have that when you're closing customs or you're reducing the hours you're reducing the security that goes with that," he said. "It's not a matter of traffic, it's a matter of having a presence – defending the first line of defence of this country."Two weeks ago, it was announced that the border which connects the small communities of Hyder, AK and Stewart, B.C. would see its hours reduced beginning April 1 and would be blocked between midnight and 8 a.m. Terrace Standard

*** Toronto's North Koreans face deportation**

Just one North Korean requesting refugee status was granted asylum in Canada in 2014, according to statistics from the Immigration and Refugee Board of Canada. This figure follows a sharp decline over the past two years that has seen the number of North Koreans granted asylum drop from a high of 222 in 2012 to 21 in 2013. Canada has tightened its screening of North Korean refugee applications since it has come to light that most seeking asylum in Canada had first resettled in South Korea following their defection. South Korea not only offers defectors refuge, but claims citizenship over all North Koreans. NOW

*** Focus: Court chides practice of using affidavits by staff**

Refugee lawyers say they won't shy away from filing affidavits from their employees in legal proceedings despite a Federal Court judge's criticism of the practice as he rejected a bid by a failed refugee claimant to defer his deportation to Sri Lanka. Federal Court Justice Peter Annis made his comments in the case of Peter v. Canada (Public Safety and Emergency Preparedness), a judicial review of the Canada Border Services Agency's refusal to postpone Emilian Peter's removal from Canada following his failed refugee

claim. Peter fled his northern Sri Lankan home in 2010, leaving behind his wife and five children to seek asylum in North America. He arrived in Canada in April 2011 via the United States and made a claim for inland refugee protection. A year later, the refugee protection division of the Immigration and Refugee Board of Canada had rejected his claim and by August 2012, he had exhausted all of his appeals. Law Times

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Le Bloc ciblé par des pirates**
Un groupe de pirates islamique soutient s'être attaqué au site Internet du Bloc québécois en raison de la récente prise de position du parti contre le port d'un voile lors des cérémonies de citoyenneté. Le piratage a été revendiqué par un groupe appelé United Islamic Cyber Force, selon le message en anglais qui était visible sur la page d'accueil de la formation politique fédérale. Plusieurs sites hébergés par le même serveur informatique que le Bloc québécois ont été victimes de la même cyberattaque, hier matin. Mais le groupe de pirates, qui a précisé être basé en Albanie, assure que c'était bel et bien le parti qu'il avait dans sa mire. Presse canadienne (Le Droit, 17; La Voix de L'Est); La Presse (La Tribune); Le Devoir; Montreal Gazette (Windsor Star; National Post); Canadian Press (Times and Transcript)

*** CIA sought to hack Apple iPhones from earliest days: The Intercept**
CIA researchers have worked for nearly a decade to break the security protecting Apple phones and tablets, investigative news site The Intercept reported on Tuesday, citing documents obtained from NSA whistleblower Edward Snowden. The report cites top-secret U.S. documents that suggest U.S. government researchers had created a version of XCode, Apple's software application development tool, to create surveillance backdoors into programs distributed on Apple's App Store. It said the latest documents, which covered a period from 2006 to 2013, stop short of proving whether U.S. intelligence researchers had succeeded in breaking Apple's encryption coding, which secures user data and communications. Efforts to break into Apple products by government security researchers started as early as 2006, a year before Apple introduced its first iPhone and continued through the launch of the iPad in 2010 and beyond, The Intercept said. Reuters (Yahoo! News)

*** Hackers attack reporters**
Hackers who attacked a U.S. employee of Ethiopian Satellite Television in 2013 have recently launched a new round of attacks against the broadcaster, an Internet watchdog group said in a report published Monday that links the spyware to the Ethiopian government. Citizen Lab, which is based at the University of Toronto's Munk School of Global Affairs, says the hackers used upgraded espionage software to send out booby-trapped emails in November and December. The broadcaster's general manager, Neamin Zeleke _ one of those targeted by the malicious messages _ says it didn't take a genius to figure out the same actors were at work. "They didn't even bother to change the email address," he said. Associated Press (Cape Breton Post, A11)

*** 'ISIS' hack hits church website - North Douglas Pentecostal one of many targets in reported hoax**
The pastor of North Douglas Pentecostal Church in Saanich says he does not feel threatened after the church's website was hacked by purported supporters of the Islamic State terrorist organization. Rev. Rod Fair said an associate pastor discovered a message reading "Hacked by Islamic State (ISIS) We Are Everywhere" accompanied by an emoticon, Arabic script, music and a banner on top of the website's template. There was also a Facebook address and a flag. The hackers posted their banner over the church website template, so no matter what page visitors tried, the banner was at the top. Times Colonist, A3

LAW ENFORCEMENT / APPLICATION DE LA LOI

OPP union targeted in criminal investigation
Three senior Ontario Provincial Police union officials - one a former Liberal candidate - have stepped aside in the wake of an RCMP criminal probe. The dramatic move Monday followed a raid Friday by the

Mounties, who swooped into the OPP Association headquarters in Barrie with a search warrant. Sources close to the association told the Star that RCMP investigators are examining financial matters at the union. RCMP Const. Jean Juneau said the search warrant has been ordered sealed by an Ontario Superior Court judge. That means details of evidence sought by the Mounties cannot yet be made public. But Juneau emphasized "no charges are imminent" in an investigation that began only recently. He would not comment further on the warrant, saying officers were searching for "evidence that could help in our investigation. We'll see later on if charges are deemed necessary." Association president Jim Christie, vice-president Martin Bain, and chief administrative officer Karl Walsh "have taken voluntary leaves of absence," the union said in a statement. Walsh, who was the provincial Liberal candidate in Barrie during the 2011 election, has been placed on administrative leave by the OPPA's board of directors. "The RCMP is conducting a criminal investigation and believed that evidence to support its investigation could be found in the OPP Association Head Office as well as the offices of president Christie, vice president Bain and CAO Walsh," the OPPA said. Toronto Star, A1; Postmedia News (Ottawa Citizen, C1 Front)

Wallin Jetted Off For Dinner With Ex And You Paid For It, RCMP Says

The RCMP says Pamela Wallin committed fraud and breach of trust by billing the Senate for travel expenses related to her work on corporate boards, with court documents alleging she described an echocardiogram as networking and a meeting with an ex-lover as parliamentary business. According to the RCMP documents released by an Ottawa courthouse Monday, the ongoing police investigation into Wallin's travel expenses involves 150 "suspicious" travel expense claims filed over three years, including 24 trips to Toronto for board-related activities. The documents - filed by the RCMP to obtain more information about Wallin's expense claims - detail $27,493 worth of allegedly fraudulent expense claims the suspended Conservative senator from Saskatchewan made for travel related to her former role as a director on the boards of Porter Airlines Inc. and Gluskin Sheff + Associates Inc. Wallin, who has repaid $154,191 in expense claims, including interest, has not been charged and none of these allegations has been proven in court. Her lawyer said Monday any expenses claimed for travel related to her board activities were done erroneously. RCMP Cpl. Rudy Exantus alleges in the documents that when confronted about these travel expenses - which would have been covered by the corporate boards as part of her compensation package - Wallin "misrepresented the nature of these trips to Toronto" during an external audit conducted by Deloitte, at times even "fabricating meetings which the RCMP was able to determine (through interviews) to have never taken place." Toronto Star, A1; Canadian Press (Waterloo Record, A1, National Post, A1, Leader-Post, A1, Red Deer Advocate, The Guardian, Times Colonist); Postmedia News (Ottawa Citizen, A1, Montreal Gazette , Vancouver Sun, Edmonton Journal, Windsor Star, The Province, Calgary Herald, Leader-Post); Presse Canadienne (L'Acadie Nouvelle, La Voix de L'Est); * Le Devoir; * Globe and Mail, A3

Petition aims to save A'burg police

Amherstburg council received a petition Monday bearing the signatures of more than 1,000 residents who want to keep the town's local police force. Lifelong resident Darlene Meloche, accompanied by her husband Kevin Meloche, appeared before council Monday to formally deliver the list of those opposing the idea of a regional force developed in conjunction with Windsor and LaSalle. "It's not that we hate the other police departments, it's not that at all," Darlene Meloche said. "We're just trying to keep stuff local. We're just trying to run our own little town." The petition had 1,010 signatures when it was originally submitted for consideration last week. Since then, Darlene said the total grew by another 155 signatures. "I'm going right through to the fall," she said of a campaign to save the force of 31 officers. "If we can get a thousand signatures in the worst February ever, imagine how many we can get when the weather turns nice?" Windsor Star

Answers to Church Avenue explosion could take months, RCMP say

Despite having happened a couple of weeks ago, the full details of an explosion and fire that sent two to hospital and left a family of four without a home remains a mystery. The explosion at 123 Church Ave., in Sussex happened late in the night of Friday, Feb. 20. RCMP, with the help of RCMP clandestine lab experts, were investigating the possibility of the explosion being linked to the production of illegal drugs, Sussex RCMP Sgt. Dale Morgan said. "We have to wait for results from our lab before we decide what charges will be laid. It could take a couple of months," Morgan said. Police were investigating reports of suspicious activity near the apartment building immediately after the explosion. The family that lived in the

apartment beside the one where the explosion happened has been given emergency lodging, food, clothing and other items from Canadian Red Cross. Telegraph-Journal, B5

Jogger attacked in park was sexually assaulted
The woman who was attacked while jogging near Glen Lake Park last week was sexually assaulted, say West Shore RCMP. Police continue to look for the attacker. "As the investigation progressed, evidence suggested a sexual assault took place," said West Shore RCMP spokesman Const. Alex Berube. The 23-year-old woman was jogging on a trail near Shoreview Drive on March 3 around 7 p.m. when a man asked her for the time. The woman was knocked unconscious and robbed of her cellphone and money, police said. When she regained consciousness, she ran to a home to call 911. West Shore RCMP have not said why there was a delay in confirming that the woman was sexually assaulted. She is being assisted by victims' services. West Shore RCMP major crime detectives and Island district RCMP forensic identification officers continue to investigate. Times Colonist, A3

RCMP crisis teams assist with P.E.I. gun incident
RCMP emergency response teams, a crisis negotiation team, and police dog services from New Brunswick aided its counterparts on P.E.I. for a gun scare incident early Saturday morning. East Prince RCMP were called to a firearms complaint shortly before 1 a.m. in a residence on Route 119 Fernwood Road in Fernwood, according to a police news release. As a result of the initial response, the teams from the province, along with an ERT unit on P.E.I., were called into assist East Prince RCMP with the investigation. The 23-year-old male suspect was arrested around 9:30 a.m. without incident and remains in RCMP custody. Sgt. Leanne Butler, media relations officer for the P.E.I. RCMP, said charges will be laid within 24 hours of the arrest, so there will be an update on the case tomorrow. "The ERT have completed their tasks and they are no longer here," she said on Saturday afternoon. "The East Prince detachment are continuing the investigation." Butler said the New Brunswick teams often supplement the P.E.I. units in such emergency calls. There were no injuries stemming from the incident, and Butler said she cannot say whether there were others in the residence at the time of the standoff. Times & Transcript, A10)

Show us entire video
An editorial states, "Canadians should have seen the video made by Michael Zehaf-Bibeau months ago. Even now, astoundingly, the RCMP won't show us the whole thing. Commissioner Bob Paulson had better have a sound investigative or ethical reason for censoring the video, because Canadians have been treated like children long enough. Paulson said 18 seconds had been edited out, for "operational" reasons he would not disclose. Presumably, if the reasons truly are "operational," we'll be able to see the edited parts eventually. In the video, Zehaf-Bibeau says that his actions are "in retaliation for Afghanistan and because Harper wants to send his troops to Iraq." He includes himself among the "mujahedeen of this world." He rambles about Canadian society, although he was born and raised in this country: "It's a disgrace you guys have forgotten God and have you let (sic) every indecency and things running your land. We don't, we don't go for this." In other words, vague Islamist boilerplate. The long wait, the dramatic buildup and the mysterious edits imbued this video with political significance it would not have had if the RCMP had simply shown it to Canadians in the days after the attack. This is convenient for the government, which uses the Oct. 22 attack as a justification for its terrorism legislation..." Postmedia News (Leader-Post, A6)

The erosion of our right to protest
An editorial states, "It is one thing to disagree with one's government. It is another to fear it. Here, in the world's most polite nation, we aren't used to looking over our shoulder at government. The history of the public's relationship with our federal governments has long been characterized by the usual ire we reserve for bureaucracy. We have always trusted it to do the wrong thing. But fear? That's something new. Maybe in B.C. we've had more reason to feel that unease. The demonizing of opponents to its pipeline plans, the use of its ministries to chill the campaigns of environmentalists - we've seen the worst of the Conservatives' heavy-handedness. But more troubling is the government's erosion of the boundary between protest and terrorism... Maybe, but maybe not. Critical infrastructure has been on the mind of the RCMP, too - most vividly in the RCMP memo Critical Infrastructure Intelligence Assessment: Criminal Threats to the Canadian Petroleum Industry. The document was dated Jan. 24, 2014. Obtained by

Greenpeace Canada and leaked to the Quebec newspaper La Presse in mid-February, the RCMP paper was "in support of the Government of Canada's strategy to ensure critical infrastructure." It all but predicted armed insurrection against Big Oil. (Sorry, my mistake. It did.) Some key passages: "There is a growing, highly organized and well-financed, anti-Canadian petroleum movement, that consists of peaceful activists, militants and violent extremists, who are opposed to society's reliance on fossil fuels." "Research and analysis done in support of ongoing RCMP criminal investigations shows those involved in the anti-Canadian petroleum movement have an interest in drawing public attention to, and in building recognition of, the perceived (italics mine) environmental threat from the continued use of fossil fuels."... " Vancouver Sun

Denial won't make the T-word go away
An editorial states, "Some people are allergic to the T-word. After a lone gunman stormed Parliament Hill last fall, killing a soldier at the National War Memorial, they said it was not possible to conclude that this was terrorism. More likely, the guy just had mental problems. "I think that we're not in the presence of a terrorist act in the sense that we would understand it," said NDP Leader Thomas Mulcair. "I don't think we have enough evidence to use that word." In the Vancouver Sun, Ian Mulgrew argued that Michael ZehafBibeau was no terrorist. He was a victim. "The vast amount of tax money devoted to his petty crimes would have been far better spent providing him with appropriate psychiatric and social care," he wrote. As for the two people who plotted to bomb the B.C. Legislature, "They, too, seem more sad sack than Satanic." Now we know better. Mr. Zehaf-Bibeau's self-made martyrdom video, released by the RCMP last week, is chillingly clear about his motives. "This is in retaliation for Afghanistan and because Harper wants to send his troops to Iraq," he said... Maybe so, but they are missing an important point. The moose does not want to become a martyr for the caliphate. A disturbing number of young Westerners do. The number of extremists is growing across Canada, according to RCMP Commissioner Bob Paulson. So far, we've done a pretty good job of catching the stupid ones. I only hope we catch the smart ones, too. We shouldn't be spooked by terror threats. But we shouldn't be in denial that they're real." Globe and Mail, A11

* **Supt. Paul Cook named Calgary police chief until Hanson's replacement hired**
Paul Cook, a superintendent and 25-year veteran of Calgary Police Service, will serve as interim chief once Rick Hanson resigns on Friday. The fact the Calgary police commission had to select the interim chief from the superintendent ranks - the third-highest tier of command - signals that all three deputy chiefs will vie to be Hanson's permanent replacement. Cook, who used to work with the police canine unit, currently serves as executive officer to Hanson. As interim boss, he'll offer continuity while the commission and a headhunting firm conduct an international search for a new chief, said Coun. Diane Colley-Urquhart, a longtime police commissioner. The police commission will select the next chief. Council only rubber-stamps the decision, as it did with the oversight body's choice of an interim department head. "He knows how the executive suite works, he is connected to the members, and he is an exceptionally accomplished senior officer and respected leader," chairman Rodney Fong said about Cook, in a statement. Calgary Herald

* **Digby awaits RCMP review of policing levels**
The town of Digby is waiting for an RCMP review of its policing levels. "It's just part of an overall review the town is looking at," Mayor Ben Cleveland said. "We're looking at all of our services that we provide to taxpayers to see whether or not we're getting fair bang for our buck." Cleveland said he thinks the community is happy with policing levels in the town, and council doesn't have any issues either. "We've had a contract with the RCMP for about 30 years now, and we're certainly satisfied with that. But dollars are tight, so we'll look at it, and if staffing levels need to stay the same, that's great. If we can offer good service at another level, then we'll look at it." Staff Sgt. Rocky Calhoun of Digby District RCMP said the issue of adequate staffing does come up from municipal councils, and he's fine with the review taking place. "Then we can move forward from there." Calhoun said there are 12 officers besides him working out the Digby office, which covers the town and Municipality of the District of Digby. The municipality has also requested the review, as has the Municipality of the District of Clare, which is partly in Digby County but policed by Meteghan RCMP. Chronicle Herald, A8

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Long line of support for Khadr's bail bid**

Professors, doctors, businessmen and even a former senior member of the U.S. military have put their names - and reputations - on the line to support the bail application of a man the Canadian government and other detractors have branded a dangerous jihadi terrorist. Foremost among those backing Omar Khadr are his longtime lawyer Dennis Edney and his wife Patricia, who have offered to take him into their home if he wins bail. "I just think he's an extraordinary young man," Patricia Edney, a manager with Alberta Health Services, said in an interview from Edmonton. "We see him as more than a client: We see him as somebody who's been abandoned by his government and suffered greatly for it." Edney, who has met the Toronto-born Khadr in prison, says she finds him gentle, articulate and gracious. Khadr's application for bail - to be heard over two days later this month by Court of Queen's Bench - aims to get him out of Bowden Institution in Innisfail while he appeals his conviction on five war-crimes charges by a U.S. military commission for incidents that occurred in Afghanistan when he was 15 years old. He pleaded guilty in 2010 to murder in violation of the law of war in the death of an American special forces soldier, attempted murder, conspiracy, spying and providing material support to terrorism as part of a deal to be repatriated to Canada from Guantanamo Bay. Despite the backing of numerous legal experts and even rulings from U.S. courts, the commission appeal court has so far put his case on hold, raising the possibility that Khadr, 28, won't get a hearing before his eight-year sentence runs out - in October 2018. Canadian Press (Edmonton Journal, A8, Waterloo Region Record, Whitehorse Daily Star, Globe and Mail, Le Devoir)

Inmate gets 7 years

An inmate at Kent Institution in Agassiz has been sentenced to an additional seven years for slashing a female corrections officer across the face and neck. Kevin Beaulieu pleaded guilty last month to aggravated assault for the unprovoked attack in June 2012. Court heard that Beaulieu walked up to Charmaine Weiss, asked her to explain something and, when she looked down, used a razor blade to slash her across the face. Weiss was transported to hospital where she underwent a three-hour surgery. B.C. Supreme Court Judge Murray Block sentenced Beaulieu, who is already serving a 7½-year term, to an additional seven years. Canadian Press (The Province, A4, Times Colonist, Vancouver Sun, 24Hrs Vancouver)

Litany of disgrace

A letter to the editor states, “It was obvious long ago things were terribly, desperately wrong with Canada's prisons, specifically in regard to the use of solitary confinement ('We Can Only Do So Much As An Institution' - March 6). But this story about what happened to Edward Snowshoe adds to the litany of disgrace. In addition to the long list of failures due to bureaucratic bungling, laziness and sheer ignorance, the fact a health-care professional should have to conduct an assessment through a "food slot" is as grotesque today as something from the Middle Ages. And that a parole officer should have to be concerned about being "perceived as a con lover" by the guards shows the tail is wagging the dog in regard to prison management. Guards are employees and required to follow the orders of management, like all other employees. Their feelings about their job should not come between them and their duties.” Globe and Mail, A10

Accused killer vouched for himself

The voice on the phone is hesitant but straining for helpfulness, just wants to help cops out. That "Mark" fellow, the one who's on the front page of Toronto newspapers, charged with four murders? "A good friend of mine," the caller tells the Crime Stoppers hotline tips-taker. "I know that that person did not do those murders. That guy they arrested for those murders is not the guy that did the murders." Indeed, the man continues, "I heard through the grapevine who did those murders, right?" There were two shooters, one with the nickname Slinky and the other known as Reds. Not this "Mark" dude at all. Cops got it all wrong. "He's not that type of guy who do something like that ... 'cause he's a really, really nice guy. Like I know it's not him, almost put my life on it that it's not him." The suspect charged by police with four counts of first-degree murder was Mark Moore. And the guy on the line is ... none other than Mark Moore, giving himself an exculpatory character reference. That Oct. 21, 2011, call was made from the phone range at the Don Jail, captured on a police intercept and played for the jury Monday at Moore's trial for first-degree

murder times four. Even the defendant in the dock grinned when the audiotape started unspooling in court. Oops. The caller had identified himself as Christopher Parker. Toronto Star, A2; * Postmedia News (Vancouver Sun, National Post, Edmonton Journal, Windsor Star, Montreal Gazette, StarPhoenix, Leader-Post, Calgary Herald, Ottawa Citizen), * CBC News

*** Gladue report sought for violent man**

The defence lawyer for a man awaiting sentencing on two significant assaults is looking into whether a "Gladue" report might be a possibility. Richard Daniel Wolfe pleaded guilty on Monday at Regina Court of Queen's Bench to sexual assault and assault with a weapon in relation to an incident from April 6, 2014, in Fort Qu'Appelle. After pleas were entered and brief facts heard, defence lawyer Kim Stinson told Justice Lian Schwann he intends to ask that a Gladue report ordered that would examineelements of Wolfe's First Nations background that might have helped contribute to his offending. While Gladue factors have been canvassed in the past as part of pre-sentence reports, stand-alone Gladue reports are relatively new for offenders in this province. Because of that, there was uncertainty on Monday as to how to go about ordering the report, which is expected to take at least a couple of months to prepare. The case was set over to March 26 so Stinson can look further into the matter. A date for sentencing has yet to be determined. At 39 years of age, Wolfe is no stranger to the courts, nor to violence. One of the founders of the Indian Posse street gang (along with his brother Daniel Richard Wolfe, who was killed in prison three years ago), Wolfe, in 1996, received close to two decades in prison for attempted murder, robbery and a weapons offence from Winnipeg. While in prison on those charges, Wolfe added to his record with convictions for assault causing bodily harm and disguise with intent, resulting in a further two-year term. It was while Wolfe was out on statutory release that he committed the latest offences, which took place early in the morning of April 6. Court heard that a woman had been drinking at a Fort Qu'Appelle house with a number of people, including Wolfe, and had eventually gone to the bedroom to sleep. Leader-Post, A4

*** Sex offender agrees to conditions prior to release**

Convicted sex offender Brian Keith Solberg told the court he welcomes the range of strict conditions placed on him as he prepares to return to the community this week. "I agree to them (the conditions) very much ...," the 64-year-old told Regina Provincial Court Judge Bruce Henning on Monday. "It gives me some good structure and it will help me behave myself." Solberg is considered a high risk to reoffend, leading the Crown to apply for a two-year recognizance that imposes hefty conditions on his freedom once his most recent sentence comes to an end on Wednesday. (...)The sentence that is expiring is a two-year term imposed in March 2013 after Solberg pleaded guilty to breaching his recognizance - one similar to the one he is about to be released on - by driving through an area of Regina known to be frequented by sex-trade workers. Solberg asked for and received the maximum two years for that offence, stating he wanted to go to the federal penitentiary to take cognitive and sex offender programming. Solberg's criminal history includes a number of sex offences, the most recent earning him a 10-year sentence for a brutal attack on a woman in British Columbia. That sentence ended in 2004 and Solberg has been on various forms of release conditions since then. While Solberg hasn't been charged with further sex offences since his release from prison on the B.C. conviction, he has landed back in custody a number of times for breaching court-ordered conditions. Leader-Post, A4

*** Lifers law a new kind of extremism**

An editorial states, “Prime Minister Stephen Harper is selling his proposed "life means life" law, the details of which are to be made public this week, on the fear ticket - insisting he is correcting flaws in the Criminal Code that will spring those who commit heinous crimes from prison early, where they can walk unchecked on the streets and threaten the safety of ordinary Canadians. Independent courts give any Canadian accused or convicted of crime faith they will be treated impartially under the law. Mr. Harper's proposed law would overturn that cornerstone of the justice system. The only hope that lifers would have of getting out of prison is by an appeal to the federal cabinet. That's a hope so faint as to be cruel. Contrary to some belief, when a Canadian gets life, they are never released from their sentence. If released from prison after 25 years (two-thirds of those on a life sentence are behind bars), the individual is on parole for the rest of their life. Slipping up on the terms of release or the commission of another crime lands them behind bars again. The rate of reoffending is very low for the one-third of first-degree murderers released to the community, notes Howard Sapers, Canada's correctional investigator.” Winnipeg Free Press, A6

*** Harper aims to bait Supreme Court**
An opinion piece states, "Between an imperious federal government and a runaway Supreme Court, we are headed for a legal and constitutional imbroglio. The Harper government, it is widely observed, has taken with increasing frequency, if not glee, to stuffing the bills it presents in Parliament with measures that are in self-evident violation of the constitution. Not only is the government making no apparent effort to "charter-proof" legislation, that is by seeking the advice of Justice department lawyers on its constitutionality in advance of its introduction, as it is required by law to do, it seems if anything to be taking advice on how to offend it. It is impossible to read the several dubious provisions of Bill C-51, the Conservatives' anti-terrorism legislation - allowing the police to detain people on suspicion an act of terrorism "may" be about to occur; permitting intelligence officers to break the law, bizarrely, with the permission of a judge; banning the promotion of terrorism "in general" - in anything but this light. Still more blatant is the bill, still to be introduced but already popularly known as the Throw Away the Key Law, requiring those convicted of certain crimes to be jailed until they are dead, without chance of parole. The inclusion of a right to appeal for clemency to the Minister of Public Safety after 35 years, supposedly in response to "legitimate constitutional concerns," must be regarded as something of a flip of the finger in the direction of the Supreme Court. How they must have laughed in the Prime Minister's Office as they drafted it. But if the government has seemed to go out of its way of late to insert rights violations in legislation, the court has seemed equally determined, in its recent decisions, to find violations of rights that aren't there. The issue, as I've written before, isn't that the court has been overturning laws with greater frequency, or to more radical effect. If the legislation under challenge plainly contradicts the constitution, that is its job - the job Parliament assigned it to do. Rather, it is the shoddy reasoning, the slapdash approach to precedent, the curiously selective research, that has many legal scholars, not necessarily given to court-bashing, raising the alarm." Postmedia News (Vancouver Sun, B7, Edmonton Journal, Windsor Star, StarPhoenix, Montreal Gazette, Leader-Post, Calgary Herald, Ottawa Citizen)

*** Good reasons for life sentences**
A letter to the editor states, "Re: Difficult to see what is accomplished by 'life', March 5. Columnist Andrew Coyne seems to have difficulty seeing what is accomplished by keeping murderers, rapists and terrorists in jail for life (until they die). When the Liberals abolished the death penalty, 72 per cent of Canadians were opposed to eliminating it. The Liberals assured Canadians that these people would spend the rest of their lives in prison. What good does it do to keep people in jail for real life? There are several good reasons: They will not get the chance to reoffend; people who have lost a loved one will get a better measure of "justice" (call it revenge if you will); and criminals will reconsider doing the crime if they really have to do the time. Some penalties given out now are a joke." Ottawa Citizen, C3

*** Open the prison door on entry and on death**
A letter to the editor states, "Kudos to Harper for life-means-life law (March 7) In defence of Harper's life-means-life law, I do not feel that the writer went far enough with his opinion. At one time Canada's laws upheld the death penalty for capital crimes such as murder, treason, etc., then along came Liberal prime ministers who changed it all. The new law abolished the death penalty except for the killing of police or corrections officers who were murdered in performance of their duties, and no one has been executed in Canada since the change. How many law enforcement officers have been murdered in the line of duty, not to mention other citizens, particularly children and the elderly?" Hamilton Spectator, A12

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Judge doesn't buy tale of biker's bounty
The federal government has won a major legal battle against the former president of the Manitoba Hells Angels over property seized under proceeds-of-crime legislation. Court of Queen's Bench Justice Rick Saull ruled Monday five items were legally taken from Dale Sweeney following his 2012 arrest in Winnipeg. They include a Harley-Davidson motorcycle, a Corvette, a Silverado, a boat and a trailer. One of Sweeney's friends had stepped forward and claimed he was the rightful owner of that property and should have it returned immediately. He filed a motion stating he purchased the items, with cash, without

any influence from Sweeney. "That simply doesn't hold any water," Saull said Monday. Several days of trial were held, including evidence from the man and investigating officers, along with an examination of financial records. Winnipeg Free Press

*** Men are victims, too: CAFE group**

Calling the Ontario government's campaign against sexual violence "sexist," a men's issues group unveiled a new billboard in downtown Toronto Monday in an attempt to draw attention to male victims of domestic abuse. "HALF of domestic violence victims are men," reads the billboard, paid for by the Canadian Association for Equality (CAFE). "NO domestic violence shelters are dedicated to us." The billboard comes after Ontario Premier Kathleen Wynne released a three-year, $41-million plan to combat sexual violence last week. The campaign, spurred in part by the high-profile sex assault allegations against Jian Ghomeshi, includes a video ad with staggering scenes of women being sexually assaulted and harassed. In a news release Monday, CAFE accused Premier Wynne of forgetting "half the victims of violence." "Premier Kathleen Wynne's violence against women initiative reinforces sexist stereotypes that ignore violence against men, gays and lesbians, and endanger children with abusive mothers," the statement reads. But declaring that men make up half of domestic violence victims risks oversimplifying a complex set of statistics, as one women's advocate noted. "If service providers were finding that there was such a need for men's shelters, there would be men's shelters," said Penny Krowitz, executive director of Act to End Violence Against Women. "If we had enough men coming forward saying, 'I need shelter from this abusive woman' or 'I need shelter from this situation,' do you not think that we would have provided those services to men?" Statistics CanadaA graph from a 2014 Centre for Justice Statistics report showing the victims of police reported intimate partner violence in Canada in 2013 (by gender and age). In backing up its claim, CAFE cites a 2009 Statistics Canada survey that found an estimated 601,000 Canadian women and 585,000 men experienced spousal violence. That study, however, also notes that women are twice as likely to be physically injured during spousal abuse than men; and almost seven times as likely to fear for their lives. National Post, A3

*** Indigenous men dealing with violence want more resources in Quebec**

Martin Hervieux, an Innu man from Pessamit, Quebec, wishes resources would have had existed for his father decades ago when his violent behaviour dominated their family life. "I would have liked it if a house for men had been accessible to my father when I was young. He was beating my mom," said Hervieux, 59. "Also, I could have used help later in my life." Hervieux is now part of the Napeuat (men's) Committee and is among a small but growing number of men involved in efforts to address family violence in Quebec's aboriginal communities. When the Napeuat Committee decided three years ago it was time to build an indigenous men's shelter, to provide a haven and support for violent men, they turned to the Women's Shelter Network for guidance. (...)But Quebec has the dubious distinction of lagging far behind other provinces and territories, in terms of providing services to aboriginal men; this, according to criminologist and professor Renée Brassard from Laval University. "We are in a punitive system," she says, "no crime, no services for men." Brassard will publish a new study in spring 2015. She and her research team met with several First Nations and Inuit men of Quebec in prison. CBC News

*** Men vital to anti-violence awareness, intervention**

The Regina Sexual Assault Centre wants to partner with local sports teams to increase awareness about violence against women, and it's hoping the Saskatchewan Roughriders will get on board. At the centre's 40th anniversary breakfast on Monday, attendees learned about the Be More Than a Bystander campaign. A partnership between Ending Violence Association of B.C. and the B.C. Lions, it has players use their public profile to raise awareness about violence against women and encourage other men to speak out. "I think it would be absolutely awesome to bring that here," said Debbie House, the sexual assault centre's administrator. She said the person-power needed to get it up and running, though, would be "challenging" for the organization and, "would be much easier if we had the Riders on board and we hope that that can happen." The B.C. campaign involves public service announcements featuring Lions players, a provincewide school education program delivered by players, a training program for amateur football coaches, and a film. "What we're trying to do is make it cool to respect women and girls," said Tracy Porteous, executive director of the Ending Violence Association of B.C. While she said that public awareness of violence against women has increased, "what's been missing until recently is the

interventions by men." Jamie Taras, director of community relations with the Lions, said, "It's tremendous to me how the kids have embraced this topic." Leader-Post, A3

*** Districts say bullying stats show greater awareness**

School superintendents say greater awareness and the fact that kids are more willing to blow the whistle on bullies are among the reasons for the high numbers of bullying cases revealed in newly released statistics. Officials in New Brunswick school districts reacted on Monday to concerns raised by an anti-bullying organization that has released numbers indicating that kids tormenting kids remains a significant problem in many of the province's schools. The statistics for the last school year obtained by Bullying Canada Inc. through a right to information request show that hundreds of cases of taunting, intimidation, cyberbullying and physical bullying were documented in the school districts. One district, Anglophone West, had 904 reported cases of bullying in the 2013-14 school year and just under 180 suspensions. The Anglophone South School District had 704 cases and 123 suspensions. David McTimoney, superintendent of Anglophone West, said the numbers released by Bullying Canada do not paint an accurate picture of what is happening in the province's schools. He said there are other surveys and reports that make it clear most students feel safe in the province's school system. Times & Transcript, B1 (Daily Gleaner, Telegraph-Journal)

*** Parents need help to address bullying**

An editorial states, "Depending on your point of view, the statistics are either encouraging or exasperating. Either way, the bullying numbers from schools around the province are enough to make a parent cringe. In the Anglophone West School District, for example, there were 904 reported cases of bullying in 2013-14, leading to 179 suspensions. What the suspensions number adds up to over the course of an academic year is, on average, one student being suspended every day the schools are open. A single elementary school in Perth Andover had 212 bullying incidents reported, well more than one a day on average. A middle school in the Fredericton area had 103 bullying reports. Our neighbours in the Anglophone South School District didn't have much to brag about with 704 reports and 123 suspensions. How students fared in the Anglophone East School District is anyone's guess. District Supt. Gregg Ingersoll says it doesn't keep a record of bullying statistics, a strange choice given the Education Act stipulates principals are required to report all bullying incidents to their district's superintendent." Daily Gleaner, A6

*** Parsons' father speaks at UN about cyberbullying**

The father of Rehtaeh Parsons says he delivered a statement to the United Nations on Monday, telling the commission on the status of women how his daughter's death after a suicide attempt in 2013 was directly related to cyberbullying. Glen Canning confirmed in an email that he delivered the statement during a panel discussion entitled Violence in the Digital Age. Parsons' family says the girl was 15 years old when she was sexually assaulted in November 2011 and bullied for months after a digital photo of the alleged assault was passed around her school in Cole Harbour. In his prepared statement, which appears on his website, Canning says he and the girl's mother have been advocating for victims of sexual assault and cybercrime, roles that have led to the realization that their daughter's case is far from unique. The statement says that for many women and teenagers suffering from online abuse, reporting such incidents can be heartbreaking and the results are often futile. Canadian Press (Chronicle-Herald, A6, Cape Breton Post, Globe and Mail, Brandon Sun, Western Star, Truro Daily)

*** Plan to boost police brass slammed**

A councillor is questioning a shuffle of Halifax Regional Police top brass that will see the force's senior ranks swell. Under a reorganization in the works, the municipality's police force is set to grow from nine managers - a chief of police, deputy chief and seven superintendents - to 13 - a chief, deputy chief, three superintendents and eights inspectors. Although that's an increase of four positions, only two are new, while two are vacancies set to be filled. But Coun. Steve Adams (Spryfield-Sambro Loop-Prospect Road) said Monday that any wiggle room in the budget should go toward fighting cybercrime, not hiring more managers. "In this day and age, I can't justify more management positions," said Adams, who is also on the Halifax Board of Police Commissioners. Chronicle-Herald, A6

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER

Le sergent Doiron «avait le coeur à la bonne place»
Combattre le terrorisme était un objectif de longue date pour le sergent Andrew Joseph Doiron. Un de ses anciens enseignants à l'école secondaire Mathieu-Martin de Dieppe se souvient de lui comme d'un «gars avec le coeur à la bonne place». «On se reverra dans quelques mois», voilà les derniers mots que le sergent Doiron a dit à Bernard Melanson, la journée même où il s'est envolé pour l'Irak. Enseignant à l'école secondaire Mathieu-Martin depuis plus de 23 ans, il a vu passer beaucoup d'élèves dans sa classe de physique. M. Melanson se souvient particulièrement du passage d'Andrew Doiron. L'Acadie Nouvelle, 3/Front

Iraq mission extension likely
The deployment of more Special Forces advisers to Iraq is being considered as the federal government weighs its options to continue Canada's contribution to the Iraq war. Military officers say they fully expect the government to extend the Iraq mission. The expansion of the Special Forces training contribution makes the most sense, they added. What is unclear at this point is the effect of the recent friendly fire death of a Canadian Special Forces soldier, Sgt. Andrew Doiron, on the government's plans. Foreign Affairs Minister Rob Nicholson said last week Canada would be in Iraq for the long term, even though the government hasn't officially announced an extension to the mission yet. Postmedia News (Ottawa Citizen, A1, The Vancouver Sun); * The Record; * Ottawa Citizen

* **État islamique**
Le nouveau ministre de la Défense a publié sur Twitter des photos mettant en scène des femmes enchaînées et une fillette censément mariée de force qu'il a faussement associées au groupe armé État islamique (ÉI) - et utilisé pour mousser la mission militaire du Canada en Irak. Dans le message qui accompagnait les trois photos, Jason Kenney félicitait les troupes canadiennes pour leur lutte contre l'ÉI et ses velléités de réduire les femmes à l'esclavagisme. Il souhaitait ainsi souligner la Journée internationale des droits des femmes. Les images publiées sur le fil de M. Kenney sont cependant trompeuses, comme l'a fait remarquer lundi Mohamed Ourya, chercheur associé à l'Observatoire sur le Moyen-Orient et l'Afrique du Nord de la Chaire Raoul-Dandurand de l'UQAM. Presse Canadienne (L'Acadie Nouvelle, 20); Ottawa Citizen

* **Fahmy in legal limbo after retrial postponed**
An Egyptian court postponed proceedings in the retrial of two Al Jazeera English journalists after key prosecution witnesses failed to appear at a session where they had been slated for cross-examination on Sunday. Defence lawyers for Canadian journalist Mohamed Fahmy and Egyptian producer Baher Mohamed had expected on Sunday to cross-examine the security officers whose testimony is central to the prosecution's case against the journalists. "It's unprecedented legal limbo," Mr. Fahmy told journalists after he emerged from the the courtroom inside Cairo's Tora Prison complex. This is the second time the prosecution's witnesses have failed to attend the retrial, the latest in a prolonged judicial ordeal for the two journalists as well as five students and an NGO worker swept up in the same case. "We come here and we respect the court. It's very unusual that the witnesses don't come twice in a row. I see it as an insult to the judiciary here," Mr. Fahmy said. Judge Hassan Farid demanded that the missing officers attend the next session of the trial "even if I have to arrest them." He also fined two of the witnesses the equivalent of $80. A note of exasperation in his voice, the judge adjourned the trial until March 19, after a session lasting less than 15 minutes. The Canadian government said on Sunday that Ottawa would continue to call for Mr. Fahmy's immediate release. Globe and Mail, A4

INTERNATIONAL

Minister suggests new devil's island in France
Dangerous jihadists should be kept on an island to stop them spreading extremism, a former French interior minister has suggested, amid warnings up to 10,000 Europeans could be waging jihad in Iraq and

Syria by the end of this year. Charles Pasqua, 88, made the controversial suggestion in response to government plans to "isolate" dangerous Islamists in French jails to stop them becoming a breeding ground for radicals. Asked during a radio interview whether that meant creating a "French Guantanamo," he replied, "We should put them on an island, and that means putting them somewhere far away. I don't see why we don't reinstate forced labour." France has a history of placing criminals on island prisons - Devil's Island off French Guiana was the most notorious lockup. Daily Telegraph (National Post, A12)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
May 8, 2015 / le 8 mai 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

'Mr. Khadr, you're free to go': judge
After spending more than a decade in prison, Omar Khadr says he'll show Canadians - and Prime Minister Stephen Harper - that he's worthy of their trust. Speaking publicly for the first time since his release on bail, the former Guantanamo Bay inmate thanked Canadians on Thursday for giving him a chance. "I will prove to them that I'm more than what they thought of me, I'll prove to them that I'm a good person," he said outside his lawyer's home. "Give me a chance, see who I am as a person not as a name, and then they can make their own judgment after that." As for the prime minister, whose government has consistently branded him an unrepentant terrorist, Khadr said: "I'm better than the person he thinks I am." The 28-year-old had his first taste of freedom in almost 13 years earlier in the day after an Alberta judge rejected a last-ditch attempt by the federal government to block his release. Supporters in the courtroom gasped in joy and Khadr smiled broadly as Appeal Court Justice Myra Bielby delivered her decision. (…) The government, which said it would fight his release every step of the way, expressed disappointment at the latest turn of events. "***(We) regret that a convicted terrorist has been allowed back into Canadian society without having served his full sentence***," **Jeremy Laurin, a spokesperson for Public Safety Minister Steven Blaney**, said in a statement. Canadian Press (The Record, A1, Chronicle-Herald, A1, Hamilton Spectator, Red Deer Advocate, Times Colonist, L'Acadie Nouvelle, La Voix de l'Est, Telegraph-Journal, The Daily Gleaner, Times & Transcript); Postmedia News (Edmonton Journal, A1, Calgary Herald, A1, Star Pheonix, Windsor Star, Vancouver Sun, National Post, The Province, Leader-Post, The Gazette); * Postmedia Network (Toronto Sun, Winnipeg Sun, Ottawa sun, London Free Press, Calgary Sun, Kingston Whig Standard); Toronto Star, A1,2; Le Devoir, A1; CBC News

Khadr veut prouver sa bonne foi
En dépit de l'opposition déterminée du gouvernement conservateur, Omar Khadr a été libéré hier. L'homme de 28 ans, qui a passé près de la moitié de sa vie derrière les barreaux, est apparu souriant et serein devant les caméras. Une juge de la Cour d'appel de l'Alberta a opposé une fin de non-recevoir à Ottawa, qui demandait au tribunal d'intervenir de toute urgence pour empêcher sa libération sous caution. En rendant son verdict au palais de justice d'Edmonton, la juge Myra Bielby a relevé que le gouvernement n'avait pas réussi à démontrer qu'une telle décision causerait un préjudice " irréparable " au Canada. L'ex-prisonnier de Guantanamo, qui était en détention depuis près de 13 ans, a été photographié dans les heures suivantes à la sortie de l'établissement. Il s'est adressé aux médias en soirée, devant le domicile de son avocat Dennis Edney, chez qui il réside durant sa libération conditionnelle. Omar Khadr souhaite étudier et éventuellement travailler dans le domaine de la santé. (…) M. Edney espère qu'en découvrant Monsieur Khadr, les Canadiens connaîtront les " mensonges " véhiculés par le gouvernement à son égard. L'avocat a accusé au passage le premier ministre Stephen Harper d'être un " fanatique " qui " n'aime pas les musulmans ". Le principal intéressé lui, espère que le premier ministre saura voir en lui un bon citoyen. " Je suis une meilleure personne que ce qu'il (Stephen Harper) pense ", a dit Omar Khadr. Ces critiques n'ont pas infléchi la position du **ministre fédéral de la Sécurité publique, Steven Blaney**, qui a rapidement dénoncé le verdict dans un communiqué. "***La décision rendue aujourd'hui nous déçoit et nous regrettons qu'un terroriste reconnu coupable puisse réintégrer la société canadienne sans avoir purgé toute sa peine***", a-t-il déclaré. Le ministre a ajouté qu'Omar Khadr s'était reconnu coupable de "crimes odieux ", dont le " meurtre " de Christopher Speer, un infirmier de l'armée américaine tué en Afghanistan en 2002 lors d'un affrontement ayant mené à l'arrestation du Canadien. La Presse (Le Quotidien, 16, Le Nouvelliste); Presse Canadienne (Le Droit, 15/Front)

*** Let's do better next time**
An editorial states, "(…) Things didn't go that way on Aug. 6, 2002. That's the day that a United States Army unit fighting in Afghanistan entered the ruins of a building that had been bombed by U.S. aircraft. In that building waited 15-year-old, Toronto-born Omar Khadr. A grenade was thrown - probably by Khadr, though some doubt the veracity of his confession. Whoever threw it, it killed U.S. army Sgt. Christopher Speer. In the resulting exchange of fire, Khadr was grievously wounded. But, thanks to rapid medical aid, he did not die. Thus began the long legal odyssey that had its latest chapter on Thursday, when a judge for the Alberta Court of Appeals in Edmonton ruled that Khadr would be released on bail pending an appeal of his conviction. Khadr was not serving a life term; he was always going to get out eventually. But the federal government had hoped to keep him behind bars for the rest of the prison term he was sentenced to by an American military tribunal. Critics of this ruling, and that includes the federal government, call this a disgrace. A terrorist will now walk freely in Canada, the **public safety minister** grumbled in a statement. Many, however, are relieved, if that's the right word: Khadr is a child soldier, they've long argued. He never should have been imprisoned and sentenced in the first place, and Canada should have done more to bring him home for rehabilitation sooner. Both sides are right." National Post, A10

Ottawa cracking down on passports for would-be terrorists or sex offenders
Ottawa says it is introducing passport measures to prevent people it calls would-be terrorists and sex offenders from travelling abroad. The changes would allow authorities to cancel, revoke or refuse passports for national security or terrorism purposes. **Public Safety Minister Steven Blaney** and Citizenship Minister Chris Alexander made the announcement on Thursday. The measures were included in the Conservatives' budget bill, which was introduced Thursday. **Blaney** and Alexander also said people who have their passports revoked or cancelled will have to wait 10 years before applying for another. The ministers added the changes would allow Federal Court justices who preside in passport cases to protect information from being disclosed but to be able to use that information in reaching their decisions. Canadian Press (Hamilton Spectator, A16, Red Deer Advocate, The Guardian, Cape Breton Post, Red Deer Advocate, The Telegram, Times Colonist, The Daily Gleaner, Times & Transcript)

Pardons

Le **ministre fédéral de la Sécurité publique et de la Protection civile, Steven Blaney**, assure que la Commission des libérations conditionnelles du Canada (CLCC) dispose du financement adéquat pour composer avec une impressionnante pile de demandes de pardon pour des crimes graves. Devant un comité des Communes, jeudi, M. **Blaney** a affirmé que l'organisation atteignait ses objectifs en matière de gestion du retard accumulé qui remonte aussi loin qu'à 2012, moment où le gouvernement conservateur a révisé le système de réhabilitation. M. **Blaney** a avancé qu'à ce stade-ci, il resterait «un peu plus de 5000 demandes à traiter». Il a ajouté que le président de la CLCC, Harvey Cenaiko, et son équipe lui avaient confirmé qu'ils disposaient des ressources suffisantes pour s'attaquer à cet épineux problème. Les propos du ministre ont fort probablement étonné les quelque 5800 personnes qui attendent, depuis des années déjà, que leur demande de pardon soit traitée pour pouvoir reprendre une vie normale. Presse Canadienne (L'Acadie Nouvelle, 19, La Voix de l'Est, Le Droit, Le Soleil); La Presse (La Voix de l'Est, Le Nouvelliste)

* **Rules on pot dispensaries pragmatic - and overdue**
An opinion piece states, "Sooner or later, it was bound to happen. With the marijuana trade recently legalized in some U.S. states and British Columbians long toking in parks and on street corners, the policing of pot use was eventually going to become less rigorous in Vancouver. (...) Pot dispensaries in the city that sprung up initially to serve customers with prescriptions for the substance have, since 2012, proliferated, from 20 dispensaries to 80 - a chaotic situation arising from the City of Vancouver's failure to act. It did nothing to curb their growth nor establish any monitoring system to oversee to whom the dispensaries are selling, let alone where they are obtaining their supplies. Having allowed the situation to get out of hand, the city now needs to get a handle on the dispensaries, and at least manage their locations. To that end the city appropriately has proposed a licensing system that would restrict their presence to arterial streets, away from places where youngsters gather, and impose an annual administration fee of $30,000. Vancouver city council has voted to have its provisions go to public hearings at the end of May with a view to having a regulatory system in place by October. The Harper Conservatives, meanwhile, are aghast at the city's plan, and sticking to their line that marijuana use is a criminal activity. Health Minister Rona Ambrose and **Public Safety Minister Steven Blaney** are urging Vancouver council and the police department to close all the dispensaries which, they insist, are illegal operations. The Vancouver Sun, B6

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

New campaign hopes to cut non-emergency calls
Thousands of non-emergency calls reach 911 dispatchers every year, but a new government video is hoping to change that statistic. On Thursday, the provincial government launched a new 911 awareness campaign through the Emergency Management Office (EMO) that shows first responders like police, RCMP, firefighters, paramedics and call takers in action while emphasizing the 911 service should be used when there's "immediate" danger to one's life or property. "Every accidental 911 call must be treated as a legitimate call," Mary Furey, minister responsible for EMO, said during the launch at Province House. "In many cases that ties up a tremendous amount of resources, when we could parallel have a true emergency." Cape Breton Post

* **Controlled burn near Fortress Louisbourg scheduled for today**
A controlled burn will happen on Parks Canada land near the Fortress of Louisbourg, beginning at 1 p.m. today. It's expected the fire will "restore cultural landscapes" and protect buried archeological objects from risk of wild fires in the future, according to a news release issued by Parks Canada on Thursday. The controlled fire will take place along the north shore of the historic site. The Fortress of Louisbourg National Historic Site will remain open to the public. The Old Town Trail will be temporarily closed to the public during the burn for the public's safety. Parks Canada says the burn, while controlled, could see smoke drift toward homes and businesses in Louisbourg. Cape Breton Post, A3

*** Oil in train wreck treated, company says**
A shipment of oil involved in an explosive train derailment in North Dakota had been treated to reduce its volatility, a company official said Thursday. Hess Corporation spokesperson John Roper said the company's oil complied with a state law that requires propane, butane and other volatile gases to be stripped out of crude before it can be transported. That conditioning process lowers the vapour pressure of the oil to reduce the chance of an ignition during a crash. The state volatility standard, which went into effect last month, came in response to a string of fiery train accidents, including a 2013 derailment in Lac-Mégantic, Que., that killed 47 people. Despite the treatment of the oil, six cars caught fire in Wednesday's derailment about three kilometres from the town of Heimdal. The town was evacuated but no one was hurt. Members of Congress have called for a stricter, national volatility standard for crude moved by rail. Associated Press (Waterloo Region Record, A4; Hamilton Spectator; Times-Colonist)

*** Sherbrooke travaille à un plan d'intervention**
La Ville de Sherbrooke est à réaliser un plan d'intervention particulier pour les situations de déraillement de train. Le directeur général adjoint à l'optimisation et à la sécurité publique Gaétan Drouin estime qu'il faudra plusieurs mois avant de terminer le plan. « Nous avons donné le mandat. Mais après les événements de Mégantic, il a fallu plusieurs mois à nos services pour qu'ils s'en remettent. C'est sans compter que nous avions encore les deux mains dans les événements de Neptune Technologies. Au travers de ça, nous avons dû refaire un plan d'action pour le verglas à la suite de la tempête de décembre 2013 et il y a eu les inondations au printemps de 2014. L'équipe de la sécurité civile a été particulièrement sollicitée », explique M. Drouin. Il ajoute qu'il est très difficile de dresser un plan d'intervention spécifique. La Tribune, 3

*** Still trapped - Four years and $115 million later, some flood evacuees no closer to home**
Many evacuees from Manitoba's 2011 flood remain stranded in temporary accommodations. The Canadian Red Cross continues to pay rent for 1,914 people. The total cost of the evacuation, as of January, was $115.6 million and rising. That's more than the estimated $100-million cost of rebuilding the Lake St. Martin reserve. Even after four years, two levels of government and four First Nations can't agree on how to get the people home. For the displaced people, it wasn't supposed to be this way. Winnipeg Free Press

*** Open-air fires banned across southern Quebec**
Open-air fires either in or close to forests have been banned in certain areas across southern Quebec because of current weather conditions. The ban was put in place on Wednesday by Quebec's ministry of forests, fauna and parks. Areas from Quebec City to the Outaouais region and everything south of that fall under the ban, including Montreal, Laval and parts of the Eastern Townships. The ban was expanded Thursday to include all areas of the province south of the 47th parallel. The ban was announced at the same time as a fire ripped through six hectares of forest in Mont St-Grégoire Wednesday. Montreal Gazette, A5

*** St. George forest fire destroys two barns - No burning order remains in place for all of New Brunswick**
Two barns were destroyed Thursday by a forest fire in the St. George area, says a local resident. Cheryl McKinley says the fire started in Bonny River and jumped the river spreading into the trees. McKinley says it was about six houses away from her home in Canal. She says her family had packed their bags and was ready to leave, but that wasn't necessary. McKinley says she saw four water bombers pass overhead. She says two barns were lost but no homes. The entire province remains under a no burning order from the Department of Natural Resources. The provincial forest fire centre reports 18 fires burning on Friday, including four that were still considered out of control as of 6:40 a.m. To date this spring there have been 102 forest fires which have burned 120 hectares. The 10-year average is 124 fires with 212 hectares burned by this time of year. CBC News

*** Manitoba infrastructure won't withstand climate change, expert says**
A water security expert says climate change will have dire consequences on Manitoba's infrastructure and consequently its economy, unless something changes. Bob Sandford, EPCOR Water Security Research Chair at United Nations University, began working to help solve water-related climate issues in

Manitoba a decade ago. His first focus was on Lake Winnipeg - now his focus is the province's infrastructure. "You see that there are larger changes to the hydrologic cycle that are causing more frequent flooding, greater storms and causing greater infrastructure damage. We are of the view that this could have serious economic consequences for the province, so our meeting today is about how we deal with those matters," Sandford told CBC's Radio Noon Thursday. Sandford spoke to the Threatened Infrastructure conference Thursday in Winnipeg, hosted by the Manitoba Capital Region. Sandford explained that the hydrologic cycle he mentioned refers to how water is naturally redistributed across the planet, through evaporation primarily from the oceans, and then distributed globally through weather patterns. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Ottawa sending wrong message: Hamdani
Hamilton lawyer and Muslim community spokesperson Hussein Hamdani says his suspension from a national security roundtable last week sends the wrong message to Canadian Muslim youth. Hamdani says youth he's been working with to prevent radicalization have been calling him and saying: "If what they (did) to you, is what they can do to us - why should we partner with them?" That suspension, Hamdani told the Rotary Club of Hamilton Thursday, plays into the "grievance" mentality present in youth in danger of radicalization: a notion that the West is at war with Islam and Muslims. "For the past week I've been spending half my time with young people explaining there is no war against Islam, there's discrimination, there's bigotry, but we're not the only ones to experience that and we must rise above it." The Hamilton Spectator, A4

*** New integrated police force for the Hill**
Six months after an Islamist gunman stormed Parliament, the Hill is getting a new integrated police force and $39 million more in protective muscle. The 400 members of the current and separate House and Senate security services will be integrated under the operational command of the RCMP and a director reporting to the Speakers of each house. The operation gets a new name, too - the Parliamentary Protective Service. The shakeup has been openly discussed for months. Details were formally made public Thursday in the Conservatives' budget bill tabled in the House of Commons, which proposes amending the Parliament of Canada Act to allow the change. The parliamentary precinct's current fragmented security operation has been criticized for years. Responsibility is divided among three agencies: The House of Commons' security handles buildings under House jurisdiction, while Senate Protective Service is responsible for East Block and the east side of Centre Block. The RCMP is responsible for the grounds. (Ottawa police is responsible for streets in the broader parliamentary precinct beyond Wellington Street.) The system's shortcomings became evident in December 2009 when 19 Greenpeace activists climbed onto the roofs of both West Block and Centre Block and unfurled climate-change protest banners. Then, on Oct. 22, 2014, Michael Zehaf-Bibeau, armed with a rifle and knife, easily sprinted past RCMP perimeter security and a House of Commons guard before dying in a hail of bullets deep in the Hall of Honour. The reorganization is not expected to encounter political opposition. MPs of all stripes, including Prime Minister Stephen Harper, were in nearby caucus rooms during the attack. The security shakeup may encounter some turbulence from organized labour. Although all current House and Senate security jobs and collective bargaining agreements will be protected, the proposed enabling legislation suggests the workplace transition for the security staffs will take time to hammer out. As well, there is speculation the parliamentary guards may seek salary parity with their higher-paid RCMP counterparts. Postmedia News (Ottawa Citizen, A10)

*** Le controversé C-51 adopté**
Le projet de loi antiterroriste controversé du gouvernement Harper a été adopté, mercredi, à la Chambre des communes. La Loi antiterroriste, aussi connue sous le nom de projet de loi C-51, a été adoptée facilement en troisième lecture par 183 voix contre 96, grâce à la majorité gouvernementale conservatrice et au soutien des libéraux, troisième parti aux Communes. La loi accorde plus de pouvoirs au Service canadien du renseignement de sécurité (SCRS) pour contrecarrer les présumés complots terroristes, et pas seulement pour recueillir de l'information. Elle accroît aussi l'échange d'information de sécurité entre organisations et agences fédérales, élargit la portée des interdictions de vol et crée une nouvelle

infraction criminelle d'encouragement à commettre un acte terroriste. En plus, la loi facilite l'obtention par la GRC d'une ordonnance de garder la paix pour restreindre les mouvements d'un suspect et prolonge les détentions préventives. L'Acadie Nouvelle, 20

* **Les conservateurs déposent un "petit" projet de loi mammouth**
La 41e législature canadienne prend peut-être fin dans un mois, mais il semble que cela laisse assez de temps pour déposer un nouveau projet de loi mammouth... et l'adopter. Le gouvernement conservateur a en effet présenté jeudi un projet de loi budgétaire qui modifie ou édicte près d'une trentaine de lois, dont certaines traitant de terrorisme, de droit d'auteur, d'immigration, de régime de retraite, de congé de maladie et de sécurité sur la colline parlementaire. Entre autres. Le projet de loi C-59 ne compte cette fois-ci " que " 157 pages. Il édicte notamment la Loi sur la prévention des voyages terroristes, qui instaure un mécanisme d'appel lorsqu'une personne voit son passeport saisi par décret ministériel. Cette personne pourra, dans les 30 jours, demander une révision judiciaire. Celle-ci pourra se dérouler à huis clos et en l'absence du principal intéressé si le juge estime que la divulgation de la preuve pourrait porter atteinte à la sécurité nationale. Le juge devra alors veiller à ce qu'un résumé de la preuve soit fournie au plaignant. L'autre loi édictée par C-59 instaure, comme promis, un régime de sanctions contre tout futur gouvernement déposant un budget déficitaire. Si le déficit est " justifié " par une récession, les ministres et sous-ministres verront leurs salaires gelés. Si le déficit n'est pas " justifié ", alors ces gens écoperont d'une réduction salariale de 5 %. Justifiés ou pas, les déficits entraîneront chaque fois une interdiction de hausser les budgets de fonctionnement des ministères pour financer des hausses salariales des fonctionnaires. Le Devoir, A2; Windsor Star (National Post, Vancouver Sun, Star Phoenix, The Gazette, Leader-Post)

* **Canada to provide anti-terror support for Philippines**
Canada will provide counterterrorism and anti-crime support to police in the Philippines, part of an effort to boost security and commercial ties with one of Asia's fastest-growing economies. Prime Minister Stephen Harper is expected to announce three new security initiatives on Friday during a visit with Philippine President Benigno Aquino in Ottawa. The leaders will also discuss ways to promote trade and investment during a meeting on Parliament Hill, a government source said. The Philippines has fought a lengthy battle against Islamic and communist insurgents in Mindanao, a region that is composed of the country's southern islands. Earlier this year, 44 Philippine police officers were killed in a botched anti-terrorism operation in the region, an event that has raised questions about Mr. Aquino's leadership. A senior Canadian government source said Ottawa's support would focus on both regional and global security concerns, including the threats of terrorism and transnational organized crime. The federal government will offer support from its counterterrorism capacity-building program to bolster maritime security at trading ports in the region, the source said. The program is intended to help Philippine authorities provide more information to Interpol, a global organization that's meant to facilitate international police cooperation. In addition, the government will offer a "train the trainers" style program to help Philippine authorities deal with improvised explosive devices in the country, the source said. The program will involve between five and seven Canadian Forces trainers. Ottawa will also provide assistance to police in the Philippines to help them combat transnational organized crime, the government official said. It was unclear on Thursday whether a specific type of crime would be targeted by the new initiative, but priority issues for Manila include drugs and human trafficking. Globe and Mail, A4

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Burning bridges
A letter to the editor states, "Last week's deal between the Ambassador Bridge and the City of Detroit was interesting but insignificant. The Ambassador Bridge Company is facing a serious political problem after their relentless attack on the new international crossing. Their lobbying efforts forced Canadians to fund Michigan's $550 million share of the freeway connect. Their lobbying forced Canadians to fund the $300 million U.S. Federal Customs Plaza. If the Ambassador Bridge Company wants a privately owned twin span, Canadians will rightfully expect them to fund the Canadian Custom's Plaza and the freeway connection to the 401. Funding will not come from Michigan or U.S. federal governments. They wouldn't

spend it on their own infrastructure. Funding will not come from any sane politician on this side of the border. They've already spent billions on a public crossing and have no reason to spend another billion to support a hostile private company." Windsor Star, A6

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

City courthouses targets for 2 suspicious parcels
The federal courthouse building in downtown Fredericton was briefly locked down on Thursday morning after police received a report of a suspicious package. Alycia Morehouse, the city's public safety spokeswoman, said police were called to the courthouse, located at the corner of Westmorland and Queen streets, at around 9:30 a.m. "The package does appear to be from outside Canada," she told The Daily Gleaner at the scene. "We are actively investigating, and we have been in contact with the National Security Enforcement Section. There have been a number of similar packages that have been received at courthouses in other jurisdictions," she said. The courthouse wasn't evacuated, but no one was allowed to enter or leave the building while police conducted the investigation. The fire department and ambulance services were also on scene as a precaution, Morehouse said. The building was deemed safe at around 11 a.m., and a parcel was removed from the building by police. Morehouse said she couldn't comment on the nature of the package, directing requests to the RCMP's National Security Enforcement Section. Daily Gleaner, A1

New weapons training facility coming to Hanwell
The Fredericton area is getting a new state-of-the-art weapons training centre. The $3.5-million facility, set to open next year in the Hanwell Business Park, will be designed to meet the specific needs of law enforcement and specialized security force organizations. Cary Baker, who speaks for the project, said the centre will allow users to conduct firearms training day and night on a 24-7 basis. "We're hoping to officially break ground with the foundation (in the) July-August time frame," said Baker, a former special operations major in the Canadian Armed Forces. "The intent is to open early 2016." Baker said the facility, dubbed the Iron Sights Training Centre, represents investments from him as well as several other individuals from within and outside the province. The 20,000-square-foot indoor complex will be constructed near the Maritime Case dealership on Timothy Drive. The facility is expected to create as many as 20 full- and part-time jobs during its first year of operation, with that number jumping to as many as 30 once capacity is reached. Baker said the unique thing about the complex is that it will be geared toward tactical shooting. "What that basically means is part of the range is designed and set up so that police officers can actually do what we call walk and shoot - more dynamic type shooting training," Baker said. "It basically falls in line with the RCMP report from the Moncton shootings last year that defined a requirement for better tactical training facilities so that police officers can train in a realistic environment - a live fire environment - using simulation systems that can re-enact or provide what we call active shoot threat scenario." Daily Gleaner, A1

Two charged in Sharif Said slaying
Two people who were in a car that confronted 21-year-old Sharif Said minutes before he was gunned down are now behind bars - one an elusive suspect known to police who is alleged to have pulled the trigger, another a man with a lengthy criminal history accused of driving the getaway car. Police have arrested Khalid Mohammad, 26, and charged him with second-degree murder. Authorities contend he didn't plan to kill Said, but that a sign of what was perceived as disrespect at a house party Saturday night led to an altercation between two vehicles Sunday morning on Tremblay Road, where the victim was gunned down. Police also arrested 28-year-old Abdulaziz Abdullah in connection with the homicide. Police allege he was an accessory after the fact, helping Mohammad to escape. Both men appeared in court briefly Thursday by video and were formally charged. They were ordered not to contact a long list of people, including each other, neighbours in the area where Said was killed and the slain man's parents.

The alleged gunman Mohammad, who goes by "AJ," is well-known to police and was a suspect in multiple shootings in 2014, a year that set a record for reported gun violence in the capital. Ottawa Citizen, A3

Returning To The Uniform

On a Sunday evening one year ago, 24-year-old David Charles Sandaker was shot dead in a busy residential neighbourhood by a member of the Edmonton police tactical team. The gunfire erupted from both police and Sandaker as officers were attempting to place him under arrest. One member was hit in the leg, receiving non-life-threatening wounds. Despite the critical incident debriefing that typically follows a case such as this, a fatal shooting can be hard on the mental health of the officer who pulled the trigger. That's where Sgt. Glen Klose and Const. Colleen Mooney enter the picture. In 2009, an officerinvolved shooting prompted city police to recognize a formal program was needed to help members involved in critical incidents return to their job. Working with the Workers Compensation Board (WCB), the reintegration team has now worked with more than 40 members involved in critical incidents such as shootings, Taser deployments or bad collisions. The team also continues to work with seven long-term members either diagnosed with PTSD or struggling with other psychological issues... . Edmonton Sun, 7

Senate staff resisted coverup

A group of senators worked behind the scenes to "kill" an internal audit of senators' housing claims, and were stopped only when two officials from the red chamber threatened to take legal action if the review was quashed, according to newly released court documents. Instead, the audit was allowed to quietly continue and, indeed, will be the subject of intense legal arguments between the Senate and suspended senator Mike Duffy's defence team, who believe the document should be introduced as evidence at his trial. The internal study could also be damaging for the Senate itself, as its findings could identify senators who improperly claimed housing expenses when their main residence was in Ottawa. The documents, filed in court this week, outline how Gary O'Brien, who was at the time the Senate clerk, raised an objection in 2013 to senators "wanting to kill the internal audit" that outlined issues with the Senate's housing allowance policy. O'Brien told RCMP investigators in September 2013 that he had informed the senators he "wasn't going to go along" with the plan. The internal audit had been written by Jill Anne Joseph, then the director of internal audit and strategic planning for the Senate. "I know I'm their servant, but on the other hand I have a professional obligation with respect to stewardship of public funds and appropriateness of procedures and all of that business," O'Brien told the investigators, according to a transcript of his RCMP interview the court released Thursday. Instead, emails quoted in the court documents suggest O'Brien and Joseph "threatened legal action if the full original audit report was not released." Conservative senators even felt Joseph "would leak the report." O'Brien told the RCMP that latter claim "was bullshit." He spoke highly of Joseph, calling her work "professional." Postmedia News (National Post, Ottawa Citizen, StarPhoenix, Windsor Star, Vancouver Sun); * Globe and Mail; * Postmedia news (Windsor Star, National Post, Vancouver Sun, Leader-Post, StarPhoenix, Montreal Gazette, Edmonton Journal, Calgary Herald, Ottawa Citizen)

SNC-Lavalin «n'est pas coupable» selon son PDG

Le grand patron de sNC-Lavalin, robert Card, assure que la firme d'ingénierie québécoise «n'est pas coupable» des accusations de corruption et de fraude, portées par la GrC dans le cadre des activités de l'entreprise en Libye. «Et nous n'avons pas l'intention de plaider coupable», a poursuivi avec aplomb M. Card devant les journalistes, en marge des résultats financiers présentés lors de l'assemblée des actionnaires tenue à Montréal. En février dernier, la GRC a déposé des accusations contre la firme. Elle allègue notamment que SNC et deux de ses entités ont versé plus de 47 millions $ en pots-de-vin, de 2001 à 2011, à des représentants du régime de Mouammar Kadhafipour des projets d'ingénierie dans ce pays d'Afrique du Nord. Selon la GRC, cet argent servait à «convaincre ces derniers d'utiliser leurs positions pour influencer les actes ou les décisions» de l'État libyen». SNC-Lavalin aurait ainsi pu frauder l'État libyen, ainsi que d'autres entités libyennes, pour un montant de près de 130 millions $. Agence QMI (Journal de Quebec, Journal de Montreal); Globe and Mail

Hells Angels, associates guilty of murder conspiracy

Fourteen Hells Angels, or associates of the gang, have avoided a trial set to begin next week by pleading guilty to taking part in a general conspiracy to murder rival members of criminal organizations during an

eight-year period. With jury selection set to begin Monday, the 14 men - 13 were tied to the gang's Trois-Rivières chapter - pleaded guilty on Thursday to a murder conspiracy charge, while any first-degree murder charges they also faced were placed under a stay of proceedings. The guilty pleas recorded on Thursday brought the number of men who have pleaded guilty in Operation SharQc to 101. Operation SharQc was a lengthy investigation led by the Sûreté du Québec that saw almost every member of the Hells Angels based in Quebec arrested in April 2009. No one arrested in Operation SharQc has had an actual trial yet, but almost all of the men who pleaded guilty Thursday were supposed to be part of a larger group whose trials are set to begin Monday with jury selection. The large group has been reduced to 10. Another two men are expected to have a trial in English at a later date, which means only 12 of the 156 people originally charged in 2009 still have cases pending. According to the SQ's website, another nine men have yet to be arrested in Operation SharQc. Besides the guilty pleas, the prosecution obtained the court's permission on Thursday to destroy two of the gang's bunkers - one in Trois-Rivières and another near Quebec City - which were significant symbols of the biker gang's defiance, especially from 1994 to 2002, the time frame referred to in the murder conspiracy charge. The men who pleaded guilty on Thursday admitted they were part of a plot the Hells Angels hatched to go after other organized crime figures who opposed their goal to monopolize drug trafficking across the province. Besides being allowed to level the buildings, the provincial government will take ownership of the land the Trois-Rivières chapter once considered its headquarters. Discussions are underway to determine which level of government will take control of the land near Quebec City. Postmedia News (Montreal Gazette, A4); Canadian Press (National Post, A8); Agence QMI (Journal de Montreal, Journal de Quebec); Le Nouvelliste; Presse Canadienne (La Voix de L'Est); * La Presse (Le Soleil, Le Quotidien)

Remaining suspects in killing of Pelican Narrows teen in custody

All seven suspects in the killing of a 17-year-old Pelican Narrows boy on a northern reserve are now in police custody. Hilliard Sewap Jr. died Saturday on the Peter Ballantyne Cree Nation. Pelican Narrows RCMP were called to a home around 6:30 a.m. after a report of a disturbance. They rushed the injured teen to Angelique Canada Health Centre, but he was declared dead. Five men and two boys were charged with second-degree murder; some of them face additional charges. An RCMP news release issued on Wednesday said three of the men were in custody and arrest warrants had been issued for the other two men - Robbie Lambert Creed Custer and Brandon Lee Matt McCallum - and two male youths. On Thursday, RCMP said Custer, McCallum and the two boys are now in custody. Postmedia News (StarPhoenix, A2)

Man wanted in killing arrested

A 30-year-old man wanted in connection with the slaying of a man in Grande Prairie, Alta., was arrested Wednesday in Nanaimo. Tommy Vernon Paul was spotted by plainclothes officers from Nanaimo RCMP as he rode a bike along Haliburton Street. He was arrested without incident. Arrangements are being made to send Paul back to Alberta, Nanaimo RCMP said. Grande Prairie RCMP issued an arrest warrant for Paul on Tuesday in connection with the killing of Adrian Snider, 25. Snider was reported missing March 31 and human remains found outside Grande Prairie on Monday are believed to be related to his death. Times Colonist, A4

*** Dziekanski's mom has say at Mountie's hearing**

When Zofia Cisowski immigrated to Canada she saw the RCMP as the symbol of democracy and trust, but that impression has been destroyed in the years since officers jolted her son with a Taser, a court has heard. "My faith in the honesty of the RCMP has forever been shaken," said the mother's letter, read at a sentencing hearing for RCMP Const. Kwesi Millington on Thursday. Millington was convicted of perjury for lying under oath during a public inquiry into Robert Dziekanski's death at Vancouver International Airport in October 2007. His defence lawyer opposed allowing Cisowski to read her victim-impact statement into the record. But B.C. Supreme Court Justice William Ehrcke rejected the argument that Cisowski didn't qualify as a victim because Millington's crime was against the "administration of justice." "It is difficult to put into a few or any words how the perjury of Mr. Millington has impacted me," Ehrcke read from Cisowski's letter. "When I came to Canada I saw the RCMP as the main symbol of Canada and what it stood for, a democracy where people could always trust the police," she wrote. Crown prosecutor Scott Fenton told the hearing that the disgraced Mountie, convicted of lying about the death of Dziekanski,

should spend up to three years in prison. Perjury carries a maximum sentence of 14 years. Canadian Press (The Province, A8, Vancouver Sun, Times Colonist)

*** Quelques crises qui ont marqué son mandat**
En froid avec le directeur général de la Ville, le chef Marc Parent partira à la fin de son contrat en septembre, après un des mandats les plus houleux de l'histoire du service de police de la Ville de Montréal. Toutes nos sources maintiennent que la relation entre le chef Marc Parent et le directeur général (DG) Alain Marcoux se serait détériorée au cours des derniers mois. Au point où le chef de police, après une courte période de réflexion, aurait refusé de signer un éventuel contrat de travail en vue d'un second mandat à la tête du Service de police de la Ville de Montréal (SPVM). Encore faut-il qu'il y ait un contrat à signer. Nos sources au gouvernement affirment que Montréal aurait tardé à demander le renouvellement du chef Parent. Après l'annonce-surprise de son départ hier, toutes les entrevues officielles donnaient à penser que tout était au beau fixe entre le DG et le policier, même si dans les faits une retentissante prise de bec les aurait opposés au début de l'année. Journal de Montreal, 4

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

'Freedom is way better than I thought'
On his first evening of freedom since he was 15 and threw a grenade at U.S. soldiers in Afghanistan, a smiling, relaxed Omar Khadr said he hopes Canadians will try to get to know who he is now. "I would like to thank the Canadian public for trusting me and giving me a chance. I will prove to them I am more than what they thought of me. I will prove to them I'm a good person. I'm excited to start my life." Eight hours earlier, an Edmonton judge ordered Mr. Khadr, now 28, released on bail, rejecting a last-ditch attempt by the Canadian government to keep him in prison, and releasing him under the supervision of Dennis Edney, his long-time lawyer. After his release, the former Guantanamo detainee went for lunch, then returned to the courthouse for some paperwork. There, he encountered some government officials. "I was surprised. Some of the sheriffs went out of their way to be kind and buy me some drinks," he told reporters who gathered to meet him at Mr. Edney's comfortable Edmonton home. (...)The bail release order from Justice Myra Bielby of the Alberta Court of Appeal was yet another major legal defeat for the Conservative government, which has seen the courts strike down its efforts to fight drugs and gun crime, reject plans for Senate reform and even say no to the Prime Minister's choice of a judge for the Supreme Court. Globe and Mail; Edmonton Sun, 1; * Maclean's, * Journal de Montréal (Journal de Québec)

Mr. Khadr, you're free to go
There are two famous photographs of Omar Khadr. (...)To the government, which vigorously fought his release on bail and expressed disappointment at a judge's decision to grant it on Thursday, he is an incorrigible terrorist in the mould of his father, Ahmed, an al-Qaida financier who enlisted his notorious family in the cause. Lying half-dead amid the rubble of a compound in the Khost district of Afghanistan, approached by U.S. soldiers clearing a cache of bombs, Omar Khadr deserves on this view to be blamed as an adult for tossing the grenade that killed U.S. Sergeant 1st Class Christopher J. Speer, then 28, a combat medic. (...) "I don't think the government is worried that Omar Khadr is a terrorist. I think the government is more worried that he is not," said Audrey Macklin, a professor and chair of human rights law at the University of Toronto, and a prominent advocate for Khadr. For the Conservative government, he has been a symbol of its counterterrorism agenda, but he also has relevance to other political goals, she said, such as its "tough on crime" platform and its effort to redefine Canadian citizenship more as a privilege than a right, something to be protected against abuse by foreigners. National Post, A1 (Windsor Star, Vancouver Sun, Leader-Post, Edmonton Journal), Associated Press (Seattle Times, Yahoo! News), Edmonton Sun, * Presse canadienne (Le Soleil, La Tribune)

Khadr's education has been built on kindness of strangers
For the past 12 years, in between interrogation sessions and working in prison factories, Omar Khadr has been trying to learn beyond his Grade 8 education. Khadr, now 28, has always known the day would come when he would finally leave prison and have to adjust to everyday life. While governments, circumstance and his parents, each in their own way, have failed Khadr, strangers have stepped into the void to help educate him. Nine Alberta university professors, most of them from The King's University in

suburban Edmonton, have spent years visiting Khadr in prison and tutoring him. Since Khadr was transferred to Alberta in May 2013, the professors have worked with him at least once a week. There are also those who offer Khadr a schooling of another kind - not in books but in the benefits of socializing and shooting the breeze. These socially adept university students and recent graduates write him letters and visit him in prison. Seven women from various countries have even started the online campaign, Free Omar Khadr Now. Toronto Star, A14

*** Omar Khadr's odds of winning U.S. appeal look good, legal expert says**

Just hours after his release, Omar Khadr told the media, "Freedom is way better than I thought." Although he is free on bail, Khadr faces legal proceedings ahead of him that could last for years. He was released in connection with the pending appeal of his conviction by a military commission in 2010 at the notorious Guantanamo Bay detention camp. In the next couple of months, Khadr also has a hearing at the Supreme Court of Canada in the federal government's appeal of an Alberta court ruling that he should be treated as a juvenile offender. He was 15 years old when he was taken into custody by American forces in Afghanistan. And on June 25, he has his first parole hearing. He has been eligible for full parole since July 1, 2013. In her initial decision granting bail release, in April, Alberta Justice June Ross cited the work of law professor David Glazier in connection with Khadr's U.S. appeal. (…) Glazier tells CBC News that Khadr's U.S. appeal will likely take at least several more years. The case is now before what's called the court of military commission review, with little progress to report after 18 months. And Glazier says the really significant rulings won't happen until the case reaches the federal court of appeals. The key merit of Khadr's appeal, Glazier says, "is that he's being tried in a military court system which, as a matter of law, should only have jurisdiction over actual war crimes' allegations, and none of the charges that have been levied against him constitute war crimes, as recognized by international law." Khadr's prosecution in 2010 "has no credible legal foundation," he adds. CBC News

*** Khadr 'forever a murderer'**

You'll have to forgive Tabitha Speer for not sharing the same excitement and enthusiasm as some in Canada seem to be feeling about the release of "child soldier" Omar Khadr. In her house in North Carolina, the child soldier left her children --Taryn, 15, and Tanner, 14 -- without a father. Omar Khadr got to walk out of prison after almost 13 years Thursday. Her husband, Sgt. Christopher Speer, will never come home. Still, the always classy Tabitha did not dare step into the media fray Thursday or lower herself into the snake pit by saying something in anger. In fact, she made special point of not commenting. Ottawa Sun, 5 (Toronto Sun)

*** No longer the demon he's made out to be?**

An opinion piece states, "Mixed feelings greet the release of Omar Khadr on bail. Torn between pangs of anger and sympathy, from the need for punitive justice to the need for compassion, vacillating from the visceral desire to see a killer justly punished to the recognition that he was a kid who has already served more time than any juvenile would serve in this country. No, I can't muster the jubilation that erupted at the decision by an Alberta judge to release the 28-year-old on bail after 12 years and nine months behind bars for killing U.S. Sgt. Chris Speer during a firefight in Afghanistan in 2002. (…)If the murder had occurred in this country, Khadr would have been tried under the Young Offender's Act of the time and faced a maximum decade of incarceration. His eight years of presentence custody in a horrific hell-hole where there are allegations he was water-boarded would have surely been double-or triple-timed to be the equivalent of 16-24 years. So enough already." Toronto Star, 5 (Ottawa Sun, Calgary Sun, London Free Press)

*** Omar Khadr - Libre, enfin!**

Un article d'opinion déclare, « Pour comprendre toute la hargne des conservateurs envers Omar Khadr, enfant-soldat en qui le gouvernement Harper refuse de voir autre chose qu'un terroriste, il vaut la peine de s'arrêter à une autre nouvelle. Howard Sapers, qui occupe présentement le poste d'enquêteur correctionnel du Canada, vient de se faire montrer la porte par le **ministère de la Sécurité publique**. La raison n'est pas claire, seule la longévité à son poste ayant été évoquée. Mais M. Sapers, ombudsman des détenus, s'est aussi souvent heurté au gouvernement..., notamment en défendant Omar Khadr en tant que détenu exemplaire. Quelle coïncidence donc que, dans la même semaine, M. Khadr sorte enfin vainqueur de l'incroyable guerre que le gouvernement lui livre depuis des années ! » Le Devoir, A8, Winnipeg Free Press

*** A week of blows for Harper**
An opinion piece states, "Even when you are prime minister of all you survey, there are times that people and events simply refuse to march in the direction you'd prefer. In a week he won't look back fondly on, Stephen Harper has now suffered two such blows in rapid succession. First, his sense of entitlement to eternal political support from his conservative home province was shattered by Tuesday's election of a solid NDP majority. What, he must wonder, are similar folks in Saskatchewan and British Columbia thinking now? And are Albertans enjoying the figurative taste of Tory blood enough to come back for seconds? And now, in what must be almost as profound a blow, Ottawa's long refusal to release its almost pathological grip on former Guantanamo Bay child inmate Omar Khadr has been rejected by an Alberta court of appeal. Khadr is not home free, mind you. Rather, he is out on bail under strict conditions as he awaits the results of appeals against American convictions for war crimes. But the fact that he has been released at all undermines the federal government's dogged insistence that the young man was virtually an existential threat to the Canadian way of life." Edmonton Journal, A20

*** Bienvenue, Omar Khadr**
Un article d'opinion de la directrice d'Amnistie internationale déclare, « Bienvenue dans un monde qui n'a pas été bienveillant avec vous. Bienvenue dans un monde où la justice sera enfin plus forte que les jeux politiques qui se sont construits sur votre personne. Encore une autre juge au Canada qui vous donne raison. En fait, il devient difficile de les compter. Cour suprême du Canada deux fois, Cour d'appel fédérale, cours fédérales de nombreuses fois, Cour d'appel de l'Alberta. Celles-là ont en fait surtout donné tort au gouvernement pour non-respect de ses engagements internationaux et nationaux. Et maintenant, la Cour du banc de la reine de l'Alberta, jugement fort conséquent celui-là pour vous : il vous donne le goût de la liberté qui vous a été niée pendant 13 ans. » Le Devoir, A8

*** Freeing Khadr is a risky business**
An editorial states, "The allegation by Omar Khadr's lawyer, Dennis Edney, that Prime Minister Stephen Harper is an anti-Muslim "bigot" is absurd. Harper is concerned about protecting Canadians from terrorism. That's his job and in Khadr's case it's perfectly understandable why the Canadian government opposed Khadr's bail application, while he appeals his U. S convictions for war crimes. In freeing Khadr Thursday, Alberta Court of Appeal Justice Myra Bielby acknowledged Khadr poses a risk to the public. But not enough, she said, that the potential harm to the public outweighed the potential harm to Khadr of keeping him imprisoned." Ottawa Sun

*** Khadr's no child**
A letter to the editor states, "If our courts have swallowed the line that Omar Khadr was a child at the time of his alleged crime, then how can Melissa Todorovic's sentence stand? Todorovic, who committed the crime of counselling to commit murder at age 14, was sentenced as an adult to life --with which I totally agree. She was well past the age of forming intent. Khadr was almost two years older than Todorovic and a young man." Toronto Sun, 16, Winnipeg Sun

Timeline: The Omar Khadr case
A look at some key developments in the Omar Khadr case. Canadian Press (Chronicle-Herald, A10), Postmedia Network (Toronto Sun, Ottawa Sun, Edmonton Sun, Kingston Whig-Standard), * Postmedia News (Ottawa Citizen), * La Presse

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Haunted by gang violence
Theresa McCuaig has pretty much seen it all when it comes to the underbelly of the nation's capital. McCuaig is the grandmother of Sylvain Leduc, the 17-year-old tortured and murdered by a group calling themselves Ace Crew. The murder took place almost 20 years ago, and Ace Crew was considered the first real gang in Ottawa. McCuaig threw herself into the court system--fighting at the federal level for changes to the Young Offenders' Act; and also became an ardent defender of victims' rights. So when

she hears Sharif Said, 21, found dead Sunday morning, might be the victim of a local gang, she's not fazed by the news. "I'm not surprised," McCuaig said in an interview with the Sun on Thursday. Major crime detectives have charged two men in the city's third homicide of the year. Khalid Mohammad, 26, is charged with second-degree murder. Abdulaziz Abdullah, 28, is charged with accessory after the fact for allegedly helping Mohammad flee. Both made a court appearance Thursday. Said's bullet-riddled body was found in the middle of Tremblay Rd. at about 8 a.m., Sunday. Police said this week it was too early to determine whether the slaying had any ties to gang activity, though investigators said it had all the hallmarks of a drug-related slaying. Ottawa Sun

PUBLIC SERVICE / FONCTION PUBLIQUE

Budget bill lets government set sick leave terms for PS
The Conservative government gave itself the power in the latest budget bill to override federal labour law and impose a contentious new sick-leave and disability regime for Canada's public servants at any time. The budget bill allows Treasury Board president Tony Clement to set aside parts of the Public Service Labour Relations Act, which governs collective bargaining in the public service, to impose new terms and conditions for sick leave and introduce a new short-term disability plan. The timing for such a move will be left up to cabinet to decide. The measures, expected to be challenged in court when passed, give the government the tools it needs to ensure the agreement it wants on sick leave and disability is implemented. The proposed measures are another shot at the labour rights of the 17 federal unions, which the government had already eroded leading up to this controversial round of bargaining over sick-leave benefits. Ottawa Citizen, A1

OTHER

*** Military didn't review videos of troops**
Promotional videos of Stephen Harper's tour of Iraq and Kuwait that revealed faces of Canadian Armed Forces members were not reviewed by the Department of National Defence before they were first posted to the Internet, contrary to what the Prime Minister's Office initially said, The Globe and Mail has learned. On Tuesday, media raised security concerns over two of the videos produced by the PMO's in-house public-relations team - footage the Conservatives quickly uploaded to the Internet to advertise Mr. Harper's Mideast trip. Initially, the PMO had assured reporters the military vetted the videos before they were published online. Senior government officials told the media that the Forces had raised no objections to what had been uploaded, statements that left the impression the military was in part responsible for the fact the videos made it online. Sources say it was only after journalists drew attention to the videos that the Canadian military had an opportunity to scrutinize the footage and to conclude, as it did later that day, that the material represented a risk to soldiers, leaving them vulnerable to attack by extremists. The Globe and Mail, A1

*** Soldier puts DART on map**
When Master Cpl. Denis Carriere heard he was headed to Nepal to provide relief after an earthquake hit the country, killing more than 7,000 people, he knew he had to work quickly. For the first time in his four-year career as a geomatics technician with Canada's Disaster Assistance Response Team (DART), he was headed overseas. He said he was excited to be part of a specialized team that provides relief in the world's most deadly natural disasters, but also knew he only had two days to make a lot of maps. "It's an art. You leave really fast and you have to figure out everything on a day's notice," Carriere said via phone from Nepal. "It's about giving people a situational awareness. If you're in the field in Nepal, there's no Wi-Fi, there's no Internet, so that mapping support when you're in a remote area is really essential for your awareness." Ottawa born and raised, Carriere has called Kingston home for the past four years. He's one of two military men from the city who were deployed as a part of DART to Nepal, where the capital city of Kathmandu and surrounding areas were devastated by the 8.1 magnitude quake. Kingston Whig Standard, A1

INTERNATIONAL

La NSA a agi illégalement avec ses collectes massives
La collecte massive de données téléphoniques opérée par l'Agence de sécurité nationale américaine (NSA) est illégale, a jugé jeudi une Cour d'appel américaine, estimant qu'elle outrepassait le cadre fixé par le Congrès. Les lois sur lesquelles s'est appuyée la NSA pour mettre en place cette collecte « n'ont jamais été interprétées pour autoriser quelque chose qui s'approche de l'ampleur de la surveillance généralisée en question ici », a estimé un tribunal de New York dans un document de 97 pages. La plainte avait été déposée par l'association de défense des libertés ACLU (American Civil Liberties Union) contre la NSA, l'agence de renseignement chargée de l'interception des communications, et le FBI après les révélations faites en juin 2013 par l'ancien consultant de la NSA, Edward Snowden. Les millions de métadonnées téléphoniques collectées par la NSA comprennent des numéros de téléphone, la durée des conversations téléphoniques ou leur localisation mais pas leur contenu. L'ACLU estime en outre que ce programme constitue une violation massive de la vie privée sans aider outre mesure à contrer le terrorisme. Le Devoir.com; Waterloo Region Record; Assocaiated Press (Calgary Herald, Montreal Gazette, Vancouver Sun, Windsor Star, National Post, Edmonton Journal, Times Colonist)

* **Floods, tornadoes cause destruction, injuries in Oklahoma**
Authorities are investigating the damage left behind by spring storms carrying more than a dozen suspected tornadoes that swept across the southern Plains, bringing floods, forcing the evacuation of an international airport and destroying homes near Oklahoma City. At least 12 people were injured, but no deaths were immediately reported from the twisters that also hit rural parts of Texas, Kansas and Nebraska on Wednesday night. The Oklahoma City area seemed to be the hardest hit. A twister destroyed homes in Grady County, southwest of the city, and it appeared another tornado touched down in the area later Wednesday evening when a second storm came through. Telegraph-Journal, A8

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
May 21, 2015 / le 21 mai 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Canadian Jihad
An east-end Montreal college is gaining a reputation as a breeding ground for jihadis after four of its students were arrested at the airport Friday, allegedly on the verge of taking off to join an overseas terror group. The latest arrests bring to 11 the number of Collège Maisonneuve students who since January have either left to join jihadi groups overseas or have been arrested on suspicion of planning to leave. The four were among 10 students from various CEGEPS - post-secondary institutions unique to Quebec - and high schools arrested at Pierre Elliott Trudeau Airport Friday, the college confirmed. They are "suspected of wanting to leave the country to join jihadist groups," the RCMP said in a statement. They had their passports confiscated and were released without charge. The police said they spoke to the families and friends of those arrested and the investigation is ongoing. (…) **Federal Public Safety Minister Steven Blaney** announced Wednesday that he will invite his provincial counterparts to an early summer meeting to discuss terrorism and radicalization. "***There is no profile of terrorists. You can come from whatever (income), whether Canadian-born or foreigner, the profile of a terrorist is very diverse***," he told CBC News Network. "***What we need to work on is the motive. We need to be able to identify at an early stage those individuals who are being radicalized and, more importantly, we have to work on the radicalizers***." Postmedia News (National Post, A1, Windsor Star, Vancouver Sun, Leader-Post, Star Phoenix, The Gazette, Edmonton Journal, Ottawa Citizen, Calgary Herald); Postmedia Network (Kingston Whig Standard, B1, London Free Press, B1, Calgary Sun, Toronto Sun, Edmonton Sun, Ottawa Sun); * La Presse (Le Quotidien)

La GRC arrête dix Québécois cherchant à joindre les djihadistes
La Gendarmerie royale du Canada a confirmé mardi soir l'arrestation de dix jeunes citoyens montréalais soupçonnés de vouloir se joindre à des groupes djihadistes. L'équipe intégrée sur la sécurité nationale a mené en fin de semaine l'opération qui a permis de «perturber les intentions» des individus arrêtés, a fait savoir le GRC dans un communiqué. Selon la GRC, l'ensemble des Montréalais interceptés par les forces policières l'ont été à l'aéroport Pierre-Elliott-Trudeau. Les suspects sont soupçonnés d'avoir eu l'intention de quitter le pays pour rallier les rangs de groupes djihadistes. La police confirme avoir rencontré les familles et les proches des jeunes arrêtés. La GRC fait savoir qu'aucune accusation n'a pour l'instant été déposée et que l'enquête est toujours en cours dans cette affaire. Les passeports des 10 jeunes leur ont tous été retirés, ajoute les autorités policières. Dans son communiqué, la GRC se montre solidaire avec les familles des individus arrêtés. (…) Le **ministre de la Sécurité publique et de la Protection civile du Canada, Steven Blaney**, a réagi aux arrestations effectuées au cours de la fin de semaine à Montréal. Il a d'entrée de jeu félicité la Gendarmerie royale du Canada et l'Équipe intégrée de la sécurité nationale pour leur vigilance continue en vue de « ***protéger nos rues et nos collectivités contre la menace terroriste continue*** », fait-il savoir dans un communiqué envoyé aux médias. Presse Canadienne (L'Acadie Nouvelle, 19); Le Devoir

Projets à venir contre la radicalisation
"Il s'agit de jeunes nés chez nous, qui sont allés dans nos établissements d'enseignement. C'est préoccupant au plus haut point. On va présenter une politique très large sur cette question qui comprendra des éléments de prévention et de détection", a lancé le premier ministre hier avant la période de questions. La ministre de la Sécurité publique, Lise Thériault, s'est elle aussi dite troublée par l'interception à l'aéroport de Montréal d'une dizaine de jeunes qui tentaient de quitter le pays pour rejoindre les rangs des djihadistes. Les mesures que Mme Thériault présentera "prochainement" permettront d'ailleurs de mieux former les premiers intervenants, comme les professeurs, pour détecter les "signes de radicalisations." "Les professeurs et les parents doivent être à l'affût", a-t-elle lancé. Le **ministre fédéral de la Sécurité publique, Steven Blaney**, a annoncé qu'une rencontre au sommet avec ses homologues provinciaux aurait lieu au début de l'été pour mettre en commun leurs ressources en matière de prévention de la radicalisation et du terrorisme. Le Journal de Montreal, 16 (Le Journal de Quebec); La Presse; * Presse Canadienne (La Tribune, Le Soleil, La Presse, Le Droit, La Voix de l'Est, Le Nouvelliste)

Radicalization concerns in Quebec on rise
Following the arrests of another 10 youths allegedly on their way to Syria, concern about radicalization in Quebec has reached a new high, both in the upper echelons of government and by parents worried about their own children joining a terrorist group abroad. Premier Philippe Couillard said Wednesday he was worried to the "highest degree" about the situation, and promised to have new measures to prevent radicalization in place "soon" - though he couldn't say when. The new strategy would involve helping parents and educators detect signs of radicalization. "These are youths who were born here and educated in our schools - it's extremely worrisome," Couillard said. (…) The RCMP seized all of their passports but has not laid any charges against them, said Const. Erique Gasse. "The investigation is ongoing - things can change," Gasse said. Neither the RCMP nor the Public Prosecution Service of Canada would say exactly how old or what gender the youths were, or how they were discovered at the Pierre Elliott Trudeau Airport, though **Federal Public Safety Minister Steven Blaney** confirmed it was thanks to a tip from parents. "***This time, thanks to the support of the parents, we were able to prevent (them from leaving)***," **Blaney** said. The RCMP met with all of the families and pleaded on their behalf for privacy. Postmedia News (The Gazette, A4)

*** Stephen Harper makes his way to Montreal for King David Award gala**
As the Victoria Day parliamentary recess draws to a close, Prime Minister Stephen Harper is set to spend the day in Montreal, starting with a midday appearance at the Pierre Elliott Trudeau International Airport, where he'll deliver an announcement alongside Quebec cabinet ministers **Steven Blaney** and Denis Lebel. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Alberta wildfire sparked by burning truck expands**
Fire crews were busy fighting a large wildfire Wednesday after an angry man set his truck on fire in a ditch near Red Earth Creek, RCMP say. Mounties still don't know exactly why the man was so upset, but the fire tripled in size Wednesday and was still growing. It was burning across 338 hectares, about twice the size of Edmonton's Terwillegar Park. Duncan MacDonnell, spokesman for Alberta's Sustainable Resource Development, said 60 firefighters are now fighting the blaze, which was the largest out-of-control fire in the province Wednesday. Edmonton Journal, A11

*** Environnement Canada va s'ajuster**
Environnement Canada et le ministère de la Sécurité publique doivent ajuster le système Québec en alerte pour éviter " de le brûler " auprès de la population et qu'il ne perde de son efficacité. Ce constat survient au lendemain du tout premier message envoyé par la plateforme depuis sa mise en application. Plusieurs auditeurs de la radio et téléspectateurs devant la télévision ont trouvé plutôt intenses les alertes émises pour Québec, mardi, informant la population qu'une menace de tornade était imminente dans certains secteurs. Voix robotisées incompréhensibles, volume assourdissant et répétition abusive du message ont été des motifs de plaintes envoyées aux diffuseurs, obligés par le Conseil de radiodiffusion et des télécommunications canadiennes de transmettre les alertes. Le Quotidien, 22

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Grown-up countries take out own trash
At first blush, the news this week might give Canadians serious pause over Ottawa's anti-terror strategy. The RCMP says officers intercepted 10 young Montrealers on the weekend on suspicion they were jetting off to join ISIL, something of a trend - at least eight junior jihadis have left Quebec since January, many connected to a single college. And then there's Jahanzeb Malik, a 33-year-old from Toronto, who police allege planned a car bombing in downtown Toronto in lieu of jetting off to join ISIL. Ironically enough, police allege, he feared that would get him busted. This too could be part of a pattern. Martin Couture-Rouleau, who in October mowed down two Canadian soldiers in Saint-Jean-sur-Richelieu, killing Warrant Officer Patrice Vincent, had reportedly wanted to travel to the Middle East to join ISIL - but had been stopped at the airport. It's understandable some are wondering why we're implementing these de facto exit controls on people determined to bring down the West and all for which it stands. If they want to leave, should we not thank them and wish them a speedy demise? Would we not prefer these people wreak their havoc overseas? In a word: no... But evidence suggests we are being vigilant, and that it's working. In a world with ISIL in it, that's about all you can hope for. Among the many knocks against the Conservatives' anti-terrorism legislation is that it could actually impede frontline anti-terror efforts: speech restrictions could deter terrorists from helpfully sharing their plans online, or an imam from inviting the RCMP's counter-violent extremism team to interact with a parishioner who's going off the rails. The successes we see this week highlight just what's at stake. Postmedia News (National Post, A1)

Integrated anti-radicalization effort key to defusing threat, experts say
A counterterrorism catch-and release campaign by Canada's national police force may have prevented 10 aspiring *jihadis* from heading off to war, but the roundup at Montréal-Trudeau airport is raising worries about what comes next for radicalized youth. On Wednesday, while federal and provincial political leaders applauded the police work, antiradicalization experts said only an integrated effort involving civilians and police can deal with youth fixated on taking up arms in the Middle East or joining terrorist groups. In Montreal, which has become a *jihadi* recruiting hotbed, the only tool appears to be handcuffs. In the past six months alone, at least seven youth have left the city to join the Islamic State in Syria or Iraq. At least 15 other teenagers and young adults have been arrested pre-emptively. Some have volunteered to be monitored, while others, such as those arrested at the Montreal airport on the weekend, were simply released after having their passports confiscated. Acting on a tip from one or more parents, the RCMP arrested the 10 youth at the airport but have released few other details. An 11th teenager was captured on video being led away from a Montreal home by investigators. None of the teenagers have been identified publicly and no charges were laid. The government may opt not to pursue a criminal case for fear that any public trial could force it to reveal sensitive intelligence methods - a chronic issue in

Canadian counterterrorism cases. The passport confiscations recalled last fall's terror attacks in which two lone-wolf assailants each killed Canadian soldiers after they were thwarted in attempts to travel abroad and possibly join jihadi groups. Officials provided no answer when asked how they might prevent similar backlash in the latest cases. Observers are increasingly asking whether the threat to Canada can be contained if the ranks of extremists and thwarted jihadis continue to grow. The RCMP's terrorism prevention program is designed to intervene before suspects mobilize toward violence, but the details of the program remain murky. In Quebec, Premier Philippe Couillard has promised oft-delayed legislation to deal with radicalization. He said a new law will be presented within weeks, meaning it will be months before any new program is enacted. Globe and Mail, A1

'The kids don't come to us and speak about joining ISIS,' Montreal imam says
For leaders of the Muslim community, news of 10 youths being intercepted while allegedly on their way to Syria is deeply troubling, says imam Salam Elmenyawi, pictured. "In a situation like this, we have no knowledge whatsoever," said Elmenyawi, president of the Muslim Council of Montreal. "The kids don't come to us and speak about joining ISIS, and we have no information from the police or RCMP or CSIS." He said all the imams have spoken against youth travelling abroad to fight, but now they want to know more. The RCMP was to introduce a prevention strategy in December 2014 that would include Muslim leaders. If a youth showed signs of radicalization, he or she would be surrounded by faith leaders, social workers and teachers to work them through it. For reasons unknown, however, the launch has been delayed until the end of 2015. Postmedia News (National Post, A5)

* **Stemming jihadi recruitment**
In the wake of the arrest of 10 young Montrealers suspected of wanting to join jihadist groups overseas, experts say more needs to be done to educate and counter the extremist rhetoric some Canadian youth have been eager to embrace. (...) One expert says it's too soon to say if the arrests in Quebec this year mean the province is a more fertile hotbed for jihad recruiting than other Canadian jurisdictions. Stéphane Leman-Langlois, a professor at Universite Laval in Quebec City, says what is particular about Quebec is the increased surveillance by authorities since two terror attacks last fall with ties to the province. Another factor may be what he calls an anti-Muslim sentiment in the province. "The one thing that stands out is the way the Muslim community is becoming more and more ostracized in Quebec ... " Leman-Langlois said. Educating youth is one key, but so is a clear strategy to fight Islamic State online propaganda, says a Concordia University religion professor. "The best way is to provide a different narrative," said André Gagné, who speaks on religious extremism. "We need as a society to give hope to people, to help them find their meaning and their way." Canadian Press (Hamilton Spectator, A10, The Record, Chronicle-Herald, Red Deer Advocate, Telegraph-Journal, Times & Transcript)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

U.S. border agent was right to shoot B.C. man
A prosecutor in Washington state says a U.S. Border Patrol agent was justified in fatally shooting a 20-year-old Prince George man who crossed the U.S.-Canada border illegally in March and sprayed the agent with bear spray. Whatcom County prosecutor Dave McEachran said the agent retreated as far as he could from Jamison Childress, and warned him that he would have to shoot if the bear spray was deployed. Alberta RCMP in Alberta said Childress was being sought on a murder charge in the killing of 18-year-old Brando Walker. Walker's partially burned body was found on the Tsuu T'ina Nation reserve near Calgary on March 7, although RCMP said he was killed in a Calgary home. The Whatcom County sheriff's office took the lead in investigating the March 19 shooting. Associated Press (Times Colonist, A6, Times & Transcript, Red Deer Advocate)

Un individu de Dixville intercepté avec 80 grammes de cannabis aux douanes
Un jeune homme de Dixville, près de Coaticook, aurait profité de sa double citoyenneté pour transporter de la drogue sur son lieu de travail en territoire américain. Mardi, en avant-midi, les douaniers américains ont interpellé le suspect de 21 ans aux douanes de Norton au Vermont alors qu'il était en possession de 80 grammes de cannabis. De plus, à la suite d'une courte enquête lancée à partir d'informations reçues du public, les policiers du poste de la MRC de Coaticook, de la Sûreté du Québec (SQ), ont pu effectuer

une perquisition en après-midi à son domicile situé sur la route 147. A cet endroit, ils ont trouvé plus de 560 grammes de cannabis, quelques comprimés de méthamphétamines et plus de 1600 $ en liquide. La Tribune

*** Deportation hearing told of alleged terror plot**
A Pakistani man accused of plotting bomb attacks on downtown Toronto lied during his testimony, his deportation hearing was told Wednesday. In closing submissions, government representative Jessica Lourenco called Jahanzeb Malik a terrorist sympathizer bent on committing terrorism in Canada. Malik's lawyer, Anser Farooq, called it suspicious that a police officer's secret recording equipment apparently failed during a key interaction with Malik. Farooq said the government provided no audio and called some of the officer's testimony "fanciful." The government, which wants to deport him, maintains Malik, 33, is an Islamic extremist who tried to recruit the officer for a plot to bomb the U.S. consulate and financial district buildings. Canadian Press (Whitehorse Daily Star, Red Deer Advocate, Times and Transcript, L'Acadie Nouvelle, The Guardian, Cape Breton Post); Postmedia News (National Post, A1, Gazette, Ottawa Citizen, Calgary Herald, Province, Windsor Star, Vancouver Sun, Leader-Post, Edmonton Journal, Star Phoenix); Toronto Star, GT3, Postmedia Network (London free Press, Kingston Whig Standard, Ottawa Sun, Toronto Sun)

*** Four-year sentence imposed for violent sexual assault**
A man who violently raped a woman will serve a four year prison sentence, then faces deportation from Canada. Olabode Abayolmi Olotu, 36, was sentenced Wednesday in Saskatoon provincial court for sexual assault causing bodily harm. The married father of two young children was convicted after a trial earlier this year of raping the 44-yearold woman, whose identity is subject to a publication ban, in the back of his car on April 20, 2014. He and the woman were in a clandestine relationship, but on that occasion, the judge found Olotu forced anal sex on the woman without her consent, leaving her bleeding and bruised. On Wednesday, Crown prosecutor Cory Bliss argued for a sentence of 4 1/2 years in prison. Olotu, originally from Nigeria, is a permanent resident of Canada - but that will change with this conviction. "He's facing deportation as soon as his sentence expires, with no chance of appealing that removal order," Mitchell said in court. "He's the sole breadwinner for the family and it's obviously going to have a massive impact on the entire family." Judge Barry Singer said the Crown was correct that the sentencing range for this offence, because of the injuries and psychological harm, should be higher than three years. He sentenced Olotu to four years in prison. Postmedia Network (Star Phoenix, A7)

*** Man faces lengthy jail term after drugs found in mail**
A Toronto man and Nigerian national is facing a lengthy prison sentence after what looked like a parcel of air valves in the mail instead turned out to be more than $250,000 worth of heroin. The shipment, intercepted by Canada Border Services Agency officers at the International Mail Processing Centre in Mississauga, was replaced by the RCMP as part of a controlled delivery to a home in Etobicoke on July 25, 2011 which led to the arrest of Peter Ukwuaba. He was convicted by Justice Casey Hill last week of importing heroin, conspiracy to import heroin and possession of heroin for the purpose of trafficking. Mississauga News (2015-05-20)

*** Un avantage compétitif pour Domtar**
La papetière obtient son accréditation au programme d'autocotisation qui facilitera son passage aux douanes Domtar fait désormais partie du Programme d'autocotisation des douanes de l'Agence des services frontaliers du Canada (ASFC), un privilège qui simplifiera l'importation de fibres de bois en provenance des États-Unis. L'usine de Windsor devient ainsi la première installation de l'industrie forestière canadienne à obtenir cette accréditation. La Tribune

*** Warn truckers of traffic circle tipping hazard**
An editorial states "Sign, sign, everywhere a sign. The designers of the Herb Gray Parkway should embrace such rock 'n roll lyrics from the 1970s because trucks are doing exactly that - rocking and rolling - as they try to negotiate the traffic circle en route to Highway 401. Yellow hazard signs warning truckers of tipping dangers - used on winding roadways throughout the United States - should be sprinkled liberally along all entrances to the parkway roundabout. In the U.S., they are sometimes referred to as "dancing truck" signs - a whimsical name, but one that truckers understand to mean slow down or find

yourself lying helplessly on your side. The dangers posed by tipping trucks are formidable for vehicles driving alongside transports on the roundabout. The latest truck to tip over there was a tanker carrying 48,000 pounds of grape concentrate. Imagine that landing on the roof of your car. It was the third truck rollover on the roundabout in six weeks. Miraculously, no one has been seriously injured or killed." Postmedia News (Windsor Star)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Spy agencies target mobile phones, app stores to implant spyware**
Canada and its spying partners exploited weaknesses in one of the world's most popular mobile browsers and planned to hack into smartphones via links to Google and Samsung app stores, a top secret document obtained by CBC News shows. Electronic intelligence agencies began targeting UC Browser — a massively popular app in China and India with growing use in North America — in late 2011 after discovering it leaked revealing details about its half-billion users. Their goal, in tapping into UC Browser and also looking for larger app store vulnerabilities, was to collect data on suspected terrorists and other intelligence targets — and, in some cases, implant spyware on targeted smartphones. The 2012 document shows that the surveillance agencies exploited the weaknesses in certain mobile apps in pursuit of their national security interests, but it appears they didn't alert the companies or the public to these weaknesses. That potentially put millions of users in danger of their data being accessed by other governments' agencies, hackers or criminals. CBC News analyzed the top secret document in collaboration with U.S. news site The Intercept, a website that is devoted in part to reporting on the classified documents leaked by U.S. whistleblower Edward Snowden. The so-called Five Eyes intelligence alliance — the spy group comprising Canada, the U.S., Britain, Australia and New Zealand — specifically sought ways to find and hijack data links to servers used by Google and Samsung's mobile app stores, according to the document obtained by Snowden. Over the course of several workshops held in Canada and Australia in late 2011 and early 2012, a joint Five Eyes tradecraft team tried to find ways to implant spyware on smartphones by intercepting the transmissions sent when downloading or updating apps. CBC.ca

LAW ENFORCEMENT / APPLICATION DE LA LOI

Gangs top police survey concerns
Gang activity was at the top of the list of concerns expressed by Saskatoon residents who took part in a survey conducted on behalf of city police. Insightrix Research Limited gathered the most recent data for 2014 and compared the results to surveys conducted in prior years. The city police force hires an independent company to conduct a community satisfaction survey every three years. Overall, the survey found public satisfaction with the police has increased. Under the category of "social disorder" - one of the many different areas measured by the survey - the most common concern was gang activity, at 26.4 per cent. Police chief Clive Weighill said he wasn't surprised. "People are watching what's going on," he said, noting police have responded to 14 shootings so far this year. In 2003, concern about gangs was measured at only five per cent, he said. Police recently formed a "gun and gang" unit by shuffling resources in the criminal investigation division. Weighill said the staff level was increased to look specifically at dismantling and disrupting local gang activity. He declined to go into specifics about the unit's strategy for dealing with gangs, but said its members will continue to work closely with community partners, adding they are "staunch supporters of Str8 up," a program that assists people leaving gang and criminal street lifestyles. Postmedia News (StarPhoenix, A1)

Costly waiting game
Red Deerians are on the hook for $100,000 every year the former RCMP building sits empty. The ex-RCMP site on 49th Street is earmarked for a new provincial courthouse to replace the crowded 1980s-built one just a block away. The previous Progressive Conservative government indicated a new courthouse in Red Deer is a priority and the city's choice for a site might be suitable. But nothing has been set in stone and the change in government has forced the City of Red Deer to step up its advocacy efforts. The city outlined some of the pressing issues in Red Deer, including the need for a new

courthouse, in a letter penned to premier-elect Rachel Notley. The city pays for basic maintenance and heating costs to keep the former police station up and running. The RCMP moved out of the building in April 2011. Red Deer Advocate, A1

RCMP memorial to be at centre of new park

Blacksmith Paul Fontaine of MacDougall Settlement considers it a great honour to be fabricating a steel monument that will be placed in a church park in honour of the three RCMP officers killed in Moncton last year. "I usually make railings and fences, so this is a real dream job for me. It's a chance to do something really meaningful and different," Fontaine said Wednesday as he and his son Luc continued working on the sculpture, which will be unveiled in the new Honour Park at Glad Tidings Church on Mountain Road in Moncton on Sunday, June 7. The steel sculpture has been taking shape at Fontaine's shop, Heritage Wrought Iron Works, for several weeks. It will stand about two metres tall and features three abstract human forms reaching up to the sky. "The three abstract human forms represent the three fallen officers, but they also represent how people in the community look out for each other," Fontaine said. "I think the problems with our society are not economic or political, but spiritual. This sculpture represents a community reaching for the heavens, reaching for the sky." This sculpture is not associated with the official monument to the fallen officers, which is now being designed for the City of Moncton and will be placed on the Riverfront Park. The sculpture was designed by Fontaine and Pastor Paul Pattison of Glad Tidings Pentecostal Church. It is made of steel that has been cut to shape and welded together for a three-dimensional shape. The three human figures stand back-to-back and face in separate directions as they reach toward the heavens. Pattison says the sculpture will be the centrepiece of the church's new Honour Park, a public park dedicated not only to the three RCMP officers but also the Metro Moncton community. The dedication ceremony will be held on Sunday, June 8, immediately following the Sunday service at 10:30 a.m. Pattison said officials from the RCMP and the City of Moncton have been invited to attend. Times & Transcript, A1

City of Moncton unveils design proposals for RCMP monument

The first thing you need to know is nothing unveiled at Moncton City Hall Wednesday night looks exactly like the memorial to three fallen Codiac RCMP members that will ultimately stand on Moncton's riverfront. The second thing you should know is every artist on the short list for the commission to create the memorial expects community input to be a key part of what the final piece will be. The City of Moncton held a public consultation regarding the memorial project Wednesday night, filling the sixth-floor meeting room of city hall to capacity. The five artists who have been shortlisted travelled to Moncton from as nearby as Sussex and as far away as Victoria to present their proposed concepts to the general public, members of city council and the widows of the three police officers. Constables Fabrice Gevaudan, Dave Ross and Douglas Larche were murdered last June 4, as they joined in police efforts to stop a man shooting up a residential neighbourhood in Moncton's northwest end. Two other police officers, Southeast RCMP Const. Darlene Goguen and Codiac RCMP Const.Eric Dubois, were wounded in two other ambushes that night. Mounties and municipal police officers from across the region ultimately captured the gunman 29 hours after the shooting began. Moncton's Justin Bourque is now serving five life sentences for the crimes. Each artist was given somewhat specific instructions of what the monument should include. Times&Transcript, A1; CBC.ca

Report urges better training, tracking use of force by police

Most Canadian police forces still do not collect the right kind of in-depth data on when they resort to pulling their weapons or using force, nor do they receive sufficient mental-health training to de-escalate confrontations that may turn deadly, a new report says. The Star obtained a copy of the research report commissioned by the federal public safety department after the Toronto police shooting of Sammy Yatim in 2013. It takes a comprehensive look at how police forces in Canada and the U.S. track their officers' use of force in encounters between police and the public. Its main conclusion is that despite years of high-profile and critical inquiries into police actions in, for example, the Yatim shooting, the Vancouver police shooting of Paul Boyd, or the RCMP tasering of Robert Dziekanski, a consistent national approach is needed toward documenting when and why officers use force against citizens... Ian McPhail, chairman of the RCMP's civilian watchdog body, said in an interview that a consistent national approach would absolutely be beneficial, but may be seen as too costly to implement. Yet, he said it may lead to a reduction in use of force, pointing to how Taser use by Mounties dropped during the commission's three-

year review of RCMP policies and practices after Dziekanski's death in 2007. The latest report, written by independent consultants John Kiedrowski, Ronald-Frans Melchers, Michael Petrunik and Christopher Maxwell, explores what it says are two of the best approaches to documenting use of force. The goal of both is to provide a 360-degree look at a subject's behaviour as well as the officer's response, and to use consistent definitions of what constitutes "force" to collect narrative data as well as statistics that could be analyzed for trends. In Canada, such analysis could reveal whether use-of-force injury suffered by an officer or a suspect is related to demographic factors such as race or ethnicity, or tied to a police officer's work shift, stress levels or other indicators such as sleep deprivation, it says. Toronto Star, A6

Police seek son of woman found dead

Homicide detectives are searching for the son of a woman found dead in a Richmond home on Tuesday. Richmond RCMP were called at around 3:30 p.m., after family members found the body of 62-year-old Redelma Belisario. The Integrated Homicide Investigation Team says an autopsy is needed to determine the cause of death, but foul play is suspected. IHIT spokeswoman Sgt. Stephanie Ashton said finding the woman's son, Darwin Lescano, 38, is a priority, calling him a suspect in her death. Postmedia News (Vancouver Sun); The Province

Police pursue 30-year-old mystery - RCMP chase new leads in Interlake man's death

Candace Derksen. Steven Pelletier. Myrna Letandre. Derek Kembel. Heather Mallett. Divas Boulanger. All of these Manitoba slaying victims share a common trait - police arrested their accused killers years after the crimes occurred. Now RCMP are hoping to add another name to the list, believing they've made a breakthrough in one of the coldest cases in their files. Michael Kalanza, 80, vanished from the Interlake community of Faulkner in 1985. His remains were found at an old limestone quarry in nearby Spearhill in 1997. A group of Ashern Central School Grade 9 students on a field trip made the discovery. Investigators believe Kalanza was the victim of foul play, although no arrests have been made. But the search for justice isn't finished. RCMP returned to the scene Wednesday, saying officers in the historical case unit recently took a fresh look at the 30-year-old mystery and now have grounds to conduct a renewed search of the site. Nearly two dozen uniformed and civilian members are involved. "These cases are never closed. They don't go into a box in the basement," RCMP spokeswoman Tara Seel said Wednesday. RCMP say they've discovered "new investigate pathways" that are largely based on advances in forensic techniques that weren't available in the late 1990s. Existing DNA samples have been resubmitted for testing, and RCMP hope this week's search might unearth some additional clues to be analyzed. "We've advanced a long way in forensic analysis," said Seel. "We're hoping to find supporting evidence to coincide with the new information we've received." Winnipeg Free Press

Cost of catching senators: $21M

It cost $21 million to find out 10 senators claimed more than $100,000 worth of ineligible expenses, CTV News reports. Auditor General Michael Ferguson's sweeping audit of the Senate has employed 142 auditors, some of them private contractors, according to the broadcaster. The auditors were commissioned to look into the expense claims of 117 current and former senators and reportedly found 10 had committed "serious spending abuses." The CTV report says the findings will be referred to the RCMP for investigation, as they were in the cases of Mike Duffy, Pamela Wallin, Patrick Brazeau and Mac Harb. The audit found problematic claims from about 30 others, but they weren't considered serious enough to warrant police involvement, according to CTV. The senators will be required to repay the money. Ferguson's complete report, due for release the first week of June, is reportedly the most expensive audit ever conducted on Parliament Hill. Postmedia News (Winnipeg Sun, Toronto Sun, Calgary Sun, Ottawa Sun, Edmonton Sun)

Pair charged in series of shootings

B.C.'s gang task force has arrested and charged two men believed to be connected to a series of shootings in Surrey. The Combined Forces Special Enforcement Unit searched a home in Surrey and seized marijuana, four rifles and a handgun. Eighteen-year-old Chandanjot Singh Gill faces several firearms charges and one count of trafficking, while 21-year-old Munroop Hayer has been charged with possession for the purpose of trafficking. Both men are from Surrey. Police say the arrests come a month after a dedicated tip line was launched. Postmedia News (Vancouver Sun, A3); The Province

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Long-term offender sent to halfway house
A designated long-term offender who stabbed a 60-year-old woman outside a Kamloops hospital has been ordered to live in a halfway house. The Parole Board of Canada has ordered Robert Semchuk to live under seven strict conditions after his prison sentence expired Tuesday. The board's written decision says the 51-year-old remains at a high risk to reoffend. Semchuk will be bound by conditions that require him not to consume drugs and alcohol and avoid people involved with criminal activity. In 2009, a B.C. Supreme Court judge named Semchuk a longterm offender and sentenced him to a nine-year prison term, which was shortened to six years with credit for time served. Canadian Press (The Province, A16, Times Colonist)

* **Un homme qui aurait menacé de tuer un gardien veut sortir de prison**
Un criminel récalcitrant qui aurait menacé de trancher la gorge d'un gardien de prison espère recouvrer sa liberté très bientôt. Dès qu'il recevra sa sentence pour avoir tué un homme en 2005. L'avocat de Marc Charrette compte bien faire sortir dès que possible son client, qui a passé presque la moitié de sa vie en prison pour divers délits. L'homme de 51 ans est incarcéré depuis 2005 pour avoir tiré à bout portant sur Jocelyn L'Écuyer dans le stationnement du Motel Oscar à Longueuil, le tuant sur le coup. (...)La Couronne, représentée par MeSylvie Villeneuve, a demandé à la juge Sophie Bourque d'imposer à Charrette une peine de 20 ans pour l'accusation réduite d'homicide involontaire à laquelle il a plaidé coupable en octobre dernier. Compte tenu du temps que l'accusé a déjà passé en détention préventive qui compterait en double, il ne lui resterait que deux ans à purger. (...) Ainsi, une gestionnaire des Services correctionnels canadiens est venue raconter à la cour les séjours tumultueux du quinquagénaire au pénitencier. Marc Charrette est un "cas exceptionnel ", selon la témoin Dominique Dulac. Menacer de trancher la gorge d'un officier, lancer un liquide inconnu en direction des agents correctionnels et couvrir d'excréments le hublot de sa cellule d'isolement ne sont que quelques exemples du "comportement problématique" de M. Charrette entre 2008 et 2010. Il a eu pas moins de 80 rapports d'in-fractions majeures pendant cette période. (...) En 2008, un jury avait condamné Marc Charrette à la prison à vie pour meurtre non prémédité. La Cour d'appel avait ordonné un nouveau procès en 2010. Journal de Montréal, 9 (Journal de Québec)

* **In the courts**
A compilation of offences from Kingston's Ontario Court of Justice for the period of May 4 to 8, 2015. Only sentences that involved a large fine, probation or incarceration are included. (...)Paul Michael Desbien, 30, was convicted of having illegal possession of marijuana while serving a federal sentence at Joyceville Penitentiary. He's since been transferred to Collins Bay Penitentiary and 45 days have been added to the five-year sentence he was already serving for aggravated assault. Federal Crown prosecutor Rachel Stephenson said Desbien was smoking marijuana in his cell in early February and a correctional officer smelled it and searched him, recovering 12.3 grams of it hidden inside his clothes. Defence lawyer Courtney Cottle said Desbien was using the weed for pain relief. She told Justice Allan Letourneau the inmate still suffers the after effects of having previously sustained burns over 65% of his body. But he was not receiving pain medication in prison, according to the defence lawyer. Desbien asked the judge to order **Correctional Service Canada** to provide medication. But Justice Letourneau said that's outside his powers. Kingston Whig-Standard

Un tueur à gages repentant
Un tueur à gages rongé par les remords pour un meurtre commis en 1996 renonce à voir sa peine de prison être réduite de huit ans parce qu'il veut épargner les proches de sa victime. "Si mon père avait été assassiné, je voudrais au moins que le tueur fasse son temps. On ramène cette histoire-là dans les médias ces jours-ci et c'est à cause de moi, parce que j'ai décidé de faire une révision judiciaire. À cause de moi, la famille a à vivre ça. Ça n'a pas de bon sens. Je ne peux pas accepter ça", a lancé André Vincent en Cour hier au palais de justice de Montréal. Dans une volte-face inattendue, l'homme de 44 ans a ainsi mis fin à une procédure qui visait à le libérer de détention huit ans avant la fin de sa peine. Reconnu coupable en 1999 du meurtre de Donald Duval, un homme d'affaires et père de famille sans

histoires, Vincent avait été condamné à la prison à vie sans possibilité de libération conditionnelle avant 25 ans. Or, le Code criminel a déjà prévu qu'après 15 ans de détention, il était possible de demander que cette date de libération soit devancée. Journal de Montréal, 7 (Journal de Québec), * 1, * La Presse (Voix de l'Est, 9)

No pass for killer mom
A murderous stepmother convicted in what the parole board called "Canada's worst case of child abuse" was denied escorted day passes, the Toronto Sun has learned. Marcia Dooley last Wednesday "accepted more responsibility for the violent injuries" she inflicted on her seven-year- old stepson, Randal, the Parole Board of Canada decision stated. Dooley, now 45, said her own childhood abuse "played a significant role" in the killing of Randal, yet she applied for escorted, temporary passes to visit her ailing mom in Scarborough, the board decision stated. "The brief (four-hour) confines of an escorted visit with family -- where Marcia could express her anger--could lead to a very difficult situation," the parole board said. Dooley's bid for escorted, temporary absences for an anger management course was also refused. (…) Marcia and Tony Dooley, now 49, were convicted of second-degree murder in the boy's Sept. 25, 1998, death. Both are now serving life sentences and Marcia -- as the main culprit--was denied parole until 2020, while Tony could apply this year but hasn't so far. Toronto Sun, 3

* **Parole granted in kidnap try**
Aaron Patrick MacDonald has been given full parole for his 2014 conviction for an attempted abduction. In 2012, MacDonald was caught with an imitation assault rifle hiding in the multimillion-dollar home of a mining executive. MacDonald was granted day parole in November 2014 with conditions that he follow psychological counselling, take the medication he has been prescribed and not have contact with the victim or member of the victim's family. His "actions had negative impacts on (the family's) lives, and they have the right to live without fear of any further contact," the Parole Board of Canada wrote in a document announcing the decision. The conditions of his day parole have been upheld for his full parole. Chronicle-Herald, A9

* **DeYoung granted parole**
Jason Kyle DeYoung has been released on parole with renewed special conditions. In 2008, DeYoung was sentenced to seven years in prison in connection with a high-speed chase through Halifax in October 2007. He was convicted of three counts of assaulting police with a weapon, robbery, uttering threats and breach of a recognizance. He was given a statutory release in September 2014 but was back behind bars in February because of failed drug tests and a fight outside a methadone clinic. "(DeYoung's) use of substances and resulting impulsive behaviours contributed directly to the current serious and violent offences, endangering public safety on the busy streets of the city," the Parole Board of Canada wrote in outlining its decision. Chronicle-Herald, A9

Arrêtée pour alcool au volant
L'ancienne agente des services correctionnels audrey Corneau est de retour devant les tribunaux après avoir été sentenciée, en décembre 2013, à une peine de trois ans et demi pour trafic de drogue à la prison de Chicoutimi. (…)L'ancienne agente a fourni un échantillon d'haleine de 217 milligrammes d'alcool par 100 millilitres de sang et a été détenue la nuit suivante sous une accusation de garde et contrôle d'un véhicule automobile avec les facultés affaiblies par l'alcool. Audrey Corneau a comparu cet avant-midi devant le même juge qui l'avait envoyée au pénitencier en décembre 2013. Au moment de l'arrestation, elle bénéficiait d'une libération conditionnelle totale depuis le 22 février après avoir purgé 14 des 42 mois de sa sentence. Elle ne s'expose pas à une révocation de sa libération parce que le délit de garde et contrôle n'est pas punissable d'incarcération, à la première offense. Journal de Québec, S2

Take your sights off gun owners, Mr. Harper
A letter to the editor by former Conservative MP Inky Mark states, "Re: last month's Supreme Court of Canada rejection of Prime Minister Stephen Harper's tough on crime agenda is good for the lawful gun owner. The top court of Canada struck down Harper's mandatory minimums for gun offences. Harper's law was deemed unconstitutional, labelled cruel and unusual. The top court stated that the law "could ensnare people with little or no moral fault" and who pose little danger to the public. Supreme Court Justice Beverley McLachlin wrote: "There exists a cavernous disconnect between the severity of the

licensing-type of offence and the mandatory minimum three-year term of imprisonment." You may ask: how does this decision affect the lawful gun owners of Canada? I've been preaching the same sermon for many years that Bill C-68 criminalizes the lawful gun owner. Harper has broken his election promise to repeal this law many times." Whitehorse Daily Star

*** We are all to blame for Omar Khadr's mistreatment**
An opinion piece states, "The term "Kafkaesque" crossed the threshold into cliché years ago, but at times the word is sorely needed. For a situation to be Kafkaesque, it must be menacingly incomprehensible, with a lone individual thrown into a dangerous but confusing situation. Omar Khadr's ordeal certainly fits that definition. The trial of Omar Khadr - Omar K. in a Kafka work, or an "alien unprivileged enemy belligerent" in Guantanamo code - is a permanent stain on Canada's record. Khadr was raised by a family with ties to Al Qaeda, trained to take up arms, accused of lobbing a grenade at a U.S. soldier at age 15, thrown into a secret prison without adequate legal assistance, beaten and tortured, forced to choose between an unjust plea deal and an unfair trial, until finally, one day 13 years later, he was released on bail. (…)The Conservatives, meanwhile, went to extraordinary lengths in refusing to assist Khadr, interfering with the judicial process and classifying him as an adult offender - all on the Canadian taxpayers' dime. When the Conservatives finally repatriated him, they did so not on principle, but because the U.S. government pressured them to. The Tories' cruelty surplus is more revealing than their fiscal one. But the blame for Khadr's mistreatment rests ultimately with us, the Canadian public. It was a democratically elected government that assisted the torturers, and a repeatedly re-elected government that tried to keep him in the penal colony." Toronto Star, A21

*** Khadr comparison insulting**
A letter to the editor states, "Regarding the letter Bomber must have Canada envy, Comparing the actions of Omar Khadr to those of Dzhokhar Tsarnaev is absolutely ludicrous. But even worse, to state that Elizabeth May, Thomas Mulcair, and the Supreme Court of Canada would support and condone Tsarnaev's killing of innocent citizens is an incredible insult to them all." London Free Press, A7

Don't forget Khadr's victim
A letter to the editor states, "I would suggest those supporting Omar Khadr spend a few minutes talking with the widow of the soldier killed by the grenade (reportedly) thrown by Khadr. Then they could ask her if it matters that he was 15, 25, or 95 years old when the grenade ended her husband's life. If Khadr and his lawyer manage to fleece the Canadian government for wads of cash, they should turn around and give the proceeds to the widow of the American soldier that died of his actions." Winnipeg Free Press, A12

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Eisenberger wants a gun ban after 'wild west' violence
Mayor Fred Eisenberger wants the city to ban guns in urban areas after a brazen "wild west" shootout in downtown Hamilton over the weekend. Eisenberger asked city lawyers Wednesday to report back to council about what the city can legally do - if anything - to curtail gun violence. He later acknowledged he hadn't "fleshed out the constitutional issues." "I think anything we can do to make guns less accessible is a positive step. We ban a lot of things in the city. My question would be 'Can we ban guns?'" he said after a general issues committee meeting. "Most reasonable people would wonder, why are people carrying guns in the first place?" While some U.S. jurisdictions allow citizens to openly carry handguns, Canadian law prevents most people from doing so. Collectors and target shooters must follow strict rules for transporting and storing the weapons. (…)Hamilton police spokesperson Catherine Martin said the service "would support any crime prevention strategy that may be available to the municipality," but didn't specifically comment on the idea of a municipal gun ban. Hamilton Spectator, A1

Changing the conversation
It did not take a sexual harassment scandal on his own turf to focus Concordia University president Alan Shepard's attention on the issue. For one thing, Shepard, who has been president and vice-chancellor of

Concordia since 2012, had ordered a review of Concordia's policies on sexual harassment and sexual assault in December, months before a Concordia student leader took her harassment case to the Quebec Human Rights Commission. And for another, Shepard has been sensitive to issues surrounding sexual assault and consent since his own undergraduate days. (...)Melissa Kate Wheeler, a former president of Concordia's Student Union, is among those pushing for better support for victims at the school. One of her main frustrations is that the Sexual Assault Resource Centre, for which she advocated during her term as president, has not been given the resources it needs to meet its mandate of educating, raising awareness, providing support and crisis intervention. Montreal Gazette, A1

*** Sex assault is a burden for the young**
Here's a fact you'll never forget once you hear it: The peak age for becoming a victim of sexual assault is 15. (...)According to crime expert Wayne Morris, who spoke to the provincial select committee on sexual violence and harassment in Kitchener on Wednesday, sex assault in North America is primarily a young person's burden. Sixty-one per cent of victims of rape, most of them young women, are 17 or younger. Eighty-three per cent are 24 or younger. They tend to have problems perceiving risk in a dangerous situation, said Morris. Perhaps because of that difficulty, they "seem to be especially vulnerable to further attack," he said. Meanwhile, most perpetrators are under 25, likely have a criminal record, and have the idea that men should be dominant and women should be submissive. Waterloo Region Record, B1

*** Power and Control: Sexual Assault Reflects Social Norms**
Canadian society was founded on a colonialist model that supported patriarchy. Men, especially men of privilege, developed a sense of entitlement to exert power and control over certain groups, one of which included girls and women. The basis of rape culture is men believing it's their inherent right to use power and control over girls and women. Historically, predominant ideas, social practices, media, government, schools, religious institutions, employers, the various levels of law enforcement and justice were established by privileged white men. All of these institutions play a role in condoning sexual assault. They accomplish this by normalizing violence against women and reinforcing the myth that the survivor is to blame. Conversely, these institutions can choose to make a difference by supporting women's rights - which, quite simply, are basic human rights. Raise the Hammer

*** 'I kind of feel sick': Teen targeted by cyberbullies speaks out after alleged sexual assault**
A young girl in Atlantic Canada is speaking out along with her parents about cyberbullying and an alleged sexual assault, urging others in similar situations to do the same. CTV News is not identifying the 15-year-old girl because she says she is a victim of sexual assault at the hands of a woman 10 years older than her. "I didn't know what she was doing to me 'cause I was like in shock, I was like frozed," the girl said. "She asked me out, and I said, 'I don't want to date you 'cause I'm not a lesbian,' and she didn't take that for an answer," the girl said. "So like then she grabbed my waist and then she was kissing me and like sticking her tongue down my throat and then she was choking me. And then she grabbed my butt." It took a couple of weeks before the girl told her parents, who immediately reported the alleged assault to police. The family says that's when things got worse. CTV News (2015-05-20)

*** Better police training, reporting on use of force needed, report urges**
Most Canadian police forces still do not collect the right kind of in-depth data on when they resort to pulling their weapons or using force, nor do they receive sufficient mental health training to de-escalate confrontations that may turn deadly, a new report says. The Star obtained a copy of the research report commissioned by the federal **public safety department** after the Toronto police shooting of Sammy Yatim in 2013. It takes a comprehensive look at how police forces in Canada and the U.S. track their officers' use of force in encounters between police and members of the public. Its main conclusion is that, despite years of high-profile and critical inquiries into police actions in, for example, the Yatim shooting, the Vancouver police shooting of Paul Boyd, or the RCMP tasering of Robert Dziekanski, a consistent national approach is needed towards documenting when and why cops use force against citizens. It also urges more substantial mental health training for frontline officers who confront troubled individuals, too, saying the research clearly shows officers who receive extensive training successfully de-escalate tensions and are less likely to use deadly force. The report concludes it's not merely a matter of public safety, but officer safety as well, because police officers often suffer injuries when situations turn violent. Toronto Star

*** Twitter fight partly to blame for Etobicoke students shooting deaths: Report**
A report into the deadly shooting last fall outside Don Bosco Catholic Secondary School blames a Twitter fight among students and a Toronto Community Housing complex nearby for having "drug-activity and gun-related issues." But the report stops short of recommending metal detectors be installed in Toronto Catholic schools, citing "practical, social and legal reasons." The Safe Schools Inquiry Panel Report will be presented Thursday night to TCDSB trustees. But CBC News has obtained an advance copy. The report contains 33 recommendations, some of which include teaching students how to use social media responsibly, reviewing students' use of electronic devices in school and investigating "the feasibility of developing a smartphone-based application that would permit students to anonymously report school-related safety concerns." The report says the mother of one of the slain students proposed the installation of metal detectors and implementation of random searches of students as ways to ensure school safety, but added that "Toronto Police Service and many student representatives appearing before the Panel argued that this not be part of the recommendations, for practical, social and legal reasons." CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER

*** Coquitlam teen admits to swatting**
A Coquitlam teen who prompted numerous “swatting” incidents last year on families around Canada and the U.S. pleaded guilty last week to a dozen more charges. The 17-year-old, who cannot be identified under a publication ban because of his age, has now admitted to a total of 23 offences of extortion, public mischief and criminal harassment. In a day-long sentencing hearing at Port Coquitlam provincial court last Friday, Crown prosecutor Michael Bauer outlined how the teen had terrorized mostly young, female gamers and their parents, in B.C., Minnesota, Utah, Arizona, Ohio and California. He had a consistent pattern of trying to connect with the online gamers — many of them fans of the game League of Legends. But when they denied his requests, he shut down their internet access, posted their personal information online, repeatedly called them late at night and contacted the police in their hometown, posing as someone else. Often, he would tell the police he was holding a family hostage, had napalm bombs or had killed someone in the house. He would demand a ransom, order a SWAT (Special Weapons and Tactics) team — hence the term "swatting" — to show up with a police helicopter, or say he would kill any law enforcement official who intervened, Bauer said. Tri-City News

INTERNATIONAL

*** ISIL victory at Palmyra threatens ruins**
Islamic State of Iraq and the Levant extremists seized almost full control of the ancient Syrian town of Palmyra after government defence lines there collapsed on Wednesday, though it remained unclear how close to the famed archeological site the extremists advanced, activists said. Syrian state TV acknowledged that pro-government forces have withdrawn from Palmyra. The fall of the town to ISIL is a stunning defeat for President Bashar Assad's forces, days after the militants launched their offensive against Palmyra in central Syria. It is also an enormous loss to the government, not only because of its cultural significance, but because it would open the way for extremists to advance to key government-held areas, including Homs and Damascus. National Post, A9; The Globe and Mail

*** BIN LADEN LETTERS SHINE LIGHT INTO INNER WORKINGS OF AL-QAEDA**
The quest to understand Osama bin Laden continues, four years after his death. The U.S. government on Wednesday released a trove of documents allegedly collected from the compound in which the world's most well-known terrorist hid and was killed in 2011. The dump of more than 100 letters, directives and miscellaneous reports (including a partial list of the titles that graced the al-Qaeda leader's bookshelf)

paints a picture of a man simultaneously inhabiting two worlds: one atop a sprawling terror organization; the other a decidedly normal, suburban existence. The Globe and Mail, A10

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
May 21, 2015 / le 21 mai 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Canadian Jihad
An east-end Montreal college is gaining a reputation as a breeding ground for jihadis after four of its students were arrested at the airport Friday, allegedly on the verge of taking off to join an overseas terror group. The latest arrests bring to 11 the number of Collège Maisonneuve students who since January have either left to join jihadi groups overseas or have been arrested on suspicion of planning to leave. The four were among 10 students from various CEGEPS - post-secondary institutions unique to Quebec - and high schools arrested at Pierre Elliott Trudeau Airport Friday, the college confirmed. They are "suspected of wanting to leave the country to join jihadist groups," the RCMP said in a statement. They had their passports confiscated and were released without charge. The police said they spoke to the families and friends of those arrested and the investigation is ongoing. (…) **Federal Public Safety Minister Steven Blaney** announced Wednesday that he will invite his provincial counterparts to an early summer meeting to discuss terrorism and radicalization. "***There is no profile of terrorists. You can come from whatever (income), whether Canadian-born or foreigner, the profile of a terrorist is very diverse***," he told CBC News Network. "***What we need to work on is the motive. We need to be able to identify at an early stage those individuals who are being radicalized and, more importantly, we have to work on the radicalizers***." Postmedia News (National Post, A1, Windsor Star, Vancouver Sun, Leader-Post, Star Phoenix, The Gazette, Edmonton Journal, Ottawa Citizen, Calgary Herald); Postmedia Network (Kingston Whig Standard, B1, London Free Press, B1, Calgary Sun, Toronto Sun, Edmonton Sun, Ottawa Sun); * La Presse (Le Quotidien)

La GRC arrête dix Québécois cherchant à joindre les djihadistes
La Gendarmerie royale du Canada a confirmé mardi soir l'arrestation de dix jeunes citoyens montréalais soupçonnés de vouloir se joindre à des groupes djihadistes. L'équipe intégrée sur la sécurité nationale a mené en fin de semaine l'opération qui a permis de «perturber les intentions» des individus arrêtés, a fait savoir le GRC dans un communiqué. Selon la GRC, l'ensemble des Montréalais interceptés par les forces policières l'ont été à l'aéroport Pierre-Elliott-Trudeau. Les suspects sont soupçonnés d'avoir eu l'intention de quitter le pays pour rallier les rangs de groupes djihadistes. La police confirme avoir rencontré les familles et les proches des jeunes arrêtés. La GRC fait savoir qu'aucune accusation n'a pour l'instant été déposée et que l'enquête est toujours en cours dans cette affaire. Les passeports des 10 jeunes leur ont tous été retirés, ajoute les autorités policières. Dans son communiqué, la GRC se montre solidaire avec les familles des individus arrêtés. (…) Le **ministre de la Sécurité publique et de la Protection civile du Canada, Steven Blaney**, a réagi aux arrestations effectuées au cours de la fin de semaine à Montréal. Il a d'entrée de jeu félicité la Gendarmerie royale du Canada et l'Équipe intégrée de la sécurité nationale pour leur vigilance continue en vue de « ***protéger nos rues et nos collectivités contre la menace terroriste continue*** », fait-il savoir dans un communiqué envoyé aux médias. Presse Canadienne (L'Acadie Nouvelle, 19); Le Devoir

Projets à venir contre la radicalisation
"Il s'agit de jeunes nés chez nous, qui sont allés dans nos établissements d'enseignement. C'est préoccupant au plus haut point. On va présenter une politique très large sur cette question qui comprendra des éléments de prévention et de détection", a lancé le premier ministre hier avant la période de questions. La ministre de la Sécurité publique, Lise Thériault, s'est elle aussi dite troublée par l'interception à l'aéroport de Montréal d'une dizaine de jeunes qui tentaient de quitter le pays pour rejoindre les rangs des djihadistes. Les mesures que Mme Thériault présentera "prochainement" permettront d'ailleurs de mieux former les premiers intervenants, comme les professeurs, pour détecter les "signes de radicalisations." "Les professeurs et les parents doivent être à l'affût", a-t-elle lancé. Le **ministre fédéral de la Sécurité publique, Steven Blaney**, a annoncé qu'une rencontre au sommet avec ses homologues provinciaux aurait lieu au début de l'été pour mettre en commun leurs ressources en matière de prévention de la radicalisation et du terrorisme. Le Journal de Montreal, 16 (Le Journal de Quebec); La Presse; * Presse Canadienne (La Tribune, Le Soleil, La Presse, Le Droit, La Voix de l'Est, Le Nouvelliste)

Radicalization concerns in Quebec on rise
Following the arrests of another 10 youths allegedly on their way to Syria, concern about radicalization in Quebec has reached a new high, both in the upper echelons of government and by parents worried about their own children joining a terrorist group abroad. Premier Philippe Couillard said Wednesday he was worried to the "highest degree" about the situation, and promised to have new measures to prevent radicalization in place "soon" - though he couldn't say when. The new strategy would involve helping parents and educators detect signs of radicalization. "These are youths who were born here and educated in our schools - it's extremely worrisome," Couillard said. (…) The RCMP seized all of their passports but has not laid any charges against them, said Const. Erique Gasse. "The investigation is ongoing - things can change," Gasse said. Neither the RCMP nor the Public Prosecution Service of Canada would say exactly how old or what gender the youths were, or how they were discovered at the Pierre Elliott Trudeau Airport, though **Federal Public Safety Minister Steven Blaney** confirmed it was thanks to a tip from parents. "***This time, thanks to the support of the parents, we were able to prevent (them from leaving)***," **Blaney** said. The RCMP met with all of the families and pleaded on their behalf for privacy. Postmedia News (The Gazette, A4)

*** Stephen Harper makes his way to Montreal for King David Award gala**
As the Victoria Day parliamentary recess draws to a close, Prime Minister Stephen Harper is set to spend the day in Montreal, starting with a midday appearance at the Pierre Elliott Trudeau International Airport, where he'll deliver an announcement alongside Quebec cabinet ministers **Steven Blaney** and Denis Lebel. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Alberta wildfire sparked by burning truck expands**
Fire crews were busy fighting a large wildfire Wednesday after an angry man set his truck on fire in a ditch near Red Earth Creek, RCMP say. Mounties still don't know exactly why the man was so upset, but the fire tripled in size Wednesday and was still growing. It was burning across 338 hectares, about twice the size of Edmonton's Terwillegar Park. Duncan MacDonnell, spokesman for Alberta's Sustainable Resource Development, said 60 firefighters are now fighting the blaze, which was the largest out-of-control fire in the province Wednesday. Edmonton Journal, A11

*** Environnement Canada va s'ajuster**
Environnement Canada et le ministère de la Sécurité publique doivent ajuster le système Québec en alerte pour éviter " de le brûler " auprès de la population et qu'il ne perde de son efficacité. Ce constat survient au lendemain du tout premier message envoyé par la plateforme depuis sa mise en application. Plusieurs auditeurs de la radio et téléspectateurs devant la télévision ont trouvé plutôt intenses les alertes émises pour Québec, mardi, informant la population qu'une menace de tornade était imminente dans certains secteurs. Voix robotisées incompréhensibles, volume assourdissant et répétition abusive du message ont été des motifs de plaintes envoyées aux diffuseurs, obligés par le Conseil de radiodiffusion et des télécommunications canadiennes de transmettre les alertes. Le Quotidien, 22

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Grown-up countries take out own trash
At first blush, the news this week might give Canadians serious pause over Ottawa's anti-terror strategy. The RCMP says officers intercepted 10 young Montrealers on the weekend on suspicion they were jetting off to join ISIL, something of a trend - at least eight junior jihadis have left Quebec since January, many connected to a single college. And then there's Jahanzeb Malik, a 33-year-old from Toronto, who police allege planned a car bombing in downtown Toronto in lieu of jetting off to join ISIL. Ironically enough, police allege, he feared that would get him busted. This too could be part of a pattern. Martin Couture-Rouleau, who in October mowed down two Canadian soldiers in Saint-Jean-sur-Richelieu, killing Warrant Officer Patrice Vincent, had reportedly wanted to travel to the Middle East to join ISIL - but had been stopped at the airport. It's understandable some are wondering why we're implementing these de facto exit controls on people determined to bring down the West and all for which it stands. If they want to leave, should we not thank them and wish them a speedy demise? Would we not prefer these people wreak their havoc overseas? In a word: no... But evidence suggests we are being vigilant, and that it's working. In a world with ISIL in it, that's about all you can hope for. Among the many knocks against the Conservatives' anti-terrorism legislation is that it could actually impede frontline anti-terror efforts: speech restrictions could deter terrorists from helpfully sharing their plans online, or an imam from inviting the RCMP's counter-violent extremism team to interact with a parishioner who's going off the rails. The successes we see this week highlight just what's at stake. Postmedia News (National Post, A1)

Integrated anti-radicalization effort key to defusing threat, experts say
A counterterrorism catch-and release campaign by Canada's national police force may have prevented 10 aspiring *jihadis* from heading off to war, but the roundup at Montréal-Trudeau airport is raising worries about what comes next for radicalized youth. On Wednesday, while federal and provincial political leaders applauded the police work, antiradicalization experts said only an integrated effort involving civilians and police can deal with youth fixated on taking up arms in the Middle East or joining terrorist groups. In Montreal, which has become a *jihadi* recruiting hotbed, the only tool appears to be handcuffs. In the past six months alone, at least seven youth have left the city to join the Islamic State in Syria or Iraq. At least 15 other teenagers and young adults have been arrested pre-emptively. Some have volunteered to be monitored, while others, such as those arrested at the Montreal airport on the weekend, were simply released after having their passports confiscated. Acting on a tip from one or more parents, the RCMP arrested the 10 youth at the airport but have released few other details. An 11th teenager was captured on video being led away from a Montreal home by investigators. None of the teenagers have been identified publicly and no charges were laid. The government may opt not to pursue a criminal case for fear that any public trial could force it to reveal sensitive intelligence methods - a chronic issue in

Canadian counterterrorism cases. The passport confiscations recalled last fall's terror attacks in which two lone-wolf assailants each killed Canadian soldiers after they were thwarted in attempts to travel abroad and possibly join jihadi groups. Officials provided no answer when asked how they might prevent similar backlash in the latest cases. Observers are increasingly asking whether the threat to Canada can be contained if the ranks of extremists and thwarted jihadis continue to grow. The RCMP's terrorism prevention program is designed to intervene before suspects mobilize toward violence, but the details of the program remain murky. In Quebec, Premier Philippe Couillard has promised oft-delayed legislation to deal with radicalization. He said a new law will be presented within weeks, meaning it will be months before any new program is enacted. Globe and Mail, A1

'The kids don't come to us and speak about joining ISIS,' Montreal imam says
For leaders of the Muslim community, news of 10 youths being intercepted while allegedly on their way to Syria is deeply troubling, says imam Salam Elmenyawi, pictured. "In a situation like this, we have no knowledge whatsoever," said Elmenyawi, president of the Muslim Council of Montreal. "The kids don't come to us and speak about joining ISIS, and we have no information from the police or RCMP or CSIS." He said all the imams have spoken against youth travelling abroad to fight, but now they want to know more. The RCMP was to introduce a prevention strategy in December 2014 that would include Muslim leaders. If a youth showed signs of radicalization, he or she would be surrounded by faith leaders, social workers and teachers to work them through it. For reasons unknown, however, the launch has been delayed until the end of 2015. Postmedia News (National Post, A5)

* **Stemming jihadi recruitment**
In the wake of the arrest of 10 young Montrealers suspected of wanting to join jihadist groups overseas, experts say more needs to be done to educate and counter the extremist rhetoric some Canadian youth have been eager to embrace. (...) One expert says it's too soon to say if the arrests in Quebec this year mean the province is a more fertile hotbed for jihad recruiting than other Canadian jurisdictions. Stéphane Leman-Langlois, a professor at Universite Laval in Quebec City, says what is particular about Quebec is the increased surveillance by authorities since two terror attacks last fall with ties to the province. Another factor may be what he calls an anti-Muslim sentiment in the province. "The one thing that stands out is the way the Muslim community is becoming more and more ostracized in Quebec ... " Leman-Langlois said. Educating youth is one key, but so is a clear strategy to fight Islamic State online propaganda, says a Concordia University religion professor. "The best way is to provide a different narrative," said André Gagné, who speaks on religious extremism. "We need as a society to give hope to people, to help them find their meaning and their way." Canadian Press (Hamilton Spectator, A10, The Record, Chronicle-Herald, Red Deer Advocate, Telegraph-Journal, Times & Transcript)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

U.S. border agent was right to shoot B.C. man
A prosecutor in Washington state says a U.S. Border Patrol agent was justified in fatally shooting a 20-year-old Prince George man who crossed the U.S.-Canada border illegally in March and sprayed the agent with bear spray. Whatcom County prosecutor Dave McEachran said the agent retreated as far as he could from Jamison Childress, and warned him that he would have to shoot if the bear spray was deployed. Alberta RCMP in Alberta said Childress was being sought on a murder charge in the killing of 18-year-old Brando Walker. Walker's partially burned body was found on the Tsuu T'ina Nation reserve near Calgary on March 7, although RCMP said he was killed in a Calgary home. The Whatcom County sheriff's office took the lead in investigating the March 19 shooting. Associated Press (Times Colonist, A6, Times & Transcript, Red Deer Advocate)

Un individu de Dixville intercepté avec 80 grammes de cannabis aux douanes
Un jeune homme de Dixville, près de Coaticook, aurait profité de sa double citoyenneté pour transporter de la drogue sur son lieu de travail en territoire américain. Mardi, en avant-midi, les douaniers américains ont interpellé le suspect de 21 ans aux douanes de Norton au Vermont alors qu'il était en possession de 80 grammes de cannabis. De plus, à la suite d'une courte enquête lancée à partir d'informations reçues du public, les policiers du poste de la MRC de Coaticook, de la Sûreté du Québec (SQ), ont pu effectuer

une perquisition en après-midi à son domicile situé sur la route 147. A cet endroit, ils ont trouvé plus de 560 grammes de cannabis, quelques comprimés de méthamphétamines et plus de 1600 $ en liquide. La Tribune

*** Deportation hearing told of alleged terror plot**
A Pakistani man accused of plotting bomb attacks on downtown Toronto lied during his testimony, his deportation hearing was told Wednesday. In closing submissions, government representative Jessica Lourenco called Jahanzeb Malik a terrorist sympathizer bent on committing terrorism in Canada. Malik's lawyer, Anser Farooq, called it suspicious that a police officer's secret recording equipment apparently failed during a key interaction with Malik. Farooq said the government provided no audio and called some of the officer's testimony "fanciful." The government, which wants to deport him, maintains Malik, 33, is an Islamic extremist who tried to recruit the officer for a plot to bomb the U.S. consulate and financial district buildings. Canadian Press (Whitehorse Daily Star, Red Deer Advocate, Times and Transcript, L'Acadie Nouvelle, The Guardian, Cape Breton Post); Postmedia News (National Post, A1, Gazette, Ottawa Citizen, Calgary Herald, Province, Windsor Star, Vancouver Sun, Leader-Post, Edmonton Journal, Star Phoenix); Toronto Star, GT3, Postmedia Network (London free Press, Kingston Whig Standard, Ottawa Sun, Toronto Sun)

*** Four-year sentence imposed for violent sexual assault**
A man who violently raped a woman will serve a four year prison sentence, then faces deportation from Canada. Olabode Abayolmi Olotu, 36, was sentenced Wednesday in Saskatoon provincial court for sexual assault causing bodily harm. The married father of two young children was convicted after a trial earlier this year of raping the 44-yearold woman, whose identity is subject to a publication ban, in the back of his car on April 20, 2014. He and the woman were in a clandestine relationship, but on that occasion, the judge found Olotu forced anal sex on the woman without her consent, leaving her bleeding and bruised. On Wednesday, Crown prosecutor Cory Bliss argued for a sentence of 4 1/2 years in prison. Olotu, originally from Nigeria, is a permanent resident of Canada - but that will change with this conviction. "He's facing deportation as soon as his sentence expires, with no chance of appealing that removal order," Mitchell said in court. "He's the sole breadwinner for the family and it's obviously going to have a massive impact on the entire family." Judge Barry Singer said the Crown was correct that the sentencing range for this offence, because of the injuries and psychological harm, should be higher than three years. He sentenced Olotu to four years in prison. Postmedia Network (Star Phoenix, A7)

*** Man faces lengthy jail term after drugs found in mail**
A Toronto man and Nigerian national is facing a lengthy prison sentence after what looked like a parcel of air valves in the mail instead turned out to be more than $250,000 worth of heroin. The shipment, intercepted by Canada Border Services Agency officers at the International Mail Processing Centre in Mississauga, was replaced by the RCMP as part of a controlled delivery to a home in Etobicoke on July 25, 2011 which led to the arrest of Peter Ukwuaba. He was convicted by Justice Casey Hill last week of importing heroin, conspiracy to import heroin and possession of heroin for the purpose of trafficking. Mississauga News (2015-05-20)

*** Un avantage compétitif pour Domtar**
La papetière obtient son accréditation au programme d'autocotisation qui facilitera son passage aux douanes Domtar fait désormais partie du Programme d'autocotisation des douanes de l'Agence des services frontaliers du Canada (ASFC), un privilège qui simplifiera l'importation de fibres de bois en provenance des États-Unis. L'usine de Windsor devient ainsi la première installation de l'industrie forestière canadienne à obtenir cette accréditation. La Tribune

*** Warn truckers of traffic circle tipping hazard**
An editorial states "Sign, sign, everywhere a sign. The designers of the Herb Gray Parkway should embrace such rock 'n roll lyrics from the 1970s because trucks are doing exactly that - rocking and rolling - as they try to negotiate the traffic circle en route to Highway 401. Yellow hazard signs warning truckers of tipping dangers - used on winding roadways throughout the United States - should be sprinkled liberally along all entrances to the parkway roundabout. In the U.S., they are sometimes referred to as "dancing truck" signs - a whimsical name, but one that truckers understand to mean slow down or find

yourself lying helplessly on your side. The dangers posed by tipping trucks are formidable for vehicles driving alongside transports on the roundabout. The latest truck to tip over there was a tanker carrying 48,000 pounds of grape concentrate. Imagine that landing on the roof of your car. It was the third truck rollover on the roundabout in six weeks. Miraculously, no one has been seriously injured or killed." Postmedia News (Windsor Star)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Spy agencies target mobile phones, app stores to implant spyware**
Canada and its spying partners exploited weaknesses in one of the world's most popular mobile browsers and planned to hack into smartphones via links to Google and Samsung app stores, a top secret document obtained by CBC News shows. Electronic intelligence agencies began targeting UC Browser — a massively popular app in China and India with growing use in North America — in late 2011 after discovering it leaked revealing details about its half-billion users. Their goal, in tapping into UC Browser and also looking for larger app store vulnerabilities, was to collect data on suspected terrorists and other intelligence targets — and, in some cases, implant spyware on targeted smartphones. The 2012 document shows that the surveillance agencies exploited the weaknesses in certain mobile apps in pursuit of their national security interests, but it appears they didn't alert the companies or the public to these weaknesses. That potentially put millions of users in danger of their data being accessed by other governments' agencies, hackers or criminals. CBC News analyzed the top secret document in collaboration with U.S. news site The Intercept, a website that is devoted in part to reporting on the classified documents leaked by U.S. whistleblower Edward Snowden. The so-called Five Eyes intelligence alliance — the spy group comprising Canada, the U.S., Britain, Australia and New Zealand — specifically sought ways to find and hijack data links to servers used by Google and Samsung's mobile app stores, according to the document obtained by Snowden. Over the course of several workshops held in Canada and Australia in late 2011 and early 2012, a joint Five Eyes tradecraft team tried to find ways to implant spyware on smartphones by intercepting the transmissions sent when downloading or updating apps. CBC.ca

LAW ENFORCEMENT / APPLICATION DE LA LOI

Gangs top police survey concerns
Gang activity was at the top of the list of concerns expressed by Saskatoon residents who took part in a survey conducted on behalf of city police. Insightrix Research Limited gathered the most recent data for 2014 and compared the results to surveys conducted in prior years. The city police force hires an independent company to conduct a community satisfaction survey every three years. Overall, the survey found public satisfaction with the police has increased. Under the category of "social disorder" - one of the many different areas measured by the survey - the most common concern was gang activity, at 26.4 per cent. Police chief Clive Weighill said he wasn't surprised. "People are watching what's going on," he said, noting police have responded to 14 shootings so far this year. In 2003, concern about gangs was measured at only five per cent, he said. Police recently formed a "gun and gang" unit by shuffling resources in the criminal investigation division. Weighill said the staff level was increased to look specifically at dismantling and disrupting local gang activity. He declined to go into specifics about the unit's strategy for dealing with gangs, but said its members will continue to work closely with community partners, adding they are "staunch supporters of Str8 up," a program that assists people leaving gang and criminal street lifestyles. Postmedia News (StarPhoenix, A1)

Costly waiting game
Red Deerians are on the hook for $100,000 every year the former RCMP building sits empty. The ex-RCMP site on 49th Street is earmarked for a new provincial courthouse to replace the crowded 1980s-built one just a block away. The previous Progressive Conservative government indicated a new courthouse in Red Deer is a priority and the city's choice for a site might be suitable. But nothing has been set in stone and the change in government has forced the City of Red Deer to step up its advocacy efforts. The city outlined some of the pressing issues in Red Deer, including the need for a new

courthouse, in a letter penned to premier-elect Rachel Notley. The city pays for basic maintenance and heating costs to keep the former police station up and running. The RCMP moved out of the building in April 2011. Red Deer Advocate, A1

RCMP memorial to be at centre of new park

Blacksmith Paul Fontaine of MacDougall Settlement considers it a great honour to be fabricating a steel monument that will be placed in a church park in honour of the three RCMP officers killed in Moncton last year. "I usually make railings and fences, so this is a real dream job for me. It's a chance to do something really meaningful and different," Fontaine said Wednesday as he and his son Luc continued working on the sculpture, which will be unveiled in the new Honour Park at Glad Tidings Church on Mountain Road in Moncton on Sunday, June 7. The steel sculpture has been taking shape at Fontaine's shop, Heritage Wrought Iron Works, for several weeks. It will stand about two metres tall and features three abstract human forms reaching up to the sky. "The three abstract human forms represent the three fallen officers, but they also represent how people in the community look out for each other," Fontaine said. "I think the problems with our society are not economic or political, but spiritual. This sculpture represents a community reaching for the heavens, reaching for the sky." This sculpture is not associated with the official monument to the fallen officers, which is now being designed for the City of Moncton and will be placed on the Riverfront Park. The sculpture was designed by Fontaine and Pastor Paul Pattison of Glad Tidings Pentecostal Church. It is made of steel that has been cut to shape and welded together for a three-dimensional shape. The three human figures stand back-to-back and face in separate directions as they reach toward the heavens. Pattison says the sculpture will be the centrepiece of the church's new Honour Park, a public park dedicated not only to the three RCMP officers but also the Metro Moncton community. The dedication ceremony will be held on Sunday, June 8, immediately following the Sunday service at 10:30 a.m. Pattison said officials from the RCMP and the City of Moncton have been invited to attend. Times & Transcript, A1

City of Moncton unveils design proposals for RCMP monument

The first thing you need to know is nothing unveiled at Moncton City Hall Wednesday night looks exactly like the memorial to three fallen Codiac RCMP members that will ultimately stand on Moncton's riverfront. The second thing you should know is every artist on the short list for the commission to create the memorial expects community input to be a key part of what the final piece will be. The City of Moncton held a public consultation regarding the memorial project Wednesday night, filling the sixth-floor meeting room of city hall to capacity. The five artists who have been shortlisted travelled to Moncton from as nearby as Sussex and as far away as Victoria to present their proposed concepts to the general public, members of city council and the widows of the three police officers. Constables Fabrice Gevaudan, Dave Ross and Douglas Larche were murdered last June 4, as they joined in police efforts to stop a man shooting up a residential neighbourhood in Moncton's northwest end. Two other police officers, Southeast RCMP Const. Darlene Goguen and Codiac RCMP Const.Eric Dubois, were wounded in two other ambushes that night. Mounties and municipal police officers from across the region ultimately captured the gunman 29 hours after the shooting began. Moncton's Justin Bourque is now serving five life sentences for the crimes. Each artist was given somewhat specific instructions of what the monument should include. Times&Transcript, A1; CBC.ca

Report urges better training, tracking use of force by police

Most Canadian police forces still do not collect the right kind of in-depth data on when they resort to pulling their weapons or using force, nor do they receive sufficient mental-health training to de-escalate confrontations that may turn deadly, a new report says. The Star obtained a copy of the research report commissioned by the federal public safety department after the Toronto police shooting of Sammy Yatim in 2013. It takes a comprehensive look at how police forces in Canada and the U.S. track their officers' use of force in encounters between police and the public. Its main conclusion is that despite years of high-profile and critical inquiries into police actions in, for example, the Yatim shooting, the Vancouver police shooting of Paul Boyd, or the RCMP tasering of Robert Dziekanski, a consistent national approach is needed toward documenting when and why officers use force against citizens... Ian McPhail, chairman of the RCMP's civilian watchdog body, said in an interview that a consistent national approach would absolutely be beneficial, but may be seen as too costly to implement. Yet, he said it may lead to a reduction in use of force, pointing to how Taser use by Mounties dropped during the commission's three-

year review of RCMP policies and practices after Dziekanski's death in 2007. The latest report, written by independent consultants John Kiedrowski, Ronald-Frans Melchers, Michael Petrunik and Christopher Maxwell, explores what it says are two of the best approaches to documenting use of force. The goal of both is to provide a 360-degree look at a subject's behaviour as well as the officer's response, and to use consistent definitions of what constitutes "force" to collect narrative data as well as statistics that could be analyzed for trends. In Canada, such analysis could reveal whether use-of-force injury suffered by an officer or a suspect is related to demographic factors such as race or ethnicity, or tied to a police officer's work shift, stress levels or other indicators such as sleep deprivation, it says. Toronto Star, A6

Police seek son of woman found dead

Homicide detectives are searching for the son of a woman found dead in a Richmond home on Tuesday. Richmond RCMP were called at around 3:30 p.m., after family members found the body of 62-year-old Redelma Belisario. The Integrated Homicide Investigation Team says an autopsy is needed to determine the cause of death, but foul play is suspected. IHIT spokeswoman Sgt. Stephanie Ashton said finding the woman's son, Darwin Lescano, 38, is a priority, calling him a suspect in her death. Postmedia News (Vancouver Sun); The Province

Police pursue 30-year-old mystery - RCMP chase new leads in Interlake man's death

Candace Derksen. Steven Pelletier. Myrna Letandre. Derek Kembel. Heather Mallett. Divas Boulanger. All of these Manitoba slaying victims share a common trait - police arrested their accused killers years after the crimes occurred. Now RCMP are hoping to add another name to the list, believing they've made a breakthrough in one of the coldest cases in their files. Michael Kalanza, 80, vanished from the Interlake community of Faulkner in 1985. His remains were found at an old limestone quarry in nearby Spearhill in 1997. A group of Ashern Central School Grade 9 students on a field trip made the discovery. Investigators believe Kalanza was the victim of foul play, although no arrests have been made. But the search for justice isn't finished. RCMP returned to the scene Wednesday, saying officers in the historical case unit recently took a fresh look at the 30-year-old mystery and now have grounds to conduct a renewed search of the site. Nearly two dozen uniformed and civilian members are involved. "These cases are never closed. They don't go into a box in the basement," RCMP spokeswoman Tara Seel said Wednesday. RCMP say they've discovered "new investigate pathways" that are largely based on advances in forensic techniques that weren't available in the late 1990s. Existing DNA samples have been resubmitted for testing, and RCMP hope this week's search might unearth some additional clues to be analyzed. "We've advanced a long way in forensic analysis," said Seel. "We're hoping to find supporting evidence to coincide with the new information we've received." Winnipeg Free Press

Cost of catching senators: $21M

It cost $21 million to find out 10 senators claimed more than $100,000 worth of ineligible expenses, CTV News reports. Auditor General Michael Ferguson's sweeping audit of the Senate has employed 142 auditors, some of them private contractors, according to the broadcaster. The auditors were commissioned to look into the expense claims of 117 current and former senators and reportedly found 10 had committed "serious spending abuses." The CTV report says the findings will be referred to the RCMP for investigation, as they were in the cases of Mike Duffy, Pamela Wallin, Patrick Brazeau and Mac Harb. The audit found problematic claims from about 30 others, but they weren't considered serious enough to warrant police involvement, according to CTV. The senators will be required to repay the money. Ferguson's complete report, due for release the first week of June, is reportedly the most expensive audit ever conducted on Parliament Hill. Postmedia News (Winnipeg Sun, Toronto Sun, Calgary Sun, Ottawa Sun, Edmonton Sun)

Pair charged in series of shootings

B.C.'s gang task force has arrested and charged two men believed to be connected to a series of shootings in Surrey. The Combined Forces Special Enforcement Unit searched a home in Surrey and seized marijuana, four rifles and a handgun. Eighteen-year-old Chandanjot Singh Gill faces several firearms charges and one count of trafficking, while 21-year-old Munroop Hayer has been charged with possession for the purpose of trafficking. Both men are from Surrey. Police say the arrests come a month after a dedicated tip line was launched. Postmedia News (Vancouver Sun, A3); The Province

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Long-term offender sent to halfway house
A designated long-term offender who stabbed a 60-year-old woman outside a Kamloops hospital has been ordered to live in a halfway house. The Parole Board of Canada has ordered Robert Semchuk to live under seven strict conditions after his prison sentence expired Tuesday. The board's written decision says the 51-year-old remains at a high risk to reoffend. Semchuk will be bound by conditions that require him not to consume drugs and alcohol and avoid people involved with criminal activity. In 2009, a B.C. Supreme Court judge named Semchuk a longterm offender and sentenced him to a nine-year prison term, which was shortened to six years with credit for time served. Canadian Press (The Province, A16, Times Colonist)

* **Un homme qui aurait menacé de tuer un gardien veut sortir de prison**
Un criminel récalcitrant qui aurait menacé de trancher la gorge d'un gardien de prison espère recouvrer sa liberté très bientôt. Dès qu'il recevra sa sentence pour avoir tué un homme en 2005. L'avocat de Marc Charrette compte bien faire sortir dès que possible son client, qui a passé presque la moitié de sa vie en prison pour divers délits. L'homme de 51 ans est incarcéré depuis 2005 pour avoir tiré à bout portant sur Jocelyn L'Écuyer dans le stationnement du Motel Oscar à Longueuil, le tuant sur le coup. (...)La Couronne, représentée par MeSylvie Villeneuve, a demandé à la juge Sophie Bourque d'imposer à Charrette une peine de 20 ans pour l'accusation réduite d'homicide involontaire à laquelle il a plaidé coupable en octobre dernier. Compte tenu du temps que l'accusé a déjà passé en détention préventive qui compterait en double, il ne lui resterait que deux ans à purger. (...) Ainsi, une gestionnaire des Services correctionnels canadiens est venue raconter à la cour les séjours tumultueux du quinquagénaire au pénitencier. Marc Charrette est un "cas exceptionnel ", selon la témoin Dominique Dulac. Menacer de trancher la gorge d'un officier, lancer un liquide inconnu en direction des agents correctionnels et couvrir d'excréments le hublot de sa cellule d'isolement ne sont que quelques exemples du "comportement problématique" de M. Charrette entre 2008 et 2010. Il a eu pas moins de 80 rapports d'in-fractions majeures pendant cette période. (...) En 2008, un jury avait condamné Marc Charrette à la prison à vie pour meurtre non prémédité. La Cour d'appel avait ordonné un nouveau procès en 2010. Journal de Montréal, 9 (Journal de Québec)

* **In the courts**
A compilation of offences from Kingston's Ontario Court of Justice for the period of May 4 to 8, 2015. Only sentences that involved a large fine, probation or incarceration are included. (...)Paul Michael Desbien, 30, was convicted of having illegal possession of marijuana while serving a federal sentence at Joyceville Penitentiary. He's since been transferred to Collins Bay Penitentiary and 45 days have been added to the five-year sentence he was already serving for aggravated assault. Federal Crown prosecutor Rachel Stephenson said Desbien was smoking marijuana in his cell in early February and a correctional officer smelled it and searched him, recovering 12.3 grams of it hidden inside his clothes. Defence lawyer Courtney Cottle said Desbien was using the weed for pain relief. She told Justice Allan Letourneau the inmate still suffers the after effects of having previously sustained burns over 65% of his body. But he was not receiving pain medication in prison, according to the defence lawyer. Desbien asked the judge to order **Correctional Service Canada** to provide medication. But Justice Letourneau said that's outside his powers. Kingston Whig-Standard

Un tueur à gages repentant
Un tueur à gages rongé par les remords pour un meurtre commis en 1996 renonce à voir sa peine de prison être réduite de huit ans parce qu'il veut épargner les proches de sa victime. "Si mon père avait été assassiné, je voudrais au moins que le tueur fasse son temps. On ramène cette histoire-là dans les médias ces jours-ci et c'est à cause de moi, parce que j'ai décidé de faire une révision judiciaire. À cause de moi, la famille a à vivre ça. Ça n'a pas de bon sens. Je ne peux pas accepter ça", a lancé André Vincent en Cour hier au palais de justice de Montréal. Dans une volte-face inattendue, l'homme de 44 ans a ainsi mis fin à une procédure qui visait à le libérer de détention huit ans avant la fin de sa peine. Reconnu coupable en 1999 du meurtre de Donald Duval, un homme d'affaires et père de famille sans

histoires, Vincent avait été condamné à la prison à vie sans possibilité de libération conditionnelle avant 25 ans. Or, le Code criminel a déjà prévu qu'après 15 ans de détention, il était possible de demander que cette date de libération soit devancée. Journal de Montréal, 7 (Journal de Québec), * 1, * La Presse (Voix de l'Est, 9)

No pass for killer mom
A murderous stepmother convicted in what the parole board called "Canada's worst case of child abuse" was denied escorted day passes, the Toronto Sun has learned. Marcia Dooley last Wednesday "accepted more responsibility for the violent injuries" she inflicted on her seven-year- old stepson, Randal, the Parole Board of Canada decision stated. Dooley, now 45, said her own childhood abuse "played a significant role" in the killing of Randal, yet she applied for escorted, temporary passes to visit her ailing mom in Scarborough, the board decision stated. "The brief (four-hour) confines of an escorted visit with family -- where Marcia could express her anger--could lead to a very difficult situation," the parole board said. Dooley's bid for escorted, temporary absences for an anger management course was also refused. (…) Marcia and Tony Dooley, now 49, were convicted of second-degree murder in the boy's Sept. 25, 1998, death. Both are now serving life sentences and Marcia -- as the main culprit--was denied parole until 2020, while Tony could apply this year but hasn't so far. Toronto Sun, 3

* **Parole granted in kidnap try**
Aaron Patrick MacDonald has been given full parole for his 2014 conviction for an attempted abduction. In 2012, MacDonald was caught with an imitation assault rifle hiding in the multimillion-dollar home of a mining executive. MacDonald was granted day parole in November 2014 with conditions that he follow psychological counselling, take the medication he has been prescribed and not have contact with the victim or member of the victim's family. His "actions had negative impacts on (the family's) lives, and they have the right to live without fear of any further contact," the Parole Board of Canada wrote in a document announcing the decision. The conditions of his day parole have been upheld for his full parole. Chronicle-Herald, A9

* **DeYoung granted parole**
Jason Kyle DeYoung has been released on parole with renewed special conditions. In 2008, DeYoung was sentenced to seven years in prison in connection with a high-speed chase through Halifax in October 2007. He was convicted of three counts of assaulting police with a weapon, robbery, uttering threats and breach of a recognizance. He was given a statutory release in September 2014 but was back behind bars in February because of failed drug tests and a fight outside a methadone clinic. "(DeYoung's) use of substances and resulting impulsive behaviours contributed directly to the current serious and violent offences, endangering public safety on the busy streets of the city," the Parole Board of Canada wrote in outlining its decision. Chronicle-Herald, A9

Arrêtée pour alcool au volant
L'ancienne agente des services correctionnels audrey Corneau est de retour devant les tribunaux après avoir été sentenciée, en décembre 2013, à une peine de trois ans et demi pour trafic de drogue à la prison de Chicoutimi. (…)L'ancienne agente a fourni un échantillon d'haleine de 217 milligrammes d'alcool par 100 millilitres de sang et a été détenue la nuit suivante sous une accusation de garde et contrôle d'un véhicule automobile avec les facultés affaiblies par l'alcool. Audrey Corneau a comparu cet avant-midi devant le même juge qui l'avait envoyée au pénitencier en décembre 2013. Au moment de l'arrestation, elle bénéficiait d'une libération conditionnelle totale depuis le 22 février après avoir purgé 14 des 42 mois de sa sentence. Elle ne s'expose pas à une révocation de sa libération parce que le délit de garde et contrôle n'est pas punissable d'incarcération, à la première offense. Journal de Québec, S2

Take your sights off gun owners, Mr. Harper
A letter to the editor by former Conservative MP Inky Mark states, "Re: last month's Supreme Court of Canada rejection of Prime Minister Stephen Harper's tough on crime agenda is good for the lawful gun owner. The top court of Canada struck down Harper's mandatory minimums for gun offences. Harper's law was deemed unconstitutional, labelled cruel and unusual. The top court stated that the law "could ensnare people with little or no moral fault" and who pose little danger to the public. Supreme Court Justice Beverley McLachlin wrote: "There exists a cavernous disconnect between the severity of the

licensing-type of offence and the mandatory minimum three-year term of imprisonment." You may ask: how does this decision affect the lawful gun owners of Canada? I've been preaching the same sermon for many years that Bill C-68 criminalizes the lawful gun owner. Harper has broken his election promise to repeal this law many times." Whitehorse Daily Star

*** We are all to blame for Omar Khadr's mistreatment**
An opinion piece states, "The term "Kafkaesque" crossed the threshold into cliché years ago, but at times the word is sorely needed. For a situation to be Kafkaesque, it must be menacingly incomprehensible, with a lone individual thrown into a dangerous but confusing situation. Omar Khadr's ordeal certainly fits that definition. The trial of Omar Khadr - Omar K. in a Kafka work, or an "alien unprivileged enemy belligerent" in Guantanamo code - is a permanent stain on Canada's record. Khadr was raised by a family with ties to Al Qaeda, trained to take up arms, accused of lobbing a grenade at a U.S. soldier at age 15, thrown into a secret prison without adequate legal assistance, beaten and tortured, forced to choose between an unjust plea deal and an unfair trial, until finally, one day 13 years later, he was released on bail. (…)The Conservatives, meanwhile, went to extraordinary lengths in refusing to assist Khadr, interfering with the judicial process and classifying him as an adult offender - all on the Canadian taxpayers' dime. When the Conservatives finally repatriated him, they did so not on principle, but because the U.S. government pressured them to. The Tories' cruelty surplus is more revealing than their fiscal one. But the blame for Khadr's mistreatment rests ultimately with us, the Canadian public. It was a democratically elected government that assisted the torturers, and a repeatedly re-elected government that tried to keep him in the penal colony." Toronto Star, A21

*** Khadr comparison insulting**
A letter to the editor states, "Regarding the letter Bomber must have Canada envy, Comparing the actions of Omar Khadr to those of Dzhokhar Tsarnaev is absolutely ludicrous. But even worse, to state that Elizabeth May, Thomas Mulcair, and the Supreme Court of Canada would support and condone Tsarnaev's killing of innocent citizens is an incredible insult to them all." London Free Press, A7

Don't forget Khadr's victim
A letter to the editor states, "I would suggest those supporting Omar Khadr spend a few minutes talking with the widow of the soldier killed by the grenade (reportedly) thrown by Khadr. Then they could ask her if it matters that he was 15, 25, or 95 years old when the grenade ended her husband's life. If Khadr and his lawyer manage to fleece the Canadian government for wads of cash, they should turn around and give the proceeds to the widow of the American soldier that died of his actions." Winnipeg Free Press, A12

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Eisenberger wants a gun ban after 'wild west' violence
Mayor Fred Eisenberger wants the city to ban guns in urban areas after a brazen "wild west" shootout in downtown Hamilton over the weekend. Eisenberger asked city lawyers Wednesday to report back to council about what the city can legally do - if anything - to curtail gun violence. He later acknowledged he hadn't "fleshed out the constitutional issues." "I think anything we can do to make guns less accessible is a positive step. We ban a lot of things in the city. My question would be 'Can we ban guns?'" he said after a general issues committee meeting. "Most reasonable people would wonder, why are people carrying guns in the first place?" While some U.S. jurisdictions allow citizens to openly carry handguns, Canadian law prevents most people from doing so. Collectors and target shooters must follow strict rules for transporting and storing the weapons. (…)Hamilton police spokesperson Catherine Martin said the service "would support any crime prevention strategy that may be available to the municipality," but didn't specifically comment on the idea of a municipal gun ban. Hamilton Spectator, A1

Changing the conversation
It did not take a sexual harassment scandal on his own turf to focus Concordia University president Alan Shepard's attention on the issue. For one thing, Shepard, who has been president and vice-chancellor of

Concordia since 2012, had ordered a review of Concordia's policies on sexual harassment and sexual assault in December, months before a Concordia student leader took her harassment case to the Quebec Human Rights Commission. And for another, Shepard has been sensitive to issues surrounding sexual assault and consent since his own undergraduate days. (...)Melissa Kate Wheeler, a former president of Concordia's Student Union, is among those pushing for better support for victims at the school. One of her main frustrations is that the Sexual Assault Resource Centre, for which she advocated during her term as president, has not been given the resources it needs to meet its mandate of educating, raising awareness, providing support and crisis intervention. Montreal Gazette, A1

*** Sex assault is a burden for the young**
Here's a fact you'll never forget once you hear it: The peak age for becoming a victim of sexual assault is 15. (...)According to crime expert Wayne Morris, who spoke to the provincial select committee on sexual violence and harassment in Kitchener on Wednesday, sex assault in North America is primarily a young person's burden. Sixty-one per cent of victims of rape, most of them young women, are 17 or younger. Eighty-three per cent are 24 or younger. They tend to have problems perceiving risk in a dangerous situation, said Morris. Perhaps because of that difficulty, they "seem to be especially vulnerable to further attack," he said. Meanwhile, most perpetrators are under 25, likely have a criminal record, and have the idea that men should be dominant and women should be submissive. Waterloo Region Record, B1

*** Power and Control: Sexual Assault Reflects Social Norms**
Canadian society was founded on a colonialist model that supported patriarchy. Men, especially men of privilege, developed a sense of entitlement to exert power and control over certain groups, one of which included girls and women. The basis of rape culture is men believing it's their inherent right to use power and control over girls and women. Historically, predominant ideas, social practices, media, government, schools, religious institutions, employers, the various levels of law enforcement and justice were established by privileged white men. All of these institutions play a role in condoning sexual assault. They accomplish this by normalizing violence against women and reinforcing the myth that the survivor is to blame. Conversely, these institutions can choose to make a difference by supporting women's rights - which, quite simply, are basic human rights. Raise the Hammer

*** 'I kind of feel sick': Teen targeted by cyberbullies speaks out after alleged sexual assault**
A young girl in Atlantic Canada is speaking out along with her parents about cyberbullying and an alleged sexual assault, urging others in similar situations to do the same. CTV News is not identifying the 15-year-old girl because she says she is a victim of sexual assault at the hands of a woman 10 years older than her. "I didn't know what she was doing to me 'cause I was like in shock, I was like frozed," the girl said. "She asked me out, and I said, 'I don't want to date you 'cause I'm not a lesbian,' and she didn't take that for an answer," the girl said. "So like then she grabbed my waist and then she was kissing me and like sticking her tongue down my throat and then she was choking me. And then she grabbed my butt." It took a couple of weeks before the girl told her parents, who immediately reported the alleged assault to police. The family says that's when things got worse. CTV News (2015-05-20)

*** Better police training, reporting on use of force needed, report urges**
Most Canadian police forces still do not collect the right kind of in-depth data on when they resort to pulling their weapons or using force, nor do they receive sufficient mental health training to de-escalate confrontations that may turn deadly, a new report says. The Star obtained a copy of the research report commissioned by the federal **public safety department** after the Toronto police shooting of Sammy Yatim in 2013. It takes a comprehensive look at how police forces in Canada and the U.S. track their officers' use of force in encounters between police and members of the public. Its main conclusion is that, despite years of high-profile and critical inquiries into police actions in, for example, the Yatim shooting, the Vancouver police shooting of Paul Boyd, or the RCMP tasering of Robert Dziekanski, a consistent national approach is needed towards documenting when and why cops use force against citizens. It also urges more substantial mental health training for frontline officers who confront troubled individuals, too, saying the research clearly shows officers who receive extensive training successfully de-escalate tensions and are less likely to use deadly force. The report concludes it's not merely a matter of public safety, but officer safety as well, because police officers often suffer injuries when situations turn violent. Toronto Star

*** Twitter fight partly to blame for Etobicoke students shooting deaths: Report**
A report into the deadly shooting last fall outside Don Bosco Catholic Secondary School blames a Twitter fight among students and a Toronto Community Housing complex nearby for having "drug-activity and gun-related issues." But the report stops short of recommending metal detectors be installed in Toronto Catholic schools, citing "practical, social and legal reasons." The Safe Schools Inquiry Panel Report will be presented Thursday night to TCDSB trustees. But CBC News has obtained an advance copy. The report contains 33 recommendations, some of which include teaching students how to use social media responsibly, reviewing students' use of electronic devices in school and investigating "the feasibility of developing a smartphone-based application that would permit students to anonymously report school-related safety concerns." The report says the mother of one of the slain students proposed the installation of metal detectors and implementation of random searches of students as ways to ensure school safety, but added that "Toronto Police Service and many student representatives appearing before the Panel argued that this not be part of the recommendations, for practical, social and legal reasons." CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER

*** Coquitlam teen admits to swatting**
A Coquitlam teen who prompted numerous “swatting” incidents last year on families around Canada and the U.S. pleaded guilty last week to a dozen more charges. The 17-year-old, who cannot be identified under a publication ban because of his age, has now admitted to a total of 23 offences of extortion, public mischief and criminal harassment. In a day-long sentencing hearing at Port Coquitlam provincial court last Friday, Crown prosecutor Michael Bauer outlined how the teen had terrorized mostly young, female gamers and their parents, in B.C., Minnesota, Utah, Arizona, Ohio and California. He had a consistent pattern of trying to connect with the online gamers — many of them fans of the game League of Legends. But when they denied his requests, he shut down their internet access, posted their personal information online, repeatedly called them late at night and contacted the police in their hometown, posing as someone else. Often, he would tell the police he was holding a family hostage, had napalm bombs or had killed someone in the house. He would demand a ransom, order a SWAT (Special Weapons and Tactics) team — hence the term "swatting" — to show up with a police helicopter, or say he would kill any law enforcement official who intervened, Bauer said. Tri-City News

INTERNATIONAL

*** ISIL victory at Palmyra threatens ruins**
Islamic State of Iraq and the Levant extremists seized almost full control of the ancient Syrian town of Palmyra after government defence lines there collapsed on Wednesday, though it remained unclear how close to the famed archeological site the extremists advanced, activists said. Syrian state TV acknowledged that pro-government forces have withdrawn from Palmyra. The fall of the town to ISIL is a stunning defeat for President Bashar Assad's forces, days after the militants launched their offensive against Palmyra in central Syria. It is also an enormous loss to the government, not only because of its cultural significance, but because it would open the way for extremists to advance to key government-held areas, including Homs and Damascus. National Post, A9; The Globe and Mail

*** BIN LADEN LETTERS SHINE LIGHT INTO INNER WORKINGS OF AL-QAEDA**
The quest to understand Osama bin Laden continues, four years after his death. The U.S. government on Wednesday released a trove of documents allegedly collected from the compound in which the world's most well-known terrorist hid and was killed in 2011. The dump of more than 100 letters, directives and miscellaneous reports (including a partial list of the titles that graced the al-Qaeda leader's bookshelf)

paints a picture of a man simultaneously inhabiting two worlds: one atop a sprawling terror organization; the other a decidedly normal, suburban existence. The Globe and Mail, A10

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
June 15, 2015 / le 15 juin 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Longer waits for parole disadvantage aboriginal offenders
The vast majority of aboriginal offenders in federal prison are held long past the date they become eligible for parole, giving them less time under supervised release and - by the government's own calculations - shrinking their chances of success at living a free life again. Almost 85 per cent of aboriginal inmates are held until federal authorities have little choice but to release them, according to a new report from the **Public Safety Ministry**, which is responsible for corrections. Under federal law, inmates must be released, under supervision, at the two-thirds point of their sentence, unless authorities believe there is a high likelihood those offenders will commit a violent crime. For non-aboriginal inmates, the corresponding figure is 69.3 per cent. The report did not explain why the figures are so much higher for aboriginals. The difficulties for aboriginal offenders in obtaining their release echo the situation at the front end of the system. A disproportionate number of aboriginals arrive in federal prison each year, despite a federal sentencing law that requires judges to consider alternatives to custody for native people. Aboriginals make up 23.2 per cent of federal inmates, but only about 4 per cent of the Canadian population. A **spokesman for Public Safety Minister Steven Blaney** commented on the report Sunday: "***Our Conservative government believes that criminals belong behind bars***," **Jeremy Laurin** said. The Globe and Mail, A1

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Crews use burns to control blaze**
Crews are fighting fire with fire as they try to contain the aggressive wildfire burning south of Lytton. The Cisco Road fire is 20 per cent contained and was last mapped at 12.7 square kilometres in total size. Rain on Friday helped slow the blaze's progress, but the area is beginning to dry out again and there are concerns that continuing hot weather could cause the flames to flare up again. Vancouver Sun, A2

*** Lac-Mégantic - Le CP tentera d'annuler l'indemnisation de 431 millions**
La Cour supérieure commencera à entendre lundi la cause des victimes de la tragédie de Lac-Mégantic pour déterminer si elles pourront recevoir plus de 431 millions de dollars en indemnisation, mais le juge pourrait en décider tout autrement en invalidant le processus de règlement. La Presse Canadienne (Le Devoir, A4); Canadian Press (The Gazette, A5)

*** MERS outbreak: 3 lessons Canada learned from SARS**
As South Korea faces an outbreak of Middle East respiratory syndrome, or MERS, Canadian health officials are staying vigilant in case the virus makes it inside our borders. It's more than a decade since severe acute respiratory syndrome, or SARS, infected 8,000 people and killed 774 around the world. Experts say that based on lessons learned from dealing with SARs, the Canadian health system is much better equipped to handle any potential outbreaks — even if the risk of MERS coming to Canada is still very low. CBC.ca

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Human Rights Watch raises concerns over B.C. terrorism trial
A terrorism trial underway in British Columbia runs disturbingly parallel with an emerging trend in U.S. anti-terror efforts targeting some of society's most vulnerable people, says an international human rights group. Human Rights Watch members have been observing the case of John Nuttall and Amanda Korody, two Vancouver-area residents found guilty earlier this month of plotting to decimate the provincial legislature with pressure-cooker bombs. Andrea Prasow, the organization's deputy Washington director, says the case resembles U.S. authorities' post-9/11 undercover operations to thwart terror attacks before they happen. "What we've seen allegations of (in B.C.) are at least similar practices to what we've seen in the U.S.," said Prasow. "Federal law enforcement authorities targeting in sting operations people who are particularly vulnerable." A B.C. Supreme Court jury convicted the pair of conspiring to commit murder and possessing explosives for the benefit or on behalf of a terrorist organization. The attack was planned for Canada Day in 2013. Canadian Press (Red Deer Advocate, A2, Star Phoenix, Vancouver Sun)

*** ISIL Fighter's mother offers new approach**
There's another side to Islamic extremism, one filled with tears, not hate. The heart-wrenching documentary film of Christianne Boudreau, mother of a dead 22-year old Islamic State fighter from Calgary, arrived in Ottawa on the weekend, part of a cross-country tour by the Extreme Dialogue project aimed at reducing the appeal of all forms of extremism among teens and young adults. A second slick film explored the hate-filled radicalization of Daniel Gallant, a former white supremacist. The effort is led by the Institute for Strategic Dialogue in Britain, with funding from the federal Kanishka Project. Packages of educational resources to accompany the films and other details are at extremedialogue.org. Ottawa Citizen, A6

*** Watch mosques, Islamic schools for radicalization**
The violent doctrine of extreme Islam is spreading in Canada through the foundation of mosques, Islamic centres and Islamic schools by wealthy Gulf state investors with radical goals, a controversial U.S. commentator is warning. Ayaan Hirsi Ali, a former devout follower of the Muslim Brotherhood, bestselling author, ex-politician and now a fellow at Harvard University's JFK School of Government, was the final witness recently at the national security and defence committee, which is preparing a report on threats to national security. "You should be looking out for the sprouting of mosques and Islamic centres. You should be looking out for the establishment of Islamic schools and anything that costs money," she said via a video link from Boston. "Countries like Saudi Arabia and the oil-wealthy Gulf countries that have

absolutely everything that money can buy, yet many of them choose, for their philanthropy, radical Islamic goals, institutions, activities, jihad." Ottawa Citizen, A6

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Residents on edge as search for escapees drags on
Residents in rural New York, unaccustomed to locking their doors, day or night, were on edge as the manhunt for two killers who cut themselves free from a maximum-security prison with power tools stretched into a ninth day. More than 800 law enforcement officers in the search for David Sweat and Richard Matt scoured the fields and Adirondack woods several miles around the Clinton Correctional Facility in Dannemora near the Canadian border. The search continues to focus on the area surrounding the prison after the jail worker accused of helping the men escape backed out of a plan that could have had the men hundreds of miles away, a prosecutor said. The now-jailed prison worker had planned to pick the men up after they cut themselves out of the prison and drive about seven hours to an unknown destination, District Attorney Andrew Wylie told CNN. But prison tailor shop instructor Joyce Mitchell backed out of the plan at the last minute, Wylie said. "One of the reasons that she didn't show up was because she did love her husband and didn't want to do this to him," Wylie said. Searchers continued to focus on an area east of the prison, which is about 30 kilometres from the Canadian border... Associated Press (Cape Breton Post, B5, Guardian); Associated Press (The Record, Chronicle-Herald) (2015-06-15); CBC News (2015-06-14)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Internet of Things a playground for hackers**
When it comes to the security of the Internet of Things, technology companies are thinking about it all wrong. "Privacy is not the main problem," Ted Harrington, executive partner with Baltimore-based Independent Security Evaluators (ISE), told a room of IT professionals at the annual SC Congress digital security conference in Toronto last week. "Why would I care about my connected light bulb getting hacked? At worst, someone gets information about how often I turn on or off my lights. Maybe an adversary could even annoy me by turning off my lights. How bad is that?" Mr. Harrington asks. But think of that "smart" light bulb as a chink in the armour of digital security. Mr. Harrington's research has found that makers of connected devices have failed to design strong protections against attackers: He's seen everything from unchangeable hard-coded passwords to unencrypted data connections. And there is a growing number of connected devices showing up in homes, cars, businesses and on our bodies. Globe and Mail, B3

LAW ENFORCEMENT / APPLICATION DE LA LOI

'I lay on the floor crying, saying thank you'
Amanda Lindhout was so anxious about a scheduled call with her National Security contact that she forgot to eat dinner. It was 8 p.m. MT last Thursday night - the eve of her 34th birthday - and Lindhout had just returned home to Canmore, Alta., from a string of speaking engagements for her bestselling memoir, A House in the Sky, which chronicles the 460 days she spent being starved, beaten, sexually assaulted and held for ransom in Somalia. She knew the caller would bear important news, namely whether a Crown prosecutor felt there was enough evidence to charge the man who led the negotiations on her capture, who terrorized her mother for months with phone calls demanding money and who had been the subject of a lengthy, covert RCMP investigation. Lindhout prepared herself for the worst; that the investigation would be closed and it would all be put to rest. In what turned out to be a conference call with more RCMP officials than she could count, she learned the opposite was true. "It never crossed my mind that they had already arrested the guy," she told the National Post in an interview Sunday. One officer who had stuck with the case over the past five years asked her "Are you sitting down?," Lindhout recalled Sunday on social media. "There were several RCMP officials on the line as he delivered the news. I was stunned that they'd made the arrest. I was even more stunned that the accused kidnapper

was in my home country." Lindhout said she fell to her knees and sobbed as the panel of officials and investigators waited on the other line... Though she had participated in the investigation for more than 5 ½ years, the freelance journalist-turned-philanthropist never shared the RCMP's confidence that Ali Omar Ader would be charged in connection with her kidnapping in Mogadishu, Somalia, on Aug. 23, 2008 when she entered the country with photojournalist Nigel Brennan in pursuit of a story. Postmedia News (Ottawa Citizen, A1, National Post, A1, Vancouver Sun, StarPhoenix, Windsor Star, Montreal Gazette, Edmonton Journal, Calgary Herald); Globe and Mail, A1, Toronto Star, A1; Edmonton Journal, A1; Canadian Press (Red Deer Advocate, The Guardian, The Telegram, Cape Breton Post, Waterloo Record, Hamilton Spectator, Chronicle Herald); Presse Canadienne (L'Acadie Nouvelle, Le Droit); National Post (The Province); Canadian Press (Toronto Star); Postmedia News (Ottawa Sun, London Free Press, Toronto Sun, Kingston Whig Standard, Calgary Sun)

Richmond County woman's remains identified

Human remains found in a wooded area last month have been identified as those of Michelle Marie Demers-Kennedy, who was killed by her son two years ago. The 57-year-old woman was reported missing from her Framboise residence on Mother's Day in 2013. Last month, her oldest son, Merlin Demers-Kennedy, 32, of Framboise, pleaded guilty to manslaughter in her death. He remains in custody until his sentencing Friday in Port Hawkesbury Supreme Court. There is a broad range of sentences for manslaughter, with the maximum being life in prison. In late May, investigators with the RCMP's Northeast Nova Major Crimes Unit identified a burial site in a wooded area off North Framboise Road and human remains were located and exhumed on May 27. With the assistance of the Nova Scotia Medical Examiner's Office, the RCMP were then able to identify the remains. Merlin Demers-Kennedy was arrested on Jan. 15, 2014, and in a statement to the RCMP he admitted to killing his mother... Cape Breton Post, A1

'She's not just taken away from me'

For two months, Kirk Babiak has been replaying the scenes in his head: The frantic phone call, the house surrounded by police, the devastating, unbelievable news that the woman he loved had been murdered. "To have this happen just makes no sense," said Babiak, whose girlfriend, Paula Stiles, was found dead inside her Sherwood Park home on the morning of April 15. "She's not just taken away from me, she's taken away from everybody - her friends, and her family and her beautiful girls. There's so many people that are just devastated and at a loss of knowing what to do next, because she filled such a big role in so many people's lives." Stiles, 44, a mother with three daughters, worked as a training supervisor at Enbridge Pipelines. She was found dead inside her house at 40 Foxhaven Court. No arrests have been made, and the cause of her death has not been released by RCMP. RCMP spokeswoman Josee Valiquette said Friday that the case remains under active investigation. RCMP previously appealed to the public for video and photographs shot in public areas in or around Sherwood Park between the night of Tuesday, April 14, and the morning of Wednesday, April 15. Investigators were also looking for two teenage skateboarders who had been in the area, and were considered to be potential witnesses. Valiquette said she did not know if the skateboarders had been located, but that investigators were still looking for tips and information in the case. Postmedia News (Edmonton Journal, A1)

Waterloo Region watching OPP talks

Ontario municipalities are keeping a close eye on provincial police contract negotiations to see if the province can whittle out years-of-service bonuses that communities say are difficult to afford. The benefit, known as retention pay, began in Toronto a little over a decade ago. The Ontario Provincial Police followed suit soon after, and over the years it found its way into most police and firefighter contracts across Ontario - including Waterloo Region - as recognition or service pay. It gives an extra three-per-cent pay after about eight years of service, six per cent after about 17 years and nine per cent after about 23 years. In Toronto, the base pay of a first-class constable is $92,433. The provincial government does not control the deals municipalities reach with their police services. But it can set trends with the agreements it strikes with the Ontario Provincial Police. As the Liberal government tries to eliminate a $10.9-billion deficit it has said any public-sector contracts must have "net zero" increases, so any small compensation boosts would have to be offset. Neither the government nor the Ontario Provincial Police Association would say if retention pay - also known as 3-6-9 - is on the table as they bargain a new deal.

But most police service boards are hoping it is, says their provincewide association. Canadian Press (Waterloo Record, A1)

Pan Am Games will test security budget
The Pan American Games will rack up police overtime; the question is how much. With years to prepare and examples from other cities to look to, organizers have dreamed up ways to leave Toronto police officers free to staff the event. That includes shutting down the city's police college and certain courtrooms for all of July, as well as nearly halving the amount of vacation officers can take that month. Those measures will limit costs to the province, which is responsible for paying officers' overtime. But they will also be a test of success for streamlining police costs, if Toronto or other major cities hope to host big events more often. "One of the most expensive things at these types of international events now is security," said Christian Leuprecht, a professor at Queens University and the Royal Military College who has written extensively on the costs of policing. Some overtime is inevitable, he said. But he will be looking to see, after the Games, how real costs stacked up against the province's $239-million security budget. "If Canada and Toronto want to be competitive in bids for these types of large events, they will need to find efficiencies," he said. "This is all plan-able and manageable." Ontario Provincial Police and thousands of private security staff will work with municipal police, including Toronto's, at the Pan Am and Parapan Games, which will last 26 days in total. Of the amount the province plans to spend, $101.5-million is slated to cover various municipal police services, $81-million for contracted private security and $57-million for the OPP, according to an Auditor-General's report on those costs from last fall. The Games' organizers have budgeted an additional $8-million for security. Toronto municipal police are budgeted for $72.7-million, overtime included, said Toronto Police Staff Sergeant Devin Kealey, a community liaison for the Games. However, those are estimates, and staffing will depend on attendance, weather and other factors, he said. Globe and Mail, A8

OPP officer arrested again
An Ottawa OPP officer has been arrested for the second time in 12 months and charged with cocaine possession and a gambling-related offence after being found in an illegal gaming house. Const. Dennis Hill, a 14-year veteran, was arrested Thursday night when OPP organized crime investigators raided a home on Snowden Street in Alta Vista to break up a common gaming house. Ten others also were charged. Officers seized marijuana, cocaine, oxycodone hash, morphine and cash. Hill, 38, has been on leave from the force, the OPP said in a statement. Last June, his own force arrested him while he was on medical leave for rehabilitation. Postmedia News (Ottawa Citizen); Postmedia News (Kingston Whig Standard)

Un appel vidéo de la GRC dans un cas de cybercrime produit des résultats
Une vidéo de la GRC du Nouveau-Brunswick lançant un appel à l'aide pour faire avancer l'enquête sur un homme de Moncton accusé d'avoir leurré jusqu'à 2000 garçons en ligne a été vue 750 000 fois et donne des résultats, rapporte la GRC. L'agente Jullie Rogers-Marsh a affirmé que la vidéo avait été partagée sur les médias sociaux par des corps policiers de plusieurs pays. La police a bel et bien reçu de l'information, mais elle n'en a pas précisé la nature ni la quantité. L'homme de 24 ans, qui ne peut être nommé en raison d'une ordonnance de non-publication, fait face à plusieurs chefs d'accusation de nature sexuelle pour avoir prétendu être une adolescente en ligne pour attirer des garçons âgés entre 10 et 16 ans. Les crimes auraient été commis entre le 12 janvier et l'automne dernier. L'accusé pourrait avoir pris au piège des victimes au Canada, aux États-Unis, au Royaume-Uni, aux Pays-Bas, en Australie et en Russie. Presse Canadienne (L'Acadie Nouvelle)

Edmonton mourns Woodall
Slain city Const. Daniel Woodall was remembered as a warm person and a joker who could always lighten the mood. Edmontonians paid respects to the slain officer during a public visitation arranged by his family Sunday at First Memorial Funeral Services in Old Strathcona. Police honour guards stood by Woodall's casket, which was draped in a Canadian flag and a police hat and photograph of Woodall on top. Next to the officers stood a framed photograph of Woodall with his smiling wife and two children, as well as a British flag to represent his home country. Denver Poburan, who trained in kung fu with Woodall, saw the officer two days before he was gunned down at a west Edmonton home while trying to serve an

arrest warrant. "I saw him on the Saturday before he died and he said, 'I'll see you on Tuesday,' and he never did," Poburan said, holding back tears. "He was a great guy. He always had a joke to lighten the mood. He took his training seriously, but he was also just a fun guy to be around." Poburan said Woodall had just earned his green belt. An aspiring officer himself, Poburan had many reasons to admire his "kung fu brother." "He was someone the class could really look up to. He was also a big inspiration for me because I want to get into policing too, and he was always encouraging for me to do that." Postmedia News (Kingston Whig Standard, London Free Press, Calgary Sun, Edmonton Sun, Winnipeg Sun, Ottawa Sun, Toronto Sun, London free Press)

La drogue «roulette russe»
Il s'avère révélateur que certains consommateurs croient que la Molly soit une nouvelle drogue, puisque les consommateurs connaissent rarement la réelle composition des comprimés et des capsules qu'ils achètent. Selon les forces policières, même les distributeurs ne sont pas toujours conscients de ce qu'on retrouve dans leurs produits. Non seulement il ne s'agit pas d'une nouvelle drogue, mais même le nom Molly - dérivé du mot «molécule» - n'est pas nouveau. Il est associé à la MDMA depuis plusieurs années. Généralement, ce qui est vendu comme étant de la Molly est une drogue à base de MDMA, mieux connue comme étant de l'ecstasy. Or, la concentration de MDMA est régulièrement réduite par un mélange avec divers produits chimiques et drogues. «Il n'y a aucune façon qu'on puisse savoir d'avance ce que le comprimé contient réellement [...] on peut se retrouver avec n'importe quoi. Ça peut être de la méthamphétamine ou d'autres drogues qui imitent les effets de la MDMA», soutient Mélanie Terrier, caporale au Service de sensibilisation aux drogues et au crime organisé (SSDCO) de la Gendarmerie royale du Canada (GRC). Autrefois, il était nécessaire d'avoir un contact rapproché avec les producteurs des comprimés pour devenir un vendeur d'ecstasy. La distribution s'est toutefois «démocratisée» et cette drogue est désormais accessible en vrac sur le Web. Le produit, conçu outre-mer, est alors expédié à l'acheteur. La Presse (Le Droit)

RCMP review of 30 flagged Senators' expenses would become a 'hell of a problem'
Senators on both sides of the aisle are concerned the Mounties will review the files of all 30 Senators flagged in Auditor General Michael Ferguson's explosive report, which would become a "hell of a problem" for the embattled Upper Chamber's image. "I've heard that the RCMP were going to take a look at all 30. Now, what that means, I don't know. You'd have to get that confirmed from them. Certainly, that's a story that's floated around, there's no question about it," said Ontario Conservative Sen. Bob Runciman, a former provincial minister of public safety and security and chair of the powerful Senate Legal and Constitutional Affairs Committee. Of the 30 flagged expenses, Mr. Ferguson referred the cases of nine Senators to the RCMP and the other 21 to the Senate's Internal Economy, Budgets and Administration Committee. Sen. Runciman and other Senators interviewed for this article said the federal police force could decide to investigate all 30. "They [the RCMP] can take a look at the findings and if they think there's something of concern, they have the ability to investigate," Sen. Runciman told The Hill Times. Liberal Sen. Céline Hervieux-Payette (Bedford, Que.) echoed Sen. Runciman's view that the RCMP could start an investigation of all 30 Senators. "We were told that the RCMP said that they will investigate, whoever they want, whenever they want and for the amount of time they want." One Senator who spoke on condition of anonymity said Senate backrooms are concerned that the RCMP is reviewing the AG audit report, monitoring media reports and, should they go ahead with an investigation, they would go back five years. Hill Times

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Bath Institution placed in lockdown
Bath Institution is in lockdown, Correctional Service Canada reported on the weekend. At approximately 9 p.m. Friday night, the lockdown was put in place at the medium-security federal institution to enable staff members to conduct an exceptional search. Normal operations will resume as soon as it is safe to do so, according to a news release. "A search would be to find any unauthorized items that offenders are not allowed to have," Shannon Mills, media relations with CSC, said in an email. "We cannot provide details as it might compromise the search." A release from CSC said the search was ordered to ensure the

safety and security of the institution's staff and inmates. The institution has a rated capacity of 340 inmates. "CSC is committed to preventing the entry of contraband into its institutions," The release states. "CSC also works in partnership with the police to take action against those who attempt to introduce contraband into correctional institutions." Kingston Whig-Standard, A3

*** Parole board rejects day passes for killer of ex-NHLer's parents**
A request for six unescorted day visits to a Sudbury halfway house from the man who killed the parents of an ex-NHL player was rejected by the parole board. Former NHL goalie Don Edwards -- whose parents Arnold and Donna were killed in 1991 by George Harding Lovie, then 32, in a small town south of Hamilton, Ont. -- said in an interview Sunday he and his family are elated with the board's decision, which took only 10 minutes following a five-hour hearing Thursday. "We're happy and we are also happy for the people in Greater Sudbury as well," said Edwards, who played 10 seasons in the NHL with the Buffalo Sabres, Calgary Flames and Toronto Maple Leafs. "People just don't realize how dangerous this guy is. "The sad thing about it is St. Leonard's (halfway) House in Sudbury had approved it, but he failed to meet any of the four requirements with the extended temporary absences such as risk and behaviour." The parole board hearing was held at the Beaver Creek correctional facility in Gravenhurst, Ont., where Lovie is serving his time. Lovie, who is considering living at the halfway house should he ever be granted parole, was convicted of two counts of first-degree murder and one count of attempted murder. He was sentenced to 25 years to life on each count. Postmedia Network (Toronto Sun, Edmonton Sun, Ottawa Sun, Winnipeg Sun, Calgary Sun, London Free Press, Kingston Whig-Standard, Cornwall Standard Freeholder, Sault Star, CNews, 24 Hours Vancouver)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Missing, murdered aboriginal women inquiry findings would be more shocking than residential school report
A letter to the editor states, “Re: "Three reasons why inquiry into extraordinary number of missing, murdered aboriginal women isn't the answer," (The Hill Times, June 8, p.12). Thank you for writing about aboriginal issues. Even when I disagree with the writer I am usually grateful for the issues being kept in the minds of your readers, most of whom are not aboriginal and judging from the comments section do not even agree with the existence of aboriginals. You say you want to have these crimes investigated as crimes. I would suggest that underneath that lies a social prejudice that you have yet to uncover. If crimes are only crimes and demographics are not important, then I look forward to your column suggesting that no money should be put into investigating abuse of seniors, ending funding to women's groups, cancelling funding for fighting gang crimes or other demographic-based initiatives. If that somehow feels uncomfortable to you please examine that reaction. My mom was Mohawk and my dad was white. I look white, was kidnapped by the government during the '60s scoop; they thought I would fare better in foster care than residential school. I was raised by decent, kind people, worked fairly steadily in various industries, never fell into addiction, married for almost 20 years and have three grown children who also work (and have avoided addiction) and a lovely new charming healthy grandson.” Hill Times.com

*** Why is the city of Vancouver regulating an illegal activity?**
An opinion piece states, “As the City of Vancouver consults with the public on its proposal to license marijuana retailers, I expect many people are not asking themselves about the details – for example, should pot shops be allowed at transit malls – but about the bigger question: What is the city doing regulating an illegal activity? Yes, storefront marijuana sales are still against the law. Marijuana can be distributed legally for medical purposes, but several conditions must be met. Among them, the patient needs a doctor’s prescription, and the purchase must be from one of a very small number of producers licensed by Health Canada. If these and other conditions are not satisfied, then possession and sale of cannabis is a criminal offence, and possession of as few as six marijuana plants carries the risk of prosecution and up to 14 years in prison. Or not. Because in Vancouver, the police have made it clear they will not enforce medical marijuana laws against store operators except when there are other public order considerations. (…)Some may still believe the best response to the reality that is marijuana in our society is to criminalize it, but it is a shrinking minority. A large and growing consensus of Canadians

understands that cannabis prohibition has failed. It has not reduced use, and it has instead encouraged the spread of organized crime gangs whose members fight over market share." Globe and Mail

* **La drogue, le crime numéro un**
En forte hausse depuis cinq ans, les infractions liées aux drogues arrivent en tête du «top 10» des crimes commis au Québec. C'est ce que permettent d'établir des données compilées par le ministère de la Sécurité publique sur les crimes commis par les 5000 détenus qui se retrouvent chaque jour dans les 19 prisons québécoises. Le trafic, la production et la possession de stupéfiants totalisaient 2173 des quelque 14 000 infractions criminelles de ces prisonniers, au 31 janvier 2015. Soit un crime sur sept. La drogue arrive loin devant le non-respect d'ordonnances du tribunal, les voies de fait et les vols. Journal de Québec, 26 (Journal de Montréal)

* **Activists looking to put Hamilton Police 'street checks' onto public agenda**
The mayor of Toronto recently called for an end to that city's controversial "carding" policing tactic. The mayor of Hamilton said a few days later the issue of "carding" or "street safety checks" hasn't come across his radar. "I'm not hearing any kind of a conversation on it at all," said Mayor Fred Eisenberger. That's set to change later this month.An activist who fears the street stops that Hamilton police acknowledge they do, leads to disproportionate targeting of racial minorities will push for answers in front of the chief and elected officials, including Eisenberger, at the next Hamilton Police Services Board meeting, June 25. That appearance will set the stage for Hamilton to enter a public debate that has been growing around the province for months. Not everyone shares the mayor's belief carding or "street stops" are not an issue here. CBC News

* **Former sex worker claims MLAs, judges, police officers, lawyers, and doctors have been clients of prostitutes**
At yesterday's Red Umbrella march in Vancouver, a former sex worker condemned federal legislation that criminalizes clients. Sheryl Kiselbach, the violence-prevention coordinator at the PACE Society, said that she and other current and former sex workers in the crowd have "dated" doctors, police officers, lawyers, judges, and MLAs. Kiselbach didn't name names, and instead emphasized the importance of supporting current sex workers who face greater dangers because of legislation passed last year by the Conservative government. "We need to help them stay safe and we need to support them," she said. The red umbrella has long been a symbol of sex workers' safety, which explains the name of yesterday's protest. Kiselbach told the crowd on the south side of the Vancouver Art Gallery that she became a plaintiff in a charter challenge against prostitution laws because she didn't want sex workers to suffer the same injustices that she endured. Straight

* **SlutWalk Demonstrators Call for Better Education on Respect, Consent**
The first ever St. John's SlutWalk drew a large crowd for a rally and march through the capital city's downtown. The event yesterday afternoon was intended to discuss sexual violence and victim blaming as socially and culturally entrenched issues that need to be addressed. Lawyer and activist Lynn Moore is trying to convince the province to bring in a course for K-12 students on respect, equality, and consent. Moore said that teaching our kid not to rape, and to get consent, is as important as teaching them math. VOCM

PUBLIC SERVICE / FONCTION PUBLIQUE

Public Service Week gets political ahead of election
The week to celebrate the hard work of Canada's public servants will take a political turn as federal unions begin a pre-election advertising campaign that accuses the Conservatives of undermining the integrity of public services. National Public Service Week kicks off Monday with the Professional Institute of the Public Service of Canada launching the release of its pre-election ads for print, online and radio to coincide with the week-long activities. "We believe the best way to mark National Public Service week is to speak out and defend the integrity of public services our members deliver, and our advertising will make sure it will be an issue in the election campaign," said Debi Daviau, PIPSC president. The 17

federal unions signed a solidarity pact to ensure they present a common front in this round of contentious bargaining over the Conservative government's plans to scrap existing sick-leave benefits that are a long-standing part of employees' contracts. Ottawa Citizen, A8

OTHER

Trekkers believed back on home soil
Two Saskatchewan trekkers deported from Malaysia are believed to be back in the province. It is believed 23-year-old Lindsey Petersen and his 22-year-old sister Danielle arrived in Regina on a flight from Vancouver late Sunday afternoon. At about 4 p.m., two people believed to be Floyd and Joanne Petersen - the parents of the siblings walked to the arrivals area of the Regina airport. The man, wearing a pink visitor's tag, was promptly escorted to another location in the airport and the woman joined him shortly after. When asked by media, the woman denied being Joanne Petersen. There was no sign of either Lindsey or Danielle Petersen with other passengers who got off the Vancouver flight, suggesting they were taken through to another area to leave the airport. Postmedia News (Star Phoenix, A1, Leader-Post, A1)

INTERNATIONAL

U.S. airstrike in Libya targets terrorist behind Algerian attack
The United States carried out an airstrike in Libya early Sunday against the mastermind of the 2013 terrorist seizure of an Algerian gas plant that left 38 foreign hostages dead, U.S. and Libyan officials said on Sunday. The Libyan government said in a statement Sunday night that the airstrikes killed the terrorist leader, Mokhtar Belmokhtar, and "a number" of other Libyan terrorists in the eastern part of the country. "The Libyan government announces that American planes undertook action that resulted in the death of the wanted terrorist Mokhtar Belmokhtar and a number of Libyans belonging to one of the terrorist groups in Eastern Libya, after consultation with the Libyan interim government to take action on terrorist leadership present on Libyan soil," according to a statement released by the government. U.S. officials confirmed that Belmokhtar was the target of the strike by at least one U.S. warplane, but they expressed caution about his fate, saying that they needed forensic proof to declare with certainty Belmokhtar's death. That could take some time unless terrorist websites issue a statement of mourning. New York Times (The Hamilton Spectator, A14, The Record, Toronto Star); * Associated Press (National Post)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
April 15, 2016 / le 15 avril 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

RCMP refugee screening a $16M flop, says internal report
A $16-million RCMP project to help keep dangerous refugees out of Canada has turned out to be an expensive security flop. An internal evaluation says the screening project delivered information too late, strayed beyond its mandate, and in the end did almost nothing to catch refugees who might be linked to criminal or terrorist groups. Meanwhile, 30 Mounties were tied up for four years on duties that did little to enhance Canada's security. "The current approach does not appear to provide much by way of relevant information to support the admissibility screening of refugee claimants," concludes the Sept. 29, 2015, report, obtained by CBC News under the Access to Information Act. The report on the anemic results was completed at about the same time as then prime minister Stephen Harper said Canada had to proceed cautiously in accepting Syrian refugees so that Canada's screening process could weed out terrorists. "When we are dealing with people that are from, in many cases, a terrorist war zone, we are going to make sure that we screen people appropriately and the security of this country is fully protected," Harper told a 2015 election rally in Welland, Ont. "We cannot open the floodgates and airlift tens of thousands of refugees out of a terrorist war zone without proper process. That is too great a risk for Canada." (…) A spokesman for **Public Safety Minister Ralph Goodale**, who is responsible for the RCMP, ***said the***

government welcomes the evaluation's feedback. "We believe in evidence-based policy and in ensuring that government resources are being used effectively and responsibly," Scott Bardsley said in an email. RCMP Commissioner Bob Paulson has said the force's new responsibilities for anti-terrorism have drained resources away from other key activities, such as fighting organized crime and market fraud. CBC

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Tornado Touches down**
Calgary Environment Canada confirmed that a tornado - the first for Alberta this year - touched down Wednesday afternoon near the intersection of Hwy. 1 and Stoney Tr., east of Calgary. Meteorologist Kirk Torneby said the tornado touched down around 3:50 p.m. but did not cause any damage and it was difficult to determine the length and width of its track. "This was driven by daytime heating, winds converging at the surface and causing a rotation, sucked up by the updraft of, in this case, rain moving through," Torneby said, adding winds reached as high as 105 to 137 km/h. "It was basically developing from the ground up to the cloud." On the 1 to 5 Fujita scale used to rate the intensity of tornadoes, this one was rated a zero since it had no impact, the agency said. Edmonton Sun, A34 (Calgary Sun); Calgary Herald

*** Heavy rain heading for northwestern Ontario, Environment Canada says**
Environment Canada is issuing a special weather statement for parts of northwestern Ontario because of significant rainfall expected to begin Friday night. A low pressure system from the upper plains states could bring heavy rain to Red Lake, Sioux Lookout, Kenora, Dryden and Pickle Lake through the weekend, says meteorologist Geoff Coulson. Rainfall amounts of 25 to 50 millimetres are possible by Sunday morning and that's a problem because of the area's delayed spring, he said. CBC News

*** Climate, flooding, devastation: Why no national strategy?**
Climate change has moved from future threat to present danger. Extreme weather events are increasing in frequency and severity. The Parliamentary Budget Officer (PBO) recently estimated that the financial cost of natural disasters driven in part by climate change will, over the next five years, be far greater than previously estimated. Policy makers must fully accept and swiftly adapt to this new reality – even as they continue with efforts to combat climate change over the longer term. The numbers are harrowing: The PBO predicts that storms, hurricanes and floods linked to climate change will cost the federal disaster fund $900-million annually over the coming five years. That compares to an average of just $54-million a year (in adjusted 2014 dollars) for the period between 1970 and 1994. That $900-million-a-year estimate is well in excess of what the federal government has currently set aside to deal with such events. Globe and Mail (2016-04-11)

*** Forest-fire season begins April 18**
The 2016 forest-fire season in New Brunswick begins on April 18. Each year, the season begins on the third Monday of April and continues through until Oct. 31 unless otherwise indicated. Anyone igniting a Category 1 fire (fires with a diameter of three metres or less) should ensure burning is allowed in that area. This can be done by calling the toll-free burn line at 1-866-458-8080 or by visiting the Department of Natural Resources' website. Category 2, 3 and 4 fires require a written permit. Applications are available at the department's regional offices. Burning grass is considered a Category 4 fire that requires a written permit. To many people, burning grass is a safe and helpful way to renew the growth of new grass in the spring. However, the reasons for spring grass burning are largely unfounded and rather than being beneficial, it is destructive and dangerous. A list of myths and facts surrounding grass burning is available online. Sackville Tribune Post

*** Déversement de mazout aux Îles : 29 documents saisis par le ministère de l'Environnement**
Le ministère de l'Environnement a dû effectuer une perquisition chez Hydro-Québec pour obtenir des documents importants dans le cadre de son enquête sur le déversement de 100 000 litres de diesel dans le port de Cap-aux-Meules en 2014. Ces documents ont contribué à l'enquête du ministère qui a conclu

que l'oléoduc était ravagé par la corrosion au moment du déversementet et qu'Hydro-Québec a manqué à ses devoirs en ne prenant pas les mesures de prudence pour l'entretien de ses équipements. Radio-Canada (2016-04-14)

*** Ontario Fire Marshal review results in 27 recommendations for Amherstburg**
The Ontario Fire Marshal issued 27 recommendations to improve service after an extensive review of Amherstburg's fire department. Town council received a report from the Office of the Fire Marshal and Emergency Management (OFMEM) at Monday's meeting. Recommendations focused primarily on administrative issues such as shoddy record keeping, a lack of prevention programs, public safety education and emergency planning. The review also concluded "a current and validated mechanism to measure fire risk within the municipality does not exist." Windsor Star, SR8

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Documents shed a little light on what spy Jeffrey Delisle sold to Russians**
The U.S. Naval Criminal Investigative Service (NCIS) has shed a little light on the information Canadian spy Jeffrey Paul Delisle was selling to the Russians. The former Canadian naval intelligence officer pleaded guilty in 2012 to spying and selling secrets for about $3,000 a month. Delisle, 45, a Halifax native and former sub-lieutenant, was the first Canadian to be convicted of spying in decades. The type of information Delisle sold to the Russians did not come out in court, but CBC News made more than a dozen freedom of information requests to various U.S. government departments. Most of the responses were heavily — if not totally — redacted, but some details were contained in documents from the NCIS. Details included the kind of threat assessments of foreign destinations that are routinely prepared for visiting American troops and officials. CBC News

Daesh targets Toronto imam on their hit list
Just days after celebrating cultural bridges, a Toronto imam has been targeted in a Daesh hit list. Daesh, also known as ISIS or ISIL, named Shaykh Abdullah Hakim Quick along with other Muslims in the West, urging followers to kill them for speaking out against the group and betraying their interpretation of Islam. Quick works with the Canadian Council of Imams, which hosted its first annual dinner on Monday night, honouring political leaders and community members. "It was a really good vibration that came out of that meeting, a lot of unity between people of different faiths," Quick told the Star. "So here comes the devil, as we would say, screaming out against us the next day." Quick first learned of the threat on Wednesday from a fellow imam in the council, but though he says he has contacted law enforcement and is taking precautions, he will not be intimidated. "I will continue to do what I have to do," he said. "Putting my trust in God. This is what Muslims do when they find themselves in difficulty, and continue on to do what's right." Michael Zekulin, a terrorism researcher at the University of Calgary, says the threat is typical of Daesh's propaganda tactics, but not necessarily legitimate. Daesh has implored its followers to go after others in the past, he said, such as Calgary-based cleric Syed Soharwardy and UFC fighter Tim Kennedy. "It never resonated," Zekulin said. More than anything, he said, the threat demonstrates the sophisticated, extensive nature of Daesh's communication network. Quick said he has never personally confronted Daesh, but the council has spoken out against the radical group. The article naming Quick appeared in Dabiq, an English-language magazine published by Daesh. Toronto Star, GT2

Victoria terror couple drop CSIS demand
A Surrey, B.C., couple convicted of a plot to bomb the Victoria legislature have abandoned an application they filed seeking further disclosure of documents from the Canadian Security and Intelligence service. Marilyn Sandford, a lawyer for the defence, Thursday told B.C. Supreme Court Justice Catherine Bruce recent delays in pursuing the matter in the Federal Court of Canada have displeased John Nuttall and Amanda Korody. "My clients have been in custody for a long time. They are anxious to proceed and they are anxious that there not be any further delay." The abandonment of the CSIS application is expected to bring an end to evidence being called by the defence in a bid to stay the charges on grounds the couple were entrapped by police. National Post, A6; * Vancouver Sun, A7 (The Province)

Get serious on crime at casinos
An editorial states, "British Columbia plans to crack down on money laundering at casinos. We hope the government's heart is truly in its task, given that total government revenues from commercial gambling in 2013-14 totalled $1.17 billion. The move is long overdue. The government has made it easier for organized crime to use B.C. casinos for money laundering and loan-sharking since it ditched the gambling-crime investigative task force seven years ago. Finance Minister Mike de Jong said Monday 22 officers with the Combined Forces Special Enforcement Unit will be dedicated to investigating groups that use gaming facilities to legalize proceeds of crime. He said police will work with the B.C. Lottery Corp. and the Gaming Policy Enforcement Branch as part of the Illegal Gaming Investigation Team. One of the challenges of being a criminal with wads of illegal money is how to make all that dirty cash seem legitimate. No problem - bring in $8,000 or $9,000 from drug deals and use it to buy gambling chips. Make a few small bets, then cash in your chips. You get a casino cheque that indicates your money is legal winnings from gambling." Times Colonist

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Sixth suspect arrested in gangland slaying
A sixth suspect in the fatal gangland shooting of Mohamed "Magic" Najdi was to face charges of first-degree murder and kidnapping at a court appearance Friday on the heels of his arrest in the Toronto area. Nedeljko Borozan, 26, was arrested Thursday and brought to Ottawa where homicide detectives were to interview him for what they allege is his role in the Jan. 10 kidnapping-turned-killing of Najdi. Borozan's arrest comes after five others have already been charged with first-degree murder and kidnapping. (…) An immigration ruling calls Borozan a "stateless person" who was born in 1989 in Yugoslavia. Borozan failed to appear in court in 2013 and a warrant was issued for his arrest. Borozan then failed to report to the Canada Border Services Agency, as he was required to do. According to a December 2008 newsletter from St. Thomas the Apostle Anglican Church, Borozan came to Canada in 1996 from Yugoslavia with his mother and brother on a "special ministerial permit" because his brother had cerebral palsy, At that time he had graduated from high school and was working full-time to earn money for university tuition, the newsletter said. In 2013, a CBSA officer and members of the Ottawa police Direct Action Response Team - the anti-gang suppression unit that is no longer operating in the city - went to his home, but his mother said he was probably at his girlfriend's house. His mother promised to personally take him to the police station the next day to turn himself in, but that didn't happen. Ottawa Citizen, A6 (Ottawa Sun)

*** Local authority calls RFP for Peace Bridge Duty Free contract**
The Buffalo and Fort Erie Public Bridge Authority, owner and operator of the land border crossing at Peace Bridge, is seeking proposals from potential tenants to run the 28,000sq ft duty free shop. The contract runs for 15 years with a five-year renewal option. The Authority owns and operates the Peace Bridge which is located at the Niagara River Crossing between Buffalo, New York and Fort Erie, Ontario. Peace Bridge is the second busiest border crossing between Canada and the USA with around 5.5 million vehicles crossing each year. Sales at the duty free shop have been between C$20 million and C$25 million a year in the past five years. A duty free shop on the Canadian side of Peace Bridge first opened for business in 1986 and was one of the earliest land border duty free shops in Ontario. The current duty free shop has parking for 146 cars, 24 trucks and ten buses. (…) The successful candidate must obtain a license to operate a duty free shop from the Canada Border Services Agency (CBSA). Moodie Report, DFNI Online

*** Lait diafiltré : le gouvernement Trudeau cherche une solution à « long terme »**
Le gouvernement Trudeau reste de marbre devant la grogne des producteurs laitiers qui réclament des mesures concrètes dans le dossier du lait diafiltré. Interpellé à plusieurs reprises sur ce sujet, jeudi, le secrétaire parlementaire du Commerce international, David Lametti, a répondu qu'il était au courant des enjeux. « Nous travaillons avec l'industrie afin de trouver une solution à long terme », a-t-il affirmé. La porte-parole du NPD en matière d'Agriculture, Ruth Ellen Brosseau, a demandé au gouvernement de cesser l'importation de ces protéines ou de compenser les producteurs qui perdent d'importantes

sommes d'argent. Elle a créé une pétition à ce sujet, qui a récolté plus de 4000 signatures en deux jours. (…) Mercredi, l'Assemblée nationale a voté à l'unanimité une motion de la députée caquiste de Mirabel, Sylvie d'Amours, pour harmoniser la définition du lait diafiltré. Québec exige que l'Agence canadienne d'inspection des aliments applique son règlement sur la composition fromagère et considère le lait diafiltré comme un concentré de protéines, à l'instar de l'Agence des services frontaliers du Canada. À l'heure actuelle, une brèche à la frontière permet à ces protéines liquides des États-Unis d'échapper aux tarifs douaniers imposés au lait, aux œufs et à la volaille. Les transformateurs les utilisent dans la production de fromage, par exemple. Huffington Post Québec (2016-04-14)

*** José Figueroa awaiting Canada work permit**

It's been a three and a half months since José Figueroa got his first taste of freedom after spending two years in sanctuary at his Walnut Grove church. Since then, Figueroa has spent his days with his wife and three kids, adapting to life without fear of being arrested by the Canadian Border Services Agency. But the Langley City man's struggles aren't over yet. Figueroa has been waiting for a work permit so he can return to his job and provide for his family. When he was granted a ministerial exemption of his deportation order at the end of December, Citizenship and Immigration Canada (CIC) indicated it would expedite the work permit, saying it should take about 45 days. Figueroa filed the required documents in early February but, still, no work permit has arrived. Langley Times (2016-04-14)

*** Bridge work could complicate international crossings**

Just as the busy travel season begins, two big bridges have major construction underway. The Peace Bridge continues building ramps to the Niagara section of the Thruway while work gets underway at the Lewiston-Queenston Bridge. "We're doing Phase One of the Lewiston plaza," said Niagara Falls Bridge Commission General Manager Lew Holloway. "We built a new duty-free which is now operational. It was operational in August. We're re-aligning I-190 as it crosses the plaza to the north to free up more space on the plaza so we can free up more space for Phase Two. We're working with GSA right now to sign a lease so that we can proceed with Phase Two." Holloway says phase two will be a $60 million project for a new headquarters and processing point for Customs and replacement of ten inspection lanes with 16 inspection lanes and a bus lane. The Ontario end of the span was completely re-built several years ago in a much larger project. WBFO 88.7

Belligerent woman may not be criminally responsible

An Edmonton woman who admitted she attacked several people, bit a woman and tried to strangle a dog, could be found not criminally responsible. Danh Thi Nguyen, 41, pleaded guilty Dec. 15, 2015, to charges of assault causing bodily harm, assault and causing distress to an animal. A judge, however, struck down her guilty plea Thursday as a result of a recent psychiatric assessment. Provincial court Judge James Wheatley then adjourned the case to June 20 for a hearing to determine whether Nguyen is not criminally responsible because of a mental disorder at the time of the attack. A psychiatric assessment says Nguyen suffers from a major depressive disorder with psychotic features. Court heard Nguyen is also subject to a deportation order and must leave Canada and return to Vietnam. Edmonton Journal, A3 (Edmonton Sun)

Cocaine courier Learning convicted, bail revoked

Almost five years after a lone courier collected a cocaine shipment in the pitch darkness of a prairie night near the remote Saskatchewan-Montana border and hauled it to B.C., he has reached the end of the road. Ronald Charles Learning, who had been on bail, left court in handcuffs Thursday after Regina Provincial Court Judge Marylynne Beaton convicted him of possession of cocaine for the purpose of trafficking. "The Crown will be asking for a significant period of incarceration," Crown prosecutor Doug Curliss said. He referred to a recent ruling in which a drug courier who moved two kilograms of cocaine got a seven-year prison sentence - and noted this case involves 30 kilos worth between $1 million and $2.3 million depending how it was packaged for sale. (…) Learning was a one-offcourier in a large-scale drug shipping network that moved 1.3 tonnes of cocaine from California, across the remote Sask.-Montana border and into B.C. between late 2009 and October 2011. Known as Project Faril, the investigation uncovered the largest drug smuggling case in Saskatchewan. Leader-Post, A3

Eliminating the barriers

Marie Antoinette Pangan doesn't want to see other immigrants forced to take the same pathway she did in becoming a permanent Canadian resident. Pangan, who is originally from the Philippines, came to P.E.I. in 2010 through the Temporary Foreign Worker Program (TFWP) with a group of about 30 others to work at a fish plant in Bloomfield. Today, the 33-year-old is a permanent resident finishing up her first year of nursing at UPEI while also working part-time at a Charlottetown nursing home. However, the journey wasn't without challenges. In particular, Pangan said finding a full-time job and saving up settlement funds were two barriers that still plague many foreign workers. "There's not always a full-time job you can apply for, that's the number one barrier," said Pangan. "Number two is the low wages from temporary jobs. In order to gain permanent residency, you have to have savings. Especially for me, my son was in the Philippines at the time, so I needed more savings than other temporary foreign workers to bring him here." Granting permanent residency to temporary workers upon arriving in Canada was one of the key recommendations proposed during a forum on migrant workers' rights at UPEI last weekend. The forum was put on in partnership by the Cooper Institute, KAIROS Canada, the Canadian Labour Congress, The Canadian Union of Public Employees and several other community groups. It brought together nearly 100 individuals, including many migrant workers, to discuss recommendations for the federal government's current review of the TFWP. The Guardian, A4

Family demands answers about man's suicide in jail

The family of an inmate who killed himself in solitary confinement at Ottawa's jail is worried he was placed in the cell and locked up for 23 hours a day as punishment for refusing a transfer to another jail. The niece of Yousef Hussein said that when her mother tried to visit her younger brother on Friday at the Ottawa-Carleton Detention Centre, she was turned away, even as other prisoner visits continued as scheduled. (...) Hussein had been in the jail for the past two years and was expecting to spend another year there awaiting trial on allegations he was a serial sex predator. Hussein was charged in May 2014 after a months-long police operation to track a man who had been sexually assaulting women across the city since 2012. Hussein was accused of choking and sexually assaulting five women and an attempted attack on a sixth. Some of the attacks occurred in the victims' homes, and police had DNA evidence allegedly linking Hussein to at least three of the attacks. Hussein maintained his innocence but was frustrated by the slow progress of the case through the criminal justice system, according to lawyers Michael Johnston and Leonard Shore. Hussein, a Jordanian national who was in Canada on an expired student visa, was also subject to a deportation order. Ottawa Citizen, A4

OCI considering temporary foreign workers for Fortune plant

Ocean Choice International (OCI) has job openings at its fish plant in Fortune but apparently no takers. Ocean Choice International placed a province-wide ad for trimmers for the company's plant in Fortune recently but didn't get much response. Karen Caines, president of the Fish, Food and Allied Workers (FFAW) union at the facility, confirmed Wednesday the possibility of bringing in temporary foreign workers has been raised in recent weeks. "The company has discussed it with the workers and with myself, but there's nothing definite," she said. "I'm waiting now for to hear back from the company to see what the position is on it." The fish plant hasn't operated since December, Caines said, and there isn't a firm date to re-open yet. (...) Temporary foreign workers have been utilized at other fish plants in the province, but should OCI do so in Fortune, it would be a first for the Burin Peninsula. The region once had numerous fish plants, but there are currently just three left. OCI has another plant in St. Lawrence and Clearwater Seafoods operates a facility in Grand Bank. Last month, the federal government approved a one-year change that will allow fish processing plants to bring in an unlimited amount of temporary foreign workers for a maximum of six months. St John's Telegram (2016-04-14)

Reverse migration is a good thing

A letter to the editor states, "Could it be that 'Sunny Ways' and the federal Liberals are on a different path than 'Happy Days' and the P.E.I. Liberals? Recently, the federal government changed the rules to allow Island processors to hire an "unlimited number" of temporary foreign workers to work in P.E.I. plants. In the throne speech, the MacLauchlan government announced plans to 'repatriate young Island workers' who have left P.E.I. for rosier employment pastures. Seems to me, even with a new initiative, the number of available jobs here is going to be minimal at best, and non-existent at the least. P.E.I. lost 2,200 jobs last year, so the task of even getting back to square one is going to be monumental. It would, however,

be good to see Islanders migrating this way for a change, and not just as 'old' people my age who want to retire here. I wish the government much luck in its endeavor; they will need it. Perhaps they should ask Justin to back off, just a bit." The Guardian, A6

CYBER SECURITY / CYBERSÉCURITÉ

*** Microsoft suit is latest tech clash with US over privacy**
As we live more of our lives online, the companies we trust with our digital secrets are increasingly clashing with authorities who want access to the messages, pictures, financial records and other data we accumulate in electronic form. Microsoft opened a new front in the battle over digital privacy this week, suing the Justice Department over its use of court orders requiring the company to turn over customer files stored in its computer centres often without notifying the customer involved. It's the latest in a series of legal challenges brought by Microsoft and some of its leading competitors. Apple recently fought a high-profile battle over the FBI's demand for help unlocking an encrypted iPhone in San Bernardino, California, and it's continuing to challenge similar demands in other cases. Other companies, including Google, Facebook and Yahoo, have increased their use of encryption. They've also sued for the right to report how often authorities demand customer information under national security laws, after former National Security Agency contractor Edward Snowden leaked details of government data-gathering efforts. Privacy advocates have applauded those moves, while authorities complain they could stymie legitimate investigations. Associated Press (Telegram, Guardian, Waterloo Region Record)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Four men charged for alleged sexual assault of teen
Four men have been charged after a 14-year-old girl said she was sexually assaulted at a house party. Police say the men - two Nova Scotians, two from Ontario, all in their 20s - were arrested after the girl reported that she had been sexually assaulted at a party in Bible Hill, N.S. "To me, it's quite unusual for us to investigate something of this seriousness with that age of a victim," said Cpl. Jennifer Clarke, spokesperson for Nova Scotia RCMP. All four men are charged with sexual assault and sexual interference. The girl went to Colchester District RCMP on Dec. 18. Police say the two Nova Scotians, both from Colchester County, ages 21 and 23, were arrested in January. A 27-year-old Sarnia, Ont., man was arrested on March 31, and a 25-yearold Cornwall, Ont., man was arrested in Ottawa on April 12. Both were returned to Nova Scotia by the RCMP, with help from the Canada Border Services Agency. Red Deer Advocate, B4 (Times Colonist)

Bail a work-in-progress for man accused of shooting at Red Deer RCMP detachment
Bail terms are still being worked out for a young Red Deer man accused of shooting BB rounds at the Red Deer RCMP detachment. Police allege that two windows were hit and damaged by pebble-sized shots on the afternoon of March 14. A suspect vehicle was pulled over shortly afterward. Cory Daniel Picard, 21, was arrested on charges of possessing a weapon for a dangerous purpose, using an imitation firearm to commit an offence, mischief causing less than $5,000 in damages and uttering threats. Now in custody at the Calgary Remand Centre, Picard appeared via video feed in Red Deer provincial court on Wednesday, represented by Red Deer defence counsel Brad Mulder. Mulder advised the Court that he is working out bail terms, but needs to secure a suitable housing arrangement for his client, who has been diagnosed with autism. Mulder said he is also awaiting additional disclosure before he can take further instructions on behalf of his client. Red Deer Advocate

Many came together after RCMP officer's death
A letter to the editor by Const. Roz Guineau states, "Tuesday, the day of RCMP Const. Sarah Beckett's funeral, was both horribly sad and bittersweet. As I waited in formation, for hours, with hundreds of my fellow first responders, I had a chance to reunite with co-workers and friends. The sharing of our stories about Sarah and our past exploits, both humorous and macabre, seemed to release a bit of the hard knot inside our hearts. When the hearse arrived, however, not a sound was heard except the catch in our

throats. As we started to march, the sky opened up and it poured down rain. It was like the heavens themselves could no longer keep the grief in. I have always held the belief that funerals are not for the departed but for those left behind. It is like a salve on the open wounds of our hearts, soothing the ache and allowing for the start of healing. The coming together and celebrating the life of our loved ones screams out to the universe that they were loved, that their life meant something and that they will not be forgotten. I believe we accomplished that Tuesday." Times Colonist, A13

RCMP has global encryption key for BlackBerrys

If you're used a BlackBerry at some point in the last six years, you're probably going to want to know about this. On Thursday, Canadians discovered that the Royal Canadian Mounted Police has had access to a global encryption key for Black-Berry devices since 2010. According to Vice, the revelations were contained in court documents that were made public after Montreal mobsters pleaded guilty to their roles in a 2011 murder. Dur ing an inves tigation into Montreal's criminal underworld, the RCMP intercepted about one million PIN-to-PIN BlackBerry messages. Government lawyers then spent almost 48 months trying to keep this fact from the public record. This global key means that Canada's federal policing agency has the ability to break the encryption on almost any message sent between BlackBerry devices. In a technical report filed with the Superior Court of Quebec, the RCMP called the key a tool "that would unlock the doors of all the houses of the people who use the provider's services, and that, without their knowledge." Toronto Sun, A17

No quick fix to Surrey's issues: RCMP

Prevention and intervention - in addition to enforcement - are key to solving Surrey's problems with drugs and gun violence, according to assistant commissioner Bill Fordy. "We will arrest the people involved in these issues, but in the long term we will not arrest our way out of this issue," Fordy, the officer in charge of Surrey RCMP, said during a Surrey Board of Trade lunch on Thursday. "I believe we will educate our way out of this issue." So far this year, there have been 32 shootings in the city related to a dial-a-dope turf war between two unnamed, low-level groups. It's similar to the turf war that played out on Surrey streets last year, however the groups involved are different. "The individuals involved in the drug trade may change, but the problem remains the same," Fordy said. "Young people are being lured into the lifestyle with illusions of money and power, but the reality is much, much different." Fordy said they're driven by greed and the issue goes beyond the police and involves the entire community, parents, extended family and friends, schools, business owners and prevention programs. Surrey RCMP are working with the school district and the city to come up with more early intervention programs - such as the Wrap Project, Code Blue and Youth Intervention Program - for young people so they can avoid getting into a criminal lifestyle in the first place, and Fordy said police are more engaged and visible in schools than ever. Province, A4 (Vancouver Sun)

Surrey shootings: where they took place - and when

Surrey RCMP are dealing with 33 instances where shots were fired this year, many of them targeted shootings. Police have confirmed information on the 23 incidents outlined in this interactive map. They will not provide details on the other 10 reports of shots fired. "There have been and will be times when it is not in the public's interest for the police to disclose a shooting," assistant commissioner Bill Fordy said at a news conference. The majority of the shootings in Surrey are linked to conflict caused by the drug trade. CBC News

RCMP not fooled by scheme to cover up car crash

Turning the ignition and putting the Nissan Versa into gear on the evening of Nov. 24, 2014, Richard James Ouimette tipped the first of several dominos that led to multiple guilty pleas on Thursday morning. Just before midnight on that November 2014 night, the Grand Bay-Westfield RCMP detachment received a call from Ouimette, 47, about a break-in and theft at his Nerepis home. This was uncanny, since officers had been at the same home looking for Ouimette a little more than an hour earlier. They found his place on Brittain Road dark, and no one home. Now, Ouimette was saying someone had smashed some glass, entered his home, taken a set of car keys and made off with the 2007 Nissan Versa he'd been fixing up for someone. That same car was what had brought police to Ouimette's home in the first place. They had received a call earlier that evening from Fredericton Police about a vehicle that had rolled over off the road. The driver had fled the scene, and when they called the owner, he said it had been in Ouimette's

care for repairs - the Versa. Ouimette said he had been in Saint John for dinner that night. The rouse was someone else must have stolen the car, crashed it in Fredericton and ran off. The RCMP officer wasn't buying it. Telegraph –Journal, B3

RCMP investigate man's body in woods

The RCMP is investigating the discovery of a man's body on a trail in the Fredericton area. Cpl. Marc Fortin said a hunter, who was checking his deer stand and game cameras, came upon the man's remains in Hanwell on Wednesday evening. He said that shortly after 5:15 p.m., police received a call from the hunter who said that while he was in the wooded area he stumbled upon the remains that appeared to have been there for a while because of the decomposition of the body. "It was confirmed when we arrived with the coroner," Fortin said. He said foul play isn't suspected. An autopsy will be conducted within the next couple of days to confirm the identity of the man as well as approximately when and how he died, he said. He said after the autopsy there will be more information available. "We have some identification for the person, but there is more that needs to be ascertained." Daily Gleaner, A3 (Times & Transcript, B2)

Mountie acquitted of assault charges

An RCMP officer on Vancouver Island has been acquitted of aggravated assault at his second trial. A B.C. Supreme Court judge in Nanaimo acquitted Const. David Pompeo Wednesday, 18 months after the B.C. Court of Appeal ordered a new trial after a September 2009 shooting. William Gillespie was pulled over south of Nanaimo on suspicion of driving while prohibited, and Pompeo testified he fired because he believed the man was armed and going for a gun. In throwing out the original conviction and its sentence of 24 months probation and 240 hours of community service, B.C.'s highest court ruled the trial judge compromised the appearance of fairness during questioning. Vancouver Sun, A12 (Province)

Fredericton police officers fired, suspended and/or facing criminal charges

Jeffrey Smiley and Cherie Campbell, former constables with the city police force, were fired after arbitration decisions to dismiss both following separate complaints of misconduct. They have filed separate applications for judicial review with the Court of Queen's Bench. The applications have been tentatively scheduled to be heard in June. Const. Darrell Brewer is scheduled to stand trial for two days this month on a charge of impaired driving, stemming from an incident Aug. 23. Cpl. Louis Lafleur will stand trial June 21 on alternate counts of having care and control of a car when impaired and having care and control of it with an elevated blood-alcohol level in connection with a July 8 incident in the city . Sgt. Tim Sowers will be sentenced June 6 on a summary charge of uttering threats to cause death and/or bodily harm and on a charge a charge of summary assault. The incidents occurred June 25 and July 11 of last year. All officers face complaints under the Police Act once their court cases are concluded. Another officer is under investigation by the RCMP in connection with an allegation of misappropriated funds while serving on the executive of the New Brunswick Police Association, an organization representing unionized municipal police officers in the province. Daily Gleaner, A7

Man faces murder charge in break-in

Late at night last Saturday, two men entered a small home in the 3,000-person town of Botwood, N.L. One would flee. The other would be fatally shot. And Gilbert Budgell, the 53-year-old man whose home they were allegedly invading, is now in police custody facing the unusually severe charge of second-degree murder. RCMP are not releasing any more details, but as is typical when police lay charges against a homeowner in a suspected self-defence scenario, the Budgell case has provoked a sharp response from across Canada. "If someone invaded my home while we were inside putting my family at risk they'd be full of bullet holes too," reads a typical post. "I'm glad he shot him. He is a hero in my book," reads a post on the Facebook page of a fellow Botwood resident. Generally, Canadian law gives residents a wide latitude to legally use violence to defend their home. As is specified in the criminal code, violence is entirely legal if someone has "reasonable grounds" to believe that the "threat of force is being made against them or another person." StarPhoenix, N3 (Province, Leader-Post)

Bomb threat closes Nanaimo school

Nanaimo District Senior Secondary, attended by more than 1,000 students, was cleared for reopening about 11:30 a.m. Thursday after Nanaimo RCMP investigated a bomb threat. Police evacuated both the school and the nearby Nanaimo Ice Centre after being called about 8 a.m., said Nanaimo RCMP Const.

Gary O'Brien. Police are not saying how the threat was received. A search using an explosivessniffing dog turned up nothing. "It was decided in consultation with the school, based on our opinion, that it was safe to go in," O'Brien said. Times Colonist, A3

Man admits being party to assault
A Moncton man will be sentenced next week after admitting to his role in an assault. Meneka Weva, 40, appeared in court on Thursday and pleaded guilty to being party to the assault of Matthew Saulnier on Oct. 13, 2015. Other charges, including break and enter, were withdrawn. Sentencing will take place April 20 and the court was told a recommendation will be made for time served. Weva has been in custody since Oct. 16. Codiac RCMP said in a news release at the time that shortly after 11 a.m. on Oct. 13, police responded to a report that a 50-year-old woman had been abducted from her Gordon Street home in Moncton and driven to Sackville. She was released by her abductors without injury. The perpetrators later returned to her home, where a 26-year-old man was threatened and assaulted during a home invasion. The man sustained serious injuries and was treated at the hospital. Times & Transcript, A12

Weapons call leads to two arrests
A weapons call near West Kings High School on Wednesday led to the charging of two youths on Wednesday night. Three boys and one man were arrested by police at the scene. After further investigation, the man and one of the boys were released without charge. "We just know there were individuals in the area, and we released two because after investigation, they didn't appear to be involved," said Cpl. Jennifer Clarke with the RCMP. A 17-year-old boy from Kingston is facing two counts of careless use of a firearm and unauthorized possession of a firearm. A 15-year-old boy from Auburn is facing two counts of careless use of a firearm, one count of pointing a firearm, unauthorized possession of a firearm, and failure to comply with conditions. "He was under court-ordered conditions," said Clarke, who didn't elaborate further. Early in the afternoon on Wednesday, police responded to an incident that occurred near the school in Auburn, Kings County. RCMP seized a .22 calibre rifle and ammunition from a residence near the school. The school was placed in a hold and secure while police responded to the weapons call. Chronicle Herald, A6

RCMP ask for help locating missing Windsor teen
Windsor District RCMP is appealing for public assistance to locate Windsor teenager Alicia Michelle Nicole McInnis, who has been missing since early March. McInnis is described as a 5'8" tall Caucasian female with a thin build, long brown hair and brown eyes. She was last seen wearing black leggings, a grey hoodie, a white sweater and boots. She has a red lip ring on the right side of her bottom lip. She has the word 'fighter' tattooed on her left wrist and the word 'and beyond' tattooed on her right wrist. McInnis has been in contact with a friend on Facebook, but both her family and police have expressed concern for her safety and want to know her whereabouts. She has been known to go for extended periods of time without contacting friends or family. Chronicle-Herald

Bones found near Hwy 2 are human
The Calgary Medical Examiners office has determined the bones found in a wooded area near Innisfail are human. The bones were found west of Hwy 2, north of Antler Hill around 7 p.m. on April 5. Innisfail RCMP detachment is working with the Calgary Major Crimes office and the Medical Examiners office to determine the sex, age, identity and length of time the remains were there. Red Deer Advocate, A5 (Calgary Sun); * Calgary Herald

*** DNA testing used to determine identity of Japanese woman who vanished in 2014**
"Scant" human remains found in the woods near Giant Mine last summer were those of Atsumi Yoshikubo, a Japanese tourist who went missing in October 2014. RCMP spokesperson Const. Elenore Sturko stated in a news release Thursday that DNA forensic analysis of bone fragments confirmed her identity. The cause of death remains unclear. The 45-year-old woman had come from Japan to visit the city and was reported missing when she didn't check out of her hotel. Extensive searches by RCMP as well as search and rescue volunteers in the area around the Ingraham Trail, the former mine site and Yellowknife Ski Club failed to find her remains. Then in November of 2014, police mysteriously announced Yoshikubo planned to disappear into the wilderness and took steps to avoid being found. Police haven't disclosed their reasons for that statement. Two Japanese media outlets reported she wrote

a suicide note before leaving Japan. On Aug. 31 last year, a resident hiking near Giant Mine called police to report what were believed to be human remains. The exact location of where the scattered bone fragments were found has not been publicly disclosed. Yelllowknifer

Atcon probe with federal investigators, says woman who filed initial complaint
A complaint filed with the RCMP over the Atcon bankruptcy is now in the hands of the police force's federal investigators, says the woman who originally brought forward the grievance over the disgraced Miramichi company. But there are also now questions as to whether some of the documents can be used. The Progressive Conservative Opposition handed over Atcon's backup computer servers in December to the RCMP after revealing that the party purchased them at a bankruptcy auction in 2013. The servers did not launch a new complaint with the RCMP, but instead supported an existing one filed by Marie-Paule Martin. It was Martin who launched an initial complaint last November, believing questions remain as to where all the Atcon loan money went. The Miramichi company's bankruptcy cost taxpayers close to $70 million. Martin now says she has been visited by RCMP federal operations Sgt. Michel Boissonnault. "He told me that he has formed a crew," Martin said. "They have brought people from all over the place, including from outside of the province, to Fredericton. "These are people who are going through all the documents." She added: "It's moving forward." Martin said specialists in accounting are a part of the team. But she added that there is also the question of whether the Atcon servers can be used as evidence, stating that Atcon officials could contend that accessing the remaining information is a break of privacy. "They have to study if those computer servers have been legally acquired," Martin said. "That's the catch." RCMP spokeswoman Const. Jullie Rogers-Marsh told the Telegraph-Journal that there "is no update" to provide on the Atcon complaint. "We're still looking at the information," Rogers-Marsh said. Times & Transcript, B1 (Daily Gleaner, Telegraph-Journal)

'I'm so ashamed,' ex-Mountie talks about assault of former spouse
Telling a court he is very ashamed of his actions, a retired RCMP officer was handed a conditional discharge and ordered to pay $1,000 to a women's shelter for assaulting his former spouse. "I am so ashamed of myself," Timothy Coxon, 47, told a judge of the domestic violence court in Regina Thursday. "I am appalled with myself. No abuse is acceptable. None whatsoever." According to information provided to the court, on different times over the course of several months from late 2011 and 2012, Coxon assaulted his former spouse in different ways. In one incident, she was pushed hard into a table. Another time he slapped her on the throat. While the incidents took place on different dates, Coxon was allowed to plead guilty to a single count of assault. He was employed with the RCMP at the time of the incidents, which took place during off-duty hours. After court, Coxon's former spouse expressed some relief that the case was concluded. "I am grateful it's over," Colette Beliveau said. Earlier, in her victim impact statement to the court, Beliveau said her life has been immeasurably changed by what happened. "I will not forgive Tim Coxon for what he robbed me of," she said, fighting back tears. "Tim Coxon used his position of authority with the RCMP to wreak havoc on my world." She said she now suffers from depression, anxiety, headaches and panic attacks. Coxon has no criminal record and successfully completed a domestic violence treatment program. CBC News

Mountie gains fame after helping Lewisporte youngsters
An RCMP officer in Lewisporte gives youth a lesson in safety and a helping hand. Constable Andre Sparkes of the Lewisporte detachment of the RCMP helped some local youth out of a tough spot today. Kim Moyles of Lewisporte is amazed that a video and photos she posted to Facebook of an RCMP officer helping her son and daughter, and their friend, get her son's dirt bike out of the mud had been viewed more than 26,000 times just hours after the post. The Telegram

Yellowknife's 4/20 event has been moved to April 24.
The marijuana celebration is normally held on the 20th day of the fourth month but Yellowknife organizer Kim McNearney said it's being moved to the following Sunday to allow more people to attend. The event will be held at Somba K'e Civic Plaza beside city hall beginning at 3:30 p.m. and includes a march through the downtown passing by RCMP headquarters and the courthouse. Yellowknifer

* **Criminals Now Getting Their Guns In Canada**
Langley resident Christina Stover obtained a firearms acquisition licence just last year, which entitled her

to buy weapons at any gun store in Canada. Within a matter of months, the 40-year-old former security guard had legally purchased 19 firearms. in March 11, police allege Stover, who had no prior criminal record, delivered a cache of guns to two men at their rented Surrey home on 192nd Street. All three were arrested the same day. Ridge Meadows Supt. David Fleugel said the "investigation has resulted in police seizing a number of firearms that were being stored illegally, and may have been destined for a criminal element in a number of communities." Police seized nine firearms, including handguns, rifles and shotguns, he said. Sources confirm that several firearms bought by Stover since last year have not been located. The investigation continues. Police see a disturbing shift in how B.C. criminals are getting their guns. They now obtain most of their illicit firearms within Canada, either by stealing them from legal owners or using straw purchasers who have licences to buy them. According to the most recent data available from the RCMP's National Weapons Enforcement Support Team (NWEST), 61 per cent of crime guns in the province were domestically sourced. "And the balance, about 39 per cent, were believed to be smuggled from the United States or elsewhere. The source was not domestic," said Insp. Chris McBryan, the officer in charge of NWEST's western region. Vancouver Sun, A1 (Province)

* **Senior robbed as she slept**
Pieces of valuable heirloom jewelry, including wedding bands, were stolen from a 102-yearold woman after someone broke into her southern Albert a home Sunday while she was sleeping. Turner Val-ley RCMP were called Sunday to a home about a break-in. Police said the culprits got into the senior's home through an unlocked window and made off with a "sizable amount" of heirloom jewelry, including a unique golden wedding band. The items were of "significant sentimental value" to the woman and her family, police said. It's believed the senior, who was home alone, may have been specifically targeted. Ottawa Sun, A17

* **Lawyers argue over cop's punishment**
The lawyer for the Toronto police officer found guilty of misconduct after ordering the "kettling" of hundreds of people during the G20 says docking him no more than 10 banked days is plenty of punishment for his actions during the summit. Supt. Mark Fenton was found guilty last year of two counts of unlawful arrest and one count of discreditable conduct under the Police Services Act for ordering the kettling of people in a rain storm during the 2010 G20. Hundreds of innocent people were swept up in two mass arrests - one at Queen St. and Spadina Ave., one near the Novotel Hotel on the Esplanade. His sentence is being determined at an ongoing police tribunal hearing. The prosecution argued for a one-year demotion in rank and lawyers representing people detained during the arrests said he should be dismissed. Fenton's lawyer, Peter Brauti, argued Thursday that the prosecution's call for demotion was "too harsh" and the complainants' call for dismissal "patently unreasonable," and would not respect the principle of progressive discipline. Instead, he is arguing Fenton should be docked no more than 10 banked days owed to him and/or receive a reprimand. Brauti said the 56-year-old cop had already paid a personal and professional price for his actions six years ago, and the hearing has had a direct result on his health and contributed to the end of his 20-year marriage. He argued Fenton has an "exemplary police record" and is a "highly dedicated officer." Toronto Star, GT3

* **A message needs to be made with police officer's sentencing for G20 'kettling'**
Superintendent Mark Fenton took charge of police on June 27, 2010 when people had taken to the streets of Toronto to protest the G20 meeting of world leaders, which led to the chaotic affair. When Mark Fenton took charge of a police command centre on June 27, 2010, Toronto was in a state of nervous disarray.The day before, thousands of people had taken to the streets to protest the G20 meeting of world leaders. A militant minority had roamed all but unchecked through downtown, smashing windows, burning police cars and hurling projectiles at police officers. Police were worried about a crowd that had reached the intersection of Queen and Spadina, a few blocks from City Hall. Reports came in that militants might assault the security fence protecting G20 dignitaries. Superintendent Fenton, a veteran commander who had immigrated to Canada from Ireland in 1982, took a fateful decision. He ordered police at the scene to surround the crowd. What followed became the most controversial episode of the G20 weekend: the "kettling." Within five minutes of Supt. Fenton's order, the crowd was boxed in, or kettled, in the centre of the intersection, with walls of police on all four sides. Then the weather started to change. The sky grew dark as rain clouds moved in. The temperature dropped, turning the warm air chilly. It started pouring. Globe and Mail

*** More funds to fight crime**

A 10-year-old organization that fights crime by uniting municipal police forces, Alberta Sheriffs and the RCMP received a boost in Thursday's provincial budget. The 2016-17 budget provides $2.6 million in new funding for the Alberta Law Enforcement Response Teams. The non-profit umbrella organization will receive $29.1 million in provincial funding under this budget, compared with $26.5 million in 2015-16. "That will support ALERT to continue doing the good work that they are doing," said Minister of Justice and Solicitor General Kathleen Ganley. "We've certainly heard from a number of partners, both in the policing world and various municipalities, that this program is really important for them." In addition, $2 million is being spent to transfer 40 sheriffs from both the Safe Communities and Neighbours (SCAN) team and the Surveillance unit back to the department. The officers will continue to preform the same duties they do now, but they'll do some with money under the Justice and Solicitor General budget instead of the ALERT budget. "It's about $4.6 million overall that came in," Ganley said. Created by the government in 2006, ALERT is a 280-member agency that brings together teams from across Alberta to investigate fugitives, grow ops, child pornography, cybercrime and other large cases. The group disrupts and dismantles serious and organized crime across the province. Calgary Herald, A7 (Calgary Sun)

*** RCMP has global encryption key for BlackBerrys**

If you're used a BlackBerry at some point in the last six years, you're probably going to want to know about this. On Thursday, Canadians discovered that the Royal Canadian Mounted Police has had access to a global encryption key for Black-Berry devices since 2010. According to Vice, the revelations were contained in court documents that were made public after Montreal mobsters pleaded guilty to their roles in a 2011 murder. Dur ing an inves tigation into Montreal's criminal underworld, the RCMP intercepted about one million PIN-to-PIN BlackBerry messages. Government lawyers then spent almost 48 months trying to keep this fact from the public record. This global key means that Canada's federal policing agency has the ability to break the encryption on almost any message sent between BlackBerry devices. In a technical report filed with the Superior Court of Quebec, the RCMP called the key a tool "that would unlock the doors of all the houses of the people who use the provider's services, and that, without their knowledge." Toronto Sun, A17; Financial Review; iClarified; Gizmodo; Techradar; WCCF Tech, Numerama; LesEchos.fr

*** Fired police officer, spouse sue city, federal government over assault investigation**

A fired police officer and his commonlaw spouse are suing the City of Fredericton and the federal government over an investigation into alleged domestic violence that ultimately led to his dismissal. Formerly Fredericton Police Force member Jeff Smiley and his partner Kimberly Burnett filed a statement of claim with the Court of Queen's Bench in Fredericton last week, naming the city and the Attorney General of Canada as defendants in the lawsuit. It notes those defendants are the employers of relevant members of the Fredericton Police Force and RCMP, respectively. Smiley was investigated, initially by the Fredericton police and then by the RCMP, in February 2014 for a suspected instance of domestic violence. He was later charged with assault and with breaching a police undertaking he signed after his initial arrest. When the matter went to trial in the fall of 2014, the assault charge was dismissed, as it was found to have occurred outside of New Brunswick, and a judge acquitted Smiley of the breach allegation. However, after a Police Act hearing into the allegations, an arbitrator ordered Smiley's dismissal in December 2015, finding he engaged in domestic abuse and other acts of misconduct. Among the allegations the couple makes in its statement of claim are that Fredericton police Chief Leanne Fitch offered Smiley an $80,000 settlement to resign from the force or she would proceed with a Police Act disciplinary process against him. "The plaintiffs say that this conduct constitutions extortion and malfeasance in public office, as Fitch knew that such conduct was likely to harm the plaintiffs," the document states. None of the allegations in the lawsuit has been proven in court. (…)The court document contends further that the RCMP investigation into his case was carried out improperly and negligently, and that the subsequent prosecution was malicious. Furthermore, the statement of claim alleges RCMP Const. Nicholas Steeves threatened and intimidated Burnett when she refused to provide an incriminating statement against Smiley in the assault investigation. Daily Gleaner, A2 (Times & Transcript)

*** Overdoses prompt public emergency**

An alarming number of drug overdose deaths in recent months has prompted B.C.'s chief health officer to declare a public health emergency. The declaration, typically reserved for a contagious disease outbreak,

is the first in Canada, where a rash of fentanyl overdoses has claimed hundreds of lives. Provincial health officer Dr. Perry Kendall on Thursday cited more than 200 overdose deaths in B.C. during the first three months of 2016, a pace that would lead to 800 deaths this year if it continued. The move is aimed at quickly gathering information on all incidents of drug overdoses - not just deaths - in order to warn users and provide help. That could include more opiate substitution programs like methadone and suboxone and wider distribution of antidote kits. First responders, emergency room staff and the B.C. Coroners Service will now provide the time and place of overdose, which drug was used, how it was taken, along with the age and sex of the patient. That would be shared with provincial health authorities and compiled at the B.C. Centre for Disease Control and ultimately made public. "We can look at where the overdose happened to see if there are hot spots or danger zones or places where we'd want to send harmreduction outreach," Kendall said. Fatal overdoses have steadily increased in B.C. since 2010, when 211 people died, reaching 474 deaths in 2015, Kendall said. Fentanyl - an opioid 100 times more powerful than morphine - was associated with a third of the deaths. People who work on Vancouver's Downtown Eastside say they're witnessing the health emergency each day. Coco Culbertson, housing manager for the Portland Hotel Society, said the number of overdoses began rising dramatically at the end of 2014. "I would say it's probably been a state of emergency for some time," she said. "We haven't seen overdoses and deaths at this level since the late '90s, pre supervised injection sites." Data gathered during the health emergency will not be used for law enforcement. The Province, A6 (Vancouver Sun)

*** Bay Roberts, Harbour Grace now separate RCMP detachments**

Bay Roberts and Harbour Grace now have separate detachments following a reorganization of the former Trinity Conception RCMP service. In the mid-1990s, the RCMP amalgamated local detachments across the province to form 11 new policing districts. The Trinity Conception detachment came into existence as a result, with offices in Bay Roberts and Harbour Grace used to serve a regional police unit ever since. A review started in the fall of 2013 to look at the state of the Trinity Conception detachment. According to Supt. Jamie Zettler, eastern district director for the RCMP's B division in Newfoundland and Labrador, the police force recognized changing demographics in the area and was aware specifically of Bay Roberts interest in having its own detachment. After reviewing a report, the RCMP's B division decided a year later that the Bay Roberts satellite office would reopen as its own detachment. Following a one-year transitional period, the Bay Roberts detachment became operational as of April 1. "That work has led to a smooth transition, ensuring public safety is not compromised," said Zettler. Grand Falls-Windsor Advertiser (2016-04-14)

*** RCMP Staff Sgt. Darren Simons receives 25-year Long Service Award**

Staff Sgt. Darren Simons of the Carlyle RCMP detachment received his 25-year Long Service Award in Carlyle on Thursday, April 7, in the presence of his wife, Tracy, his son, Nathan, and his fellow RCMP members and co-workers. Assistant Commissioner Brenda Butterworth-Carr of “F” Division in Regina, said it was “a privilege” to present Simons with his Long Service Award and praised his “leadership, investment in community and dedication throughout his career in each of his postings. Thank you for your service and for your leadership.” Carlyle Observer

*** Ridge Meadows RCMP investigate gun trafficking case that's part of disturbing trend**

Langley resident Christina Stover obtained a firearms acquisition licence just last year, which entitled her to buy weapons at any gun store in Canada. Within a matter of months, the 40-year-old former security guard had legally purchased 19 firearms. Then, on March 11, police allege Stover, who had no prior criminal record, delivered a cache of guns to two men at their rented Surrey home on 192nd Street. All three were arrested the same day. Ridge Meadows Supt. David Fleugel said the “investigation has resulted in police seizing a number of firearms that were being stored illegally, and may have been destined for a criminal element in a number of communities.” Police seized nine firearms, including handguns, rifles and shotguns, he said. Sources confirm that several firearms bought by Stover since last year have not been located. The investigation continues. Police see a disturbing shift in where B.C. criminals are getting their guns. Maple Ridge Times

*** WeeMedical the second dispensary raided in Campbell River**

RCMP in Campbell River, British Columbia executed their second search warrant in a week when they raided WeeMedical, today. On April 6, RCMP raided Trees Dispensary, confiscating product and arresting

branch manager Ben Hinton before later releasing him without charge. No charges were laid in today's raid at WeeMedical. RCMP say this is part of an ongoing investigation, and that dispensaries like these are not legal. "Campbell River RCMP is committed to ensuring local businesses are abiding by federal and provincial law, and will continue to investigate any businesses believed not to be following these laws," said Const Sara Clark, Media Relations officer for the Campbell River RCMP. The City of Campbell River also announced this week that they are seeking to craft a bylaw amendment outlawing marijuana business that are not sanctioned by Health Canada. While these business are already illegal, the city says they want to ensure there is clarity for those seeking to open a dispensary. Lift Cannabis News Magazine (2016-04-14)

*** Homeless take over Nanaimo man's backyard**
Wayne Schmidt couldn't believe his eyes when he woke up this morning. "I look out my back window and there's a camp in my backyard so in disbelief I looked there for a little bit and tried to process what's going on then phoned the police," says the Pine Street resident. A number of homeless people had moved in with their shopping carts and tents overnight, laying claim to his backyard that resembles an empty lot. "And I wake up and look out there and go whoa holy cow," he says. When asked to move, he says they refused. "What do you do? I don't know. So I can't leave the property. I'm just sort of who are these people it's pretty brazen." So his neighbour asked them again while waiting for police, who were held up on other calls. "That is private property it's not fine," yells his neighbour to the campers still inside the tent. "Look what's happened in Victoria. Is this the same scenario? It ain't happening," says Schmidt. "And are other people having this problem? Does the city need to deal with homeless?" Nanaimo City bylaws says year to date there have been 15 calls about squatters in residential neighbourhoods and they are quickly addressed and people are told to move on. (…)So there's relief when about 4 hours after his first call, RCMP arrive and order the campers to move out. Where they've gone though RCMP say could well be someone else's property. CHEK News (2016-04-14)

*** GRC : « Une des plus importantes saisie de drogue aux TNO depuis les 10 dernières années »**
La Division G de la Gendarmerie royale du Canada de Yellowknife a marqué un grand coup aux Territoires du Nord-Ouest le 4 avril dernier en procédant à l'arrestation de 14 individus et en saisissant une importante quantité de drogue et 75 000 $. L'opération nommée « Green Manalishi » s'est déroulée en soirée, le lundi 4 avril dernier, à N'Dilo, Yellowknife et Dettah. Plus de 30 agents ont été déployés pendant cette soirée de perquisition sur laquelle la GRC travaillait depuis le milieu 2015. « C'est une saisie importante, certainement une des saisies en frais de volume les plus importantes des 10 dernières années aux Territoires du Nord-Ouest. Par contre, chaque saisie a un certain impact. Nous sommes heureux d'avoir pu enlever ces quantités de stupéfiants de nos communautés », a commenté le sergent de la Division G de la GRC de Yellowknife, Alexandre Laporte. Quatorze personnes ont été arrêtées dans la soirée du 4 avril, dont plusieurs ont été relâchées depuis. Aquilon (2016-04-14)

*** La GRC dit être plus efficace à Moncton : contraventions en hausse de 35 %**
Le nombre de contraventions décernées par la GRC dans la région de Moncton, au Nouveau-Brunswick, a augmenté de 35 % comparativement à 2015. Le surintendant Paul Beauchesne, du détachement Codiac de la GRC, a présenté ces données à l'Autorité policière régionale de Codiac mercredi soir. M. Beauchesne a précisé que les agents ont décerné 369 contraventions en mars, contre 212 durant le même mois l'année dernière. Il explique ces résultats par des méthodes policières plus efficaces grâce aux renseignements reçus du public. Les policiers resserrent ensuite leur surveillance aux endroits où les automobilistes ont tendance à commettre des infractions. Paul Beauchesne ajoute que la GRC encourage tous ses agents à surveiller la circulation automobile. Il n'est plus question d'une seule unité spécialisée en ce domaine. En janvier dernier, les policiers ont décerné 295 contraventions, contre 264 durant le même mois en 2015. Le nombre de contraventions en février dernier (307) était deux fois plus élevé qu'en février 2015 (150). Radio-Canada (2016-04-14)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Taypotat loses bid for reduced prison sentence
Deadly drunk driver Blaine Thomas Taypotat will get no break on his sentence from the Saskatchewan Court of Appeal. Delivering the court's decision Thursday, Justice Maurice Herauf said the judge who sentenced Taypotat to 9 1/2 years in prison for manslaughter and impaired driving causing death made no error. (With credit for time already served, there were 6 1/2 years remaining at the time of his sentencing in June). Three years ago, Taypotat was driving with a blood-alcohol level three times the legal limit when he "gunned it" after initially stopping at an RCMP roadblock, drove through a crash scene south of Saskatoon, and struck Justin Knackstedt, a 23-year-old conservation officer who was helping to direct traffic. Taypotat then raced offand crashed his own vehicle. Herauf said the Supreme Court noted in a recent decision that courts can consider the prevalence of such offences in one's jurisdiction in determining a fit sentence. "Here we note that Saskatchewan has one of the highest incidences of injury and death caused by impaired driving," he said. That prevalence combined with the fact manslaughter and fatal drunk driving offences can carry life sentences "reinforce our view that there's simply no basis for this court to intervene," he added in a decision made unanimous by Justices Georgina Jackson and Peter Whitmore. StarPhoenix, A11 (Leader-Post)

Dylan Dingwell pleads not guilty
Two New Minas, N.S., residents have entered not guilty pleas to a joint charge of possessing cocaine for the purpose of trafficking. Dylan Alexander Dingwell, 28, formerly of P.E.I., and co-accused Maria Paredrakos-MacCumber, 28, entered pleas in Kentville provincial court April 11 and elected a trial by provincial court judge alone. The April 11 appearance included a bail hearing for Dingwell, who was ultimately released from custody on a $25,000 surety with the Crown's consent. Paredrakos-MacCumber was released on conditions following her arrest. (...) Dingwell was convicted of manslaughter for killing his brother in Charlottetown in 2011. He was released from custody on full parole in 2014. Guardian, A4

*** Rapist's appeal denied by court**
Manitoba's highest court has refused to interfere in a case in which a career criminal went on a random rampage that involved four separate attacks - including the rape of an eight-year-old boy. Peter Laporte was convicted of eight charges following a lengthy trial in 2012 that included 65 witnesses. He was then branded a dangerous offender and given an indefinite prison sentence with no guarantee of ever being released. Laporte, 41, filed an appeal of his conviction, claiming the trial judge shouldn't have allowed so-called similar-fact evidence to be used against him, should have permitted his charges to be severed into separate trials and should have screened out "hearsay" evidence that was used against him. Winnipeg Free Press

*** Inmates used shirts to sop up blood of victim, inquest told**
A Stony Mountain Institution corrections officer found it "bizarre" inmates leaving the prison's recreation hall were wearing jackets over their bare chests. But it didn't take long for Vincent Larouche to realize what happened when he found inmate David Tavares lying on the ground after following a blood trail. "His head was in a pool of blood," Larouche told an inquest Thursday looking into Tavares' death. "We started CPR... I had noticed a lot of (the other inmates) had no shirts on under their jackets. I thought it was bizarre. "I guess a lot of them used their personal shirts to mop up the blood." Tavares, 40, of Thunder Bay, Ont., died March 20, 2005. The cause was later determined to be blunt-force trauma. Four inmates were later charged in his death, with three being convicted. Winnipeg Free Press, B3 (2016-04-15); CTV News (2016-04-14)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** N.S. plans new legislation to replace cyberbullying law**
Nova Scotia will draft new legislation to replace its pioneering cyberbullying law inspired by the death of teenager Rehtaeh Parsons. Supreme Court of Nova Scotia Judge Glen McDougall struck down the original CyberSafety Act in December, saying it violated the Charter of Rights and Freedoms. Justice

Minister and Attorney General Diana Whalen said Thursday that the province accepts the act was too broad, and will not appeal the decision. Whalen said "targeted consultations" will take place over the next several months to ensure the new law protects the public and addresses the concerns raised in the court decision. The original law was passed in May 2013 in response to public outrage over Parsons' death less than a month earlier. Canadian Press (Chronicle-Herald, A3)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Nil

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Pharmacists, pot producers in smouldering dispensing dispute**
Canada's pharmacists and medical marijuana producers are engaged in a brewing dispute over how pot should be distributed to patients. If they can't reach an agreement, it could leave Ottawa with a tough decision as it crafts new regulations for the sector. The pharmacists believe they are the only ones who can provide proper clinical advice and oversight over the growing use of medical pot, and think they should control distribution. The marijuana producers, on the other hand, believe the current mail-order system is a resounding success, though they are open to involvement from pharmacies. "By any metric, the medical cannabis system in Canada is working exceedingly well," said Cam Battley, chair of the advocacy committee at the Canadian Medical Cannabis Industry Association (CMCIA). (…) Phil Emberley, the CPhA's director of professional affairs, said pharmacists still think more evidence is needed around marijuana's use as medicine. But as Canadians use the product in increasingly large numbers, he said pharmacists are needed to ensure patient safety. "We know that there are side effects with marijuana, and potential drug interactions as well," he said. "We feel that a lot of patients are accessing medical marijuana without being protected from some of those concerns." The pot companies want to increase patient access to marijuana, so they are broadly supportive of pharmacies playing a role in distribution. They recognize that some patients will always prefer to get their medicine from a pharmacist. But they oppose the outright takeover of their direct-mail distribution system by pharmacies. Postmedia Network (Windsor Star, B8, Edmonton Journal, Ottawa Citizen)

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Aboriginal protesters occupy federal offices across Canada, demanding Trudeau visit Attawapiskat**
Several groups of indigenous activists have occupied the offices of Indigenous and Northern Affairs Canada in Toronto and staged a sit-in in Winnipeg, demanding that Justin Trudeau visits a northern Ontario community struggling with a recent spate of suicide attempts. A group of about 30 people first occupied the Toronto building around 10 a.m. on Wednesday morning, police said. More than 30 hours into the protest, it continues to be peaceful, police said. A second group of activists staged a sit-in in the Winnipeg INAC office Thursday evening. Maanii Oakes, a protester in the group occupying the office said the group is disappointed to not have received a response from the federal government. Protesters staged a "die-in" in the INAC

office and hung up Attawapiskat First Nation and Mohawk Warrior Society banners on Wednesday. National Post

OTHER / AUTRE

*** The government's Saudi hypocrisy**
An editorial piece states, "The Liberal government had until recently tried to have it both ways on the deal to sell LAV armoured fighting vehicles to Saudi Arabia. On the one hand, it displayed its moral qualms about the sale, negotiated by the previous Harper government. On the other hand, it claimed that it had to honour the agreement because, well, a done deal is a done deal. Remember when John Turner insisted, "I had no option"? He did. And as documents released this week show, so did the Trudeau government. The contract was signed in 2014, back when a Liberal government was a distant prospect. But it was revealed this week, final approval of the deal from Foreign Affairs Minister Stéphane Dion only took place a few days ago, on April 8. That ministerial approval, including a review of the potential for human rights violations by Saudi Arabia, was necessary to give the contract effect and allow the sale of billions of dollars' worth of armoured fighting vehicles to go forward." Globe and Mail, A10; iPolitics

INTERNATIONAL

EU passes airline info sharing law
European Union lawmakers approved Thursday a scheme to share airline passenger information that nations hope to use to track foreign fighters travelling to and from conflict areas like Syria and who might pose a danger in Europe. The move ends years of wrangling over how to balance security needs and privacy rights. Lawmakers came under great pressure to adopt the scheme in the wake of the Nov. 13 attacks in Paris that killed 130 and last month's suicide bombings in Brussels, which left 32 dead. The so-called Passenger Name Record law was approved at the European Parliament in Strasbourg, France, by 461 votes to 179, with nine abstentions. "PNR will be a precious tool for boosting the security of European citizens by helping to detect early the movement of jihadi terrorists that take air transport throughout Europe, but also between Europe and other regions of the world, to prevent them taking action," Interior Minister Bernard Cazeneuve said. Critics say that many of those linked to the attacks were already known to the authorities, and that the scheme will needlessly collect private information about ordinary citizens, as well as be costly and cumbersome to operate. Chronicle-Herald, B4; Le Devoir

Illegal gold now more lucrative than cocaine in Peru, Colombia
In Peru and Colombia, the world's biggest producers of cocaine, illegally mined gold is now a more valuable export than the drug, according to a new study. Organized criminal groups have moved into this sector, leaving workers vulnerable to labour exploitation, human trafficking and sexual offences, the study says. (…) Once gold is laundered, it becomes indistinguishable from legal gold and can be easily moved across borders. The study estimates that 28 per cent of gold mined in Peru is illegal, earning criminals $3.3 billion a year. In Colombia, it estimates 80 per cent of gold production is illegal, worth between $1.9 billion and $2.6 billion a year. That makes illegal mining more lucrative than cocaine production: Organized crime groups in Peru produce about 295 tonnes of the drug a year, earning about $1.9 billion, and Colombia's drug cartels earn a similar amount in wholesale proceeds from both heroin and cocaine, according to the United Nations World Drug Report. The Revolutionary Armed Forces of Colombia, commonly known as FARC, receives as much as one-fifth of its funding from illegal mining, the gold study says. The guerrilla group is currently negotiating a peace deal with the Colombian government. Toronto Star, A1

Neuf morts et des centaines de blessés

Un puissant séisme de magnitude 6,5 a fait neuf morts et plus de 800 blessés, jeudi, au Japon, en plus de détruire plusieurs maisons dans le sud du pays. Parmi les blessés, 53 sont dans un état grave. Les neuf victimes étaient âgées de 29 à 94 ans, mais la plupart étaient des personnes âgées. La secousse a frappé à 21 h 46, heure locale, à une profondeur de 11 kilomètres près de la ville de Kumamoto, sur l'île de Kyushu, selon l'Agence météorologique du Japon. Le porte-parole du chef du gouvernement, Yoshihide Suga, a dit que le premier ministre visiterait la région vendredi pour évaluer les dommages. Quelque 1600 soldats ont été dépêchés sur les lieux, selon le porte-parole. Des images présentées à la télévision montrent les militaires, remettant des couvertures aux milliers de personnes qui ont dû évacuer leurs résidences. Quelque 44 000 personnes ont été hébergées dans des refuges, mais certaines d'entre elles ont pu réintégrer leur domicile en matinée. Au moins 19 maisons se sont effondrées, et les autorités ont reçu des milliers d'appels témoignant de résidences écroulées et de victimes prisonnières des décombres. Associated Press (Le Droit, 19)

*** Five arrested in UK after inquiry linked to Brussels and Paris terror attacks**

Four men and a woman were held in Birmingham and at Gatwick airport following joint investigation with authorities in Belgium and France. Counter-terror police in the West Midlands have arrested five people on suspicion of preparing terrorist acts following an investigation that involved Belgian and French authorities. West Midlands police said it had been working with Belgian and French authorities to "address any associated threat to the UK following the attacks in Europe". Four people – three men aged 26, 40 and 59 and a 29-year-old woman – were arrested in Birmingham on Thursday night and a 26-year-old man was arrested at Gatwick airport in the early hours of Friday. Assistant chief constable Marcus Beale, who leads on counter terrorism for the West Midlands, said: "This action forms part of an extensive investigation by West Midlands counter terrorism unit, together with the wider counter terrorism network, MI5 and international partners including Belgian and French authorities to address any associated threat to the UK following the attacks in Europe." The arrests were pre-planned and intelligence-led, Beale added, and there was no risk to the public at any time and there is no information to suggest an attack in the UK was being planned. The Guardian

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
April 16, 2016 / le 16 avril 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

BlackBerry and Apple divided over encryption
BlackBerry Ltd. prides itself both on its reputation for security and close relationships with many of the world's most powerful governments. In an era where consumers are increasingly aware of surveillance from law enforcement and spy agencies, those two points of pride may start coming into conflict. A report by Vice News on Thursday, citing court documents, details how the Royal Canadian Mounted Police obtained a key to unlock messages sent between BlackBerry phones as early as 2010. The situation stands in stark contrast to the clash that erupted between Apple Inc. and the U.S. government earlier this year when the U.S. tech firm refused to redesign its software to let the FBI bypass encryption on an iPhone used by a shooter in the San Bernardino attacks. BlackBerry chief executive John Chen stepped into the encryption debate in December. "We are indeed in a dark place when companies put their reputations above the greater good," Chen said in a blog post. A spokeswoman for BlackBerry declined to comment on the Vice story. Harold Pfleiderer, a spokesman for the RCMP, declined to comment on the specifics of the case, saying the force's investigations are governed by Canadian law and court orders. **Canada's Minister of Public Safety Ralph Goodale**, which oversees the RCMP, declined to comment on the specifics of the case but said he welcomes a public debate on encryption. ***"Canadians need to reflect on this new and emerging area of law, privacy and crime prevention,"* Goodale** said in an emailed statement. Bloomberg (Vancouver Sun, C3; Waterloo Region Record, Hamilton Spectator, Windsor Star, Ottawa Citizen, Calgary Herald)

Pas de promesse sur la vente d'armes
Le Journal s'est entretenu avec le ministre Dion quelques jours avant que celui-ci ne donne son feu vert, cette semaine, à la vente de 900 véhicules blindés à l'Arabie saoudite. Le ministre des Affaires étrangères Stéphane Dion ne peut promettre que le Canada ne vendra plus d'armement à des régimes totalitaires comme l'Arabie saoudite. Mais le gouvernement fera preuve de plus de rigueur à l'avenir, s'engage-t-il (…) Il faut regarder les intérêts du Canada et de ses alliés. Si on est en guerre avec un pays, on ne lui vendra pas quoi que ce soit. Si on est en guerre avec un pays, on ne lui vendra pas quoi que ce soit. La raison pour laquelle on ne peut employer le terme de guerre est que, sur le plan politique, l'État islamique veut prétendre qu'il est un État. Et le mot guerre veut dire un conflit armé entre deux États (…) C'est pourquoi nous avons établi un nouveau plan que nous jugeons beaucoup plus efficace afin de non seulement combattre Daesh, mais aussi empêcher qu'un autre groupe terroriste renaisse de ses cendres (…) Le Canada n'est pas immunisé. Ça nous est déjà arrivé d'ailleurs. **Le ministre de la Sécurité publique** travaille de très près avec toutes nos forces policières. Moi-même, j'ai des responsabilités à ce sujet avec nos groupes de recherche d'informations. On essaie de protéger le mieux possible la population. Il n'y a pas d'objectif plus important pour le gouvernement. Le Journal de Montréal, 53 (Journal de Québec)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Sparse snowfall reduces spring flooding risks
Just as Yukon temperature records fell left and right over the past winter, it's been another below-average season for snowfall across much of the territory. In the Whitehorse area, for instance, the snowpack conditions were 42 per cent below normal as of April 1, according to the snow survey bulletin and water supply forecast published this week. Given normal spring and summer conditions from here on, the bulletin is forecasting the spring runoff in the Whitehorse area will be down 20 per cent. Meanwhile, the flow of the Yukon River coming out of Marsh Lake will be down 25 per cent. The water content of the snowpack in the Pelly River basin has diminished 21 per cent, 20 per cent in the Liard River basin, 18 per cent in the Stewart River basin and 22 per cent in the Southern Lakes. "The potential for flooding in these basins is quite reduced," hydrologist Ric Janowicz of Environment Yukon pointed out in an interview this week. Whitehorse Daily Star, 10

*** Fuel spill reported in English Bay near Vancouver's False Creek**

The Canadian Coast Guard says a small amount of diesel fuel was spilled into English Bay near False Creek Friday but has caused no environmental damage. Investigators were not able to trace where the diesel originated from, but was it was first observed near the boat launch docks in front of the Kitsilano Coast Guard station, according to Coast Guard information officer Michelle Imbeau. "The pictures are dramatic but the spill is not serious," she said. "The spill was determined to be diesel and was deemed to be not recoverable. It will evaporate." The company that cleans up oil spills on Canada's west coast says it has not been activated and doesn't expect it will be called in. Vancouver Sun; Canadian Press (News 1130, CFJC Kamloops); Global News; CTV News; Georgia Straight;

* **Fuel spill caused by overturned truck blocks Highway 2 near Meacham, Sask.**
A fuel spill caused by an overturned diesel fuel truck is causing delays on Highway 2, about three kilometres south of the village of Meacham, Sask. Part of the highway had to be blocked off while Sask Environment coordinated the spill clean up Friday afternoon. CBC News

* **B.C., Alberta, differ on school utilization rate**
The B.C. Education Ministry is forcing the province's school districts to have their schools 95-percent full before they can get funding for seismic upgrades. But next door in Alberta, the Calgary district is working on a plan to reduce its capacity, from the current level of 85 per cent, down to 80 per cent (...) In Vancouver, the board is looking at closing as many as 21 schools to get to a 95-per-cent utilization rate, as mandated by the ministry of education, and required before schools will be upgraded for earthquake safety. Vancouver Sun, A5

How to avoid the 'silent killer'
For many young families, it's a familiar sound that requires attention but seldom spells life-threatening danger: a toddler crying in the night. But for Kamloops, B.C., resident Monique Ruppel, having heard it at 3 a.m. for the second time one night in January, it was a different story when she went to see what was troubling her daughter, Celia. Her husband, Kyle, also woke immediately and they both realized they were dizzy, and felt headaches, nausea and burning eyes. When they reached the crib, Celia began vomiting. The family was in the throes of carbon monoxide (CO) poisoning, but because they didn't have a CO alarm, they hadn't been alerted to the danger. Protection from CO poisoning should not hinge on the cries of a child or luck, say safety experts. And steps have been taken in recent years to make safeguards - the proper installation of CO alarms in residences - the law of the land (...) In the one year since all Ontario homeowners have had to be in compliance with the law, director/deputy, prevention and risk management of the Ontario Office of the Fire Marshal and Emergency Management, Al Suleman, has seen positive changes. "Ever since we've introduced the regulation and compliance has kicked in, almost on a weekly basis, we're seeing families holding their CO alarms and saying, 'It saved our lives,' " says Suleman. Toronto Star, L11

* **Frozen berry mix sold at Costco recalled over possible hepatitis A contamination**
The Canadian Food Inspection Agency has issued a recall for a frozen berry mix sold exclusively at Costco due to possible hepatitis A contamination. The federal agency is recalling 1.5kg bags of Nature's Touch Organic Cherry Berry Blend with best-before dates up to and including March 15, 2018. The bags are sold at Costco warehouse locations in Ontario, as well as Quebec, New Brunswick, Nova Scotia and Newfoundland and Labrador. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

* **«Des attaques il y en aura toujours, mais on est mieux préparé»**
Les 325 spécialistes de la Sûreté du Québec, de la GRC et provenant de différents milieux sont rassemblés au Collège militaire royal, lui même théâtre d'un drame lié au terrorisme il y a un peu plus d'un an. Des gens venus en apprendre un peu plus sur les menaces qui pèsent ou encore pour poser des questions sur les solutions à adopter. Dire les vraies choses, les appeler par leur nom: c'est ce que prône Fatima Houda-Pepin, elle-même musulmane. «C'est en arrivant au Canada, moi, il y a 40 ans, que j'ai découvert l'islamisme radical. Je n'ai pas amené ça avec moi. C'est ici que j'ai découvert les cercles d'endoctrinement. C'est ici que j'ai découvert les discours haineux, les plus virulents, à l'égard des

mécréants, les juifs, les chrétiens, même les musulmans. C'est ici que j'ai découvert que le Canada, c'est le paradis des islamistes, finalement.» Ils ont notamment discuté de la délicate question de la sécurité dans les aéroports. Cette discussion tombe à point, moins d'un mois après les attentats de Bruxelles qui ont coûté la vie à 32 personnes (...) Le spécialiste croit effectivement que c'est en se préparant qu'on réussit à diminuer les risques. «De plus en plus aussi, l'Organisation de l'aviation civile internationale tente d'être un pas ou deux en avant des gens. Des attaques terroristes il y en aura toujours, le risque zéro n'existe pas, mais on est beaucoup mieux préparé», ajoute M. Duchesneau.
Selon le SCRS, une soixantaine de Canadiens qui ont joint des organisations terroristes à l'étranger sont revenus chez nous. «C'est sûr, avec ce qui se passe en Europe, c'est désolant de voir qu'il y a des pertes de vies humaines. Mais, au Québec et au Canada, on demeure encore une place ou un pays qui est très sécuritaire par rapport à d'autres pays», explique le sergent Hakim Bellal de la GRC. TVA Nouvelles (2016-04-15)

Radicalisation - Les programmes de prévention sont-ils efficaces?
Très peu d'études ont mesuré l'efficacité réelle des programmes de prévention de la radicalisation auprès des jeunes. Certains programmes pourraient avoir l'effet contraire à celui recherché, en relayant le discours délétère du groupe État islamique (EI), pensent certains experts. Des chercheurs ont réfléchi à cet enjeu lors d'un colloque tenu cette semaine à l'Université Concordia. Réflexions sur une question complexe. Une mère pleure la mort de son fils de 22 ans, un jeune épris de justice parti combattre aux côtés des chevaliers de l'Islam. En arrière-plan, le drapeau noir du groupe État islamique flotte au ralenti, tandis que l'écran recrache les images de jeunes djihadistes fiers et victorieux, brandissant leurs armes devant les bombes qui réduisent la Syrie en ruines. Tiré d'Extreme Dialogue, une vidéo visant à contrer la radicalisation diffusée dans les écoles albertaines et financée par le gouvernement fédéral, ce bombardement d'images par moments similaires aux films d'action concoctés à Hollywood laisse plusieurs spécialistes de la prévention de la radicalisation perplexes. Ces images racontent la triste histoire d'une mère albertaine, Christianne Boudreau, et de son fils, Damian Clairmont, tué en Syrie lors de combats en 2013. Converti à l'islam à l'insu de sa mère, le jeune décrocheur dépressif a fui le Canada en 2012 pour se joindre au groupe EI, en dépit de la surveillance dont il faisait l'objet par le Service canadien du renseignement et de la Sécurité (SCRS). " Ce programme part d'une bonne intention, mais le message est erroné. Si on veut éviter la radicalisation ou déradicaliser, ne parlons pas de ça, ne leur donnons pas le mode d'emploi. Par moments, cela ressemble à un cours de base sur le groupe EI et sur comment se rendre en Syrie ", soutient Khaled Nour, de Queens University, qui a étudié les réactions de plusieurs adolescents exposés à cette vidéo. Le Devoir, B1

Perspectives - Anti-extrémisme extreme
Les parents d'enfants qui fréquentent une garderie au Royaume-Uni ont reçu récemment une lettre hors de l'ordinaire : les éducatrices doivent désormais enseigner les " valeurs britanniques " et surveiller les signes de radicalisation des petits d'âge préscolaire. Il n'est jamais trop tôt pour prévenir l'extrémisme, semble-t-il. Le mois dernier, un service de garde de la ville anglaise de Luton -- où vit une importante minorité de 50 000 musulmans --, a pris au sérieux la directive du gouvernement : l'établissement a menacé de signaler aux autorités un " suspect " âgé de quatre ans qui avait dessiné son père en train de couper un concombre. Les éducatrices avaient compris que le garçon dessinait non pas un concombre, mais un engin explosif artisanal appelé " cooker bomb ". Scandalisée de passer pour une terroriste, la mère du garçon a diffusé une vidéo où elle montre un concombre à son enfant. Qu'est-ce que c'est ? demande-t-elle. " A cuker-bum ", répond-il comme un bambin de quatre ans. Un autre garçon, de 10 ans celui-là, a eu le malheur d'évoquer en classe des mots qui ressemblaient à " maison terroriste ". Son père a été interrogé par la police (...) Le professeur britannique avait un message pour les gouvernements, comme ceux du Québec et du Canada, qui cherchent des moyens de combattre la radicalisation : il existe un danger d'aller trop loin. De chercher des signes d'extrémisme partout (...) Le gouvernement britannique se défend d'aller trop loin. Après tout, les écoles ont vraisemblablement servi de base à la radicalisation de jeunes dans l'histoire récente. Au moins trois attentats d'al-Qaïda au Royaume-Uni (en 2003, 2005 et 2006) ont impliqué des jeunes, dont un de 15 ans, qui sont devenus extrémistes quand ils fréquentaient l'école. Le Devoir, B1

Alberta's new Islamophobia hotline receives dozens of calls
An Alberta-wide hotline to help people report incidents of vandalism or discrimination related to

Islamophobia has received 53 calls since it was launched about three weeks ago. The organization behind the hotline says it is difficult to gauge whether that represents a high number of calls. "We'll consider it successful when we don't get any calls," said Mustafa Farooq, vice-president of public policy at the Alberta Muslim Public Affairs Council (…) AMPAC is investigating "roughly 30" of the calls received, Farooq said. Five callers have been encouraged to file reports with police in either Calgary or Edmonton, or with the RCMP, he said. CBC News

B'ys and spies
If you see small groups of members of the United States Navy walking back-to-back down George Street in a circular formation, it's apparently for their own safety. In fact, if you take the U.S. Navy's advice, you'll never walk down George Street alone, and if you do visit the area, you'll be wary of drugs, prostitution and motorcycle gangs. That information was actually sold to the Russians by a Canadian spy. It's well past April Fool's Day, so you can stop looking for the punchline. The story is both bizarre and true. CBC Nova Scotia reported Friday that some of the information a Canadian spy was selling to Russians was about a warning the U.S. Navy gave to any of its crews who were in port in St. John's. St. John's Telegram, A1

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Ottawa hits back over Oberlander
Stung by a legal defeat, the federal government wants the Supreme Court to rule that politicians acted within the law in revoking the citizenship of Helmut Oberlander, 92, for serving in a Nazi death squad. In Waterloo on Friday, Prime Minister Justin Trudeau said his Liberal government is committed to prosecuting immigrants such as Oberlander who lie about their past to become citizens. "There is one condition in which citizenship can be revoked, and that is when it was acquired based on fraud, misinformation and not representing clearly who one was," Trudeau said (…) The government said it wants the Supreme Court's "direction and guidance" on issues around the depth of Oberlander's involvement in the death squad, his level of complicity in its murders, and the threats that the Nazis might have made against him to make him comply. This is after the Federal Court of Appeal ruled in February that the federal cabinet, in revoking his citizenship in 2012, failed to properly consider "the extent to which (Oberlander) made a significant and knowing contribution" to the death squad. That ruling restored Oberlander's citizenship (…) Jewish groups who are clamouring for Oberlander's deportation applaud the government for not abandoning the Oberlander prosecution despite a string of legal defeats (…) Oberlander supporter Ernst Friedel said that by not abandoning its prosecution, the government is unjustly targeting a man who committed no war crime, and is wasting public money pursuing a case it has lost three times and can't win. "It's laughable," said Friedel, a director with the German-Canadian Congress, which opposes the government's bid to deport Oberlander. Waterloo Region Record, A1

Mugesera condamné à la prison à vie
Le Rwandais Léon Mugesera, qui a lutté pendant 16 ans pour éviter sa déportation du Canada, a été condamné à la prison à vie au Rwanda pour avoir incité ses compatriotes à commettre un génocide. L'homme de 63 ans aurait déjà porté la décision en appel, ont rapporté plusieurs médias, vendredi. L'ancien résidant de la ville de Québec était accusé d'avoir livré un discours enflammé devant un millier de personnes au Rwanda en 1992 dans lequel il traitait les Tutsis de coquerelles, suggérant qu'ils devaient être exterminés. La Presse Canadienne (Le Droit, 31; La Voix De L'Est, Le Soleil, L'Acadie Nouvelle, Le Devoir, *Le Nouvelliste); La Presse; Canadian Press (Montreal Gazette)

CYBER SECURITY / CYBERSÉCURITÉ

Microsoft suit latest tech clash with government over privacy
Microsoft opened a new front in the battle over digital privacy this week, suing the Justice Department over its use of court orders requiring the company to turn over customer files stored in its computer centres - often without notifying the customer involved. It's the latest in a series of legal challenges brought by Microsoft and some of its leading competitors. Apple recently fought a high-profile battle over

the FBI's demand for help unlocking an encrypted iPhone in San Bernardino, Calif., and it's continuing to challenge similar demands in other cases. Other companies, including Google, Facebook and Yahoo, have increased their use of encryption. They've also sued for the right to report how often authorities demand customer information under national security laws, after former National Security Agency contractor Edward Snowden leaked details of government data-gathering efforts. Associated Press (Toronto Star, B5)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Province adding $23 million to tackle gun and gang violence

The B.C. government will spend $23 million more for police, prosecutors and programs to combat the province's gangs and gun problem. Premier Christy Clark announced the new funding in Surrey Friday, where there have been 32 shootings so far this year, primarily over drug-trade turf wars. But she stressed that B.C.'s gang problem is not isolated to one community because gangsters are like "cockroaches" who move frequently to ply their illegal trade. "The frequency and public nature of recent gang shootings is unacceptable and demands this additional, strategic deployment of resources. People deserve to feel safe no matter where they live in B.C.," Clark said. "This needs to be a provincewide initiative (…)" RCMP Deputy Commissioner Craig Callens, the top RCMP officer in B.C., welcomed the news. "We appreciate the additional funding and support being provided to the RCMP, CFSEU-BC and our law enforcement partners, who are all working together to target, investigate, prosecute and disrupt those individuals and groups that pose the highest risk to public safety in our province," Callens said. "As part of B.C.'s guns and gangs strategy, we will be heightening our enforcement activities, increasing the level of information and intelligence-sharing and enhancing our prevention and community engagement programs." B.C. will look at whether laws need to be changed to better deal with gangsters and gun crimes, Clark said. "Gangs evolve. Criminals come up with new ways to commit crimes," she said. Vancouver Sun, A13; Canadian Press (Guardian, Times Colonist, Cape Breton Post)

Drugs And Guns In Surrey

It was just after 9 p.m. on March 11 when Ishaan (Lucky) Dhanoa's white sedan struck a tree near 79th Avenue and 123 Street in Surrey. Passersby ran to his aid, but the 21-year-old died in hospital a short time later. At first, police just called his death "suspicious." Later, the Integrated Homicide Investigation Team was called in and police confirmed he'd been shot - the only fatality so far this year from Surrey's frequent gun violence. Few details have emerged about the unsolved slaying. Dhanoa had not amassed any criminal charges or convictions in his short life. But sources say he was involved in the low-level drug trade, like others linked to the public gunplay that has plagued Surrey. Dhanoa's grandmother Amarjit Shant spoke briefly to The Vancouver Sun this week. She said the family is struggling with the tragedy, but has no idea why it happened (…) Surrey RCMP say most of those involved in the gun violence are typically young and working on the front line of the local drug trade, meaning they take calls from customers, package drugs for street sales and make deliveries for the city's numerous dial-a-dope lines. The violence comes from their battles over turf, personal disputes and the fact they have ready access to firearms even at the lowest rung of the drug business. Several of the 2016 shootings have been linked to two warring groups. The Sun has looked into the background of several of those charged this year, searching for common threads in their life stories. Vancouver Sun, A12

La GRC obtient la clé de cryptage des BlackBerry

La Gendarmerie royale du Canada (GRC) a obtenu la clé unique de cryptage des téléphones BlackBerry des particuliers, demandée pour les besoins d'une enquête et permettant un accès aux conversations privées, selon des médias. «C'est une question qui à l'évidence préoccupe beaucoup de personnes», a déclaré vendredi le premier ministre Justin Trudeau en déplacement à Waterloo, là où est basé le siège social de BlackBerry. La révélation a été faite dans des documents judiciaires obtenus par les sites d'information Vice News et Motherboard, où il est question de la surveillance entre 2010 et 2012 d'une organisation mafieuse de Montréal soupçonnée du meurtre d'un homme. La GRC a intercepté et décrypté près d'un million de messages BlackBerry dans le cadre de son enquête, a indiqué Vice News. Agence France-Presse (Le Soleil, 52; Gadgets 360, NDTV)

Police tried to stop truck before it hit Mountie's cruiser in fatal crash
Police tried to stop a pickup truck minutes before it struck West Shore RCMP Const. Sarah Beckett's police cruiser, killing her, the RCMP said Friday. The crash is now being investigated by the Independent Investigation Office of British Columbia. "On Friday, IIO confirmed they will be conducting an independent investigation into the events leading up to the fatal collision and whether the actions or inactions of any police officer may have been a contributing factor," said Staff Sgt. Rob Vermeulen. Beckett, a 32-year-old mother of two, died April 5 when her police car was struck in the intersection of Peatt Road and Goldstream Avenue in Langford. The driver of the pickup truck that hit the cruiser was taken into custody and released the next day without being charged. A criminal investigation into the crash is being led by the RCMP Island District General Investigations Section. The Saanich Police Department is overseeing the collision-scene investigation. Times Colonist, A1/FRONT; Canadian Press (Vancouver Sun, Waterloo Region Record, *StarPhoenix); *Global News

RCMP won't share details on Tisdale murder-suicide
As the one-year anniversary of the shocking deaths of a mother and her three young children in Tisdale approaches, RCMP say they will soon be done their investigation - but will not share any information with the public. "Investigations such as this take an emotional toll and has a lasting impact on investigators," StaffSgt. Murray Chamberlin of the RCMP's major crimes unit said in a statement issued to media on Friday. "We see and hear things throughout the course of investigation and are not immune to the effects a tragedy such as this has on families and communities as a whole. We thank the Tisdale community who reached out to RCMP members to offer support; your gestures are appreciated." StarPhoenix, A2; Canadian Press (Leader-Post, Guardian, National Post, Red Deer Advocate, *Waterloo Region Record, *Hamilton Spectator)

RCMP use Taser on disabled veteran with electronic surgical implant
A disabled veteran from Lunenburg County says an encounter with RCMP in February left him so traumatized he's scared to open his front door. "I'm staring out the windows now. If the wind blows, I jump," says Bruce Webb, who lives with his fiancée Lori Fuller above the Purple Leprechaun Roadhouse, a restaurant she owns in Bayport, N.S. Webb, 53, faces charges of assaulting a police officer and resisting arrest, but believes he was the victim in a late night encounter with police on Feb. 28. Webb says when the Purple Leprechaun Roadhouse is closed, he uses the space as a living room. He says he'd fallen asleep watching TV in an assisted-lift chair when RCMP arrived. Video from security cameras inside the restaurant show RCMP officers banging on doors and shining lights through the windows. It was the second time that night police had been at the location (…) Security video shows Webb refusing to let police in while blues music blares in the empty restaurant. Webb tells the officer he's calling 911. The officer then forces his way in by breaking down the door. There's an immediate physical confrontation. CBC News; *Windsor Star

*** RCMP investigating shooting in North Preston**
RCMP are investigating a shooting that happened early this morning in the community of North Preston. Police say they were called to Cain Street after shots rang out around 5 a.m. It appears a home and a vehicle were struck by bullets. Police confirm there were no injuries as a result of the shooting. Global News; CBC News

RCMP looking for Alberta woman wanted for murder
RCMP are asking the public for help finding 28-year-old Florencine Leandra Potts, who is wanted for second-degree murder. After being released from custody by a judge, Potts failed to appear in Wetaskiwin Provincial Court and an arrest warrant was issued. RCMP said they recently received information that she is on the Samson First Nation and is believed to be “avoiding apprehension.” Global News

*** Remains identified as missing local man**
RCMP have identified human remains found last week near Innisfail as those of a missing 42-yearold Edmonton man. On April 5, RCMP officers were called to a wooded area at around 7 p.m. after someone discovered human bones. On Friday, the Calgary Medical Examiner's Office identified the remains as Dwayne Demkiw, 42, who disappeared May 31, 2015. He was last seen leaving his workplace in the

area of 149 Street and 128 Avenue at around 4 a.m. Family members said he worked at Saint Pete's as a DJ. Several hours later, the 42-year-old's black four-door 2002 Acura 3.2 TL was found on fire near 86 Avenue and Bonaventure Drive in Calgary. Edmonton Journal, A11 (Edmonton Sun)

*** Woman's death still puzzles**
One year after the discovery of the body of Paula Stiles in her Sherwood Park home, RCMP are still searching for her killer. Stiles, 44 , had three daughters and worked as a training supervisor at Enbridge Pipelines. She was found dead April 15, 2015, inside her house at 40 Foxhaven Court. No arrests have been made in the case. RCMP have not released the cause of her death. At a press conference Friday, Strathcona County RCMP Supt. Gary Peck said police hope someone will come forward to aid the investigation. Postmedia Network (Edmonton Sun, A4; Edmonton Journal)

*** Missing teen sought**
Codiac Regional RCMP are asking for the public's help in locating a 17-year-old girl from Moncton. Police say Felicity Mae Strutt was reported missing after she left her home in Moncton on April 9. She was last seen in the Moncton area that evening. Police have been making efforts to locate her, but so far have been unable to do so. It is believed she may be with acquaintances in the Moncton area and police want to confirm her well-being. Times & Transcript, A10

*** Edmonton man arrested in Yellowknife drug bust**
An Edmonton man was one of eight people arrested after Yellowknife RCMP searched five properties and seized drugs, guns, cars and cash. Around 30 officers from across the Northwest Territories executed search warrants at five locations within Yellowknife Thursday evening. Officers seized fentanyl pills, crack cocaine, cocaine, psychedelic mushrooms, marijuana, anabolic steroids and a large quantity of cash that investigators believe may be the proceeds of illegal drug sales. Postmedia Network (Edmonton Sun, A8; Edmonton Journal)

Police boat untied in North Van
Police are looking for two men suspected of untying an RCMP boat in North Vancouver, causing it to drift into the path of other vessels. North Vancouver RCMP were called early Friday morning when the Canadian Coast Guard reported that the patrol vessel Inkster was adrift and had floated into the path of the SeaBus, a commuter ferry that travels Burrard Inlet. Police and the coast guard got the 20-metre vessel back undamaged, but North Vancouver RCMP Cpl. GeoffHarder said in a release that the mischief could have been extremely dangerous. Vancouver Sun, A18; Canadian Press (Vancouver Province, *Times Colonist)

RCMP say cyber criminals are getting better
The RCMP has received several complaints regarding businesses having their emails spoofed. Cyber criminals are creating new email addresses that are very similar to legitimate business emails and sending requests for money transfers that appear to be from persons of authority in the company. The differences in the email addresses are very subtle with only a letter or a period changed. Some of these attempts appear to be as simple as criminals finding a target's email addresses online and others appear to be as a result of compromised email accounts. Unlike the usual spam messages, with spoofing the cyber criminals will take the time to study a targeted business. This allows the fraudster to identify vulnerabilities and to add details to their email messages making them appear legitimate. Guardian, A4

Let first responders know they're appreciated
An comment piece states “Following the death of Const. Sarah Beckett, we as a community were given the opportunity to experience a full regimental funeral to honour her sacrifice in the line of duty. Life can change in an instant. First responders (police officers, firefighters, ambulance crews and military personnel) put their lives on the line for us, every shift, every day. The outpouring of support for Beckett's family, the RCMP and police in general was unprecedented. What will it take for all of us to appreciate the services they provide to us before one of them dies in the line of duty?” Times Colonist, A13

Métro video filming suspects arrested
The video was posted publicly online on March 26 by an account that was created that same day and

hasn't shown any activity since. Titled "Lowest Point in Montreal," it showed three men running around Montreal's métro system, and has since garnered more than 150,00 views. On Thursday, Montreal police arrested three men in connection with the video, ages 22, 28 and 53. They were released after promising to appear in court in early May, and are expected to face charges of breaking and entering, public mischief and possibly possessing tools for breaking and entering, Montreal police said. If convicted, police said they could face up to 10 years in prison. Montreal Gazette, A7

Fingerprint system gets thumbs up

The phrase "book 'em" has gotten a whole lot easier for the Fredericton Police Force.
Since the introduction earlier this year of a electronic fingerprint scanner, members of the department can now move with a newfound efficiency. Gone are days when a suspect's finger had to be dabbed in ink and then stamped on a paper. Sgt. David Cooper, who heads up the department's forensic identification section, said there's no doubt the new system is a time saver. Telegraph-Journal, A4

* **Why can't report be made public?**

The names of the victims and the officers involved. Testimony from civilian and police witnesses. Photo and video evidence. The director's report produced at the conclusion of a probe by the Special Investigations Unit (SIU) contains the key evidence relied upon by the top civilian police watchdog when making the serious decision whether to criminally charge a police officer or clear them of wrongdoing. Importantly, it may also include the weight given to each piece of evidence, valuable information in cases where witness accounts may vary or information conflicts. But the report prepared by the director of the SIU, the agency that probes deaths, serious injuries and allegations of sexual assault involving police in Ontario, goes straight to the desk of the attorney general - and nowhere else. Toronto Star, GT1

* **What the SIU usually keeps behind doors**

The subject officer is the focus of the investigation. In the case of a fatal shooting, the officer who pulled the trigger (there is sometimes more than one subject officer). The SIU does not release the identity of this officer unless the officer is criminally charged, citing a policy based on the Freedom of Information and Protection of Privacy Act (FIPPA) protecting the personal information of every individual involved in an SIU investigation. The argument for why you should know: Secrecy means the public cannot know if the officer in question has a history of misconduct or prior involvement in another incident where a civilian was injured or killed. It also limits the ability of the public to come forward with information about the officer that could be relevant to the investigation. Toronto Star, GT2

* **Lock-ups found scrimping on meal plans to cut costs**

Jenny Reid never worried much about her clients' dietary wellbeing before she started practising law in Woodstock, Ont. Over a 27-year career in seven jurisdictions across the country, Ms. Reid had seen some gloomy variations of the generic bologna sandwich and apple served to most inmates in police custody, but nothing that ever caused alarm. That changed when she began working in the 40,000-person seat of Oxford County last year. At one case meeting, she met a group of accused Toronto men who seemed more concerned with their own hunger than the serious counterfeiting charges filed against them, so she asked what they had eaten in police lock-up. "And they told [me] they weren't given a meal, just a granola bar and apple juice," she said. "I'd never heard of that before. ... When I raised it at a local bench and bar meeting, they tried to say it was an anomaly." Over a number of subsequent cases, Ms. Reid learned that passing off granola bars as balanced meals was anything but an aberration - it was part of a detainee meal plan endorsed by the local public-health department (...) Police in Vancouver, Halifax, Saint John and elsewhere have turned to prepackaged snacks to feed inmates despite domestic law and international agreements stating that prisoners must be fed three square meals a day (...) Unlike provincial and federal jails, police lock-ups generally keep inmates for less than 72 hours. For example, the average stay of an inmate at Woodstock Police Station is 7.34 hours, according to a 2015 audit. The shorter terms do not reduce the state's legal obligations, however. The United Nations Standard Minimum Rules for the Treatment of Prisoners states that every prisoner should be fed food "of nutritional value for health and strength, of wholesome quality and well prepared and served." Globe and Mail, A9

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Killer wants earlier shot at parole**
The heartless killer whose hail of gunfire outside the Duke of York Tavern in 2008 killed Bailey Zaveda and seriously injured four others says his aboriginal heritage should get him a shorter sentence. Kyle Weese, now 31, is safely behind bars, serving a life term at Millhaven with no possibility of parole for 22 years. But he has filed an appeal, scheduled to be heard next month, where he contends the sentencing judge didn't give enough weight to his First Nations background -- and that should shave six years off the time he must wait before applying for release. It's a terrifying thought. Weese was a career criminal with a frighteningly long history of gun violence. At the time of the Duke of York shooting, he had 31 convictions and had only been out of prison a few months for opening fire and wounding a man over a petty dispute (...) Convicted of second-degree murder and four counts of aggravated assault, Weese faced an automatic life term with a minimum of ten years before he'd be eligible for parole. Justice Mary Lou Benotto ruled Weese would have to wait 22 years -- one of the stiffest parole ineligibility terms on record for his crime. "Mr. Weese has left a swath of destruction behind. He disregards court orders and has shown no possibility of rehabilitation," the judge said in sentencing him in 2011. "He is a dangerous person who must be separated from society." Before sentencing an aboriginal offender, the courts are mandated by Section 718.2(e) of the Criminal Code -- the so-called Gladue principles -- to take into consideration the unique circumstances of their colonial heritage and to find alternatives to their over-representation in the nation's prisons. Postmedia Network (Toronto Sun, Edmonton Sun, Ottawa Sun, Winnipeg Sun)

*** Man who convinced kids to try to drown mom deserves more time in jail, prosecutor says**
Kitchener man who convinced his children to try to drown their mother should spend more time in jail, despite already serving almost eight years, the prosecutor says. Calling it a horrific crime, general Crown counsel Fraser Kelly said on Friday he is seeking an "upper reformatory sentence," which would be in the range of 15 months to two years (...)The man, who can't be named to protect the identity of his children, was convicted in December of attempted murder and conspiracy to commit murder for encouraging his children to try to drown their mom - his ex-wife - in the bathtub. He convinced his children their mother was possessed by the devil and planned to poison them, the trial heard (...) His children, who are now 24, 22 and 19, testified their dad was livid after getting divorce papers in the mail. "I was brainwashed. I was young, naive and foolish," the youngest son said. Both sons were charged and received absolute discharges. It was the second time the man was convicted for the same crimes. He was sentenced to 12 years in prison in 2010. The convictions were overturned last year by the Ontario Court of Appeal, which said the first trial moved into dangerous territory when the father was depicted as a "Jesus nut." Waterloo Region Record

*** Dangerous sex offender has appeal denied**
A convicted sex offender has had his appeal refused after being denied parole last August. Richard Norman Ryan has had both day and full parole denied since being incarcerated in 2001. He is serving his second federal sentence. The Parole Board of Canada in 2015 said Ryan still denies the crime he was convicted of, whereby he held a 26-year-old university student against her will in a motel in the late 1990s. He was convicted of sexual assault, uttering threats and unlawful confinement in connection with the incident. He was on statutory release at the time of the crime. While awaiting the hearing, he was escorted by a correctional officer on a visit to see his dying mother. He snuck out a bathroom window and was at large for 25 days, setting up camp in a tent near Long Harbour before being found by police. Ryan was sentenced to an indeterminate period of time after being designated a dangerous offender.St. John's Telegram, A7

*** Prison term for repeat child porn offender**
A 35-year-old repeat child porn offender will be prohibited from using the Internet, save for a limited number of circumstances, for the rest of his life after flouting a recognizance intended to reduce his risk to children. Judge Carol Snell said she considered a pair of breaches to be at the "highest level of seriousness" when she handed down a four-year prison sentence to Wade Lyle Ellingson for those and for an additional charge of accessing child pornography. Leader-Post, A6

Accused gang murder conspirator granted bail
A Calgary man accused of being part of a conspiracy to murder the notorious B.C. Bacon brothers seven years ago has been ordered released on $200,000 bail. Reasons for the release of Billy Ly, 31, cannot be reported due to a publication ban that was imposed at the bail hearing in B.C. Supreme Court in Vancouver. Justice Catherine Bruce, who impwosed the ban, said Thursday that the recognizance bail will consist of $50,000 cash and $150,000 in sureties. Ly, who was arrested in Calgary in January, will be subject to strict bail conditions (...) Jamie Bacon is awaiting trial in the Surrey Six murders. Jarrod Bacon was convicted of conspiracy to traffic in cocaine and sentenced to 14 years in prison. Postmedia Network (Calgary Sun, A16; Calgary Herald)

Top Court strikes down two crime laws
The Supreme Court of Canada has struck down two federal laws from the previous Conservative government's tough-oncrime agenda, ruling both to be unconstitutional. The decisions put an end to rules for minimum sentences for specific drug crime convictions and limits on credit for pre-trial detention in certain conditions where bail is denied, giving trial judges more leeway. The top court said Parliament has the right to set laws to maintain public safety, but the rules should not be so broad that they capture offenders whose incarceration would benefit neither themselves nor the public. Prime Minister Justin Trudeau said his government is reviewing the laws around mandatory minimum sentences. "There are situations where mandatory minimums are relevant," Trudeau said. Canadian Press (London Free Press, N5; Vancouver Sun, Montreal Gazette, Ottawa Citizen, Toronto Star, Waterloo Region Record, *Telegrapjh-Journal, *Guardian, *Chronicle-Herald, *Times & Transcript, *Ottawa Sun, *Toronto Sun, *Edmonton Sun, *Times Colonist); *Globe and Mail; *La Presse Canadienne (La Tribune, Le Soleil, La Voix de l'Est, Le Droit); Journal de Québec (Journal de Montréal)

B.C. inmates win bid for addiction therapy
Prisoners struggling with opiate addictions in British Columbia jails have gained the same right to medical treatment as people outside the corrections system. B.C. Corrections has implemented a new policy after four men who alleged they were denied opiate replacement therapy launched a charter challenge last month. The men, who are addicted to opiates and range in age from their 20s to late 40s, are now under the care of doctors after a settlement that will also give other prisoners access to timely therapy. "We know, regrettably, there are drugs in provincial and federal institutions," their lawyer, Adrienne Smith, said Friday. "The fentanyl epidemic doesn't stop at the prison gate." "This is a step in the right direction to keep people well, particularly when they're at a good place being able to ask for medical support." Canadian Press (Times Colonist, A4; *Vancouver Sun, Red Deer Advocate)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Inside Insite: B.C.'s supervised injection clinic
Before there was fentanyl, the highly addictive opioid at the centre of an ongoing national crisis, there was OxyContin, another drug that took the lives of vulnerable populations. And before Oxy, there was heroin. In Vancouver's impoverished Downtown Eastside, heroin's ravages helped tip the province into a public-health crisis in the late 1990s. Born of necessity 13 years ago, Insite, a supervisedinjection clinic that remains the only one of its kind of North America, persevered under the former Conservative government's tough-on-crime anti-drug strategy, which ran counter to such treatment models. After successfully battling the government in a series of court cases, the facility has emerged as a model in harm reduction, representing a new approach to addiction treatment that the federal Liberal government has embraced - and one many communities, including Toronto, are trying replicate. Federal Health Minister Jane Philpott has publicly voiced support for harm-reduction facilities and, in January, visited Insite, describing the experience as "extremely moving." Globe and Mail, A14

* **Put community safety first, not addicts**
An open letter states "For or against a safe injection sites in Sandy Hill matters little. What does matter is safety. What perimeter around the community centre would police be authorized to patrol, or not, in order to maintain safety for its residents? What would constitute a "no go" zone for police around an SIS?

Would police simply have to ignore offences committed by those having just safely injected in a"no go zone"? Who would compensate the dozens of nearby residences for a likely devalued property at a moment of sale? Would an SIS be more feasible near the ByWard Market/Sussex Avenue area, where there are fewer residents?" Ottawa Citizen, B7

Race relations remain tense in Montreal North

Ricardo Lamour says he's afraid Quebecers won't remember why people marched on that snowy April 6 evening in Montreal North. He fears they won't recall those peaceful hours, when hundreds sang songs, chanted protest slogans and paid homage to two men who were shot by police in the neighbourhood. Instead, he's worried our collective memories will be punctuated by that brief flurry of violence, by the sound of broken glass and images of thick smoke plumes billowing above a pair of smouldered cars (...) Other witnesses interviewed by the Montreal Gazette corroborated this version of events, claiming that after hours of peaceful marching, the event was hijacked by "outsiders in masks." Further complicating matters are conflicting accounts from within the Montreal police department (...) Though the march was originally slated as a vigil for friends and family of 18-year-old Fredy Villanueva, who died in 2008, recent events added a layer of tension to the proceedings. Last month, police shot Jean-Pierre Bony with a rubber bullet during a drug raid at a Montreal North apartment building (...) Though they died in vastly different circumstances, both Bony and Villanueva were men of colour. Residents of Montreal North - one of the city's most ethnically diverse neighbourhoods - see the police intervention that led to Villanueva's death as a clear cut example of racial profiling. Montreal Gazette, A3

How a week of horror unfolded

Robert Sutherland was heading to bed last Saturday night when there was an urgent knock on his door. "We need you at the hospital for security," the 27-year-old man was told. Sutherland hopped in his truck and raced the few gravel blocks from his clapboard home to the reserve's small hospital, not sure what he would find. What he saw has turned the eyes of the world to this beleaguered fly-in reserve near James Bay in Northern Ontario, where raw pain and defiant pride exist in equal measure, where young people have no memory of ever drinking water from a tap at home, where housing is in short supply and often mould-ridden, where drug and alcohol abuse are rampant and almost everyone has been touched by suicide. Before last Saturday, Attawapiskat, population 2,000, was already in the midst of a suicide epidemic. More than 100 residents, children and adults, have attempted to kill themselves since last fall - 28 in March alone. As the number of suicide attempts mounted, a group of students, desperate to turn things around, walked for three days onto a winter road to convince their peers that suicide is not a solution. They walked in the tradition of other First Nations. They walked because it was a way to move forward - because the living can walk and the dead can't. And then, last weekend, things exploded. National Post, A6

*** Coroner's jury calls for mental-health help in rural B.C**

A coroner's jury in Kamloops has concluded an inquest into the death of 18-yearold Jacob Setah by calling for better mental health services in rural communities. The recommendation was among 15 made by jurors examining Setah's death after he escaped from a psychiatric unit and jumped from the upper floors of the parkade at Royal Inland Hospital in Kamloops in June 2014. During the four-day inquest, jurors heard Setah was being held under the Mental Health Act and had been transferred to Kamloops from his home in Williams Lake against the wishes of his family. Times Colonist, A6

*** Deep Dive Into Violence**

UBC psychology professor Don Dutton, who is about to retire at age 72, has never had a strong desire to be the centre of attention, let alone infamous. To his mind, he just follows the evidence. But the expert on forensic psychology ranks high for controversy, at least in Canada. Dutton has written hundreds of peer-reviewed articles and more than eight books and textbooks. He has won dozens of grants and served as an expert witness in scores of legal cases, including appearing for the prosecution in the 1995 murder trial of former NFL quarterback O.J. Simpson. The more than 250 students who take Dutton's courses each year learn about everything from the reliability of eyewitness accounts to personality disorders, from the roots of genocide to what makes serial killers tick. But on one subject, now known as intimate-partner violence, Dutton has become too hot for many Canadians to handle. Vancouver Sun, G5

*** Canada has a gun problem - and here's why**
Canada has a gun problem. These five words are sure to inflame passions and set off intense disagreement among some Canadians. This is because the words challenge many Canadians' view of themselves and what they believe to be their level-headed approach to firearm ownership.After all, when it comes to guns, Canada is a haven of calm, social liberalism, isn't it? One that stands in stark contrast to the violent world of the neighbouring United States. It's a view firmly laid down by Michael Moore in his film Bowling for Columbine and perpetuated, if nothing else, by the relative absence of debate about gun deaths in Canadian news media. The problem, however, is one born from perspective. From where Canadians stand, their country probably feels safe. After all, according to data from the U.S. Centers for Disease Control and Prevention, there were more than 56,000 gun homicides in the United States between 2009 and 2013. Canada, during that period, tallied 977 firearm homicides, according to Statistics Canada. The difference is so stark, it risks being blinding. Of course, the difference is partly because Canada has far fewer guns. The estimated number of firearms (legal and illegal) in the hands of civilian owners in Canada is about 10 million, about 31 guns per 100 people. The United States has far more guns: about 310 million, almost one gun a person. Globe and Mail, F9

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Annual 4/20 pot protest set to proceed at Sunset Beach**
Vancouver's Sunset Beach is set to get a whole lot greener Wednesday with marijuana activists planning a smoke out at the park for the annual 4/20 pot protest. City staff told activists to find a new venue after last year's protest at the Vancouver Art Gallery drew tens of thousands of smokers, but the park board rankled at their suggestion of a beach venue, where city bylaws prohibit smoking. While the Non-Partisan Association-led park board made political hay of the move and continues to worry about its financial impact, head 4/20 organizer Jeremiah Vandermeer said park staffhave been meeting with him regularly to make sure the protest goes smoothly. "Because of the grey area that marijuana is currently in, it's politically difficult for anybody to accept full responsibility for what happens down there," Vandermeer said in an interview Friday. "They can't come out and say they support us 100 per cent and that we're permitted, but we do everything we can in working with them - just like every permitted event would - and the reason is because we want to make it as safe as possible for everyone." Vandermeer said he and others on his team have been meeting weekly and monthly with "every single person that you can possibly imagine with the park board," from rangers to groundskeepers. They've also been working with the city manager's office, police and other emergency responders, he said. Vancouver Sun, A4 (Ottawa Citizen)

PUBLIC SERVICE / FONCTION PUBLIQUE

PSAC seeks 9% wage hike over 3 years
The largest federal union is seeking a nine-per-cent raise for public servants over three years as part of the first wage proposal tabled since the current marathon round of bargaining began two years ago. The Public Service Alliance of Canada's five bargaining teams tabled the same three-per-centa-year wage hike during its latest bargaining session with Treasury Board negotiators this week. PSAC president Robyn Benson said the union tabled the proposal as a bid to move bargaining forward after two years of making little progress. "We have given the Liberals ample time to reach a fair agreement with federal government workers that will strengthen the public service," said Benson. "We expect the government to respond with proposals that are a real change from the previous government's agenda." The contentious

round of contract talks has dragged on over the hot-button issue of sick leave. The Liberals, like the Conservatives before them, want to replace the existing banked sick leave regime with a new short-term disability plan. That proposal is a non-starter with PSAC and other unions, which have signed a solidarity pact vowing not to make concessions on sick leave. Until now, wages have barely been discussed. Wage increases and the length of a contract are typically the last issues sorted out before reaching a deal. It's unclear whether PSAC negotiators are heading into the final stretch or whether the union is simply trying to change the channel offsick leave. Ottawa Citizen, A13

OTHER / AUTRE

Hostages make plea for ransom in video

With machetes pressed against their necks, two Canadian men held hostage for more than six months in the Philippines appeared in a video released Friday to make a "final urgent appeal" to Ottawa to comply with their captors' ransom demands. If payment of 300 million pesos ($8.35 million) is not received by April 25, the video message warns, one member of the captured group - which includes a Norwegian man and a Filipino woman - will be beheaded. "We're told that this is the absolute final warning, so this is a final urgent appeal to governments, Philippine, Canadian, and families, if 300 million is not paid for me by 3 p.m. on April 25th, they will behead me," hostage John Ridsdel, a semiretired former mining executive, said in the grainy video. A spokeswoman for Global Affairs Canada said Friday the government was aware of the video but could not comment or release any information that might "compromise ongoing efforts or endanger the safety of Canadian citizens (…)" Their captors belong to the militant Islamist group Abu Sayyaf (…) Formed in the early 1990s with funding from al-Qaida, Abu Sayyaf is a collection of autonomous gangs spread across the jungles of the Sulu Archipelago with poor communications and no centralized leadership. They appear to be taking a page from ISIL's playbook by posting these staged videos and using social media, Abuza said. However, there is no evidence the Islamic State of Iraq and the Levant controls the groups or provides any resources, he said. **Public Safety Canada** listed Abu Sayyaf as a terrorist group in 2003. National Post, A3 (London Free Press, Vancouver Sun, Ottawa Citizen, Kingston Whig-Standard); Reuters (Winnipeg Sun, Toronto Sun, Calgary Sun, Edmonton Sun); Toronto Star; Journal de Montréal

INTERNATIONAL

Powerful earthquakes in Japan kill at least 32

Army troops and other rescuers rushed Saturday to save scores of trapped residents after a pair of strong earthquakes in southwestern Japan killed at least 32 people, injured about 1,500 and left hundreds of thousands without electricity or water. Rainfall was forecast to start pounding the area soon, threatening to further complicate the relief operation and set off more mudslides in isolated rural towns, where people were waiting to be rescued from collapsed homes. Kumamoto prefectural official Riho Tajima said the death toll stood at 22 from the magnitude-7.3 quake that shook the Kumamoto region on the southwestern island of Kyushu early Saturday. On Thursday night, Kyushu was hit by a magnitude-6.5 quake that left 10 dead. CBC News

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
May 3, 2016 / le 3 mai 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

RCMP settles sex harassment suit with Catherine Galliford
Former spokeswoman went public about her allegations with CBC News: Cpl. Catherine Galliford, whose allegations of sexual harassment in the RCMP sparked widespread attention, has accepted a settlement that ends a four-year legal battle with the national force. The former high-profile British Columbia spokeswoman for the force first went public with her claims of long-term sexual harassment over two decades with the RCMP on the CBC in November 2011. That opened up a flood of similar complaints. (…) In February, Galliford wrote to **Ralph Goodale**, the new **minister of public safety**, saying, "I have been off duty sick from my workplace due to ongoing harassment, sexual harassment, sexual abuse and sexual exploitation." She said she was "an extremely professional, compassionate and capable police officer until I developed health issues due to the ongoing misogyny, harassment, lying and both criminal and sexual corruption which I observed within an organization which I once revered." Galliford was awaiting an eight-week trial in early 2017 after a postponement from early 2015. The letter to **Goodale** said, "I [went] through 11 legal discoveries in rooms full of lawyers (for the various defendants) asking me about my sex life, my childhood, my high school boyfriends, my parental upbringing and whether or not I had my uniform altered to make it 'tighter.'" CBC News

Canadian Red Cross launches new emergency preparedness app
A new app by the Canadian Red Cross aimed at helping people prepare for natural disasters is now available for download. The "Be Ready" app gives users specific tips on how to get ready for emergencies like planning escape routes or having a checklist of necessary items for the home. The Canadian Red Cross said the app should be a must for Canadians. "It's about getting the message out to the people of Saskatchewan and Canada about the importance of being prepared," Canadian Red Cross Provincial Disaster Management Dave Kyba explained. It's a thought echoed by **Public Safety and Emergency Preparedness Minister Ralph Goodale**. ***"It will empower Canadians to take better responsibility for their own personal preparedness,"*** he said. ***The app also has real time alerts for emergencies such as floods, severe weather, and wildfires. Last year was the worst wildfire season on record with blazes ravaging over 17,000 square km of forest in the province.*** (...) **Goodale** also said ***natural disasters and human-caused hazards are increasing in frequency. "These events pose a real threat not only to the safety of our communities but also to our economic stability so it's crucial we focus on prevention and mitigation,"*** **Goodale** said. The app is available in both English and French, and for download on iOS for Iphone and Android devices. Global News; 620 CKRM

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Canadians mark National Emergency Preparedness Week**
Plan, prepare and be aware is the theme of National Emergency Preparedness Week, which is marked across Canada this week. The City of Red Deer encourages all residents and families to follow three easy steps to prepare for emergencies including knowing the risks in your community, making an emergency plan for yourself and your family and obtaining a 72-hour emergency kit. "People who are prepared for emergencies can be less reliant on first responders and other government and non-profit services when disasters occur," said Karen Mann, the city's Emergency Management coordinator. "Preparedness does not have to be costly or take a lot of time. It can be done as a family in ways that are both fun and effective." The theme this year also aims to get residents thinking about how they can access timely, accurate information before, during and after an emergency event. Red Deer Advocate, A3

*** Canadian Red Cross launches app to help prepare for emergencies**
A new app has been designed to help Canadians prepare for emergencies and disasters. The app, called Be Ready, was launched by the Canadian Red Cross across the country on Monday, with the Saskatchewan rollout happening in Regina. Be Ready alerts users about weather conditions that could prompt emergency situations such as floods, forest fires and tornadoes. It uses data feeds collected by the Weather Network (...) According to the Red Cross, the app is important for emergency preparedness because only 47 per cent of Canadians have any type of emergency supply kit in their homes. However, three quarters of Canadians feel confident they would know what to do in an emergency situation. CBC News

*** Drones are the future of search and rescue**
After a 7.8-magnitude earthquake ripped through Ecuador's coastal region last month, Toronto-based GlobalMedic answered the call for aid with a posse of drones, which can survey, map and pinpoint damage as well as the location of survivors. The group's founder, paramedic Rahul Singh, says they're the way of the future for humanitarian aid. GlobalMedic creates pop-up hospitals in war and disaster-struck countries, provides water purification and landmine clearance, and delivers drugs and training to local doctors around the world. Its volunteers are deployed from Eastern Ukraine to Iraq. But, Singh explains, cutting-edge technology is increasingly a vital partner in saving lives, and is expanding its reach. Toronto Star, A2

Sizzling weather stokes wildfire fears
An estimated 500 to 700 people were told they could return to their homes Monday night, after a wildfire threatening the southwest edge of Fort McMurray moved farther away. The fire burned about 1,250 hectares and was about 1-1/2kilometres from the nearest home, a news conference in the city heard

Monday afternoon. Fort McMurray Mayor Melissa Blake lifted a mandatory evacuation order for the Prairie Creek area, imposed Sunday night, though one remained in place for Centennial Park. "We're certainly very happy that no one's had their properties damaged, no one's been hurt, and we hope that continues," Fort McMurray fire Chief Darby Allen said. Bernie Schmitte, provincial wildfire manager for Fort McMurray, said 36 firefighters battled the blaze Monday, assisted by helicopters and water bombers, while 128 firefighters were on standby. A hot, dry spring and a snowpack that pales in comparison to most years means great swaths of Alberta are under high to extreme fire danger, fanning the worry that fires will flare-up across the province. Forty-three counties and municipal districts were under fire bans Monday, including Sherwood Park and Strathcona and Parkland counties. Postmedia (Edmonton Journal, A1; Calgary Herald, Calgary Sun, Edmonton Sun); Canadian Press (Red Deer Advocate, A1; St. John's Telegram, Times Colonist, Times & Transcript, *Whitehorse Daily Star, *Castanet, Maclean's, *Metro News); *CTV News; *CBC News

Edmonton could hit 29 C on Tuesday, melting 50-year-old record for May 3

Edmonton could break several temperature records in the coming days, including a 50-year-old mark for May 3. Temperatures hit 28 C Monday, nearly breaking the previous record of 28.5 C set in 1980 (...) Residents can expect some short-lived respite from the heat Thursday, when a cold front from the north is expected to bring temperatures down to 19 C, but the heat should return by the weekend. "The cold front might bring a little bit of shower activity towards Thursday, but it might just be hit and miss weather," said George Pearce, a forecaster with Environment Canada. It's also causing prime wildfire conditions across Alberta (...) Although the forecast doesn't bode well for wildfire management, Edmonton Fire Rescue Services has not declared a fire ban for the city. Edmonton Journal

*** Wildfire in La Ronge, Sask., prompts call for regional fire ban**

A wildfire in the Town of La Ronge, Sask., has prompted a push for a regional fire ban. On Monday, the La Ronge regional fire department responded to a fire bordering the new Mowery subdivision. The fire originated in a heavily forested area, before spreading to other homes. Nearby homes were proactive, dousing their lawns just in case the fire spread. Firefighters controlled the fire with the help of a water helicopter. La Ronge Mayor Thomas Sierzycki said his town was packed with snow up until about mid-April, but since then they've seen very hot, dry conditions and gusting winds. CBC News

*** Near-record warm weather on the way for Saskatchewan**

Environment Canada' sevenday weather forecast for Regina and area predicts daytime highs of 26 C Tuesday and Wednesday, then a peak of 29 C on Thursday before things cool down - a bit - for the weekend. That's not record-setting for this time of year, but pretty close, says Phillips. The records for early May, set in 1918 and 1992, are in the low 30s. But these temperatures are also a long way from the long-term average for southern Saskatchewan in the first week of May: daytime highs around 17 C and nighttime lows of about 1 C. And because a high-pressure ridge has parked itself atop our region, there's no sign this weather pattern will change in the near future, he added. (...) So that raises a question: will we pay for this with an abnormally dry summer - maybe even a drought? (...) But Phillips pointed out that hot weather means there will be a bigger need for moisture, though there doesn't seem to be any coming over the next week, at least. Nobody knows that better than Sask911, the provincial agency that co-ordinates response to wildfires of all kinds. Leader-Post, A3

Wildfires spark two evacuation alerts in northeast

Unseasonable heat is once again searing northeastern British Columbia, fuelling wildfires that have prompted evacuation alerts around two communities. The Peace River Regional District says residents about 60 kilometres northeast of Fort St. John should be ready to leave on short notice as the Siphon Creek wildfire is uncontained and burns nearby. It has now charred an estimated 40 square kilometres, more than doubling in size since Friday, in part because of temperatures that reached 23 C Sunday and are expected to reach 27 C this week. Winds gusting to 40 kilometres per hour are also forecast, potentially complicating firefighting efforts in the Cecil Lake area about 30 kilometres east of Fort St. John, where two small wildfires threaten a number of homes. Canadian Press (Vancouver Sun, A5)

Heat is on as weather records fall

May is off to a scorching start, with sky-high temperatures Monday shattering records in almost two dozen

municipalities across B.C. At Vancouver airport, the mercury hit 24.7 C, breaking the previous record of 23.9 set in 1945. It was even hotter in downtown Vancouver's Coal Harbour, where temperatures reached 27.2, more than five degrees higher than the previous 22.1 record set in 1998. In the Fraser Valley, Chilliwack sizzled with a high of 29.9 that broke the century-plus old mark of 28.3 set in 1898. Neighbouring Abbotsford and Hope reached 29.6 and 30.4, respectively, surpassing records set in the mid-1940s. Postmedia (Vancouver Province, A3; Vancouver Sun)

Firefighters hope rain brings relief to province's dangerously dry conditions, fearing wildfires
New Brunswick firefighters are worried that the province is headed for a fire season similar to 1986, the worst season in memory, during which hundreds of fires destroyed thousands of hectares. In fact, the amount of forest burned so far this season is 51 per cent higher than the 10-year seasonal average, with more than 200 hectares burned in the province since April 18. The 10-year average is 132 hectares for the whole forest fire season, according to the Department of Natural Resources. The extremely dry conditions have resulted in a continuous provincewide burning ban over the past two weeks, and yet there have been 165 fires across the province in that time. The majority of these have been grass fires. It's not clear what caused most of the blazes, but fire departments are reminding people of the burning ban that's in effect for most of the province. Daily Gleaner, A3; L'Acadie Nouvelle

* **Air search for Nunavut MLA Pauloosie Keyootak cost $339K**
The federal and territorial governments spent a combined $339,139.70 on planes and helicopters in the search and rescue of Nunavut MLA Pauloosie Keyootak and two others this spring. The Government of Nunavut spent just over $75,000 and the rest was spent by the Canadian Armed Forces. Keyootak, his son and nephew left Iqaluit in mid-March on two snowmobiles on their way to Qikiqtarjuaq with a planned stop in Pangnirtung. When the group failed to make it to Pangnirtung, a ground search was started on March 27. Civilian and military air crews joined the search in the following days. The group was found on March 31, 183 kilometres south of Iqaluit on the Hall Peninsula. They had gotten turned around in bad weather and a GPS system on a smartphone led them further astray. They were not carrying a SPOT device or a satellite phone. In an email to CBC News, a Canadian Armed Forces spokesperson said the approximate total incremental cost was $263,632.57 for "CH-149 Cormorant and CC-130 Hercules Search and Rescue aircraft fuel consumption, accommodation and temporary duty allowances for aircrew and aircraft landing fees" from March 29 to 31. CBC News

* **Ottawa verse 75 M$ en douce**
Le gouvernement fédéral a discrètement versé 75 millions $ dans le fonds d'indemnisation pour les victimes et les créanciers touchés par la catastrophe de Lac-Mégantic, une contribution qui l'a mis à l'abri de toute poursuite judiciaire. L'ancienne ministre des Transports Lisa Raitt a déclaré que les négociations pour cette entente, qui concerne aussi 24 autres défendeurs, avaient commencé avant que les conservateurs ne perdent les élections d'octobre. Le nouveau gouvernement libéral a refusé de dévoiler combien il avait déboursé pour le fonds d'indemnisation de 460 millions $, même si au moins deux parties accusées d'actes répréhensibles en lien avec le déraillement et l'explosion d'un convoi de pétrole au coeur de la ville québécoise ont révélé le montant de leurs contributions. Dans une récente entrevue, Mme Raitt a toutefois affirmé que cette somme était publique puisqu'elle figurait dans le budget supplémentaire des dépenses et dans les états financiers trimestriels de Transports Canada sous la rubrique « règlement hors cour ». Le montant indiqué s'élève à 75 millions $. La Presse Canadienne (La Tribune, 7; Le Soleil, Le Nouvelliste); Canadian Press (Kingston Whig-Standard, National Post, Times Colonist, Toronto Sun, Edmonton Sun, Calgary Sun, Ottawa Sun, Globe and Mail)

* **CN Rail struggled with track issues months after resuming operations**
Canada's biggest railway struggled to keep some heavily used track in adequate repair even after a string of derailments last year showed the danger of moving oil on poorly maintained track, documents obtained by Reuters show. Three trains derailed along one 476 km section of Canadian National Railway Co. track in northern Ontario in February and March last year. The third train spilled crude oil in and around a river near the town of Gogama, igniting a fire that burned for days. More than 100 pages of correspondence and inspection reports obtained by Reuters under Canada's freedom of information law show that a March inspection by Transport Canada, the ministry responsible for rail safety, found a number of problems with the track. But the documents also show that during a July inspection, months after normal

operations resumed, inspectors found new track problems, including rail that had been secured with too few bolts, and defective ties. CN brought its trains back up to normal speeds in late May. CN Rail told Reuters the July inspection ultimately uncovered 57 defects, including 10 that required temporary speed reductions. Seven of those 10 were on the main line. CN said the defects found in July were repaired by Sept. 3. Transport Canada lifted its March safety notice on Dec. 15, 2015, signalling that it believed safety problems in the area had been resolved. But the regulator has not conducted a track inspection since July. Reuters (2016-05-02)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Spy agency cagey on privacy breaches: Bureau won't put a number on cyber-snoops since 2007
The Communications Security Establishment is refusing to release the number of privacy breaches the agency has logged since 2007. Documents obtained by the Star state the intelligence and cyber defence agency has maintained a central database for certain privacy violations since 2007. These breaches are categorized as minor "procedural errors" or more serious "privacy incidents," and reviewed by the CSE Commissioner's office every year. "In these files, CSE records any incidents it identifies that put at risk the privacy of a Canadian in a manner that runs counter to (or is not provided in) its operational policies," says a September 2014 letter from former CSE chief John Forster to a senior Treasury Board official. The Star requested just the number of breaches - no details about what actually transpired or the Canadian personal information involved - but was told the agency could not comply due to "operational security concerns." "Releasing the number of (breaches) would provide insight into CSE's capacity to conduct operations, the extent of its capabilities, the degree to which partner organizations benefit from sharing and the reach of the programs," wrote spokesperson Ryan Foreman in an email last week. CSE is one of Canada's most technologically sophisticated agencies, responsible for collecting foreign intelligence and protecting Canadian networks from cyber-attacks. It is forbidden to use its surveillance tactics against Canadian citizens, except under specific circumstances. But disclosures from U.S. whistleblower Edward Snowden have aroused suspicion about CSE's tools and tactics as part of the Five Eyes alliance that also includes the U.S., U.K., Australia and New Zealand. Documents tabled in Parliament last month show CSE logged 13 privacy and information breaches in 2015, affecting at least 630 individuals. The agency did not report any of the privacy breaches to the federal privacy commissioner, as CSE determined that there was "no significant risk" to the individuals involved. CSE further refused to report the activities that led to the breaches. Toronto Star, A2

Ex-CSIS source guilty of fraud
Ontario Superior Court Judge Timothy Ray could not have been clearer Monday in delivering his verdict to former construction boss and CSIS informant Roland Eid. "ICI (Construction) was a sham from early 2007 until its demise," Ray said in delivering a summary of his 89-page decision. ICI was the construction company launched by Eid in 2006. It went bankrupt early in 2008 after Eid transferred $1.7 million from its coffers to a personal account in Beirut. The money was never returned. The judge found Eid guilty of 10 counts of breaching the Criminal Code and the Bankruptcy and Insolvency Act. He found Eid had defrauded ICI creditors, causing them to suffer collective losses of $3.8 million. The judge also found that Eid had "perpetrated a fraud by taking $1.7 million which were trust funds belonging to the subcontractors and suppliers out of Canada and beyond their reach." Eid's defence contended the money was to have been used to finance a new construction project in Lebanon and Syria. He claimed the Syrian government would match the money deposited in his Beirut account - money that Eid said he would return to ICI in Ottawa. Ottawa Citizen, A1 (Ottawa Sun)

*** Going up in smoke: Terrorist financing and contraband cigarettes**
In 2000, the United States authorities caught two Lebanese brothers for running a multimillion-dollar smuggling operation, moving low-tax cigarettes from North Carolina to high-tax Michigan. It was a major coup for the Bureau of Alcohol, Tobacco, Firearms and Explosives. But the bureau was shocked when it realised where the profits of the syndicate were diverted to: designated terrorist organisation Hizbollah. The bureau quickly stepped up its focus on the ties between cigarette smuggling and terrorism (...) A new study from the Macdonald- Laurier Institute in Canada in March addressed the links between illicit cigarettes and terrorism squarely. "Canadian law-enforcement seizures of contraband tobacco routinely

include high-powered weapons, hard and designer drugs, stolen vehicles and other merchandise, and lots of cash," it said in a report. "Globally, money from contraband tobacco and cigarettes is a major source of revenue for the likes of ISIS, Al-Qaeda and Hizbollah." Trading in cigarettes is a popular choice for terrorists because they are easy to smuggle, have low barriers of entry, enjoy a huge market and provide high profits. As a legal product in almost all countries, it does not carry the same risks and draconian penalties as drugs. Straits Times

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Gas station owners guilty of hiring illegal workers

The owners of an Alberta gas station were fined $36,000 Monday, admitting they illegally hired foreign workers. Yoo and Yoo Enterprises Ltd. pleaded guilty in Edmonton provincial court to four offences under the Immigration and Refugee Protection Act relating to employing a foreign national in a capacity in which they were not authorized to be employed. In exchange for the guilty plea involving nine Filipino workers, charges against Soon Sang Yoo and his son, Hyun Suk Yoo, were withdrawn, as well as other charges against the company. According to an agreed statement of facts, the Yoos own and operate the Mundare Esso gas station. They were losing workers in 2013 and having difficulty recruiting Canadian citizens or permanent residents to work for their business. (…) Federal prosecutor Michelle Ferguson told court that Hyun Suk Yoo knew the workers were foreign nationals and that they were not authorized to be employed at the Mundare Esso. Court heard that once they began working, Yoo would have the family friend start the paperwork so the worker could get a new work permit authorizing them to work at Mundare Esso. (…) Four of the workers involved were able to successfully obtain new work permits authorizing them to work at Mundare Esso, but the other five were arrested during a during a Dec. 11, 2013 raid by the Canadian Border Services Agency. Defence lawyer Dan Chivers told court the Yoos are "extremely remorseful and embarrassed" over the workers' situation. Postmedia Network (Edmonton Sun, A17, Edmonton Journal)

Evraz to lay off 90 workers at Regina pipe mill this week

Evraz North America is laying off 90 workers at its pipe operations in Regina later on this week, in addition to about 30 layoffs in its steel mill last month, according to a spokesman for the Chicago-based steelmaker. "I can confirm that we have announced layoffs at our 24-inch pipe mill, effective May 7, impacting approximately 90 employees and expected to last three weeks,' said Christian Messmacher, vicepresident of investor relations and strategy for Evraz North America. "This necessary production adjustment is due to market demand and unfairly traded and subsidized steel pipe imports,' Messmacher said. "Similarly, we have issued layoff notices impacting 49 employees at our Calgary tubular facility effective May 15, subject to be postponed or cancelled as market conditions evolve this week." (…) In February, the Canadian International Trade Tribunal (CITT) found that Canadian producers have been injured due to dumped and subsidized imports of certain line pipe products from China. The decision applies anti-dumping and countervailing duty measures established by the Canada Border Services Agency to restore market-based pricing to Chinese exporters. "Today's decision allows Canadian pipe manufacturers to compete more effectively in an exceptionally difficult oil and gas market," said Conrad Winkler, president and CEO of Evraz North America. "Evraz and other steel operations continue to be impacted by the flood of unfairly traded line pipe imports." Postmedia Network (StarPhoenix, C3, Leader-Post)

Dieudonné revient à Québec

Dieudonné reviendra à Québec le temps de deux spectacles, a appris Le Soleil. Le controversé humoriste défendra sa production En paix le 16 mai, à LaScène Lebourgneuf, dans le cadre d'une tournée qui comporte des haltes à Montréal et à Trois-Rivières. Cette nouvelle visite est orchestrée par les productions de la Plume - gérées par la femme de Dieudonné - en conjonction avec une équipe de coordination québécoise, composée notamment de Gino Sainte-Marie, fondateur du Festival de jazz de Québec, et de Louis Tall. M. Tall est conscient que Dieudonné M'Bala M'Bala a été au coeur de plusieurs controverses. Il a assuré cependant, au nom des productions de la Plume, qu'il n'y a rien de litigieux dans cette nouvelle proposition : «Avec le spectacle En paix, il n'y a eu aucune poursuite. Il joue depuis 2015 et il a joué partout en France. Et c'est pour ça qu'il voulait le présenter au public québécois. Il sait qu'il est beaucoup aimé dans la province.» (…) Une question demeure toutefois : avec «son casier [judiciaire] de

12 pages» et ses «12 condamnations», dont il fait état dans En paix, Dieudonné pourra-t-il se produire au pays ou sera-t-il refoulé à la frontière? A Montréal, le maire Coderre y est allé d'un message sans équivoque dans Twitter, indiquant qu'il n'était pas bienvenu, tandis que la ministre fédérale du Patrimoine, Mélanie Joly, a soutenu qu'il reviendrait à l'Agence des services frontaliers de trancher. Pour sa part, M. Tall affirme que l'équipe de Dieudonné respecte la liberté d'expression du maire de Montréal et se pliera à la décision des autorités. «La production s'en remet aux douanes et à l'immigration canadienne pour prendre la décision sur son entrée ou pas. Ils sont bienveillants des lois. Ils se sont préparés pour donner le plus d'information possible aux douanes.» Le Soleil, 11 (La Presse)

Little bit of U.S. in Manitoba
Take an hours-long drive on a Manitoba gravel road north of the Minnesota border and you'll come across something curious: a piece of the U.S. located well inside Canada's mainland. Minnesota's Northwest Angle in Lake of the Woods touches no other American land. It's just a snippet of Canada that happens to be American. Why? It was apparently a mistake on a map in 1783 that was never corrected. The border was intended to cut through the lake, but the map was wrong, and actually included not just water, but a large peninsula. Only a few dozen people live there - mostly those who run fishing lodges. But for residents who make it home, it's a day-long journey through Canada and back into the U.S. just to go grocery shopping. That includes a stop at a small Canadian border post, a drive through Canada, then another border crossing back into the main United States. "It pretty much takes up your day," resident Jason Goulet told CBS News. Postmedia Network (Winnipeg Sun, A2, Toronto Sun, Calgary Sun, Edmonton Sun)

Trial delayed again
A trial involving the man implicated in B.C. teen Amanda Todd's suicide has been delayed again. Aydin Coban faces charges in the Netherlands, including child pornography and extortion allegedly involving 39 people, but Dutch officials say the case will not go to trial until after summer. Coban also faces extradition to Canada on five charges connected to Todd, who killed herself in 2012 after being bullied over nude photos posted through social media by an online harasser. The Province, A8; Canadian Press (Red Deer Advocate, Whitehorse Daily Star, Times Colonist, Times & Transcript)

Final bidding process for Gordie Howe bridge project stalled
The final step in the bidding process to select the contractor to build the Gordie Howe International Bridge has been delayed by several months, after it was initially scheduled to begin at the start of the year. "I am concerned," said local MP Brian Masse (NDP Windsor-West). "Obviously, there is urgency to move the project along, but we haven't heard anything. "If there is an administrative problem or a political problem, we should know." The Windsor-Detroit Bridge Authority has not released its final request for bids from the three consortiums shortlisted in January. Known as request for proposals, it is the final step in the process to select a contractor for the project. The RFP includes specifications and details for consortiums to follow in order to assemble final design and cost estimates to construct the bridge. (…) Interim chairman Dwight Duncan leads the WDBA board. He previously stated the new Trudeau government remains committed to the project and it remains a high priority. Duncan on Monday said he had no further comment on the status of the RFP process. "Infrastructure developments of the magnitude of the Gordie Howe International Bridge project require a great deal of preparatory work to be completed before actual construction starts," Butler said. "The WDBA is working to move the project forward as soon as possible." WDBA has repeatedly stated a contractor would be in place by the end of this year, but that appears unlikely given the delay in launching the RFP. It also raises questions whether the scheduled 2020 completion deadline for the bridge project can be met. Windsor Star, A3

*** Les producteurs laitiers érigent un barrage devant les bureaux de Parmalat**
Les producteurs laitiers venus d'un peu partout dans la province ont organisé un coup d'éclat en bloquant la rue Saint-Jacques, dans le quartier Notre-Dame-de-Grâce à Montréal, devant les bureaux de la compagnie laitière Parmalat. Le barrage a commencé très tôt ce matin, aux alentours de 4h30. Par cette action, les producteurs de lait veulent notamment dénoncer l'importation de lait diafiltré au pays. Cette substance est un lait ayant été filtré à plusieurs reprises pour obtenir un produit ultra protéiné. Au Canada, elle est utilisée par les grands transformateurs québécois dans la fabrication de yogourt ou de fromage. Non seulement les usines américaines vendent ces sous-produits à des prix très bas pour s'en

débarrasser, mais ils entrent au pays, librement, sans normes de contrôle et surtout, exempts des tarifs douaniers. (…) À la frontière canadienne, le lait diafiltré est identifé comme un ingrédient, ce qui fait en sorte qu'il n'est pas assujetti aux tarifs douaniers imposés pour l'importation de lait, oeufs et volailles. Ces tarifs peuvent s'élever de 200 % à 300 %. TVA Nouvelles (Journal de Montréal, Journal de Québec)

*** Federal MPs Encouraged to Press for Reinstatement of Emergency Swine Transportation Protocol**

Canadian pork producers are being encouraged to urge their Members of Parliament to put pressure on the Canadian Food Inspection Agency to reinstate a swine transportation protocol designed to keep PED out of Canada. The Canadian Food Inspection Agency has terminated an emergency transportation protocol that allowed Canadian swine transport vehicles returning from U.S. farms to be sealed at the border then washed and disinfected at certified Canadian truck washes and, as of May 2, is requiring those transports to be cleaned in the U.S. before re-entering Canada. Harvey Wagner, the Manager of Producer Services with Sask pork, says there is a high risk those trucks will become contaminated in those U.S. truck washes. FarmScape

More tourists have visited New Brunswick cities in February 2016 than July 2015

With the summer tourism season quickly approaching, Saint John tourism operators are preparing for an influx of visitors to the city because of the low Canadian dollar. According to a study done by Statistics Canada, about 28,400 people visited New Brunswick from the United States in February alone, which is about 7,000 more than last July during tourist season. Ellen Tucker, the president of Freedom Tours and Travel, said she expects her tour bookings to increase this summer. "The value of the Canadian dollar is probably the biggest reason. We found there's a big increase in travel to Canada." Telegraph-Journal, B3

*** Labeaume en mission économique à New York**

Le maire Labeaume mènera une délégation de chefs d'entreprise et d'acteurs touristiques de la région de Québec à New York la semaine prochaine, afin de faire rayonner la ville et identifier de nouvelles opportunités d'affaires. Au total, une vingtaine de compagnies, d'hôtels et d'organismes seront du voyage, qui se déroulera du 9 au 11 mai. La mission économique de l'an dernier a eu de telles retombées que le maire de Québec estime important de renouveler l'expérience. (…) Avec l'approche de l'été, le moment est opportun pour vendre Québec comme destination de vacances aux Américains. La valeur du dollar canadien par rapport au billet vert favorise aussi nos voisins du sud, qui sont plus nombreux à traverser la frontière depuis le début de l'année. « Pour janvier et février, on parle d'une augmentation de 26 % aux douanes, donc le timing est très bon d'aller se pointer à New York », estime André Roy, directeur de l'Office du tourisme. Radio-Canada (2016-05-02)

*** He's behind bars for 14th birthday sex try with Canadian girl**

A Garden Grove resident accused of exchanging lewd videos with a Canadian teenager and traveling to that country to have sex with her on her 14th birthday surrendered Monday to face federal charges. Paul Binh Do, 29, was charged in April with one count each of traveling with the intent to engage in illicit sexual conduct and receipt of child pornography, according to Thom Mrozek of the U.S. Attorney's Office.(…) Do met the girl online, and the two exchanged videos of them individually "engaging in sexual conduct," prosecutors allege. On May 2, 2014, Do traveled to Canada to "celebrate the 14th birthday" of the girl and to have sex with her, but Canadian authorities stopped him at the border, according to Mrozek. During his detention in Canada, Do allegedly was found to be in possession of digital devices that contained lewd videos of the victim, according to Mrozek. Do is also accused of calling the girl and asking her to falsely tell authorities that she lied to him about her age, Mrozek said. Authorities in Canada were already investigating Do, prompting his detention in Calgary as he attempted to enter the country, Mittal said. MyNewsLA (2016-05-02)

Employment agency fills hospitality shortages with millennials

An immigration and staffing agency that was once one of the largest recruiters of temporary foreign workers is now looking to millennials to fill vacancies in the tourism, hotels and restaurants in remote locations across Canada, including Fort McMurray, Bonnyville and Banff. The program, called Mobilize Jobs and launched in January 2015, promises young Canadians a chance to explore spectacular parts of Canada and gain work experience as they slog away in low-wage jobs, including housekeeping and

waiting tables. "My long-term goal is to reduce youth unemployment drastically," said Benjamin Guth, program manager of Mobilize Jobs and vice president of Diamond Global Recruitment Inc., the staffing agency to which Mobilize belongs. The program came to fruition after Diamond's clients, especially those in Alberta, were hard-hit by changes to the temporary foreign worker program that started in 2014 with a moratorium on restaurants using the program. It continued with restrictions on the number of temporary foreign workers businesses could hire and the process for hiring them. "We were bringing in about 1,000 people a year for about 100 different employers from about 8 difference countries ... almost overnight, we weren't able to fill a lot of those shortages," recalled Guth. At the same time, the tourism and hospitality business in various parts of the country was struggling with a long-term labour shortage intensified by changes to the TFWP. Calgary Herald (2016-06-02)

Entendre ou pas Dieudonné

Un article d'opinion déclare, « Il y sera. Ou pas. L'humoriste Dieudonné doit entamer le 11 mai à Montréal une tournée québécoise qui se poursuivra jusqu'à Trois-Rivières la semaine suivante. Une dizaine de spectacles prévus dans une petite galerie d'art africain de la rue Ontario affichent déjà complet. Ce sera aux services frontaliers canadiens de déterminer s'il doit ou non être admis au pays. L'humoriste pourrait en effet être refoulé à la frontière, dès son arrivée à l'aéroport Trudeau, en raison de son casier judiciaire français. Et la sempiternelle question de se poser de nouveau : devrait-on _ ou pas _ permettre à un artiste aussi controversé de se produire chez nous ? Il y a bien des arguments valables en faveur et en défaveur de la présence de Dieudonné au Québec. Le maire de Montréal Denis Coderre a déjà statué, sur sa plateforme médiatique préférée, Twitter, que l'artiste était persona non grata en nos terres. « Une personne qui incite en Europe à la haine raciale et qui est un fomenteur de tensions sociales n'est pas le bienvenu à Mtl. Dieudonné OUT », a écrit le maire Coderre lorsque la série de spectacles de Dieudonné a été annoncée, le mois dernier. On comprend aisément son indignation. Depuis 15 ans, le discours public de Dieudonné _ artistique comme citoyen _ n'a eu de cesse de se radicaliser. Ce provocateur-né cherche constamment la confrontation, la controverse et la polémique. Et il l'a le plus souvent trouvée sur son chemin. L'humoriste a été condamné à plusieurs reprises, en multipliant les déclarations ambiguës, les insinuations perfides et les amalgames à propos du peuple juif. (…) Menacer de le refouler à la frontière, c'est ni plus ni moins faire le jeu de cet opportuniste sans scrupules, dont la victimisation est devenue le fonds de commerce. Comment justifier la tentative de musellement d'un humoriste alors que l'on clame partout, en particulier depuis la tragédie de Charlie Hebdo, l'importance du droit à la libre expression des artistes ? » La Presse +

* **Captive to our own barriers**

An opinion piece states, "Populism has dangerous overtones. America's anger over trade agreements and recent European hostility towards immigration are not just matters of intolerance but also isolationism - putting up barriers to trade and mobility. Limiting competition among countries for people, goods, services and capital will have consequences. History teaches us that trade and mobility lead to higher incomes and wealth over time. It is not just consumers who benefit from lowerpriced goods through gains from trade. Economies create new "Silk Roads" that ultimately lead to sharing innovative ideas. When trade and capital flows decline, it is often associated with low growth. (…) Then there are government controls over immigration. Immigrants bring their labour skills to their new home, as well as increased demand for goods and services, enabling businesses to improve productivity and achieve lower unitproduction costs. This, however, is not a widely accepted fact. Many industrialized nations still believe that foreign workers take jobs away from locals and potentially disrupt their "normal" way of life. Despite its good record of integrating immigrants in the economy, even good-natured Canada notoriously limited immigrants after the First World War and, more recently, began imposing stricter limits on temporary foreign workers in the name of "protecting" Canadian jobs. Walls are built quickly whenever populism dominates politics. So let's be honest. Because the latest anti-globalization trend puts up barriers to mobility and trade, it can only make politicians happier, since they have new power to regulate and tax their own markets. And since governments, especially those in an isolationist mood, typically fail to pick wise taxation and regulation policies, it will be workers who end up being the real losers when their incomes only stagnant." National Post, FP7

Mr. Trump, build that wall
A letter to the editor states, "Of the three actors performing for the U.S. Republican presidential nomination, Donald Trump, Sen. Ted Cruz and Ohio Gov. John Kasich, only Trump might build a wall along the U.S.-Canada border. Hopefully, he will. That might stop the U.S.-inspired drug and gun crime crossing into Canada through Surrey and seeping into the Okanagan-Similkameen, which includes Penticton and Princeton." The Province, A12

* **Shooting club opens range for public tours**
It was specifically an open house for the Loyalist Shooting Club (LSC) here on Saturday, but it was also the first opportunity for the public to get a glimpse of a new facility that will be catering to emergency responders. What was once a public school in Tincap, located on County Road 29, is now close to opening as a place used by gun registrants, people looking to complete particular firearm courses, and emergency workers practicing emergency situations. The facility, owned by the security company Reticle Ventures Canada, still has elements of a school, but it is quickly changing. There are still classrooms, but the lessons will be vastly different - with one of the rooms on Saturday housing a shooting simulator. A few feet away from a back entrance was a shooting range with 10 contained bullet paths, purchased from the Canadian government and once used by the Canadian Border Service Agency. Brockville Recorder (2016-05-02)

* **Last chance to see Peace Tower before demolition**
With a demolition date looming, visitors to the International Peace Garden will get one last chance to pay homage to the Peace Tower this summer. The crumbling monument was scheduled to come down last fall, but the garden's board of directors decided to hold off for one more season. It will be demolished in the fall. "We thought the longer the tower is up, the longer it remains in the minds of the people," board president Charlie Thomsen said. The Peace Tower's four concrete columns straddle the Canada-U.S. border and the structure has become an iconic feature of the grounds. Winnipeg Free Press, A8; Radio-Canada (2016-05-02)

CYBER SECURITY / CYBERSÉCURITÉ

Only one way to keep a secret
Secrets are becoming an endangered species. Maybe privacy, too. The FBI has cracked Apple's iPhone, which even Apple apparently couldn't do. In Canada, the RCMP reportedly has cracked Blackberry's supposedly ultrasecure messaging system. This must have come as a disturbing surprise to the world leaders who use a Blackberry, including U.S. President Barack Obama, British Prime Minister David Cameron and the Dalai Lama, among others. Of course, Canadian authorities would never stoop to reading the secret, encoded Blackberry messages exchanged by friendly world leaders like Cameron or Obama, but they wouldn't be human if they didn't wonder what the Dalai Lama was hiding. Quantum computers now in the works supposedly will be fast and powerful enough to quickly decode even the most elaborate encryption. It is beginning to look like we can't keep secret anymore any kind of digital record. We'll have to go back to whispering our secrets. The risk then is that an important message might be misheard: World leader A: "Psst. I am seriously worried about North Korea." StarPhoenix, A3

LAW ENFORCEMENT / APPLICATION DE LA LOI

Searchers locate body of missing teen
17-year-old Natuashish resident Kirby Mistenapeo found 11 km from home. Following an exhaustive two-week search, the RCMP confirmed a body located Monday afternoon outside Natuashish is that of 17-year-old Kirby Mistenapeo. RCMP said that at 10:30 a.m. they were notified searchers had located human remains on the ice approximately 11 kilometres west of the community, in an area known as Little Sango Bay. Kirby had been missing since April 21. A land and air search for the teen was hampered by inclement weather throughout the time he was missing. Three helicopters and an RCMP Twin Otter plane from Happy Valley-Goose Bay were conducting the extensive air search. The ground search saw search and rescue members from Rigolet and Happy Valley-Goose Bay flown into the community to complement

the search team on the ground. The Innu Nation also sent people from Sheshatshiu to assist with the search efforts. RCMP members from Happy Valley-Goose Bay, Makkovik, the Labrador Relief Team and Hopedale were helping with the search as well. Telegram, A6

*** RCMP changes 'outdated' recruitment process**

The RCMP is changing how it recruits new members after being told that the process was "too long, inflexible and outdated." One of the changes will allow people with permanent resident status, who have lived in Canada for the last 10 years, to apply. Physical abilities will no longer be tested as part of the application process and that evaluation will now be assessed at the RCMP training academy in Regina. Under the new rules, applicants from British Columbia, Alberta, Saskatchewan or Manitoba will also be able to select their home province for their first post after graduation. The force says in a news release that the move will help it stay competitive and build a diverse workforce, but also that standards won't be compromised. The RCMP said it will not do interviews on the changes. "We will not be providing any interviews on the modernization of the recruitment process," Annie Delisle, media relations officer for the RCMP, said in an email to The Canadian Press. "We invite you to submit questions in writing if you need any details from the news release." Times & Transcript, B4 (Leader-Post) (2016-05-03); CBC (2016-05-02)

RCMP seek access to Panama Papers for tax probe

RCMP Commissioner Bob Paulson says the Mounties are "hopeful" they will soon get access to the Panama Papers as part of a criminal investigation into income-tax evasion and money laundering by Canadians with assets in offshore tax havens. Commissioner Paulson would not disclose how the RCMP expect to obtain the 11 million leaked documents known as the Panama Papers, which date back four decades and are allegedly connected to the Panamanian law firm Mossack Fonseca, which specializes in the creation of shell companies in tax havens around the world. "Yes, we are interested in getting our hands on them and what criminality it may represent and what investigations that we should pursue," Commissioner Paulson told reporters after testifying before the Senate committee on national security and defence. "We are obviously interested what those papers and the discussions around those papers - what it means and what criminality may be at play." RCMP Deputy Commissioner Mike Cabana had told senators the RCMP have discussed with "foreign partners" how the force could obtain the documents and said they expected to "see the documents in their entirety." Deputy Commissioner Cabana said the RCMP have not been involved in discussions with the government of Panama.When reporters later asked Commissioner Paulson whether the RCMP were planning to obtain the massive records of shell companies and offshore accounts through either judicial warrant or voluntary disclosure, he was circumspect. Globe and Mail, A4; Toronto Star, A4; * HR Reporter (2016-05-02); La Presse Canadienne (L'Actualité)

Organized crime figure gets 15 years

Piccirilli sentenced for trafficking, conspiracy and firearms charges. A well-connected drug trafficker arrested a decade ago received a 15-year sentence in a case that took many twists and turns before finally reaching its end on Monday. "Good luck to you, Mr. Piccirilli," Quebec Court Judge Marie Suzanne Lauzon told Sergio Piccirilli, 56, after reading her decision at the Laval courthouse. With the time he has served offand on since he was arrested in 2006, Piccirilli was left with a prison term of nine years and nine months. When Piccirilli learned how much time Lauzon calculated as the remainder of his sentence, he appeared to be somewhat in a state of disbelief. He turned his head toward two relatives who were seated in the courtroom and let out a sigh. While it might be the end of the case in Quebec Court, Piccirilli's lawyer, Patrice Duliot, filed an appeal of the decision Lauzon made in January in which she found Piccirilli guilty of 23 charges including conspiracy, issuing orders for the benefit of a criminal organization and trafficking in methamphetamine, cocaine and marijuana. Piccirilli was also found guilty of the illegal possession of a powerful automatic rifle he obtained after learning leaders in the Rizzuto organization placed a contract on his head, in 2005, while he was under investigation by the RCMP. Piccirilli was warned by police back then that they had credible information someone wanted him dead. He and members of a Mafia clan based in Granby were at odds with the Rizzuto organization over who was responsible for how a smuggled shipment of marijuana, worth millions of dollars, arrived in the U.S. spoiled and rotten. While Piccirilli argued with leaders in the Rizzuto organization (he even showed up at their hangout in St-Léonard in 2005 armed with a pistol), he was being investigated in Project

Cleopatra, a Combined Forces Special Enforcement Unit investigation led by the RCMP. Montreal Gazette, A7

ASIRT probes shooting
The province's police watchdog is investigating an RCMP-involved shooting in Red Deer Sunday night in which an armed man was injured. The Alberta Serious Incident Response Team or ASIRT said Mounties received a 911 call after 7 p.m. involving a possibly suicidal armed man at a downtown apartment building. "The man advised police that he had a gun and made statements suggesting he was prepared to use it on himself or anyone who attended," ASIRT said in a statement. When three RCMP officers arrived, they found the man on the second floor and a confrontation ensued, resulting in one of the members discharging his service weapon. RCMP say police opened fire "in their efforts to ensure public safety." The 28-year-old man was shot once and was taken to hospital in stable condition. Postmedia Network (Edmonton Sun, A6, Calgary Sun, Calgary Herald)

Human remains found on farm near Brooks
Members of the Brooks RCMP detachment have launched an investigation after a local rancher made a grisly discovery on his property. On the evening of April 28, officers responded to the farm, located approximately 10 kilometers west of Brooks city limits, after the rancher found human remains while tending to his cattle. The RCMP forensic unit and police dog services processed the scene and members of Medicine Hat search and rescue performed a thorough search of the area. An autopsy conducted by the Medical Examiner's office in Calgary confirmed the remains are human but additional testing is required to determine the age, gender and identity of the deceased. Red Deer Advocate, A10 (2016-05-03); CBC (2016-05-02)

Police shoot out-of-control cow
Animal gets loose at cattle sale, injures spectators, charges RCMP officers. An out-of-control cow that got loose and injured several people at Saturday's cattle sale in Lawrencetown was shot by an RCMP officer after police received a 911 call. The distraught animal was being off-loaded and got loose, said Annapolis District RCMP Staff-Sgt. Dan MacGillivray. Police got the call at 10 a.m. and arrived at the scene only to be charged by the animal at one point. "It was, I guess, stressed out, or was acting erratically," said MacGillivray, adding there was a veterinarian at the exhibition grounds and the owner of the animal was close by. "I guess it hurt a couple of people. It appears like this animal was attacking people - (that was) the information our officers had." MacGillivray said the veterinarian was there with a tranquilizer gun, but may not have been able to get in position to use it. "Our officers were there and were trying to control the public," said MacGillvray. "The animal crossed Highway 1. At one point the animal came towards the police car with its head down. Our officers got out of the way." Telegram, A7 (Cape Breton Post)

Polar bear shot and killed by RCMP in Deep Bay, Fogo Island
Release says bear came ashore, approached officers and bystanders. Fogo Island RCMP shot and killed a polar bear that had wandered into the community of Deep Bay Monday morning. The RCMP said in a news release, around 9:30 a.m., officers responded to a call of a polar bear swimming in the harbour at Deep Bay. RCMP and Fisheries and Oceans officers responded and found the bear coming ashore near the community's wharf. RCMP officers moved bystanders back and fired a warning shot in hope of scaring the bear away, but the animal continued to advance, approaching the officers and bystanders. The news release says "an RCMP officer was required to shoot the bear out of safety concerns for those in the area." While en route to the incident, the RCMP said its officers consulted with a conservation officer from the Forestry and Agrifoods Agency. They remained in contact with the conservation officer, by phone, throughout the incident. Canadian Press (Telegram, A5, Guardian, A5, Times & Transcript, Cape Breton Post); National Post, A2

'He wanted help'
Inquiry hears details of soldier's suicide. An Afghan war veteran committed suicide in an Edmonton military cell block on the same day he was told he was being transferred from his regiment to a holding unit for injured or ill soldiers. Testimony pointing to substandard holding cells, ineffective computers, an uncharged defibrillator and inconsistent supervision abilities was given Monday at the start of a public

inquiry into Cpl. Shaun Collins' suicide on March 9, 2011. "The cell block does not meet any Canadian standards," said Warrant Officer James Dean Boyd, the top officer at the guard house and one of the people who found Collins' body. Boyd described the building as a piecemeal combination of four older buildings and including elements such as barred cell doors that have been since identified as hanging risks. He got drunk He said Collins had gone earlier that day to The Junior Ranks, a military-only bar on the base, and gotten drunk. His transfer, from the Princess Patricia's Canadian Light Infantry regiment to the Joint Personnel Service Unit, landed him in a place soldiers go when they are unable, for reasons including injury or mental health, to operate with their home unit. (…) Seven those at the guard house weren't reliable. After putting in the wrong name to begin with, three separate database searches - Edmonton Police, RCMP and military - showed no history for Collins, despite two previous suicide attempts and a history with depression. Postmedia Network (Edmonton Sun, A4, Calgary Herald, Edmonton Journal)

Police watchdog probes shooting at downtown apartment complex

Alberta's police watchdog is investigating after a 28-year-old man was shot by local RCMP on Sunday. Red Deer RCMP responded to a 911 call of an armed man, possibly suicidal, at the River Valley Apartments (5017-49th Street) around 7: 15 p.m. on Sunday. The man told police he had a gun and suggested he was prepared to use it on himself or others, say police. Three police officers entered the building and found the man on the second floor. A confrontation occurred, which resulted in an officer discharging his weapon. The man sustained a non-life threatening single gunshot wound. He was provided with emergency medical attention and transported to Red Deer Regional Hospital Centre where he was admitted and remains in stable condition. No other injuries were reported. Red Deer Advocate, A1

Transportation Safety Board of Canada looking at P.E.I. death

Board deploying team to investigate workplace death of Troy Jeffery on oyster barge Friday. The Transportation Safety Board of Canada (TSB) announced Monday that it is deploying a team to P.E.I. to investigate the workplace fatality of Troy Jeffery. Jeffery, 46, died as a result of injuries sustained during a workplace accident in Poplar Grove on Friday. He was working on an oyster barge on the water at the time of the accident. The TSB is an independent government agency that investigates safety issues in the marine, pipeline, railway and aviation industries. It often recommends changes to safety procedures as a result of its investigations. Jeffery's death is also being investigated by the East Prince RCMP and the provincial Occupational Health and Safety. Guardian

Pas de délais avant de lancer une enquête

Les policiers prennent tous les cas de fugues avec sérieux, assure la constable Jullie Rogers-Marsh. Elle précise qu'il n'y a pas de temps minimum d'attente requis avant de pouvoir signaler la disparition d'un individu. «Aussitôt qu'il y a une inquiétude sur le bien-être d'une personne et qu'elle est introuvable, vous faites bien de contacter les policiers. Nous sommes là pour ça et nous tenterons de la retrouver.» Le travail d'enquête commence dès la réception de l'appel d'urgence. Les policiers tenteront de recueillir le plus d'information possible sur la personne recherchée. Pour ce faire, ils parleront à des membres de sa famille, à ses amis, à son employeur ou à ses enseignants, afin de déterminer où elle a été vue pour la dernière fois. Chaque cas est différent et demande une approche sur mesure, explique l'agente. Les médias d'information ne sont pas systématiquement sollicités dans ces recherches, précise-t-elle. Lorsque les recherches stagnent, et que la GRC a besoin de l'aide du public, un communiqué de presse est rédigé. «On peut parler directement aux gens et avoir des informations très rapidement. En quelques minutes, nous pouvons avertir des milliers de gens sur la disparition d'une personne. Ça nous aide énormément pour nos recherches.» L'Acadie Nouvelle, 5

Mountie fined for lying

A Coquitlam RCMP officer who admitted lying to the Insurance Corp. of B.C. has been fined $3,000. Const. Fareez Vellani pleaded guilty to one count of providing false information material to a claim, an offence under the Insurance (Vehicle) Act. Sentencing took place Friday in provincial court in Port Coquitlam. In addition to being fined, Vellani was ordered to pay $511.88 restitution and a $459 victim surcharge. The offence took place Feb. 13, 2015, in Maple Ridge. According to an RCMP news release from August 2015, the charge related to damage to Vellani's personal vehicle and his subsequent reporting of that damage to ICBC. Province, A8

RCMP changes 'outdated' recruitment process
The RCMP is changing how it recruits new members after being told that the process was "too long, inflexible and outdated." One of the changes will allow people with permanent resident status, who have lived in Canada for the last 10 years, to apply. Physical abilities will no longer be tested as part of the application process and that evaluation will now be assessed at the RCMP training academy in Regina. Under the new rules, applicants from British Columbia, Alberta, Saskatchewan or Manitoba will also be able to select their home province for their first post after graduation. The force says in a news release that the move will help it stay competitive and build a diverse workforce, but also that standards won't be compromised. The RCMP said it will not do interviews on the changes. "We will not be providing any interviews on the modernization of the recruitment process," Annie Delisle, media relations officer for the RCMP, said in an email. "We invite you to submit questions in writing if you need any details from the news release." Red Deer Advocate, A6

Importation d'alcool
la GRC continue de donner des contraventions. Si vous envisagiez aller au Québec faire le plein d'alcool au cours des prochains jours - du moins pour plus qu'une douzaine de «chopines» - risquez-vous d'avoir une mauvaise surprise à votre retour? Cela dépend à qui vous posez la question. Le coordonnateur de l'opération policière ayant mené, en 2012, à la saisie de l'alcool de Gérard Comeau, le caporal René Labbé de Campbellton confirme qu'à ce moment-ci, le statu quo perdure à la frontière. «On attend des consignes de nos supérieurs, mais au moment où l'on se parle, rien n'a changé. On respecte bien évidemment la décision du juge (Ronald) LeBlanc, mais nous n'avons pas reçu de consigne comme quoi nous n'avions plus à nous préoccuper de l'importation d'alcool. Ainsi, on continue à faire appliquer la loi en vigueur jusqu'à ce que l'on reçoive des indications contraires, que la GRC et le gouvernement prennent position», mentionne le policier. Porte-parole de la GRC au niveau provincial, Jullie Rogers-Marsh confirme que son organisation étudie la question en collaboration avec le Bureau des poursuites pénales, question d'avoir l'heure juste dans ce dossier. «On est en train de réviser la décision et les impacts qu'elle aura sur le travail de nos membres. Nous sommes responsables de faire appliquer les lois, mais ce n'est pas nous qui effectuons les changements», indique-t-elle, renvoyant la balle au gouvernement. L'Acadie Nouvelle, 3; * Times & Transcript, A4 (Daily Gleaner, A1, Telegraph-Journal)

It could be a bloody summer
Gun homicides already up by 200% over last year. Just in case you are keeping score, there has been a 200% increase in shooting murders since this time last year. You read it right - 200%. There's no spin. No politics. You can check the statistics on the Toronto Police website yourself. It will show you that by May 3 in 2015, guns were used to kill victims in six homicides. This year, killers armed with guns have so far claimed 18 lives. That's a dozen more shooting murders in 2016 compared to the same time frame the year before. Overall, murders are way up, too - 100% to be precise. At this time in 2015, Toronto had 14 murders. There have been 28 so far this year. Of those 28, 13 have not yet resulted in arrests. Toronto Sun, A4

*** Fatal overdoses in Kamloops already double what they were in 2015**
Following two more overdose deaths on the weekend, Kamloops Mounties are working on a messaging campaign to inform drug users and dealers of the dangers of fentanyl. It likely won't be known for weeks whether fentanyl was involved in Kamloops' most recent overdose deaths - a 44-year-old man and a 36-year-old woman found dead at a house in Rayleigh on Friday night - but the drug has prompted warnings from police, coroners and community groups in recent months. The weekend deaths bring to at least 13 the number of fatal overdoses in Kamloops so far this year - nearly double the tally for all of 2015. Kamloops saw seven deaths last year from overdoses of illicit drugs, which is on par with the annual average of 7.2 for the city going back to 2007. In 2016, however, the numbers are spiking - especially in the Tournament Capital. According to BC Coroners Service data, Kamloops is the only city in the province to have recorded more overdose deaths in the first three months of 2016 than in all of 2015. The only cities with more recorded overdose deaths than Kamloops so far this year are Vancouver, Surrey and Victoria. Kamloops RCMP Cpl. Jodi Shelkie said the risk to drug users is real. "It's a life or death situation every time you choose to use drugs," she said. "Dealing with drugs in our community is an ongoing priority. It's always first and foremost in our minds, but especially now with all these overdoses

and deaths. "We're working at targeting, identifying and arresting the people who are bringing these drugs into Kamloops." Vancouver Sun

*** Surrey RCMP ask for public help in locating missing man**
Surrey RCMP are asking for the public's help in finding a 61-year-old man who has gone missing. Edward Burns was last seen Monday morning at 6 o'clock, near 123rd Street and 82nd Avenue. Police say they and his family are worried about his well-being, and Burns has a medical condition that affects his mobility. CKNW

*** Cocaine, oxycodone, morphine and cash seized in Gander traffic stop**
Two men have been arrested and charged with multiple offences, after police seized cash and drugs from a vehicle in Gander last week. RCMP stopped the vehicle early in the morning of Thursday, April 28. Police seized 28 ounces of cocaine and a "large quantity" of oxycodone and morphine pills. In addition, officers found more than $15,000 in cash. CBC News

*** RCMP hope new system will reduce response times**
Kelowna RCMP could move toward an expanded zone-based model of policing that changes how officers are deployed, city council heard Monday. A sophisticated computer system is helping police managers better understand the frequency and complexity of calls that come from different areas of the city. Within a year or so of compiling the data, RCMP Supt. Nick Romanchuk said, the detachment could be using an expanded zone-based policing model beyond the one currently in use. That system, he said, amounts to dividing Kelowna into two sections: "Rutland and everywhere else." Expanding the zone system, Romanchuk explained, could have significant operational efficiencies that reduce police response time. By way of example, he said it would ensure an RCMP member who happens to be in McKinley Landing wouldn't be the one expected to also respond to a call in Kettle Valley. Kelowna Daily Courier (2016-05-02)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

His hideous crimes, their unceasing anguish
Another year, another victim impact statement. Linda Bright's sisters have had to prepare so many during the 38 years since she was brutally raped and strangled by a man who's now one of Canada's longest-serving prisoners. (…) And dutifully, they'll go to Quebec next week to talk to a parole board about things too painful to discuss with their own families. It's all in an effort to stop Donald Armstrong's latest attempt to get out of St. Anne de Plain maximum security prison, near Montreal, this time, on escorted day passes. (…) Their efforts are not in vain, said Scott Newark, a former Crown prosecutor in Alberta and victims' advocate who attended parole hearings for one of Canada's most notorious serial killers, Clifford Olson. (…)That said, Newark said the presence of families before the National Parole Board adds an important layer of accountability to parole decisions. (…) Armstrong was sentenced to life with no chance of parole for 25 years. But there was no closure for Bright's family. More than six times since then, they've fought Armstrong's attempts to get out or move to minimum-security facilities. Usually, there is advance notice. Nearly every year, Ashley is contacted by Corrections Canada with an update about Armstrong's next move. She also gets calls about his medical appointments and other updates on his status. Once, she learned Armstrong had been moved from a medium-to minimum-security prison. When Ashley balked at the move and complained, he was moved back. (…) "It's always been about the community. We can't bring our sister back. But what we can do is warn the public, let them know what Corrections Canada is thinking of doing," said Ashley. " "Let them know, he will be someone's neighbour, in someone's neighbourhood," she said. "Everybody's a potential victim." London Free Press, A1

*** End of Lockdown and Search at Bowden Institution - Medium Security Unit**
The lockdown put in place at the medium security unit at Bowden Institution on April 28, 2016 has ended. The institution has resumed its normal operations. Correctional Service Canada (CSC) is strengthening measures to prevent the entry of contraband into its institutions in order to ensure a safe and secure environment for everyone. CSC also works in partnership with the police to take action against those who

attempt to have contraband brought into correctional institutions. Visits to the institution have resumed. Marketwired (2016-05-02)

Parole decision today for killer of Reena Virk
Kelly Ellard, convicted of seconddegree murder in the death of Reena Virk in 1997, is expected to find out today if she will be granted day parole from prison. Ellard, who turned 33 in August, was 15 years old when she smashed Virk's head against a tree and then held Virk's head under water until she stopped moving. Virk was a 14-year-old Grade 9 student when she was killed on Nov. 14, 1997, after she was swarmed by a group of teenagers under the Craigflower Bridge. Eight days later, her body was discovered floating in the Gorge during an aerial search conducted in response to rumours of the assault and killing. (...) Ellard is scheduled to attend her first day-parole hearing today, seven years after the Supreme Court of Canada rejected an appeal of her second-degree murder conviction. She waived her right to a full parole hearing four times while serving her life sentence, but remained eligible for day parole and applied for release several months ago. (...) Should Ellard's request for parole be granted, she would be placed under a release plan that includes a requirement that she live in a halfway house, a parole official said. A release plan usually includes conditions such as abstaining from intoxicants and avoiding criminally active peers. Times Colonist, A1; * Huffington Post

* **Trial begins for man accused of injuring cop**
Much of a trial being heard this week at Regina Court of Queen's Bench is expected to turn on five words: "Police! Show me your hands!" "Those words, ladies and gentlemen, are pivotal to this case," Crown prosecutor Kim Jones told the jury hearing the case this week against Jason John Dunlop. During his opening remarks to the jury, Jones said the entire incident from two years ago in which a Regina Police Service plainclothes member was seriously injured took place in a matter of seconds. During those seconds, the Crown alleges the police officer and his partner were trying to arrest Dunlop on a warrant when Dunlop, driving a stolen truck, drove away, pinning the officer between two vehicles. Dunlop, 35, is standing trial on four charges, all dating from May 14, 2014: Criminal negligence causing bodily harm, dangerous driving causing bodily harm, leaving the scene of an accident in which bodily harm occurred, and evading police. While Jones said there is no suggestion Dunlop deliberately hit the officer, the prosecutor suggested to the jury that Dunlop's actions showed a "wanton and reckless disregard" for the other man's safety. In outlining the case the Crown intends to present, Jones said Dunlop, from Red Deer, was on statutory release or parole and was the subject of a warrant for a breach when he ended up in Regina. Leader-Post, A3

* **Tobby Carrier : la Cour Suprême fera part de ses intentions jeudi**
C'est jeudi que la Cour suprême du Canada indiquera si elle accepte ou non de se pencher sur la cause de Tobby Carrier de Matane. La Couronne s'est adressée au plus haut tribunal du pays pour annuler la décision de la Cour d'appel du Québec ordonnant la tenue d'un nouveau procès pour le jeune homme de 26 ans. Tobby Carrier a été reconnu coupable en février 2013 du meurtre de son frère et de tentative de meurtre sur ses parents. Il purge actuellement une peine de prison à vie sans possibilité de libération conditionnelle avant 2023. TVA Nouvelles (2016-05-02)

* **La marijuana en chiffres**
Inoffensive, la marijuana ? Le débat médical est ouvert, mais le débat judiciaire, lui, est entendu. Près de 60 000 cas de possession sont recensés chaque année par la police. La judiciarisation de ces cas coûterait, selon certaines évaluations, jusqu'à deux milliards de dollars par année. Ce qui fait dire à certains que la légalisation pourrait être payante. (...) Un cas de possession ne signifie pas une incarcération. Les données précises sur le nombre de prisonniers derrière les barreaux pour cause de cannabis n'existent pas, mais on sait que 26 % des quelque 15 000 détenus fédéraux y sont pour des raisons de drogue (toutes sortes confondues). Le Devoir, A4

Ellard should show remorse
An opinion piece states, "Out of horrible tragedies can come heartwarming stories of change and redemption. Such is not the case with Kelly Ellard, who killed 14-yearold Reena Virk in 1997. Ellard is scheduled to attend her first day-parole hearing today, seven years after the Supreme Court of Canada rejected an appeal of her second-degree murder conviction. Parole makes sense when a person has

accepted responsibility for her crime, has shown remorse and has embarked upon a better path. The hearing is a chance for Ellard to show she has done these things. Virk, a troubled girl seeking acceptance, had been beaten by a group of teenagers after being lured to the Craigflower Bridge. She extricated herself from her attackers and tried to make her way across the bridge, but was followed by Ellard, 15 years old at the time, and Warren Glowatski, then 16. They dragged her under the bridge and attacked her again; Glowatski watched as Ellard held Virk's head under water. Her body was found nine days later. (...) When the verdict was rendered, Glowatski showed no remorse, offered no apology. He received an automatic life sentence, with the chance of parole in seven years. In the years following his conviction, Glowatski grew and matured. He fully admitted his role in Virk's death and showed remorse. After being given day parole in 2007, he frequently spoke to students and at-risk youth about avoiding a criminal path. Much of his renewal has come through the help of Suman and Manjit Virk, Reena's parents. They took part in a restorative-justice session with Glowatski in 2006. The Virks heard him take responsibility for his actions, and they forgave him. Their support was critical as he has travelled the difficult road from convicted killer to free man. Ellard's is a different story entirely. Virk's parents have said they want to forgive Ellard, who has never publicly admitted killing their daughter, but they say that process can only begin when they see that Ellard has made improvements in her life." Times Colonist, A10

*** A judicial review**

A letter to the editor states, "Your front-page story, Killer's helper appeals (April 29), left me with mixed feelings. On one hand, Loretta Saunders was a beautiful Inuit Canadian woman and I want her murderer(s) punished to the full extent of the law. However, if Victoria Henneberry is not guilty of second-degree murder, as she claims, then I do not want her in jail or punished too harshly if she is guilty of a lesser offense. Henneberry was never tried in court for her part in the crime because she pleaded guilty to second-degree murder last April. She then missed a 30-day deadline to file an appeal of her conviction, but last July was allowed to file a late application. Nova Scotia Legal Aid denied Henneberry's application for a lawyer to handle the appeal. She now is asking Nova Scotia's highest court to appoint a lawyer to handle her appeal. In her letter to the court, Henneberry says her conviction should be overturned and a new trial ordered because she panicked when entering her plea: "I was distraught, under a great deal of stress and panicked." Her being distraught under those circumstances is understandable, but it's important she has chosen to speak directly to the court and say she is not guilty of second-degree murder." Chronicle-Herald, A7

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Which cop shot me?

The Special Investigations Unit investigator was waiting outside the door to the Brampton courtroom, minutes from taking the stand. With him was the complete investigative file on case #15-OFD-046 - information that, so far, had been treated as a state secret. Suzan Zreik's quest for information and justice had come to this: subpoenaing the lead investigator on her case, via a drastic legal manoeuvre. There was no other way, she felt, to know which Peel police officer shot her (...) Last November, the SIU, the civilian watchdog that investigates police incidents involving serious injury or death, ruled the unnamed officers' conduct was legally justified. No charges would be laid in Ekamba-Boekwa's death or in Zreik's shooting. In the words of SIU director Tony Loparco, Zreik was "in the wrong place at the wrong time through no criminal fault of anyone else." Michael Moon, Zreik's lawyer, disagrees. Toronto Star, A1

Will old SIU reports see light of day?

The retroactive release of all Special Investigations Unit directors' reports - including censored details related to the police-shooting death of Andrew Loku - looms as part of a new review of police oversight, Attorney General Madeleine Meilleur said Monday. Under fire from critics outraged that only nine of 34 pages were made public from the SIU probe of Loku's shooting by Toronto police last July, Meilleur said Monday that more information will be forthcoming. That could include the release of the thousands of secret reports prepared by SIU directors since the civilian watchdog was created in 1990 - including the

138 fatal police shootings the agency has probed. But critics say the release of the reports is meaningless if key information, such as evidence provided by witnesses, is kept secret. In an interview Monday, Meilleur said her ministry has asked Justice Michael Tulloch, the judge appointed to review all Ontario police oversight bodies, to make the release of past and future SIU director's reports among the first issues he tackles. Toronto Star, A1

It could be a bloody summer
Just in case you are keeping score, there has been a 200% increase in shooting murders since this time last year. You read it right - 200%. There's no spin. No politics. You can check the statistics on the Toronto Police website yourself. It will show you that by May 3 in 2015, guns were used to kill victims in six homicides. This year, killers armed with guns have so far claimed 18 lives. That's a dozen more shooting murders in 2016 compared to the same time frame the year before. Overall, murders are way up, too - 100% to be precise. At this time in 2015, Toronto had 14 murders. There have been 28 so far this year. Toronto Sun, A4

Police take proactive tack on gangs
Winnipeg police rolled out an anti-gang campaign in three languages Monday in an effort to deter street-gang recruitment this summer. Pamphlets in English, Arabic and Portuguese call for an end to gang violence. They're part of a campaign that includes posters and a public information evening for parents at the Magnus Elias Recreation Centre, 430 Langside St., from 6 p.m. to 8 p.m tonight. "We, as a police service, are being proactive. We're engaging them, the parents, and often it's a one-parent family, to come out," said Insp. Max Waddell, head of the Winnipeg Police Service organized crime unit. "We can arm them with the information so they can get connected with the appropriate social service agency for after-school programming into the summer," Waddell said at a news conference Monday. Winnipeg Free Press, B2

P.E.I. social workers, police learn new strategies to prevent tragedies
The legacy of Nash Campbell is beginning to take shape, as front-line workers on P.E.I. learn new ways to respond to crises before they turn into tragedy, acting on a key recommendation of a coroner's inquest into the tragic 2013 murder-suicide. The four-year-old boy and his mother, Trish Hennessey, were found dead in a burned-out vehicle after a custody battle. "Many, many service providers were significantly affected by that case," said Michele Dorsey, deputy minister of Justice and Public Safety (...) More than a hundred social service workers — including police officers and school officials — met in Charlottetown today to learn about what`s called collaborative risk-driven intervention, a system now used in more than 50 communities across Canada. CBC News

Violence against women needs to end
An opinion piece states "I hate being a man. I wake up every morning and look at myself in the mirror and see the same weight on my shoulders. The weight of being categorized along with the worst of the world's worst. It's something that, according to statistics, half of the planet and I share along with the likes of Paul Bernardo, Russell Williams, and Bruce Allan Wilson - just to name a few of the monsters. These monsters - rapists and predators of violence against women - are all men. I'm a man. A couple of stories in the news this past week made that weight a little heavier. In the first, an Oklahoma court ruled that forced oral sex is not rape if the victim is unconscious from drinking alcohol. The fact that a court made that judgment is absurd in itself. Judge Robert Hudson - a man - made the ruling. The second story was that 80 people were arrested in a province wide child pornography investigation. Three of the arrested are from Kingston. Of the 80 arrested, 63 names were released, 62 were men. This is why the weight gets heavier as a man. Because men are the monsters. The statistics are staggering." Kingston Whig-Standard, A5

* **Breathalyzer ruling will have ripple effect**
Criminal lawyers across Canada woke up Monday to discover that the infallibility of the instrument at the heart of nearly every impaired driving prosecution was as much a myth as a winged insect secreting loonies under the pillows of gap-toothed children. For decades, expert after expert and case after case have entrenched the view that the breath testing machines operating at police detachments from St. John's to Victoria are highly reliable scientific instruments. Nearly every case involving an allegation of

"over 80" (where the concentration of alcohol in a person's blood is alleged to exceed 80 milligrams of alcohol per 100 milliliters of blood) is proven on the basis of a breath test. Although the Criminal Code speaks of blood-alcohol concentration ("BAC"), the intrusiveness and costs associated with blood testing mean that in practice the vast majority of court cases rely on breath-testing as a proxy to determine BAC. The invincibility and infallibility of the police breath instruments has only become more entrenched as forces across the country upgraded from the older Intoxilyzer 5000C model to the shiny new 8000C. London Free Press; Postmedia (Winnipeg Sun, Toronto Sun, Edmonton Sun, Ottawa Sun)

* **Fatal overdoses in Kamloops already double what they were in 2015**
Following two more overdose deaths on the weekend, Kamloops Mounties are working on a messaging campaign to inform drug users and dealers of the dangers of fentanyl. It likely won't be known for weeks whether fentanyl was involved in Kamloops' most recent overdose deaths — a 44-year-old man and a 36-year-old woman found dead at a house in Rayleigh on Friday night — but the drug has prompted warnings from police, coroners and community groups in recent months. The weekend deaths bring to at least 13 the number of fatal overdoses in Kamloops so far this year — nearly double the tally for all of 2015. Kamloops saw seven deaths last year from overdoses of illicit drugs, which is on par with the annual average of 7.2 for the city going back to 2007. Kamloops This Week (Vancouver Province, Vancouver Sun) (2016-05-02)

* **Amount of synthetic drugs in Saskatoon 'almost unparalleled': Weighill**
We are witnessing an "almost unparalleled" amount of synthetic drugs like fentanyl on the street says Saskatoon's police chief. Clive Weighill told Global News it's the demand for drugs that is driving up the rates for crimes like robbery and burglaries. "We've seen crime increasing through the end of 2014, through 2015, and now 2016 again, and it's not just in Saskatoon," said Weighill. "I just had a meeting with the western Canadian chiefs, and it's happening in Edmonton, Calgary, Regina, Prince Albert, Yorkton ... its mainly attributable to methamphetamine, fentanyl type drugs, synthetic drugs where people are getting highly addicted very quickly, and they need money." Global News (2016-05-02)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Inuit voices 'want to be heard'
First it was one niece, murdered just over a decade ago, and then, within a few months, another, both lives cut short before the age of 31. A few years later, a third niece, age 23, was killed. For Levinia Brown, 69, of Rankin Inlet, Nunavut, the pending inquiry into missing and murdered indigenous women means both bringing up painful memories of lost loved ones, and the chance to speak publicly of the pain and grief common to many families in the North. It's also, she hopes, an opportunity for Inuit voices to be heard. "We need to talk about it, and heal from it. But it's a very difficult subject," she said in an interview. "I'm appreciative that it's being paid attention to. At least people are going to have awareness that this has happened, and let's stop it, because we don't want any more hurting families." As attention grows to the issue of violence against indigenous women and the upcoming inquiry, some Inuit family members are concerned their perspective will be overlooked. Inuit represent a minority - 4 per cent, though fast-growing - of the aboriginal population in Canada. On a per-capita basis, however, the North is home to Canada's highest homicide and family violence rates, which many say require urgent action. In a report on its pre-inquiry consultation to be released Tuesday, Pauktuutit Inuit Women of Canada - a national organization - highlighted a need to ensure Inuit priorities will be addressed. Globe and Mail, A3

Review policing during inquiry
Aboriginal women tend to be "underprotected and overpoliced," making it vital that the behaviour of police be examined in the upcoming inquiry on missing and murdered women, advocates said Monday. Indigenous women are grossly overrepresented in the system and commonly suffer from poverty and abuse, said Kim Pate, executive director of the Canadian Association of Elizabeth Fry Societies. Those who end up behind bars often share similar, vulnerable backgrounds with those who are murdered or go missing, she added. "We know that the rates of violence ... against indigenous

women are particularly high, and they are also more likely to not have had support in addressing that violence." Pate said she hopes the inquiry will untangle the issues that make indigenous women vulnerable to becoming victims, as well as those that might make them more likely to end up in the criminal justice system. "If we end up with recommendations for better supports for women . . .we will end up seeing fewer people in all of those situations in my opinion." Dawn Lavell-Harvard, president of the Native Women's Association of Canada, said many of the crimes linked to aboriginal women are related to desperation and circumstance. Canadian Press (Toronto Star, A6; Charlottetown Guardian, St. John's Telegram, Cape Breton Post, Huffington Post)

Missing Persons Week marked with prayer, song

Though it's a long list, the Provincial Partnership Committee on Missing Persons wants families to know their loved ones are not forgotten. At Saskatchewan's fourth Missing Person's Week event, 122 white-covered chairs adorned with yellow and green ribbons were lined up in a silent tribute to the province's missing people. After the formal presentations, the faces of those people were projected onto a screen - the images ranging from very grainy ones to smiling faces from family photo albums. The event began with a prayer and song by elder Lorraine Yuzicapi of the Standing Buffalo Dakota Nation near Fort Qu'Appelle. She told the crowd she can't help but get emotional when she talks about missing persons. Unfortunately, Yuzicapi, like far too many others, knows what it's like to have a loved one go missing. In July 2005, her granddaughter, Amber Redman, disappeared. Leader-Post, A4

How to cover our indigenous communities

Many of us will someday tell our children about this apparent tipping point in our collective nationhood: when "reconciliation" between indigenous and non-indigenous communities came crashing on to the public radar and the news media and government suddenly grew a conscience. We all want to believe that reconciliation is a process that has begun to unfold. Indeed it has, but only just. Prime Minister Justin Trudeau's recent private visit to Shoal Lake 40 First Nation (which straddles the border between Manitoba and Ontario) is indicative of this change, as was the mainstream media appetite to cover it. But VICE Canada was given exclusive access to the trip in order to generate footage for a series it is producing on indigenous youth in isolated reserve communities. VICE has produced a number of investigative works, including a documentary on the lack of water in many reserve communities, and a provocative piece showcasing the work of volunteers searching for bodies in Winnipeg's Red River. One could argue the online publication has paid its dues. So while the PMO could have handled the exclusivity of this visit with more tact, the outrage shown by traditional corporate media at being excluded suggests we have a long way to go on the road to reconciliation. Ottawa Citizen, A9

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Victoria could allow 'edibles' at cannabis dispensaries

The City of Victoria is considering rules for its illegal cannabis dispensaries that would be more permissive than Vancouver's landmark bylaw, permitting the sale of controversial "edibles" and allowing pot shops to be located closer to schools. Medical marijuana advocates in the provincial capital praised the draft rules for the city's 32 existing dispensaries, which will be voted on by council later this week. The new proposal comes as officials in Vancouver began cracking down on dispensaries, handing out tickets to nearly two dozen shops over the weekend. Victoria is poised to become the second Canadian city to regulate dispensaries, which have proliferated in areas where municipal officials and police departments have taken a hands-off approach. Advocates say Canada now has about 300 dispensaries, which operate outside of Ottawa's mailorder medical marijuana system. The changes at the municipal level are taking place as a federal task force prepares to begin crafting legislation to legalize recreational marijuana, which could happen within two years. Victoria's proposed rules would allow dispensaries to sell edibles and operate 200 metres from schools and other pot shops. In Vancouver, city hall adopted rules that keep the shops 300 metres from such sensitive locations and also banned edibles after concluding baked goods and candies infused with cannabis were too attractive to children. Mayor Lisa Helps said her city's rules are not much looser than Vancouver's, despite recommending a business licensing fee of about $5,000 for successful applicants, compared with the $30,000 that for-profit shops in Vancouver must pay. Under provincial law, she said her city can only charge enough to recover the costs

of regulation, while Vancouver has the ability to "charge whatever the heck they want" under its own special charter. CBC

*** Pot shop rules to be discussed by Victoria city council Thursday**
The federal Liberals have said they'll have legislation ready in a year to legalize marijuana in Canada. But some Victoria's city politicians don't want to wait. Councillors will discuss potential regulations on the city's rapidly growing number of pot shops Thursday. Many of the potential bylaws they'll consider will look familiar to anyone who's followed Vancouver's drive to regulate its dispensaries. But not all. "We really have the optimal positioning of being able to watch them and, frankly, learn from some of their mistakes," said Councillor Jeremy Loveday, referring to Vancouver city council, speaking on CBC's All Points West. Loveday has a lengthy wish list for Victoria. He wants to ensure video surveillance is mandatory in all dispensaries, that they're not permitted to advertise to minors, that pot shops follow existing noise and smell bylaws, and that there is a minimum distance of 200 metres between each dispensary, and between dispensaries and schools. CBC News

*** Vancouver bylaws close 22 pot shops, but many owners vow to fight rules**
Vancouver's crackdown on unlicensed medical marijuana dispensaries has begun, with bylaw inspectors issuing 44 tickets to date and confirming that 22 stores have already closed. Vancouver's crackdown on unlicensed medical marijuana dispensaries has begun, with bylaw inspectors issuing 44 tickets to date and confirming that 22 stores have already closed. But many owners are refusing to shut their doors and are mulling legal action, while others are refocusing their business efforts on cities without regulations including Toronto. "It's absurd that these businesses that have laid the groundwork for access and legalization are being punished and shut down when they do no harm," said cannabis activist Jodie Emery. "A lot of Vancouver dispensary owners in the last year have set up plans to move to other jurisdictions like Toronto because the regulations here are too restrictive." Sudbury.com; CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

Nil

OTHER / AUTRE

Canada to join anti-torture protocol after years of delay
Canada is prepared to join a key United Nations anti-torture agreement more than a decade after it was first passed. The UN's optional protocol to the convention against torture allows for the establishment of national and international systems for inspecting detention centres where torture often takes place in secrecy. It was first approved by the world body in 2002. Although dozens of countries have signed on, Canada has not ratified the protocol. The Harper government twice promised to do so, but never did. The new Trudeau government will follow through, says Chantal Gagnon, a spokesperson for Foreign Affairs Minister Stephane Dion. "The minister just announced that we agree that the government of Canada should join this important protocol," Gagnon said of what Dion had to say at a private reception earlier Monday. "We are taking the first step towards doing so by beginning formal consultations on the optional protocol with provincial and territorial governments." Mohamed Fahmy, who spent more than a year in a prison in Egypt, welcomed the move on Twitter, calling it history in the making. Activist groups have been pressing for ratification for years Amnesty International Canada retweeted Dion's announcement and has a news conference on the subject scheduled for Tuesday. Supporters of the protocol say it is an important step in freeing the world from the practice of torture. They say Canadian ratification would strengthen the country's ability to press other countries to open detention centres to increased scrutiny. Canadian Press (Toronto Star, A4, Red Deer Advocate, Toronto Sun)

Visit at your own peril
Two Europeans kidnapped in Mindanao in 2012 and taken to Jolo Island to be ransomed were birdwatchers visiting the southern Philippines because they hoped to add a sighting of the rare Sulu hornbill to their life lists. One escaped two years later after a knife fight with his captors; the other is still

missing. Their abductors were the same terrorist gang that last week executed Calgarian John Ridsdel. The Abu Sayyaf group, its allegiance pledged to the Islamic State of Iraq and the Levant, relies on tourist ransoms for much of its funding Despite this Islamist insurgency, which has raged for decades in the country's south, the government tourist office's slogan - "It's more fun in the Philippines" - seems to be working: the number of visitors is up about 20 per cent so far this year. The Philippines has one of the fastest-growing economies in Asia. Most of the country is safe; parts of the south definitely are not. Abu Sayyaf is still holding 11 foreigners in Sulu province, including British Columbian Robert Hall, who was abducted with Ridsdel. Ten Indonesian sailors were released Sunday, with Indonesian and Filipino media reporting the sailors' employer had paid a total of US$1 million to buy their freedom. The Philippine tourist office's website makes no mention of the potential risks for tourists travelling to Sulu. Rather, it describes the province's 400 hundred islands as a "glorious" places of "fabulous beauty" that "nurtures a harmonious coexistence of the two most dominant religions, Catholicism and Islam." National Post, A1

Kurdish battle with Iraqi forces raises questions about military training
Canadian-supported Kurdish fighters fought in a bloody battle with forces allied with Iraq's government, even as the Trudeau government kicked offa new public relations campaign to boost public support for its mission in that volatile country. As defence chief Gen. Jon Vance was in Erbil last week reassuring journalists that Canada's mission to Iraq was designed to strengthen the country, Kurdish troops supported and trained by coalition forces had just finished fighting a Shiite militia aligned with Iraq's government. Ten people were killed in the battle, raising questions about Canadian and coalition training of the Kurds and what will come in the aftermath of the eventual defeat of Islamic extremists in Iraq.
More Canadian special forces are being assigned this summer to train the Kurds in northern Iraq and the Liberal government is sending tens of millions of dollars of aid, equipment, and eventually weapons, to the Kurds. The Kurds have used their training to battle the extremists from the Islamic State of Iraq and the Levant (ISIL) but also have as their ultimate goal the establishment of their own independent state.
In a public relations push, shepherded by Vance and in close cooperation with Prime Minister Justin Trudeau's office, the military is promoting what it is calling a successful training mission by the Canadian Special Operations Regiment from Petawawa, Ont. That mission is to strengthen Iraq, military commanders say. Ottawa Citizen (Kingston Whig-Standard, B1, London Free Press, Vancouver Sun, Calgary Herald)

INTERNATIONAL

*** Pakistan fourth most dangerous country for journalists**
According, to the annual report by Freedom Network, titled, Growing Sounds of Silence – The Year of Censorship, in the year 2014, 14 journalists were killed. But, it is the year 2015 that has really proved to be the year of gags and curbs on free speech. Pakistan has been ranked the fourth most dangerous country in the world for journalists, with a total of 115 killings since 1990, according to a report issued by International Federation of Journalists (IFJ). Pakistan is rated “Not Free” in the Freedom of the Press Index 2016, and is ranked 147th out of 195 countries and territories worldwide. According to the Report, journalists in Pakistan experience official attempts to restrict critical reporting, as well as high levels of violence from both State and non-State actors. The Constitution and certain legislations authorize the government to curb freedom of speech on subjects that include the Constitution itself, the armed forces, the Judiciary, and religion. Harsh blasphemy laws have occasionally been used to suppress the media. The News

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
May 12, 2016 / le 12 mai 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Fort McMurray Fires:

To money for thousands of evacuees
Crews are working around the clock to restore power and natural gas to Fort McMurray, Alta., but the chief operating officer of the utility that serves the area says it's impossible to say how soon residents will be able to go home. It's slow and dangerous work. (…) In Ottawa, Liberals are putting all hands on deck with a special cabinet committee to co-ordinate Fort McMurray aid and reconstruction efforts in advance of the prime minister's visit Friday. Justin Trudeau has received an appeal from Notley for enhanced employment insurance benefits for the Edmonton area as a consequence of last week's mass evacuation of more than 80,000 people. But that's just one thread of a multi-government effort that's expected to go on for months or years. Nine different ministries are involved in the federal ad hoc committee, which will be chaired by Calgary MP Kent Hehr, who serves as veterans affairs minister and associate minister of defence. **Public Safety Minister Ralph Goodale** said this week that a dozen federal departments and agencies are involved in the Fort McMurray response. The Red Cross announced that it would distribute $50 million in donations directly to evacuees within the next 48 hours, while the Alberta government is

setting up a debit card system for registered evacuees. The federal Disaster Financial Assistance Arrangements - a 46-year-old program that uses a formula to provide funds to provinces in the case of major natural disasters - will automatically kick in to cover uninsured losses. Canadian Press (Toronto Star, A9, Calgary Herald, Calgary Sun, Waterloo Region Record, Hamilton Spectator, Red Deer Advocate, CBC News); Huffington Post (2016-05-11)

*** Alberta premier says oil city saved from worst of wildfire**
At least two neighborhoods in this oil sands city were scenes of utter devastation with incinerated homes leveled to the ground from a wildfire that Fort McMurray's fire chief called a "beast ... a fire like I've never seen in my life." But the wider picture was more optimistic as Fire Chief Darby Allen said 85 percent of Canada's main oil sands city remains intact, including the downtown district. Alberta's premier declared the city had been saved, adding that officials hope to provide a schedule within two weeks for thousands of evacuated residents to begin returning to their homes. (...) ***"We are now turning our minds more and more to the recovery effort,"*** **Federal Public Safety Minister Ralph Goodale** said. ***"This is going to be a long term endeavor because at the moment there is no power and gas, no palatable water supply. There's dangerous hazardous material all over the place. It's going to take a very careful, thoughtful effort to get that community back in a livable condition,"*** **Goodale** said. Seattle PI

*** Hunk Justin Trudeau Turns Down Russia's Offer To Help**
Trudeau expressed gratitude towards Russia's offer to dispatch water bombers and fire fighting specialists to battle the growing flames, but said he did not need international help. In addition to help coming from different provinces across the country, Trudeau has said that international help will not be required. He added that it is "touching" to see the global community coming together to help and offer support to those affected by the catastrophe. As reported by Global News, countries including the U.S., Russia, Mexico, Australia, Taiwan, Israel and the Palestinian Authority have offered help. (...) Meanwhile, **Public Safety Minister Ralph Goodale** emphasized the need of a break in the weather. ***"The decision was made by the firefighters in the emergency management system that (foreign help) wasn't necessary because of the nature of this blaze,"*** **Goodale** said. ***"This beast is so big the only thing that will fix it is rain."*** Morning News USA

Other:

*** Two-tier pardons fees examined as part of Trudeau government review**
People convicted of minor offences would pay less than those guilty of serious crimes when applying for a pardon under a scenario being studied by the federal parole board. The Parole Board of Canada quietly launched an online consultation this week asking people what they think of the $631 application charge for a criminal pardon - a fee that quadrupled under the previous Conservative government. The consultation, which runs until June 6, is part of a sweeping Liberal review of Harper government changes that made people wait longer and pay more to obtain a pardon, which was renamed a record suspension. (...) The office of **Public Safety Minister Ralph Goodale** says the government will review the waiting period, fee and new name with a view to considering fairness, proportionality and the role that expunging a criminal record plays in rehabilitation. ***"The goal of the corrections system is for offenders to become contributing members of society after their release to make our communities safer,"*** said Scott Bardsley, a spokesman for **Goodale**. ***"Inaccessible pardons cause a major barrier to good employment as many positions require criminal record checks."*** Canadian Press (CTV News, News 1130, CP24)

*** Canada joins alliance to crack down on corruption**
Canada is joining the United States, Britain and three other countries in setting up the International Anti-Corruption Coordination Centre to crack down on global corruption and recover looted assets. The centre, to be based in London, will work with Interpol and law enforcement agencies from around the world. Australia, New Zealand and Switzerland are also helping co-found the organization. It will "provide international co-ordination and support to help law enforcement agencies and prosecutors work together across borders to investigate and punish corrupt elites and recover stolen assets," according to an announcement Thursday by British Prime Minister David Cameron. The announcement came at the start of an anti-corruption summit in London. The conference is being attended by about a dozen Prime

Ministers and Presidents from around the world including Nigerian President Muhammadu Buhari and Afghan President Ashraf Ghani, two countries Mr. Cameron recently described as "fantastically corrupt". The heads of the World Bank, International Monetary Fund and senior members of the International Olympic Committee are also taking part. **Public Safety Minister Ralph Goodale** is representing Canada. Globe and Mail

Politics this morning: Liberals make string of platform promise announcements
Democratic Institutions Minister Maryam Monsef announced yesterday that the Liberals are moving ahead with electoral reform, and are forming an all-party committee that explores possible replacements for the electoral system. However, a majority of the seats on the committee will be Liberal, causing opposition to voice concerns that whatever option the Liberals want will be passed through. The government made a promise in the lead-up to the 2015 election that it would replace the current first-past-the-post system by introducing new legislation within 18 months of taking power. Meanwhile, the Conservatives are still pushing for a national referendum, which the Liberals have maintained they will not call for. Aside from electoral reform, the Liberal government went on an announcement spree yesterday, naming a list of platform promises that they are moving forward with, including a press release from **Public Safety Minister Ralph Goodale** stating that a Canada-US Redress Working Group has been created to rectify issues faced by those whose names have been wrongfully added to the no-fly list. The President of the Treasury Board, Scott Brison, also sent out a press release stating that he would make an announcement this morning at 9:30 regarding government of Canada-related advertising and communications. The Liberal government pledged to make government advertising non-partisan, and appoint an Advertising Commissioner to help the Auditor General oversee government advertising. Hill Times

*** Anti-Semitic French Comic Can't Enter Canada, But He Has a Plan to Do His Montreal Shows Anyway**
The organizers of several sold-out shows for the notorious comic who has faced a litany of hate speech convictions are implementing "plan B" after he was denied entry into Canada earlier this week. Dieudonné M'bala M'bala, known better as just Dieudonné, was supposed to kick off a 10-show series at a small downtown art gallery on Wednesday, followed by two more in Quebec City and one in Trois-Rivières. "There's a little setback, I have to do a round-trip but I'll be coming back ... I'll be in Montreal tonight,"Dieudonné posted in French on his Facebook page, before being forced to get on a flight back to France. His brief stay in Canada occurred the same day he was convicted of hate speech in France, given a two-month suspended jail sentenced, and ordered to pay a €10,000 fine for anti-Semitic speech in a show, according to French media reports. (...) Meanwhile, speaking in the House of Commons on Tuesday, Conservative immigration critic Michelle Rempel asked if the government had used "its power to prevent this man from entering Canada. "Dieudonné M'Bala M'Bala has been convicted many times for hate speech, slander, and glorifying terrorism. This evening, he is supposed to put on a so-called comedy show in Montreal," she said. "Did the government use its power to prevent this man from entering Canada?" **Minister of Public Safety Ralph Goodale** wouldn't answer, saying simply that border guards ***"take all relevant factors into account, including the existence of a criminal record."*** Vice News (2016-05-11)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Fire

*** Comité ministériel spécial sur les incendies de forêt en Alberta**
Ottawa a mis sur pied un comité spécial de neuf ministres afin de gérer les lendemains des incendies qui ont ravagé le nord de l'Alberta et détruit une partie de la ville de Fort McMurray. C'est le ministre des Anciens Combattants, Kent Hehr, qui présidera le Comité spécial sur les feux de forêt du nord de l'Alberta, regroupant notamment les ministres responsables de la Sécurité publique, de la Santé, des Ressources naturelles, de l'Infrastructure, de l'Assurance-emploi et du Développement social. Le comité spécial tiendra sa première rencontre jeudi. La Croix-Rouge a par ailleurs annoncé mercredi qu'elle

fournirait immédiatement 50 millions de dollars aux milliers de personnes forcées de fuir Fort McMurray. Presse canadienne (Le Devoir; Le Droit)

*** Care must be taken in restoring utilities to Fort McMurray**
Crews are working around the clock to restore power and natural gas to the fire-ravaged city of Fort McMurray, but the chief operating officer of the utility that serves the area says it's impossible to say how soon residents will be able to go home. It's slow and dangerous work. "If you can imagine a charred power line pole that we don't want to take out of service, but we want to reinforce - it's something we obviously want to do with great care," ATCO COO Siegfried Kiefer said Wednesday following the company's annual meeting. "Both of the products we deal with are invisible and both can kill you." More than 80,000 people were forced to flee when a ravenous wildfire attacked several neighbourhoods in the northern Alberta city last week. Red Deer Advocate, A6

*** Workers prep for oilsands return - Oil operations prep for production**
Workers for one of the largest oilsands companies affected by the wildfire that devastated Fort McMurray, Alta., will begin returning to the shuttered facilities on Thursday, a union official said on Wednesday, offering the latest indication that the key petroleum production area was slowly coming back online. Meanwhile, the Alberta Premier Rachel Notley and the head of the Canadian Red Cross announced that residents of Fort McMurray would be offered direct financial aid. Ken Smith, President of Unifor Local 707, a union that represents 3,400 Suncor Energy workers, said the company was starting to fly employees back to its oilsands base plant from Thursday. "It will take a few days to get the plant up and in condition to start handling feed. The mine can get going as soon as the trucks and shovels are ready, but it will take the plant a bit longer to become functional," Smith said. "There are a lot of different units that run to make everything happen up there; it's a very complex work site." Smith said they would be flown to Suncor's Firebag site, about 120 km north of Fort McMurray, and transported by bus to the base plant. Suncor Chief Executive Steve Williams had said a day earlier that none of the company's facilities in the area, which have a production capacity of about 350,000 barrels per day (bpd), had been damaged, and he expected to be able to restart production soon. Reuters (Whig-Standard, B1)

*** Suncor couldn't say it trusted the province's Fort McMurray fire analysts**
Suncor Energy has confirmed it used its own analysts to predict the path of wildfires near its facilities in Fort McMurray, and one source told Metro on background that it did so because it thought the government's fire modelling and predictions were potentially flawed. As wildfires encroached on the city, both the government and Suncor had fire prediction specialists that traced the path of the quickly spreading inferno. Sneh Seetal, spokeswoman for Suncor Energy, couldn't say Suncor trusted the judgement of government analysts. "It's not really a yes or no type answer — I think it's too simplistic and doesn't look at the complexity of the unprecedented situation," Seetal said. Metro News

*** Alberta fires likely won't devastate national economy**
A quick restart of Canadian oil sands production will probably spare the country's economy any significant damage from wildfires that ripped through Alberta this month. Fires that knocked an estimated one million barrels a day offline over the past week will trim 2016 growth by around one-tenth of a percentage point, according to the median forecast in a Bloomberg survey of 10 economists. They see the economy expanding 1.6 per cent this year... There are still risks that production restarts could be slowed by pipeline and power generation outages, shortages of diluent and even problems finding staff. Canadian natural gas producers are also suffering, given oilsands operations are major customers. Another unknown is how the destruction spreads through the economy and affects areas such as consumer spending. "It's a huge shock to Fort McMurray, a sizable shock to Alberta and for an economy of C$2 trillion, in terms of the economic impact, it's a modest hit," said Craig Wright, chief economist at Royal Bank of Canada. The key is "when does it come back on?" Bloomberg (Vancouver Sun, D4)

*** Forestry firms assess the damage- Economic hit will hinge on how wildfires moved through the timber**
The multibillion dollar oilsands facilities around Fort McMurray weren't the only large industrial operations at risk when wildfires tore through the region over the past week. Alberta's $4 billion forest products industry also felt the heat, quite literally. Two industry players in particular - Fort McMurray-based

Northland Forest Products, a big sawmill operator, and Boylebased Alberta-Pacific Forest Industries, one of Canada's top pulp producers - suffered unspecified losses to timberlands that will take months to quantify. Company officials with both firms say they'll start assessing the extent of the fire damage in coming weeks, once smoke from the blaze, which now covers an estimated 220,000 hectares, starts to clear. "As far as we know our homes are OK, but we haven't had any information since Thursday or Friday so we really don't know what's going on," says Howard Ewashko, who co-owns Northland with his brother Craig and also lives on the same street in Fort McMurray. "Right now we're just trying to get our servers online and we're chatting to our customers and our contractors, and assuring them that we're still around. As soon as we can we'll start shipping wood and start harvesting this winter again." The good news? Northland's sawmill north of Fort McMurray, which pumps out about 300,000 board feet of lumber annually, was untouched by the blaze. The company's co-owners remained on site throughout the evacuation. Meanwhile, Alberta-Pacific's huge pulp mill, which is located far to the southwest of the fire's path, was never threatened by the blaze. But Alberta-Pacific's massive Forest Management Agreement (FMA) - which gives it authority over 6.4 million hectares of forested land, or an area nearly 30 times larger than the fire zone itself - was affected. Edmonton Journal, B8

*** 22 pompiers néo-brunswickois en renfort en Alberta**

Une équipe de 22 pompiers a quitté le N.-B. mercredi pour aller combattre les feux de forêt qui ravagent l'Alberta. Andy Soucy, garde forestier basé à Edmundston, s'apprête à passer 14 jours sur la ligne de feu. Il fait partie du groupe de pompiers venus des quatre coins du Nouveau-Brunswick, mobilisés par le ministère des Ressources naturelles pour prêter main-forte. A leur arrivée à Edmonton, ils seront informés de la situation sur place puis envoyés dans l'une des régions touchées. «On va nous donner un plan d'action avant de partir pour Fort McMurray ou ailleurs. On ne va pas aller au coeur du foyer. On va être en action à des endroits stratégiques sur les flancs du feu et orienter l'incendie vers une direction moins dangereuse pour les gens», explique-t-il avant de prendre l'avion. Acadie Nouvelle, 5; Telegraph-Journal

*** Eyes inside the evacuation zone**

As the fires raged, when most everyone else was leaving Fort McMurray, Lou Callan stayed put. Along with a small contingent of residents of the northern Alberta town who refused to leave - or sneaked back in - Mr. Callan stayed in the city for more than three days after the mandatory-evacuation order was issued, when most of an estimated 2,400 houses and buildings burned. The 51-year-old spent his time driving around, trying to avoid the RCMP and doing tasks and chores for people who wanted to be there, but couldn't. His photos and video of the cityscape in the days after the evacuation gave thousands of people an early glimpse of whether their homes were still standing or not. "I was just helping. That's all," he said in an interview from Lamont, Alta., where he and his wife are now staying at a hotel. An eight-minute video he posted from a drive around the town on Thursday last week has garnered more than 74,000 views. In the video, Mr. Callan, with a friend, point out which neighbourhoods and streets are still standing, and which are in better shape than they expected - punctuated by colourful commentary as they travel the empty streets. Globe and Mail, A11

*** 'Speed matters' - Red Cross provides Fort McMurray evacuees with $50M immediately**

The Red Cross is providing an immediate payment of $50 million to evacuees of the Fort McMurray forest fire to add to emergency funds the Alberta government is providing. CEO Conrad Sauve says each adult is to receive $600 and each child will get $300. The money is to be electronically transferred within the next two days. "This is the most important cash transfer we have done in our history and the fastest one,' he said Wednesday at a news conference with Alberta Premier Rachel Notley. "(It's) a combination of both the ability to raise money very fast in Canada and also use electronic means to transfer money directly into the hands of those affected." Everyone has unique needs and giving evacuees cash lets them decide how best to spend the money, Sauve said. "We know already that the damage resulting from the wildfire will be in the billions and it will take years to recover. But we also know that the needs of those affected are immediate." Sauve said $67 million has been donated to the Red Cross so far and much of that will be matched by the provincial and federal governments. Notley reminded people that the Alberta government is also providing immediate monetary assistance. Debit cards are being handed out at evacuee centres and other locations across the province. Canadian Press (St. John's Telegram, B10; Chronicle-Herald)

* **Fort McMurray evacuees on frustrating path to safely return home**
Frustration is mounting among some displaced Fort McMurray residents who are becoming increasingly anxious to get home after last week's wildfires but still have no idea when – or how – that will take place. In her daily media briefing on Wednesday, Premier Rachel Notley reiterated plans to have more information for evacuees in the next two weeks, but stressed that it's not yet safe for people to return to the northern Alberta community. She said the re-entry of residents isn't based on a specific timeline, but on meeting certain criteria to ensure the safety and security of residents. "We are very, very aware of the stress and the anxiety that many evacuees are feeling …," she said. "And we understand, of course, the desire to get back home." Globe and Mail

* **Fort McMurray evacuees in Lac La Biche moved to longer-term housing in Bonnyville - Bus loads of evacuees staying in Lac La Biche are expected to arrive in Bonnyville Wednesday evening**
Some Fort McMurray residents staying at an evacuation centre in Lac La Biche are on the move again, travelling to Bonnyville Wednesday night for longer-term housing. The town of Bonnyville started out as a check-in centre for some of the 80,000 people who fled the wildfires last week. The province has since designated the town of 7,000 people as an official reception centre, offering financial assistance to house evacuees during the upcoming weeks before anyone is allowed back into Fort McMurray. Bonnyville has room for around 300 evacuees, in hotels and work camps, said Chris Cambridge, chief administration officer for the Municipal District of Bonnyville. CBC News

* **Wood Buffalo municipal council meets for first time since fire**
Members of Wood Buffalo's municipal council spent their first meeting since Fort McMurray's evacuation mapping out its role in the recovery effort. All of council was present in the River Valley Room of Edmonton City Hall, the new official meeting place for the coming weeks of government in exile. At issue was how the fire would impact projects, programs and services in the municipality and what role the province would play. Worry about providing a stable, happy community quickly enough for the evacuees was evident during the meeting... Repeated questions by Coun. Lance Bussieres and Coun. Allan Vinni about the province's authority in the rebuilding process and in approving re-entry prompted Larivee to stress the province was looking to help the municipality, not take over. "Sometimes we think we built Fort McMurray in spite of the province," not by working with it, Vinni said. Larivee assured council she respected municipal autonomy, and that didn't change because of the emergency. "What you will be responsible for is the rebuilding of your community when you get there," she said. Shane Schreiber, managing director of Alberta Emergency Management Agency, said the province's powers during the state of emergency were laid out in section 19 of the Emergency Management Act. Edmonton Sun, A7; Calgary Herald

* **How other provinces are offering to help displaced Fort McMurray residents**
Hundreds of people lined up at centres across Alberta Wednesday to get their share of emergency funds being offered to residents of Fort McMurray displaced by the wildfire. People can also apply for Alberta Works, which provides an emergency allowance for things like food, accommodation, replacement clothes and utility bills; but to qualify, you must be in the province of Alberta. So what about those who have sought refuge in other provinces? Fort McMurray has a large population hailing from Newfoundland and Labrador. Spokesman John Tompkins said the Department of Advanced Education and Skills will assist evacuees in that province. "People affected by the wildfires in Alberta who have relocated to Newfoundland and Labrador are encouraged to avail of provincial supports and services, including income support and emergency assistance," he said. In Ontario, a government spokeswoman said people who qualify can get help through Ontario Works Emergency Assistance. Global News

* **Fort McMurray wildfire: Ontario provides $500K to Canadian Red Cross for relief**
The Ontario government is contributing half a million dollars to wildfire relief in Alberta. Premier Kathleen Wynne said in a statement Wednesday that the $500,000 will go to the Canadian Red Cross to help its relief efforts for people displaced by the Fort McMurray forest fire. Ontario has committed to sending up to 119 firefighters and supervisory staff, and 82 of them are currently on the ground in Alberta. "Ontario's fire program is recognized around the world for its ability to respond to risks related to public safety. We will

continue to provide the appropriate personnel and support to the people of Alberta throughout this disaster," Bill Mauro, the province's Minister of Natural Resources and Forestry, said in a statement. CBC News

*** Fort McMurray evacuees line up outside Butterdome for debit cards**
Thousands of evacuees from Fort McMurray lined up outside Edmonton's Butterdome on Wednesday to receive government-issued emergency relief debit cards. The province and the Red Cross announced earlier in the day that electronic transfers and pre-loaded debit cards would be given to those impacted by the wildfire. CBC News; Edmonton Sun; Calgary Sun

*** Harrowing tales from Fort McMurray evacuees - Insurance team hearing stories as it assesses damage**
One family told of driving through neighbours' backyards in a desperate bid to flee their burning city. Others spoke about being separated from loved ones as they escaped the wildfires in Fort McMurray, and of the agonizing wait before being reunited. "The stories are very moving," said Trevor Brick, western regional claims manager for Waterloo-based Economical Insurance. "These are people coming up who have potentially lost everything." Brick and about 20 colleagues are present at three evacuation centres in Edmonton, Calgary and Lac La Biche, about halfway between Fort McMurray and Edmonton. Call centres in Edmonton, Calgary, Vancouver and Mississauga are also fielding questions and claims. In Alberta, Economical staff are providing claims support and much-needed emergency funds to policyholders forced to flee their homes and businesses. But they're also there to listen to their clients' harrowing tales. "For myself, I find it's a very humbling experience," said Brick, who's worked in Alberta for nine years. Economical has already distributed $1 million in emergency funds to affected policyholders, said vice-president of claims Rocco Neglia, who arrived in Alberta Tuesday morning. Waterloo Region Record, A1

***Disaster app could aid in wildfire recovery**
A made-in-B.C. damage assessment tool is being offered to the government of Alberta as it struggles with the damage caused by a wildfire in Fort McMurray. The smartphone-based app allows field workers to send damage assessments and photos to a central command centre in seconds, a process that used to take hours, if not days. "Reporting from the field gives us real-time data," said Steven Bibby, manager of security and emergency services at B.C. Housing, the lead agency for building damage assessment in the province. "It can tell us how many evacuees might be able to return home right away or how many don't have a home to return to, unfortunately. That gives you the opportunity to line up all the additional supports that people need, everything from psycho-social assistance to cleaning kits and financial help." The public safety division of Alberta Municipal Affairs is in the "planning stages" for deployment of the system, says chief fire administrator Kevan Jess. As disasters unfold, field workers are typically dispatched to collect information on long paper forms and to take pictures, which they return for data entry at government command centres. From data collection, travel, data entry and mapping, the process can take up to 24 hours. Vancouver Province, A17

*** Wildfire's climate impact**
In the fight against climate change, forests play a critical role - drawing more greenhouse gases out the atmosphere than they emit. But when they burn, much of those stored gases are released back into the atmosphere. So far, the fires in Fort McMurray have released the equivalent of roughly five per cent of Canada's annual greenhouse gas emissions from all other sectors, said Werner Kurz, a senior research scientist with the Canadian Forest Service in charge of Canada's National Forest Carbon Accounting System. The average emissions from forest fires in the boreal plains, where the northern Alberta fires are occurring, are about 170 tonnes of carbon dioxide equivalents per hectare, Kurz said. Multiply that by 239,390 hectares, the size of the Fort McMurray fire on May 11, and the fire has already released about 41 megatonnes of CO2 equivalents in the form of carbon dioxide, methane, and nitrous oxide. Edmonton Sun, A9

*** Will Alberta fires tip the pipeline debate?**
An opinion piece states "After a week of debate over the link, or lack thereof, between climate change and the Fort McMurray wildfires, another reality emerges. When the economic cost of this tragedy is tallied, Justin Trudeau's Liberal government is going to be under renewed pressure to approve a pipeline

and get oil to market from a province staggering under the weight of historic economic troubles. Oil production in Alberta is down a million barrels a day - this in a province already coping with jobless rates unseen in 20 years, which bled 21,000 jobs last month before the fires, and now must cope with oilpatch shutdowns and international investor nervousness. Beyond Alberta, the fires are going to have a huge impact on the Canadian economy. Instead of a tipping point on the climate change debate - which has been tepid and inconclusive in the face of such suffering - it could be an economic tipping point on the pipeline debate. Just days before the inferno, Alberta Premier Rachel Notley had made what she called her best case for approval of pipelines to Trudeau and his cabinet meeting in Alberta. She used statistics to stress the importance of Alberta to the national economy and she reminded the cabinet, in detail, of measures she is taking to reduce the province's carbon footprint. Tuesday, she was announcing that the oil industry will move as quickly as possible to getting the sector back to work, 'rolling up their sleeves' and doing what they love. It's a small step toward rebuilding the provincial economy and helping the Canadian economy. It was left to her unlikely allies in the House of Commons, the Conservatives, to pivot and push on the pipeline question. But Trudeau gave no quarter. 'The only way to build pipelines in the 21st century is to demonstrate the community's support, the partnerships with indigenous peoples, and the strong science that is going to demonstrate that we understand that environmental protection and economic development go hand in hand,' Trudeau said." Toronto Star (Red Deer Advocate)

Other

*** B.C. snowpack reaches record low for May - Average snow levels around the province are 53% of normal, the lowest for May in 36 years**

Snow in B.C. has melted early and quickly this spring, leaving a record-low amount of snowpack on B.C. mountains for May. Many regions have snow levels less than half of normal for this time of year, according to the latest bulletin from the River Forecast Centre, released this week. The provincial average is 53 per cent of normal — the lowest level since 1980 when record-keeping began... While the low snowpack is record-breaking, it is still difficult to forecast what kind of drought conditions B.C. might be in for this summer, Gardner said. May and June are historically rainier months in the B.C. Interior, so normal or high rainfall there could still make for a typical summer, he said. "If it stays dry ... things are sort of setting up for what could be a potential for drought this summer." A new drought information portal from the B.C. government will provide updated information on streamflow and drought levels around the province this year. CBC News

*** Manitoba fires still growing - Weather changes made little impact on the state of Caddy Lake forest fires**

Cooler temperatures and some rain didn't keep two forest fires along the Manitoba-Ontario boundary from growing in the past day. Manitoba officials said Wednesday afternoon that the fire northeast of Caddy Lake has grown to about 5,800 hectares, up 700 from Tuesday. The Beresford Lake fire, meanwhile, has grown to 73,000 hectares - up substantially from the day before, when it was approximately 56,000 hectares. "While weather conditions have improved, there was little rain in the eastern region over the last 24 hours," a press release from Manitoba Sustainable Development reads. "South winds are expected to continue to affect fire suppression efforts." The fires, which have been burning since late last week, have forced the ongoing evacuation of 61 properties on Wallace Lake and others in the Beresford cottage subdivision in Nopiming Provincial Park. The east shore of Caddy Lake in Whiteshell Provincial Park is also closed until further notice, with an evacuation notice remaining in effect there, and cottagers from Ingolf, Ont., were evacuated last week. In the meantime, fire crews from Manitoba and Ontario have received air support from other jurisdictions. On Tuesday afternoon, two BAE-146 jets from Minnesota dropped fire retardant on flames in an effort to protect hydro lines near Kenora. And a water bomber group from the Northwest Territories - which includes two CL-125 aircraft and a bird dog plane - has joined firefighting efforts in Manitoba. In total, about 100 people are working to protect cabins and property in Manitoba, provincial officials said. Winnipeg Sun, A8

*** Busloads of firefighters race in - Ground crews to supplement water bombers**

Hundreds of firefighters poured into Whiteshell Provincial Park and northwestern Ontario to battle a wildfire that's consumed 14,400 hectares and keeps growing. The additional firefighters will work on the ground, supplementing the water bombers that have fought the fires so far. Until Wednesday, it had been

too hot and dry for crews on the ground, but changing weather conditions allowed the movement to a ground attack. As of Wednesday, no one had been hurt and only a few sheds had been lost. The fire is within a kilometre of Caddy Lake, but it's been that close for a couple of days without getting any nearer, said Gary Friesen, manager of wildfire programs for Manitoba. "It's a favourable weather situation right now - (9620 acres) of that are in Manitoba," Friesen said. "What rain we did have allowed us to get crews in. "We have firefighters coming from the north by busloads. These are emergency firefighters the department hires and certifies" for just such situations, Friesen said. "We have firefighters coming from all over Ontario." Friesen said the wind has pushed the fire to the north. The forecast is for much cooler temperatures, which will help, he said, pointing out that what helps Manitoba has just the opposite effect in Ontario. Winnipeg Free Press, A3

* **N.S. sends firefighters to Manitoba**
More than 20 Nova Scotia firefighters are headed west on May 13 to help fight wildfires in Manitoba. "People across Nova Scotia are concerned about Canadians out west and want to help," said Natural Resources Minister Lloyd Hines. "Our well-trained wildfire fighters are ready to help our western neighbours in their time of need. We wish our crew well while working under tough conditions out west, and a safe return." Hines's ministry has promised to ensure that proper firefighting resources are maintained in Nova Scotia and also remains ready to help its federal and provincial counterparts as needed. The Nova Scotia firefighters were requested for Manitoba through the Canadian Interagency Forest Fire Centre. The province is a member of the Canadian Mutual Aid Resource Sharing Agreement, first established in the early 1980s, which ensures all provinces and territories will receive help if forest fires become too big for them to handle. Chronicle-Herald, A10

* **At least 10 fires in Peace region deliberately set**
Investigators say arson is believed to be the cause of at least 10 wildfires in northeastern British Columbia. The Environment Ministry said fire investigators and conservation officers have found evidence that the fires in the Peace region were deliberately set. Some of the fires have caused property damage, said Chris Postuma with the B.C. Conservation Officer Service. He declined to provide details, saying an investigation is ongoing. The blazes are believed to be connected, and the extra conservation officers brought in to help investigate are asking for tips from the public. Canadian Press (Times-Colonist, A12)

* **Firefighters prepare for dry summer - Territorial firefighters get ready for a season of heat with FireSmarting**
Territorial firefighters in the South Slave and Deh Cho are in the midst of training for another year of wildfires. Richard Olsen, manager of fire operations for the Department of Environment and Natural Resources, said crews in Fort Providence and the Deh Cho were expected to start refresher training this week. In Fort Simpson, that included fitness testing at the recreation centre on May 9. More than 20 firefighters showed up for that testing, which included 31 laps up and down a ramp while carrying weight _ 25 of those laps were done wearing a 54-pound pack. The test also required two laps dragging a simulation of a hose. A re-test is expected to take place in two weeks for firefighters who could not make the fitness testing or whose scores were below the acceptable level. Deh Cho Drum (NWT)

* **Stay fire smart this summer**
In the wake of the Slave Lake fire in 2011 the Alberta Government, through the department of Environmental Sustainable Resources and Development have spent many hours mentoring Albertans about being FireSmart. Initial concentration has been in area that are surrounded by forest. The FireSmart website states that methods can reduce the likeliood of a large uncontrollable forest fire. It also recognizes the benefit of controlled burns to rid than area of old, dying and dry forest. FireSmart will come into different neighborhoods, advice and help the area become FireSmart. Nordegg chose to do the FireSmart program after a fire became close to the town a few years ago. Neighborhoods or individuals that are interested should visit the website http://wildfire.alberta.ca/fire-smart/ documents/FireSmart-HomeownersAssessment-Jun2015.pdf. The website has a number of different assessments available to help people determine how safe their buildings are in case of a fire. Information is also available at ESRD offices. Red Deer Advocate, C3

* **Canadian Pacific Railway train derails east of Saskatoon - Close to a dozen cars have derailed, railway crews surveying the damange**
Canadian Pacific crews were called to an 11-car train derailment east of Saskatoon on Wednesday. At around 3:45 p.m. CST, a westbound train derailed about 16 kilometres east of Saskatoon. Eight of the 11 cars were empty; the other three were carrying cement. Several tank cars appeared to come right off their wheels, leaving the cars lying on their sides and the wheels still on the track. A CP spokesperson said there were no injuries and no reports of any hazardous leaks or fires. The derailed cars were not causing any road blockages. CBC News

* **Comox's coast guard loss Sidney's gain**
At least nine employees are moving their jobs to Sidney after the Canadian Coast Guard closed its marine traffic and services centre in Comox. Scott Hodge, of Unifor Local 2182, which represents the Comox employees, said he and two others have moved and the rest will arrive soon. Another nine people were unwilling to relocate and have lost their jobs. "I'm disappointed," said Hodge, who was part of an effort to stop the closing of the Comox centre. Marine traffic and services centres act as the marine equivalent of air traffic controllers, communicating with ships as they move into, through and out of Canadian waters. The centres also listen for distress calls and pass along information such as weather warnings and navigation alerts. The decision to close the Comox station, along with those in Vancouver and Ucluelet, was made by the previous Conservative government. Comox employees were notified March 29 that the centre would close on May 10. Centres in Sidney and Prince Rupert remain open, and the emergency response station in Kitsilano in Vancouver has since reopened. Critics, including Unifor and Vancouver Island New Democrat MPs, said closing the Comox communications centre was foolish, even dangerous. Some argued that Comox, on the east coast of Vancouver Island, would be sheltered from any tsunamis, while Sidney and Prince Rupert could be at risk. But on Friday, the parliamentary standing committee on fisheries and oceans, which was reconsidering the closing, accepted the Canadian Coast Guard's argument that mariner and public safety wouldn't be imperilled by the move and gave its approval. In a dissenting report, the New Democrats pointed out that of the 6,000 total marine emergency calls handled annually in Canada, the station at Comox handled 1,000. Times-Colonist, A7

* **Lac-Mégantic - La communauté rejette le scénario d'un mur de protection**
La voie de contournement de Lac-Mégantic reste « la seule solution possible ». La communauté n'acceptera jamais le scénario améliorant la sûreté du chemin de fer qui passe au centre-ville en érigeant des murs de béton allant jusqu'à cinq mètres de hauteur, prévient le maire, Jean-Guy Cloutier. « La voie actuelle qui passe au centre-ville, on n'en veut pas. Le scénario qui prévoit des modifications avec des murs de béton de 15 pieds de haut, on ne fera jamais ça, dit le maire de Lac-Mégantic au Devoir. La voie de contournement, c'est ce qu'on veut et c'est ce qu'on dit à nos citoyens. Quand on leur dit ça, ils ont le sourire », ajoute-t-il. La firme AECOM a dévoilé mardi un rapport préliminaire sur la façon d'améliorer la sûreté du transport par train à Lac-Mégantic. Presque trois ans après la tragédie qui a fait 47 morts, la petite ville reste traumatisée par la catastrophe. Plus de 65 % des adultes de Lac-Mégantic présentent des symptômes modérés ou sévères de stress post-traumatique, selon des chiffres de la Santé publique cités par AECOM. Plus du tiers (34 %) souffrent de détresse psychologique et 14 % ont des troubles anxieux -- des proportions nettement plus élevées qu'ailleurs en Estrie. Le Devoir, A4

* **De la parole aux actes**
Une pièce d'opinion dit « Avec la présentation des résultats de la première phase de l'étude de faisabilité de la firme AECOM sur le projet de voie de contournement à Lac-Mégantic, citoyens et élus ont au moins une idée de ce qui s'offre à eux pour placer le centre-ville à l'abri d'une nouvelle catastrophe ferroviaire et retrouver la paix d'esprit. Toutefois, des deux scénarios présentés mardi soir, une voie de contournement de 11,9 km au coût de 115 millions $ ou le maintien du tracé actuel avec l'ajout d'un mur de protection, le second doit être rejeté sans hésitation. Car, appelons cela de la sagesse populaire, le refus exprimé par le maire Jean-Guy Cloutier et de nombreux citoyens au sujet de ce « statu quo amélioré » est tout à fait légitime. Nous comprenons que la firme AECOM a voulu présenter cette option afin de fournir un élément comparatif aux gouvernements. Mais ériger un corridor de béton de près de trois mètres de hauteur pour enclaver la voie ferrée actuelle est une idée digne des années 1960, qui insulte l'intelligence des citoyens. Une telle structure défigurerait le centre-ville, obligerait les personnes qui habitent à proximité

de la voie ferrée à vivre devant un mur et aurait un effet dévastateur sur ce qui fait le charme de la capitale du Granit : une vue imprenable sur le lac Mégantic. » La Tribune, 14

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Clark calls on Ottawa to boost tracking of real estate transactions
B.C. Premier Christy Clark says the federal government needs to step up efforts to track real estate transactions because British Columbians want to be assured that everyone is paying their fair share of taxes. The day after her government launched an initiative to collect citizenship data on home buyers - in response to concerns about foreign ownership driving up real estate prices - the Premier said her province has had to fill the information gap "to help us come up with the right solutions" to the spiralling cost of home ownership, particularly in Metro Vancouver. The gap in federal tracking was exposed in March in records showing that dozens of Vancouver-area real estate firms are failing to comply with federal anti-money-laundering laws that require them to identify who their clients are and where their money comes from. The Financial Transactions and Reports Analysis Centre (FinTRAC), which enforces the legislation, said it found "significant" or "very significant" deficiencies within some five dozen B.C. brokerages in the past year. It decided to step up scrutiny over worries that money primarily from China is being laundered through Vancouver real estate. "I think [FinTRAC] can up their game, I think they are trying to now," Premier Clark told reporters Wednesday. "They would probably tell you they are not where they want to be right now but they have begun that process, so that's great. We're partnering with them to work more closely with them now so that sharing of information is going to make a real difference," she said. "I think now, in Vancouver in particular, people are really seeing the need for that to be tightened up." Globe and Mail, A1

Montréal - Début de l'enquête préliminaire des deux présumés terroristes
Sabrine Djermane et Mahdi El Jamali, ces jeunes Montréalais accusés d'activités terroristes, ont assisté mercredi au début de leur enquête préliminaire, frappée d'un interdit de publication au palais de justice de Montréal. La présence de plusieurs personnes appuyant le couple a forcé les agents de sécurité et même la juge Hélène Morin à intervenir pour assurer la bonne marche des procédures. " Ce n'est pas un lieu pour fraterniser ", a dit la juge à de jeunes hommes qui entraient et sortaient, tout en manifestant les uns avec les autres des signes physiques et verbaux d'entente cordiale. Les agents de sécurité ont aussi demandé à certains d'entre eux de se tenir comme il faut. Toutes les places réservées au public, sauf une, étaient occupées par de jeunes hommes du même âge que les accusés. Certains ont d'ailleurs échangé des sourires complices avec Mahdi El Jamali. Deux de ces jeunes hommes ont pourtant assuré au Devoir qu'ils ne connaissaient pas les accusés, sauf par personnes interposées. " On ne les connaît pas directement. Ce sont des amis d'amis. C'est la première fois qu'on vient ici ", a expliqué un jeune homme à la sortie du palais de justice. Sabrine Djermane et Mahdi El Jamali fréquentaient le collège de Maisonneuve. Alors âgés de 18 et 19 ans, ils ont été arrêtés par la Gendarmerie royale du Canada le 14 avril 2015. Diverses perquisitions s'en sont suivies. Les deux accusés n'ont pas été remis en liberté depuis. Le Devoir, A4; CBC News (2016-05-11)

* **Concordia veut freiner les discours haineux sur internet**
Constatant que les propos haineux sont en hausse sur les réseaux sociaux, des chercheurs de l'Université Concordia ont lancé un portail pédagogique, en anglais pour l'instant, afin de tenter de contrer les discours violents. Le groupe derrière l'initiative SOMEONE (SOcial Media EducatiON Every day) souhaite proposer une approche face à la haine et face aux propos tranchés et radicaux. «Il nous faut aider les communautés de la planète à aborder les propos haineux non seulement d'un point de vue préventif, mais aussi sous un angle pédagogique. Si nous les conscientisons aux dangers de tels discours, alors nous aurons un impact positif sur la société», a expliqué Vivek Venkatesh, professeur agrégé au Département des sciences de l'éducation de l'Université Concordia. (…) Sécurité publique Canada a accordé une subvention de 187 340 $ au projet SOMEONE, qui s'inscrit dans une stratégie de lutte contre le terrorisme et les études sur l'extrémisme violent. Journal de Montréal (2016-05-11)

* **Radicalisation: renforcer l'identité des jeunes**

Des chercheurs du Collège de Maisonneuve estiment que le climat qui régnait au cégep après que des étudiants soient partis pour la Syrie était néfaste pour beaucoup de jeunes et propice à la radicalisation. Dans un rapport rendu public le 10 mai, ils appellent au dialogue entre tous les groupes pour prévenir le phénomène. L'Institut de recherche sur l'intégration professionnelle des immigrants a procédé à l'automne à une enquête où une trentaine d'étudiants et des employés du Collège de Maisonneuve ont été interrogés, à la demande de Québec. Le gouvernement provincial a commandé l'étude en juin 2015, dans le cadre du plan La radicalisation au Québec : agir, prévenir, détecter et vivre ensemble et pour lequel le collège a reçu 400 000$. (…) Pour les chercheurs, les enjeux entourant la radicalisation dépassent les murs du cégep. La présence d'espaces de discussion et l'importance de favoriser les échanges entre les groupes sont primordiaux, puisque très peu d'étudiants immigrants, de première et deuxième générations, s'identifient à la société québécoise, peut-on lire dans le rapport. Journal Métro (2016-05-11)

* **Voile islamique et djihadisme : trajectoires personnelles**
Le port du voile islamique et la radicalisation djihadiste soulèvent au Québec et ailleurs des débats enflammés. Quel que soit son niveau de connaissance du sujet, chacun a un avis sur ces questions mêlant religion et société. Loin de la rumeur médiatique, des chercheurs se penchent sur les personnes qui vivent au cœur de ces problématiques. Les résultats préliminaires de leurs études ont été présentés dans le cadre du plus récent congrès de l'Acfas. (…) Politologue, et codirecteur de l'Observatoire sur la radicalisation et l'extrémisme violent de l'université de Sherbrooke, David Morin questionne quant à lui la place du religieux chez les djihadistes canadiens. Après avoir étudié plus de 80 trajectoires individuelles de jeunes radicalisés, il n'y a pas vu de schéma, mais avant tout une grande part de hasard due au nombre incalculable de facteurs issus de leur environnement. Ainsi, il estime impossible de prédire la trajectoire de radicalisation religieuse d'un individu. Pour ces jeunes, le départ pour le djihad, que ce soit en Syrie, en Irak, au Yémen ou en Afghanistan, peut être vécu parfois comme une quête spirituelle, mais bien souvent comme un retour à leur identité sociale. Ils ressentent alors l'islam en tant que « culture attaquée » plutôt que comme une foi profonde. « Beaucoup de djihadistes croient l'islam menacé par un grand complot occidental » explique le chercheur, soulignant la présence accrue chez ces jeunes, majoritairement des hommes de nationalité canadienne, de théories du complot, et de celle du choc des civilisations. La religion ne devient alors qu'une « esthétique du langage qui vient enrober la radicalisation ». Agence Science-Presse (2016-05-11)

No apparent threat
An opinion piece by Ed Lehman, vice-president of the Regina Peace Council, states, "The following paragraph is from the Defence Policy Review Public Consultation Document - 2016 released by Defence Minister Harjit Sajjan on April 6: "In accordance with its 2005 decision, Canada does not participate in the United States ballistic missile defence system for the defence of North America. Should this decision be revisited given changing technologies and threats? Would a shift in policy in this area enhance Canadian national security and offer an avenue for greater continental co-operation? Or are there more effective areas in which to invest to better protect the North American continent?" Twice, Canadians have clearly spoken out advising our leaders that we want no part of the U.S. anti-ballistic missile system. Twice, our leaders heard our voices. Major world powers have continued to expand their nuclear arsenals. The U.S. alone has announced a trillion-dollar program to upgrade and expand its nuclear weapons. The other major powers are doing likewise. The very existence of these weapons then leads the military to push for additional expenditures for "defence," such as the proposal that Canada join the U.S. antimissile system Canada is under no threat now because we are not the world's bully. More and more weapons are not leading to enhanced national security; in fact the more weapons a country has, the more insecure it is." Leader-Post, A6

* **Cognitive dissonance: Why don't Bill C-51 opponents hate the census, too?**
An opinion piece states, "Yesterday, May 10, was Census Day, the deadline for the completion of the 2016 Canadian census. This year marks the reintroduction of the mandatory long form census, which was made voluntary by the Harper government in 2010. Failure to complete the census could lead you to be fined, imprisoned or both. This move has been celebrated by many in the mainstream media and on social media, with numerous triumphant cries hailing the return to "evidence based policies." This struck me as odd. Since when did giving the government personal and private information become cool? In the

age of Snowden, the NSA, and Bill C-51, isn't handing over piles of information to the government something we're supposed to protest and be scared of? Bill C-51 was an overhaul of Canada's anti-terrorism laws and was met with vehement opposition. One of the biggest criticisms of C-51 had to do with privacy concerns. Opponents feared the prospect of the government collecting personal data like their internet browsing history or travel habits, and sharing it between different departments of government. Yet many of these same individuals welcome the return of the long form census. What could possibly explain this apparent contradiction? The easy explanation is partisan bias. Bill C-51 was a product of the "evil, anti-democratic" Conservative government led by Stephen Harper who is either "Hitler, like Hitler, or worse than Hitler" depending on which Harper-hater you asked." The Rebel (2016-05-11)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Weil «très soulagée»
La ministre de l'Immigration, Kathleen Weil, est «très soulagée» que le polémiste Dieudonné ait été refoulé par l'Agence des services frontaliers du Canada (ASFC). Il représente selon elle un risque pour la paix sociale. «C'est très inquiétant lorsque quelqu'un rentre au pays, rentre ici, donc destiné au Québec, et qu'il sème des propos haineux, a affirmé Mme Weil. Ça dérange les gens.» Dieudonné M'Bala M'Bala prévoyait donner une douzaine de représentations de son spectacle au Québec, dont une dans la capitale le 16 mai. Le controversé personnage a une fiche bien remplie de condamnations par les tribunaux français pour des délits d'injure raciale et de provocation à la haine raciale. Le jour même de son arrivée au Québec, il a été condamné pour des propos antisémites tenus dans l'un de ses spectacles, La bête immonde. «Moi, je connais des gens qui ont participé à des spectacles juste pour voir, pour vivre l'expérience, a témoigné la ministre Weil. Et c'est extrêmement dérangeant. [...] Pour la paix sociale, c'est très bien qu'il n'ait pas pu rentrer au pays. Je suis très soulagée.» Après avoir été refoulé, Dieudonné avait publié un message sur sa page Facebook promettant de revenir dans la métropole dès mercredi. «Petit contretemps je dois faire un aller-retour, mais je reviens... Je serai à Montréal demain.» Le Soleil, 41

Role in drug conspiracy lands jail time
A 26-year-old woman has been sent to prison for three years for her role in a Saint John-based, inter-provincial cocaine trafficking conspiracy. Tamara Jones, formerly of Seeleys Cove, was busted during Operation J-Tornado, an almost three-year-long RCMP-led investigation involving local police agencies, Canadian Border Services and forces in other provinces. Although a target when police executed raids in New Brunswick, Quebec and Halifax on Sept. 10, 2014, Jones wasn't apprehended until early October 2014. She had been working on a pipeline in Alberta at the time of the raids. Jones's part in the conspiracy was as one of the network's lower level dealers. Crown prosecutor Jillian Jordan told the court at Jones's sentencing on Monday that the ring leaders would receive bulk weight of raw cocaine that would be cut with another substance, to increase quantity and profits, before being doled out to lower level dealers for street sale. "A specific pattern of communication and conduct would emerge amongst the lower level dealers each time a fresh supply of cocaine was obtained," said Jordan. Jones was caught conducting 14 transactions between May 30, 2014, and August 2014. Over that time, she purchased between 25 to 35 ounces of cocaine, which is about the weight of one litre of milk. Jones was said to have paid more than $20,000 for the drug. Some "re-ups" would come a day apart, other times she was silent for almost three weeks. Jones, like the rest of those already convicted as part of Operation J-Tornado, was taken down via multiple covert techniques that have become familiar to courts in Saint John. RCMP engaged a police agent in 2014 who Jordan said had "a close relationship with the targets of the investigation." The agent's identity is now protected by a publication ban. Telegraph-Journal, B3

Pro-Israeli group lauds ban on comic: Canada turns away french comedian
Federal border officials "made the right call" this week to turn away a controversial French comic at Montreal's airport, Canada's Centre for Israel and Jewish Affairs said Wednesday. Dieudonne M' bala M'bala, who has been convicted multiple times for inciting racial hatred and anti-Semitism, had been scheduled to perform a series of shows in Montreal starting Wednesday night. "Admissibility to Canada is not a right but a privilege," Rabbi Reuben Poupko, the centre's co-chair, said in a statement. "Dieudonne

forfeited this privilege with his numerous criminal convictions for hate speech, incitement to violence and glorification of terrorism. Border Services Canada agents made the right call yesterday in upholding the specific criteria required for entry into the country." However, it was reported Wednesday afternoon that those who had purchased tickets to see Dieudonne perform might still get to see him. Show promoter Gino Ste- Marie told VICE News that technology would allow ticket holders to see the comedian "virtually." Details could not be immediately confirmed. Marie-Claude Chiasson, a Canada Border Services Agency spokeswoman, said Wednesday she could not speak to specific cases. However, she said those seeking entry into Canada may be deemed inadmissible for a variety of reasons, including involvement in criminal activity and human rights violations. Dieudonne, who invokes what has been described as a Nazi-like salute in his shows, has courted controversy for years. In 2012, Belgian authorities reportedly forced Dieudonne to stop mid-performance after determining his act contravened local laws. In 2014, Britain banned the comedian from entering the country. Ottawa Citizen, N6 (National Post); La Presse+; Le Nouvelliste; Le Soleil; Journal de Montreal;

What are they smoking?: Plain packaging laws for cigarettes benefit criminals
In late March, nearly 120,000 pounds of tobacco were seized in Quebec, the biggest tobacco smuggling bust in North American history. Seven-hundred police officers conducted 70 raids, arresting nearly 60 people to break up a vast cross-border tobacco smuggling ring accused of using profits to purchase cocaine and launder money as far away as Europe, while defrauding the Canadian government of half a billion dollars in lost tax revenue. The sheer size and scope of this criminal enterprise, and the police operation required to break it up, grabbed headlines across North America. In the 30 years of my career that I have spent on global investigations - the last 10 focused exclusively on the links between tobacco smuggling and criminal groups, a common theme has emerged: If there is money to be made selling something, organized criminal groups will sell it. Each year, more than 400 billion cigarettes are sold illegally across the globe, making cigarettes the most widely smuggled legal product in the world. Why? No other commodity is as easy to smuggle, or carries such light legal penalties in exchange for such massive profit. This month, 'plain packaging' laws initiated in Australia about one year ago come into force in most of Europe. Australia was the first country to introduce plain packaging, which bans the use of all trademarks on tobacco packs and requires that all tobacco products be sold in drab, virtually identical, government designed packaging. The objective: Reduce smoking. The results so far: A win for criminals. Here in Canada, after the massive police raid in March, the Trudeau government announced it will also introduce plain packaging - music to the ears of those recently handcuffed by Canadian police. Toronto Sun, A58 (Calgary Sun)

* **An attack on his father-in-law could mean deportation for one Mexican man**
Assaulting his father-in-law could mean a federal jail term and possible deportation for a Mexican immigrant convicted Wednesday in the attack. Defence counsel Brad Popovic told provincial court Judge Eugene Creighton his client is in Canada on a work visa and his status, and that of his Calgary wife, are up in the air. Creighton convicted Luis Garcia Chavez in connection with a Nov. 17, 2014, attack on Kelly Allan at the victim's Keoma home northeast of Calgary. Garcia Chavez got into an argument with Allan over his treatment of the victim's stepdaughter, Sarah Fergusson, after a dinner party at his in-law's home. The offender and Fergusson had left the residence, but got into an argument on their way home to Calgary. Garcia Chavez told her to get out of the car in -27C weather, with no footwear or jacket, before she was able to get someone to take her back to her parents' residence. When Garcia Chavez returned to the house, Allan, who had been drinking, came outside to confront him, Creighton noted. But the judge did not believe the offender's version of how Allan suffered facial fractures that hospitalized him for 15 days and required three separate surgeries on his face. Calgary Herald

* **Two South Asians acting as immigration consultants in Montreal accused of immigration fraud**
The Canada Border Services Agency (CBSA) announced on Tuesday that Rajinder Singh and Resham Singh, acting as immigration consultants, were summoned to appear in court and are facing three charges under the Immigration and Refugee Protection Act (IRPA) and two charges under the Criminal Code. Rajinder Singh was arrested and appeared on Tuesday morning at the Montreal court house, and Resham Singh received a summons to appear on June 9 at the same court house. Rajinder Singh and Resham Singh are accused of counselling persons to misrepresent information in their immigration applications and refugee protection claims, as well as forging and using counterfeit documents. They are

also accused of having acted as immigration representatives in return for compensation, when in fact they were not authorized. Benoit Chiquette, Regional Director General, Quebec Region, CBSA, said: "The CBSA conducts investigations and prosecutes immigration offenders with the full force of the law. Immigration frauds are criminal acts. Do not be a victim of fraud. Dishonest consultants can take advantage of people who want to come to Canada, and they represent a serious threat to the integrity of Canada's immigration system. This is why the CBSA acts to prosecute those responsible in the courts." Voice; La Presse; Radio Canada

Liberals stick to their guns on Saudi arms agreement: PM fears for Canada's business reputation despite videos of armoured vehicles being used on dissidents

Canada is obliged to uphold its reputation for honouring business deals and therefore must sell $15-billion of armoured vehicles to Saudi Arabia, Justin Trudeau said on Wednesday when asked about video footage that shows the Saudis using similar machines against civilians in the Mideast country. "We need to be able to project [to] the world that when Canada agrees to something, it sticks to its word," the Liberal Prime Minister told MPs in the Commons. Footage published by The Globe and Mail on Wednesday shows armoured vehicles being used against minority Shia Muslim dissidents. (…) John Packer, director of the University of Ottawa's Human Rights Research and Education Centre, said the Liberals should put the Saudi deal on hold and reassess the risks Canadian vehicles may be deployed against civilians. "Evidently, the export-control process didn't quite look at everything or not closely enough ... the export should at least be put on hold pending close scrutiny and evaluation. This is an opportunity to get it right and avoid making a terrible mistake contrary to both the letter and spirit of Canadian law and to good sense."The Saudis' use of combat machines against its Shia population goes to the very heart of the controversy over whether the Trudeau government is breaking Canada's weapons export-control rules. The export-control regime clearly stipulates that Ottawa must not issue export permits for weapons sales to countries with poor human-rights records "unless it can be demonstrated that there is no reasonable risk that the goods might be used against the civilian population." Globe and Mail, A1

Don't use Clement products: Health Canada

Health Canada is warning people to stay away from a controversial line of American alternative medicine products. The warning comes a day after the government announced it was investigating the LifeGive line of products being sold by controversial alternative medicine guru Brian Clement. "These products are not authorized for sale in Canada," the department said. "LifeGive health products have not been reviewed by Health Canada for safety, quality or effectiveness. "Health Canada is working with the Canada Border Services Agency to stop the importation of any shipments of LifeGive health products from entering Canada. Should this company continue to sell unauthorized health products, Health Canada will take appropriate action," the department said. In public appearances and videos Clement claims to cure cancer and other diseases with wheat grass suppositories and a diet of raw vegan foods through his Hippocrates Health Institute. Clement gained notoriety in Ontario in 2014 and 2015 when two Aboriginal girls were taken off chemotherapy for leukemia in favour of Clement's treatments and traditional native medicine. One girl died and the other has returned to chemotherapy. Clement appeared last weekend at a health and wellness fair on the Six Nations reserve. He declined to be interviewed. Hamilton Spectator, A4

If anything, 'better in than out' underestimates our TPP gains

In the fractious politics of trade, a recent, supportive C.D. Howe Institute report on Canada's stake in the Trans-Pacific Partnership made a welcome contribution. For Canada and its 11 partners, the TPP promises market-oriented rules for industries unknown two decades ago and a stronger gateway to the Asia-Pacific, the world's fastest-growing region. But even that positive study understates the benefits of the agreement. The study does not discuss geopolitical gains, which may be the TPP's most important contribution - as eight former U.S. secretaries of defence pointed out recently. The TPP will strengthen links across the Pacific and reinvigorate a rules-based approach to global trade. (…) Global negotiations have mostly won the war against tariff barriers; in the United States, they are now 78-percent lower than after the Second World War. But regulatory obstacles - non-tariff barriers - have mushroomed. The World Trade Organization and others now see such barriers as the main bottleneck; the Peterson Institute estimates they are five times as restrictive as tariffs for TPP trade. The new, authoritative Elsevier Handbook of Commercial Policy concludes that accords such as the North American free-trade

agreement have increased trade as much as five times more than could be expected from tariff cuts alone because they reduce non-tariff barriers and uncertainty about future trade relations. Globe and Mail, B4

*** Dispute over speeding led to man getting shot three times**
Yelling at a speeding motorist to slow down almost got a Calgary-area man killed, court heard Wednesday. Crown lawyer Ron Simenik said Charlemangne Literato was shot three times by Mathew Van Schaik after asking the driver of an SUV who passed him to lay offthe gas. Simenik, reading from a statement of agreed facts, said Literato was leaving Anytime Fitness in Airdrie in the early morning hours of last Sept. 27, when he saw Michael Sharman drive past at what he felt was a high rate of speed. "Literato ... yelled at the Mercedes SUV to 'slow down,' (...) Literato was hit in his upper right thigh, in his right wrist and in his lower back. The third bullet remains in the victim's buttocks, Simenik said. In a victim impact statement, read in by the prosecutor, Literato, a temporary foreign worker employed as a cook, said he has had difficulty in his job since the shooting since he can't stand for more than two hours. Calgary Sun, A3; Edmonton Journal; Calgary Herald

*** Foreign workers program worked**
An opinion piece states, "Re: In review of Temporary Foreign Worker program, don't forget the farmers, May 9. Edward Dunsworth argues that temporary foreign workers (TFW), as well as seasonal agricultural workers (SAWP), must be granted permanent residency upon arrival. He seems to think failure to do so undermines Canada's reputation as an inclusive multicultural democracy. But he fails to understand that the key to the success of these programs rests on the word "temporary" or "seasonal." The fastest way to bring these programs to an end would be to grant the workers permanent residency upon arrival. In the case of SAWP, it would be to terminate one of the most successful programs ever designed to help Canadian farmers and at the same time put desperately needed money in the hands of Caribbean and Mexican farm workers. The key was to get unskilled workers to do the hard work of picking fruit and other crops when the harvest was ready. The employer had to pay the workers' return transportation, pay the prevailing wage rate, and provide satisfactory accommodation. The larger part of the earnings was held back until the workers returned home, to ensure the money was available to be spent in their own country." Ottawa Citizen, A10

*** Parkway pointless without new bridge**
An opinion piece states, "We have just built a new parkway to lead up to a new bridge, the Gordie Howe International Bridge. Being a dual citizen of the U.S. and Canada, it really aggravates me when I have to wait an hour to cross the river. It seems like every time that I am on the Ambassador Bridge, there is construction. The Ambassador Bridge has two lanes - one for trucks and one for cars and SUVs. Everyday, around 68,000 travellers cross the Ambassador Bridge - 10,000 of those travellers are trucks, leaving the other 58,000 people congested in one lane. We need to make Windsor great again and build the new bridge. However, we have shown no progress in starting it, making the new parkway merely pointless." Windsor Star, A8

'Make dating great again'
A new dating website is offering to pair americans with Canadian singles to save them from a Donald Trump presidency. MapleMatch.com promises love and a U.S. escape plan if Trump becomes commander-in chief. The website promises to "make dating great again," parodying the presumptive republican presidential nominee's slogan. "It's easy to say, 'This is just about americans trying to find a way to get residency in Canada," CEO Joe Goldman said in an interview. "I think ... many americans may be frustrated by the community that they're in or the dating pool they've had access to. "Why not seek something different? Why not seek something Canadian?" The Texas-based Goldman acknowledges that american have cried "We're moving to Canada" before, but he says Trump's divisive policy proposals - like building a wall along the Mexican border and creating a national database of Muslims - make the call of the north all the more real. "The idealization of Canada by americans has happened for a long time," he said. "I guess americans might be excited about the potential of meeting someone who likes hockey and doesn't mind a little maple syrup in their pancakes." Canadian Press (Toronto Sun, A2, Winnipeg Sun. Edmonton Sun, Ottawa Sun)

CYBER SECURITY / CYBERSÉCURITÉ

*** IBM and eight universities join fight against cyber crime**
IBM wants its Watson computer system to learn how to fight cybercrime and it's asking eight leading universities, including three in Canada, for help. Watson - IBM's question answering computer system - was originally designed to compete (and win) on the television quiz show Jeopardy, but the technology has since been used on other problem-solving projects. Now IBM is launching Watson for Cyber Security - a cloud-based version of their cognitive technology - that will be trained over the next year to examine threats of cybercrime. Caleb Barlow, vice-president of IBM Security, said it is becoming increasingly difficult for security staff to deal with the growing number of cyber threats. Canadian Press (Red Deer Advocate, C4)

*** Roadmap for cybersecurity - Liberals must ensure police have right tools, writes Pierre-Yves Bourduas**
An opinion piece states "The reported recent cyberattacks on the National Research Council time signal served as a reminder that the proposed review of cybersecurity by the Liberal government should be welcome news. Three components will be considered in the review: securing government systems, partnering to secure vital cybersystems outside the federal government, and helping Canadians to be secure online. Considering that information technologies and the Internet provide criminals with innovative and highly sophisticated ways to commit a plethora of new crimes - and old crime in new ways - the government review should be broadened to determine whether or not law-enforcement agencies have the necessary tools to detect, deter, investigate and prosecute cybercriminals. In 2014, the Canadian Anti-Fraud Centre received more than 14,000 complaints of cyber-related fraud for more than $45 million in reported losses. During the same year, the RCMP National Child Exploitation Co-ordination Centre received nearly 8,500 reported incidents concerning online child sexual exploitation. These statistics only provide a partial picture of the magnitude of the problem." Ottawa Citizen, A11

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Cocaine bust nabs 13**
Thirteen people were arrested on Wednesday after police busted what they called a well-structured organized crime network that imported and trafficked cocaine. Talks were ongoing with another suspect located in Italy, while a 15th person was also being sought, the RCMP said. The alleged Montreal based ring imported a total of 1.4 tonnes of the drug, the Mounties said. American and Canadian authorities seized 220 kilograms of cocaine during Project Clemenza, a three phase investigation that began in 2010. Authorities said they also confiscated $2 million that was to be used to help import the drugs from the U.S. Most of the accused are from the Montreal area, although one lived in Ottawa and another was already detained in Kingston. Quebec provincial police, the Montreal and Laval forces, the Canada Border services agency and the Canada revenue agency also took part in the investigation. Canadian Press (Toronto Sun, A57, Calgary Sun, Edmonton Sun, Waterloo Region Record); Journal de Québec, 36 (Journal de Montréal); Postmedia Network (Montreal Gazette, A3, Winnipeg Sun, Calgary Sun, Ottawa Sun, Edmonton Sun, Toronto Sun); La Presse, 10; CBC News (2016-05-12); CBC News; National Post; CTV News; CFRA News; Montreal Gazette; Presse canadienne (Actualité); Hebdo Rive Nord; Métro; Journal de Montréal (Journal de Québec); Le Devoir (2016-05-11)

*** Auxiliary Mounties sidelined**
They're a highly trained army of law enforcement volunteers ready and willing to help in the wildfire-ravaged city of Fort McMurray. But hundreds of auxiliary Mounties from Alberta are being left on the sidelines. As Canada's national police force conducts a review of the volunteer constabulary, some 300 trained members of Alberta's auxiliary, as well as those from other provinces, have been benched, even as the same number of sworn RCMP officers have been flown into the province from as far away as Newfoundland to help. (…) One auxiliary member, whom Postmedia has agreed not to identify, said he has been ready to go since the first call came out, and questions why RCMP's K Division isn't willing to take advantage of a group of trained individuals ready to do whatever is needed to pitch in. "I've literally

had my uniform, my duty belt and my equipment sitting in the trunk of my car for the last week," said the member, who volunteers with a rural Alberta detachment. "We all know what we signed up for." Listed among the duties of auxiliary constables in their charter for Alberta's K Division is the potential to be called in to help deal with disasters, such as the one in Fort McMurray, which is likely to become Canada's costliest natural disaster. "Auxiliary candidates recruited into the program are registered as emergency services workers through Alberta Transportation Utilities, Disaster Services, and as such, may sometimes be called upon to assist the RCMP in an emergency," the charter reads. In January, all 1,600 members of Canada's RCMP auxiliary were informed of immediate changes to the program, including an end to ride-alongs and firearms familiarization training, as well as more clearly distinguishable uniforms. The review was sparked by the slaying of RCMP Const. David Wynn, who was gunned down at a St. Albert Casino last year. Edmonton Journal, A5 (Calgary Sun, Calgary Herald)

Mounties busy in Fort McMurray

RCMP officers in Fort McMurray are investigating 100 cases of forcible entry into evacuated homes after authorities finished canvassing the city Tuesday morning. Of those, 91 were discovered by initial canvass teams, while others are being reported as officers continue to patrol the area. All cases of forcible entry are being treated as criminal investigations. However, police are cautiously optimistic most did not involve criminal activity. "Our investigators have observed many cases where valuables were clearly visible within the home, which would indicate something other than a criminal act had occurred," said RCMP Insp. Kevin Kunetzki said Wednesday at a press conference at RCMP K Division, 11140 109 St. "We will followup, starting by contacting the homeowners to see if they can explain the incident." Canvassing efforts, which included Anzac and neighbouring rural homes, also resulted in 29 cases where police discovered occupied homes. Police could not confirm how many people were removed from their homes, but said none were forcibly removed. "It was only a very small, handful of people who refused to leave," Kunetzki said. "The vast majority of residents in those areas were very cooperative and understood the safety concerns, and evacuated the area without incident. Police also provided cellphones and vehicles to those who did not have any so they could evacuate safely. "They wanted the assistance they just didn't have the means, so we were able to provide that," Kunetzki said. Postmedia Network (Edmonton Sun, A6, Calgary Herald, Edmonton Journal, Calgary Sun)

No flood of gun seizures

RCMP have seized some guns following the fire in Fort McMurray, but won't be a conducting a mass seizure of firearms like they did after the flood in southern Alberta. Sgt. John Spaans said Tuesday that officers have taken one or two guns found in public places, but are not going into homes looking for more. He said he's not sure if the decision had anything to do with what happened in high river during the floods. Flood water forced thousands of people from their homes in high river in June 2013. as Mounties searched for people who were stranded in the town, they kicked in doors and took firearms. Canadian Press (Toronto Sun, A56, Ottawa Sun,)

Six males charged in multiple sexual assaults

Six males, including a youth, have been charged with multiple sexual assaults on the University of B.C. campus in Vancouver and in at least two other communities. RCMP detachments at UBC, in North Vancouver and Burnaby, along with the Vancouver Police Department and Transit Police, joined forces to investigate the offences. Vancouver Police Supt. Mike Porteous says a number of brave women came forward to report the difficult and horrific details of the surprise attacks, in some cases after an assailant broke into their homes. RCMP Chief Supt. Jodie Boudreau says only two of the individuals who have been charged are connected and both are alleged to have been involved in the same assault. Canadian Press (Telegram, B10, Cape Breton Post, Guardian, Waterloo Region Record, Times Colonist); * Globe and Mail; Vancouver Sun, A2

*** Gabriola man faces child porn charges**

A 70-year-old Gabriola Island man has been charged with one count of possession of child pornography after a search of his property stemming from information out of England. Douglas Densley Green has been released on a number of court-imposed conditions, including that he stay away from any location where children younger than 16 might reasonably be expected to attend. More than 40 items were seized in March during a search of Green's residence and other residences on the property. Preliminary forensic

examinations have been carried out on computers and electronic media. The investigation developed after the Kent Police Department in England obtained information in December that a Canadian resident was allegedly involved in an offence linked to children younger than 16. B.C.'s Integrated Child Exploitation Unit was contacted and a criminal investigation was started. After tracing a computer address, investigators believed that the suspect was on Gabriola Island, and the case was forwarded to the Gabriola Island RCMP. Gabriola officers continue to investigate and are working with Crown counsel to decide whether further charges could be filed. "This type of crime doesn't really have borders, in a sense, so unfortunately, a lot of this type of stuff has Internet communities or Internet groups that are from various countries, potentially," said Cpl. Markus Muntener, Gabriola Island detachment commander. He said this sort of case is rare for Gabriola. "It's a small island with a fairly small population, obviously, and small police detachment, so we don't really deal with these types of cases very often, thankfully." Times Colonist, A6

*** Man, teen arrested after shooting face drug, firearm charges**
Two people arrested after a shooting in Kent County last month appeared in provincial court on Wednesday to face a series of drug and firearm charges. Frank Hannay, 44, of Clairville, is charged with 12 offences while and Emma Lirette, 18, of Moncton, is facing 10 charges. Both accused return to court Thursday to set bail hearing dates. Hannay and Lirette are both charged with producing marijuana between April 15 to 22 in Clairville, possessing more than three kilograms of marijuana for the purpose of trafficking and possessing methamphetamine. Hannay is also charged with four separate counts of violating four separate court orders banning him from possessing firearms. He's also charged with possessing a prohibited firearm - a sawed-off shotgun - unlawful storage of a firearm, possessing a prohibited firearm with readily available ammunition, attempting to obstruct justice by concealing evidence and breach of probation. Lirette is accused of obstruction, two counts of breaching probation, unlawful storage of a firearm, possession of a prohibited firearm - the shotgun - and possessing a prohibited firearm with available ammunition. Richibucto RCMP arrested two men and a woman on April 26 as a result of a shooting investigation in Clairville, 43 kilometres northwest of Moncton. Police said in a news release that on April 21 at around 2 a.m., they received a 911 call from the Adamsville area regarding a person suffering from a gunshot wound. It was determined the individual was the victim of a shooting that occurred earlier in the night at a residence in Clairville. Along with Hannay and Lirette, the RCMP also arrested Jamie Melanson, 21, of Moncton, and charged him with careless use of a firearm, assault with a weapon and pointing a firearm. Times & Transcript, A5

*** Le déraillement près de Plaster Rock a été provoqué, conclut la GRC**
Le déraillement survenu lundi à Sisson Ridge, près de Plaster Rock, au Nouveau-Brunswick, est le résultat d'un acte délibéré, selon la GRC. Huit wagons ont quitté les rails, mais aucun ne s'est renversé. Un porte-parole de l'Organisation des mesures d'urgence avait alors déclaré que la sécurité du public n'était aucunement menacée, même si l'un des wagons contenait du pétrole. La GRC et le CN mènent une enquête conjointe, a indiqué la porte-parole de la police fédérale, Jullie Rogers-Marsh. Les policiers demandent à toute ayant des renseignement sur cette affaire de communiquer avec eux. Radio-Canada

*** RCMP pleas scheduled on 4 Labour Code charges**
The RCMP is expected to enter pleas Thursday on charges the force violated four health and safety provisions of the Canada Labour Code in connection with the 2014 Moncton Mountie shootings that left three officers dead and two others wounded. There is also the chance a "possible resolution" could be reached between the national police force and the Crown. The RCMP was scheduled to enter pleas on the charges on April 7, but Crown prosecutor Paul Adams told the court then that ongoing discussions were taking place between the parties to work on a possible resolution and more time was needed. Adams didn't elaborate on what he meant by "possible resolution." The Crown prosecutor did say he expects to have a clear idea of where the case is going at Thursday's court appearance. Lawyer Ian Carter, who represented the RCMP in court on April 7, said at that time they were working at "narrowing the issues" and would be in a position to tell the court what the RCMP would be doing at the next court appearance. CBC News; Radio-Canada

Racial bullying case handled properly - Casey

Provincial Education Minister Karen Casey says she is confident that reports of racially targeted actions against a teacher at Forest Heights Community School in Chester Basin are being dealt with effectively. News that a Forest Heights teacher was the subject of racial bullying at the school first surfaced last week on LighthouseNow.ca. Witnesses said they saw a Confederate flag attached to a vehicle parked at the school several times and that a snare was hung over the door of a classroom bent into the shape of a noose. "The incident occurred some time ago and I have been in touch with the South Shore Regional School Board," Casey said in a statement to the Chronicle Herald. (...) RCMP spokeswoman Jennifer Clarke said an incident was reported to Lunenburg District RCMP on Feb. 24. "We can't confirm whether the investigation involved a group of students or a single one, because our investigation did not lead to any charges being laid." She said no further details could be disclosed because there was insufficient evidence to lay charges. Chronicle-Herald, A4

Fausse intervention policière dans une école de Shippagan
Les grands moyens ont été déployés mercredi après-midi à l'école Marie-Esther de Shippagan. Pas d'urgence cependant. Policiers, pompiers et ambulanciers mobilisés participaient à un exercice d'entraînement en conditions réelles. Pendant une heure et demie, les forces en présence ont simulé «une menace active dans l'école», décrit Patrice Ferron, agent de programmes communautaires pour la GRC. Pour des questions de confidentialité, il n'en dira pas plus. Le personnel et les enseignants ont également été mis à contribution. Aucun élève n'a participé. Cet exercice a permis aux forces de l'ordre de vérifier leurs techniques d'intervention et l'efficacité de leurs systèmes de communication. Une fois le dispositif levé, tous tiraient un bilan positif. «Nous sommes satisfaits. Nous avons respecté les délais impartis», commentait Patrice Ferron, aussitôt l'école à nouveau accessible au public. (...) La GRC organise régulièrement ce genre d'opération à grande échelle. La précédente s'est déroulée l'année dernière à Campbellton. Acadie-Nouvelle, 8

Police use of tasers on rise
With more and more weapons on the streets, it's no wonder police are using Tasers more often, Saskatoon's police chief says. In 2015, city police used Tasers 17 times - 10 more than in 2014. "It gives our officers an extra option," Chief Clive Weighill said outside the board of police commissioners meeting on Wednesday. Weighill said several cases of officers using Tasers involved people threatening harm to themselves. He said in cases like that, Tasers provide a way for officers to subdue the person without using firearms or other types of more violent or deadly force. In that way, a spike in the use of non-lethal Tasers to stun rather than seriously injure suspects is a good thing, he said. Officers pointed their guns nine times in 2015 - four fewer times than the previous year. There were also fewer cases of take downs and "joint locks," according to a report received by the board. An officer discharged a firearm in one additional case. Coun. Darren Hill, who is a member of the police board, said he's OK with seeing Tasers used more if it means a reduction in other types of force. "I had no problem with tasers being up at 17, seeing the decreases in other areas," he said at the meeting. StarPhoenix, A1

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Matsqui Institution in lockdown while search conducted**
A lockdown has been in place in Matsqui Institution in Abbotsford since 10:30 p.m. Tuesday. Correctional Service Canada said Wednesday the lockdown, which involves prisoners being confined to their cells, was implemented to enable staff to conduct what was described as an exceptional search. "The search was ordered to ensure the safety and security of the institution, its staff and inmates," CSC said in a news release. "Normal operations will resume as soon as it is considered safe to do so." No other information was available, although CSC said it's committed to preventing the entry of contraband into its institutions. Vancouver Sun

*** A look at CORCAN**
Collins Bay Penitentiary is now considered one of the largest prisons in Canada — with three security levels and over 500 staff members. The prison offers up a range of programs for inmates — including schooling and more hands-on training. Newswatch's Morganne Campbell takes a closer look at one program that's making a difference. You're looking at the old prison farm grounds on the southwest

corner of Collins Bay Institution. The buildings that once housed livestock have either been shuttered or are being used by CORCAN — a rehabilitation program.... that provides inmates with job skills. Chris Stein / CORCAN Operations Manager: "Right now seven individuals are involved in the apprenticeship program with Ministry of Colleges and Universities and there are an additional 30 offenders that are receiving skills training in various trades." (...)Craig Chinnery/CORCAN Operations Manager: "Employment is tracked with the inmates that leave and up until warrant expiry we've had a 74 percent success rate in employment in welding and related fields." (...)Curtis Jackson: "The Correctional Service of Canada continues to assess you know the feasibility and what is required so that is still in the process of you know in terms of costs and what initiatives need to be taken so that's currently under review." CKWSTV (2016-05-11)

*** Judge leaves sentencing option open for man convicted of drug offences**

A judge often has various sentencing options to choose from, but it is rare for a judge to give a convicted person a choice regarding their sentence. That is what happened in the Surpreme Court of Newfoundland and Labrador in Corner Brook when Justice David Hurley delivered his decision to sentenced Jordan Butler Wednesday afternoon. (...)Crown attorney Adam Joyce had asked Hurley to give Butler three years in jail, since Butler had prior convictions for drug charges. Butler's lawyer, Robby Ash, had requested a sentence in the range of two years. (...)Hurley told Ash and Butler that they could accept a full two-year sentence, if Butler would rather serve his time at a federal facility where programs might be of a higher quality than in a provincial prison setting. A straight two-year sentence would mean no probation as federal sentences use the parole system and are never accompanied by probation orders, which fall under provincial jurisdictions. (...)After court had adjourned, Ash consulted with Butler and with Corrections Canada. The matter was recalled and Ash informed Hurley the defence would actually go with the federal option of a two-year sentence with no probation. Western Star

Police seek help with murders, Dechamp remains in custody

Tyrell Peter Dechamp remains in the Ontario corrections system awaiting his fate after his capture on a Canadawide warrant in April. Dechamp, 26, was sought by Halifax police after he skipped curfew at a halfway house he was residing in on Gottingen Street on April 19. He was found and apprehended April 28 in Ottawa, three days after the warrant was issued. Dechamp was arrested without incident for being unlawfully at large. No weapons or drugs were found at the scene. At the time, police said he was going to be returned to Halifax. Detective Constable Steve Sermet, who was a part of the arrest, previously told the Chronicle Herald the process Dechamp might go through. "There'll probably be a parole officer speaking with him and at that point after the interview, he'll probably be taken back to Halifax," said Sermet. He said the interview would be conducted within five business days. He's been in the custody of Canada's Correctional Services for two weeks, and the transfer has yet to take place. Though privacy law kept Correctional Service Canada from discussing specifics, they did say Dechamp was under their jurisdiction. "He is being supervised by us," said Kyle Lawlor, spokesman for Ontario. "When conditions are breached, the parole board often assesses things and can revoke parole. Even if he was out in the world, he may still be under our jurisdiction. Things may have to be reassessed now." He referred questions about the specifics of Dechamp's case to the Parole Board of Canada. Chronicle-Herald, A3

Long-term offender gets another jail term

A man with a long history of alcohol-related crimes - including 14 impaired driving convictions - has been sentenced to 15 months in jail for violating orders not to drink. Robert Samuel Noseworthy was sentenced in provincial court in St. John's Wednesday, shortly after he pleaded guilty to breaching a long-term supervision order (LTSO). With 1.5 times credit given for time served, it leaves about nine months left on his term. (...)The 66-year-old had recently been released from prison after serving a seven-year term for charges of driving while disqualified and impaired driving causing bodily harm. That sentence was handed down in March 2011. At that time, Noseworthy was declared a long-term offender, which means that when his jail term expires, he will be closely supervised in the community for 10 years. He was the first convicted drunk driver to be declared a long-term offender in the province. Noseworthy was released in August 2015 to serve the rest of his term in the community. The Telegram, A5

Hells Angels associate abandons appeal

A Hells Angels associate who was convicted in the manslaughter of a Kelowna man has abandoned an appeal of his jail sentence. In October 2014, B.C. Supreme Court Justice Mark McEwan sentenced Anson Schell to three years in prison for his role in the fatal beating of Dain Phillips, 51, in 2011. Schell had an appeal of his conviction dismissed in January and Crown counsel John Gordon told a B.C. Court of Appeal judge Wednesday Schell had dropped his sentence appeal. Phillips was severely beaten by men wielding baseball bats and hammers and left bleeding in the middle of a road. He never regained consciousness and was later taken off life support. Norman Cocks and Robert Thomas, two members of the Hells Angels, pleaded guilty to manslaughter and received 15-year jail terms. They admitted they wielded the weapons during the fatal assault. Four others - brothers Daniel and Matthew McRae, Schell and Robert Cocks, the father of Norman Cocks - were also charged and went to trial. The Province, A12 (Vancouver Sun)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

* **Dozens of Aboriginal women pick up phone to complain about Quebec police abuse**
It's been just a month since Quebec Public Security Minister Martin Coiteux invited Aboriginal women across Quebec to call a new toll-free line if they'd been assaulted by police. In that short time, 44 women have reached out. Coiteux said the new line was an alternative to calling the Montreal police force, which is in charge of investigating allegations against eight Sûreté du Québec officers that surfaced last fall in a Radio-Canada *Enquête* report. Calls to the new hotline are being directed to an existing paralegal counselling service for aboriginal people – Services parajudiciaires autochtones du Québec. (…)Patricia Bouchard, a community worker at the Sexual Assault Prevention Centre in Val d'Or, says it's "appalling" the number is so high. CBC News

* **Child abuse up: Study**
More children are being sexually abused and exploited than ever before, according to a new study. The disturbing conclusion comes from a two-year study by ECPAT International, which took a look at child sexual exploitation in travel and tourism. U.S.-based Ernie Allen, former president of the International Centre for Missing and Exploited Children, served on the study's task force. "I had a police commanding officer say to me, 'The only way not to find this problem in any community is simply not to look for it,'" Allen pointed out. Here's what Allen had to say ahead of the study's release on Thursday: "We've made great progress but the problem's actually worse. It's different, it has changed in its nature, more kids are being harmed today than ever before, and the quality and level of services to help those children is really poor in most of the world." On human trafficking and exploitation in Toronto: "I think it is a phenomenon that is really no different than any other major metropolitan area. One of the big challenges that all of us face now is that this is a problem that has migrated from the streets to the Internet. so today there are mechanisms, websites, for example, that advertise sexual services and some of those are kids. so that what we have seen happen is that the risks are less to the provider of the service, the risks are less for the prospective customer, and we simply have to address that." Toronto Sun, A62

* **Saskatoon police service missing its response goals for serious calls**
A report presented to Saskatoon's police board says the city's police department isn't hitting its target for responding to the most serious calls. Police have a goal of making it to 80 per cent of priority one calls within 12 minutes, but according to the service's annual report card, they only hit the mark 61 per cent of the time last year. Police Chief Clive Weighill says he's concerned the statistics are being skewed because several new types of calls were added to the "priority one" category over the last two years. In the past, Weighill says only three or four types of calls such as homicides or officers needing assistance got the most serious ranking, but now he says assaults have been added to the list. Weighill says the service is undergoing a full independent review of its operations, which is expected to wrap up before the end of the year. He says he expects the review will uncover whether the response time issue is a statistical anomaly, or the result of other factors. The report card showed overall crime down in Saskatoon, particularly violent crimes against individuals. Canadian Press (The Telegram, Cape Breton Post); CKOM (2016-05-11)

*** Quarterly crime report: Overall crime has decreased so far this year in Maple Ridge and Pitt Meadows**
Overall crime has decreased in Maple Ridge and Pitt Meadows, according to Ridge Meadows RCMP's recent crime statistics for the beginning of 2016. The number of property related crimes in Maple Ridge and Pitt Meadows during January to March were lower than the year before, whereas crimes against persons increased, Ridge Meadows RCMP reported. Mounties released its Crime Statistics for the First Quarter of 2016 on Wednesday. Maple Ridge Times

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

*** Liberals in action: task force here, policy review there**
An opinion piece states, "Public Services Minister Judy Foote announces the creation of a task force to conduct a sweeping review of Canada Post, including whether door-to-door delivery should end, as the Conservatives authorized and the Liberals opposed. The task force will report in 2017 with government action to follow. (…) Indigenous and Northern Affairs Minister Carolyn Bennett announces the forthcoming creation of a commission to examine the issue of missing and murdered aboriginal women. Consultations with native communities are already under way, the commission will be appointed in mid-2016 and it will take up to two years to offer conclusions and recommendations. (…) Election campaign promises are one thing; doing something sensible with them turns out, predictably, to be much harder." Globe and Mail, A13

*** Indigenous men murdered at an alarming rate, but no inquiry?**
A letter to the editor states, "I understand why the Liberal government has decided to hold a federal inquiry into missing and murdered Indigenous women. What I don't understand is the lack of concern or attention by the government and the media to the fact that the rate of homicides among Indigenous men is about three times the rate of homicides for Indigenous women. According to Maclean's Magazine, the homicide rate for Indigenous women is 3.6 per 100,000 population, compared to an appalling 10.8 homicides per 100,000 for Indigenous men. Why has the government and the media not addressed nor even discussed this startling statistic?" Sudbury.com (2016-05-11)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

Bugs in new PS pay system being worked out, staff told
Federal officials say the government's pay centre was swamped with a record number of calls about payroll problems last week, but they're confident they've worked out most of the bugs plaguing the rollout of the new automated pay system. Brigitte Fortin, assistant deputy minister at Public Services and Procurement, said Wednesday the second phase of the $300-million Phoenix pay system that rolled out earlier this month processed 293,000 paycheques on May 4, the first payday after 190,000 new files were added to the system. But the Public Service Alliance of Canada doesn't think the rollout is going as smoothly. PSAC president Robyn Benson said Tuesday the union has taken its concerns about the Phoenix rollout, which she called "seriously flawed," to the department. She said public servants are still not getting paid properly, or not at all, and pay centre employees are swamped. "The stress continues to mount for employees in Miramichi (N.B.) who are working on the new system. ... We have been sounding the alarm on this for months." (…) Debi Daviau, president of the Professional Institute of the Public Service of Canada, said the union fielded twice the number of complaints in the second rollout compared

with the first, but that it had been braced for more. The problem, she said, is that it went ahead before the system was ready. "I do see them do the right things, but when you have one person not being paid that is a problem. But when thousands aren't paid, it is catastrophic, so no effort would be too much effort in fixing this." Ottawa Citizen, A4

OTHER / AUTRE

Kin fear for ex-Londoner being held in Pakistan
The last nine months have been "absolute hell" for the family of a former Londoner who became a high-rankingpolitician in Pakistan, but now languishes in jail there, says one relative. Human Rights Watch has waded intothehigh-profile case, callingthe allegations against Asim Hussain, a former government minister and close ally of Pakistan's oustedpresident, politically motivated. Hussain , 63, has been detained in Pakistan since he was arrested on Aug. 26, 2015, on allegations of financing terrorism. His supporters say his health has been steadily deteriorating - he's had kidney failure and a heart attack while in custody - and are demanding he be granted bail and a fair and speedy trial. "It's just been absolute hell," Hussain's relative, who asked not to be named out of fear of retribution, said Wednesday by phone from Karachi, Pakistan. The chairperson of a board overseeing five hospitals, Hussain was initially accused of financing terrorism and treating terrorists at one of his Karachi hospitals - all claims he denies. (…) An orthopedic surgeon back home, Hussain hoped to practise in Canadabut couldn't get the necessary certifications. He moved his family back to Pakistan six years later and resumed his career in surgery Hebecame the chairperson of the Ziauddin Group of Hospitals, five Karachi hospitals named after his grandfather, Dr. Ziauddin Ahmed, a prominent figure in Pakistan's independence movement. While many of his colleagues from the Zadarari government fled the countryfollowingthe Pakistan People's Party loss in the 2013 election, Hussain chose to stay in Pakistan. The party had been in power since 2008. The relative said Canadian government officials have been helpful so far, keeping in communication and attending one of Hussain's hearings. London Free Press, A1

*** Arabie Saoudite - Des blindés utilisés contre des dissidents n'alarment pas Dion**
Le gouvernement Trudeau a encore dû défendre mercredi le contrat de vente de véhicules blindés conclu avec l'Arabie saoudite après la diffusion de vidéos montrant que le régime utilise vraisemblablement ce type d'équipement pour réprimer des dissidents. Mais Ottawa ne s'en formalise pas puisque les véhicules en cause ne sont pas canadiens. Les images obtenues et analysées par le Globe and Mail datent de 2012 et de 2015. Elles montrent que des véhicules semblables à ceux que le Canada vendra à l'Arabie saoudite ont été utilisés dans des affrontements avec la minorité chiite dans l'est du pays. " Notre équipe d'experts regarde toujours ce genre d'information et les scrute à la loupe, a réagi en matinée le ministre des Affaires étrangères, Stéphane Dion. Si jamais ça devait être un équipement canadien [qui est utilisé contre les civils], on réagirait. Mais comme l'article le dit lui-même, pour le moment ce ne sont pas des équipements canadiens. " (…) Les révélations de mercredi ont relancé le débat sur la décision du gouvernement Trudeau d'honorer le controversé contrat de 15 milliards. En vertu d'une loi canadienne de 1947, un fabricant de matériel militaire doit obtenir l'aval du gouvernement fédéral avant d'exporter ses produits vers les pays où les droits de la personne font l'objet de violations graves et répétées de la part du gouvernement, à moins " qu'il puisse être démontré qu'il n'existe aucun risque raisonnable que les marchandises puissent être utilisées contre la population civile ". Le gouvernement a évalué que l'Arabie remplissait cette condition. Mais plusieurs organismes jugent précisément le contraire, vu le bilan du pays en matière de respect des droits de la personne. Ottawa fait d'ailleurs l'objet d'une poursuite en Cour fédérale visant à invalider le contrat. Le Devoir, A2

Will Canada give Iran a free pass?
An editorial states, "Canadians can be forgiven for missing Iran Accountability Week on Parliament Hill last week. Between the tragic fires in northern Alberta, Justin Trudeau's celebrity meet-andgreets with Prince Harry and Alex Trebek, and startling ethical revelations about Kathleen Wynne's Liberal government in Ontario, Iran Accountability Week was easy to miss. Conservative foreign affairs critic Tony Clement and Conservative Senator Linda Frum hosted the program in hopes of bringing greater awareness to the problematic elements of re-engaging with Iran. They aimed to shine a light onto the nefarious activities carried out by the Iranian regime. Greater attention should be given to the world's

biggest state sponsor of global terrorism. Financing is the lifeblood of any terrorist organization, and Iran is notorious for enabling jihadists and aiding their capacity to carry out murderous attacks. In 2012, the Harper government designated the Islamic Republic of Iran as a statesponsor of terror and expelled I ranian diplomats f rom Ottawa - regime members suspected of spying in North America. The feds named Iran's Islamic Revolutionary Guards Corps, known as the Qods Force, as being instrumental in creating, training and arming terrorist organizations including the Taliban, Hezbollah, Hamas, and Palestinian Islamic Jihad, among others. (...) But that was then and this is now. Prime Minister Justin Trudeau is taking a different approach. Trudeau's global affairs minister, Stephane Dion, implied Harper was wrong to stand up to Iran's terrorism and announced Canada will soon re-open diplomatic ties. As a part of this re-engagement, Canada may have to withdraw its designation of Iran as a state sponsor of terrorism. Calgary Sun, A15 (Edmonton Sun, Toronto Sun, Ottawa Sun, Calgary Sun)

*** Hard evidence of soft hypocrisy**

An editorial states, "The Saudi arms deal, and the Liberal government's handling of it, keeps looking worse. After inheriting from the Harper Conservatives the $15-billion sale of light-armoured vehicles, the Trudeau government did the necessary thing, and vowed to carry through with the contract. A deal is a deal, after all, argued the government. Canada can't be a reliable global partner if a new government tears up the sales agreements of the previous one. And there were hundreds of jobs at stake in the Ontario factory where the LAVs will be built. But it was a controversial deal, one that drew more criticism in January when the Saudis executed 47 "terrorists" - another word for dissidents. The mass killing refocused Canadians' attention on the country's toxic human rights ecology. Ottawa pressed on, though. A confidential Liberal government review of the deal, released in response to a lawsuit, argued that Saudi Arabia was a key Canadian ally in the region, a partner in the fight against terrorism and a bulwark against an expansionist Iran. Those realpolitik arguments, along with the threat to Canadian jobs, Canada's reputation and the benefits of Canada currently hosting thousands of Saudi university students, were used by Minister of Foreign Affairs Stéphane Dion to justify the export permits. Now The Globe has published solid evidence that the Saudis have on at least two occasions used LAVs to control and kill dissidents inside its borders. Not Canadian-built LAVs, mind you, but similar vehicles made in other countries." Globe and Mail, A12

INTERNATIONAL

Attacks kill at least 77 in Baghdad

Daesh spread carnage across the Iraqi capital on Wednesday, killing scores in bombings at two checkpoints and a busy market in what appeared to mark an escalation in attacks on civilians as the group loses ground on the battlefield. At least 77 people were killed, according to health officials. The tally is expected to rise as several people are critically wounded. The Associated Press, citing medical and security officials, said the death toll reached at least 88, the bloodiest day in the capital in several years. Daesh, also known as ISIS and ISIL, asserted responsibility for the blasts in posts distributed on social media. Toronto Star, A3

Islamic State brand losing power in U.S., FBI director says

Fewer Americans are travelling to fight alongside the Islamic State and the power of the extremist group's brand has significantly diminished in the United States, FBI director James Comey said Wednesday. The FBI encountered "6, 8, 10" Americans a month in 2014 and the first half of 2015 who travelled to the Middle East or tried to go there to join the Islamic State, but that number has averaged about one a month since last summer in a sustaining downward trend, Comey said. "There's no doubt that something has happened that is lasting, in terms of the attractiveness of the nightmare which is the Islamic State to people from the United States," he told reporters during a round-table Wednesday. He did not offer an explanation for the decline, though the FBI has worked aggressively in the last year to identify and intercept Americans who might be determined to reach Syria. One other possibility is that the Islamic State has encouraged more of its followers to carry out violence at home. The FBI still has "north of 1,000" cases in which agents are trying to evaluate a subject's level of radicalization and potential for violence. "There's still a presence online, and troubled people are still turning to this and at least being

interested in it," Comey said. "But they've lost their ability to attract people to their caliphate from the United States in a material way." Waterloo Region Record, A5

*** Migrants - L'accord UE-Turquie en danger**

L'accord sur les migrants conclu entre l'Union européenne et la Turquie traverse " un moment très dangereux ", a mis en garde mercredi à Strasbourg un ministre turc, soulignant que son pays se refusait à modifier sa loi antiterroriste comme l'exigent les Européens. " Tous les accords que nous avons conclus jusqu'à présent, basés sur la confiance, la bonne volonté, la responsabilité et la prise de risques politiques, font face à un moment très dangereux ", a estimé le ministre chargé des Affaires européennes, Volkan Bozkir, lors d'une visite au Parlement européen. M. Bozkir faisait référence aux exigences européennes pour accorder une exemption de visas aux Turcs dans l'espace Schengen. La Commission européenne a ouvert la voie le 4 mai à cette exemption, dont Ankara a fait une condition pour continuer d'appliquer son accord migratoire controversé avec l'UE. Mais l'exécutif européen a assorti son avis favorable de réserves, estimant qu'Ankara devait encore remplir cinq critères parmi les 72 fixés pour l'obtenir, dont une révision de sa législation antiterroriste, au champ trop large selon Bruxelles. Le Parlement européen, ainsi que les États membres, devront donner leur aval à l'exemption de visas, une fois qu'Ankara aura rempli tous les critères. La loi turque antiterroriste " est conforme aux standards européens ", et la modifier " est complètement impossible ", a prévenu M. Bozkir, insistant sur le fait que son pays devait faire face au " terrorisme du PKK " (Parti des travailleurs du Kurdistan) et avait subi récemment au moins cinq attentats suicide. Le Devoir, B6

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
May 19, 2016 / le 19 mai 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Des gestes « inacceptables » condamnés par le gouvernement
Le gouvernement a condamné hier les gestes « inacceptables » d'agents de la Gendarmerie royale du Canada (GRC) qui ont espionné deux journalistes de La Presse sans en avoir l'autorisation il y a neuf ans, dans l'espoir de découvrir qui leur avait révélé les plans terroristes attribués à Adil Charkaoui. À la fin du mois de juin 2007, les journalistes Joël-Denis Bellavance et Gilles Toupin avaient dévoilé dans La Presse le contenu d'une étude confidentielle du Service canadien du renseignement de sécurité (SCRS). Les espions canadiens y relataient notamment une conversation du Montréalais Adil Charkaoui, qui évoquait un plan pour détourner un avion. M. Charkaoui a toujours nié l'existence de cette conversation. La GRC avait déterminé que le document ultraconfidentiel obtenu par La Presse était authentique. Elle voulait identifier la source qui l'avait remis aux journalistes. Une enquête criminelle avait été déclenchée. Hier, le réseau CBC a fait état de nouveaux documents obtenus grâce à la Loi sur l'accès à l'information, qui révèlent que les policiers ont filé les reporters pendant neuf jours, au mois d'août 2007. Les règles d'enquête de la GRC exigent pourtant d'obtenir une autorisation spéciale pour espionner des sujets « sensibles » comme des professeurs d'université, des journalistes, des leaders religieux, des syndicats ou des politiciens. Les policiers ont lancé leur filature sans obtenir cette autorisation. Après neuf jours,

lorsqu'ils ont finalement demandé l'autorisation, elle leur a été refusée par l'officier responsable, Bob Paulson, qui est depuis devenu le grand patron du corps policier. (…) Le premier ministre Justin Trudeau a déclaré hier que la conduite des enquêteurs était « inacceptable ». Le **ministre de la Sécurité publique, Ralph Goodale**, a pour sa part répondu en Chambre à une question du Nouveau Parti démocratique (NPD) en condamnant fermement le comportement des policiers. ***« La liberté de la presse est une valeur canadienne fondamentale qui est inscrite dans la Charte. La surveillance non autorisée était entièrement inacceptable. Elle était en contradiction avec une directive ministérielle. Elle était en contradiction avec les politiques de la GRC. Elle a été stoppée quand le quartier général de la GRC en a été informé, et les enquêteurs ont été réprimandés »***, a-t-il expliqué. Interrogé par les journalistes au Parlement, le **ministre** a ajouté que le commissaire Paulson avait déjà offert personnellement ses excuses à La Presse. ***« S'il y a le moindre doute à ce sujet, le commissaire Paulson tiendra une nouvelle rencontre »***, a ajouté **M. Goodale**. ***« Nous devons travailler très fort pour nous assurer que ça n'arrive plus jamais. »*** La Presse +, 12; Canadian Press (Kingston Whig-Standard, Chronicle-Herald, Ottawa Sun, Times & Transcript, The Guardian, Cape Breton Post, Global News); Le Devoir

Mulcair veut une enquête

Le chef du Nouveau Parti démocratique (NPD), Thomas Mulcair, demande l'ouverture d'une enquête publique sur la filature dont deux journalistes ont fait les frais. Il a ainsi réagi au reportage de la CBC, qui a rapporté mercredi que des enquêteurs de la Gendarmerie royale du Canada (GRC) ont pris en filature les journalistes Joël-Denis Bellavance et Gilles Toupin, du quotidien montréalais La Presse, pendant neuf jours en août 2007. Les agents ont exercé une surveillance physique des reporters à la suite de la parution d'un article sur Adil Charkaoui, selon ce qu'a rapporté la société d'État, qui tient ces informations d'une note de breffage préparée à l'intention du **ministre de la Sécurité publique**. Le chef néo-démocrate juge que l'actuel titulaire du ministère, **Ralph Goodale**, doit déclencher une enquête publique pour faire la lumière sur cette affaire, qui représente selon lui rien de moins qu'un «scandale d'État». «Ce n'est pas quelqu'un qui a fait un petit mauvais coup là! (...) **M. Goodale** doit commander une enquête publique immédiatement», s'est exclamé M. Mulcair en point de presse dans le foyer des Communes. «Sans permission judiciaire en flagrante contravention de la loi, des agents de la GRC en train de traquer des journalistes, c'est un scandale d'État», a-t-il enchaîné. Dans un communiqué publié en après-midi, le **ministre Goodale** a semblé écarter l'idée, signalant au passage que ***«les agents responsables ont été réprimandés»***. ***«Cette surveillance a contrevenu à la directive ministérielle sur les enquêtes délicates du secteur adoptée en 2003 par le gouvernement libéral précédent (...) Les dirigeants de la GRC ont réaffirmé la politique existante, laquelle n'a pas été suivie»***, a-t-il expliqué. (…) Pour la Fédération professionnelle des journalistes du Québec (FPJQ), ces pratiques sont tout simplement inadmissibles, a écrit dans un courriel sa présidente, Lise Millette. «Cette situation n'est qu'un exemple de plus démontrant la fragilité de la protection des sources qui doit faire l'objet d'une affirmation claire de la part du **ministère de la Sécurité publique** responsable de la GRC», a-t-elle insisté. Presse canadienne (Le Nouvelliste, 39, Le Droit, La Tribune, Voix de l'Est, Huffington Post Québec); * CBC News (2016-05-18)

Security agencies flag possible pitfalls of heightened scrutiny

As the Liberals prepare to bolster a review of national spy services, two federal security agencies have flagged serious headaches that might come with more scrutiny, internal documents show. The RCMP fears more eyes looking over its shoulder could compromise criminal investigations, while the electronic spies at the Communications Security Establishment warn against creating a super-watchdog with its associated "burden and costs," say notes obtained under the Access to Information Act. The Trudeau government plans to usher in a national security committee of parliamentarians, whose members would have access to classified records. It is also studying gaps in the current web of watchdogs that monitor intelligence services to ensure a comprehensive system is in place. Existing review bodies cannot look at issues beyond their specific agency of focus, and have "limited authority" to collaborate with one another, say briefing notes prepared for **Public Safety Minister Ralph Goodale**. It means the Civilian Review and Complaints Commission, which oversees the RCMP's national security activities, might be barred from exchanging notes on an alleged scandal with the watchdog that keeps an eye on the Communications Security Establishment. (…) The watchdog who monitors the Communications Security Establishment has called for legislative changes to encourage and authorize more co-operation between his office and

the watchdog that oversees the Canadian Security Intelligence Service. Talking-point notes prepared for CSE chief Greta Bossenmaier's use last year at a Senate committee say that "changes to our review regime are ultimately a policy question and it would not be appropriate for me to comment." "I would note, however, that before moving to a 'super-bureaucracy' — with its associated burden and costs — existing review bodies should be optimized and their collaboration should be further facilitated." The notes prepared in November for **Goodale** point out that some departments and agencies involved in national security activities lack external review. The most "noticeable omission" is the Canada Border Services Agency, which has a "high number of public complaints that are currently triaged by internal mechanisms," the briefing materials say. Other federal agencies that have security responsibilities but no external review bodies are Global Affairs Canada, National Defence, the Privy Council Office, **Public Safety Canada**, and Immigration, Refugees and Citizenship Canada, the notes add. Canadian Press (Times Colonist, Sudbury, Maclean's, Metro News, Winnipeg Free Press)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Wildfire / Feu de forêt à Fort McMurray

*** Evacuee re-entry possible June 1**
The Alberta government says people from the fire-ravaged city of Fort McMurray could start going home starting June 1 if conditions are safe, but warned there will only be basic services and a partially open hospital. "Remember, many hazards remain in Fort McMurray," Premier Rachel Notley said Wednesday. Canadian Press (Red Deer Advocate, A3; Chronicle Herald; The Telegram; Charlottetown Guardian; Cape Breton Post; Times Colonist; Ottawa Sun; Hamilton Spectator, Whig-Standrad); Reuters (Toronto Sun, A56); Calgary Sun, A4; StarPhoenix, A8; Calgary Herald, A1/Front; Journal de Montréal, 7; Postmedia Network (Ottawa Sun, Toronto Sun, Edmonton Sun, Winnipeg Sun)

*** Cities should stop building in disaster-prone areas, says insurance bureau head**
The head of the Insurance Bureau of Canada says local governments need to stop developments on flood plains or near fire-prone boreal forests to prevent widespread damage from future natural disasters. Don Forgeron says the devastating Fort McMurray fire will be the costliest natural disaster in Canadian history, costing insurers somewhere between $3 billion and $9 billion. Canadian Press (The Telegram, B5; Vancouver Sun; Calgary Herald)

*** Evacuees relieved, wary over re-entry plans**
Most Fort McMurray wildfire evacuees, many of them scattered across the country, were relieved Wednesday to hear that they will be allowed to return home earlier next month. But others were wary. "We were actually evacuated on Tuesday, May 3, and we had our baby on May 4 in Edmonton, so we aren't going to be going anywhere until we're sure of what the emergency services and the critical services look like," said Stefan Sophr, a technical manager for SGS Canada. Postmedia Network (Edmonton Sun, A3; Edmonton Journal); Calgary Herald, A2

*** As fires burn, oil companies weigh profit and safety**
Major oil sands operators, bleeding cash as massive production facilities sat idle, said conditions appeared favourable enough last week to send thousands of workers back to remote camps as wildfires raged in northern Alberta's boreal forest. But within days, legions of tradespeople were packed on to buses and sent to isolated lodges north of the Fort McKay First Nation. For many, it was their first stop in a two-part evacuation - the second in as many weeks - as shifting winds and tinder-dry conditions pushed flames closer to industrial plants run by Suncor Energy Inc. and Syncrude Canada Ltd. Globe and Mail, B1

*** 'We Will Rebuild Our City'**
The massive operation to return residents to Fort McMurray is set to begin June 1, nearly a month after 88,000 people were forced to flee a wildfire still burning up much of northeastern Alberta. Premier Rachel Notley outlined her government's longawaited re-entry plan Wednesday, saying residents will soon be

allowed to return to their homes in a phased, multi-day process starting with the least damaged areas. Edmonton Sun, A3

* **Alberta Wildfires**
Re-entry to Fort McMurray and other communities will take place only when key conditions are met, including: The wildfire is no longer an imminent threat; Air quality is safe; Emergency services have been fully restored; Safe transportation to and within the community has been restored; Emergency medical care and transport, and mental health support, is available. Calgary Herald, A5

* **Step up and support Alberta wildfire victims at Zumbathon**
Three women in Fredericton have decided to dance their way to the Red Cross in support of Fort McMurray. The Fort Mac Zumbathon charity event will be held on Friday evening at the Barkers Point Elementary School gym. Daily Gleaner, A2

* **Woman who survived Alberta wildfires grateful for hot showers, clean clothes**
Erin Scott will never take hot showers and clean clothes for granted again. The Harvey woman, who was evacuated from her Fort McMurray home on May 3, flew into Fredericton early Tuesday morning. Daily Gleaner, B4

* **Wind, low humidity, help northern Alberta wildfire make big one-day jump**
There has been a dramatic increase in the size of a northern Alberta wildfire that has already destroyed hundreds of structures in Fort McMurray and is now licking close to the boundary with Saskatchewan. An overnight report from Alberta Sustainable Resource Development says the blaze has now covered more than 4,200 square kilometres. Canadian Press (Daily Star, 10)

* **Shaw Charity Classic to help Fort Mac kids**
Some of the biggest names in golf had Fort McMurray on their minds. Shaw Charity Classic executive director Sean Van Kesteren happened to be in Houston two weeks ago for a PGA Tour Champions stop in that city, and several of the senior stars mentioned to him that they had been following the gut-wrenching wildfire news from northern Alberta. Calgary Herald, B12

* **Des Acadiens disent être forcés de travailler malgré la fumée et le feu**
Les incendies de forêt qui ravagent le nord-est de l'Alberta font craindre le pire à plusieurs travailleurs de Fort McKay, qui estiment être pris au piège alors que l'immense brasier se trouverait à moins de 40 km de leur lieu de travail. «C'est insensé de devoir travailler alors que le feu qui vient de détruire le camp BlackSand n'est qu'à 38 km d'ici», déplore un travailleur d'origine acadienne qui s'est confié mercredi à l'Acadie Nouvelle. L'Acadie Nouvelle, 3

* **Ford gives $500K fore fire relief**
Ford Motor Company of Canada and Canadian Ford dealers are donating more than $500,000 to the Canadian Red Cross for relief and recovery efforts related to the severe wildfires in Fort McMurray and surrounding areas, the company announced Tuesday. Windsor Star, SR2

* **Fort Mac refugees have trucks, belongings stolen**
Two people fleeing the wildfire that ravaged Fort McMurray, alta., have had their belongings stolen in saskatoon. Police say the couple's two pickup trucks were taken over the weekend from a hotel parking lot. Canadian Press (Ottawa Sun, A5); StarPhoenix, A2

* **Shaw Classic among golf entities helping Fort McMurray relief**
Some of the biggest names in golf had Fort McMurray on their minds. Shaw Charity Classic executive director Sean Van Kesteren happened to be in Houston two weeks ago for a PGA Tour Champions stop in that city, and several of the senior stars mentioned to him that they had been following the gut-wrenching wildfire news from northern Alberta. Calgary Sun, S2

* **Feux hors de contrôle à Fort McMurray Les habitants devront encore attendre**

Le retour progressif des dizaines de milliers d'habitants évacués de Fort McMurray, au coeur d'une région ravagée par les feux de forêt, a été repoussé au 1er juin en raison de foyers d'incendie toujours actifs mercredi autour de la ville pétrolière. Agence France-Presse (Le Droit, 25)

*** Researcher tracking health of firefighters**
A researcher has started tracking the health of firefighters helping battle the massive wildfire in Fort McMurray, Alta. Nicola Cherry, an occupational epidemiologist at the University of Alberta, is taking blood, urine and breath samples of firefighters as they return from northeastern Alberta in a mobile laboratory she received two weeks ago. Red Deer Advocate, A3; Postmedia Network (Edmonton Journal, A1/Front; Calgary Herald)

*** B.C. premier says climate change is sparking need for national forest fire plan**
Climate change is leading to more wildfires and the country needs a national forest firefighting strategy, says B.C. Premier Christy Clark. While the country has been transfixed by the raging fires around Fort McMurray in northern Alberta, British Columbia's interior is experiencing similar fire conditions this spring that have received far less attention. Canadian Press (Red Deer Advocate, A3; Times Colonists; Globe and Mail)

*** Wildfire fails to torch Ewashko family's spirit**
The fire came in waves at Howard Ewashko's family business: once on Tuesday afternoon, again in the evening. Both times, Ewashko, his brother Craig, and a small band of workers at the sawmill north of Fort McMurray saw the "beast" of a wildfire threaten their operations, before it turned back. Calgary Herald, B1/Front

*** Winnipeg musicians expect to raise $10K for Fort Mac, other wildfire victims**
Winnipeg musicians, including members of Harlequin, Doc Walker and Slow Motion Walter, will be rocking out Thursday night at Nashville's Bar Winnipeg on Regent Avenue in support of those affected by the Fort McMurray wildfires. CBC News

*** In Fort McMurray, a struggle to keep the phone lines open**
As wildfires ripped through Fort McMurray, telecom providers in the city have grappled with power outages, fuel shortages and the threat of losing key pieces of infrastructure as they worked to keep communications services online for emergency responders and the eventual return of their customers. Telus Corp. and Shaw Communications Inc. are the two main operators in the area and both have crucial structures in the heavily damaged Beacon Hill neighbourhood. With widespread power outages in the area, they have been forced to rely on generators and faced challenges refuelling, especially during the height of the blaze. Globe and Mail, B1

*** Wildrose leader unsung hero in Fort McMurray**
An opinion piece states, "If you think Premier Rachel Notley has done a good job reacting to the Fort McMurray fire, spare some applause for an overlooked political player in this drama: Wildrose Leader Brian Jean..." Edmonton Journal, A12

*** Climate and Wildfires**
A letter to the editor states, "I've been accused of being insensitive for writing about the climate irony of the Fort McMurray wildfire, which continues to dominate the news in Canada. Many people have argued that now is not the time to discuss global warming and climate change. I insist that now is precisely the right time to make the link between epic wildfires and climate change..." Winnipeg Sun, A12

*** "It's just the weather, not climate change**
A letter to the editor states, "Re: "Alberta government preparing for climate related disasters," May 17. There seems to be some confusion between "weather" and "climate." Climate is defined as the long-term weather, so any impending climate-related disasters will emanate from solar hibernation causing the Earth to cool for at least 20 to 30 years..." Calgary Herald. A17

Other / Autres

* **Flood plan lacking: audit - Feds' effort to rebuild flooded First Nations communities disorganized**
The federal government's effort to rebuild four communities so evacuees from flooded First Nations could return home is disorganized, poorly resourced and plagued with delays, an audit of the program found late last year. The audit of Operation Return Home paints an unflattering portrait of how Indigenous and Northern Affairs Canada stepped up after thousands of indigenous Manitobans were forced out of their homes in May 2011. The audit reviewed INAC's response to the flooding between April 1, 2013 and Sept. 30, 2015. Winnipeg Free Press, A3

* **Nuclear is the missing link in our climate debate**
An average-sized nuclear plant produces roughly the same amount of electricity from 4,000 wind turbines. So reports the International Energy Agency. A few dozen windmills, let alone a few hundred, can often be counted on to create a public furor in the area where they are built. Just ask the mayors in eastern Ontario where the provincial government is approving windmills over furious local objections. Globe and Mail, A13

* **Lifeline to Safety**
A helicopter whipping wind and water hovers directly above your boat, lowering a rescue basket while raising your adrenalin. And you can't help but think: Welcome to a day at the office, coast guard-style. The Canadian and U.S. coast guards conducted a joint medicalevacuation training session in the western base of Lake Erie this week, creating awareness for water safety just ahead of Safe Boating Awareness Week, which begins Saturday. Windsor Star, A2

* **Plenty of campsites left for May long weekend, province says**
Roll out your sleeping bags and pack the marshmallows. The unofficial kick off to summer camping season in Manitoba looks to be a good one...The Mantario hiking trail remains closed due to the wildfires in the area. CBC News

* **Forest fire evacuation alert cancelled**
Residents of a town northwest of Edmonton are no longer under immediate threat of a forest fire. Alberta Emergency Alert cancelled a two-hour evacuation alert for people in Fox Creek and those who live south of the hamlet of Little Smoky. Red Deer Advocate, A3

* **Thick smoke forces cancellation of La Loche culture camps**
Dozens of La Loche youth are disappointed that forest fire smoke has caused the cancellation of their cultural camps. "Obviously the kids are bummed. They were looking forward to it, but it's the safest thing," said Leanne Gailey, assistant principal of La Loche Elementary School. StarPhoenix, A3

* **Dawson-area blaze remains active**
No new wildfires were reported Tuesday in the territory. The lightning-caused fire near Hunker Creek, 24 kilometres southeast of Dawson City, remains active, Yukon Wildland Fire Management officials reported today. Daily Star, 5

* **Man pinned under truck for 32 hours**
A B.C. man has survived a 32-hour ordeal pinned under a pickup truck on a remote road north of Kamloops. Simpcw First Nations elder Roy Lampreau left his Barrierearea home on Monday morning to look for firewood...Search and rescue crews from Kamloops and Merritt also arrived before a band member found Lampreau on a remote road with his leg pinned under one of his truck's tires. Lampreau is recovering from the ordeal, Matthew said. Canadian Press (Times Colonist, A5)

* **Poll suggests Calgarians oppose Springbank dam**
It's not just landowners in Springbank opposed to a dry reservoir on rural land west of Calgary, a new poll suggests. The survey commissioned by the group Don't Damn Springbank reached out to Calgary residents for their opinions, and found 55 per cent of respondents prefer a dry dam in McLean Creek over the Springbank proposal as the best option to prevent future flooding in the city. Calgary Herald, A8

*** New faces sought for important work**
The people you hope to never need are looking for new recruits. The local branch of the Canadian Coast Guard Auxiliary is looking for new volunteer members for the upcoming season according to local unit leader and district training co-ordinator for Nunavut and the NWT Paul MacDonald. Inuvuk Drum

*** Search continues for missing Red Deer woman (MIGHT BE DUPLICATE IN LE)**
Police are continuing to search for a Red Deer woman who has been missing for three months. Police have also undertaken ground searches in Red Deer over the past three months with support from search and rescue teams, Police Dog Services and the RCMP helicopter. Red Deer Advocate, A5

*** If disaster strikes, would you be ready?**
An editorial states, "Picture this. You're at work when Mother Nature begins throwing a tantrum. Maybe it's a winter storm of historic proportions. Maybe it's torrential rain, enough that local creeks and rivers flood their banks and streets are flooded. Maybe it's violent hail, power outages and transportation gridlock. Maybe it's an ice storm…" Canadian Press (Cape Breton Post, C1)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Liberals expected to take summer to consult on Bill C-51 changes**
The Liberals have yet to repeal controversial anti-terrorism law C-51 seven months after taking office, and are now poised to carry out consultations over the summer to see what changes Canadians are looking for. Global News (2016-05-18)

*** Wanted: One spy agency whistleblower**
An opinion piece states, "Canada's digital spy agency, the CSE, has refused to release to *The Toronto Star* the number of privacy violations they've incurred since 2007. *The Star* only requested the number of privacy violations. No personal details, no details at all. Just "How many times did you guys mess up?" And the CSE refused because they said it would "provide insight into" its operations. What possible insight can you get from the number of privacy violations? Is that number the missing link in the terrorists' plan to blow up the parliament buildings? Is it the code they need to hack into the mainframe? More likely, the CSE is afraid of the one actual insight you could get from the number of privacy violations, which is "Wow, that's a lot of privacy violations. Maybe we should do something about that." This comes shortly after the revelation that the CSE shared an unknown number of Canadians' internet activity records with foreign countries for a "number of years." Which is barely a bigger outrage than the fact they mass collect our internet activity records. But the outrages will keep coming, because this huge, secret agency has no meaningful oversight. And when powerful people act with impunity, injustice predictably follows. So if there's a Canadian Edward Snowden and you're watching this, it's time to blow the whistle. And if you do, I will reward you with this coupon for 100 free foot massages. You can be a guy or a girl, doesn't matter. But it expires in 2017, so… clock's a-tickin." Rabble (2016-05-18)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

It's simple: Migrants don't belong in jail
Canada, stop jailing innocent migrants. Just stop. It's not hard. The Canadian government may not resettle another 25,000 Syrian refugees in coming years. It might disappoint many Canadians, but even if the difficulty of an important undertaking isn't sufficient reason to forego it, difficulty is at least a reason. Canada could easily, however, stop habitually detaining immigrants and refugees, including children. There is no reason not to quit. Every year, Canada throws a large town's worth of migrants in maximum- and medium-security prisons and in prison-like "holding centres." It held 7,300 people in 2013 and 8,500 in 2014, on average for a few weeks. It can jail a child. It can jail her for as long as it likes. It decrees that under certain circumstances, it must jail her. And it need not recognize her as "innocent until proven guilty" - she is charged with no crime, after all - but can force her to prove that she deserves to be released from her cell. It should stop doing that. Just stop it. Knock it off. It's so easy. Other countries

don't do this. The Global Detention Project has called Canada an outlier on detention for immigrants and refugees among industrialized democracies. Most countries that Canada might want to be compared to, it notes, somehow manage not to routinely jail migrants or create mandatory detention laws. Kingston Whig-Standard, A4 (London Free Press)

Skimpy Savings
Offering to accept the Canadian dollar at par, Bellis Fair Mall in Bellingham hopes to persuade Canadians to make a cross-border shopping trip during holiday long weekends. It's easy to understand why: Southbound crossings at Blaine, Lynden and Sumas were down about 12 per cent in March 2016 compared with the same month in 2015 and retail sales in Bellingham have slumped. We'd like to help out, but is it worth the trip? A $500 purchase in the U.S. would cost $613.88 at the current exchange rate. Because Bellis Fair is giving our 77-cent US dollar equal standing with the U.S. currency, you save $113.88. However, for a single day trip, there are no personal exemptions on duty and taxes on returning to British Columbia. And bear in mind that duty is based on where products are manufactured, not where they were purchased. Also, both duty and taxes are calculated in Canadian dollars. So, if that US$500 is spent on apparel manufactured outside NAFTA, duty and taxes amount to $197.42, more than offsetting any exchange rate savings. Vancouver Sun, A12

*** Canada Border Services Reminds Legal Permanent Residents Travelling to Canada by Air of eTA Requirements**
The Canada Border Services Agency ("CBSA") issued a reminder to Lawful Permanent Residents ("LPRs") of the United States regarding new guidance for travelling to Canada by air. The Electronic Travel Authorization ("eTA") is a new Canadian entry requirement for visa-exempt foreign nationals travelling to Canada by air, which went into effect on March 15, 2016. Visa-exempt foreign nationals who fly to or transit through Canada are expected to have secured eTA first. Exceptions to this requirement include U.S. citizens and travelers with a valid Canadian visa. LPRs of the United States need an eTA before boarding a flight to Canada as of March 15, 2016. Until September 29, 2016, travelers who do not have an eTA can board their flight, as long as they have appropriate travel documents, such as a valid passport. The Border Services officers can admit travelers without an eTA into the country, but they will remind travelers of the new requirement. LPRs travelling to Canada should apply for an eTA, which costs $7 Canadian. In most cases, an eTA is granted within minutes of applying. National Law Review

*** La mairesse de Syracuse reçoit l'UMQ**
La délégation de la mission économique organisée par l'Union des municipalités du Québec (UMQ) dans l'État de New York a effectué un premier arrêt à Syracuse, en fin de journée mercredi, où la mairesse Stephanie Miner a brièvement expliqué les raisons qui devraient favoriser le développement de relations d'affaires entre les deux régions. Avocate spécialisée en droit du travail, l'élue démocrate a entrepris sa carrière politique comme conseillère municipale en 2001. Elle se retrouve à la tête d'une ville qui affiche le plus haut taux de pauvreté chez les populations noires et hispaniques. Entre 2009 et 2013, plus d'une personne sur trois à Syracuse vivait sous le seuil de la pauvreté. Par contre, cette région est favorisée par de nouvelles occasions d'affaires, témoigne la mairesse. «Les infrastructures et les échanges commerciaux sont des enjeux constants pour nous, en raison de notre situation géographique, à mi-chemin entre le Canada et la ville de New York, la porte d'entrée du monde. Au moment où s'ouvre le canal de Panam [les nouvelles écluses], où de plus en plus de biens traversent notre pays et de plus en plus de biens transigent aux ports à New York et au New Jersey, des endroits tels que Syracuse, Rochester et Buffalo observent différentes façons pour introduire les biens vers les marchés. Gardez cela en tête, quand vous vous demanderez de quels biens avez-vous besoin ou comment pouvez-vous en envoyer plus rapidement.» Le Soleil, 27 (Le Quotidien, Le Nouvelliste)

*** American 'cheese glut' could impact Canada's dairy farmers**
"Save your country, eat three more pounds of cheese!" It's a rallying cry every American needs to get behind if they want to consume the country's surplus of the good stuff. With America's dairy industry expected to produce a record 212.4 billion pounds of milk this year – the most, ever – that overflow is funneling towards cheese makers who have clinched their own record: 1.19 billion pounds of cheese in commercial cold storage.Unfortunately, as attractive as guilt-free patriotic cheese munching sounds to our neighbours to the south, that surplus could spell trouble for Canada's dairy farmers, says Sylvain

Charlebois, dean of the faculty of management and professor in food distribution and policy at Dalhousie University. The potential issues centre around something called diafiltered milk, a U.S. protein used as a stand-in for milk in cheese. On the one hand, the Canadian Border Services Agency classifies diafiltered milk as a protein ingredient, whereas the Canadian Food Inspection Agency considers diafiltered milk as milk. "Canada has been importing a lot of diafiltered milk into [the country] – that could actually put some pressure on the dairy industry in Canada, enticing processors to import even more," says Charlebois. In late April, NDP agriculture critic Ruth Ellen Brosseau took to the Parliamentary steps with 200 Quebecois dairy farmers (the province is home to nearly half of the country's dairy farms) to protest the importation of diafiltered milk, calling on the house to "recognize the magnitude of the economic losses to Canadian dairy producers from the importation of diafiltered milk, which totaled $220 million in 2015." Yahoo Finance

*** Only Toronto, Ottawa accept more Syrians than London**

Health care. Insurance. Junior hockey. Those are some of the things London does well. But as a new city hall report outlines, we're also really good at something else - taking in refugees. London, according to a staff report headed to a city council committee, has accepted the third largest number of Syrian refugees of any Ontario municipality. Only Toronto and Ottawa have taken in more newcomers from the war ravaged nation. "We have infrastructure, we have quite a number of community organizations, social service supports, and we mobilized quickly," said Valerian Marochko, head of the Cross Cultural Learner Centre, a resettlement agency that's taken a leadership role in the local response to the refugee crisis. "It doesn't surprise me London accepted a great bulk of the refugees. We've always been a caring community," said Coun. Virginia Ridley, who chairs the community and protective services committee getting the report next Wednesday. "It's just a reflection of what kind of community I know London to be." Canada began receiving its first 25,000 Syrian refugees in December, hitting that target in March. In raw numbers, 1,110 refugees have arrived in London. Another 381 are in the pipeline - their applications are in progress. On top of those, another 661 Syrian refugees will be here by the end of this year, counting individuals and families fr om all the different refugee categories. "The community has responded very positively," the report says. Dhira Ghosh is events co-ordinator for the London Arts Council and the London Heritage Council, both of which teamed up with the Cross Cultural Learner Centre to help refugees get used to London's cultural environment. She says the city's size - not too big, not too small - may have worked in its favour. "I think London was a little bit more nimble-footed" than larger centres, Ghosh said. London Free Press, A3

Windsorites need to embrace and invest in bicycling now: With change today comes opportunity, Lori Newton, Tom and Sue Omstead write

Once the hub of all things to do with motorized vehicles, Windsor-Detroit has a chance to be the same for non-motorized vehicles. Windsor can no longer afford to continue to operate the way it did 40 years ago. Change is here and with change comes opportunity. We must take advantage of the global movement to reduce our carbon footprint and create pedestrian and bicycle friendly communities connected through green corridors. The future is neighbourhoods where everyone - from 8 to 80 - can enjoy a healthier, more independent lifestyle that doesn't depend on owning a car. Canada and the U.S. are investing heavily in cycling. The Trans Canada Trail is a 24,000-kilometre network that will link over 1,000 communities and the Atlantic, Pacific and Arctic oceans by the end of 2017. The U.S. already has over 18,000 km of interconnected bike routes in 23 states, including Michigan. (…) Windsor could tap into that movement. Instead, local bicyclists riding a 200-km loop of Essex County to raise funds for the ALS Society in June will have to bypass Windsor because organizers couldn't find a safe, efficient cycling route through the city. Opportunity lost. Where to begin? Support a bike lane on the Gordie Howe International Bridge and the pedestrian/bicycle ferry proposal to connect downtown Detroit to downtown Windsor. Connect the missing link between the Ganatchio Trail and Windsor's beautiful waterfront so cyclists can safely travel the full length of Riverside Drive. Windsor Star, A8

Canada: Beware the Trump Doctrine

An opinion piece states, "Needless to say, Republican presidential nominee Donald Trump is a polarizing figure. Having just returned from the U.S., the contorted body language of everyday citizens spoke volumes as I carefully asked them about their thoughts on The Donald. Many of the expletive-filled replies are not suitable for print in a reputable newspaper. The operative words were "America first" and

"American exceptionalism." "My foreign policy will always put the interests of the American people and American security above all else. It has to be first. Has to be. That will be the foundation of every single decision that I will make," he explained. (…) Still, it would not be a stretch to suggest that the Trump doctrine could have important repercussions for Canada and the Trudeau government. Reading between the lines, you could expect a Trump White House to push Canada hard on its lack of defence spending and its non-commitment to ballistic missile defence for North America. His administration would no doubt be difficult to deal with on the trade front (get ready for a rough ride on softwood lumber and the NAFTA trade pact), on securing U.S. engagement in the world generally and the United Nations specifically (particularly given Trump's isolationist proclivities), and, most significant, on matters involving the thinning out of the Canada-U.S. border (no wall perhaps, but a further thickening of the border space)." Guardian, A7

*** Let's raise the bar for New Canadians: It's hard to understand the Liberals' rationale for changes to citizenship**

An opinion piece states, "Welcome to Canada! Now, here's what we expect. We expect you to at least have the intention of living here and not treat a Canadian passport as an insurance policy. We expect that your commitment to Canada includes paying your fair share of taxes. We expect that if you can't speak one of Canada's two official languages that you will do all you can to gain a working knowledge of it, regardless of your age. That means more than just taking language classes. We expect you to try to speak English or French whenever you can so you're not exiled into a language ghetto or complicit in building one. Because you can vote here, we expect that you'll pay at least as much attention to the local news as you do the news from your homeland. And we do not expect, but we hope, that your interest in your homeland will diminish as the years go by. We expect that you learn more about Canada than the minimum required to pass the citizenship test. Canada is no more the place that you came from than it is the United States or even the Canada you might think you know from television and the movies. We expect you to recognize the falsity of the notion that Canada is a young nation. It is not. It is now one of the world's oldest nations. Since its founding 149 years ago, millions of Canadians have forged a distinct culture through hard work and idealism. A mosaic is the symbolic way we express that Canada is a country of immigrants. But it is not a blueprint for a society where each different cultural, religious or ethnic community lives side-by-side but without touching. The mosaic symbolizes the respect Canadians have for diversity that's been codified in the Charter of Rights and Freedoms. But being part of a mosaic also means recognizing that individual citizens and even particular groups are only part of the larger whole." Vancouver Sun, A3

*** Lay blame where it rightly belongs**

An opinion piece states, "Re: Blame Ottawa for Nicola's deception, by Jennifer Shabo, May 11. Jonathan Nicola is not a child. He is a 30-year-old man who plotted, planned and cajoled his way into Canada. He lied again when he completed immigration forms requesting money for assistance. Money to which he was not entitled and that is fraud. He continued to lie until he got caught at the U.S. border. If Jennifer Shabo thinks that Ottawa is to blame, she should sit through the thousands of fraudulent applications such as Jonathan Nicola's who are very accomplished liars and frauds. There are many legitimate immigrants who are waiting for their final documents so that they can begin the process of becoming Canadian citizens. I have such a friend and it angers me that frauds like Jonathan Nicola make it more challenging for the immigration workers to process the legitimate applications. I commend Citizenship and Immigration Canada for its hard work. The liars and fraudsters are to blame, not that department." Windsor Star, A8

U.S. officials seize $4,000 fraud cash

U.S. customs officers have intercepted $4,000 mailed to fraudsters by a Canadian senior who fell victim to a phone scam. "Every year, thousands of people lose money to telephone scams - from a few dollars to their life savings," said David Beculheimer, acting port director with U.S. Customs and Border Protection. "Scammers will say anything to cheat people out of their money. Everyone's a potential target." Officers working at the Fort Street cargo facility found a parcel on April 26 that was sent through United Parcel Service. It contained $4,000 in Canadian cash. It was destined for Kentucky. But officers determined the address listed wasn't real and had links to previous fraudulent activity. RCMP investigated and determined the person who shipped the package lives at a nursing home in Canada. Customs and

Border Protection said the person fell victim to a criminal organization that preys on the elderly. Customs and Border Protection seized the cash and the book. The RCMP will help get it back to the victim. Windsor Star, SR2

CYBER SECURITY / CYBERSÉCURITÉ

*** Tax deadline gaffe cost Canada Revenue Agency estimated $1.5 million**
The taxman had to forgo as much as $1.5 million in interest when the Canada Revenue Agency extended last year's tax filing deadline after mistakenly giving the wrong date. Agency officials estimated that moving the income-tax returns deadline to May 5, from the usual April 30 midnight deadline, meant $1.43 million in lost interest from Canadians who filed their taxes late over those five days, according to documents released under the Access to Information Act. The information comes more than a year after the Star first requested details about the error that likely resulted from repeating an old message, or possibly copying and pasting information from 2014, when a five-day extension was granted to taxpayers due to a hacking incident. The $1.43-million figure assumes all tax payments - totaling $2.09 billion - were late by five days, based on a five-per-cent interest rate, but the CRA said it has no way of knowing what the true financial impact was. By May 6, it had received 24.7 million individual tax returns, in line with projections. The $1.43-million estimate was provided to show "a worst-case scenario," CRA spokesman David Walters said in an email. "It is not possible to determine the exact cost as we do not know when individuals would have filed and paid their taxes, if the extension had not been granted," Walters said. Last April, the agency did not disclose cost implications, stating that "given the extended period is short, and most taxpayers filed by April 30, the costs resulting from the filing extension will be negligible." Toronto Star

*** LinkedIn: Hacker stole more user passwords**
LinkedIn said Wednesday a 2012 breach resulted in more than 100 million of its users' passwords being compromised - vastly more than previously thought. The business social network said it believes to be true a purported hacker's claim that 117 million user emails and passwords were stolen in the breach, up from the 6.5 million user credentials that the company originally said were compromised. Those 6.5 million passwords were reset in 2012 and the company advised the rest of its users to change passwords, too. The hacker, who goes by the name "Peace," was trying to sell the passwords on the dark web for five bitcoin, or about $2,200 US, according to a Forbes report. Times Colonist, D9; London Free Press (Kingson Whig-Standard, Cape Breton Post, Telegram)

*** U.S. intelligence: Foreign hackers spying on campaigns**
The United States sees evidence of hackers, possibly working for foreign governments, snooping on the presidential candidates, the nation's intelligence chief said Wednesday. Government officials are assisting the campaigns to tighten security as the race for the White House intensifies. The activity follows the pattern set in the last two presidential elections. Hacking was rampant in 2008, according to U.S. intelligence officials, and both President Barack Obama and Mitt Romney were targets of Chinese cyberattacks four years later. Nevertheless, cyber experts say Donald Trump and Hillary Clinton's campaign networks aren't secure enough to eliminate the risk. "We've already had some indications" of hacking, James Clapper, director of national intelligence, said Wednesday at the Bipartisan Policy Center in Washington. He said the FBI and the Department of Homeland Security were helping educate the campaigns. Of the attacks, Clapper predicted, "we'll probably have more." The revelation comes after Clapper's office released a document this month saying foreign intelligence services tracked the 2008 presidential election cycle "like no other." The document was in a slide show used to warn incoming Obama administration officials that their new jobs could make them prey for spies. Times & Transcript, B4 (ChronicleHerald)

*** Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat**
A Bangladeshi central bank official's computer was used by unidentified hackers to make payments via SWIFT, and carry out one of the biggest-ever cyber heists, a Bangladeshi diplomat said on Thursday at the end of a Philippine Senate inquiry. There were certain indications about who the hackers were, Bangladesh Ambassador John Gomes told a panel looking into how the $81 million in stolen money

ended up in the Philippines, citing information shared by the U.S. Federal Bureau of Investigation. Gomes said the hackers were neither in the Philippines nor in Bangladesh, but he had no other information. Yahoo Canada News (Yahoo Tech News)

*** Hong Kong launches fresh plan to fortify cyber security after SWIFT heist**
Hong Kong's central bank has a launched a new program to strengthen lenders' ability to protect their critical technology systems after recent attacks by unidentified groups on a global messaging system used by the financial community. The Hong Kong Monetary Authority's latest measure, known as the "Cybersecurity Fortification Initiative (CFI)," plans to raise the level of cybersecurity at banks in Hong Kong through a three-pronged approach and follows similar steps taken by its counterparts from London to Vietnam. The FBI, authorities in Dhaka and private forensic experts are investigating the February cyber heist in Bangladesh where thieves raided a central bank account kept at the Federal Reserve Bank of New York, stealing $81 million. Yahoo Tech News (Times of India)

*** TeslaCrypt no more: Ransomware master decryption key released**
TeslaCrypt's master key has been released to the public, shutting down the ransomware for good in an unexpected twist in the malware's story. TeslaCrypt, which often targets gamers, lands on systems through malicious downloads, web domains which load exploit kits and phishing campaigns. As ransomware, TeslaCrypt will infect systems and encrypt user files, sticking up a landing page and removing access to the PC until a ransom is paid, usually in virtual currency Bitcoin. What made TeslaCrypt a particularly severe case is that the developers behind the malware were very active, and researchers found it difficult to crack the software before new, even more sophisticated versions were released into the wild. After posing as a victim of the ransomware, an ESET researcher used the support chat system on the payment website to ask if they would consider releasing the master TeslaCrypt decryption key. While you might expect the cybercriminals to laugh at such an idea, they did not -- and instead they agreed to do so and posted it on the website for all to use, closing the payment system on the website in the process. ZD Net

*** Flaws in networking devices highlight tech industry's quality control problem**
Security flaws discovered in common networking equipment could give malicious hackers a direct pipeline into data centers and business applications, even allowing them to remotely turn off power to critical information systems and industrial machinery. Researchers at the Georgia cybersecurity firm BorderHawk revealed to Passcode that vulnerabilities in a widely used type of business hardware known as remote power managers (RPM) may affect thousands of companies across the country. BorderHawk would not reveal the name of the company that makes the flawed hardware. But it is advising businesses, which often rely on these kinds of network-connected devices to remotely manage equipment, to ensure they aren't accessible from the Internet and to make sure they have been updated with newer software and firmware. Christian Science Monitor

LAW ENFORCEMENT / APPLICATION DE LA LOI

Call public inquiry over Mountie monitoring of journalists
NDP Leader Tom Mulcair says a public inquiry should be called after it was revealed Mounties monitored two journalists in 2007. Mulcair's comments come after CBC News reported a rogue group of RCMP officers investigating a leak of a secret document spied on the two for more than a week without authorization. The report, based on a government briefing note obtained by the broadcaster, says Mounties placed two Ottawa-based journalists, Joel-Denis Bellavance and Gilles Toupin, under physical surveillance for nine days in 2007. CBC also says the surveillance was carried out without the required permission of Bob Paulson, an acting assistant commissioner at the time. Paulson is now the commissioner of the RCMP. Red Deer Advocate, B5; Toronto Star, A9; Journal de Montréal, 26

*** Bust cost hundreds of thousands for drug buys, covert agent**
Over the final four months of Operation J-Tornado in 2014, RCMP spent $104,000 buying drugs from two Saint John-based drug distribution networks, according to one of the RCMP sergeants in charge of the operation. The expense was just a fraction of what was needed from taxpayers to execute what lead to

what investigator Sgt. Marco Vachon said was an unprecedented infiltration of previously impenetrable criminal organizations. The covert police agent who made everything possible was paid more than a half a million dollars, Vachon said. Details about the cost of the operation were presented during Vachon's testimony at the trial of two men alleged to be part of one of the networks - Shane Stephen Williams, of Smithtown, and Joshua Eldon Kindred, of Saint John. Vachon took the stand on Tuesday afternoon and spent the entirety of Wednesday continuing with his evidence. Revealing his version of how the RCMP infiltrated the networks that resulted in the arrest of dozens in September 2014, Vachon gave many details not yet heard at trial, including that the agent's contract was for $525,000 and the price expensed for drugs. Vachon said the agent opened a door to the organizations that, between the start of the investigation in November 2011 and the late winter of 2014, police hadn't been able to pry open. Police could conduct surveillance and build covert sources, Vachon said, but specially encrypted Blackberry devices kept them from getting any dirt they could take to court on the heads of the networks. "It was two-and-a-half years of probing, two-and-a-half years of trying to figure out what's going on. It was frustrating, because we had intelligence the group was using communication devices the RCMP could not intercept," said Vachon, providing what he called the "Reader's Digest" of 2011 to early 2014. Telegraph-Journal, B1

Accused admitted role in Edmonton slaying during first meeting, undercover Mountie testifies
The very first time he met him, accused killer Shawn Wruck revealed to an undercover RCMP officer that he had been involved in the slaying of his former girlfriend, court heard Wednesday. Testifying at Wruck's first-degree murder trial, the officer identified as C said Wruck and his current girlfriend had come for dinner and drinks at the Kelowna, B.C., condo where he and another undercover officer were staying as part of a Mr. Big sting operation. The officer testified he told Wruck a story about having a former girlfriend who had caused him lots of grief and said Wruck responded by saying "he had one and got rid of her." C told court he asked Wruck what he meant and said Wruck replied "Dead," then explained that he had two women who belonged to the Redd Alert native street gang come over and choke the woman to death, and then he "dumped the body." The officer testified Wruck pantomimed the killing using a choking motion with his hands and then rolling his eyes to the back of his head and then said he watched "her life leaving her." The officer cannot be named under a court-ordered publication ban and the courtroom itself was closed to the public, with only accredited media being allowed in by sheriffs guarding the entrance. Edmonton Journal, A4 (Edmonton Sun)

Man arrested after 911 call of rifle near school
A 21-year-old Digby man was arrested Tuesday after a 911 call about a person carrying an assault rifle and duffel bag near Digby Elementary School. Officers responded at 2 p.m. and the school's doors were locked as a precaution. An unarmed man was quickly located by police on the trails near the school and arrested without incident. Police also located a semi-automatic rifle, ammunition and a bag in woods close to where he was arrested. The man is facing several firearms-related charges and will appear in Digby Provincial Court at a later date. RCMP spokeswoman Cpl. Jennifer Clarke said the man was unarmed at the time of his arrest. She also downplayed any risk to the children. "There was no harm intended but it was in proximity to the school," said Clarke. Any gun sighting near a school is treated seriously. Clarke said several officers responded and a police dog unit was called. Tri-County school board superintendent Lisa Doucet said the incident was short-lived. "We are always cautious in any situation, so our students and staff practise the protocols around hold-and-secures and lockdowns." She said staff handled the situation, followed protocol, worked with the RCMP and communicated with parents. Chronicle-Herald, A4; * Truro Daily

Les proxénètes et les clients, eux ?
On dirait qu'on a passé l'hiver à chercher des adolescentes qui avaient fugué de leur maison, d'un centre jeunesse, Et qu'elles disparaissent comme ça, pour rien. Enfin, on sait à peu près comment ça se passe. La séduction d'un « ami » lié à un gang de rue ; le party pendant quelques jours(…) Ainsi vont les budgets de police, ainsi vont les statistiques. Comme les budgets sont limités, on concentre les ressources sur les priorités. Tantôt, c'est le crime organisé italien, tantôt les motards, tantôt les crimes économiques, tantôt les agressions sexuelles, tantôt le trafic de stupéfiants ou les vols de banque, selon les époques. La semaine dernière, un officier de la GRC déplorait publiquement l'assèchement des budgets contre la lutte au crime organisé : tout va à la lutte contre le terrorisme, disait-il. Plusieurs autres escouades se plaignent exactement de la même chose. (…) On n'a jamais vu un corps de police déclarer

qu'il avait suffisamment d'argent, c'est entendu. Il n'y a pas de limite à la lutte contre le crime. Dans le cas des fugues des centres jeunesse, un rapport commandé par le gouvernement cet hiver indique une augmentation des cas. La Presse +, 14

Montreal police to try out cameras on 30 officers
Smile, you could be on candid camera the next time you encounter a Montreal police officer. The introduction of portable cameras, or body cams, was announced Wednesday by Mayor Denis Coderre and Montreal police chief Philippe Pichet, who both hailed the pilot project as a step forward in modern policing practices. The pilot project will involve about 30 officers who will be identified with a "Camera" badge on their uniforms. The first phase of the project will see cameras worn by officers patrolling the métro and those doing traffic duties in the southern district of the city. A second phase, in the fall of 2016, will see cameras introduced at two or three stations, where police interventions could possibly take place in private spaces. The impact of body cams on police/citizen relations, program costs, privacy issues and other concerns, will be evaluated in March 2017 by the city, followed by a public consultation. The decision whether to expand the use of body cams across the Montreal police department will come after recommendations are presented to the city in May 2017. Coderre said the use of body cameras is nothing new in the modern North American context, and Montreal now becomes the first city in Quebec to experiment with the technology. "Boston, our neighbour, is about to launch its own pilot project. Montreal is headed in the same direction," he said. "We have the same thing in Toronto and Calgary ... We need to be in tune with the times. And the times, as we can see, have clearly changed." Coderre said the two main objectives of the project are to provide greater transparency in public security matters and, by doing so, inspire public confidence in the police department. Montreal Gazette, A1 (2016-05-19); Cape Breton Post (2016-05-18)

* **Out of the shadows: A night in the life of 'kickass' undercover RNC team**
"I got the money. I just want to see the goods, that's all." A rough-looking man, with a big brown beard, hood up, wearing dark clothes talks on his cell phone on Jensen Camp Road in St. John's. He's grabbed the attention of the group of young men hanging around the neighourhood. What they don't know is that he's a cop, looking for a missing teen wanted on a warrant. Forget everything a police officer typically looks like — the crisp uniform, the clean-shaven face — and you'll find Sgt. Alex Brennan. He's coming out from undercover and has agreed to speak with CBC. A 20-year veteran of the Royal Newfoundland Constabulary and colonel in the military, Brennan projects a friendly authority, but heads up what he calls a "kickass" team within the RNC. Brennan's departure from his clean-cut image as a military leader to gruff undercover cop is startling. But he and the other three men on his team need to blend into places the average cop would never go undetected. CBC News (2016-05-18)

* **No to corruption abroad, but yes to ensuring fair trial**
An opinion piece states, "Foreign governments and civil society have frequently criticized Canada's lax enforcement of its anti-corruption law, the Corruption of Foreign Public Officials Act (CFPOA). Just three weeks ago, however, the Supreme Court of Canada released World Bank Group v. Wallace, a precedent-setting decision on the CFPOA that paves the way for increased enforcement of Canada's anti-corruption laws. It also creates interesting challenges for the right to a fair trial when that enforcement results in a criminal prosecution. (…) The project, however, was to be funded in part by the World Bank, which has a keen interest in ensuring that its projects are free from corruption. In 2012-2013, the RCMP laid charges against three SNC-Lavalin executives over an alleged bribe concerning the Padma bridge project in Bangladesh. Interestingly, the World Bank conducted the original investigation and shared its information with the RCMP. This raised a host of complex legal issues. In the resulting prosecution (which is continuing), the defence sought access to those parts of the World Bank's investigative file that had not been turned over to the RCMP. The trial judge granted the defence request. The World Bank then appealed this ruling directly to the Supreme Court on the basis that the World Bank, as an international organization, enjoys immunity from such court orders. The Supreme Court agreed. The Supreme Court's ruling will have ramifications for all CFPOA prosecutions in the future. International organizations such as the World Bank are uniquely positioned to investigate allegations of transnational corruption. A number of these organizations intervened in the Supreme Court case to support the World Bank's position, including the European Bank for Reconstruction and Development, the African Development Bank Group and the Asian Development Bank. All of them suggested that they might have to stop sharing information with

domestic law enforcement authorities if a court could force them to turn over all of their documents." Globe and Mail, B4

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Prison locked down
The medium-security Bath Institution west of Kingston was put in lockdown mode Wednesday morning. At about 10:30 a.m., the lockdown was put in place to enable staff members to conduct an exceptional search. A news release from Correctional Service Canada didn't reveal what they were searching for. The release did say the search was ordered to ensure the safety and security of the institution, its staff and inmates. Visits have been suspended until the search is completed, and normal operations will resume as soon as it is considered safe to do so. Kingston Whig-Standard, A3

*** Nurses fear more attacks**
Graphic security camera video caught the moment a violent, severely mentally ill patient attacked a nurse in the forensic unit of the Brockville Mental Health Centre in October 2014, stabbing her four times in the neck with a pen. In the video, the patient, Marlene Carter, is walking alongside her nurse escort in the hallway of the hospital's forensic unit when she pulls a pen from her pants pocket and strikes the nurse without warning about her head and neck. The attack lasted just seconds before staff overpowered Carter as another staff member helped the victim to safety. The video was played Wednesday on the first day of a trial of the Royal Ottawa Health Care Group, which operates the Brockville hospital. The ROHCG is charged with five violations of Ontario's Occupational Health and Safety Act, meant to keep workers safe from workplace violence. Carter, now 44, was a federal prisoner transferred to Brockville in August 2014 because no institution in her home province of Saskatchewan had been able to deal with her. She had spent 28 years in custody - virtually her entire adult life - and had a history of suicide attempts, repeatedly banged her head so hard that she suffered permanent brain damage, and had a long list of assaults on correctional officers and caregivers. (…) Carter was charged with aggravated assault for the attack but was found not criminally responsible. In January she was transferred back to Saskatchewan to be closer to her family and her Cree culture. The Crown argues that the ROHCG should have done more to prepare staff for Carter's arrival in Brockville and had inadequate equipment, procedures and training in place to deal with such a violent patient. Ottawa Sun, A12 (Ottawa Citizen)

*** Appeals court asked to overturn conviction of child-killer Cyr**
Wearing a T-shirt emblazoned with a photo of her young daughter in happier times, Amanda Trevors returned to a Regina courtroom for the appeal launched by the man convicted of killing the girl. "It is difficult to sit through again," she conceded Wednesday after the Saskatchewan Court of Appeal reserved decision on a bid by Adam Riley Cyr to overturn his conviction and win a new trial. "Difficult" was also a word used by Cyr's lawyer Marianna Jasper to describe the case. (…)Cyr, who sat quietly in shackles throughout the proceeding, is serving a life sentence without parole eligibility for 12 years. Leader-Post, A4

Family of boy stabbed by mother 'lived in fear'
He was six years old when his mother took him into the bathtub and stabbed him repeatedly in the neck and stomach. Three years later, the physical wounds have healed, but time has not erased the pain inflicted on "Neil" and his family. Although his mother pleaded guilty to aggravated assault and was sentenced on April 19 to five and a half years in prison, Neil, his father and brother say they "lived in fear" for nearly three years while the criminal charges dragged through court. "We are not getting any degree of closure out of the process," said his father, "Jason". (…) Jason said for the first time in years he and his kids feel safe speaking publicly about the case that has consumed them. They want to speak out victim's experiences with the court system so often go unreported, they said. Postmedia Network (StarPhoenix, A1, Leader-Post, National Post, Edmonton Journal, Calgary Herald)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Ontario, Ottawa expand free access to overdose antidote
Ontario and the federal government are rushing to close policy gaps that medical experts say have contributed to the deadly toll wrought by opioid addiction and the rise of bootleg fentanyl across the country. On Wednesday, both governments launched massive expansions in free access to naloxone, a cheap, life-saving antidote to opioid overdoses. Ontario Health Minister Eric Hoskins announced that his province - the country's largest per capita consumer of prescription opioids - would join B.C. and Alberta in dispensing free naloxone to anyone through community pharmacies, no prescription required. The federal government, meanwhile, added naloxone to the list of drugs covered under the Non-Insured Health Benefits, the national pharmaceutical program for aboriginals, a group that has faced disproportionate numbers of opioid-related deaths in some regions. Both Ontario and Ottawa have faced criticism that their response to the crisis has been slow. Taken together, the new initiatives add a much-needed sense of urgency to tackling the opioid crisis, medical experts say, and address the fact that a potentially life-saving drug is reaching a small minority of people in the country's largest province and in aboriginal communities. (…) In Ontario, opioid overdoses killed 663 people in 2014, 173 linked to fentanyl, a powerful painkiller that has become a lucrative source of income for organized crime. In 2015, Alberta and British Columbia recorded 418 overdose deaths related to fentanyl, a 10-fold increase over the previous three years. Globe and Mail, A1

* **Crime prevention week**
Terry Lee Ropchan wants to put the power back in people's hands. The Central Alberta Crime Prevention's executive director said more people are getting an understanding of how they can get involved and what are the things that they can do to promote safety in their communities. "Graffiti is one of those things that affect our neighbourhoods or affect how we feel in our neighbourhoods," said Ropchan. "When you drive into a neighbourhood and you see graffiti, you instantly have a negative reaction to it. We just want to put the power back in the people's hands." There's lots of things that you can do if you are frustrated or you don't feel safe in your neighbourhood, she said. "Come and talk to us because it could be some resource or some information that we have," said Ropchan. "It could be a connection to start a meeting or it could be some community project that needs to be developed. We can be that catalyst to work with the city or whoever they need to get their project up and going. We are excited. We want people to come and talk to us." As May is Crime Prevention Month, there are several events planned throughout the month. Red Deer Advocate, C5

* **Sudbury's crime rate drops**
Hydro and food prices might be going up, along with temperatures across the globe, but residents may take heart in the announcement that thefts, assaults and arsons are all on the decline. "It's a good news story for Sudbury," said Chief Paul Pedersen at a police board meeting on Wednesday. "The trend, as we've seen for a number of years, is that crime is going down." Pedersen shared numbers crunched annually as part of a crime tracking process that is uniformly applied across the province. They show that overall offences in 2015 were 434 fewer than the previous year, while the service's ability to lay charges, expressed as the clearance rate, improved by 3.9 per cent. "Total criminal offences have gone down by 5.3 per cent," said Pedersen. "But what's really good is that our ability to solve the crime that's left is going up." The positive trend isn't unique to Sudbury, although neither is the city lagging behind others of a comparable size. Sudbury Star; Sudbury.com (2016-05-18)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Pot shop proponents set for city hall showdown today**
Marijuana activists are planning to show up at a meeting of the city's licensing and standards committee today to voice their concerns over Mayor John Tory's move to crack down on the growing number of pot shops across Toronto. Last week, Tory wrote a letter to Tracey Cook, municipal licensing and standards executive director, asking the committee to review the operations of marijuana dispensaries in the city and make recommendations for changes. These would include whether it's possible to licence them, or control where they set up operations near schools, community centres and other dispensaries. "Over the past few months, residents and businesses in different parts of Toronto have raised concerns about the rising number of marijuana dispensaries opening in their neighbourhoods," Tory said in the letter. "The speed with which these storefronts are proliferating, and the concentration of dispensaries in some areas of our city, is alarming." This week, some dispensary owners received letters from the city that say they're operating in violation of bylaws. "They just basically said there's an infraction on a bylaw," said Tania Cyalume, co-owner of the Queens of Cannabis dispensary on Bloor Street West. "They're basically just trying to scare dispensary owners into closing down." CBC News; Toronto Star; Radio-Canada (2016-05-19); Globe and Mail; CTV News; CP24 (2016-05-18)

Canada's move to legalize marijuana violates international law, experts say
The Trudeau government has plans to introduce legislation next year that will legalize marijuana across the country. But this violates three international drug control conventions, according to an international lawyer. In an opinion piece published in the *Canadian Medical Association Journal* (CMAJ) on Monday, authors Steven J. Hoffman and Roojin Habibi claim that allowing possession of pot would violate three separate conventions: the Single Convention on Narcotic Drugs of 1961 as amended by the 1972 Protocol, the Convention on Psychotropic Substances of 1971 and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988. Marijuana is considered a Schedule 1 narcotic as classified by the World Health Organization (WHO). Schedule 1 narcotics are considered to pose a serious health risk to the public and are some of the most strictly regulated substances which include LSD and ecstasy. Global News (2016-05-18)

*** Pot activist Larsen's supporters hold rally after court appearance**
Pedestrians cheered, car drivers honked and even a bus driver showed support by blasting the horn as marijuana users banded together to march for marijuana legalization, and to support pot activist Dana Larsen during his first court appearance in Calgary. Larsen, known for his "Overgrow Canada" campaign in which he vowed to give out a million marijuana seeds countrywide, was arrested in Calgary last month during one of his giveaway events. (…) Larsen pledged not to take a plea bargain or deal, and said he will take the case to the highest court that will hear it. "If they persist, then I feel like we might get the laws against cannabis seeds overturned. That would be my goal, assuming they want to go forward with this." Larsen's supporters, some of whom were smoking from bongs and joints as they marched through downtown, were equally optimistic about his case. Some were annoyed that city police charged Larsen. "The police are wasting our expensive resources, and the courts are wasting law enforcement resources," said Keith Fagan, one of the organizers of the rally, who also attended Larsen's seed handout event last month. "I think this case will be thrown out, I really do." Larsen says he believes Canada's impending legalization of marijuana will be the ultimate reason for his case being dropped. Calgary Herald, A14

*** Some area mayors want cut from legal pot, Bradley says**
Mayor Mike Bradley said some Southwestern Ontario mayors believe municipalities should receive a cut of the federal government's income from legalizing and regulating recreational marijuana. He made those comments as a standing committee of Lambton County passed a motion Wednesday asking county council to support the Simcoe Muskoka District Health Unit's call for the federal government to consider public health issues as it moves to legalize marijuana use. Ottawa has said it will introduce legislation in 2017 to legalize recreational marijuana. London Free Press, A8

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

Search under way for EgyptAir plane with 66 aboard that crashed into Mediterranean
An EgyptAir flight from Paris to Cairo with 66 passengers and crew on board crashed in the Mediterranean Sea early Thursday morning, Egyptian aviation officials said. Egyptian Prime Minister Sherif Ismail said it was too early to say whether a technical problem or a terror attack caused the plane to crash. "We cannot rule anything out," he told reporters at Cairo airport. EgyptAir Flight 804 was lost from radar at 2:45 a.m. local time when it was flying at 37,000 feet, the airline said. It said the Airbus A320 had vanished 16 kilometres after it entered Egyptian airspace, around 280 kilometres off the country's coastline north of the Mediterranean port city of Alexandria. The aviation officials later said the plane crashed and that a search for debris was now underway. The "possibility that the plane crashed has been confirmed," as the plane hasn't landed in any of the nearby airports, said the officials, who spoke on condition of anonymity because they were not authorized to speak to the media. Egyptian armed forces were searching for the plane, which was carrying 56 passengers, including one child and two babies, and 10 crew. The pilot had 6,000 flight hours. Earlier, the airline said 69 people were on board. In addition to the unidentified Canadian, EgyptAir said passengers included 30 Egyptians, 15 French citizens and others from Britain, Belgium, Iraq, Kuwait, Saudi Arabia, Chad, Portugal and Algeria. Global Affairs Canada said it was "aware of the possibility that a Canadian may have been on board the flight" and that the department was "monitoring the situation closely." The statement added that Canadian officials in Cairo and Paris are working with local authorities to confirm this information. Associated Press (National Post, StarPhoenix, St John's Telegram, The Guardian, CTV News, CBC News); Vancouver Sun; * Agence France-Presse (Journal de Montréal)

Dion to discuss human-rights issues during Saudi visit
Foreign Affairs Minister Stéphane Dion will travel to Saudi Arabia next week for talks on how to thwart the expansion of Islamic State and al-Qaeda in the region and government insiders say he will use the visit to speak out about human-rights abuses against women and Shia minorities. Mr. Dion is seeking a tête-à-tête with 30-year-old Deputy Crown Prince Mohammed bin Salman, the powerful son of the Saudi King, who is the also the Defence Minister and head of the country's economic council. Canada's Foreign Affairs Minister was invited to the Red Sea port of Jeddah for a meeting on Tuesday of the Gulf Cooperation Council, whose members are Saudi Arabia, Bahrain, Kuwait, Oman, Qatar and the United Arab Emirates. The Arab Gulf states have provided large sums of money and arms to Western-backed rebels fighting the Syrian government and Islamic State extremists and are part of a Saudi-led coalition fighting Shia Houthi militants in neighbouring Yemen who are aligned with Iran. The United Nations has accused the Saudi-led coalition of being responsible for twice the number of civilian deaths in Yemen as all other combatants and for having triggered a severe humanitarian crisis in an already poor country that has led to an expansion of alQaeda in the Arabian Peninsula. "Let's not forget these are allies we are talking to about security, but it doesn't mean we will be shy about raising our own concerns and that includes human rights across the board," a government insider told The Globe and Mail. The Saudis are using Canadianmade combat vehicles in Yemen right now to fight Houthi rebels - machines very similar to those Canada will be shipping to the House of Saud under a $15-billion deal brokered by Ottawa. Globe and Mail, A3

SNC-Lavalin reçoit un prix pour un projet controversé en Algérie
Les Grands Prix du génie-conseil québécois ont honoré SNC-Lavalin pour un projet en Algérie que la firme pourrait avoir décroché avec le concours d'une société secrète établie aux îles Vierges britanniques dont le nom vient d'apparaître dans les Panama Papers. Lors d'un gala organisé lundi par l'Association des firmes de génie-conseil (AFG), SNC-Lavalin a reçu le prix dans la catégorie « international » pour le complexe Koudiat Acerdoune, lequel comprend notamment une usine de traitement de l'eau et un réseau de conduites de 75 kilomètres. Le projet de 327,4 millions CAN, réalisé en 46 mois, alimente aujourd'hui en eau potable quelque 880 000 personnes. Le chantier avait toutefois été entaché par la mort, en 2008,

de 12 travailleurs algériens de SNC lors d'un attentat terroriste. C'est l'Agence nationale des barrages et transferts d'Algérie qui avait attribué ce contrat à SNC-Lavalin en novembre 2006. En janvier 2005, le même organisme étatique avait donné à la multinationale québécoise un contrat semblable, mais d'une valeur de plus de 700 millions, pour le transfert d'eau du barrage de Taksebt. Ce projet a remporté l'un des Grands Prix du génie-conseil québécois en 2009. Grâce à la base de données des Panama Papers, Radio-Canada et le Toronto Star ont révélé hier que SNC avait versé près de 22 millions à Cadber Investments, une entité des îles Vierges britanniques, pour décrocher des contrats en Algérie, y compris 4 millions US pour celui de Taksebt. Les fonds ont transité par un compte de la succursale de la Banque Royale du Canada à Genève, en Suisse. La Presse +, 4

*** United Arab Emirates jailed my father for months without anyone knowing**
An opinion piece by Marwa Alaradi states, "The United Arab Emirates arbitrarily detained my father, and now they're neglecting his health. My father disappeared off the streets of Dubai two years ago and was locked up in the U.A.E.'s notorious secret prison system by state security agents. My father's name is Salim Alaradi, and he is a 45-year-old Canadian-Libyan citizen, a family man and determined businessman who has a record of international humanitarian philanthropy. For over a year now, Canadian and international media have followed the developments of my father's case. On May 30, a court's final verdict will be given with no right to appeal. His jailers have failed to treat him with basic dignity, and, whatever direction the legal process takes, it will be a longtime before my father recovers from the dehumanizing conditions under which he's been kept. My father's case, and our campaign to free him, has brought worldwide attention to these issues, and various organizations - from the UN Human Rights Council to Amnesty International - have criticized the UAE for human rights violations committed against my father and his co-accused, Kamal and Mohamed Eldarat (U.S. nationals). My father was jailed for months without anyone knowing his whereabouts or why he was being detained. His health is failing and, as observers and investigators from the UN, the Canadian government and numerous human rights organizations have reiterated again and again, my father has been mistreated. In other words, the detention and torture he endured has destroyed his health physically and mentally." Windsor Star, A8

INTERNATIONAL

Gains against Daesh harbingers of future terror
Another day brought another horrible set of headlines out of Baghdad: On Tuesday, four bombings, one after another, killed dozens of people and left streaks of blood and strewn body parts across public markets. As familiar as the last week of violence in Baghdad - more than 200 killed since last Wednesday - might seem to those who have watched Iraq over the years, this is not business as usual here. The U.S. history in Iraq tells us that successful bombings in Baghdad are not to be taken lightly. The official talking points say the new wave of bombings is a sign that Daesh is losing. The terrorists are lashing out in Baghdad because they are abandoning territory to pro-Iraqi ground forces and U.S.-led airstrikes. They're "on the defensive," as Brett McGurk, U.S. President Barack Obama's special envoy here, said. There is truth to that line. Daesh, also known as ISIS and ISIL, is losing territory in Iraq and Syria. And the recent wave of bombings is out of the very first page in the group's playbook, back when Daesh was Al Qaeda in Iraq. But this is not the group's final death throes - not yet. Since their beginnings, the Sunni extremists of Daesh have been driven by the desire to wage a sectarian holy war, and have been amply willing to barter their lives in return for terrorizing and inciting the Shiite population. The Iraqi capital has been its most fertile ground for sowing fear. Toronto Star, A15

*** La France «clairement » dans le viseur de l'État islamique**
La France est «clairement visée» par le groupe État islamique (ÉI), qui pourrait mener «une campagne terroriste caractérisée par le dépôt d'engins explosifs dans des lieux où est rassemblée une foule importante», a déclaré le patron de la Direction générale de la Sécurité intérieure (DGSI). «Nous savons que Daech (acronyme arabe de l'ÉI) planifie de nouvelles attaques – en utilisant des combattants sur zone, en empruntant les routes qui facilitent l'accès à notre territoire – et que la France est clairement visée», a expliqué Patrick Calvar, auditionné le 10 mai par la Commission de la défense nationale et des forces armées de l'Assemblée nationale, dont le compte-rendu a été rendu public hier. «Daech se trouve dans une situation qui l'amènera à essayer de frapper le plus rapidement possible et le plus fort possible:

l'organisation rencontre des difficultés militaires sur le terrain et va donc vouloir faire diversion et se venger des frappes de la coalition», a-t-il estimé. Agence France-Presse (Journal de Montréal)

'Some of them pray, some of them don't pray. But all of them kill'
Clutching her daughter tightly to her chest, Zarah Ali leans close to the visitor and whispers her story.She doesn't want the nearby camp guard to hear. If he learns that her 22-month-old daughter was fathered by a Boko Haram fighter, the gossip could sweep across the refugee camp, bringing her the stigma and ostracism that afflicts many women who were forced into "marriage" with the Islamist radicals. Ms. Ali, the 20-year-old daughter of a Muslim farming family in northeastern Nigeria, knows more about Boko Haram than most. She was its captive - twice. She escaped once, fled across the border to Cameroon and was captured again. She spent months under Boko Haram's control. And despite the group's Islamist ideology and its claims of allegiance to the Islamic State movement, she scoffs at its professions of faith. "Some of them pray, some of them don't pray," she says. "But all of them kill." In her months of captivity, she remembers how Boko Haram would gather the people of the occupied villages and preach to them about how to "slaughter" their enemies. In contrast to their religious pretenses, they often recruited followers with offers of money and threats of violence, she says. "They are unbelievers and thieves," she says. "They kill Christians, but they also kill many Muslims. They kill people and take their property." New studies of Boko Haram are confirming what Ms. Ali has witnessed. The group was founded by a charismatic Islamic preacher, but religious beliefs are no longer the driving force behind the group. Many of its followers today are instead motivated by economic factors or anti-government grievances. Mercy Corps, a United Statesbased humanitarian aid agency, recently interviewed 47 former Boko Haram members in northeastern Nigeria. Its study gives fresh insight into the brutal militia that has killed and abducted thousands of people in Nigeria and neighbouring countries. Globe and Mail, A11

*** West plays waiting game in ongoing Libyan mess**
An editorial states, "When "Prime Minister" Fayez al-Sarraj of the "Government of National Accord" (GNA) arrived in Libya a month ago, U.S. Secretary of State John Kerry said it was "not the time for obstructionists to hold back progress." A noble sentiment, but it does make you want to ask Kerry: When would be the right time for obstructionists to hold back progress? Next Tuesday? It was one more slice of the meaningless waffle when Western politicians discuss what to do about the Libya mess. The country has collapsed into violence and chaos since NATO bombers drove longruling dictator Moammar Gadhafi from power in 2011, and Kerry has no good plan for dealing with it. Sarraj's GNA merely adds a third contender to the rival governments that already claim to rule the country, and not one of them actually controls much territory. It is the hundreds of militias that really control Libya's territory, and the fortunes of the contending governments rise and fall depending on how many militias will agree to back them (in return for favours and subsidies, of course). Western governments are finally paying attention to Libya mainly because ISIS (Islamic State) fighters are active there, and because refugees are flowing into Europe from Libya again now that the route through Turkey and Greece has been blocked. The Italian, British and French governments have been talking of sending 6,000 troops into Libya to train a Libyan army that could take on ISIS and defeat it. There are already American, British, French and Italian special forces teams in the country, and there have been at least four American air strikes against ISIS camps in Libya since December. It all sounds like a full-scale Western military intervention in Libya is imminent - except it has been sounding like that for the past six months, and the intervention still hasn't happened." Kingston Whig-Standard, A4 (Red Deer Advocate, London Free Press)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
June 10, 2016 / le 10 juin 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Shooting victim known to police: Toronto Police say man was targeted
Toronto Police and the family of a man shot dead earlier this week are both issuing public appeals for help in solving the city's 33rd homicide of the year. Det. Sgt. Joyce Schertzer is asking people to come forward if they have information on the shooting death of Sukh Deo, or knowledge of a black Honda Civic believed to be involved. Deo's family is echoing that call and asking the public not to judge their relative by media accounts they say are untrue. Deo, 35, was gunned down on Tuesday in the typically peaceful midtown neighbourhood of Yonge Street and Eglinton Avenue. Media reports have said Deo was from Vancouver and allegedly had ties to gang activity there. Schertzer confirmed that Deo was not from Toronto and said his shooting was targeted, but would not comment further. She said he was known to police, but not to the local police service. Other media reports have said Deo and his family lived in a luxury Oakville home. The Oakville Beaver reports that the Oakville home was raided by tactical officers in early 2014 and it is alleged investigators seized a Bentley, Rolls-Royce and Land Rover at the time. (…) Deo's death comes in a year that has seen a dramatic spike in gun violence throughout the city. Toronto Police Chief Mark Saunders and Mayor John Tory have both spoken out on the need for public support to end the spate of shootings. In a letter to federal **Public Safety Minister Ralph Goodale** and

his Ontario counterpart Yasir Naqvi, Tory linked the rise in gun violence to firearms from the United States, saying about half of illegal guns seized by police have been smuggled across the border. Canadian Press, A4 (The Record, Hamilton Spectator)

New committee to keep spies in line
Federal spying and other clandestine national security activities will face new and unprecedented parliamentary scrutiny under long-promised Liberal legislation to be unveiled within days. The Grits will introduce a bill creating an all-party committee of parliamentarians, chaired by Ottawa Liberal MP David McGuinty, to keep a dedicated eye on the effectiveness, legality and strategic direction of the country's expanding national security apparatus. The move fulfils a key Liberal election promise, but also renews questions about the status of the government's much-promised overhaul of the controversial Antiterrorism Act of 2015, otherwise known as Bill C-51, rushed through Parliament last spring under Conservative majority rule. (...) The office of **Public Safety Minister Ralph Goodale**, responsible for Canada's chief spy agency and the RCMP, confirms the proposed legislation will be tabled before MPs start their summer break June 23. Details remain under wraps. Canada is the only nation among major western allies that does not allow parliamentarians access to classified security and intelligence information about spying, policing and other sensitive national security operations. Ottawa Citizen, B3

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Wildfire / Feu de forêt à Fort McMurray

* **Fort McMurray: Rachel Notley Promises South African Firefighters Will Get A Pay Bump**
South African firefighters who joined the battle against the Fort McMurray blaze will get every penny they were promised, Alberta Premier Rachel Notley said Thursday. "I can say right now that every hour that every firefighter from South Africa — or anywhere else — has worked on these fires will be compensated in accordance with our laws in this province," Notley said in Calgary.The South African group that employs the 300 workers said they would be leaving after only a week on the job because of a pay dispute. The organization Working on Fire said senior managers were coming to Canada to address concerns and oversee the return. Canadian Press (Huffington Post); Globe and Mail; CBC News; Independent Online

* **Heavy rain in Fort McMurray could lead to flash flooding**
After weeks of worrying about a massive wildfire and smoke, people in the Fort McMurray area have a new concern - rain. Environment Canada has issued a warning of heavy rain in the region and possible flash floods. The warning says up to 66 millimetres of rain could result in washouts nears rivers, creeks and culverts. The Alberta government says the rain is increasing hazardous conditions by eroding soil around damaged trees. The province says trees with weakened roots could easily fall without any wind and slopes will be slippery. Despite the rain the government says people must continue to follow the ban on fires and off-highway vehicles as the forest is expected to dry out again. Canadian Press (CTV News, St. John's Telegram, Charlottetown Guardian); Global News; CBC News

* **Commercial flights scheduled to return Friday to Fort McMurray airport, but expect delays**
While the Fort McMurray International Airport will reopen to commercial flights Friday, passengers will have to be patient as airlines work around emergency responders still using the skies above the city. "The situation is evolving right now," said Fort McMurray International Airport spokesperson Jillian Phillipp. "We are scheduled to open (Friday), but the (provincial government) and Agriculture and Forestry is still using the air space for emergency response to the wildfire." According to Chris Chodan, spokesperson for the Edmonton International Airport, one flight scheduled for Friday between Edmonton and Fort McMurray, taking off at 8:35 a.m. Friday, has already been cancelled. As firefighters continue to battle the wildfire still raging near Fort McMurray - which as of Thursday night was around 71-per-cent contained, covering an estimated 586,707 hectares - anyone flying in or out of Fort McMurray on a commercial flight should be prepared for changes or cancellations. "We are working to get back to a full schedule," said Phillipp, "but it's just going to take a bit of time." Edmonton Journal

*** Airlink brings relief team to aid Fort Mac recovery**
A U.S. non-profit has linked up with Air Canada to fly in volunteers who are sifting through toxic debris in Fort McMurray. Airlink, a rapid-response disaster and humanitarian relief organization in Washington, D.C., that links non-profits with partner airlines, has flown in at least 19 Team Rubicon volunteers into Fort McMurray on donated flights from Air Canada, Alaska Airlines and United Airlines since June 7. Team Rubicon is an American non-profit working to provide incident, volunteer and debris management in support of residents returning to homes destroyed in the Fort McMurray wildfire. Calgary Herald, A12

*** Defaults on rise in Alberta, ratings agency warns**
However you slice it, Alberta consumers are feeling the ripples of the oil and gas downturn at home, on the road and in the shopping aisle. The recent wildfires in Fort Mc-Murray and the impact of weak pricing in the oil and gas industry are putting stronger pressures on the province's economy than was previously known, according to a report by DBRS released Thursday. The ratings agency said it expects Alberta will suffer a contraction in real GDP of 1.5 per cent in 2016 - and warns that this estimate does not fully factor in the extended shutdowns of oil operations north of Fort McMurray. Calgary Herald, B1/FRONT

*** Fort McMurray shops and restaurants slow to spring back to life**
Ten days after residents started trickling back into Fort McMurray, much of the city has begun to look and sound like itself. Highway 63 is buzzing with trucks. More workers are back on the job at oilsands sites. The city's waste disposal service is preparing to resume a normal collection schedule. The Miskanaw Golf Club on MacDonald Island Park has started taking tee times. But most of Fort McMurray's small business sector remains closed. While cleaning crews are busy vacuuming, wiping and spraying inside some retail outlets, other businesses look as if they haven't been touched since the May 3 evacuation. Postmedia (Edmonton Journal, A2)

*** Lives pulled from the ashes**
In the grips of final stage cancer, all Quentin Thomas wanted to do was to spend his last few days at home in peace. Fort McMurray's wildfire wouldn't give him that peace, forcing the bed-ridden 48-year-old to be evacuated with the rest of the city. "They had to take him out in a bed sheet," said his brother Sheridan Thomas. "He died three days later in the Lac La Biche hospital." That same day he died, his family received confirmation that Thomas' home in Stone Creek had been destroyed. On Wednesday, his son and brother returned to the home on Prospect Drive for the first time to look for any mementos of their relative. But rather than fumble around in the hazardous debris themselves, the Thomases had help from a group of specially trained volunteers. Postmedia (Edmonton Sun, A10; Edmonton Journal, Calgary Herald)

*** Cenovus, CNRL restore production as fire threat eases**
Operations are returning to normal in the Wabasca area of northern Alberta after a wildfire prompted two companies to cut back heavy oil production earlier this week. Cenovus Energy Inc. said Thursday it was bringing about 50 staff back on-site and was in the process of restarting oil production at its Pelican Lake facility. The company removed 118 staff from the facility and shut down about 23,000 barrels a day of production after a wildfire was discovered about a kilometre away from the site Tuesday. Canadian Press (Calgary Herald, B4; Red Deer Advocate, Times Colonist); Globe and Mail

Other / Autres

*** Canada's forest ministers call on feds to do more in fight against wildfires**
An already devastating wildfire season has prompted forest ministers across the country to call for a more national focus on battling big blazes. The Canadian Council of Forest Ministers has released the *Canadian Wildland Fire Strategy: A 10-year Review and Renewed Call to Action* in which they say more needs to be done. "Recent wildfire seasons in British Columbia and the devastating situation in Fort McMurray have shown all of us that no province can go it alone when fighting wildfires," B.C. Forest Minister Steve Thomson said. "We need a cohesive, national strategy to ensure we are all better prepared (...)"While the goals still exist, the ministers say progress over the past 10 years has been slower and more costly than anticipated. "The federal, provincial and territorial governments must

recommit to the strategy as partners and effectively support its continued implementation to ensure that Canada is able to meet the challenges that lie ahead," the report says. CBC News

*** YARMOUTH COUNTY: Residents stirred, not shaken by small quake**
Residents of the Pubnico area took to social media Thursday afternoon, asking each other if what they had just felt was an earthquake. "We didn't know what it was at first," said Rosette d'Entremont of Lower West Pubnico. "We thought maybe it was a big truck going by or thunder but it didn't stop. The noise kept going." The seismogram on the Natural Resources Canada website recorded several small spikes of activity around the time of the rumbling that was felt throughout eastern Yarmouth County. Natural Resources seismologist Stephen Halchuk confirmed that a 3.0 magnitude earthquake happened at 5:43 p.m. 20 kilometres north of Yarmouth. Chronicle-Herald, A4; CBC News

*** Severe thunderstorm warnings in effect for parts of southwestern Manitoba**
A tornado warning was downgraded to severe thunderstorm warnings in parts of southwestern Manitoba Thursday evening, and residents took to social media to document #mbstorm. Environment Canada has issued severe thunderstorm warnings for Melita to Boissevain, including Turtle Mountain Provincial Park, from Minnedosa to Riding Mountain National Park and from Virden to Souris. Severe thunderstorm watches have also been issued for much of southwestern Manitoba. Winnipeg Free Press; CBC News

*** Super-sized El Nino over**
This year's monstrous El Nino, nicknamed Godzilla by NASA, is dead. It heated up the globe, but didn't quite end California's four-year drought. In its monthly update Thursday, the National Oceanic and Atmospheric Administration said the El Nino has ended, 15 months after its birth in March 2015. El Nino is a natural warming of parts of the central Pacific that changes weather worldwide. "There's nothing left," NOAA Climate Prediction Center deputy director Mike Halpert said. "Stick a fork in it, it's done." Halpert said this El Nino triggered droughts in parts of Africa and India and played a role in a record hurricane season in the Pacific. It also added to man-made warming, as Earth has had 12 straight record hot months and is likely to have its second straight record hot year. Associated Press (Chronicle-Herald, A10)

*** 2013 Calgary floods spawned 'increased demand' for services from non-profits: World Conference on Disaster Management speaker**
Non-profit organizations need to be prepared for natural disasters so they can help deliver public services, speakers suggested Tuesday at the World Conference on Disaster Management. From research conducted after the floods in affecting southern Alberta in 2013, the Calgary Chamber of Voluntary Organizations found that fewer than 50% of non-profit organizations "actually had business continuity plans in place," said Matt Sawatsky, emergency preparedness coordinator for CCVO. One part of a CCVO project involves helping non-profits prepare themselves for an emergency, Sawatsky suggested during a presentation Tuesday at the World Conference on Disaster Management. Canadian Underwriter (2016-06-09)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Iran loses key court battle to terror victims
The Iranian government lost a key court battle Thursday when an Ontario judge ordered the Islamic republic's non-diplomatic assets in Canada to be handed over to victims of terrorist groups sponsored by Tehran. The long-awaited ruling by the Ontario Superior Court dismissed every argument Iran's lawyers had made at a trial held in Toronto in January, leaving Tehran financial responsible for the actions of the terrorists it has backed. "Terrorism is one of the world's greatest threats," Justice Glenn Hainey wrote. "The broad issue before the court is whether Iran is entitled to immunity from the jurisdiction of Canadian courts for its support of terrorism." Iran's diplomatic buildings in Ottawa remain unaffected, but several nondiplomatic properties and the contents of a list of bank accounts were awarded to the victims of the Iraniansupported terror groups Hamas and Hezbollah. The $13-million case was the first challenge of the Justice for Victims of Terror Act. The 2012 law allows victims to collect damages from state sponsors of terror groups. Canada has designated Iran and Syria state sponsors of terrorism. "The JVTA continues to do its job in holding Iran - the world's most egregious state sponsor of terror - accountable for its terrorist

crimes," said Danny Eisen of the Canadian Coalition Against Terror, which represents victims and lobbied for the law. "As Canada seeks to re-engage Iran it is critical that Iran continue to be held to account in Canadian courts for its terrorism and human rights abuses." Postmedia Network (National Post, A1, Vancouver Sun)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

La F1 crée 4 fois plus d'offres d'escortes

Le nombre d'annonces d'escortes offrant des services sexuels sur le «Kijiji du sexe» a quadruplé à l'approche du Grand Prix de Montréal, d'après un outil d'analyse créé par un ex-policier. Pas moins de 1000 annonces ont été placées pour la grande région de Montréal dans la seule journée d'hier sur ce site dont nous tairons le nom pour ne pas nuire aux enquêtes policières. (...)«On a déjà identifié des cibles. Plusieurs dizaines de policiers surveilleront tous les endroits où il est possible d'acheter des services sexuels», explique l'inspectrice-chef du SPVM Johanne Paquin, responsable du plan d'action sur la prostitution et la traite de personnes. (...)La frontière canado-américaine et l'aéroport de Montréal seront aussi plus surveillés qu'à l'habitude. «Nos agents peuvent déceler si une voyageuse se trouve sous l'emprise d'une autre personne qui l'accompagne. On va mettre l'accent là-dessus», rapporte Dominique McNeely, porte-parole de l'Agence des services frontaliers du Canada. Des dizaines de policiers de la GRC seront aussi présents «dans des lieux stratégiques» pour appuyer le SPVM. «On va chercher des infos sur le terrain, pour remonter ensuite jusqu'à ceux qui font le trafic humain. Et on veut vraiment faire réaliser aux consommateurs qu'ils encouragent l'exploitation sexuelle. Même s'ils font quelque chose une fois pour le plaisir, c'est criminel», souligne la caporale Camille Habel, porte-parole de la GRC. Journal de Québec, 27 (Journal de Montréal)

Désengorger les frontières

Vous avez déjà poireauté de longues minutes à la frontière en cuisant dans la voiture, tout en rageant contre l'inefficacité des douanes ? Vous n'êtes pas seul. La frontière terrestre vers les États-Unis est franchie chaque année à 47 millions de reprises par des (...) Ottawa veut donc s'inspirer du système de prédédouanement des aéroports. Un projet-pilote sera mis en place dans les gares ferroviaires de Vancouver et de Montréal et devrait être élargi aux gares d'autocars, puis aux autoroutes. (...) Selon une étude du Congrès, l'économie américaine perd 116 millions de dollars pour chaque minute de retard dans les couloirs d'inspection de la frontière sud. Ce qui représente des milliards de dollars et des milliers d'emplois. Parce que chaque dollar investi est multiplié dans le commerce interfrontalier, il y aura lieu de songer à un programme 560 pour les points d'engorgement de la frontière canado-américaine. Il suffit de rappeler que 2,5 millions de camions de marchandises franchissent chaque année la frontière entre Détroit et Windsor. L'actualité, 35

B.C. man admits leading cross-border drug-smuggling operation, knows 'how bad it looks'

A B.C. man being sentenced in Seattle Friday for leading a major drug-smuggling ring says he's turned his life around since the charges were laid against him in 2009. Sean Doak wants U.S. Federal Court Judge Robert Lasnik to consider how far he's come in his rehabilitation despite years of involvement in the B.C. drug trade. "I have chosen to live a different life and have lost all interest in criminal activity," Doak, 42, said in a letter to the judge filed this week. "I recognize how bad it looks and is that I reoffended while on parole. This was a relapse in my criminal addiction and I am sorry for this." His lawyer Michele Shaw is asking Lasnik to sentence Doak to seven years in jail. But the U.S. Attorney wants a sentence that is six months longer, noting that Doak "fought extradition tooth and nail" before the Supreme Court of Canada refused to hear his appeal last October. "Mr. Doak was the leader and organizer of this group because he was the one with experience, connections, money and knowledge of the Canadian drug trafficking world," Asst. U.S. Attorney Susan Roe said in her sentencing memo. Vancouver Sun, 761 (The Province)

Travellers facing longer security lines at airports

Canadians risk flight delays and even longer airport security lines unless Ottawa boosts screening funding to address growing passenger levels, industry experts are warning. "It is on the cusp of being a real problem, with serious, serious delays," says John Gibson, chairman of the Canadian Airports

Council. Canadian airports aren't currently facing the chronic disruptions that are increasingly angering U.S. passengers. Still, lines have steadily grown over the last few years as Canadian funding hasn't kept pace with the 21 per cent increase in passenger growth over the last five years. The Canadian Air Transport Security Authority (CATSA) says, on average, it screens 85 per cent of passengers within 15 minutes. But waits can be much longer at some large airports during peak travel times, with additional pressure potentially coming during the rush of summer travel - and the number of passengers is growing by 3.5 per cent each year. If nothing is done to address the bigger volumes, Gibson said, passenger waits could regularly reach an hour. Red Deer Advocate. C3

Why can't our airport screening be better?
An opinion piece states, "Chuck Strahl was a well-liked and respected minister in the Harper government. One day, as minister of transport, he held a photo op-cum announcement at the Ottawa airport. He promised measures to speed up screening at airports. A good news announcement if ever one existed. Except that shortly after, a new test appeared. Selected passengers would now be required to show the palms of their hands and be checked for powder residue, in case they had been making bombs or other explosives. Agents for the Canadian Air Transport Security Authority (CATSA), when asked how this new test jibed with the minister's declaration, delivered their usual blank stares. We are only administering Transport Canada's policies, the agents correctly replied. (…)In Canada, for reasons no CATSA officer has ever been able to explain to an inquiring traveller, the Nexus card gets the traveller into a shorter line but then he or she is given the same scrutiny as everyone else - despite having been prescreened to get the Nexus card." The Globe and Mail, A13

Report highlights foreign worker abuse
Changes made to the Temporary Foreign Worker Program by the Harper government since 2014 increase the risk that low-wage migrant workers who come to Canada will be abused, according to a report released Wednesday afternoon by the Metcalf Foundation, a charitable organization in Ontario. "We've seen a rise in concern about the widespread exploitation of workers under the program, but what we know well is that those experiences of exploitation are a product of the system we've created," said Fay Faraday, the report's author and a human rights lawyer. With the federal government's review of the TFWP, the report, entitled "Canada's Choice," says that Canada is at a crossroads with respect to immigration. "Are we going to choose decent work? Or are we going to choose entrenched exploitation?" said Faraday, who advocates for a system that offers working class migrants a chance to lay down roots. Calgary Herald, A3

CYBER SECURITY / CYBERSÉCURITÉ

*** Why the meaningless hack attacks?**
An opinion piece states "On Monday, Drake was hacked. On Tuesday, Lana Del Rey was hacked. This followed a spate of social media hijackings, including virtual violations of Katy Perry, Kylie Jenner, the NFL and Chelsea Handler. As the Huffington Post noted: "It Appears Every Celebrity Twitter Account Is Being Hacked Right Now." It does. But to what end? Before we go any further, let me be clear: Hackers, I am not making fun of you. I'm not. Since I can barely recall my passwords - remind me to change my Star email to xd7wg43sasd+jgs68#?s after this column - I respect your ability to unearth ones you never created. So please do not steal my identity or pilfer my meagre RRSP or commandeer my texts unless you have time to send long overdue replies to distant relatives, in which case I'll give you the damn password. I'm just trying to understand your motivation. Toronto Star, E3

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Beef up number of Mounties abroad or lose ground on terrorism, organized crime**
As the threat from terrorism and organized crime becomes more global, Canada's national police force is facing questions over whether to send more of its members abroad - in other words, take the fight to the bad guys before they land on our shores. A newly released internal report says the RCMP's "international footprint" is relatively small compared to its allies. While the RCMP has 55 liaison officers and criminal

analysts abroad, Britain and Australia each have roughly twice as many. Unless the RCMP's international presence is beefed up, it runs the risk of being "unable to fully respond" to terrorism, drug trafficking, money laundering, illegal migration and cyber crime, the report warns. "The fact that combating criminality and instability in other countries leads to safer homes and communities in Canada should by now be beyond question, and ought to be both a cornerstone and raison d'etre of and for Canada's international policing efforts," says the report, completed by an RCMP analyst in late 2014 and obtained under access-to-information legislation. In an interview, RCMP Chief Supt. Eric Slinn said the number of deployments is constantly being evaluated. He noted the 55 personnel stationed abroad today are a "significant improvement" from the 38 members the force had just a few years ago. The fact that combating criminality and instability in other countries leads to safer homes and communities in Canada should by now be beyond question. "Quite candidly, I don't think we take a second seat behind anybody," he said. "We do in terms of numbers, but in our capabilities and our relationships and what we can leverage and get done, I feel very strongly we've got some solid people and we're doing a good job for Canadians." The release of the report comes at a time when public safety and intelligence officials are trying to keep tabs on roughly 180 people who left Canada and are suspected of engaging in terrorist activities abroad. Postmedia Network (National Post) (2016-06-09)

RCMP's BlackBerry-cracking methods could be revealed in Quebec court

A Quebec court could today pull back the curtain on secretive police techniques, including how the RCMP intercepted BlackBerry text messages to prove a murder conspiracy plot, as a judge considers whether to lift a publication ban in a case involving the Montreal Mafia. The case stems from Project Clemenza, a police operation that resulted in scores of organized crime arrests in 2014. At the time, police announced they had intercepted more than one million BlackBerry messages tied to allegations of drug trafficking, kidnapping, arson, weapons and other violent offences. (…) Chief Supt. Jeff Adam, who oversees the RCMP's Technical Investigations Services, declined to discuss with CBC News the specific methods used. But given rapid changes in technology and public concern in the post-Snowden era, as mobile developers move toward more secure "end-to-end" encryption, he says investigators are finding their jobs increasingly difficult. "What we're seeing now is … the best evidence of people conspiring to commit a crime is lost to us. And that's what we call 'going dark,'" Adam said. CBC News

Complaint against RCMP in limbo

A young woman who went to the police station in search of an acquaintance was struck in the face and legs by RCMP officers while in handcuffs, a year-old complaint alleges - one that remains unresolved to this day. The Jan. 7, 2015 incident, which was captured on video, prompted her lawyer Gary Wool to file a complaint on the woman's behalf with the Civilian Review and Complaints Commission for the RCMP, which investigates allegations from the public of Mountie wrongdoing. The woman was charged with assault causing bodily harm to a police officer, a charge withdrawn after the Crown prosecutor viewed the video at her lawyer's request. The Lethbridge Regional Police Service in Alberta was called in to carry out a criminal investigation. The complaint filed in May of last year is based on surveillance footage because the woman doesn't have a clear memory of what happened. The complainant, who Yellowknifer has been unable to contact and whose name has been withheld in records obtained, went to the city's RCMP building on 49 Avenue after being told someone she knew was being held by police. (…)She was handcuffed and taken to the booking area. Her shoulders were being held by Const. Miranda Porr and Const. Cory Wallace and her face was about three inches from a wall. (...)Three years ago Wallace admitted to a March 2013 assault against a prisoner in courthouse cells. However, the charge was stayed in court by the Crown after the officer attended a community justice hearing. (…)The complaint was taken seriously by the complaints commission. A cover page on the report sent to RCMP Commissioner Bob Paulson in Ottawa states the allegations "may require a code of conduct or criminal investigation." Yellowknifer

ASIRT looks into gunfire, alleged bid to ram into officer's car

An investigation is underway into the circumstances surrounding an RCMP officer firing his weapon Wednesday after a police vehicle was allegedly rammed. The Alberta Serious Incident Response Team, or ASIRT, said Thursday it was conducting an investigation into the events that unfolded when Spirit River RCMP responded to a report of a suspected impaired driver. RCMP said that an officer caught up with the vehicle, a black Ram 3500, on Range Road 61 on Wednesday afternoon. The driver allegedly

turned and sped toward the officer's Chevy Tahoe. The officer got out and the pickup accelerated toward the officer. ASIRT said only that an "incident occurred" that led to the police officer firing his gun. RCMP made no mention Wednesday of the officer firing his weapon. The suspect was later arrested without injury, ASIRT said. He has not been formally charged. Edmonton Journal, A11

Relatives grateful for RCMP's work
Family and friends of a little girl who died from a devastating brain injury 12 years ago says no matter what a jury decides about the man accused of killing her, they'll finally have closure. The jury began Thursday deliberating in the case of James Paul Turpin, 37, who's accused of killing two-year-old Kennedy Corrigan in Central Blissville in April 2004. Deliberations will continue Friday. He was charged last year with second-degree murder, and his trial has unfolded over the past four weeks in a Fredericton courtroom. Turpin claimed Kennedy slipped in the bathtub while he had sole care of her the morning of April 2, 2004, and she struck her head. He had been dating Kennedy's mother, Connie Corrigan, in early 2004, which is why he was alone with the girl and his own three-year-old daughter in the Corrigan home on the date in question (...)Tracy O'Toole, Connie's best friend, said the family was relieved the case finally went to trial after so long. "This is what we wanted and so much more," she said. O'Toole read a brief statement from Connie Corrigan, who thanked the RCMP, witnesses and prosecutors for the work they put into Kennedy's case. Daily Gleaner, A5

* **Edmonton holds inaugural First Responders Day to show appreciation**
When bad things happen, they're the first to step up. They walk into burning buildings, while others run away. They face down dangerous criminals, pull people from twisted car wrecks, rush them to hospital. On Thursday, Edmonton said thank you by commemorating June 9 as the city's first ever First Responders Day. (...)First responders with Edmonton police, emergency medical services, fire rescue, sheriffs, peace officers, the military fire department, corrections and the RCMP were all acknowledged. CBC News (2016-06-09)

* **Opération Malaise sur l'exploitation sexuelle d'enfants: 2 arrestations vendredi**
Deux autres suspects ont été arrêtés jeudi lors d'un nouveau volet de l'opération policière baptisée Malaise qui lutte contre l'exploitation sexuelle des enfants sur Internet. La Sûreté du Québec (SQ) rapporte que Jean Simoneau, 73 ans, de Magog, et Ross Perrin, 62 ans, de Montréal, qui faisaient l'objet de mandats d'arrestation, comparaîtront au tribunal vendredi au Palais de justice de Montréal. Ces deux hommes devront faire face à des accusations en lien avec des contacts sexuels qu'ils auraient eu avec des gens d'âge mineur et pour de l'exploitation sexuelle. (...) L'Équipe d'enquêtes sur l'exploitation sexuelle des enfants sur internet (ESEI), qui a procédé aux arrestations, regroupe des enquêteurs de la Sûreté du Québec et de la Gendarmerie royale du Canada. Presse canadienne (L'Actualité, Huffington Post, La Presse)

Historical gravestones vandalized
Vandals toppled over and broke historical gravestones marking early Island settlers in a Cowichan Valley cemetery last week, RCMP say. "It's inexcusable," said Cpl. Krista Hobday from the North Cowichan/Duncan RCMP. "These are historical items dating back to the mid-1800s." Sometime between June 6 and 8, vandals pushed over 13 gravestones at the Pioneer Cemetery on the corner of Pioneer and Herd Roads, Hobday said. Two of the markers were broken. The cemetery holds the graves of the earliest settlers in the area, she said. Unfortunately, it is also known to be a party spot. "In other cemeteries, family or someone might replace the gravestones, but who is going to replace these ones? They're a piece of our history." Times Colonist, A5

Battleford RCMP warn of attempted child abduction
Battleford RCMP are investigating a report of an attempted abduction of a child from a school yard in Battleford. The alleged incident was reported to have occurred some time between 2 to 2:15 p.m. on Thursday June 9th. Police says a 10-year old child was grabbed by an arm and directed to come with the suspect to a nearby vehicle. The child screamed and the man was reported to have let go of the child and fled in the vehicle. The child was not injured during this incident. 620 CKRM

* **RCMP arrest and charge third teen in brutal assault north of Winnipeg**

RCMP say they have arrested a third suspect in the violent assault of two workers at an addictions centre north of Winnipeg. During the May 29 attack Jackie Healey, a 23-year-old work placement student, suffered a fractured skull, broken teeth and blindness in her left eye. The other victim, a support worker at the facility, has extensive damage to her face, jaw and eye. Two youths, aged 16 and 17, were charged late last month with aggravated assault and robbery. Police say a third teen has been arrested and charged, but declined to provide further details. The Manitoba government has said it will conduct a workplace safety investigation into the attack at the Behavioural Health Foundation in Selkirk. Canadian Press (Brandon Sun), CBC News (2016-06-09)

* **Quatre carabines et 500 plants de marijuana saisis**
Un homme âgé de 33 ans a été arrêté à la suite d'une perquisition qui a mené à la saisie de quatre armes à feu et d'une importante quantité de plants de marijuana. Lundi, des agents de la GRC ont exécuté un mandat de perquisition dans une résidence de Bairdsville, près de Perth-Andover. La police affirme avoir saisi plus de 500 plants de marijuana à diverses étapes de croissance, ainsi que de l'équipement pour faire pousser de la marijuana, à l'intérieur comme à l'extérieur. Selon la GRC, une fois à maturité, le nombre de plants saisis aurait pu permettre de produire plus de 250 000 cigarettes de marijuana. La police a aussi saisi quatre carabines. Acadie nouvelle, 5

* **Muskrat Falls entrance blocked by protesters**
A group of protesters stopped traffic at the gate to the Muskrat Falls construction site Thursday. "[We] are trying to protect our people, our culture and our land," Jerome Jack told the CBC. Jack says he has been working for the Innu First Nation as an impact benefit agreement coordinator, but his phone has been cut off and he's uncertain of his employment. "A lot of deals were going on behind closed doors without my knowledge, without my people's knowledge, without my elders' knowledge." Jack says the First Nation was recently presented with an environmental assessment, including a caribou study, which he says was conducted by a private organization hired by Nalcor. (...)The protesters eventually let traffic out but say they will not be letting people in. "It seems to be a very peaceful protest." said Hubert Loder, who represents the project's unionized workers. RCMP were on site to monitor the protest. CBC News (2016-06-09)

Justice dept. pledges to save money
Manitoba's most popular baby names these days are Liam and Emily, Justice Minister Heather Stefanson revealed Thursday morning. Stefanson announced the information as the minister responsible for vital statistics, as she and critic Andrew Swan kicked off a civil and relatively tame first hour of committee hearings into Stefanson's departmental budget. (...)Stefanson said the province is spending $325,000 for three RCMP officers to serve as provincial police on Sioux Valley First Nation near Brandon, after that community opted out of Dakota-Ojibway policing. Justice is spreading an additional $232,000 among five agencies providing services to victims of crime, and $44,000 will allow retired justices of the peace to help clear up backlogs in traffic court. Winnipeg Free Press, A4

Mountie trades gun for horse
The face of the RCMP in the NWT has left her post in Yellowknife to join the iconic RCMP Musical Ride. Const. Elenore Sturko's last day on the job in Yellowknife was June 3. She had been the Mounties' media liaison officer for Yellowknife and the NWT since September 2014. Sturko lived in Yellowknife back in 2004 when she worked for CBC North. In 2010, she left the media organization to join the RCMP and began her policing career in Langley, B.C. She was posted back in Yellowknife in 2012. The musical ride, based in Ottawa, is performed by a full troop of 32 riders and their horses. Their performance consists of intricate figures and drills choreographed to music. Sturko said she had to go on a five-week course to determine whether she is suitable for the musical ride. (...)It is not clear who, if anyone, is going to replace Sturko as media relations officer. Yellowknifer

* **Smoke shops not helping Dakota First Nations**
An editorial states, “Earlier this week, several Dakota First Nation members who were charged for selling contraband tobacco lost a legal bid to have the case tossed out on the grounds that their people have no official treaty with Canada, and therefore the courts have no jurisdiction. As the Winnipeg Free Press reported, the two accused, - smoke shop owner Craig Blacksmith and employee Tammy Walters – were

arrested during a 2014 raid by RCMP on Dakota Plains near Portage la Prairie. RCMP, the Dakota Ojibway Police Service and Manitoba Finance taxation officials seized 4,800n cartons, which amounted to 951,225 cigarettes. More than 1,840 tins of chewing tobacco, six firearms, one vehicle and an unspecified amount of cash were also seized. All told, finance officials calculated $292,572.68 of tax was avoided. (...) For anyone who has been following the ongoing and controversial issue of the non-treaty Dakota in western Manitoba, this argument – that Dakota Plains has no official treaty status in Canada, and therefore should not be subject to Canadian law – is a familiar refrain, one that has not seen much traction in our federal or provincial courts." Brandon Sun

*** Quebec will soon have registry**

Bill 64, which requires the registration of long guns, was adopted on Thursday at the National Assembly, on the eve of the adjournment of the current parliamentary session. Since its filing last December, the bill to provide Quebec with a firearms registry did not have unanimous approval among the population, particularly in rural areas where there are many hunters. The bill passed with 99 votes in favour and eight against. There were no abstentions. About a third of the Coalition Avenir Québec (CAQ) caucus, seven MNAs, voted against the bill, as well as Sylvie Roy, a former CAQ member from Arthabaska, who became an independent. Premier Philippe Couillard imposed party discipline on his MNAs in order to pass the bill, but not the CAQ; their caucus was divided on the issue. Some Liberals and members of the PQ had reservations, but all rallied in the end, passing the bill. The bill was tabled last December by Public Safety Minister Pierre Moreau, and it was his successor, Martin Coiteux, who brought it to fruition. The gun registry, once in place, probably in 2018, will replace the federal firearms registry that was abolished by former prime minister Stephen Harper. His decision triggered concerns in Quebec. Under Bill 64, any firearm on Quebec territory must be registered with a unique number, and shall be listed in a file. Montreal Gazette, A10; Presse canadienne (Voix de l'Est, Le Quotidien, Le Soleil, La Tribune); Agence QMI (Journal de Québec); CBC News (2016-06-09)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Segregation used most in Manitoba jails

Nearly one in 10 prisoners in Manitoba's jail system is kept in segregation, believed to be the highest proportion in the country and significantly higher than the rate recorded in the federal system. But as the federal government, Ontario and Saskatchewan have announced they are reviewing their policies on solitary confinement, Manitoba says it will not follow suit. Manitoba's new Justice Minister, Heather Stefanson, said through a spokeswoman that the province does not plan to review its policy. "There are no plans to review segregation policies at this time," Amy McGuinness said. Just less than 9 per cent of the inmates held in Manitoba's provincial jails are kept in segregation, on average, according to the province's ministry of justice. That's the highest rate in Canada, based on an array of single-day figures gathered from across the country by The Globe and Mail, and much higher than the estimated 5 per cent in the federal correctional service. (...) The neighbouring province of Saskatchewan said this week that it is reviewing its segregation policy. The Globe recently reported that Richard Wolfe, an indigenous man who co-founded the Indian Posse street gang, spent 640 straight days in solitary confinement at a Saskatchewan provincial jail from 2014 to 2016. Mr. Wolfe died of an apparent heart attack at the penitentiary in Prince Albert on May 27. Saskatchewan joins Ontario, which announced a wholesale review of solitary confinement policy last year, and the federal Correctional Service Canada, which has ushered in a series of reforms to its solitary confinement regime. The CSC changes came in the wake of a damning coroner's inquest into the suicide of an isolated teen inmate, Ashley Smith, as well as a Globe and Mail investigation into the death of Edward Snowshoe, who took his own life after languishing in a solitary cell. Studies have found that prolonged spells in solitary confinement can lead to a range of health problems, including hallucinations, anxiety, loss of impulse control, severe depression, heart palpitations and reduced brain function. In many cases, according to one study, the damage is irreversible. Globe and Mail, A1

Parolee ditches ankle monitor

A federal inmate released on parole earlier this month had no intention of following any of the conditions attached to his release. "I told them right from the start, I wasn't going [to Saint John] and I didn't want to

leave the institution," said Andrew Donald MacKenzie in Moncton provincial court on Thursday. MacKenzie was arrested Wednesday on a charge of being unlawfully at large while serving a sentence and pleaded guilty. Prosecutor Eric Lalonde said the federal inmate was released on parole from a prison in the region on June 3 and he was wearing an ankle monitor to track his movement. MacKenzie was supposed to take a specified route to Saint John where he had to live while on parole. Instead, he came to Moncton and ditched his tracking device Times & Transcript, A3

Escaped inmate
An escaped Joyceville Institution inmate has been recaptured by Ontario Provincial Police in Amherstview. Det. Const. Steve Sermet of the provincial Repeat Offender Parole Enforcement (ROPE) Squad confirmed that Roger Strome was arrested near the intersection of County Road 6 and Taylor-Kidd Boulevard on Thursday. During the 4 p.m. inmate count on Wednesday, Strome, 44, was unaccounted for. Strome started his 10-year, three month, 15-day sentence on Jan. 8, 2008, after being convicted of 74 counts of theft of property-related offences, including break and enter and possession of property obtained by crime and theft. His sentence was scheduled to end on April 22, 2018. Kingston Whig-Standard, A3; Peterborough Examiner (2016-06-09)

Drunk driver loses appeal
After losing an appeal of his nine-year sentence for a deadly drunk driving crash, Brian Okemahwasin insisted he still needs to set the record straight and may head to a higher court. "I just took off at the wrong time," he told the Saskatchewan Court of Appeal on Thursday, describing the crash that claimed the life of an elderly Regina man almost two years ago to the day. "I wasn't looking for a lesser sentence. I just didn't want to sound like a monster," added Okemahwasin. During his submissions, several times - seemingly struggling for words - Okemahwasin alluded to his treatment and abuse in an Indian residential school as a child. "I'm not trying to sound like a victim here. ... Being 10 years old, who do I go to? How do you tell someone that?" he said. "My life was ruined. It was taken. ... Alcohol was the only ah - ," he said, his voice trailing off. On June 8, 2014, Garry Tatham left home early that Sunday morning to go wash his wife's car. Around 7 a.m., he was stopped at a red light on Albert Street at 6th Avenue North when a Ford F-150 driven by Okemahwasin slammed into the rear of the car. The then 41-year-old Saskatoon man had been spotted driving recklessly on Highway 11 earlier that morning. (…) In May 2015, Regina provincial court Judge Jeff Kalmak off sentenced Okemahwasin to nine years in prison after he pleaded guilty to impaired and dangerous driving causing death. With credit for time already served, seven years and seven months remained on the sentence. Postmedia Network (Leader-Post, A1, StarPhoenix)

*** Vancouver court to hear appeal in Armstrong teen's murder**
The man found guilty of murdering an Armstrong teen in 2011 will have his appeal heard tomorrow in Vancouver. Matthew Foerster was sentenced to 25 years in prison after a jury found he had beaten and killed 18-year-old Taylor Van Diest on Halloween of 2011. Her body was discovered along some train tracks. Foerster was given no chance of parole after he was convicted. The now 30-year-old was found guilty in 2014. 640 Toronto; Global News

*** Disgraced fire official paroled**
Robb Kidd, a former top-ranking officer with the Kingston Fire Department, is back in the news tonight. He's appealing his sentence on sex-related crimes. But C-K-W-S news has learned that while waiting for a July court date — Kidd has been released from custody. Here's Newswatch's Morganne Campbell. He spent three decades as a rising star within Kingston's Fire Service, acting as the assistant to the Fire Chief and director of fire prevention. That was until Robb Kidd's dramatic fall from grace. Convicted of making and possessing child pornography, indecent exposure and voyeurism in March of last year. And after serving only one sixth of his nearly four year prison term…..Kidd is free on parole — and is residing at his home in Battersea. Kidd was granted full parole last week under a former policy which was abolished in 2014, but still applied to Kidd because his case was grand-fathered. Holly Knowles: "Accelerated Parole Review is a review that takes place by the Parole Board of Canada for first time offenders who are convicted of non-violent offences." (…) The parole board has also advised Kidd not contact any of his victims or their families, and must continue treatment for sexual deviancy. CKWS (2016-06-09)

'Violent sexual offender' faces new charges
A man Yellowknife RCMP previously warned the public about and called a "violent sexual offender" now faces 10 new charges, including sexual assault, in Pangnirtung, Nunavut. Jonah Keyuajuk was subject of the rare public warning that said he poses "a risk of significant harm to the public" in August of last year when he was being released at the end of a jail sentence. Police applied to have a judge place strict conditions on his freedom after release. Within a day of being released here last summer, he was charged with and later convicted of violating his conditions. (…) Keyuajuk returns to court June 14 in Iqaluit. He has numerous violent and sex-related crimes on his record. A 2014 psychological assessment diagnosed him as a psychopath. A Parole Board of Canada report about Keyuajuk from 2014 states the man had denied committing crimes and claimed he was wrongfully convicted. The report states during an interview with a psychologist he denied he required treatment for sexual offences, that he has an anger problem and he minimized his offences against women. Yellowknifer

Sentence hearing looms for men who worked together to kill mobster
Six of eight men implicated in the Nov. 24, 2011 murder of Salvatore Montagna are scheduled for a sentence hearing Friday. The six pleaded guilty March 30 to being part of the conspiracy to murder the mobster. Here is a breakdown of those involved: Paul Cherry writes. (…) CALOGERO MILIOTO, 45: Prior to his arrest in connection with Montagna's murder, Milioto had been arrested twice before in Quebec but the charges never stuck. One of those cases involved Project Crosière, an investigation into how several criminal organizations based in Quebec were purchasing cocaine from a Mexican drug cartel and smuggling it into Canada. More than 60 people were arrested in the investigation in 2008 including Milioto and Antonino Milioto, who was reported to be Calogero's father. A search warrant at Antonino Milioto's home turned up 10 kilograms of cocaine and he ended up serving a 66-month prison term. According to decisions made by the Parole Board of Canada while he served that sentence, Antonino Milioto was considered by police to be a member of the Mafia in Montreal. Montreal Gazette, A5

*** Top court may examine dangerous offender law**
A fight over the constitutionality of the dangerous offender law is headed for the Supreme Court of Canada. Vancouver lawyer Gary Botting is seeking leave to appeal to Canada's highest court a recent B.C. court ruling that upheld the law following an earlier ruling that struck it down as unconstitutional. Botting, who represents dangerous offender Donald Boutilier, says that if the Supreme Court agrees to hear the appeal, a lot will be riding on it, since at least a dozen other cases have agreed to await the outcome of the case in which he is involved. In May 2012, Boutilier pleaded guilty to two counts of robbery, assault with a weapon, two counts of use of a firearm in the commission of an offence and dangerous driving. The Crown sought to have him declared a dangerous offender, but Botting argued in court that the law was unconstitutional because it had removed the discretion of judges to consider prospects of treatment at the "designation" stage of the process, leaving it for the sentencing stage. In declaring the law unconstitutional, Justice Peter Voith found provisions of the law to be overbroad and capable of including a category of offender who might not actually be dangerous, such as people who were mentally unwell or drug addicted and might have prospects for treatment. The judge suspended his declaration of invalidity of the law for a year to give Parliament a chance to amend the dangerous offender legislation. However, he refused to grant Boutilier an exemption and declared him a dangerous offender. Vancouver Sun, A13

*** Guides finish week of training ahead of KP tours**
It's the hottest ticket in town this summer. Tens of thousands of tickets have already been sold to take a tour of Kingston Penitentiary. Guided tours of the notorious prison start on Tuesday. But as Newswatch's Paul Soucy found out, tour guides were getting their training today. This is how most summer student jobs start – with orientation. But this summer job – is anything but ordinary. These 31 students are training to be tour guides at Kingston's newest attraction. CKWS (2016-06-09)

*** This Is Not My Life: A Memoir of Love, Prison, and Other Complications**
An opinion piece states, "I once managed a local museum where, occasionally, individuals charged with misdemeanours would work off their community service hours. One of them, call her "Wanda," was an intelligent and capable single mother. She and I were the same age, and often discussed personal

relationships. I talked about my lack thereof, and she talked about her boyfriend, incarcerated at the Atlantic Institution, a federal corrections facility for repeat and violent offenders in Renous, New Brunswick. One day, when Wanda was chatting about a recent visit there, she asked, "Why don't you come up with me some weekend? There's lots of really nice guys in there." I politely turned down her suggestion, but what if I had seriously considered it as an opportunity for romance? Perhaps I'd now have a story similar to that of Diane Schoemperlen, a Governor General's Literary Award–winning Canadian novelist and short-story writer whose five-year relationship with an inmate of the former Frontenac Institution in Kingston, Ontario, has resulted in her latest book, the memoir *This Is Not My Life*. It's an often frustrated – and frustrating – account of how Schoemperlen, damaged, needy, and full of romantic notions, allows her life and well-being to become secondary to that of "Shane," equally damaged and needy – but also inherently dangerous. (…)Self-examination aside, Schoemperlen recounts the quotidian details common to the partner of a prison inmate, including the intense inventory of self, clothing, and driver's licence in preparation for visits, writing letters to parole officials, psychologist appointments, frantic middle-of-the-night phone calls, delays, and disappointments. She also describes her relationships with other inmates and their families, the prison employees, and the inner workings of the carceral system, and becomes something of a prisoners' rights crusader, denouncing Bill C-10, the Conservatives' "tough on crime" legislation." Quill and Quire (2016-06-09)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Criminalité en baisse et accidents routiers en hausse**
Avec 14 078 infractions au Code criminel en 2015, la ville de Laval a connu son plus bas nombre en 5 ans, apprend-on dans le rapport déposé par le Service de police de Laval (SPL) devant le conseil municipal, le 7 juin. Pierre Brochet, directeur du SPL, rappelle que cette tendance est observée un peu partout en Amérique de Nord. «Chez nous, il faut tout de même souligner l'ajout de nouvelles techniques d'enquête où nous nous attaquons directement aux réseaux, ce qui amène nécessairement une telle diminution», mentionne-t-il. Les crimes contre la propriété et la personne ont notamment connu une baisse respective de 6 et 12 % par rapport à l'an dernier. Courrier Laval (2016-06-09)

*** Crime, collisions were up in Timmins in 2015**
Timmins Police Service processed roughly 25% more criminal charges last year than the year before. That was just one of the facts revealed Thursday as police chief John Gauthier presented the 2015 annual report to the police services board. Timmins Press (2016-06-09\0

*** Fentanyl-related fatalities up 200% in Fort St. John –**
Fentanyl-related fatalities are up 200 per cent in Fort St. John and the North Peace so far this year, according to new data released Thursday by the BC Coroners Service. In the first four months of the year, there have been six fatal fentanyl-related overdoses in Fort St. John, Pink Mountain and Wonowon -- a sharp increase from the two deaths reported in all of 2015. The numbers were updated from the Coroners Service's last report on May 13, when just two fentanyl fatalities were reported so far in 2016. "The revised data has been updated to reflect more final toxicology reports," said spokesperson Barb McLintock. In each of the deaths, fentanyl was detected either alone or in combination with other drugs, the Coroners Service says. Alaska Highway News (2016-06-09)

*** Illicit drugs overtake car accidents as the number-one cause of unnatural deaths in B.C.**
So many people have died of overdoses in B.C. this year that illicit drugs are now killing more people than automobile accidents. That's according to the province's chief coroner, who was in Vancouver today (June 9) for a meeting about the problem that was hosted by the B.C. Centre for Disease Control. "Last year, there were 300 deaths in motor vehicle incidents, and this year, as the minister said, we've had 308 deaths already from illicit drug overdoses," Lisa LaPointe said at a news conference. "If this trend were to continue, we'd be looking at about 750 deaths this year. So it's hugely significant. The number of people dying from illicit drug overdoses is higher than any other unnatural category." Straight (2016-06-09)

*** Alberta fentanyl-death data to be more detailed: government**

Alberta's fentanyl-related death data will be more detailed so that information will better target prevention efforts, according a spokesman with Alberta Justice. In late May, Alberta Health issued a release saying it's taking immediate steps to strengthen surveillance measures at the Office of the Chief Medical Examiner, after W-18 was linked to an overdose death. Dan Laville, spokesman for Alberta Justice, said the new surveillance measures will also include reporting fentanyl-related deaths on a quarterly basis and assigning someone to a director level to oversee other duties. "We're looking at the type of information that will target prevention efforts," Laville said. Metro News (2016-06-09)

*** La police en Ontario parle Arabe? C pas vrai!**
Des images de voitures du service de police de la ville de London, en Ontario, ont été largement reprises et partagées sur les réseaux sociaux au cours des dernières semaines. La raison de l'intérêt des internautes pour ces photos? Le texte en arabe sur les voitures de police qui a suscité énormément de commentaires, questions et appels adressés au Service de police de London. (…) Les réactions négatives liées à l'arabe peuvent sans doute être attribuées à la propagation sur internet d'un discours islamophobe qui va de pair avec l'augmentation des incidents à caractère islamophobes à travers le monde. Un sondage mené par Angus Reid Public Opinion en 2013 et dont les résultats avaient été publiés par la revue Maclean's, faisaient état d'une détérioration de la perception de l'Islam à travers le Canada au cours des quatre années précédentes. La façon dont les Canadiens voyaient les autres grandes religions — le christianisme, le judaïsme, le sikhisme, l'hindouisme et le bouddhisme — n'avait quasiment pas changé alors que l'islam était perçu négativement par une majorité des Canadiens Le maire de London, Matt Brown, a fait part de son outrage concernant un présumé incident raciste. La victime, un étudiant du nom de Mohammad Sharifi, a déclaré à la CBC que les deux agresseurs lui auraient crié plusieurs insultes racistes avant de le frapper à plusieurs reprises au visage. Il s'agit là du troisième incident impliquant des insultes raciales au cours des huit derniers mois à London, poussant ainsi le maire de la ville à prendre position contre la discrimination et la xénophobie. Il a déclaré : « Nous devons faire de notre communauté un environnement sûr et inclusif pour tous, indépendamment de la race, le sexe, l'orientation sexuelle — quoi que ce soit, » a-t-il dit. « Les crimes haineux ne seront absolument pas tolérés à London. Ils ne devraient être tolérés nulle part dans la province ou le pays. » Radio-Canada (2016-06-09)

*** Tight cop budget slowing response times: union**
A tight Winnipeg police budget has sparked longer emergency response times this year, according to the head of the Winnipeg Police Association. "To prevent layoffs, they've had to sacrifice safety," said Moe Sabourin, the union's president. Sabourin notes police tweeted warnings about long wait times due to high call volumes that exceeded resources twice in late May. "Our calls for service are right off the (chart). Where we are today, the calls for the services are 10,000 more than they were at this point last year," said Sabourin. On May 28, for example, police noted there were more than 150 calls in the queue throughout much of the previous night. Sabourin believes that's why he personally had to wait 30 minutes for backup after making an off-duty theft arrest on May 27, a top priority call he said would usually trigger a response within about five minutes. "It is a safety concern ... Thirty minutes is completely unacceptable," said Sabourin. Winnipeg Sun (2016-06-09)

*** There are perverts everywhere, but we needn't tolerate them**
An opinion piece states, "The perverts: We brush them off, most of the time. That guy on the sardine-packed subway rubbing his groin against your bum and you're just not sure if it's unavoidable proximity or deliberate pressing of the flesh. Because females are socially engineered to just let it ride. (…) From the police blotter in recent weeks: A 13-year-old girl followed through Fairview Mall by a male who took photographs "deemed sexual in nature"; a man videotaping women in the washroom of a downtown business; another man caught by a mall security guard using the phone on his camera to videotape under the door of a changing stall; a man arrested after aiming his cellphone up a woman's skirt on the subway; the pounce-and-run sex assaulter at the Finch station; a 36-year-old charged with four counts of sex assault on the Bloor-Danforth line; 46 counts of voyeurism laid against a Brantford man who allegedly used electronic surveillance devices to surreptitiously record three females when they showered. The Sûreté du Québec cop accused of spying on couples in a Quebec City hotel - by appropriating a security camera from the National Assembly. (…) Last year, the TTC reported 56 sexual assaults on Toronto's subway system - any type of touching of a sexual nature - down 16 per cent from 2014. The crime,

however, is largely under-reported and, in crowded subway cars, a passenger might not even realize she (or he) has been targeted or touched." Toronto Star, A2

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

*** Justice dept. pledges to save money**
Manitoba's most popular baby names these days are Liam and Emily, Justice Minister Heather Stefanson revealed Thursday morning. Stefanson announced the information as the minister responsible for vital statistics, as she and critic Andrew Swan kicked off a civil and relatively tame first hour of committee hearings into Stefanson's departmental budget. Former NDP justice minister Swan repeatedly pressed Stefanson to say whether the Pallister government has established a cabinet committee on healthy children - which the NDP contends it is required to do by legislation - and whether it has constituted an aboriginal issues committee. Stefanson repeatedly answered that both are important issues, but such committees are not within her jurisdiction. Stefanson acknowledged she and Municipal and Indigenous Relations Minister Eileen Clarke will have the lead roles in Manitoba's involvement in the national inquiry on murdered and missing indigenous girls and women. Said Swan: "She's making the case that the aboriginal-issues committee needs to be constituted as quickly as possible." Winnipeg Free Press, A4

*** Despite progress, domestic violence rates still high**
Maria Hendrika has a penchant for sticking things through. If her long tenure with Regina Transition House wasn't enough, she has also been involved in the Provincial Association of Transition Houses and Services of Saskatchewan (PATHS) since its inception 30 years ago. The group was formed to provide a single voice for shelters, share best practices and set standards. (…) Saskatchewan has the "dubious distinction," as Hendrika called it, of having the highest rates of domestic violence and sexual assault as well. She wants to ensure that reports of assault are taken seriously and that there are safe ways for women to report. She would also like to see more attention paid to missing and murdered indigenous women. "This is a huge issue. People talk about murdered and missing like it's just a thing. No, these are people," said Hendrika. "These are daughters; these are wives." StarPhoenix, BR10

*** Iskwe draws from identity in her art**
With her face masked in geometric shapes, singer Iskwe appears like an abstract painting. She at first gives the impression that she is an upbeat R&B singer before quickly showing her art goes much deeper than that by moving to spoken word and songs that reflect her Dene-Cree and Irish background. Going only by her stage name, which translates to "woman" in Cree, Iskwe is bringing her chameleon-like performance to Yellowknife this summer for Folk on the Rocks. (…)While it certainly took time to raise enough money for the studio space, Iskwe explained she needed those extra years to grow into the singer she is today. Her first album touches on the usual subjects of love, loss and self reflection but her most well-known track titled Nobody Knows picks up on a more serious topic. After the 15-year-old indigenous girl Tina Fontaine was murdered in Winnipeg, Iskwe was both devastated and touched to see her community gather and share their sadness. The song is an ode to the 1,500 missing and murdered indigenous women across the country. "I had been hearing from a lot of people that have been impacted directly and it had been very much around me and this one acted as that tipping point," Iskwe said. "The numbers are so high and it came at that moment where it was like, 'That's enough. No more of this.'" Yellowknifer

*** Not Completely Happy**
An opinion piece states, "Not sure if you should be celebrating National Aboriginal Day on Tuesday, June 21?? Me either. Sure, I love an Indian Taco (the messier, the better) just as much as the next person. I absolutely *adore* a loud and colourful powwow outdoors on a summer day, and I most *certainly* am thrilled to celebrate the wide array of indigenous artists, authors, academics and awesome community builders across Turtle Island on a year-round basis. But if we're talking history, we can almost guarantee it's not all calories and colourful culture. (…) Saskatchewan has been a leader in missing persons for quite some time. According to CBC's database, there are 32 indigenous women who called Saskatchewan home

before they vanished. In January 2015, Nadine Machiskinic was brought to the hospital at four in the morning after being found injured at the bottom of a laundry chute of the Delta Hotel in Regina. Police issued a statement saying the "death of Machiskinic revealed no indication of foul play."A coroner's report, on May 20 says the 29-year-old mother of four's death was "accidental". "A young aboriginal woman, who lived a high-risk lifestyle in the sex trade, ends up at the Delta Hotel at 4 a.m. CST, and falls down a laundry chute and it's not anything to be considered suspicious?"Delores Stevenson, aschiskinic's aunt, told CBC. Machiskinic's death is just another story with details that barely skim the surface of Saskatchewan's dark, complex problems rooted in the ongoing effects of colonialism. Cases like Machiskinic's are common across the country. Within the past year, indigenous people are, yet again, faced with a system that continues to fail them." Planet S (2016-06-09)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Liquor board bosses, RCMP take part in planning for legalized marijuana market
Liquor board heads from across the country have quietly been meeting in New Brunswick with government officials from each province over the future sale of marijuana. The private gathering in Saint Andrews included a presentation from a top federal enforcement cop, panel discussions with industry growers, and research from policy experts in preparation for the sale, distribution and regulation of pot - now that Ottawa is moving toward legalization. The result of the multi-day meeting will now see liquor bosses move to brief their respective governments on the best practices they discussed at length with North America's top marijuana authorities. "Attendees were from the liquor boards, the Departments of Public Safety from each province and senior leaders from the beverage alcohol industry," said NB Liquor president and CEO Brian Harriman in an email. The Telegraph-Journal reported earlier this year that the NB Liquor boss has been heading research by liquor boards from across the country to prepare for legalized pot. The annual summer meeting of the Canadian Association of Liquor Jurisdictions was then slated for New Brunswick, stretching from this past weekend until Wednesday, with an entire roster of marijuana players lined up to speak. That included RCMP Cpl. Shane Holmquist, a supervisor on the Federal Serious Organized Crime Section's marijuana enforcement team. (…)Harriman said the meeting had more than 200 attendees from across Canada. Provincial government spokeswoman Elaine Bell said it was actually the Department of Public Safety that hosted the Association of Liquor Administrations of Canada at the annual conference. "While the legalization of marijuana is a federal decision, the working group of officials from multiple departments and agencies continues its work in anticipation of legislation to be tabled by the federal government in the future," Bell said. The working group is gathering research and assessing policy implications, with a balanced focus on examining health and safety risks and identifying job and revenue-generation opportunities for the province." Prime Minister Justin Trudeau has proposed legalizing and regulating pot, also pledging to work with local authorities to come up with distribution methods, which could vary from province to province. Times & Transcript, A1 (Telegraph-Journal, Daily Gleaner)

*** Despite the crackdowns, marijuana entrepreneurs are betting on "edibles"**
Virginia Maria Vidal started medicating with marijuana in 2003, after the birth of triplets left her with post-natal discomfort. She ran into trouble over the years, once being arrested, charged, and eventually acquitted of possessing 19 grams of pot. Even after obtaining a licence to use medical marijuana, the 45-year-old mother of six and caregiver to a grandparent with dementia found the smoke to be a nuisance and embarrassing. So she ground it into tea instead. (…) Ms. Vidal says the crackdowns aren't having a big impact on revenue – she also sells her product online and says demand is growing – but she's still worried. "It's going to be quite the battle," she says. "We need our Prime Minister to stand with us." Producing edibles in any form is illegal, however jurisdictions such as Vancouver and Victoria have chosen to ignore the law and regulate them instead. The federal laws are rarely enforced because the framework of regulations governing marijuana for medical purposes is evolving, and unlicensed producers continue to sell in stores or by mail. Last year, a Supreme Court judgment ruled that licensed patients couldn't be limited to consuming cannabis in smoking form only, but did not comment on the legality of edibles. Further, in February a federal court struck down restrictions preventing licensed patients from growing their own medical marijuana, giving the government six months to rewrite the laws. Globe and Mail

PUBLIC SERVICE / FONCTION PUBLIQUE

Nil

OTHER / AUTRE

Canadian imprisoned: 'She won't be able to cope': Retired professor was studying women's role in Iranian Politics
Homa Hoodfar, the recently retired Concordia University professor detained in Iran, was researching women's participation in political life in Tehran when she was arrested and held for interrogation by Iranian security forces this week. She has not been permitted to leave Tehran's Evin prison since Monday, and has been denied access to both legal counsel and consular assistance. The prison is notorious around the world for its housing of political prisoners, and in Canada because of the 2003 torture death within its walls of Montreal-based photographer Zahra Kazemi. There are fears Hoodfar is being used by hardline leaders of the Revolutionary Guard to pressure the more conciliatory President Hassan Rouhani, under whose rule Iran has agreed to nuclear regulation in exchange for the easing of sanctions. Hoodfar, 65, who has Iranian, Canadian and Irish passports, was first arrested in March as she was preparing to leave Iran to celebrate Nowruz, the Iranian new year, with her family in Britain. Her computer, books, passport and personal effects were seized. Freed on bail, she was interrogated at various times over the weeks since, largely over her research during Iran's recent election, in which 17 women were elected, most aligned with Rouhani. Postmedia Network, A1 (National Post, London Free Press, Windsor Star, Montreal Gazette, Ottawa Citizen, Vancouver Sun, Calgary Herald, StarPhoenix); Globe and Mail

* **Clock is ticking on Canadian hostage Robert Hall's life**
Robert Hall may have just about 72 hours left to live. The family of John Ridsdel knows that the murderous, ISIS-inspired thugs known as Abu Sayyaf meet their deadlines. Ridsdel was beheaded April 25. Unless they get somewhere between $8 million and $16 million, the radicalized Islamic group that has terrorized the province of Mindenoa in the Philippines have set the date for fellow Canadian Hall's turn. June 13 — this Monday — at 3 p.m. they say they will kill him. Those close to Hall don't believe Abu Sayyaf are bluffing and are hoping for a movie-style saviour mission for the one-time Calgarian, held with his Filipina girlfriend, Marites Flor, and Norwegian Kjartan Sekkingstad. Winnipeg Sun

* **An international anti-corruption court is a fine idea, but not necessary**
An opinion piece states, "Managing partner of Martin Kenney & Co., Solicitors, a specialist investigative and asset-recovery practice focused on multijurisdictional fraud and grand corruption cases. He is co-chair of ICC FraudNet's Task Force India. As a Canadian I find it encouraging that my compatriots could be at the forefront of the attack on grand corruption and its perpetrators. But while the idea of Canadian backing for an international anti-corruption court is commendable, I believe the world already has existing systems in place to deal with these issues. For example, it is likely that the nature of the criminal offences described in a recent Globe and Mail op-ed by Harvard University's Robert Rotberg already fall within the remit of the existing International Criminal Court (ICC). This court, based in The Hague, has the power to try war crimes, genocide and crimes against humanity under the Rome Statute. Grand corruption should be considered a crime against humanity under Article 7(1)(k) of the Rome Statute, which punishes "other inhumane acts ... causing great suffering, or serious injury to body or to mental and physical health." Adopting such an understanding of grand corruption, as advocated by many human-rights organizations and commentators, would place its prosecution under the remit of the ICC. If criminals effectively suck the financial lifeblood out of a country, it leaves the country devoid of infrastructure and denies children education and the populace basic medication and health care. It leads, over all, to a torturous existence. This undeniably causes great suffering and serious injury to mental and physical health. This is why grand corruption is a slow, painful and degrading crime against humanity." Globe and Mail, B4

* **Coup de filet contre le trafic de faux médicaments**

Un vaste coup de filet mondial contre le trafic de faux médicaments a permis l'arrestation de 393 suspects et la saisie de millions de produits potentiellement dangereux, d'une valeur estimée à 67,5 millions de dollars canadiens, a annoncé Interpol jeudi. La neuvième opération Pangea, qui a rassemblé les polices de 193 pays, du 30 mai au 7 juin, a permis la saisie d'environ 12,2 millions de faux médicaments et la suspension de 4932 sites Internet proposant ces produits délictueux. Près de 700 enquêtes ont été lancées à travers le monde, précise l'organisation policière internationale basée à Lyon (est de la France), dans un communiqué. Agence France-Presse (Le Devoir, A5)

*** Increase police funding, former Canadian officer says**
A former senior Canadian police officer has advised that funding be increased to train the local police force to investigate money laundering and other financial crimes. The advice comes from former National Director of the Royal Canadian Mounted Police Proceeds of Crime programme Garry Clement who will participate in the 8th Annual Anti Money-laundering and Financial Crimes Conference in July. Speaking on Thursday's OBSERVER AM programme, Clement said, "I think we've done a great job of putting in regulations requiring our financial institutions to have stringent standards and a lot of reporting. But governments don't put the commensurate amount of requirements on law enforcement." Speaking of the Americas in general, Clement said, "I think there is probably an erosion of ability because they haven't put as much money into it as they probably should." The former national director's advice was to increase law enforcement cooperation to tackle financial crimes. "When you look at the Caribbean islands, there's probably some value at law enforcement looking at partnership taskforces... sort of a white collar crime task force," Clement said. Antigua Observer

INTERNATIONAL

Suicide bombings kill 31 in, around Iraqi capital
Two suicide attacks in and around the Iraqi capital on Thursday killed at least 31 people and wounded dozens, officials said. The deadliest attack took place in a commercial area of a majority Shiite neighbourhood in Baghdad. At least 19 civilians were killed and 46 wounded, police said. Another suicide bomber rammed his explosives-laden car into an Iraqi army checkpoint north of Baghdad, killing at least 12 people, police said. Seven civilians and five troops were killed in the attack in the town of Taji, about 20 kilometres (12 miles) north of the capital, a police officer said. At least 32 people were wounded, he added. Medical officials confirmed the casualty figures. All officials spoke on condition of anonymity as they were not authorized to brief the media. In an online statement, the Islamic State group claimed responsibility for the attack in the New Baghdad neighbourhood, saying it targeted Shiite militia members. It later claimed responsibility for the Taji bombing in a second online statement, saying it was targeting the Iraqi army. The Associated Press could not verify the authenticity of the statements, but they were posted on a militant website commonly used by the extremists. Associated Press, B6 (Telegram)

*** Kurdish militant group says it was behind Istanbul bombing**
The Kurdistan Freedom Hawks (TAK), an offshoot of the outlawed Kurdistan Workers Party (PKK) militant group, said on Friday it carried out a suicide bombing in Turkey's biggest city Istanbul this week that killed 11 people. A car bomb ripped through a police bus in central Istanbul during the morning rush hour on Tuesday near the main tourist district, a major university and the mayor's office. Reuters (CBC News)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
June 13, 2016 / le 13 juin 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Saskatchewan reeling after Orlando shooting
Dan Shier, co-chair of Regina Pride, was celebrating Saskatchewan Pride Month in Saskatoon when he heard the news: Fifty people died and another 53 were injured after a shooting in a gay nightclub in Orlando, Fla. "Obviously, kind of shock and some remorse with the news, and some heavy hearts," Shier said. The Queen City is gearing up for its own pride celebrations, kicking off on June 18, 2016. And while the shooting will be on everyone's minds, the festivities will continue as planned. (…) **Ralph Goodale**, **Minister of Public Safety and Emergency Preparedness**, also spoke about the shooting. "***We have to make sure that we are doing everything we can do to make sure Canadians are safe,"*** **Goodale** said in a phone interview. ***"As Canadians in this month celebrate pride in many ways, it's extremely important now that those celebrations go forward, and go forward with a sense of determination and safety and security."*** CTV News (2016-06-12); 620 CKRM; * CBC News

*** Regina's LGBTQ community and religious group 'condemn' deadly shooting in Orlando**
Regina residents described their shock when they heard the news about the deadliest shooting in U-S history where 50 people were killed at a popular gay nightclub in Orlando. "I'm shaking, not sure if you

can tell, but I'm shaking because of all of it," Lisa Phillipson said. Phillipson is the contracts director with Queen City Pride. She said the shooting hate crime shows there's a need for more public education. "And the fact that this shows that reinforces the need that we need to have more activism and more parades and more marches," Phillipson said. **Public Safety Minister Ralph Goodale** said there's no immediate threat to Canada at this time. He noted that when tragedies like this occur, security detail does increase. ***"Everything is double checked and triple checked,"*** **Goodale** said. ***"There is no immediate connection to Canada in any way."*** – **Goodale**. He also expressed his condolences to the family, calling the shooting a ridiculous and sad brutality. ***"Our thoughts and prayers go out to the victims and their families who are suffering through an absolutely unspeakable and entirely tragic loss,"*** he said. Global News (2016-06-12)

Le Canada condamne la tuerie survenue à Orlando
La classe politique canadienne a condamné le carnage survenu dans une discothèque d'Orlando, en Floride, qui a fait 50 victimes et des dizaines de blessés, dimanche. Le premier ministre Justin Trudeau a publié un communiqué dans lequel il s'est dit « profondément choqué et attristé d'apprendre la nouvelle au sujet de la fusillade à Orlando, en Floride, qui a fait tant de morts et de blessés ». Il a ajouté qu'il « est effroyable de penser qu'au moins 50 vies ont été perdues en raison de cet acte de terrorisme intérieur visant les membres de la communauté LGBTQ2 ». (…) Le **ministre de la Sécurité publique** du **Canada Ralph Goodale** a écrit sur Twitter qu'il était bouleversé par ce qui est considéré comme la pire tuerie par balle de l'histoire des États-Unis et que les Canadiens condamnaient une telle violence. Selon les policiers américains, l'attaque a eu lieu dans la nuit de samedi à dimanche, lorsqu'un tireur a ouvert le feu dans une boîte de nuit gaie. L'assaillant est mort plus tard sous les tirs des policiers. **M. Goodale** a ajouté que ses prières et ses pensées allaient vers les proches des victimes. ***Choqué à la fusillade meurtrière à Orlando. Les Cdns condamnent cette violence brutale. Pensées + prières avec victimes et proches.-*** **Ralph Goodale (@RalphGoodale**) 12 juin 2016. Presse canadienne (Le Devoir, Express Drummondville); Journal de Montréal (2016-06-12)

Akwesasne Mohawks want Canadian government follow-through on independent oversight of border services agency
In light of its longstanding and difficult relations with the Canada Border Services Agency, the Mohawk Council of Akwesasne is supporting creation of an independent oversight mechanism for the operations of the border agency. The Canadian government recently signaled that it is looking for ways to improve transparency and increase public confidence in the CBSA, according to a press release from the MCA. Akwesasne community members routinely cross through the CBSA port in Cornwall, Ontario, sometimes several times a day, while traveling from one part of the community to another to travel to work, attend school, attend health related appointments, visit family, or otherwise meet social, cultural, economic, and recreation needs, the MCA said in a statement. (…) The Canadian **Minister of Public Safety and Emergency Preparedness Ralph Goodale** said the government is examining how to best provide the CBSA with appropriate review mechanisms, particularly after numerous civil rights groups have called for the creation of an independent watchdog to oversee the border agency. On May 26, MCA Grand Chief Abram Benedict wrote to **Minister Goodale** expressing the Mohawk Council's support for the establishment of an independent oversight mechanism for the CBSA. "While we appreciate the importance of ensuring that the border is secure for national security as well as for the safety of all citizens, we expect CBSA to treat people with respect in an open and transparent manner. Law enforcement officials should be held to the highest standard of review and scrutiny in their interaction with the public," the MCA statement said. North Country Now (2016-06-12)

"The Chinese Foreign Minister recently scolded a Canadian journalist for asking about China's human rights record in a press conference in Ottawa and while here demanded a meeting with the PM. Do you think the federal government responded appropriately?"
Mathieu R. St-Amand, Bloc-Québécois strategist: "The Chinese government's difficulty with the concept of a free press is nothing new. By expressing its dissatisfaction to the Chinese about an objectionable statement by one of that country's diplomats, the Trudeau government has done the bare minimum of what would be expected in such a situation. "However, if this government is serious about promoting freedom of the press, it should call an inquiry into the surveillance of two *La Presse* reporters by the RCMP. Beyond **Public Safety Minister Ralph Goodale's** rhetoric, the government should take this direct

attack on the freedom of the press seriously. A public inquiry would shed light on several unanswered questions about RCMP practices. By not calling an inquiry, the government is attempting to cover up one of the most serious attacks on freedom of the press in recent years. "Canada must defend freedom of the press at home in front of countries where this freedom is curtailed. However, the government needs to do more than simply lecture offenders; it must ensure that this freedom is unrestricted here. Justin needs to lead by example instead of talking down to people for once." Hill Times

Canada's surveillance crisis now hiding in plain site
An opinion piece by Michael Geist states, "Three years ago this month, Edward Snowden shocked the world with a series of disclosures that revealed a myriad of U.S. government-backed surveillance programs. (…) While these programs attracted attention for a day or two, it was the Conservatives' introduction of Bill C-51, the anti-terrorism legislation that granted the government a host of new powers, that finally succeeded in generating a sustained focus on Canadian surveillance law. The bill became law with few amendments, but emerged as the public's shorthand for the need for reforms to surveillance activities. **Public Safety Minister Ralph Goodale** and the new Liberal government have promised changes, with expectations that they will focus initially on a new "super" oversight body for security agencies and later open the door to further amendments. Yet despite assurances that improved oversight will provide adequate safeguards against intrusive surveillance, in recent months it has become apparent that weak oversight represents only a small part of the problem. Consider this year's report from the Communications Security Establishment (CSE) Commissioner, who uses legal language to obscure an otherwise clear admission that there are ongoing metadata violations within the CSE. The report notes that metadata activities were "*generally* conducted in compliance with operational policy" and that the "CSE has halted *some* metadata analysis activities" that were the subject of previous criticisms. The use of words like "generally" and "some" are no accident. The CSE Commissioner could have just as easily written that the CSE still does not conduct its metadata activities in full compliance with the law and that it has refused to stop some activities that were the subject of complaints. Yet the soft framing turns what should be a major story and source of concern into something largely ignored by the general public." Hill Times (Toronto Star)

*** Will Liberals defend Charter values on C-51?**
An editorial states, "When did the federal Liberals stop being liberals? In recent weeks we've seen an allegedly liberal government swerve, dodge and obfuscate to justify a bill - C-14 on assisted dying - which some courts and many constitutional scholars agree does not respect the Supreme Court's decision on Charter rights. The Supreme Court gave Trudeau one job to do. They even made it simple by giving him the language to use. Some provinces already had rules he could adapt. (…) Triangulation is the same strategy that, a year ago, lead Trudeau to support Bill C-51, Harper's version of homeland security. As with C-14 , many respected constitutional lawyers and rights groups said sections of C-51 violated the Charter. When an uproar over the moral hollowness of Trudeau's position offended actual liberals, he promised a Liberal government would fix C-51. Recently, the **Minister of Public Security** told the Commons he hopes a C-51 fix-it bill will be tabled ***"before Parliament rises for the summer."*** But will the Liberals fix C-51? Or "balance" it? How will we know? Paul Cavalluzzo - former commission counsel in the Maher Arar inquiry - has done the research on what needs to be fixed to make C-51 Charter-compliant. He's filed an application asking an Ontario court to strike down several provisions of C-51 because they trample Charter rights. His analysis is a valuable scorecard for any forthcoming Liberal bill. "Our main concern is the power C-51 attempts to give a judge to authorize a violation of Charter rights and freedoms if CSIS applies for a warrant to break the Charter," says Cavalluzzo in an interview. "In our view this is totally alien to our constitutional order." He argues the entire idea needs to be scrapped." Winnipeg Sun, A9 (Toronto Sun, Ottawa Sun, Edmonton Sun)

Missing Mountie
An opinion piece states, "Could Bob Paulson's days as top banana of the RCMP be numbered? If he doesn't start showing more cooperation in bringing about fundamental change to the nation's police force, he could be headed for a change in his career path. Some critics would argue it comes not a moment too soon. The organization he runs is more top down than Donald Trump. As the Force evolved in the Harper years, when labour laws were razed like old growth forests, Paulson's Mounties are not exactly members of Dudley Do-Right's RCMP. Paramilitary and politicized, the RCMP is in danger of becoming the fossil

force of law and order in Canada — and far worse, the kept police of the government of the day. Paulson's immediate problem resembles arrogance. As one senator put it to me, Paulson recently "stiffed" a Senate committee by sending deputies — two assistant commissioners — to answer questions regarding Bill C-7, the very controversial RCMP union bill. (…) Despite all that, though, there is a sense amongst his critics that he just doesn't get it. The Chair of the Civilian Review and Complaints Commission of the RCMP, Ian McPhail, testified before the Senate committee that his investigation into workplace harassment, requested by **Public Safety Minister Goodale**, had been impeded by senior Mounties. The Commissioner himself had forbidden McPhail to speak to RCMP members without the members first informing the Commissioner.(…) It is not all on Paulson. Since 2006, the RCMP has acted in such a way as to raise real questions about its independence and its impartiality. That was the year the Mounties weighed in to the federal election in dramatic fashion. Former Commissioner Guiliano Zaccardelli publicly announced an investigation into the then-Liberal government's handling of an income trust tax decision included in the federal budget. The RCMP had two press releases prepared to announce their investigation a month away from the election — one including the minister of the day's name, **Ralph Goodale**, and the other leaving it out. They opted to name, and some might say shame, the minister." iPolitics (2016-06-12)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Wildfire / Feu de forêt à Fort McMurray

*** South African President drawn into firefighters' pay dispute**
As 300 disgruntled South African firefighters prepared to fly home from Alberta on Sunday, questions were mounting over a contract that gave them barely one-third of the daily amount Alberta had allocated for their services. The issue has sparked a political uproar in South Africa that reached the highest levels on the weekend, when President Jacob Zuma ordered his environment minister to find "a solution to the impasse." While some South Africans criticized the firefighters for going on strike just six days after beginning their work in Alberta, many others - including an opposition leader - said their strike was justified by the need to fight for their rights and equal pay. Alberta Premier Rachel Notley and other officials have confirmed that Alberta agreed to pay $170 a day for each of the South African firefighters. Yet the firefighters signed contracts in which they will receive only a "stipend" of $50 a day - far below the Alberta minimum wage of $11.20 an hour. This discrepancy was "disturbing" and "not acceptable," Ms. Notley said last Thursday. The payment of $170 daily to their South African employer was intended to cover the $50 stipend, plus their regular South African pay (as little as $10 a day), along with "payroll burden, administration costs, training and other costs of preparing the firefighters to travel," according to Kim Connors, executive director of the Canadian Interagency Forest Fire Centre, which was responsible for bringing the firefighters to Canada. In addition, Alberta is covering all of their costs for accommodation, travel and meals. Globe and Mail, A16; CBC News

Other / Autre

*** Body of missing Corner Brook woman Patricia Boyd found**
A Corner Brook woman who was reported missing two weeks ago has died. The body of 57-year-old Patricia Boyd was found on Saturday. The Royal Newfoundland Constabulary and the Bay Islands Volunteer Search and Rescue Team had been searching places like the North Shore Highway and the Riverside Drive area of Corner Brook in the weeks since Boyd went missing on May 26. CBC News

*** Is another dust bowl coming?**
An opinion piece states "In the 1930s, a bad drought and an economic malaise upended farming systems around North America causing the Dust Bowl. Could climate change and the persistent post-2008 economic doldrums do the same? On one hand, the environmental signals are sobering. The drought in California seems to be long-lasting and even this year's record El Niño, which many had hoped would bring rainfall to the Southwest, seems to have done little. In Africa and India, hundreds of millions are facing food insecurity due to a combination of drought and armed conflict. Meanwhile in Canada, the Prairie Climate Centre has recently published an atlas suggesting the wildfires in Fort McMurray are a

taste of things to come. This year's hot, dry weather is consistent with climate change models that project the number of days reaching above 30°C each year will increase by three to four times in the Prairies over the century… Humanity is on the cusp of a major transformation as we come to grips with the necessity of feeding nine to 11 billion people on an increasingly hot and crowded planet. Thanks to climate change, meeting this challenge requires that we be far more thrifty with our resources and create not only productive but also resilient systems. The tools of the digital agricultural revolution are only just now emerging, but they will come to define how humanity feeds itself in the future. Canada, and the Canadian industry, should be at the forefront of this revolution." Hill Times

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Toronto 18 may have been shock for Canada, but it was not harbinger of a path to ruin
An opinion piece by Phil Gurski, president/CEO of Borealis Threat and Risk Consulting, states, "June 2 marks the 10th anniversary of the arrest of 17 men in the Greater Toronto Area in the culmination of a massive terrorism investigation by Canadian authorities. In what came to be known as the "Toronto 18" (the last subject was arrested in August 2006) Canadians were rudely introduced to homegrown terrorism five years after 9/11. For those who have forgotten the details, here is a short synopsis. A group of men in the Toronto area, led by an Afghan immigrant (Fahim Ahmad), attended a "training camp" near Orillia, Ont., in December 2005, chose three targets (the CSIS office in Toronto, the financial district and a military base), built a detonator, and bought fertilizer, all without knowing that their every move was being followed by CSIS and the RCMP. Their arrest saved the lives of thousands. The event was a seminal one for me as a CSIS analyst and I'd like to reflect on what this meant then as well as what is means now. (…) Fourthly, the case showed that CSIS and the RCMP could work hand in glove to successfully stop a terrorist act from occurring. The investigation started with CSIS and was handed over to the Mounties when it was clear a criminal act was being planned. CSIS sources became RCMP agents (not always an easy thing to do) more or less seamlessly and a serious terrorist attack was averted. There is little doubt that the CSIS-RCMP relationship has had its ups and downs but the two do work together well and Canadians are safer as a result. Lastly, despite more foiled plots and two successful ones in the interim, Canada remains in a good position when it comes to homegrown terrorism. We are not in the same league as France or Belgium or the U.K., or even the U.S. Our government has done a much better job at understanding the threat and putting measures into place, both soft and hard, to deal with it. We had the five-year $10-million Kanishka research project which, although many thought it under-delivered (I am among that group), set the stage for a more robust and more mature academic environment to look at terrorism where none existed before. **Public Safety Canada's** Citizen Engagement branch developed a community outreach program that was the envy of all our allies and the creation of the new Office of the Coordinator for Counter Radicalization and Community Outreach will hopefully enhance this effort. There is more work to be done but these are all enviable achievements." Hill Times

*** Des parcours qui sèment la consternation**
Pourquoi des jeunes dont les parents ont choisi de venir s'installer en Occident, comme c'est le cas du tireur du club Pulse, en viennent-ils à la violence au nom de groupes djihadistes ? Les experts interrogés par La Presse avancent plusieurs pistes. Des études ont démontré que les immigrants de deuxième génération, dont Omar Mateen faisait partie, « peuvent être à risque d'épouser des idéologies supportant la violence », note Jocelyn Bélanger, ancien chercheur au centre contre la radicalisation de Montréal et professeur adjoint à l'Université de New York à Abou Dhabi. Bien que ce soit l'exception, plusieurs exemples d'immigrants de deuxième génération qui ont complètement dérogé des valeurs de leur famille pour adhérer au terrorisme peuvent être observés. Les frères Salah et Brahim Abdeslam, l'un cerveau des attentats de Paris, l'autre mort en déclenchant sa ceinture d'explosifs, ont grandi en Belgique dans la commune de Molenbeek dans une famille ouverte. Nés de parents marocains immigrés en France, puis en Belgique, ils ont eu une adolescence parsemée de petits larcins avant d'embrasser l'idéologie de l'EI à l'insu de leurs proches.(…) Il y a aussi la jeune Maha Zibara, ex-élève du collège de Maisonneuve, arrêtée l'an dernier avec une dizaine de jeunes alors qu'elle s'apprêtait à quitter le Canada. Son père, un entrepreneur d'origine libanaise, était démoli. M. Zibara et sa famille sont de confession chiite, un courant minoritaire au sein de l'islam. Un jour, Maha Zibara a rejeté complètement la voie de ses parents. « Elle est venue me dire que les chiites sont des mécréants », avait-il raconté à l'époque. Pourquoi, alors, des

jeunes nés ici et élevés dans des familles qui n'adhèrent pas aux valeurs islamistes se radicalisent-ils ? Certains enfants issus de l'immigration récente sont perdus, hantés par une ambigüité identitaire, répond Mounia Ait Kabboura, chargée de cours à l'Université du Québec à Montréal et experte du radicalisme islamique. « Ils ne se retrouvent nulle part. Ils sont dans la culture religieuse et dans la culture occidentale, et c'est difficile de mélanger les deux », dit la chercheuse, qui a étudié la question auprès de jeunes établis au Québec. LaPresse+, 14

* **PM soft on terrorists**
A letter to the editor states, "It's a shock to see the "Canadian leading Bangladesh branch of ISILstory on Wednesday. Could someone please explain why the Trudeau government refuses to criminally charge citizens who become terrorists and revoke their citizenship? What incentive is their for a would-be terrorist to stay in Canada knowing this country will do nothing to revoke their citizenship if they return to Canada? The Trudeau government is weak when it comes to our citizens becoming terrorists!" The Province

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Border Security reality TV show pulled for privacy concerns
Canada's border agency is pulling the plug on the controversial reality TV program Border Security after the federal privacy commissioner found the agency violated the rights of a construction worker filmed during a raid in Vancouver. Privacy commissioner Daniel Therrien recently informed the British Columbia Civil Liberties Association, which spearheaded a complaint on behalf of Oscar Mata Duran, that the Canada Border Services Agency breached the Privacy Act by allowing production company Force Four to film the agency's examination of the migrant labourer. "As a matter of principle, it is our view that federal government institutions cannot contract out of their obligations under the Act," says the commissioner's 26-page report of findings. In light of the well-founded complaint, Therrien's office recommended the border agency end its participation in the television program, which the agency agreed to do. Agency spokeswoman Esme Bailey confirmed that Border Security: Canada's Front Line would not return for a fourth season. The commissioner also urged the agency to carry out a formal privacy impact assessment before embarking on any significant future initiative involving the use of personal information. Border Security began airing on the National Geographic Channel in 2012, chronicling encounters between border officers and the public. The unscripted series was seen by millions of Canadians and has aired in dozens of other countries. Times & Transcript, B4 (The Province, Vancouver Sun); Toronto Star; The Canadian Press (Guardian, Cape Breton Post); Chronicle Herald; The Record

* **Réseau de présumés trafiquants de drogue démantelé dans l'Est ontarien**
La Police provinciale de l'Ontario (PPO) a arrêté mercredi dernier cinq personnes lors de la saisie d'une importante quantité de marijuana dans une résidence d'Alfred-Plantagenet. Sur place, les policiers ont saisi des plants, de la résine et d'autres dérivés dont la valeur totale est estimée à 245 000 $.Des hommes de 18, 19 et 39 ans ainsi que deux femmes de 24 et 54 ans devront répondre, entre autres, à des accusations de production et de possession de drogue et de possession d'armes à feu. L'Agence des services frontaliers du Canada (ASFC) avait mené à une première enquête dans cette affaire après avoir contrôlé des colis destinés à une adresse d'Alfred-Plantagenet. Ceux-ci contenaient de la marijuana.

Canada's choice for migrant workers: decent work or entrenched exploitation?
Canada's Temporary Foreign Worker Program (TFWP) is at a crossroads. After years of escalating concern about employers' growing reliance on, and widespread exploitation of, low-wage migrant workers, the Standing Committee on Human Resources, Skills and Social Development and the Status of Persons with Disabilities (HUMA Committee) is reviewing the controversial program and will report to the minister of Employment, Workforce Development and Labour. At this crucial moment, what will Canada choose: secure status and decent work, or entrenched exploitation for migrant workers? Canada's Choice, my new report published by the Metcalf Foundation maps what is at stake. The findings are troubling. Low-wage migrant workers face deeper insecurity now than before the 2014 "reforms" by the previous government. Hill Times

War resister wants PM to keep his word

* An opinion piece states "Like much of the rest of the world, Rodney Watson has spent a lot of the last week thinking about the world's most famous war resister. But Muhammad Ali's televised memorial service Friday had particular resonance for Watson, who watched it from the room above the First United Church in Vancouver's (…) A new Insights West poll released this week shows a majority of Canadians support the idea of making Iraq War resisters like Watson permanent residents of their adopted country. Watson, 38, said he appreciates the widespread support of "the good and conscientious citizens of Canada" evidenced in the poll results, and he hopes the federal government will notice and take action on behalf of himself and 14 other Iraq War resisters in Canada. "For those same ones shedding crocodile tears and praising Muhammad Ali, who have the power to actually do something, I have to say, 'What about us?'" said Watson, who served in Mosul, Iraq, in 2005 and 2006. He left the U.S. for Canada in 2009 to avoid another deployment to Iraq, and sought sanctuary in the First United Church. The Canadian government ordered him deported in 2009." Vancouver Sun, A8

* **Mother of Sask. overdose victim testifies**

It's perfectly legal to buy the ingredients to manufacture the deadly opioid fentanyl. Anyone with an Internet connection can order the stuffonline. Marie Agioritis, a Saskatoon mom who lost her son Kelly to a fentanyl overdose two years ago, is joining forces with a Canadian senator, hoping a new law making those ingredients illegal will put a dent in the fentanyl trade. Q What is the government doing to combat the spread of this drug? A Agioritis was in Ottawa last week testifying at a Senate committee hearing on a new bill aimed at making the ingredients for manufacturing fentanyl illegal. Sen. White, who introduced Bill S-225, says without making the ingredients illegal it's tough for police and customs agents to crack down on the trade. Leader Post

Don't like the airport security line? Pay to shorten it

Let the users pay! Some airport and airline executives have somehow got it in their heads that airport security is like universal health care, and that if wait times at the airport are too long, then the federal government ought to fix things by spending more public money. But if we want to shorten the lengthening lineups at airports, and the way to do it is to hire more security agents, it only makes sense to raise the money to do this from users: airline passengers. Canada's airports are supposed to be user-pay affairs. You pay an airport improvement fee when you fly, and an airport security fee too, embedded in the price of a ticket. Alternatively, the Canadian Air Transport Security Authority can figure out how to become more efficient, and move more people through screening, faster. The last federal Liberal budget gave an additional $29-million to CATSA, but taxpayers shouldn't be subsidizing air travel. Nor should air travel be subsidizing taxpayers: At the moment, the security tax on air travellers appears to be taking in more money than Ottawa is giving to CATSA and airport security. User-pay makes sense; user-pay-plus-a-little-extra-for-Ottawa does not. Globe and Mail

CYBER SECURITY / CYBERSÉCURITÉ

* **Mafiaboy finds new mission in life**

Mafiaboy is now a man and he's on a mission. As a 15-year-old hacker in 2000, Mafiaboy (real name: Michael Calce) paralyzed the websites of the biggest names in media and e-commerce, including CNN, Amazon and eBay. The RCMP and FBI tracked him down in Île-Bizard. He pleaded guilty to 58 charges and spent eight months in a youth detention centre. Now 31, Calce recently started a cyber-security company - Optimal Secure - focusing on the financial sector in Montreal, Toronto and Vancouver. His specialty: "penetration testing." Companies hire him to try to penetrate their computer defences so they can secure systems before hackers strike. Computer hacking is a constant threat. In recent weeks alone, hackers have broken into some of Facebook's Mark Zuckerberg's accounts; forced the University of Calgary to pay a $20,000 ransom after crippling its computer systems; and stolen $81 million U.S. from the Federal Reserve Bank of New York. The Montreal Gazette sat down with Calce and learned that "spear-phishing email attacks" are among the scary things to fear online today. (This interview has been edited and condensed.) Gazette, A3

* **Massive North Korea cyber attack thwarted after hacking South Korea: report**

North Korea has hacked into more than 140,000 computers at large South Korean conglomerates and government agencies and planted malicious codes that may have been intended for a massive cyber attack that has been thwarted, a news report said on Monday. The hacking originated from an internet address traced to the North Korean capital and targeted a software used by about 160 companies and government agencies to manage their computer networks, Yonhap news agency reported, citing the police. The internet address was identical to the one used in a 2013 cyber attack against South Korean banks and broadcasters that froze their computer systems for more than a week. Reuters (Yahoo! News)

* **After Bangladesh: How a massive hack shook the banking world**
It was the start of a weekend in Bangladesh when an official at the country's central bank checked a printer in a server room. The tray was empty, which was strange. There should have been a sheaf of reports confirming payment instructions sent through the Swift system, the network that connects 11,000 banks around the world. The printer glitch was no accident, but a deliberate strategy by criminals to hide their tracks. A day earlier, cyberthieves had issued instructions to transfer $951-million (U.S.) out of Bangladesh Bank's account at the New York Federal Reserve. Most were declined, but $81-million was transferred to a bank in the Philippines, never to be seen again. The theft in early February sent shock waves through the global banking community. It was not simply enormous in size, but ambitious in its selection of target: the Swift system, the backbone of international finance. The methods deployed were highly sophisticated, involving a combination of technical prowess and intimate knowledge of how Bangladesh Bank interfaced with Swift. Gottfried Leibbrandt, chief executive of Belgium-based Swift, called the Bangladesh cyberattack "a watershed" for the banking industry. "There will be a before and an after Bangladesh," he said last month. What's more, it wasn't an isolated incident: Swift was aware of at least two other cases where cyberthieves used the same modus operandi, albeit with far less success. Four months after the theft, much remains unknown about the perpetrators and their methods. It's not clear, for instance, how the malicious code was implanted into the systems at Bangladesh Bank. And both private firms and law-enforcement authorities are conducting investigations to uncover the culprits. Some signs point to a gang of expert cybercriminals; others point to the possible involvement of a state actor. The theft shows that cybercriminals are growing increasingly audacious. Globe and Mail, B1

* **The G7 and cyberspace: 'give peace a chance'**
An opinion piece states “The G7 summit meeting hosted by Japan May 26-27 issued a document entitled 'G7 Principles and Actions on Cyber.' This cyber policy statement was the most elaborate one issued by the G7 since 2011. The intervening years have revealed continuity on some prominent themes, such as support for the free flow of information and respect for human rights online. However, the increasing use of cyber operations by authoritarian regimes in suppressing dissent and the infringement of privacy rights via mass state-conducted cyber surveillance, has revealed the stress such rights are under. The removal of Russia from the G8 context may have allowed for stronger commitments in the field of human rights, but it also highlights the challenge of achieving international cooperation on cyber security against a backdrop of deteriorating geopolitical relations between leading cyber powers. In this crucial realm of international cyber security, the pronouncements from the G7 summit are not all that reassuring. The goal of a peaceful cyberspace is conspicuous by its absence from the statement. The G7 will promote security and stability in cyberspace, but there is no apparent aspiration to keep cyberspace a realm of peace rather than war. The statement speaks of taking ‘decisive and robust measures in close cooperation against malicious use of cyberspace both by states and non-state actors,’ but these measures are not specified and the tone here suggests they will not be of a diplomatic nature. The G7 appear to be laying the ground for undertaking military responses to cyber operations they deem hostile by affirming that ‘cyber activities could amount to the use of force or an armed attack within the meaning of the UN Charter.’ Suffering ‘an armed attack’ entitles a state under the UN Charter to exercise the right of self-defence, thus this framing of such an eventuality is fraught with serious politico-military consequences. How and by whom such a determination of a cyber attack is made is left unaddressed in the G7 statement and there is clearly wide scope for unilateral (and potentially dangerous) interpretation and action in this regard.” Hill Times

LAW ENFORCEMENT / APPLICATION DE LA LOI

Seeking clues in cold case: Ground search relates to 1982 disappearance of Henrietta Millek
Search crews looked for evidence near Makinsons this weekend after receiving a tip on a decades-old missing-person case. Henrietta Millek, originally from Nain, was living in St. John's at the time of her disappearance in December 1982. She was 25 at the time. Originally, it was believed Millek's last known location was at a club in downtown St. John's. It was reported she may have left the bar against her will. Her belongings, including her purse, were left there, and she never returned for them. RNC Const. Geoff Higdon told reporters Saturday new information led to a ground search in the area of Roaches Line almost 34 years after she disappeared. "Recently we received information that the last known location may have been in the area of the Trans-Canada Highway, and I guess what at that time would have been Roaches Line, as Veterans Memorial (Highway) wasn't here," said Higdon. "We believe she may have been headed towards Makinsons, and we do know that she never made it to her destination, unfortunately, and the information was that her last known location was here on the Trans-Canada Highway, so we're searching the area between those two points." Almost 100 searchers scoured the area in the morning, and they were expected to continue all day. Crews from the RNC, the RCMP, the Rovers - Central Avalon Search and Rescue and the Avalon North Wolverines were involved. Telegram, A1

Police investigate chapter in New Glasgow Gate Keepers gang
Police executed a search warrant at the New Glasgow chapter of the Gate Keepers motorcycle group early Sunday. "Members of the Nova Scotia RCMP executed a search warrant on MacLean Street in New Glasgow in relation to an ongoing investigation," said Corp. Jadie Spence, a media relations officer for Nova Scotia RCMP. "It's a clubhouse for the Gate Keepers motorcycle gang," he said. Spence said there are currently seven chapters of the Gate Keepers in Nova Scotia, including one in Musquodoboit Harbour, where that chapter held a party over the weekend. "They're a support group of the Hell's Angels, who don't have a presence in Nova Scotia at present," Spence said. They were assisted by the New Glasgow Regional Police and Pictou County RCMP. The warrant was executed at about 6 a.m. The street was closed down. On Sunday at 6 p.m., police were still at the scene. There was no word about specifics of the investigation, Spence said. "There are no arrests and no charges at this point in time," Spence said. ChronicleHerald, A6; Cape Breton Post

Canadian officials offer condemnation and sympathy after Florida mass shooting
After a mass shooting on Sunday that killed at least 50 people and injured dozens more at a gay nightclub in Florida, many Canadians were reflecting on what the violence means for the LGBTQ community. Candlelight vigils to mourn the victims were planned in several Canadian cities Sunday night. Hundreds crowded for a candlelight vigil in Toronto in a predominantly gay neighbourhood. (…) The executive director of Pride Toronto, a not-for-profit with the goal of bringing together the city's LGBTQ community, said the massacre was a grim reminder of the setbacks his community faces. "It reminds us that hate and discrimination are still a big part of this society, and that because of this, some of our brothers and sisters this morning lost their lives," Mathieu Chantelois said on Sunday. The organization also runs Toronto's pride month, and Chantelois said Pride Toronto was already working with city police and the RCMP but would see if there were any additional security steps that could be taken. "The main objective of Pride is to create a safe space for our community to gather together and feel comfortable," he said. Spencer Chandra Herbert, a member of the British Columbia legislature, was in Quesnel, B.C., celebrating the small town's second annual pride celebration with his husband when he heard the news. His immediate reaction was disbelief. Canadian Press (Ottawa Sun, A4, Red Deer Advocate, Hamilton Spectator); Canadian Press (National Post); * CBC News

How the quest for cheap beer may change Canada
An opinion piece by former Ontario cabinet minister John Milloy states, “Canadians like to talk about trade. Remember the dust-up over the Trans-Pacific Partnership agreement in the last federal campaign, or earlier passionate debates over the Canada-U.S. Free Trade Agreement and its successor, the North American Free Trade Agreement? There is one exception. When it comes to free trade within Canada, no one ever seems to pay much attention. We better start. A recent New Brunswick court decision, likely to end up at the Supreme Court of Canada, has the potential to radically change our country and its economy. Although Canadians may maintain a fierce loyalty to their province or region, I also like to think we see our nation as a place where citizens are free to travel, live and enjoy life wherever they want. (…) Enter Gerard Comeau, a retired New Brunswick steelworker who went in search of cheap beer across the

border in Quebec. Such an appalling act of bad citizenship does not go unnoticed in Canada. The RCMP immediately stopped him upon his return and fined him for transporting more alcohol across the border than allowed under the modest limit set by the New Brunswick government." Hamilton Spectator

*** Protesters arrested at Muskrat Falls site**
Six people were arrested Sunday during a protest at the Muskrat Falls development site, the Happy Valley-Goose Bay RCMP stated in a news release. Demonstrators began their protest last Thursday at Nalcor's hydroelectric site at Muskrat Falls, blocking the entrance road into the project. On Friday the Supreme Court of Newfoundland issued a court order that directed the protesters to leave Nalcor's property. The RCMP continued to monitor the protest. On Sunday at 11:55 a.m., five protesters refused to comply with that court order and were arrested, the RCMP stated. A short time later, another group of protesters arrived and one protester was arrested for obstruction, police said. All six protesters were to be held overnight in custody and will appear in provincial court at Happy Valley-Goose Bay Monday. Five protesters are charged with breaching a court order and all six are charged with obstruction. The RCMP continues to monitor the situation at the Muskrat Falls site, but no additional incidents have been reported and the on-going protest remains peaceful, police said. Telegram, A5; CBC News

*** HALIFAX: RCMP escort Canada's 911 Ride**
The RCMP escorted Canada's 911 Ride in both the Halifax area and Annapolis Valley over the weekend. The annual police-escorted 911 Ride raises funds for families of fallen emergency service personnel, helps children who are victims of violent crimes, and provides public access to defibrillators in local communities. This year's Atlantic Ride took 70 participants through the South Shore and Peggys Cove areas on Saturday. Riders departed Halifax at 8:30 a.m., headed to Peggys Cove, then on to Lunenburg and Bridgewater. The riders returned to Halifax Saturday afternoon. Chronicle Herald, A5

*** RCMP seize guns in Delburne**
Police seized a number of stolen firearms and took a man and woman into custody at a campground in Delburne on Friday. Three Hills RCMP and the Priority Crimes Task Force launched an investigation in early May after RCMP received intelligence about stolen firearms. The search warrants were executed at two trailers in Barking Fox Campground with the assistance of Police Dog Services and K Division's Emergency Response Team. A man and a woman were taken into custody. RCMP continue to investigate. No other information was released. Red Deer Advocate, A3

*** Larry Tremblay est le nouveau patron de la GRC au N.-B.**
Le commissaire adjoint Larry Tremblay devient le 30e commandant de la Division du N.-B. de la GRC. Il remplace le commissaire adjoint Roger Brown qui prend sa retraite après plus de 35 années au service de la GRC, dont les trois dernières à titre de commandant au N.-B.. Avant de se joindre à la Gendarmerie, Larry Tremblay a fait partie de la Marine royale canadienne pendant près de quatre ans. Il possède une expérience de plus de 30 ans au sein de la GRC à différents postes. Il a débuté sa carrière au N.-B. où il a passé 11 ans. Il a ensuite travaillé à l'Unité mixte d'enquête sur le crime organisé et à la Section antidrogue de la région d'Ottawa et a oeuvré au sein de services spécialisés à Regina et à Milton en Ontario. De 2004 à 2008, il a travaillé au Service canadien du renseignement de sécurité (SCRS) avant de devenir directeur général des Opérations criminelles de la GRC. L' Acadie Nouvelle, 10

*** Woman in witness protection program sues RCMP for negligence**
Woman who helped on drug case says RCMP compromised her identity, which forced her into witness protection A woman in the federal witness protection program is suing the RCMP for negligence and for undermining her trusted relationship with Canada's national police force.The details of her case are contained in a judgment by Ontario Superior Court Justice Patrick Smith, who granted an injunction forcing the RCMP to continue financially supporting the woman, known as Jane Doe, as well as allowing her to expand the scope of her lawsuit against the Mounties. The document tells the story of a woman who did the right thing, only to lose it all — family, friends, a good job and her mental health. The heavily redacted court ruling summarizes the woman's claims, which included that after tipping off police about a drug crime, the RCMP compromised her identity and refused to own up to it. The court ruling states that after happening upon intelligence related to a crime syndicate, she shared what she knew with her

municipal police force. The RCMP then used that information to investigate and prosecute several members of a criminal syndicate on drug-related charges. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Prisons paying more for native spiritual services
Federal prisons are paying significantly more each year for indigenous spiritual services than for all other religions combined. Indigenous people make up about 25 per cent of the 14,865 people who are currently incarcerated in federal prison. The Correctional Service of Canada (CSC) is spending $8 million annually on sustaining spiritual services for indigenous offenders - versus $6.75 million for other religions. Spokesperson Avely Serin said "Elder services" help offenders follow a "traditional healing path" and provide advice to the heads of institutions about "access to ceremonial objects and traditional medicines within the institution." As of last October, 85 per cent of indigenous offenders in custody, or 3,156, had undergone an "elder review," Serin said. The cost was about $2,500 per person. (...) The correctional service takes "a lot of criticism for the overrepresentation of First Nations people in the prison system," said Catherine Latimer, executive director at the John Howard Society. She suggested that could be one reason for the extra funding. Indigenous people make up a quarter of the prison population versus 4.3 per cent of the general population, according to Canada's Correctional Investigator. Indigenous offenders do have better outcomes when "reconnected with their spiritual and cultural traditions," said the Correctional Investigator of Canada's annual report for 2014-15. But spiritual services help offenders of other religions, too, said Kate Johnson, a former chaplain at Joyceville Institution in Kingston, Ont. Almost half of offenders are Christian, a majority of those Catholic, and just over five per cent are Muslim. Postmedia Network (London Free Press, NP5, National Post, Leader-Post, Edmonton Journal, Vancouver Sun, Windsor Star, Montreal Gazette, Calgary Herald, StarPhoenix, Province, Ottawa Citizen)

Kingston Penitentiary tours send wrong message
An opinion pieces states, “Three years ago, Kingston Penitentiary was decommissioned and briefly opened its doors to tourists to raise funds for the local United Way. Hugely popular, tickets for the October 2013 "KP" tours quickly sold out, generating more than $180,000 in 15 days. Wanting in on the action, the Correctional Service of Canada (CSC) partnered with Habitat for Humanity to offer another block of tours in November 2013, with proceeds to go toward expanding the construction of affordable housing by federal prisoners in the name of "rehabilitation and reintegration." These tours also sold out fast, fostering further debate in the Kingston, Ont. area about the potential for KP to become a major tourist attraction. This week, tickets went on sale for a new series of guided tours at KP led by students and supported by retired correction service employees. The tours are being sold by project partners - the City of Kingston, CSC and the St. Lawrence Parks Commission - as "a rare and unique opportunity to go behind the walls of Canada's oldest and most notorious maximum security prison." Many from the Kingston area and elsewhere are hoping to enter the facility, which opened in 1835. From late June until the end of October, it is estimated that KP visitors will "pump more than $6 million into the local economy."” Toronto Star, A15

Egale calls for Trudeau apology
The assault on a gay night club in Orlando has cast a shadow over two reports that call for an apology from Justin Trudeau's government and restitution for homosexuals who were prosecuted and persecuted under Canadian policies in the past, and who still suffer discrimination today. One report, prepared by Egale, a national organization that advocates for lesbian, gay, bisexual and transgender Canadians, asks the Prime Minister to acknowledge in principle the need for an apology and redress for homosexuals who were criminally targeted because of their sexuality. Germany and Australia (through its state governments), are already at work on some combination of pardons, apology and redress. Egale said on Sunday that it remains committed to releasing the report after the weekend's tragedy. It will be delivered to Justice Minister Jody Wilson-Raybould on Monday and through her to the Prime Minister's Office. An advance copy was provided to The Globe and Mail. The report proposes that retired Supreme Court Justice Frank Lacobucci be asked to lead a one year study on what shape an apology, restitution and action to prevent future discrimination against sexual minorities should take. The report advocates "a process of 'truth and rehabilitation,' whereby the federal government will acknowledge the wrongs done to

our community and commit to a process to make it right." (…) Gay rights activists hope he will announce that he embraces the recommendations of both reports in principle beforehand. But moving from a pardon to an apology with promise of redress may be more than this government is prepared to embrace, however other countries proceed. Globe and Mail, A17

*** Fraudster released on early parole after seven months in jail**

Unrepentant and still contesting his conviction, former Regina businessman-fraudster Steven Vincent Weeres is now a parolee, mere months into a lengthy prison sentence. As a non-violent offender serving his first federal term behind bars, Weeres, 57, qualified for Accelerated Parole Review and is now out after seven months. "The basic difference is that they're eligible for parole at onesixth of their sentence, rather than one-third," Parole Board of Canada spokesman Patrick Storey explained. (The federal government ended the program in 2011, but courts have since ruled the change doesn't apply retroactively to those, like Weeres, whose crimes predate the revamped law.) "You preyed on unsuspecting individuals and bilked them of thousands of dollars. You impacted your victims' financial well-being, emotional well-being and their credit ratings," states his recent parole decision. "However, the board finds that you do not have a significant history of violence, nor have you been involved in the use of weapons. There is no indication that you have exhibited a pattern of violent behaviour, or that you have risk factors that would likely lead you to commit an offence involving violence," it continues. The board granted Weeres day and full parole on May 6. The Leader-Post has learned he's residing in a B.C. halfway house. Contacted by phone Saturday, Weeres said his appeal of conviction for fraud and money laundering "is still moving forward." He never appealed his sentence. No date for the appeal has been set. StarPhoenix, A7 (Leader-Post)

*** Most Wanted**

A man convicted of killing a fellow inmate at Bowden Institution is one of two most wanted this week. Keith Clinton Sandmaier - born Sept. 9, 1977 - is wanted on a Canada-wide warrant. A February fatality inquiry heard his criminal history includes stabbing to death Tung David Louie with a steak knife over a $30 debt when the pair were inmates at the minimum-security southern Alberta federal prison. Louie, who was serving a 12-year sentence for weapons, drugs and robbery offences, was unarmed when he got into a June 2011 fight with Sandmaier in a common area of Bowden Institution. Sandmaier was armed with a knife, though authorities were unable to confirm where he got it, and he stabbed Louie five times, according to an inquiry report into the homicide. At the time of the killing, Sandmaier had been awaiting a hearing because guards had found a sharp wooden weapon in the cell he shared with another inmate. Prison officials had deemed both inmates suitable to remain in the prison's general population. Parole records previously revealed that Sandmaier was motivated by a $30 debt when he stabbed Louie to death in an outdoor common area in the medium-security prison south of Red Deer. Sandmaier later pleaded guilty to manslaughter and was sentenced to five years. Edmonton Sun, A53

Distillery district for KP, harbour refloated

As the city sets its sights forward - on the future of its waterfront - Robert Kiley looks back. For the Ontario Green party candidate, the project is a chance to make good on last year's promise. During the federal election last November, Kiley was the campaign manager for MP candidate Nathan Townend. Amid federal campaign promises, one of the points in Townend's campaign was focused locally: on Portsmouth Olympic Harbour and Kingston Penitentiary. "Nathan and I put our heads together and said: 'What would be a local, sustainable and livable solution to revitalizing both [sites]?'" Kiley said. When the pair noticed a "budding brewery culture" in Kingston, they concocted a plan. A local distillery district could be built, alongside the often-discussed idea of an international sailing hub. In addition to local beer, the district would be a collective of Kingston artisans, food services and accommodations. "Green values are resiliency in the local economy, resiliency in local food systems, and resiliency in community engagement," Kiley explained. With this idea, all three values came together. When Townend was unsuccessful in his MP race, with 4.46 per cent of the vote in Kingston, the idea was put aside temporarily. Now, Kiley is taking the city's call for ideas as a chance to fulfil their promise anyway. "Currently, the city is hosting one-on-one interviews about the Kingston Pen site, and [this week] they'll be having an information session," Kiley explained. In preparation, he put together an online petition last Tuesday, to measure support and "add a bit of weight" to the idea. As of 6 p.m. Friday, the petition of www.change.org had garnered 121 signatures. Kingston Whig-Standard, A2

*** Un baromètre**
Arrêté, jugé sommairement puis gracié de façon théâtrale au moment où il allait être exécuté, Dostoïevski croupit quelques années au bagne, en Sibérie. Il en rapporte notamment la matière de ses Carnets de la maison morte, vaste récit de ses observations en prison. (…) Depuis que je m'intéresse davantage au sort fait aux prisonniers à l'heure de l'austérité, j'ai croisé sur les chemins de la prison quelques-uns de ces êtres de bonté. (…) Dans les prisons québécoises, un problème de surpopulation et de manque de services de base se pose plus que jamais. Depuis quelques mois, ce problème est illustré de façon éclatante à la suite de la fermeture de la maison Tanguay, une prison pour femmes. Bien qu'elles ne purgent que de brèves peines pour des délits mineurs, ces détenues ont été transférées à l'Établissement Leclerc, un ancien pénitencier fédéral de longue durée pour hommes. Certains, rappelait Dostoïevski, pensent " qu'il suffit que les détenus soient bien nourris, bien entretenus, qu'on suive toutes les prescriptions de la loi pour que les choses aillent bien ". Mais le traitement humain ne tient pas qu'à l'administration du règlement, rappelait-il aussi. La prison est une bête énorme qui écrase physiquement et moralement. On ne réhabilite pas une vie brisée en l'écrasant davantage. La semaine dernière, au moment de répondre à des questions au sujet des traitements douteux subis par les femmes de la prison Leclerc, le ministre Martin Coiteux a eu à peine le temps de dire quelques mots avant que, du milieu de la meute médiatique, on ne s'empresse de lui demander pourquoi certains prisonniers avaient droit à des cours de yoga, de zumba ou à de la zoothérapie. Le Devoir, A2

*** Ministers can't avoid tough issues**
An editorial states, "How long does it take a politician to make the transition from opposition to government? There's no hard and fast rule. Some MLAs who've spent a long time on opposition benches make a seamless transition into government, occupying cabinet portfolios with such ease and comfort it looks as though they have done it before. (…) Last week, a national news report revealed Manitoba's provincial jail system relies more on solitary confinement than any other province. The overuse of solitary is top of mind following the death of Richard Wolfe, a Saskatchewan prisoner who spent 640 consecutive days in a cell, alone, for 23 of 24 hours each day. Wolfe died from a heart attack after being transferred to a federal jail. Solitary confinement has always been prickly for politicians. On the one hand, human rights adocates and prison-welfare experts almost universally decry it. The United Nations has declared it a form of torture. Several provinces are reviewing their policies to ensure no inmate spends inordinate amounts of time segregated from other prisoners. On the other hand, the welfare of convicted criminals has never been a compelling issue for the majority of voters. Some of our least compassionate citizens celebrate the inherent cruelty of solitary. So, perhaps it made sense that, when asked by the *Globe and Mail* whether she was concerned that Manitoba was leading all provinces in the use of solitary, Stefanson said via a spokeswoman the province had "no plans to review segregation policies at this time." That response is simply unacceptable. Stefanson, a long-suffering opposition MLA, is getting a well-deserved first taste of governing. And the reality of government is that you must be ready and willing to respond when an issue such as this arises. Even those not on your personal top-10 list of pressing policy issues. The story required a response of some sort." Winnipeg Free Press, 8

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Gay communities react to targeted hatred**
Eric Pineault says his heart sank Sunday morning when he went on Facebook and learned of a gunman's deadly assault on an Orlando, Fla., gay nightclub. Pineault, the president of Montreal Pride, had visited the Pulse a couple years ago while on vacation. It was a smallish club with the usual Top-40 tunes and thrumming house music. But like all other gay nightclubs, it was a place of comfort - where you could let your guard down. "People can hang out and be themselves. It is not always possible to hold your lover's hand on the street. There, you can kiss and be yourself," he said. "No boundaries." (…) Violence against the LGBT community around the world remains a "grave concern," said a blog post on the Amnesty International website last month. (…) Data from Statistics Canada show that, in 2013, most police-reported hate crimes were non-violent, typically involving mischief, such as graffiti. However, two-thirds of cases motivated by hatred for someone's sexual orientation involved violence. A 2015 Justice Canada

report found that police data were likely to "seriously underestimate" the extent of hate crimes targeting the LGBT community because they were less likely than other victim groups to report incidents to police. "Analysis of calls to a hotline in Toronto run by the 519 Church Street Community Centre shows that a high incidence of hate-motivated incidents directed at gays and lesbians involve physical assault," the report said. "Only a minority of incidents reported to the hotline had been reported to the police." As Pride organizers from Vancouver to Montreal scrambled Sunday to organize vigils to mourn those killed in Orlando, they also said they planned to step up their vigilance and reach out to police to see if any security enhancements were needed at their events. London Free Press, NP4 (National Post, Calgary Herald, Ottawa Citizen, Windsor Star, StarPhoenix, Leader-Post); La Tribune (La Presse)

*** How Tory changed tough approach to keeping city safe**

In June 2003, Toronto mayoral candidate John Tory ran a tough-on-crime campaign that promised to add 400 police officers to the force's roster - even if it meant raising property taxes. The fact was the crime rate had been falling for decades. But just days before Tory released his crime platform, a man was charged with raping and murdering 10-year-old Holly Jones in her west end neighbourhood. "John Tory, 2003 edition, would not have been unlike many, many candidates who try to get elected by seizing the anti-crime agenda," says city hall veteran Councillor Joe Mihevc. That fall, Tory won the controversial backing of the Toronto police union, but lost the election to David Miller. Thirteen years later, Tory is mayor and gun violence has spiked. Twenty-one of the city's 33 homicide victims were killed by a firearm. (Receiving much less attention are the 17 pedestrian deaths on Toronto streets this year.) There is no evidence of an upward trend in the overall crime rate. But the default reaction of the police union and some right-wing commentators is that more cops should be hired. Whether doing that would make a difference is a hotly debated subject. Tory is not among those calling for more police. Instead, when Tory talks about keeping Toronto safe, he refers to better deployment and outsourcing certain policing tasks to ensure more officers focus on gritty crime-fighting, not "monitoring left turns." "A lot of other things have changed, too. I think we've all resolved to make sure that we find different ways to do policing in the city of Toronto," Tory told a recent news conference on gun violence. The mayor is recognizing that "the real task of keeping cities safe ... is complicated," says Mihevc. "There's crime prevention, lighting, making sure young boys are kept busy ... that of course is not a very sexy campaign slogan." This week could be a watershed moment for policing in Toronto - and Tory. On Thursday, his "transformational task force" on policing will unveil an interim report recommending ways to reorganize and modernize the force, while cutting costs. Earlier this year, after Mihevc and other councillors tried to flatline the police budget, which pushed past $1 billion, council voted 41-1 on a motion saying there is an "urgent and abiding" need to restrain policing costs. Tory, who sits on the police board, urged councillors to let the task force do its work. Toronto Star, GT1

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

*** Missing: Annie Yassie was 13 when she disappeared over 40 years ago**

Eva Yassie's dream about her missing baby sister is almost always the same. Annie Yassie is still 13, she is standing in the distance and she is smiling. But when Eva asks her questions, Annie doesn't answer. When Eva tries to touch her, Annie can't be reached. "It really disturbs me, these dreams," Eva Yassie says, taking a long drag on a hand-rolled cigarette. "I call her name and see if she can.... She just looks at me and smiles, and fades away. I can't get no answers." Questions have haunted Eva Yassie for 42 years, since June 22, 1974, when Annie disappeared into the night a few kilometres outside Churchill, Man. She was just a kid, 13, just back to Dene Village from residential school. CBC News (2016-06-12)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Decriminalize marijuana, NDP urges Liberals**

The New Democrats are urging the Liberal government to decriminalize pot before they legalize it. Prime Minister Justin Trudeau campaigned on a promise to legalize, regulate and restrict access to marijuana, and his government plans to get started next spring. Meanwhile, the existing criminal law remains on the books and police are expected to enforce it. The NDP is introducing an opposition day motion on Monday calling on the House of Commons to recognize there is a contradiction in giving people criminal records for something the government has said should not be a crime. The motion also calls on the government to decriminalize simple possession of marijuana for personal use immediately. "Arresting people and giving them criminal records for possession of small quantities just doesn't seem fair, in light of their commitment, apparently, to legalize marijuana," New Democrat MP Murray Rankin said Sunday. Rankin also said the law is being applied inconsistently across the country, which adds to the unfairness. Rankin said one way to decriminalize it without having to wait for legislation to make its way through Parliament would be to have Attorney General Jody Wilson-Raybould issue a directive under the Public Prosecutions Act ordering Crown counsel to avoid proceeding with prosecution for simple possession offences. "I just think the sensible thing to do would be to no longer charge people until we can get the reformed regime in place," said Rankin. Health Minister Jane Philpott formally announced in April the federal government's plan to legalize and regulate marijuana when she spoke to the United Nations General Assembly in New York. Canadian Press (Telegram, A10, Red Deer Advocate, Calgary Sun, Winnipeg Sun, Toronto Sun, Edmonton Sun, Waterloo Region Record, Hamilton Spectator, Toronto Star, Chronicle Herald)

* **'Craft cannabis' growers fight for legal role**

Travis Lane has been growing marijuana since high school, when his first pot plant swiftly withered and died in his bedroom closet. By the time he was 20, he had cultivated a small basement grow-operation. Now in his mid-thirties, Lane owns an online dispensary and runs two 390-plant operations on Vancouver Island. He employs two growers and raises his plants without pesticides or liquid fertilizer. "I don't want to hide what I do. I'm good at what I do. I'm proud of being good at what I do," he said. "I've been proactive my whole life in trying to move towards a time where I can openly be a cannabis professional." Lane holds two Health Canada licences for the grow sites, making his pot production legal for medical purposes. But with the federal Liberals committed to legalizing cannabis for recreational use, Lane is among the smaller-scale growers fighting for a seat at the table. The government is still in the early stages of developing the legislation it plans to introduce next spring. Those behind a budding "craft cannabis" movement warn, however, that if the law favours large-scale commercial producers, then jobs and potential tourism revenues will be lost and the black market will continue to thrive. Canadian Press (Red Deer Advocate, A10, Telegram, National Post)

* **MADD Canada calls for roadside drug-testing equipment for police**

Mothers Against Drunk Driving wants police forces across Canada to be enforcement-ready for people driving while under the influence of legal marijuana. Danielle Cole, president of MADD greater Fredericton chapter, said she met with MPs in Ottawa to start getting prepared for the legalization of marijuana - the drug most likely to be the cause of impairment behind the wheel. MADD Canada is calling for an amendment to the Criminal Code about driving while under the influence of drugs. Cole said there is a strong misconception among young people about the use of marijuana and driving. "If you ask a teenager about this, they'll tell you they drive better [high]," she said. In 2014, MADD reported 2.6 per cent of all impaired driving charges were drug-related. In 2012, New Brunswick had 83 deaths related to traffic accidents of which there were 17 drug-related driving impairments accidents causing death, which is lower than the 22 alcohol-related driving deaths. Five deaths involved both drugs and alcohol. That is more than Prince Edward Island, but less than Nova Scotia and Newfoundland. Daily Gleaner, A2

* **Details on marijuana task force coming, to deal with supply, jurisdiction, retail, taxes**

A marijuana industry official says existing licensed producers could supply just 10 to 15 per cent of what demand will be once recreational use of marijuana is legalized. Insiders say the questions a government task force on marijuana legalization must deal with include how and where consumers will purchase it, how much involvement the provinces will have in its regulation, how adequate supply will be created, and what level of taxes should be applied. Multiple sources have confirmed a report that former Liberal cabinet minister Anne McLellan has been appointed to lead the task force, though this has not been publicly announced yet, and that the whole task force and its mandate will be revealed before MPs break for the summer on June 23. Don Gracey, a partner with the CG Group, which is lobbying the federal

government on behalf of a prospective producer of marijuana, was among the people who said this is true, as did another person who has been in discussions with the government on this matter but asked not to be identified."Anne McLellan has been appointed the chair of this task force," said Mr. Gracey, whose client Georgian Bay Biomed is in the process of building a production facility in Collingwood, Ont., initially planned for medicinal marijuana but which will now also be used for recreational pot. "We understand that the provinces have been asked for and have submitted, I guess what could be categorized as, nominees for provincial representation on the task force." Hill Times

* **Colorado pot retailer advises province on weed**
One of Colorado's largest marijuana retailers says that provinces legalizing pot must educate the public on potency and put in place rules on packaging from the outset. It was a message that liquor board heads and government officials from across the country heard at a private gathering in Saint Andrews last week. The chief information and security officer of Denver's The Green Solution, Nick Speidell, spoke at the conference quietly hosted by New Brunswick's Department of Public Safety in preparation for the sale, distribution and regulation of pot - now that Ottawa is moving toward legalization. Speidell told the Telegraph-Journal in an interview that he spoke on "the good and the bad" of the development of recreational marijuana in Colorado. The state is one of a few U.S. jurisdictions that have already legalized the sale and recreational use of cannabis products. "Colorado was the beta," said Speidell, whose family owned and operated recreational and medical dispensary, boasts the largest selection of marijuana and marijuana-infused products with 11 locations in and around Denver. "We had to learn some lessons, but if you follow some of the best practices and the case studies out here you won't have to make those same mistakes." Speidell's words were directed primarily at edibles - marijuana baked into brownies, cakes, chocolate bars and candy, among other forms - that are becoming a popular alternative to smoking cannabis. Times & Transcript, A10 (New Brunswick Telegraph-Journal)

PUBLIC SERVICE / FONCTION PUBLIQUE

PM to meet young public servants
Prime Minister Justin Trudeau will meet Monday with about 100 public servants, all under age 35, to discuss how their generation will influence policy and change the way the bureaucracy works. Trudeau, also the minister of youth, will be joined by his top bureaucrat, Privy Council Clerk Michael Wernick and Treasury Board president Scott Brison - both of whom have indicated the public service needs a rapid infusion of young blood and new leadership to take over from baby boomers and deliver on the Liberals' agenda. That discussion will be an interactive town hall, which every public servant across the country can watch online, to kick offthis year's National Public Service Week and address the widening generational gulf the Liberals are trying to manage. The annual pat-on-the-back for Canada's 250,000 public servants lost its lustre under the Conservative government. It was during public service week when former Treasury Board president Tony Clement put public servants on notice that he was targeting their sick leave and all but accused them of being malingerers. The lunches and awards to celebrate the work of public servants continued, but the unions boycotted. Last year, the week turned political when the large unions launched pre-election campaigns to get rid of the Conservatives and restore public services. That's all changed with the Liberals. Scientists are unmuzzled, public servants are going to conferences, and diplomats can talk again. The long-form census is back, ministers say they want policy advice and Brison is repealing legislation to restore the old rules for collective bargaining. Not all unions are boycotting this year, but the giant Public Service Alliance of Canada is because of the slow pace of negotiations and the Liberals' failure to "respect public servants." Ottawa Citizen, A5

* **Time to empower next generation of public servants, says Canada's top bureaucrat**
As the annual Public Service Week gets underway today, Canada's top bureaucrat says there's a clear focus this year on empowering the next generation inside the federal bureaucracy. In fact, the Clerk of the Privy Council, Michael Wernick, will lead a virtual town hall Monday morning aimed specifically at young bureaucrats. "I'm pushing for a theme of engaging with our younger cohorts, because this issue of generational renewal is important to me." said Wernick, who himself was headhunted into the federal government 35 years ago this month. Over those decades, Wernick said he has witnessed the many ebbs and flows of the federal government's relationship with its workers. There have "already [been]

changes in tone, for sure" under Prime Minister Justin Trudeau, said Wernick, the man who gave him his current job.(...) Ray Paquette, who works at Public Services and Procurement Canada and is on the negotiating team for the Professional Institute of the Public Service (PIPSC), said the Liberals have made some changes - but not nearly enough. "We have a big problem. The science community is still being muzzled, not being able to openly discuss projects that they're on, [and that] would benefit the people of Canada," he said. "The federal government is still holding them back from being able to do their job properly." (...)Debi Daviau, the president of PIPSC, said at a rally in Ottawa on Friday there's a simple solution to helping the government deliver, and it includes building the right environment. "There was a very difficult and toxic environment created over the past nine years. And from my perspective, something needs to come from the top if they're going to have the capacity to deliver the commitments of this government," said Daviau. CBC News

OTHER / AUTRE

*** Robert Hall, Canadian hostage, executed by Philippine militants Abu Sayyef**
A Canadian man being held hostage by a militant group in the Philippines has been killed. The extremist group Abu Sayyef had warned it would kill Robert Hall today if a multi-million dollar ransom wasn't paid. Sources close to the situation in Jolo, the island where the al-Qaeda-linked group is based, and within Philippine security, confirmed Hall's death early Monday to CBC News. Hall, who was from Calgary, had been held since Sept. 21, 2015 - one of four hostages that included former mining executive and fellow Canadian John Ridsdel, who was killed by the group in late April. Ridsdel and Hall were abducted from a seaside resort along with a Filipino woman and a Norwegian man. An official announcement is expected shortly. The condition of the remaining hostages is not known. CBC News; Globe and Mail; Agence France-Presse (EuroNews)

'There's blood everywhere'
It had been an evening of drinking, dancing and drag shows. After hours of revelry, the party-goers crowding the gay nightclub known as the Pulse took their last sips before the place closed. That's when authorities say Omar Mateen emerged, carrying an AR-15 and spraying the helpless crowd with bullets. Witnesses said he fired relentlessly - 20 rounds, 40, then 50 and more. In such tight quarters, the bullets could hardly miss. He shot at police. He took hostages. When the gunfire finally stopped, 50 people were dead and dozens critically wounded in the deadliest mass shooting in modern U.S. history. Mateen, who authorities said had pledged allegiance to Islamic State in a 911 call shortly before the attack, died in a battle with SWAT team members. Authorities immediately began investigating whether the assault was an act of terrorism and probing the background of Mateen, a 29-year-old American citizen from Fort Pierce, Florida, who had worked as a security guard. At least 53 people were hospitalized, most in critical condition, officials said. A surgeon at Orlando Regional Medical Center said the death toll was likely to climb. "There's blood everywhere," Orlando Mayor Buddy Dyer said. The gunman's father recalled that his son recently got angry when he saw two men kissing in Miami and said that might be related to the assault. Mateen's ex-wife said his family was from Afghanistan but that her ex-husband was born in New York. His family later moved to Florida. A law enforcement official said the gunman made a 911 call from the club in which he professed allegiance to the leader of the Islamic State, Abu Bakr al-Baghdadi. (...) "I am deeply shocked and saddened to learn today so many people have been killed and injured following a mass shooting in Orlando, Florida. While authorities are still investigating and details continue to be confirmed, it is appalling that as many as 50 lives may have been lost to this domestic terror attack targeting the LGBTQ2 community." Prime Minister Justin Trudeau, in a statement. Associated Press (The Guardian, B10); Le Devoir; Canadian Press (Waterloo Region Record); Canadian Press (National Post); Toronto Star; La Presse (2016-06-12)

*** Calgarians show solidarity and vow to take on hate**
Calgarians gathered by the hundreds Sunday night in solidarity with the victims of the worst mass shooting in U.S. history. The attack, which targeted a crowded gay nightclub in Orlando, Fla. , early Sunday morning, left 50 dead and as many wounded. The Olympic Plaza vigil was more noise than silence. The crowd of about 500 people cheered to celebrate the LGBTQ community and made noise to make it known they needed to be strong in the face of hatred. (...) Alberta's premier said she was

repulsed and outraged by "the hatred that fuelled this crime," and she extended thoughts and prayers to the victims and their loved ones "who are suffering this moment." "And we resolve to make sense of these senseless events by re-committing ourselves to building communities where love and solidarity triumph over hatred and division," Notley said in a statement. Calgary Muslim groups condemned the "barbaric" attacks in Florida as they asked people of all faiths to "stand together" and "unite against terrorism and extremism." "Terrorists and extremists want to divide us but we refuse to be divided," Muslims Against Terrorism and the Islamic Supreme Council of Canada said in a release. "We demand that Daesh (ISIS) and its sympathizers should be brought to justice." Calgary Sun, A6

*** L'Iran condamne la décision d'un tribunal canadien**

L'Iran a condamné samedi la décision d'un tribunal canadien de saisir 13 millions de dollars d'actifs non-diplomatiques du gouvernement iranien au profit de familles de victimes d'attentats coordonnés par Téhéran et perpétrés par le Hamas et le Hezbollah, selon la justice canadienne. Le jugement, obtenu vendredi par l'AFP, exige que les familles d'Américains décédés dans huit attentats -- perpétrés entre 1983 et 2002 -- reçoivent les propriétés et les comptes bancaires détenus par le gouvernement iranien au Canada en guise de dédommagements. Le porte-parole du ministère iranien des Affaires étrangères, Hossein Jaber Ansari, a dénoncé cette décision, la jugeant " contraire aux engagements internationaux du gouvernement canadien ", selon l'agence officielle iranienne Irna. " Elle est également contraire aux affirmations du nouveau gouvernement canadien pour normaliser les relations entre les deux pays ", a ajouté M. Jaber Ansari. " Toute normalisation des relations diplomatiques entre les deux pays nécessite une révision des politiques extrémistes et erronées du gouvernement canadien. " Selon les médias canadiens, ces actifs appartenant au gouvernement iranien totaliseraient environ 13 millions de dollars canadiens. Cette poursuite a été déposée au Canada en vertu d'une nouvelle loi, adoptée en 2012, qui permet aux victimes et à leurs familles d'obtenir des dommages et intérêts saisis auprès d'États soutenant des actes considérés comme terroriste. L'Iran est ainsi considéré par le Canada. Agence France-Presse (Le Devoir, B2)

*** Canada needs to probe war crimes in Afghanistan**

An opinion piece states, "Justin Trudeau was only a backbench opposition MP during the Afghan detainee scandal, and spoke just once in Question Period about allegations of Canadian complicity in acts of torture. But what he said on Nov. 29, 2009, was insightful: "We need to get at the truth. The international reputation of Canada and our military is at stake." Trudeau was responding to a story broken by the Star in May 2007, which grew into a scandal that ultimately led to the prorogation of Parliament in December 2009. As one detainee told reporter Rosie DiManno, "They whipped me with rubber hoses. Another time, they used a chain to hang me from the ceiling, my head toward the floor." The same detainee said Canadian officials visited the prison operated by the Afghan National Directorate of Security (NDS), but were never allowed to speak with prisoners. As the late James Travers wrote, also in this newspaper, the story was part of a "long march into twilight" for Canada. The country that "gave the world Lester Pearson's peacekeeping and Brian Mulroney's stand against apartheid" now had to struggle "with Stephen Harper's apparent blindness to compelling evidence of Afghanistan prisoner abuse." (...)Three months later, the Afghanistan Independent Human Rights Commission estimated that "one in three prisoners handed over by Canadians are beaten or even tortured." In March 2007, the U.S. State Department reported that: "Complaints of serious human rights violations committed by representatives of national security institutions, including arbitrary arrest, unconfirmed reports of torture, and illegal detention were numerous."(...) Six years have passed since Justin Trudeau spoke from the backbenches about Afghan detainees. Now, as prime minister, he can put his insight into action. Nothing would do more to strengthen Canada's reputation as a progressive and principled country than investigating possible war crimes by our own soldiers and officials. Nothing would do more to help Canada win a UN Security Council seat. We need to get at the truth, and we need to do so now." Toronto Star, A15

INTERNATIONAL

*** Police had previously interviewed gunman**

The gunman suspected of killing 50 people at a gay Florida nightclub, Omar Mateen, a 29-year-old American, was a person of interest to authorities in 2013 and again in 2014. The FBI says agents twice investigated the man, but closed those cases after interviewing him. FBI agent Ronald Hopper said Sunday that Mateen had been interviewed in 2013 and 2014. Hopper said agents first investigated Mateen after he made inflammatory comments to co-workers alleging possible ties to terrorists. Mateen was interviewed twice and, when investigators were unable to verify the details of his comments, the FBI closed the probe. In 2014, the agency looked into potential ties connecting Mateen to Moner Mohammad Abusalha, the first American to carry out a suicide attack in Syria. Like Mateen, Abusalha lived in Fort Pierce, Florida. Hopper says agents determined that contact was minimal and did not constitute a substantive relationship or a threat at that time. The FBI says he referred to the Islamic State of Iraq and the Levant (ISIL) in a 911 call before the slayings. Mateen's ex-wife, who spoke to the Washington Post on the condition of anonymity, said his family was from Afghanistan but that her ex-husband was born in New York. His family later moved to Port St. Lucie, Fla., where he worked as a security guard. CBS News Justice and Homeland Security correspondent Jeff Pegues reported that an ISIL-related Twitter account has an alleged photograph of Mateen. Pegues also reported that Mateen pledged allegiance to the ISIL at some point. Postmedia Network (Windsor Star, NP3, StarPhoenix, Vancouver Sun, Ottawa Citizen, National Post, Leader-Post, Edmonton Journal, Montreal Gazette, London Free Press, Calgary Herald); The Province; Globe and Mail; Associated Press (Acadie Nouvelle); Toronto Star; La Presse (La Tribune); TVA Nouvelles

*** Daesh, style US**

Ce qui ajoute à l'horreur, c'est qu'on est déjà programmé. On s'attend au pire. On ne sait pas quand, ni où, on ne veut pas vraiment le savoir, mais on sait que ça arrivera. On entre déjà en mode statistique. On compare les chiffres des tués et des blessés. « Ça » quoi, au fait ? On n'avait pas encore identifié les corps qu'il fallait choisir son camp : une autre manifestation du terrorisme islamiste ou une autre tuerie de masse américaine ? C'est les deux, évidemment. La force du groupe État islamique est qu'il s'adapte aux terrains, dans sa guerre. Il peut former des combattants hyper-organisés ou inspirer des individus qui agissent seuls en son nom. Des commandos d'Européens venus dans ses camps qui retournent faire des assassinats coordonnés de type militaire, comme à Paris, à Tunis ou à Bruxelles. Ou un couple comme celui de San Bernardino, qui s'en va descendre 14 collègues dans un party de Noël en Californie, et qui le fait au nom du groupe État islamique. Ou un type (apparemment) seul comme hier. L'ex-femme d'Omar Mateen a dit au Washington Post qu'il était violent, pas vraiment religieux et surtout instable psychologiquement. C'est possible. Ça n'en fait pas moins un candidat excellent. Qu'il tue dans une attaque coordonnée avec un commando ou qu'il tue tout seul, ça change beaucoup de choses dans l'enquête. Ça ne change rien au résultat. Il n'en a pas moins tué 50 personnes au nom du même commanditaire. On n'en sait pas assez long sur l'état mental de Mateen. Mais quoi qu'il en soit, on ne peut pas mettre sur le compte des seuls troubles mentaux un massacre aussi ciblé. Un discours homophobe violent est bien incrusté dans certaines branches de l'islam. La Presse+, 6

*** Time running out to find EgyptAir black boxes**

Egyptian investigators say time is running out in the search for the black boxes from an EgyptAir plane that crashed into the Mediterranean last month, killing all 66 people on board. In a statement Sunday, they say that searches by ships in the area will intensify, given that only around five days remain before the batteries of the flight's data and cockpit voice recorders expire and they stop emitting signals. The boxes could reveal whether a mechanical fault, a hijacking or a bomb caused the disaster. Finding them without the signals is possible but more difficult. Since the plane disappeared from radar en route to Cairo from Paris, only small pieces of debris and human remains have been retrieved from the crash site. No group has claimed an attack. Daily Gleaner, B1

*** One of Lebanon's biggest banks targeted by blast**

A powerful bomb in Beirut destroyed several cars, severely damaged one of Lebanon's biggest banks and injured one person on Sunday. The state-run National News Agency said the bomb was placed under a car. Lebanese Interior Minister Nohad Machnouk, speaking to the private LBC station, confirmed the report but did not say whether anyone was deliberately targeted by the blast, which shook nearby buildings. Associated Press (Toronto Star, A12)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
June 13, 2016 / le 13 juin 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Saskatchewan reeling after Orlando shooting
Dan Shier, co-chair of Regina Pride, was celebrating Saskatchewan Pride Month in Saskatoon when he heard the news: Fifty people died and another 53 were injured after a shooting in a gay nightclub in Orlando, Fla. "Obviously, kind of shock and some remorse with the news, and some heavy hearts," Shier said. The Queen City is gearing up for its own pride celebrations, kicking off on June 18, 2016. And while the shooting will be on everyone's minds, the festivities will continue as planned. (…) **Ralph Goodale**, **Minister of Public Safety and Emergency Preparedness**, also spoke about the shooting. "***We have to make sure that we are doing everything we can do to make sure Canadians are safe,"*** **Goodale** said in a phone interview. ***"As Canadians in this month celebrate pride in many ways, it's extremely important now that those celebrations go forward, and go forward with a sense of determination and safety and security."*** CTV News (2016-06-12); 620 CKRM; * CBC News

*** Regina's LGBTQ community and religious group 'condemn' deadly shooting in Orlando**
Regina residents described their shock when they heard the news about the deadliest shooting in U-S history where 50 people were killed at a popular gay nightclub in Orlando. "I'm shaking, not sure if you

can tell, but I'm shaking because of all of it," Lisa Phillipson said. Phillipson is the contracts director with Queen City Pride. She said the shooting hate crime shows there's a need for more public education. "And the fact that this shows that reinforces the need that we need to have more activism and more parades and more marches," Phillipson said. **Public Safety Minister Ralph Goodale** said there's no immediate threat to Canada at this time. He noted that when tragedies like this occur, security detail does increase. ***"Everything is double checked and triple checked," Goodale*** said. ***"There is no immediate connection to Canada in any way."*** – **Goodale**. He also expressed his condolences to the family, calling the shooting a ridiculous and sad brutality. ***"Our thoughts and prayers go out to the victims and their families who are suffering through an absolutely unspeakable and entirely tragic loss,"*** he said. Global News (2016-06-12)

Le Canada condamne la tuerie survenue à Orlando
La classe politique canadienne a condamné le carnage survenu dans une discothèque d'Orlando, en Floride, qui a fait 50 victimes et des dizaines de blessés, dimanche. Le premier ministre Justin Trudeau a publié un communiqué dans lequel il s'est dit « profondément choqué et attristé d'apprendre la nouvelle au sujet de la fusillade à Orlando, en Floride, qui a fait tant de morts et de blessés ». Il a ajouté qu'il « est effroyable de penser qu'au moins 50 vies ont été perdues en raison de cet acte de terrorisme intérieur visant les membres de la communauté LGBTQ2 ». (…) Le **ministre de la Sécurité publique** du **Canada Ralph Goodale** a écrit sur Twitter qu'il était bouleversé par ce qui est considéré comme la pire tuerie par balle de l'histoire des États-Unis et que les Canadiens condamnaient une telle violence. Selon les policiers américains, l'attaque a eu lieu dans la nuit de samedi à dimanche, lorsqu'un tireur a ouvert le feu dans une boîte de nuit gaie. L'assaillant est mort plus tard sous les tirs des policiers. **M. Goodale** a ajouté que ses prières et ses pensées allaient vers les proches des victimes. ***Choqué à la fusillade meurtrière à Orlando. Les Cdns condamnent cette violence brutale. Pensées + prières avec victimes et proches.- Ralph Goodale (@RalphGoodale***) 12 juin 2016. Presse canadienne (Le Devoir, Express Drummondville); Journal de Montréal (2016-06-12)

Akwesasne Mohawks want Canadian government follow-through on independent oversight of border services agency
In light of its longstanding and difficult relations with the Canada Border Services Agency, the Mohawk Council of Akwesasne is supporting creation of an independent oversight mechanism for the operations of the border agency. The Canadian government recently signaled that it is looking for ways to improve transparency and increase public confidence in the CBSA, according to a press release from the MCA. Akwesasne community members routinely cross through the CBSA port in Cornwall, Ontario, sometimes several times a day, while traveling from one part of the community to another to travel to work, attend school, attend health related appointments, visit family, or otherwise meet social, cultural, economic, and recreation needs, the MCA said in a statement. (…) The Canadian **Minister of Public Safety and Emergency Preparedness Ralph Goodale** said the government is examining how to best provide the CBSA with appropriate review mechanisms, particularly after numerous civil rights groups have called for the creation of an independent watchdog to oversee the border agency. On May 26, MCA Grand Chief Abram Benedict wrote to **Minister Goodale** expressing the Mohawk Council's support for the establishment of an independent oversight mechanism for the CBSA. "While we appreciate the importance of ensuring that the border is secure for national security as well as for the safety of all citizens, we expect CBSA to treat people with respect in an open and transparent manner. Law enforcement officials should be held to the highest standard of review and scrutiny in their interaction with the public," the MCA statement said. North Country Now (2016-06-12)

"The Chinese Foreign Minister recently scolded a Canadian journalist for asking about China's human rights record in a press conference in Ottawa and while here demanded a meeting with the PM. Do you think the federal government responded appropriately?"
Mathieu R. St-Amand, Bloc-Québécois strategist: "The Chinese government's difficulty with the concept of a free press is nothing new. By expressing its dissatisfaction to the Chinese about an objectionable statement by one of that country's diplomats, the Trudeau government has done the bare minimum of what would be expected in such a situation. "However, if this government is serious about promoting freedom of the press, it should call an inquiry into the surveillance of two *La Presse* reporters by the RCMP. Beyond **Public Safety Minister Ralph Goodale's** rhetoric, the government should take this direct

attack on the freedom of the press seriously. A public inquiry would shed light on several unanswered questions about RCMP practices. By not calling an inquiry, the government is attempting to cover up one of the most serious attacks on freedom of the press in recent years. "Canada must defend freedom of the press at home in front of countries where this freedom is curtailed. However, the government needs to do more than simply lecture offenders; it must ensure that this freedom is unrestricted here. Justin needs to lead by example instead of talking down to people for once." Hill Times

Canada's surveillance crisis now hiding in plain site
An opinion piece by Michael Geist states, "Three years ago this month, Edward Snowden shocked the world with a series of disclosures that revealed a myriad of U.S. government-backed surveillance programs. (…) While these programs attracted attention for a day or two, it was the Conservatives' introduction of Bill C-51, the anti-terrorism legislation that granted the government a host of new powers, that finally succeeded in generating a sustained focus on Canadian surveillance law. The bill became law with few amendments, but emerged as the public's shorthand for the need for reforms to surveillance activities. **Public Safety Minister Ralph Goodale** and the new Liberal government have promised changes, with expectations that they will focus initially on a new "super" oversight body for security agencies and later open the door to further amendments. Yet despite assurances that improved oversight will provide adequate safeguards against intrusive surveillance, in recent months it has become apparent that weak oversight represents only a small part of the problem. Consider this year's report from the Communications Security Establishment (CSE) Commissioner, who uses legal language to obscure an otherwise clear admission that there are ongoing metadata violations within the CSE. The report notes that metadata activities were "*generally* conducted in compliance with operational policy" and that the "CSE has halted *some* metadata analysis activities" that were the subject of previous criticisms. The use of words like "generally" and "some" are no accident. The CSE Commissioner could have just as easily written that the CSE still does not conduct its metadata activities in full compliance with the law and that it has refused to stop some activities that were the subject of complaints. Yet the soft framing turns what should be a major story and source of concern into something largely ignored by the general public." Hill Times (Toronto Star)

*** Will Liberals defend Charter values on C-51?**
An editorial states, "When did the federal Liberals stop being liberals? In recent weeks we've seen an allegedly liberal government swerve, dodge and obfuscate to justify a bill - C-14 on assisted dying - which some courts and many constitutional scholars agree does not respect the Supreme Court's decision on Charter rights. The Supreme Court gave Trudeau one job to do. They even made it simple by giving him the language to use. Some provinces already had rules he could adapt. (…) Triangulation is the same strategy that, a year ago, lead Trudeau to support Bill C-51, Harper's version of homeland security. As with C-14 , many respected constitutional lawyers and rights groups said sections of C-51 violated the Charter. When an uproar over the moral hollowness of Trudeau's position offended actual liberals, he promised a Liberal government would fix C-51. Recently, the **Minister of Public Security** told the Commons he hopes a C-51 fix-it bill will be tabled ***"before Parliament rises for the summer."*** But will the Liberals fix C-51? Or "balance" it? How will we know? Paul Cavalluzzo - former commission counsel in the Maher Arar inquiry - has done the research on what needs to be fixed to make C-51 Charter-compliant. He's filed an application asking an Ontario court to strike down several provisions of C-51 because they trample Charter rights. His analysis is a valuable scorecard for any forthcoming Liberal bill. "Our main concern is the power C-51 attempts to give a judge to authorize a violation of Charter rights and freedoms if CSIS applies for a warrant to break the Charter," says Cavalluzzo in an interview. "In our view this is totally alien to our constitutional order." He argues the entire idea needs to be scrapped." Winnipeg Sun, A9 (Toronto Sun, Ottawa Sun, Edmonton Sun)

Missing Mountie
An opinion piece states, "Could Bob Paulson's days as top banana of the RCMP be numbered? If he doesn't start showing more cooperation in bringing about fundamental change to the nation's police force, he could be headed for a change in his career path. Some critics would argue it comes not a moment too soon. The organization he runs is more top down than Donald Trump. As the Force evolved in the Harper years, when labour laws were razed like old growth forests, Paulson's Mounties are not exactly members of Dudley Do-Right's RCMP. Paramilitary and politicized, the RCMP is in danger of becoming the fossil

force of law and order in Canada — and far worse, the kept police of the government of the day. Paulson's immediate problem resembles arrogance. As one senator put it to me, Paulson recently "stiffed" a Senate committee by sending deputies — two assistant commissioners — to answer questions regarding Bill C-7, the very controversial RCMP union bill. (…) Despite all that, though, there is a sense amongst his critics that he just doesn't get it. The Chair of the Civilian Review and Complaints Commission of the RCMP, Ian McPhail, testified before the Senate committee that his investigation into workplace harassment, requested by **Public Safety Minister Goodale**, had been impeded by senior Mounties. The Commissioner himself had forbidden McPhail to speak to RCMP members without the members first informing the Commissioner.(…) It is not all on Paulson. Since 2006, the RCMP has acted in such a way as to raise real questions about its independence and its impartiality. That was the year the Mounties weighed in to the federal election in dramatic fashion. Former Commissioner Guiliano Zaccardelli publicly announced an investigation into the then-Liberal government's handling of an income trust tax decision included in the federal budget. The RCMP had two press releases prepared to announce their investigation a month away from the election — one including the minister of the day's name, **Ralph Goodale**, and the other leaving it out. They opted to name, and some might say shame, the minister." iPolitics (2016-06-12)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Wildfire / Feu de forêt à Fort McMurray

*** South African President drawn into firefighters' pay dispute**
As 300 disgruntled South African firefighters prepared to fly home from Alberta on Sunday, questions were mounting over a contract that gave them barely one-third of the daily amount Alberta had allocated for their services. The issue has sparked a political uproar in South Africa that reached the highest levels on the weekend, when President Jacob Zuma ordered his environment minister to find "a solution to the impasse." While some South Africans criticized the firefighters for going on strike just six days after beginning their work in Alberta, many others - including an opposition leader - said their strike was justified by the need to fight for their rights and equal pay. Alberta Premier Rachel Notley and other officials have confirmed that Alberta agreed to pay $170 a day for each of the South African firefighters. Yet the firefighters signed contracts in which they will receive only a "stipend" of $50 a day - far below the Alberta minimum wage of $11.20 an hour. This discrepancy was "disturbing" and "not acceptable," Ms. Notley said last Thursday. The payment of $170 daily to their South African employer was intended to cover the $50 stipend, plus their regular South African pay (as little as $10 a day), along with "payroll burden, administration costs, training and other costs of preparing the firefighters to travel," according to Kim Connors, executive director of the Canadian Interagency Forest Fire Centre, which was responsible for bringing the firefighters to Canada. In addition, Alberta is covering all of their costs for accommodation, travel and meals. Globe and Mail, A16; CBC News

Other / Autre

*** Body of missing Corner Brook woman Patricia Boyd found**
A Corner Brook woman who was reported missing two weeks ago has died. The body of 57-year-old Patricia Boyd was found on Saturday. The Royal Newfoundland Constabulary and the Bay Islands Volunteer Search and Rescue Team had been searching places like the North Shore Highway and the Riverside Drive area of Corner Brook in the weeks since Boyd went missing on May 26. CBC News

*** Is another dust bowl coming?**
An opinion piece states "In the 1930s, a bad drought and an economic malaise upended farming systems around North America causing the Dust Bowl. Could climate change and the persistent post-2008 economic doldrums do the same? On one hand, the environmental signals are sobering. The drought in California seems to be long-lasting and even this year's record El Niño, which many had hoped would bring rainfall to the Southwest, seems to have done little. In Africa and India, hundreds of millions are facing food insecurity due to a combination of drought and armed conflict. Meanwhile in Canada, the Prairie Climate Centre has recently published an atlas suggesting the wildfires in Fort McMurray are a

taste of things to come. This year's hot, dry weather is consistent with climate change models that project the number of days reaching above 30°C each year will increase by three to four times in the Prairies over the century... Humanity is on the cusp of a major transformation as we come to grips with the necessity of feeding nine to 11 billion people on an increasingly hot and crowded planet. Thanks to climate change, meeting this challenge requires that we be far more thrifty with our resources and create not only productive but also resilient systems. The tools of the digital agricultural revolution are only just now emerging, but they will come to define how humanity feeds itself in the future. Canada, and the Canadian industry, should be at the forefront of this revolution." Hill Times

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Toronto 18 may have been shock for Canada, but it was not harbinger of a path to ruin
An opinion piece by Phil Gurski, president/CEO of Borealis Threat and Risk Consulting, states, "June 2 marks the 10th anniversary of the arrest of 17 men in the Greater Toronto Area in the culmination of a massive terrorism investigation by Canadian authorities. In what came to be known as the "Toronto 18" (the last subject was arrested in August 2006) Canadians were rudely introduced to homegrown terrorism five years after 9/11. For those who have forgotten the details, here is a short synopsis. A group of men in the Toronto area, led by an Afghan immigrant (Fahim Ahmad), attended a "training camp" near Orillia, Ont., in December 2005, chose three targets (the CSIS office in Toronto, the financial district and a military base), built a detonator, and bought fertilizer, all without knowing that their every move was being followed by CSIS and the RCMP. Their arrest saved the lives of thousands. The event was a seminal one for me as a CSIS analyst and I'd like to reflect on what this meant then as well as what is means now. (...) Fourthly, the case showed that CSIS and the RCMP could work hand in glove to successfully stop a terrorist act from occurring. The investigation started with CSIS and was handed over to the Mounties when it was clear a criminal act was being planned. CSIS sources became RCMP agents (not always an easy thing to do) more or less seamlessly and a serious terrorist attack was averted. There is little doubt that the CSIS-RCMP relationship has had its ups and downs but the two do work together well and Canadians are safer as a result. Lastly, despite more foiled plots and two successful ones in the interim, Canada remains in a good position when it comes to homegrown terrorism. We are not in the same league as France or Belgium or the U.K., or even the U.S. Our government has done a much better job at understanding the threat and putting measures into place, both soft and hard, to deal with it. We had the five-year $10-million Kanishka research project which, although many thought it under-delivered (I am among that group), set the stage for a more robust and more mature academic environment to look at terrorism where none existed before. **Public Safety Canada's** Citizen Engagement branch developed a community outreach program that was the envy of all our allies and the creation of the new Office of the Coordinator for Counter Radicalization and Community Outreach will hopefully enhance this effort. There is more work to be done but these are all enviable achievements." Hill Times

*** Des parcours qui sèment la consternation**
Pourquoi des jeunes dont les parents ont choisi de venir s'installer en Occident, comme c'est le cas du tireur du club Pulse, en viennent-ils à la violence au nom de groupes djihadistes ? Les experts interrogés par La Presse avancent plusieurs pistes. Des études ont démontré que les immigrants de deuxième génération, dont Omar Mateen faisait partie, « peuvent être à risque d'épouser des idéologies supportant la violence », note Jocelyn Bélanger, ancien chercheur au centre contre la radicalisation de Montréal et professeur adjoint à l'Université de New York à Abou Dhabi. Bien que ce soit l'exception, plusieurs exemples d'immigrants de deuxième génération qui ont complètement dérogé des valeurs de leur famille pour adhérer au terrorisme peuvent être observés. Les frères Salah et Brahim Abdeslam, l'un cerveau des attentats de Paris, l'autre mort en déclenchant sa ceinture d'explosifs, ont grandi en Belgique dans la commune de Molenbeek dans une famille ouverte. Nés de parents marocains immigrés en France, puis en Belgique, ils ont eu une adolescence parsemée de petits larcins avant d'embrasser l'idéologie de l'EI à l'insu de leurs proches.(...) Il y a aussi la jeune Maha Zibara, ex-élève du collège de Maisonneuve, arrêtée l'an dernier avec une dizaine de jeunes alors qu'elle s'apprêtait à quitter le Canada. Son père, un entrepreneur d'origine libanaise, était démoli. M. Zibara et sa famille sont de confession chiite, un courant minoritaire au sein de l'islam. Un jour, Maha Zibara a rejeté complètement la voie de ses parents. « Elle est venue me dire que les chiites sont des mécréants », avait-il raconté à l'époque. Pourquoi, alors, des

jeunes nés ici et élevés dans des familles qui n'adhèrent pas aux valeurs islamistes se radicalisent-ils ? Certains enfants issus de l'immigration récente sont perdus, hantés par une ambigüité identitaire, répond Mounia Ait Kabboura, chargée de cours à l'Université du Québec à Montréal et experte du radicalisme islamique. « Ils ne se retrouvent nulle part. Ils sont dans la culture religieuse et dans la culture occidentale, et c'est difficile de mélanger les deux », dit la chercheuse, qui a étudié la question auprès de jeunes établis au Québec. LaPresse+, 14

* **PM soft on terrorists**
A letter to the editor states, "It's a shock to see the "Canadian leading Bangladesh branch of ISILstory on Wednesday. Could someone please explain why the Trudeau government refuses to criminally charge citizens who become terrorists and revoke their citizenship? What incentive is their for a would-be terrorist to stay in Canada knowing this country will do nothing to revoke their citizenship if they return to Canada? The Trudeau government is weak when it comes to our citizens becoming terrorists!" The Province

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Border Security reality TV show pulled for privacy concerns
Canada's border agency is pulling the plug on the controversial reality TV program Border Security after the federal privacy commissioner found the agency violated the rights of a construction worker filmed during a raid in Vancouver. Privacy commissioner Daniel Therrien recently informed the British Columbia Civil Liberties Association, which spearheaded a complaint on behalf of Oscar Mata Duran, that the Canada Border Services Agency breached the Privacy Act by allowing production company Force Four to film the agency's examination of the migrant labourer. "As a matter of principle, it is our view that federal government institutions cannot contract out of their obligations under the Act," says the commissioner's 26-page report of findings. In light of the well-founded complaint, Therrien's office recommended the border agency end its participation in the television program, which the agency agreed to do. Agency spokeswoman Esme Bailey confirmed that Border Security: Canada's Front Line would not return for a fourth season. The commissioner also urged the agency to carry out a formal privacy impact assessment before embarking on any significant future initiative involving the use of personal information. Border Security began airing on the National Geographic Channel in 2012, chronicling encounters between border officers and the public. The unscripted series was seen by millions of Canadians and has aired in dozens of other countries. Times & Transcript, B4 (The Province, Vancouver Sun); Toronto Star; The Canadian Press (Guardian, Cape Breton Post); Chronicle Herald; The Record

* **Réseau de présumés trafiquants de drogue démantelé dans l'Est ontarien**
La Police provinciale de l'Ontario (PPO) a arrêté mercredi dernier cinq personnes lors de la saisie d'une importante quantité de marijuana dans une résidence d'Alfred-Plantagenet. Sur place, les policiers ont saisi des plants, de la résine et d'autres dérivés dont la valeur totale est estimée à 245 000 $.Des hommes de 18, 19 et 39 ans ainsi que deux femmes de 24 et 54 ans devront répondre, entre autres, à des accusations de production et de possession de drogue et de possession d'armes à feu. L'Agence des services frontaliers du Canada (ASFC) avait mené à une première enquête dans cette affaire après avoir contrôlé des colis destinés à une adresse d'Alfred-Plantagenet. Ceux-ci contenaient de la marijuana.

Canada's choice for migrant workers: decent work or entrenched exploitation?
Canada's Temporary Foreign Worker Program (TFWP) is at a crossroads. After years of escalating concern about employers' growing reliance on, and widespread exploitation of, low-wage migrant workers, the Standing Committee on Human Resources, Skills and Social Development and the Status of Persons with Disabilities (HUMA Committee) is reviewing the controversial program and will report to the minister of Employment, Workforce Development and Labour. At this crucial moment, what will Canada choose: secure status and decent work, or entrenched exploitation for migrant workers? Canada's Choice, my new report published by the Metcalf Foundation maps what is at stake. The findings are troubling. Low-wage migrant workers face deeper insecurity now than before the 2014 "reforms" by the previous government. Hill Times

War resister wants PM to keep his word

* An opinion piece states "Like much of the rest of the world, Rodney Watson has spent a lot of the last week thinking about the world's most famous war resister. But Muhammad Ali's televised memorial service Friday had particular resonance for Watson, who watched it from the room above the First United Church in Vancouver's (…) A new Insights West poll released this week shows a majority of Canadians support the idea of making Iraq War resisters like Watson permanent residents of their adopted country. Watson, 38, said he appreciates the widespread support of "the good and conscientious citizens of Canada" evidenced in the poll results, and he hopes the federal government will notice and take action on behalf of himself and 14 other Iraq War resisters in Canada. "For those same ones shedding crocodile tears and praising Muhammad Ali, who have the power to actually do something, I have to say, 'What about us?'" said Watson, who served in Mosul, Iraq, in 2005 and 2006. He left the U.S. for Canada in 2009 to avoid another deployment to Iraq, and sought sanctuary in the First United Church. The Canadian government ordered him deported in 2009." Vancouver Sun, A8

* **Mother of Sask. overdose victim testifies**

It's perfectly legal to buy the ingredients to manufacture the deadly opioid fentanyl. Anyone with an Internet connection can order the stuffonline. Marie Agioritis, a Saskatoon mom who lost her son Kelly to a fentanyl overdose two years ago, is joining forces with a Canadian senator, hoping a new law making those ingredients illegal will put a dent in the fentanyl trade. Q What is the government doing to combat the spread of this drug? A Agioritis was in Ottawa last week testifying at a Senate committee hearing on a new bill aimed at making the ingredients for manufacturing fentanyl illegal. Sen. White, who introduced Bill S-225, says without making the ingredients illegal it's tough for police and customs agents to crack down on the trade. Leader Post

Don't like the airport security line? Pay to shorten it

Let the users pay! Some airport and airline executives have somehow got it in their heads that airport security is like universal health care, and that if wait times at the airport are too long, then the federal government ought to fix things by spending more public money. But if we want to shorten the lengthening lineups at airports, and the way to do it is to hire more security agents, it only makes sense to raise the money to do this from users: airline passengers. Canada's airports are supposed to be user-pay affairs. You pay an airport improvement fee when you fly, and an airport security fee too, embedded in the price of a ticket. Alternatively, the Canadian Air Transport Security Authority can figure out how to become more efficient, and move more people through screening, faster. The last federal Liberal budget gave an additional $29-million to CATSA, but taxpayers shouldn't be subsidizing air travel. Nor should air travel be subsidizing taxpayers: At the moment, the security tax on air travellers appears to be taking in more money than Ottawa is giving to CATSA and airport security. User-pay makes sense; user-pay-plus-a-little-extra-for-Ottawa does not. Globe and Mail

CYBER SECURITY / CYBERSÉCURITÉ

* **Mafiaboy finds new mission in life**

Mafiaboy is now a man and he's on a mission. As a 15-year-old hacker in 2000, Mafiaboy (real name: Michael Calce) paralyzed the websites of the biggest names in media and e-commerce, including CNN, Amazon and eBay. The RCMP and FBI tracked him down in Île-Bizard. He pleaded guilty to 58 charges and spent eight months in a youth detention centre. Now 31, Calce recently started a cyber-security company - Optimal Secure - focusing on the financial sector in Montreal, Toronto and Vancouver. His specialty: "penetration testing." Companies hire him to try to penetrate their computer defences so they can secure systems before hackers strike. Computer hacking is a constant threat. In recent weeks alone, hackers have broken into some of Facebook's Mark Zuckerberg's accounts; forced the University of Calgary to pay a $20,000 ransom after crippling its computer systems; and stolen $81 million U.S. from the Federal Reserve Bank of New York. The Montreal Gazette sat down with Calce and learned that "spear-phishing email attacks" are among the scary things to fear online today. (This interview has been edited and condensed.) Gazette, A3

* **Massive North Korea cyber attack thwarted after hacking South Korea: report**

North Korea has hacked into more than 140,000 computers at large South Korean conglomerates and government agencies and planted malicious codes that may have been intended for a massive cyber attack that has been thwarted, a news report said on Monday. The hacking originated from an internet address traced to the North Korean capital and targeted a software used by about 160 companies and government agencies to manage their computer networks, Yonhap news agency reported, citing the police. The internet address was identical to the one used in a 2013 cyber attack against South Korean banks and broadcasters that froze their computer systems for more than a week. Reuters (Yahoo! News)

* **After Bangladesh: How a massive hack shook the banking world**
It was the start of a weekend in Bangladesh when an official at the country's central bank checked a printer in a server room. The tray was empty, which was strange. There should have been a sheaf of reports confirming payment instructions sent through the Swift system, the network that connects 11,000 banks around the world. The printer glitch was no accident, but a deliberate strategy by criminals to hide their tracks. A day earlier, cyberthieves had issued instructions to transfer $951-million (U.S.) out of Bangladesh Bank's account at the New York Federal Reserve. Most were declined, but $81-million was transferred to a bank in the Philippines, never to be seen again. The theft in early February sent shock waves through the global banking community. It was not simply enormous in size, but ambitious in its selection of target: the Swift system, the backbone of international finance. The methods deployed were highly sophisticated, involving a combination of technical prowess and intimate knowledge of how Bangladesh Bank interfaced with Swift. Gottfried Leibbrandt, chief executive of Belgium-based Swift, called the Bangladesh cyberattack "a watershed" for the banking industry. "There will be a before and an after Bangladesh," he said last month. What's more, it wasn't an isolated incident: Swift was aware of at least two other cases where cyberthieves used the same modus operandi, albeit with far less success. Four months after the theft, much remains unknown about the perpetrators and their methods. It's not clear, for instance, how the malicious code was implanted into the systems at Bangladesh Bank. And both private firms and law-enforcement authorities are conducting investigations to uncover the culprits. Some signs point to a gang of expert cybercriminals; others point to the possible involvement of a state actor. The theft shows that cybercriminals are growing increasingly audacious. Globe and Mail, B1

* **The G7 and cyberspace: 'give peace a chance'**
An opinion piece states “The G7 summit meeting hosted by Japan May 26-27 issued a document entitled 'G7 Principles and Actions on Cyber.' This cyber policy statement was the most elaborate one issued by the G7 since 2011. The intervening years have revealed continuity on some prominent themes, such as support for the free flow of information and respect for human rights online. However, the increasing use of cyber operations by authoritarian regimes in suppressing dissent and the infringement of privacy rights via mass state-conducted cyber surveillance, has revealed the stress such rights are under. The removal of Russia from the G8 context may have allowed for stronger commitments in the field of human rights, but it also highlights the challenge of achieving international cooperation on cyber security against a backdrop of deteriorating geopolitical relations between leading cyber powers. In this crucial realm of international cyber security, the pronouncements from the G7 summit are not all that reassuring. The goal of a peaceful cyberspace is conspicuous by its absence from the statement. The G7 will promote security and stability in cyberspace, but there is no apparent aspiration to keep cyberspace a realm of peace rather than war. The statement speaks of taking ‘decisive and robust measures in close cooperation against malicious use of cyberspace both by states and non-state actors,’ but these measures are not specified and the tone here suggests they will not be of a diplomatic nature. The G7 appear to be laying the ground for undertaking military responses to cyber operations they deem hostile by affirming that ‘cyber activities could amount to the use of force or an armed attack within the meaning of the UN Charter.’ Suffering ‘an armed attack’ entitles a state under the UN Charter to exercise the right of self-defence, thus this framing of such an eventuality is fraught with serious politico-military consequences. How and by whom such a determination of a cyber attack is made is left unaddressed in the G7 statement and there is clearly wide scope for unilateral (and potentially dangerous) interpretation and action in this regard.” Hill Times

LAW ENFORCEMENT / APPLICATION DE LA LOI

Seeking clues in cold case: Ground search relates to 1982 disappearance of Henrietta Millek
Search crews looked for evidence near Makinsons this weekend after receiving a tip on a decades-old missing-person case. Henrietta Millek, originally from Nain, was living in St. John's at the time of her disappearance in December 1982. She was 25 at the time. Originally, it was believed Millek's last known location was at a club in downtown St. John's. It was reported she may have left the bar against her will. Her belongings, including her purse, were left there, and she never returned for them. RNC Const. Geoff Higdon told reporters Saturday new information led to a ground search in the area of Roaches Line almost 34 years after she disappeared. "Recently we received information that the last known location may have been in the area of the Trans-Canada Highway, and I guess what at that time would have been Roaches Line, as Veterans Memorial (Highway) wasn't here," said Higdon. "We believe she may have been headed towards Makinsons, and we do know that she never made it to her destination, unfortunately, and the information was that her last known location was here on the Trans-Canada Highway, so we're searching the area between those two points." Almost 100 searchers scoured the area in the morning, and they were expected to continue all day. Crews from the RNC, the RCMP, the Rovers - Central Avalon Search and Rescue and the Avalon North Wolverines were involved. Telegram, A1

Police investigate chapter in New Glasgow Gate Keepers gang
Police executed a search warrant at the New Glasgow chapter of the Gate Keepers motorcycle group early Sunday. "Members of the Nova Scotia RCMP executed a search warrant on MacLean Street in New Glasgow in relation to an ongoing investigation," said Corp. Jadie Spence, a media relations officer for Nova Scotia RCMP. "It's a clubhouse for the Gate Keepers motorcycle gang," he said. Spence said there are currently seven chapters of the Gate Keepers in Nova Scotia, including one in Musquodoboit Harbour, where that chapter held a party over the weekend. "They're a support group of the Hell's Angels, who don't have a presence in Nova Scotia at present," Spence said. They were assisted by the New Glasgow Regional Police and Pictou County RCMP. The warrant was executed at about 6 a.m. The street was closed down. On Sunday at 6 p.m., police were still at the scene. There was no word about specifics of the investigation, Spence said. "There are no arrests and no charges at this point in time," Spence said. ChronicleHerald, A6; Cape Breton Post

Canadian officials offer condemnation and sympathy after Florida mass shooting
After a mass shooting on Sunday that killed at least 50 people and injured dozens more at a gay nightclub in Florida, many Canadians were reflecting on what the violence means for the LGBTQ community. Candlelight vigils to mourn the victims were planned in several Canadian cities Sunday night. Hundreds crowded for a candlelight vigil in Toronto in a predominantly gay neighbourhood. (…) The executive director of Pride Toronto, a not-for-profit with the goal of bringing together the city's LGBTQ community, said the massacre was a grim reminder of the setbacks his community faces. "It reminds us that hate and discrimination are still a big part of this society, and that because of this, some of our brothers and sisters this morning lost their lives," Mathieu Chantelois said on Sunday. The organization also runs Toronto's pride month, and Chantelois said Pride Toronto was already working with city police and the RCMP but would see if there were any additional security steps that could be taken. "The main objective of Pride is to create a safe space for our community to gather together and feel comfortable," he said. Spencer Chandra Herbert, a member of the British Columbia legislature, was in Quesnel, B.C., celebrating the small town's second annual pride celebration with his husband when he heard the news. His immediate reaction was disbelief. Canadian Press (Ottawa Sun, A4, Red Deer Advocate, Hamilton Spectator); Canadian Press (National Post); * CBC News

How the quest for cheap beer may change Canada
An opinion piece by former Ontario cabinet minister John Milloy states, “Canadians like to talk about trade. Remember the dust-up over the Trans-Pacific Partnership agreement in the last federal campaign, or earlier passionate debates over the Canada-U.S. Free Trade Agreement and its successor, the North American Free Trade Agreement? There is one exception. When it comes to free trade within Canada, no one ever seems to pay much attention. We better start. A recent New Brunswick court decision, likely to end up at the Supreme Court of Canada, has the potential to radically change our country and its economy. Although Canadians may maintain a fierce loyalty to their province or region, I also like to think we see our nation as a place where citizens are free to travel, live and enjoy life wherever they want. (…) Enter Gerard Comeau, a retired New Brunswick steelworker who went in search of cheap beer across the

border in Quebec. Such an appalling act of bad citizenship does not go unnoticed in Canada. The RCMP immediately stopped him upon his return and fined him for transporting more alcohol across the border than allowed under the modest limit set by the New Brunswick government." Hamilton Spectator

*** Protesters arrested at Muskrat Falls site**
Six people were arrested Sunday during a protest at the Muskrat Falls development site, the Happy Valley-Goose Bay RCMP stated in a news release. Demonstrators began their protest last Thursday at Nalcor's hydroelectric site at Muskrat Falls, blocking the entrance road into the project. On Friday the Supreme Court of Newfoundland issued a court order that directed the protesters to leave Nalcor's property. The RCMP continued to monitor the protest. On Sunday at 11:55 a.m., five protesters refused to comply with that court order and were arrested, the RCMP stated. A short time later, another group of protesters arrived and one protester was arrested for obstruction, police said. All six protesters were to be held overnight in custody and will appear in provincial court at Happy Valley-Goose Bay Monday. Five protesters are charged with breaching a court order and all six are charged with obstruction. The RCMP continues to monitor the situation at the Muskrat Falls site, but no additional incidents have been reported and the on-going protest remains peaceful, police said. Telegram, A5; CBC News

*** HALIFAX: RCMP escort Canada's 911 Ride**
The RCMP escorted Canada's 911 Ride in both the Halifax area and Annapolis Valley over the weekend. The annual police-escorted 911 Ride raises funds for families of fallen emergency service personnel, helps children who are victims of violent crimes, and provides public access to defibrillators in local communities. This year's Atlantic Ride took 70 participants through the South Shore and Peggys Cove areas on Saturday. Riders departed Halifax at 8:30 a.m., headed to Peggys Cove, then on to Lunenburg and Bridgewater. The riders returned to Halifax Saturday afternoon. Chronicle Herald, A5

*** RCMP seize guns in Delburne**
Police seized a number of stolen firearms and took a man and woman into custody at a campground in Delburne on Friday. Three Hills RCMP and the Priority Crimes Task Force launched an investigation in early May after RCMP received intelligence about stolen firearms. The search warrants were executed at two trailers in Barking Fox Campground with the assistance of Police Dog Services and K Division's Emergency Response Team. A man and a woman were taken into custody. RCMP continue to investigate. No other information was released. Red Deer Advocate, A3

*** Larry Tremblay est le nouveau patron de la GRC au N.-B.**
Le commissaire adjoint Larry Tremblay devient le 30e commandant de la Division du N.-B. de la GRC. Il remplace le commissaire adjoint Roger Brown qui prend sa retraite après plus de 35 années au service de la GRC, dont les trois dernières à titre de commandant au N.-B.. Avant de se joindre à la Gendarmerie, Larry Tremblay a fait partie de la Marine royale canadienne pendant près de quatre ans. Il possède une expérience de plus de 30 ans au sein de la GRC à différents postes. Il a débuté sa carrière au N.-B. où il a passé 11 ans. Il a ensuite travaillé à l'Unité mixte d'enquête sur le crime organisé et à la Section antidrogue de la région d'Ottawa et a oeuvré au sein de services spécialisés à Regina et à Milton en Ontario. De 2004 à 2008, il a travaillé au Service canadien du renseignement de sécurité (SCRS) avant de devenir directeur général des Opérations criminelles de la GRC. L' Acadie Nouvelle, 10

*** Woman in witness protection program sues RCMP for negligence**
Woman who helped on drug case says RCMP compromised her identity, which forced her into witness protection A woman in the federal witness protection program is suing the RCMP for negligence and for undermining her trusted relationship with Canada's national police force.The details of her case are contained in a judgment by Ontario Superior Court Justice Patrick Smith, who granted an injunction forcing the RCMP to continue financially supporting the woman, known as Jane Doe, as well as allowing her to expand the scope of her lawsuit against the Mounties. The document tells the story of a woman who did the right thing, only to lose it all — family, friends, a good job and her mental health. The heavily redacted court ruling summarizes the woman's claims, which included that after tipping off police about a drug crime, the RCMP compromised her identity and refused to own up to it. The court ruling states that after happening upon intelligence related to a crime syndicate, she shared what she knew with her

municipal police force. The RCMP then used that information to investigate and prosecute several members of a criminal syndicate on drug-related charges. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Prisons paying more for native spiritual services
Federal prisons are paying significantly more each year for indigenous spiritual services than for all other religions combined. Indigenous people make up about 25 per cent of the 14,865 people who are currently incarcerated in federal prison. The Correctional Service of Canada (CSC) is spending $8 million annually on sustaining spiritual services for indigenous offenders - versus $6.75 million for other religions. Spokesperson Avely Serin said "Elder services" help offenders follow a "traditional healing path" and provide advice to the heads of institutions about "access to ceremonial objects and traditional medicines within the institution." As of last October, 85 per cent of indigenous offenders in custody, or 3,156, had undergone an "elder review," Serin said. The cost was about $2,500 per person. (...) The correctional service takes "a lot of criticism for the overrepresentation of First Nations people in the prison system," said Catherine Latimer, executive director at the John Howard Society. She suggested that could be one reason for the extra funding. Indigenous people make up a quarter of the prison population versus 4.3 per cent of the general population, according to Canada's Correctional Investigator. Indigenous offenders do have better outcomes when "reconnected with their spiritual and cultural traditions," said the Correctional Investigator of Canada's annual report for 2014-15. But spiritual services help offenders of other religions, too, said Kate Johnson, a former chaplain at Joyceville Institution in Kingston, Ont. Almost half of offenders are Christian, a majority of those Catholic, and just over five per cent are Muslim. Postmedia Network (London Free Press, NP5, National Post, Leader-Post, Edmonton Journal, Vancouver Sun, Windsor Star, Montreal Gazette, Calgary Herald, StarPhoenix, Province, Ottawa Citizen)

Kingston Penitentiary tours send wrong message
An opinion pieces states, “Three years ago, Kingston Penitentiary was decommissioned and briefly opened its doors to tourists to raise funds for the local United Way. Hugely popular, tickets for the October 2013 "KP" tours quickly sold out, generating more than $180,000 in 15 days. Wanting in on the action, the Correctional Service of Canada (CSC) partnered with Habitat for Humanity to offer another block of tours in November 2013, with proceeds to go toward expanding the construction of affordable housing by federal prisoners in the name of "rehabilitation and reintegration." These tours also sold out fast, fostering further debate in the Kingston, Ont. area about the potential for KP to become a major tourist attraction. This week, tickets went on sale for a new series of guided tours at KP led by students and supported by retired correction service employees. The tours are being sold by project partners - the City of Kingston, CSC and the St. Lawrence Parks Commission - as "a rare and unique opportunity to go behind the walls of Canada's oldest and most notorious maximum security prison." Many from the Kingston area and elsewhere are hoping to enter the facility, which opened in 1835. From late June until the end of October, it is estimated that KP visitors will "pump more than $6 million into the local economy."” Toronto Star, A15

Egale calls for Trudeau apology
The assault on a gay night club in Orlando has cast a shadow over two reports that call for an apology from Justin Trudeau's government and restitution for homosexuals who were prosecuted and persecuted under Canadian policies in the past, and who still suffer discrimination today. One report, prepared by Egale, a national organization that advocates for lesbian, gay, bisexual and transgender Canadians, asks the Prime Minister to acknowledge in principle the need for an apology and redress for homosexuals who were criminally targeted because of their sexuality. Germany and Australia (through its state governments), are already at work on some combination of pardons, apology and redress. Egale said on Sunday that it remains committed to releasing the report after the weekend's tragedy. It will be delivered to Justice Minister Jody Wilson-Raybould on Monday and through her to the Prime Minister's Office. An advance copy was provided to The Globe and Mail. The report proposes that retired Supreme Court Justice Frank Lacobucci be asked to lead a one year study on what shape an apology, restitution and action to prevent future discrimination against sexual minorities should take. The report advocates "a process of 'truth and rehabilitation,' whereby the federal government will acknowledge the wrongs done to

our community and commit to a process to make it right." (…) Gay rights activists hope he will announce that he embraces the recommendations of both reports in principle beforehand. But moving from a pardon to an apology with promise of redress may be more than this government is prepared to embrace, however other countries proceed. Globe and Mail, A17

*** Fraudster released on early parole after seven months in jail**

Unrepentant and still contesting his conviction, former Regina businessman-fraudster Steven Vincent Weeres is now a parolee, mere months into a lengthy prison sentence. As a non-violent offender serving his first federal term behind bars, Weeres, 57, qualified for Accelerated Parole Review and is now out after seven months. "The basic difference is that they're eligible for parole at onesixth of their sentence, rather than one-third," Parole Board of Canada spokesman Patrick Storey explained. (The federal government ended the program in 2011, but courts have since ruled the change doesn't apply retroactively to those, like Weeres, whose crimes predate the revamped law.) "You preyed on unsuspecting individuals and bilked them of thousands of dollars. You impacted your victims' financial well-being, emotional well-being and their credit ratings," states his recent parole decision. "However, the board finds that you do not have a significant history of violence, nor have you been involved in the use of weapons. There is no indication that you have exhibited a pattern of violent behaviour, or that you have risk factors that would likely lead you to commit an offence involving violence," it continues. The board granted Weeres day and full parole on May 6. The Leader-Post has learned he's residing in a B.C. halfway house. Contacted by phone Saturday, Weeres said his appeal of conviction for fraud and money laundering "is still moving forward." He never appealed his sentence. No date for the appeal has been set. StarPhoenix, A7 (Leader-Post)

*** Most Wanted**

A man convicted of killing a fellow inmate at Bowden Institution is one of two most wanted this week. Keith Clinton Sandmaier - born Sept. 9, 1977 - is wanted on a Canada-wide warrant. A February fatality inquiry heard his criminal history includes stabbing to death Tung David Louie with a steak knife over a $30 debt when the pair were inmates at the minimum-security southern Alberta federal prison. Louie, who was serving a 12-year sentence for weapons, drugs and robbery offences, was unarmed when he got into a June 2011 fight with Sandmaier in a common area of Bowden Institution. Sandmaier was armed with a knife, though authorities were unable to confirm where he got it, and he stabbed Louie five times, according to an inquiry report into the homicide. At the time of the killing, Sandmaier had been awaiting a hearing because guards had found a sharp wooden weapon in the cell he shared with another inmate. Prison officials had deemed both inmates suitable to remain in the prison's general population. Parole records previously revealed that Sandmaier was motivated by a $30 debt when he stabbed Louie to death in an outdoor common area in the medium-security prison south of Red Deer. Sandmaier later pleaded guilty to manslaughter and was sentenced to five years. Edmonton Sun, A53

Distillery district for KP, harbour refloated

As the city sets its sights forward - on the future of its waterfront - Robert Kiley looks back. For the Ontario Green party candidate, the project is a chance to make good on last year's promise. During the federal election last November, Kiley was the campaign manager for MP candidate Nathan Townend. Amid federal campaign promises, one of the points in Townend's campaign was focused locally: on Portsmouth Olympic Harbour and Kingston Penitentiary. "Nathan and I put our heads together and said: 'What would be a local, sustainable and livable solution to revitalizing both [sites]?'" Kiley said. When the pair noticed a "budding brewery culture" in Kingston, they concocted a plan. A local distillery district could be built, alongside the often-discussed idea of an international sailing hub. In addition to local beer, the district would be a collective of Kingston artisans, food services and accommodations. "Green values are resiliency in the local economy, resiliency in local food systems, and resiliency in community engagement," Kiley explained. With this idea, all three values came together. When Townend was unsuccessful in his MP race, with 4.46 per cent of the vote in Kingston, the idea was put aside temporarily. Now, Kiley is taking the city's call for ideas as a chance to fulfil their promise anyway. "Currently, the city is hosting one-on-one interviews about the Kingston Pen site, and [this week] they'll be having an information session," Kiley explained. In preparation, he put together an online petition last Tuesday, to measure support and "add a bit of weight" to the idea. As of 6 p.m. Friday, the petition of www.change.org had garnered 121 signatures. Kingston Whig-Standard, A2

*** Un baromètre**
Arrêté, jugé sommairement puis gracié de façon théâtrale au moment où il allait être exécuté, Dostoïevski croupit quelques années au bagne, en Sibérie. Il en rapporte notamment la matière de ses Carnets de la maison morte, vaste récit de ses observations en prison. (…) Depuis que je m'intéresse davantage au sort fait aux prisonniers à l'heure de l'austérité, j'ai croisé sur les chemins de la prison quelques-uns de ces êtres de bonté. (…) Dans les prisons québécoises, un problème de surpopulation et de manque de services de base se pose plus que jamais. Depuis quelques mois, ce problème est illustré de façon éclatante à la suite de la fermeture de la maison Tanguay, une prison pour femmes. Bien qu'elles ne purgent que de brèves peines pour des délits mineurs, ces détenues ont été transférées à l'Établissement Leclerc, un ancien pénitencier fédéral de longue durée pour hommes. Certains, rappelait Dostoïevski, pensent " qu'il suffit que les détenus soient bien nourris, bien entretenus, qu'on suive toutes les prescriptions de la loi pour que les choses aillent bien ". Mais le traitement humain ne tient pas qu'à l'administration du règlement, rappelait-il aussi. La prison est une bête énorme qui écrase physiquement et moralement. On ne réhabilite pas une vie brisée en l'écrasant davantage. La semaine dernière, au moment de répondre à des questions au sujet des traitements douteux subis par les femmes de la prison Leclerc, le ministre Martin Coiteux a eu à peine le temps de dire quelques mots avant que, du milieu de la meute médiatique, on ne s'empresse de lui demander pourquoi certains prisonniers avaient droit à des cours de yoga, de zumba ou à de la zoothérapie. Le Devoir, A2

*** Ministers can't avoid tough issues**
An editorial states, "How long does it take a politician to make the transition from opposition to government? There's no hard and fast rule. Some MLAs who've spent a long time on opposition benches make a seamless transition into government, occupying cabinet portfolios with such ease and comfort it looks as though they have done it before. (…) Last week, a national news report revealed Manitoba's provincial jail system relies more on solitary confinement than any other province. The overuse of solitary is top of mind following the death of Richard Wolfe, a Saskatchewan prisoner who spent 640 consecutive days in a cell, alone, for 23 of 24 hours each day. Wolfe died from a heart attack after being transferred to a federal jail. Solitary confinement has always been prickly for politicians. On the one hand, human rights adocates and prison-welfare experts almost universally decry it. The United Nations has declared it a form of torture. Several provinces are reviewing their policies to ensure no inmate spends inordinate amounts of time segregated from other prisoners. On the other hand, the welfare of convicted criminals has never been a compelling issue for the majority of voters. Some of our least compassionate citizens celebrate the inherent cruelty of solitary. So, perhaps it made sense that, when asked by the *Globe and Mail* whether she was concerned that Manitoba was leading all provinces in the use of solitary, Stefanson said via a spokeswoman the province had "no plans to review segregation policies at this time." That response is simply unacceptable. Stefanson, a long-suffering opposition MLA, is getting a well-deserved first taste of governing. And the reality of government is that you must be ready and willing to respond when an issue such as this arises. Even those not on your personal top-10 list of pressing policy issues. The story required a response of some sort." Winnipeg Free Press, 8

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Gay communities react to targeted hatred**
Eric Pineault says his heart sank Sunday morning when he went on Facebook and learned of a gunman's deadly assault on an Orlando, Fla., gay nightclub. Pineault, the president of Montreal Pride, had visited the Pulse a couple years ago while on vacation. It was a smallish club with the usual Top-40 tunes and thrumming house music. But like all other gay nightclubs, it was a place of comfort - where you could let your guard down. "People can hang out and be themselves. It is not always possible to hold your lover's hand on the street. There, you can kiss and be yourself," he said. "No boundaries." (…) Violence against the LGBT community around the world remains a "grave concern," said a blog post on the Amnesty International website last month. (…) Data from Statistics Canada show that, in 2013, most police-reported hate crimes were non-violent, typically involving mischief, such as graffiti. However, two-thirds of cases motivated by hatred for someone's sexual orientation involved violence. A 2015 Justice Canada

report found that police data were likely to "seriously underestimate" the extent of hate crimes targeting the LGBT community because they were less likely than other victim groups to report incidents to police. "Analysis of calls to a hotline in Toronto run by the 519 Church Street Community Centre shows that a high incidence of hate-motivated incidents directed at gays and lesbians involve physical assault," the report said. "Only a minority of incidents reported to the hotline had been reported to the police." As Pride organizers from Vancouver to Montreal scrambled Sunday to organize vigils to mourn those killed in Orlando, they also said they planned to step up their vigilance and reach out to police to see if any security enhancements were needed at their events. London Free Press, NP4 (National Post, Calgary Herald, Ottawa Citizen, Windsor Star, StarPhoenix, Leader-Post); La Tribune (La Presse)

*** How Tory changed tough approach to keeping city safe**

In June 2003, Toronto mayoral candidate John Tory ran a tough-on-crime campaign that promised to add 400 police officers to the force's roster - even if it meant raising property taxes. The fact was the crime rate had been falling for decades. But just days before Tory released his crime platform, a man was charged with raping and murdering 10-year-old Holly Jones in her west end neighbourhood. "John Tory, 2003 edition, would not have been unlike many, many candidates who try to get elected by seizing the anti-crime agenda," says city hall veteran Councillor Joe Mihevc. That fall, Tory won the controversial backing of the Toronto police union, but lost the election to David Miller. Thirteen years later, Tory is mayor and gun violence has spiked. Twenty-one of the city's 33 homicide victims were killed by a firearm. (Receiving much less attention are the 17 pedestrian deaths on Toronto streets this year.) There is no evidence of an upward trend in the overall crime rate. But the default reaction of the police union and some right-wing commentators is that more cops should be hired. Whether doing that would make a difference is a hotly debated subject. Tory is not among those calling for more police. Instead, when Tory talks about keeping Toronto safe, he refers to better deployment and outsourcing certain policing tasks to ensure more officers focus on gritty crime-fighting, not "monitoring left turns." "A lot of other things have changed, too. I think we've all resolved to make sure that we find different ways to do policing in the city of Toronto," Tory told a recent news conference on gun violence. The mayor is recognizing that "the real task of keeping cities safe ... is complicated," says Mihevc. "There's crime prevention, lighting, making sure young boys are kept busy ... that of course is not a very sexy campaign slogan." This week could be a watershed moment for policing in Toronto - and Tory. On Thursday, his "transformational task force" on policing will unveil an interim report recommending ways to reorganize and modernize the force, while cutting costs. Earlier this year, after Mihevc and other councillors tried to flatline the police budget, which pushed past $1 billion, council voted 41-1 on a motion saying there is an "urgent and abiding" need to restrain policing costs. Tory, who sits on the police board, urged councillors to let the task force do its work. Toronto Star, GT1

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

*** Missing: Annie Yassie was 13 when she disappeared over 40 years ago**

Eva Yassie's dream about her missing baby sister is almost always the same. Annie Yassie is still 13, she is standing in the distance and she is smiling. But when Eva asks her questions, Annie doesn't answer. When Eva tries to touch her, Annie can't be reached. "It really disturbs me, these dreams," Eva Yassie says, taking a long drag on a hand-rolled cigarette. "I call her name and see if she can.... She just looks at me and smiles, and fades away. I can't get no answers." Questions have haunted Eva Yassie for 42 years, since June 22, 1974, when Annie disappeared into the night a few kilometres outside Churchill, Man. She was just a kid, 13, just back to Dene Village from residential school. CBC News (2016-06-12)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Decriminalize marijuana, NDP urges Liberals**

The New Democrats are urging the Liberal government to decriminalize pot before they legalize it. Prime Minister Justin Trudeau campaigned on a promise to legalize, regulate and restrict access to marijuana, and his government plans to get started next spring. Meanwhile, the existing criminal law remains on the books and police are expected to enforce it. The NDP is introducing an opposition day motion on Monday calling on the House of Commons to recognize there is a contradiction in giving people criminal records for something the government has said should not be a crime. The motion also calls on the government to decriminalize simple possession of marijuana for personal use immediately. "Arresting people and giving them criminal records for possession of small quantities just doesn't seem fair, in light of their commitment, apparently, to legalize marijuana," New Democrat MP Murray Rankin said Sunday. Rankin also said the law is being applied inconsistently across the country, which adds to the unfairness. Rankin said one way to decriminalize it without having to wait for legislation to make its way through Parliament would be to have Attorney General Jody Wilson-Raybould issue a directive under the Public Prosecutions Act ordering Crown counsel to avoid proceeding with prosecution for simple possession offences. "I just think the sensible thing to do would be to no longer charge people until we can get the reformed regime in place," said Rankin. Health Minister Jane Philpott formally announced in April the federal government's plan to legalize and regulate marijuana when she spoke to the United Nations General Assembly in New York. Canadian Press (Telegram, A10, Red Deer Advocate, Calgary Sun, Winnipeg Sun, Toronto Sun, Edmonton Sun, Waterloo Region Record, Hamilton Spectator, Toronto Star, Chronicle Herald)

* **'Craft cannabis' growers fight for legal role**

Travis Lane has been growing marijuana since high school, when his first pot plant swiftly withered and died in his bedroom closet. By the time he was 20, he had cultivated a small basement grow-operation. Now in his mid-thirties, Lane owns an online dispensary and runs two 390-plant operations on Vancouver Island. He employs two growers and raises his plants without pesticides or liquid fertilizer. "I don't want to hide what I do. I'm good at what I do. I'm proud of being good at what I do," he said. "I've been proactive my whole life in trying to move towards a time where I can openly be a cannabis professional." Lane holds two Health Canada licences for the grow sites, making his pot production legal for medical purposes. But with the federal Liberals committed to legalizing cannabis for recreational use, Lane is among the smaller-scale growers fighting for a seat at the table. The government is still in the early stages of developing the legislation it plans to introduce next spring. Those behind a budding "craft cannabis" movement warn, however, that if the law favours large-scale commercial producers, then jobs and potential tourism revenues will be lost and the black market will continue to thrive. Canadian Press (Red Deer Advocate, A10, Telegram, National Post)

* **MADD Canada calls for roadside drug-testing equipment for police**

Mothers Against Drunk Driving wants police forces across Canada to be enforcement-ready for people driving while under the influence of legal marijuana. Danielle Cole, president of MADD greater Fredericton chapter, said she met with MPs in Ottawa to start getting prepared for the legalization of marijuana - the drug most likely to be the cause of impairment behind the wheel. MADD Canada is calling for an amendment to the Criminal Code about driving while under the influence of drugs. Cole said there is a strong misconception among young people about the use of marijuana and driving. "If you ask a teenager about this, they'll tell you they drive better [high]," she said. In 2014, MADD reported 2.6 per cent of all impaired driving charges were drug-related. In 2012, New Brunswick had 83 deaths related to traffic accidents of which there were 17 drug-related driving impairments accidents causing death, which is lower than the 22 alcohol-related driving deaths. Five deaths involved both drugs and alcohol. That is more than Prince Edward Island, but less than Nova Scotia and Newfoundland. Daily Gleaner, A2

* **Details on marijuana task force coming, to deal with supply, jurisdiction, retail, taxes**

A marijuana industry official says existing licensed producers could supply just 10 to 15 per cent of what demand will be once recreational use of marijuana is legalized. Insiders say the questions a government task force on marijuana legalization must deal with include how and where consumers will purchase it, how much involvement the provinces will have in its regulation, how adequate supply will be created, and what level of taxes should be applied. Multiple sources have confirmed a report that former Liberal cabinet minister Anne McLellan has been appointed to lead the task force, though this has not been publicly announced yet, and that the whole task force and its mandate will be revealed before MPs break for the summer on June 23. Don Gracey, a partner with the CG Group, which is lobbying the federal

government on behalf of a prospective producer of marijuana, was among the people who said this is true, as did another person who has been in discussions with the government on this matter but asked not to be identified."Anne McLellan has been appointed the chair of this task force," said Mr. Gracey, whose client Georgian Bay Biomed is in the process of building a production facility in Collingwood, Ont., initially planned for medicinal marijuana but which will now also be used for recreational pot. "We understand that the provinces have been asked for and have submitted, I guess what could be categorized as, nominees for provincial representation on the task force." Hill Times

* **Colorado pot retailer advises province on weed**
One of Colorado's largest marijuana retailers says that provinces legalizing pot must educate the public on potency and put in place rules on packaging from the outset. It was a message that liquor board heads and government officials from across the country heard at a private gathering in Saint Andrews last week. The chief information and security officer of Denver's The Green Solution, Nick Speidell, spoke at the conference quietly hosted by New Brunswick's Department of Public Safety in preparation for the sale, distribution and regulation of pot - now that Ottawa is moving toward legalization. Speidell told the Telegraph-Journal in an interview that he spoke on "the good and the bad" of the development of recreational marijuana in Colorado. The state is one of a few U.S. jurisdictions that have already legalized the sale and recreational use of cannabis products. "Colorado was the beta," said Speidell, whose family owned and operated recreational and medical dispensary, boasts the largest selection of marijuana and marijuana-infused products with 11 locations in and around Denver. "We had to learn some lessons, but if you follow some of the best practices and the case studies out here you won't have to make those same mistakes." Speidell's words were directed primarily at edibles - marijuana baked into brownies, cakes, chocolate bars and candy, among other forms - that are becoming a popular alternative to smoking cannabis. Times & Transcript, A10 (New Brunswick Telegraph-Journal)

PUBLIC SERVICE / FONCTION PUBLIQUE

PM to meet young public servants
Prime Minister Justin Trudeau will meet Monday with about 100 public servants, all under age 35, to discuss how their generation will influence policy and change the way the bureaucracy works. Trudeau, also the minister of youth, will be joined by his top bureaucrat, Privy Council Clerk Michael Wernick and Treasury Board president Scott Brison - both of whom have indicated the public service needs a rapid infusion of young blood and new leadership to take over from baby boomers and deliver on the Liberals' agenda. That discussion will be an interactive town hall, which every public servant across the country can watch online, to kick offthis year's National Public Service Week and address the widening generational gulf the Liberals are trying to manage. The annual pat-on-the-back for Canada's 250,000 public servants lost its lustre under the Conservative government. It was during public service week when former Treasury Board president Tony Clement put public servants on notice that he was targeting their sick leave and all but accused them of being malingerers. The lunches and awards to celebrate the work of public servants continued, but the unions boycotted. Last year, the week turned political when the large unions launched pre-election campaigns to get rid of the Conservatives and restore public services. That's all changed with the Liberals. Scientists are unmuzzled, public servants are going to conferences, and diplomats can talk again. The long-form census is back, ministers say they want policy advice and Brison is repealing legislation to restore the old rules for collective bargaining. Not all unions are boycotting this year, but the giant Public Service Alliance of Canada is because of the slow pace of negotiations and the Liberals' failure to "respect public servants." Ottawa Citizen, A5

* **Time to empower next generation of public servants, says Canada's top bureaucrat**
As the annual Public Service Week gets underway today, Canada's top bureaucrat says there's a clear focus this year on empowering the next generation inside the federal bureaucracy. In fact, the Clerk of the Privy Council, Michael Wernick, will lead a virtual town hall Monday morning aimed specifically at young bureaucrats. "I'm pushing for a theme of engaging with our younger cohorts, because this issue of generational renewal is important to me." said Wernick, who himself was headhunted into the federal government 35 years ago this month. Over those decades, Wernick said he has witnessed the many ebbs and flows of the federal government's relationship with its workers. There have "already [been]

changes in tone, for sure" under Prime Minister Justin Trudeau, said Wernick, the man who gave him his current job.(...) Ray Paquette, who works at Public Services and Procurement Canada and is on the negotiating team for the Professional Institute of the Public Service (PIPSC), said the Liberals have made some changes - but not nearly enough. "We have a big problem. The science community is still being muzzled, not being able to openly discuss projects that they're on, [and that] would benefit the people of Canada," he said. "The federal government is still holding them back from being able to do their job properly." (...)Debi Daviau, the president of PIPSC, said at a rally in Ottawa on Friday there's a simple solution to helping the government deliver, and it includes building the right environment. "There was a very difficult and toxic environment created over the past nine years. And from my perspective, something needs to come from the top if they're going to have the capacity to deliver the commitments of this government," said Daviau. CBC News

OTHER / AUTRE

*** Robert Hall, Canadian hostage, executed by Philippine militants Abu Sayyef**
A Canadian man being held hostage by a militant group in the Philippines has been killed. The extremist group Abu Sayyef had warned it would kill Robert Hall today if a multi-million dollar ransom wasn't paid. Sources close to the situation in Jolo, the island where the al-Qaeda-linked group is based, and within Philippine security, confirmed Hall's death early Monday to CBC News. Hall, who was from Calgary, had been held since Sept. 21, 2015 - one of four hostages that included former mining executive and fellow Canadian John Ridsdel, who was killed by the group in late April. Ridsdel and Hall were abducted from a seaside resort along with a Filipino woman and a Norwegian man. An official announcement is expected shortly. The condition of the remaining hostages is not known. CBC News; Globe and Mail; Agence France-Presse (EuroNews)

'There's blood everywhere'
It had been an evening of drinking, dancing and drag shows. After hours of revelry, the party-goers crowding the gay nightclub known as the Pulse took their last sips before the place closed. That's when authorities say Omar Mateen emerged, carrying an AR-15 and spraying the helpless crowd with bullets. Witnesses said he fired relentlessly - 20 rounds, 40, then 50 and more. In such tight quarters, the bullets could hardly miss. He shot at police. He took hostages. When the gunfire finally stopped, 50 people were dead and dozens critically wounded in the deadliest mass shooting in modern U.S. history. Mateen, who authorities said had pledged allegiance to Islamic State in a 911 call shortly before the attack, died in a battle with SWAT team members. Authorities immediately began investigating whether the assault was an act of terrorism and probing the background of Mateen, a 29-year-old American citizen from Fort Pierce, Florida, who had worked as a security guard. At least 53 people were hospitalized, most in critical condition, officials said. A surgeon at Orlando Regional Medical Center said the death toll was likely to climb. "There's blood everywhere," Orlando Mayor Buddy Dyer said. The gunman's father recalled that his son recently got angry when he saw two men kissing in Miami and said that might be related to the assault. Mateen's ex-wife said his family was from Afghanistan but that her ex-husband was born in New York. His family later moved to Florida. A law enforcement official said the gunman made a 911 call from the club in which he professed allegiance to the leader of the Islamic State, Abu Bakr al-Baghdadi. (...) "I am deeply shocked and saddened to learn today so many people have been killed and injured following a mass shooting in Orlando, Florida. While authorities are still investigating and details continue to be confirmed, it is appalling that as many as 50 lives may have been lost to this domestic terror attack targeting the LGBTQ2 community." Prime Minister Justin Trudeau, in a statement. Associated Press (The Guardian, B10); Le Devoir; Canadian Press (Waterloo Region Record); Canadian Press (National Post); Toronto Star; La Presse (2016-06-12)

*** Calgarians show solidarity and vow to take on hate**
Calgarians gathered by the hundreds Sunday night in solidarity with the victims of the worst mass shooting in U.S. history. The attack, which targeted a crowded gay nightclub in Orlando, Fla. , early Sunday morning, left 50 dead and as many wounded. The Olympic Plaza vigil was more noise than silence. The crowd of about 500 people cheered to celebrate the LGBTQ community and made noise to make it known they needed to be strong in the face of hatred. (...) Alberta's premier said she was

repulsed and outraged by "the hatred that fuelled this crime," and she extended thoughts and prayers to the victims and their loved ones "who are suffering this moment." "And we resolve to make sense of these senseless events by re-committing ourselves to building communities where love and solidarity triumph over hatred and division," Notley said in a statement. Calgary Muslim groups condemned the "barbaric" attacks in Florida as they asked people of all faiths to "stand together" and "unite against terrorism and extremism." "Terrorists and extremists want to divide us but we refuse to be divided," Muslims Against Terrorism and the Islamic Supreme Council of Canada said in a release. "We demand that Daesh (ISIS) and its sympathizers should be brought to justice." Calgary Sun, A6

*** L'Iran condamne la décision d'un tribunal canadien**

L'Iran a condamné samedi la décision d'un tribunal canadien de saisir 13 millions de dollars d'actifs non-diplomatiques du gouvernement iranien au profit de familles de victimes d'attentats coordonnés par Téhéran et perpétrés par le Hamas et le Hezbollah, selon la justice canadienne. Le jugement, obtenu vendredi par l'AFP, exige que les familles d'Américains décédés dans huit attentats -- perpétrés entre 1983 et 2002 -- reçoivent les propriétés et les comptes bancaires détenus par le gouvernement iranien au Canada en guise de dédommagements. Le porte-parole du ministère iranien des Affaires étrangères, Hossein Jaber Ansari, a dénoncé cette décision, la jugeant " contraire aux engagements internationaux du gouvernement canadien ", selon l'agence officielle iranienne Irna. " Elle est également contraire aux affirmations du nouveau gouvernement canadien pour normaliser les relations entre les deux pays ", a ajouté M. Jaber Ansari. " Toute normalisation des relations diplomatiques entre les deux pays nécessite une révision des politiques extrémistes et erronées du gouvernement canadien. " Selon les médias canadiens, ces actifs appartenant au gouvernement iranien totaliseraient environ 13 millions de dollars canadiens. Cette poursuite a été déposée au Canada en vertu d'une nouvelle loi, adoptée en 2012, qui permet aux victimes et à leurs familles d'obtenir des dommages et intérêts saisis auprès d'États soutenant des actes considérés comme terroriste. L'Iran est ainsi considéré par le Canada. Agence France-Presse (Le Devoir, B2)

*** Canada needs to probe war crimes in Afghanistan**

An opinion piece states, "Justin Trudeau was only a backbench opposition MP during the Afghan detainee scandal, and spoke just once in Question Period about allegations of Canadian complicity in acts of torture. But what he said on Nov. 29, 2009, was insightful: "We need to get at the truth. The international reputation of Canada and our military is at stake." Trudeau was responding to a story broken by the Star in May 2007, which grew into a scandal that ultimately led to the prorogation of Parliament in December 2009. As one detainee told reporter Rosie DiManno, "They whipped me with rubber hoses. Another time, they used a chain to hang me from the ceiling, my head toward the floor." The same detainee said Canadian officials visited the prison operated by the Afghan National Directorate of Security (NDS), but were never allowed to speak with prisoners. As the late James Travers wrote, also in this newspaper, the story was part of a "long march into twilight" for Canada. The country that "gave the world Lester Pearson's peacekeeping and Brian Mulroney's stand against apartheid" now had to struggle "with Stephen Harper's apparent blindness to compelling evidence of Afghanistan prisoner abuse." (...)Three months later, the Afghanistan Independent Human Rights Commission estimated that "one in three prisoners handed over by Canadians are beaten or even tortured." In March 2007, the U.S. State Department reported that: "Complaints of serious human rights violations committed by representatives of national security institutions, including arbitrary arrest, unconfirmed reports of torture, and illegal detention were numerous."(...) Six years have passed since Justin Trudeau spoke from the backbenches about Afghan detainees. Now, as prime minister, he can put his insight into action. Nothing would do more to strengthen Canada's reputation as a progressive and principled country than investigating possible war crimes by our own soldiers and officials. Nothing would do more to help Canada win a UN Security Council seat. We need to get at the truth, and we need to do so now." Toronto Star, A15

INTERNATIONAL

*** Police had previously interviewed gunman**

The gunman suspected of killing 50 people at a gay Florida nightclub, Omar Mateen, a 29-year-old American, was a person of interest to authorities in 2013 and again in 2014. The FBI says agents twice investigated the man, but closed those cases after interviewing him. FBI agent Ronald Hopper said Sunday that Mateen had been interviewed in 2013 and 2014. Hopper said agents first investigated Mateen after he made inflammatory comments to co-workers alleging possible ties to terrorists. Mateen was interviewed twice and, when investigators were unable to verify the details of his comments, the FBI closed the probe. In 2014, the agency looked into potential ties connecting Mateen to Moner Mohammad Abusalha, the first American to carry out a suicide attack in Syria. Like Mateen, Abusalha lived in Fort Pierce, Florida. Hopper says agents determined that contact was minimal and did not constitute a substantive relationship or a threat at that time. The FBI says he referred to the Islamic State of Iraq and the Levant (ISIL) in a 911 call before the slayings. Mateen's ex-wife, who spoke to the Washington Post on the condition of anonymity, said his family was from Afghanistan but that her ex-husband was born in New York. His family later moved to Port St. Lucie, Fla., where he worked as a security guard. CBS News Justice and Homeland Security correspondent Jeff Pegues reported that an ISIL-related Twitter account has an alleged photograph of Mateen. Pegues also reported that Mateen pledged allegiance to the ISIL at some point. Postmedia Network (Windsor Star, NP3, StarPhoenix, Vancouver Sun, Ottawa Citizen, National Post, Leader-Post, Edmonton Journal, Montreal Gazette, London Free Press, Calgary Herald); The Province; Globe and Mail; Associated Press (Acadie Nouvelle); Toronto Star; La Presse (La Tribune); TVA Nouvelles

*** Daesh, style US**

Ce qui ajoute à l'horreur, c'est qu'on est déjà programmé. On s'attend au pire. On ne sait pas quand, ni où, on ne veut pas vraiment le savoir, mais on sait que ça arrivera. On entre déjà en mode statistique. On compare les chiffres des tués et des blessés. « Ça » quoi, au fait ? On n'avait pas encore identifié les corps qu'il fallait choisir son camp : une autre manifestation du terrorisme islamiste ou une autre tuerie de masse américaine ? C'est les deux, évidemment. La force du groupe État islamique est qu'il s'adapte aux terrains, dans sa guerre. Il peut former des combattants hyper-organisés ou inspirer des individus qui agissent seuls en son nom. Des commandos d'Européens venus dans ses camps qui retournent faire des assassinats coordonnés de type militaire, comme à Paris, à Tunis ou à Bruxelles. Ou un couple comme celui de San Bernardino, qui s'en va descendre 14 collègues dans un party de Noël en Californie, et qui le fait au nom du groupe État islamique. Ou un type (apparemment) seul comme hier. L'ex-femme d'Omar Mateen a dit au Washington Post qu'il était violent, pas vraiment religieux et surtout instable psychologiquement. C'est possible. Ça n'en fait pas moins un candidat excellent. Qu'il tue dans une attaque coordonnée avec un commando ou qu'il tue tout seul, ça change beaucoup de choses dans l'enquête. Ça ne change rien au résultat. Il n'en a pas moins tué 50 personnes au nom du même commanditaire. On n'en sait pas assez long sur l'état mental de Mateen. Mais quoi qu'il en soit, on ne peut pas mettre sur le compte des seuls troubles mentaux un massacre aussi ciblé. Un discours homophobe violent est bien incrusté dans certaines branches de l'islam. La Presse+, 6

*** Time running out to find EgyptAir black boxes**

Egyptian investigators say time is running out in the search for the black boxes from an EgyptAir plane that crashed into the Mediterranean last month, killing all 66 people on board. In a statement Sunday, they say that searches by ships in the area will intensify, given that only around five days remain before the batteries of the flight's data and cockpit voice recorders expire and they stop emitting signals. The boxes could reveal whether a mechanical fault, a hijacking or a bomb caused the disaster. Finding them without the signals is possible but more difficult. Since the plane disappeared from radar en route to Cairo from Paris, only small pieces of debris and human remains have been retrieved from the crash site. No group has claimed an attack. Daily Gleaner, B1

*** One of Lebanon's biggest banks targeted by blast**

A powerful bomb in Beirut destroyed several cars, severely damaged one of Lebanon's biggest banks and injured one person on Sunday. The state-run National News Agency said the bomb was placed under a car. Lebanese Interior Minister Nohad Machnouk, speaking to the private LBC station, confirmed the report but did not say whether anyone was deliberately targeted by the blast, which shook nearby buildings. Associated Press (Toronto Star, A12)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
June 14, 2016 / le 14 juin 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Des changements à venir sous peu, promet le PLC
Le drame d'Orlando a une fois de plus relancé le débat sur le contrôle des armes à feu aux États-Unis, mais aussi au Canada. Si les libéraux de Justin Trudeau ne se sont pas engagés à restaurer un registre, ils ont promis d'annuler certains assouplissements apportés par le précédent gouvernement. Ils ne sont pas encore passés à l'action, mais promettent que c'est pour bientôt. ***« Nous travaillons très fort à la mise en oeuvre des propositions incluses dans notre plateforme***, a assuré lundi le **ministre de la Sécurité publique**, **Ralph Goodale**. ***Nous irons de l'avant avec les changements que nous avons suggérés à ce qui était connu comme le projet de loi C-42. »*** C-42 est ce projet de loi conservateur qui a modifié les règles régissant le transport des armes à autorisation restreinte telles que le AR-15 dont s'est servi le tueur d'Orlando ou des armes prohibées. Désormais, un propriétaire peut transporter son arme n'importe où sur le territoire, pas seulement de son domicile à son centre de tir attitré. Les libéraux ont aussi promis d'obliger les acheteurs d'armes à présenter leur permis de possession au moment de la transaction, et les vendeurs, à en vérifier la validité. La Loi sur les armes à feu stipule plutôt, à l'heure actuelle, que le vendeur ne doit avoir « aucun motif de croire » que l'acheteur n'a pas de permis. (…) Les partis d'opposition se sont offusqués d'une pétition parrainée par le député conservateur Bob Zimmer

demandant que le AR-15 soit retiré de la liste des armes à autorisation restreinte au Canada. (…) Le **ministre Goodale** a rappelé que, sous son gouvernement, le pouvoir de classifier les armes est retourné entre les mains des fonctionnaires. ***« Je n'ai reçu aucun avis de la GRC suggérant des changements »,*** a-t-il soutenu. Le Devoir, A3; Journal de Montréal

Tory MP backed petition for easing access to AR-15s
A Conservative MP sponsored a petition last month calling on the federal government to loosen controls around the rifle used in Sunday's mass shooting in Orlando. Bob Zimmer presented the petition in the House of Commons on May 13. The petition, which garnered more than 25,000 signatures, asks the **Public Safety Minister** to reclassify the AR-15 semi-automatic rifle and return it to non-restricted status. "We, the undersigned, lawful firearm owners of Canada, request (or call upon) the **minister of public safety and emergency preparedness** to reclassify the Armalite Rifle-15 back to nonrestricted status so we can once again use this rifle to lawfully participate in the Canadian cultural practices of hunting," the petition reads. Such rifles have been used in a number of mass shootings in the United States, including the attack on a gay nightclub in Orlando early Sunday morning. The AR-15 is capable of spraying dozens of rounds from a single magazine. Speaking in the House last month, Mr. Zimmer said he was "honoured" to present the petition. Globe and Mail, A10

Premier pushes cybersecurity agenda in Ottawa
Premier Brian Gallant says he's asked the federal government to set up its cybersecurity infrastructure in New Brunswick as the province attempts to carve out a new niche as a centre of excellence in the emerging industry. Gallant was in Ottawa on Monday in his role as minister responsible for innovation - a position created by the current Liberal government. The premier met with federal Innovation, Science and Economic Development Minister Navdeep Bains, as part of larger meetings with provincial and territorial counterparts responsible for economic development and innovation. Gallant then met with **Public Safety and Emergency Preparedness Minister Ralph Goodale**. The meetings come as the province attempts to grow its tech sector. "I made it very clear to the **minister** that one of the best things that government could do is actually set up some of their cybersecurity shops in New Brunswick," Gallant said. "They have a lot of cybersecurity within the defence sector or whether it's their IT sector, so we certainly believe that Fredericton, New Brunswick, and especially with [Canadian Forces Base] Gagetown we have a lot to offer. "This would very much further help develop the cluster that we have in cybersecurity [and] would allow for a lot of synergies and collaboration." He added: "I made that pitch to the **minister**." Telegraph-Journal, A1 (Times & Transcript, Daily Gleaner)

* **Canada's Government announces Passenger Protect Inquiries Office**
The **Honourable Ralph Goodale, Minister of Public Safety and Emergency Preparedness**, announced that Canada is launching a new Passenger Protect Inquiries Office (PPIO). As a first step, the Government has created the PPIO to assist travelers who have experienced difficulties related to aviation security lists.This is part of the Government's plans to introduce a domestic redress system to better deal with false name matches against Canada's Secure Air Travel Act (SATA) list under the Passenger Protect Program (PPP). The SATA list identifies individuals who are suspected of posing a threat to transportation security and/or who are attempting to travel by air to commit certain terrorism offences. Unfortunately, innocent individuals who have the same or similar names as individuals on the SATA list or the U.S. No-Fly list can sometimes be delayed in obtaining a boarding pass as a result of false name matches.A redress system will allow individuals whose names closely match those on the SATA list to apply for a unique identification number. They could use this number at the time of a ticket purchase to clear their name in advance and prevent delays at airports. To put this new system in place, important regulatory and data system changes are required. While those changes are underway, it may still take more than 18 months before they can be fully implemented. (…)***"Eliminating false positives in airport security screening is complex, but we are committed to a long-term solution through a domestic redress system. As we work towards that goal, we are taking steps to problem-solve and help those who have been affected, while at same time ensuring that aviation security remains strong and effective in keeping Canadians safe,"*** said **Ralph Goodale**, **Minister of Public Safety and Emergency Preparedness**. Travel Daily News

* **Fixing Surveillance Starts with Spy Agencies Coming Clean**

An opinion piece states, "Three years ago this month, Edward Snowden shocked the world with a series of disclosures that revealed a myriad of U.S. government-backed surveillance programs. The Snowden revelations sparked a global debate over how to best strike the balance between privacy and security and led to demands for greater telecom transparency. The initial Canadian response to the surveillance debate was muted at best. Many Canadians assumed that the Snowden disclosures were largely about U.S. activities. That raised concerns about Canadian data being caught within the U.S. surveillance dragnet, but it did not necessarily implicate the Canadian government in the activities. Within months, it became clear that Canadian securities agencies were enthusiastic participants in numerous surveillance initiatives. Canadians played a lead role in projects focused on tracking travellers using airport Wi-Fi networks, monitoring millions of daily uploads and downloads to online storage sites, aggregating millions of emails sent by Canadians to government officials, and targeting mobile phones and app stores to implant spyware. Moreover, the U.S. collection and mining of "metadata" -- the data about data that covers geographic information and details about social links -- was also at the heart of Canadian activities with a ministerial authorization granting officials the power to capture the potentially sensitive personal information with minimal oversight. While these programs attracted attention for a day or two, it was the Conservatives' introduction of Bill C-51, the anti-terrorism legislation that granted the government a host of new powers, that finally succeeded in generating a sustained focus on Canadian surveillance law. The bill became law with few amendments, but emerged as the public's shorthand for the need for reforms to surveillance activities. **Public Safety Minister Ralph Goodale** and the new Liberal government have promised changes, with expectations that they will focus initially on a new "super" oversight body for security agencies and later open the door to further amendments." The Tyee

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Wildfire no longer growing**
The huge wildfire known as "The Beast" that tore through parts of Fort McMurray and northeastern Alberta is classified as being held for the first time since it became out of control in early May. Wildfire information officer Lynn Daina said the designation means the fire is no longer growing, but is not yet under control. Daina said it's an important day for firefighters who have been battling the blaze for weeks. "It is a big deal. It is like the happy dance day," she said Monday. "There has been so much and so many people on this fire - more than 2,000 at its peak working it daily." The perimeter of the fire, including burned areas, covers just under 5,900 square kilometres. Daina said the work of firefighters combined with recent rainy weather and high humidity checked the fire's growth. The Regional Municipality of Wood Buffalo estimates that about half of the more than 80,000 people who fled the Fort McMurray area on May 3 are back in the community after being allowed to return this month. Canadian Press (Red Deer Advocate, A5; Charlottetown Guardian; St. John's Telegram; Times and Transcript); Globe and Mail

*** Fort McMurray mental health services deal with hundreds of calls per day in wake of wildfire**
Ask people in Fort McMurray to describe the city's character and a common theme emerges. "We're a pretty resilient bunch," business leader Mike Allen says. "There has been a calm," says homeowner Robert Hodder. "Tough as they come," adds oilsands worker Kristen Thomas. Around the city, municipal leaders will proudly announce there is no place more prepared in Canada to deal with a disaster. Safety is a way of life for the blue-collar workforce, locals said. People know how to handle adversity. Yet for all the truth in Fort McMurray's hardy reputation, it's also clear the recent wildfire has taken its toll on the emotions and the psyche. Since the evacuation of the city early last month, Alberta Health Services has received more than 8,700 contacts from people seeking some form of mental health support -- an average of about 225 per day. Ottawa Sun (Toronto Sun; Winnipeg Sun; Calgary Sun; Edmonton Sun; Edmonton Journal

*** Début des livraisons de gaz naturel liquéfié**
Gaz Métro, Stornoway et le gouvernement du Québec ont annoncé lundi le début de l'approvisionnement en gaz naturel liquéfié à la mine de diamant Renard, de Stornoway, dans le Nord-du-Québec. La mine de Stornoway est située à plus de 1000 kilomètres de Montréal. Le gaz naturel liquéfié y sera acheminé par camion. Pour les fins du projet, les partenaires envisagent quelque 800 camions par année - ce qui

semble avoir été bien reçu par les communautés concernées. Patrick Godin, vice-président et chef de l'exploitation chez Stornoway, a fait un parallèle avec la tragédie de Lac-Mégantic, qui a été déclenchée par le transport de pétrole par train. «Le transport du gaz naturel liquéfié offre des opportunités beaucoup plus sécuritaires et, sur de longues distances chez nous, je peux vous dire qu'avec notre partenaire Gaz Métro, lorsqu'on a eu à développer l'acceptabilité sociale de notre projet, tous les maires "impactés", les services d'incendie étaient excessivement heureux de voir leur village traversés par du gaz naturel liquéfié au lieu de le voir avec des énergies comme du diesel», a-t-il dit. Le transport de gaz naturel liquéfié par train n'y serait pas possible, de toute façon, puisque la voie ferrée ne se rend pas aussi loin que la mine Renard, a noté M. Godin. Presse canadienne (Le Quotidien, 18)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Couple who tried to bomb legislature were 'lone-wolf terrorists'**
Some of John Nuttall's plots might have seemed impractical but that's how "lone-wolf terrorists" operate - they start with "crazy ideas" and then settle on one, the Crown told an entrapment hearing Monday. The Crown portrayed Mr. Nuttall and his wife, who were convicted last year in a plot to bomb the B.C. Legislature, as willing terrorists who were not entrapped by undercover police. But the judge on Monday questioned the couple's intellectual capacity - at one point citing an incident in which they tried to mentally will themselves to forget a person's name. Mr. Nuttall and Amanda Korody were found guilty last June of conspiring to murder persons unknown and making or possessing an explosive substance - in both cases for the benefit of or at the direction of a terrorist group. They were arrested on Canada Day, 2013, after they placed potentially explosive pressurecooker devices outside the government building. (…) Prosecutor Peter Eccles told the court Mr. Nuttall and Ms. Korody "planned and committed these terrorist crimes of their own free will" and were not pushed into it by anyone. "They did it because they wanted to," he said. Mr. Eccles said the RCMP had solid grounds to begin investigating Mr. Nuttall. He said a man Mr. Nuttall met at a mosque in 2011 called police and told them Mr. Nuttall had been talking about fighting a holy war in Afghanistan. Mr. Nuttall and his wife had recently converted to Islam. The Canadian Security Intelligence Service also contacted the RCMP in early 2013 to inform them Mr. Nuttall had been attempting to purchase potassium nitrate, which can be used in explosives. Mr. Nuttall's counsel has said that information was not corroborated and argued that while police may have had reasonable suspicion to begin their investigation, it should have become clear Mr. Nuttall was not engaged in terrorist activity and was "all talk." Lawyers for Mr. Nuttall and Ms. Korody have said their clients were isolated and impoverished, rarely venturing far from the Surrey basement suite where they lived. But Mr. Eccles said a person can be radicalized online and does not need a large circle to commit a terrorist act. Globe and Mail, S1; Vancouver Sun, A4 (The Province)

*** La surveillance policière a ses limites**
D'Orlando à Boston, en passant par Saint-Jean-sur-Richelieu ou Paris, le même scénario : celui d'attentats dont les auteurs ont déjà attiré l'attention des milieux policiers, mais qui réussissent néanmoins à passer aux actes. Un constat d'échec des services de renseignement? Non, répondent différents experts. Les médias américains soulignaient tous lundi que le FBI avait déjà eu à l'oeil Omar Mateen, l'auteur de la tuerie d'Orlando. Il avait d'abord été repéré à la suite de propos inquiétants tenus lorsqu'il était garde de sécurité dans un tribunal. Selon ce que précisait lundi matin le directeur du FBI, James Comey, l'enquête du FBI avait alors duré 10 mois, période pendant laquelle son nom est resté dans le fichier des personnes à surveiller. (…) C'est là un problème bien concret des agences de renseignement, note Dave Charland, analyste des questions de sécurité nationale -- et ancien agent de renseignement au Service canadien du renseignement de sécurité (SCRS) : avoir des informations, mais pas suffisamment pour aller plus loin. (…) Pour le grand patron de la Gendarmerie royale du Canada (GRC), Bob Paulson, la tuerie d'Orlando rappelle surtout que la prévention d'attaques par des loups solitaires représente un grand " défi ". Il a d'ailleurs rappelé lundi que la GRC enquêtait sur Couture-Rouleau lorsqu'il a tué un soldat à Saint-Jean. " J'aime penser que les structures que nous avons actuellement sont robustes et que la coordination entre les différentes agences gouvernementales est bonne [pour assurer de pouvoir] intervenir de manière préventive. " Le Devoir, A3

*** Des loups à la fois solitaires et solidaires**

La stratégie des combattants islamistes qui consistait à recruter des sympathisants pour venir leur prêter main-forte sur le théâtre de luttes armées appartient au passé, explique Ray Boisvert, ancien directeur adjoint du Service canadien du renseignement de sécurité (SCRS). " C'est al-Qaïda qui a commencé cela pour diminuer la pression sur les combattants. Ils ont dit : "Ne venez plus. Restez chez vous. Faites quelque chose chez vous." C'était une stratégie pour enlever de la pression sur eux. Et ç'a fonctionné. " Tandis que les regards se retournent sur la scène intérieure, " la pression est soulagée ", au moins symboliquement. Le loup solitaire est " celui qui n'a pas reçu d'ordre formel ", explique Sami Aoun, professeur à l'Université de Sherbrooke et cofondateur de l'Observatoire sur la radicalisation et l'extrémisme violent. " La détermination de la cible et le timing, c'est lui. D'ordinaire, il ne délibère pas au préalable. Il se prépare seul. " Dans la plupart des cas, il s'avère plus difficile d'anticiper son action que celle d'un groupe. (...) Les succès des loups solitaires n'en restent pas moins notables. " Ils ont eu du succès avec ça. Dès la première édition d'Inspire, c'était le ton : "Prenez un pick-up F-150, soudez des lames de métal devant et lancez-vous dans une rue de piétons en attendant qu'on vienne vous tuer." A Victoria, le couple qui voulait faire exploser des bombes lors de la fête du Canada, John Nuttall et Amanda Korody, c'était ça. Les attentats de Boston, la même chose. " A la hache, avec des bombes artisanales, à l'arme de chasse ou au fusil d'assaut, tout est bon pourvu que l'action surgisse de manière à surprendre et à frapper l'imaginaire. Plusieurs documents largement disponibles en ligne donnent des idées pour procéder. Et les relais numériques ne manquent pas. " Ils en arrivent à obtenir les mêmes conseils " de plusieurs sources différentes, dit Ray Boisvert. Le Devoir, A2

*** Le SPVM se dit bien préparé en cas d'attaques comme à Orlando**

Il est impossible d'être entièrement prêts à faire face à un massacre comme celui d'Orlando, mais les policiers de Montréal sont bien formés pour réagir, assure un grand patron du Service de police de la Ville de Montréal (SPVM). «Le réflexe est là», explique le directeur adjoint Fady Dagher. «Depuis la fusillade à Dawson, tous nos policiers de première ligne passent à travers une formation en situation de tireur actif», ajoute-t-il. En octobre 2015, une simulation de grande envergure s'est déroulée à plusieurs endroits à Montréal dans le but de préparer les forces policières à des situations multiples comme celles survenues lors des attentats de Paris. «Les policiers ont dû réagir dans une situation de tireur actif dans les rues du centre-ville de Montréal pendant que dans l'île Sainte-Hélène se déroulait une situation de prise d'otages à la bombe chimique dans un autobus.» Il ajoute que 80 policiers ont récemment été formés afin de reconnaître les comportements de radicalisation pouvant mener à la violence. La Presse

*** Muslims say shooter 'hijacked' their religion**

The Ahmadiyya Muslim Jama'at's motto is "Love for all, hatred for none," and the Islamic movement's imam reiterated that in an interview. "It's not only 50 people that are killed, it's an attack on humanity at large," Khalid Minhas said (gunman Omar Mateen was the 50th fatality). Once again, community members feel as though their religion has been "hijacked," misused and misquoted, he said of the attack and the perpetrator's proclaimed association with the faith. "Such acts of terrorism have no place in Islam," Minhas said. Shamoon Rashid, president of the Saskatoon North branch of Ahmadiyya Muslim Jamaat, said everyone has a right to different views, but it doesn't mean people should be treated differently. "The Quran teaches us that the killing of one innocent person is as if you have killed the whole of humanity," Rashid said. The Ahmadiyya community proactively combats radicalization through community outreach and strives to create a place of belonging for youth. This helps eliminate radicalization at its roots, said Noman Hassan, a spokesman for the group. Daniel Kuhlen, chair of the Islamic Association of Saskatchewan (Saskatoon) media and outreach committee, noted it is the second week of Ramadan, the month that is supposed to represent peace. "It is just astounding for those who observe Ramadan to have to wake up one morning to realize that someone has perpetrated such a heinous crime, such a terrible act of violence during what is the holiest month of the year for Muslims." Both extremism and phobia-driven politics only serve to divide communities, Kuhlen said. "It weakens the social bond between us." StarPhoenix, A3

*** De nouveaux panneaux sensibiliseront les utilisateurs**

Le gouvernement fédéral espère que ses nouveaux panneaux affichant l'inscription « Drones interdits » éloigneront les opérateurs de ces aéronefs sans pilote à bord des aéroports et du trafic aérien commercial en général. Le ministre fédéral des Transports Marc Garneau a dévoilé les panneaux lors d'une conférence de presse, lundi, à l'aéroport d'Ottawa. Cette mesure est annoncée dans le cadre de la

campagne de sensibilisation nationale sur la sécurité alors que le gouvernement s'apprête à proposer une nouvelle réglementation sur l'utilisation des drones - qui prévoira de nouvelles catégories, un processus d'enregistrement simplifié et de nouvelles exigences de marquage. M. Garneau a souligné qu'il était important que les utilisateurs sachent comment faire voler leurs appareils de façon sécuritaire et légale. Presse canadienne (Le Quotidien, 18)

*** What inspires atrocity?**

An editorial by Wesley Wark, expert on terrorism and national security, states, "The massacre at a nightclub in Orlando, frequented by the LGBT community, was another heartbreak for both the community and an American society riven by gun violence and fearful of terrorism. The violent rampage by 29-year-old Omar Mateen, armed with an assault rifle and other weaponry, is bound to cause further deep-seated confusion about the distinctions between terror attacks and other varieties of hate crimes. We have seen this confusion in Canada around the October 2014 attack on Parliament Hill and the Moncton shooting of five RCMP officers in June 2014. Unfortunately, in the world of ISIL-inspired acts, the distinction between terrorism and hate crime vanishes. Just how deeply Mateen was motivated by the ISIL cause remains to be seen and will be a vital part of the now launched FBI investigation(...) Whatever the outcome of investigations into Mateen's background, attack planning, ISIL links, and motivations; whatever we learn about the depth or shallowness of his jihadist connections; whatever we learn about his personal beliefs and mental health, the terrible truth is that terror, hate crime and mental illness all merge in the violent world of ISIL. It is driven by apocalyptic sectarianism, something never before seen in a transnational jihadist terror organization." Ottawa Citizen, A9

*** Orlando was a publicity stunt**

An editorial states, "Forty-nine peaceful clients of a gay nightclub in Orlando, Florida were shot dead and another 53 wounded early Sunday by a terrorist loyal to so-called Islamic State. The city of Orlando had a horrific day. LGBTTQ* folks around the world were reminded of the hatred and mortal danger that stalks them. Wielding a legal AR-15 semi-automatic rifle and a handgun, a 29-year-old American-born Muslim, opened fire at the crowded Pulse Orlando club early Sunday. He was killed in a gun battle with police. Meanwhile, U.S. authorities at the White House and the Federal Bureau of Investigation say the killer was a "homegrown extremist" who espoused support for both Islamic State and Hezbollah. Meanwhile, Islamic State radio called the shooter Omar Matten "one of the soldiers of the caliphate in America." The radio station hailed the attack. (...) Canada has suffered similar attacks and may easily suffer more. One Canadian soldier died and another was wounded when an IS sympathizer drove a car at them in a shopping centre parking lot at St Jean, Quebec in October, 2014. A couple of days later a Montreal drug addict killed an army reservist on guard duty at the national war memorial in Ottawa and then ran into the Centre Block of Parliament where he was shot and killed. Canada mourned its dead and moved on. The damage to the nation went no further. Islamic State appears to rely on these attacks as a way of recruiting new sympathizers to its cause and Canadian police have been keeping a close eye on Canadians who show signs of IS sympathies that could lead to overt acts of terrorism. This is the prudent thing to do, though the Orlando case shows this method is only useful up to a point. The FBI had received tips about the perpetrator of the Orlando attack, interviewed him three times and then closed the file because they found no grounds for further investigation. Police forces and intelligence agencies should continue refining their techniques. It seems unlikely, however, that they will devise sure ways of recognising who will kill and who will not. (...) The bad news for Americans and Canadians out of the Orlando outrage is that our neighbours include a tiny number of people who are listening to Islamic State propaganda. A few of them may attempt terrible crimes, but we cannot tell who they are or where they will strike. This may go on for many years, because the authors of IS propaganda can probably find a new home after they are driven out of Iraq and Syria. Canada, the United States and nations of western Europe should prepare for the continuation of these types of attacks, but recognize they are limited and its citizens remain relatively secure. These democracies will not be brought to its knees by terrorists. Canadians and their police forces should continue to watch for IS sympathizers who may start collecting weapons and explosives. We should not, however, fear that the nation is at risk." Winnipeg Free Press, Z1

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

'Border Security' TV show canned over privacy violation
Canada's border agency is pulling the plug on the controversial reality TV program "Border Security" after the federal privacy commissioner found the agency violated the rights of a construction worker filmed during a raid in Vancouver. Privacy commissioner Daniel Therrien recently informed the British Columbia Civil Liberties Association, which spearheaded a complaint on behalf of Oscar Mata Duran, that the Canada Border Services Agency breached the Privacy Act by allowing production company Force Four to film the agency's examination of the migrant labourer. "As a matter of principle, it is our view that federal government institutions cannot contract out of their obligations under the Act," says the commissioner's 26-page report of findings. In light of the well-founded complaint, Therrien's office recommended the border agency end its participation in the television program, which the agency agreed to do. Agency spokeswoman Esme Bailey confirmed that "Border Security: Canada's Front Line" would not return for a fourth season. The commissioner also urged the agency to carry out a formal privacy impact assessment before embarking on any significant future initiative involving the use of personal information. Times and Transcripts, B4

Cocaine courier gets nine years
A courier hired to move 30 kilos of cocaine - one load of some 1.3 tonnes a drug shipping network moved through Saskatchewan - is now feeling the weight of a hefty prison term. A first-time convicted offender, Ronald Charles Learning was sentenced Monday to nine years in prison for possession for the purpose of trafficking. With credit for time already served, eight years, 204 days remain, plus an additional 30 days for breaching release conditions. "Mr. Learning, you're serving a significant period of incarceration," Regina Provincial Court Judge Marylynne Beaton said. Peering through the glass of the prisoner's dock, the 33-year-old man originally from Golden, B.C., simply nodded. "He was not acting on his own, but rather was part of a larger criminal organization," Beaton noted. Learning is the last of six men - busted in Canada and the U.S. - sentenced for their role in the mega-smuggling ring that moved cocaine from California to B.C. via the remote Saskatchewan-Montana border. As Beaton summarized, between January 2010 and October 2011, the group was responsible for importing 16, multi-million-dollar cocaine shipments. In turn, the group exported 790,000 ecstasy pills south. Leader-Post, A1

G4S defends employee screening practices
The security company that employed both the Florida nightclub gunman and an armoured car guard who killed three co-workers in Edmonton in 2012 has defended its hiring practices, but says it cannot guarantee employees won't commit violent crimes. Communications director Katie McLeod of the Canadian arm of U.K.-based G4S says the global security company does as much as it can to investigate prospective employees before hiring them, using both government and its own checks to screen them. "In Canada, you must have your provincial security licence before you are even considered for employment and that follows all sorts of processes with the different provincial authorities," McLeod said Monday. "It varies from province to province," she added. Omar Mateen, a G4S employee in Orlando, Fla., has been identified as the gunman who killed 49 people and wounded more than 50 others in an attack early Sunday on a gay nightclub in the city. (...) He fled the shootings with more than $300,000 before being apprehended in British Columbia at the Canada-U.S. border two days later. Canadian Press, A10 (Red Deer Advocate); Associated Press (Telegram, Record, Hamilton Spectator, Edmonton Journal)

Human-trafficking trial opens for Round 2
A second trial opened Monday for a Vancouver man who was found guilty at his first trial of human trafficking after luring his Filipina nanny into coming to Canada. In 2013, a B.C. Supreme Court jury found Franco Orr guilty of three counts under the Immigration and Refugee Protection Act. Orr, the first person in Canada to be convicted under the act's human-trafficking provisions, was sentenced to 18 months in prison. His wife, Nicole Huen, was acquitted of the charges. Orr launched an appeal and in March 2015 a three-judge panel of the B.C. Court of Appeal overturned his convictions and ordered a new trial. The Province, A14; (Vancouver Sun)

*** EWN Special Report: Canadian man thought to be Mbuyisa Makhubu spent 12 years in jail**

Eyewitness News has learnt that a Canadian man, suspected of possibly being June 16 icon Mbuyisa Makhubu, was released from detention after 12 years. Victor Vinnetou appeared before a hearing of the Immigration and Refugee Board of Canada (IRB) after refusing to cooperate with authorities there for over a decade. In 2013, the South African government announced that Vinnetou may be Makhubu, but an initial DNA test proved to be inconclusive. The Canadian Border Services Agency says Vinnetou was in detention for 12 years because it could not confirm his country of origin. Spokesperson Travis O'Brien says, "He was detained under the Immigration and Refugee Protection Act, between 11 August 2004 and 16 January 2016, because his identity could not be determined." Eyewitness News

Deux Américains passeront l'été à l'ombre
Détenus dans une affaire d'importation illégale d'armes à feu, deux Américains arrêtés à la frontière canadienne au début juin passeront l'été au Centre de détention de Sherbrooke. Le Californien Jonathon Bryce Darcangelo et Spencer Truesdell du Texas ont réglé leurs comptes avec la justice à Sherbrooke, puis condamnés à une peine de détention de cinq mois. (…) Défendus par Me Patrick Fréchette, les deux accusés ont présenté des excuses aux autorités canadiennes. La juge Hélène Fabi de la Cour du Québec les a condamnés à cinq mois de prison. Elle a retranché le temps de détention provisoire à la suite de la suggestion commune des avocats au dossier. Il leur reste donc quatre mois et demi de prison à purger. Une interdiction de posséder des armes au Canada pour dix ans a été imposée. Les deux Américains s'étaient retrouvés derrière les barreaux après avoir omis de déclarer leurs armes chargées aux douanes canadiennes. Les deux individus s'étaient vu refuser leur remise en liberté sous conditions. La Tribune, 31

Competition Bureau acted on false info, Moose alleges
A former principal of Moose International Inc., who was manufacturing counterfeit jackets on the side, provided false information to the Competition Bureau that triggered an investigation, it was alleged on Monday. The allegations were contained in Moose International's response to Competition Bureau charges that it falsely advertised premium parkas as made-in-Canada. "In 2015, the Bureau received false information from a former principal of Moose who had, in late 2013 or early 2014, organized and carried out the clandestine manufacture, importation and sale of counterfeit Moose Knuckles jackets (conduct which has resulted in criminal charges against him)," according to the response filed by Moose International on June 10 and made public by the Competition Bureau on Monday. The document does not name the principal or say what the charges were. Moose Knuckles CEO Ayal Twik said the company cannot release any further details as it's a pending legal matter. Acting on the false information, the Bureau requested the Canada Border Services Agency stop certain shipments of Moose jackets so they could be photographed, the document goes on to say. Toronto Star, 59

***SNC Rebounds as Trudeau Readies $95 Billion Canada Building Jolt**
SNC-Lavalin Group Inc., the Canadian construction company that spent decades building roads, smelters and power plants from Alaska to Australia, has its sights on a piece of the C$120 billion ($95 billion) infrastructure spending boom planned in its home country. (…) SNC is among the finalists to build the Gordie Howe International Bridge between Detroit and Windsor, Ontario, which may carry a price tag of more than C$4 billion. It's also in the running for the Toronto area's Finch West light-rail transit system, which is valued at about C$1.2 billion by Yuri Lynk, an analyst at Canaccord Genuity. Bloomberg

CYBER SECURITY / CYBERSÉCURITÉ

***China, US hold talks to bridge cybersecurity differences**
Chinese and American officials said Tuesday they're committed to bridging their differences on cybersecurity and moving to implement recent agreements, as they held talks amid complaints over China-based hacking operations that the U.S. says may have already cost U.S. companies tens of billions of dollars. Repeated meetings between the sides on cybersecurity indicate the seriousness with which the Obama administration regards the issue, the U.S. ambassador to China, Max Baucus, said at the start of the two-day talks in western Beijing. U.S. officials have been particularly eager to build on an agreement forged during Chinese President Xi Jinping's visit to the White House in September that says neither government will support commercial cyber-theft. The deal was viewed by Washington as a diplomatic

breakthrough, although U.S. officials have not conclusively determined that it has led to a decline in hacks against U.S. companies. Associated Press (Yahoo! News)

*** Apple's new file system revolves around encryption**
One of Apple's quietest announcements at WWDC might also be its most important. The company has introduced a brand new file system, simply called Apple File System (APFS) that makes security its centerpiece. It offers a unified encryption method for virtually every device Apple makes, ranging from the Apple Watch to the Mac. That includes multikey encryption, which makes it tough to crack even if you have physical access to the storage. In short, the FBI won't be happy: Encryption is now a core part of the operating system, not just something bolted on after the fact. APFS also acknowledges the advances in technology in the nearly two decades since Apple's current file system, HFS+, hit the scene. It's optimized for flash storage, uses extremely fine-grained time stamps (down to the nanosecond) and supports a whopping 9 quintillion files on a single volume. You'll also see "snapshots" (read-only instances of the file system) that make Time Machine-style backups easier. Engadget

LAW ENFORCEMENT / APPLICATION DE LA LOI

Extremist group kills Canadian hostage as ransom bid fails
As military helicopters chattered across the skies of Jolo Island in pursuit of a trio of kidnapped sailors held in the lawless region of the southern Philippines, negotiators frantically tried to strike a ransom deal ahead of a 3 p.m. Monday deadline. Their failure was made clear on Monday evening, when remains were found outside a Catholic cathedral in Jolo City. The Canadian government said it has compelling reason to believe Canadian Robert Hall was killed. But his death has left behind difficult questions about why a kidnap-for-ransom group would turn down a large offer of money and instead kill a high-value hostage. Among the Canadians seeking Mr. Hall's release, everyone knew how high the stakes were. Eight weeks earlier, the extremist criminal group Abu Sayyaf had beheaded Canadian mining executive John Ridsdel, who was seized together with Mr. Hall and two others from a yacht marina in late September. To prevent the same from happening to Mr. Hall, a Calgary born metalworker, pilot, film actor and adventurer, his family and friends had assembled about $1.4-million to pay a ransom. RCMP officers, federal civil servants from departments such as Public Safety, Global Affairs and Justice, and Canadian Security Intelligence Service agents had all sought to win the hostage's release. (…) In Ottawa, Mr. Trudeau defended his government's refusal to pay ransoms, despite the death of two Canadians on his watch at the hands of extremists in the Philippines. "We will not turn the maple leaf worn with pride by over three million Canadians abroad into a target," Mr. Trudeau said as he mourned Mr. Hall's death. RCMP Commissioner Bob Paulson said the Mounties are pursuing those who killed Mr. Hall and Mr. Ridsdel. "We have been working with the authorities there to try and prevent this tragedy, but it illustrates again the terrorist threat throughout the world, in terms of this terrible kidnap and terrible tragedy." In 2014, the RCMP lured to Canada one of the people who had held journalist Amanda Lindhout captive in Somalia. A spokesman for Foreign Affairs Minister Stéphane Dion said Canada tried its best to free Mr. Hall. Globe and Mail, A1; Red Deer Advocate, A7 (Times Colonist, Daily Gleaner); Globe and Mail

Crown bosses probed over gifts: Report turned over to RCMP
Unnecessary travel on the taxpayer's dime, and gifts of booze, theatre tickets and rounds of golf have resulted in the suspension of three top-level executives at an Alberta Crown corporation, and the dismissal of its entire board. An anonymous tip to government in November sparked an investigation by the province's internal auditor, who examined senior executive expenses at the Agriculture Finance Services Corp. The resulting report has been handed over to the RCMP to investigate whether there was criminal wrongdoing. Suspended with pay are the corporation's president and managing director, Brad Klak; its chief operating officer, Merle Jacobson; and its vice-president of innovation and product development, Wayne McDonald. None of them could be reached for comment. Edmonton Journal, A1 (Calgary Herald)

RCMP officer cleared
A former Red Deer Mountie has been acquitted of charges laid against him in connection with the arrest of a Red Deer teenager in the summer of 2012. Const. Eric Pomerleau, 30, went to trial in Red Deer

provincial court on May 10 and 11 of this year on charges of assault with a weapon, common assault and assault causing bodily harm. The charges were laid after a member of the public accused Pomerleau of using excessive force during the arrest of the boy, whose name is withheld because he was a minor at the time. Judge Marilyn Smith, normally based in Leduc provincial court, heard that Pomerleau had pepper sprayed the youth to subdue him while he was in the back of the police car; pushed him to the floor while taking him to his cell, and bloodied his nose after reentering the cell to conduct a second search. In a decision announced from her courtroom in Leduc on Monday, Smith said she found Pomerleau's actions were reasonable in each of the three incidents, given that Pomerleau had been confronted with an aggressive and combative "client" and that there were no other police officers available to provide backup. She also pointed out that he is both smaller and lighter than the boy he had arrested and was not aware until later that day that he was only 16 years old. Red Deer Advocate, A1; Edmonton Journal

Teen's body recovered in Jervis Inlet

Operators of a Christian retreat say they are doing all they can for the family of a South Korean teenager who drowned while attending the camp north of Vancouver. A post on the website of the Malibu Club Young Life camp thanks the RCMP, coast guard and camp staffwho scoured the waters of the Malibu rapids in Jervis Inlet. Searchers using sonar located the body of the 16-year-old on Friday, two days after he fell into the water. The RCMP has confirmed the body was recovered. The victim was an exchange student attending high school in Idaho, and was at the camp with other students. Vancouver Sun, A4 (Times Colonist)

RCMP head's comments on unionization draw fire

RCMP Comm. Bob Paulson came under fire Monday over his proposal to strip Mounties of the right to bargain essential working conditions as they form the first ever RCMP union. Senators, including two former Mounties, a former Quebec police union head and a labour lawyer, grilled Paulson over Bill C-7, the government's proposal to allow Mounties to unionize within strict parameters. At one point, Sen. Larry Campbell, a former Vancouver RCMP member and the bill's sponsor in the senate, told Paulson his arguments were "ludicrous." The bill excludes from the bargaining table any negotiation over law enforcement techniques, transfers and appointments, performance appraisals, discharges or demotions, conduct including harassment, probation, basic requirements for carrying out a Mountie's or reservist's duties and the uniform or equipment provided to RCMP. In testimony to a senate committee, the country's top cop admitted it was senior RCMP managers who proposed listing the no-go zones in order to be transparent "because we thought in this very acrimonious season of an RCMP union drive there would be criticism that we were trying to pull a fast one." Toronto Star, A7; Canadian Press (Red Deer Advocate, A8, Times & Transcript)

Dartmouth opens clinic for veterans: Mental health facility designed for operational stress injuries first of its kind in N.S.

With veterans returning to Nova Scotia from places like war-torn Afghanistan, over 1,300 Veterans Affairs clients are currently being supported with a disability benefit for a mental health condition in the province, according to federal numbers. A new Dartmouth clinic will be available to treat them, along with the province's portion of Canada's 3,816 RCMP former members and and 1,156 Second World War/Korean War veterans also on disability for operational stress injuries (OSI) such as anxiety disorders, depression and post-traumatic stress disorder (PTSD). The Nova Scotia Operational Stress Injury Clinic is the first of its kind in Nova Scotia. "It's more important today than ever before, given that we're tracking numbers of mental health issues coming back from Afghanistan at quite significant rates," Veterans Affairs Minister Kent Hehr told the Chronicle Herald. Chronicle Herald, A5

Mountie accused of stealing guns

A B.C. Mountie has been charged with theft after two guns, "growing nutrients" and a generator were allegedly taken from an evidence locker. A sergeant with the detachment has been charged with four counts of breach of trust and four counts of theft, RCMP said Monday. The sergeant's name was not released. Canadian Press, A4; Vancouver Sun

Online scam targets newcomers, says Winnipeg man who lost nearly $5000

A recent Red River College grad, originally from Hong Kong, is out nearly $5000 after falling victim to an elaborate online job scam. "I'm emotionally hurt because when I know people here are so friendly, and then [someone] uses your trust to scam you, that hurt me so much," said Bart Cheng. Cheng recently finished the business administration program at the college and thought he was accepting an administrative assistant's job with a construction company that was setting up shop in Winnipeg. Cheng says he found the job on the Workopolis job posting site in May. The ad was for a position at an unnamed company, which he contacted through email. A phone interview followed shortly after. (...)Cheng says he fell for the scam because they used legitimate businesses to make it appear as though the job was real. He also feels that the scam targets newcomers to Canada who are eager to find work and aren't familiar with Canadian business practices. (...)The company's CFO, says it has no affiliation with Kiwi Construction or any job posting being advertised as such. He said the company has reached out to both RCMP and WPS. The Winnipeg Police say they are investigating this incident but say that people should always be skeptical when it comes to exchanging information online, especially when that exchange involves the transfer of money. CBC News (2016-06-13)

New Glasgow police search clubhouse after Hells Angels welcome home party
The raid of a Gate Keepers clubhouse in New Glasgow that began the morning after a Hells Angels welcome home party in Musquodoboit Harbour stretched into a second day Monday with police combing the property from top to bottom. The MacLean Street location was the target of search warrant by RCMP, who were armed and had a perimeter set up for more than 24 hours. They arrived at 6:30 a.m. Sunday and remained there even though no arrests were made. RCMP spokesman Const. Mark Skinner offered little information. "All I can say is this is part of an ongoing investigation," he said. He wouldn't draw a connection between the raid and the reported patching in of a number of Gate Keepers as hangaround members of the Hells Angels. "We can confirm this was a Gate Keepers location, but we really can't release any more information at this time about the investigation," he said. The Hells Angels had their party Saturday night, and there has been speculation it might signal a permanent return of the biker club to the area. They have maintained influence through Darksider and Gate Keeper presence in the province. Chronicle Herald; Cape Breton Post (2016-06-13)

Pride Toronto will have more security but not more uniformed police officers
Plans are in the works to increase security for Pride Toronto, but organizers say they do not want more uniformed police officers patrolling Pride events and Toronto police say they understand the concern. Citing the "challenging relationship" some members of the LGBT community have with police, Pride Toronto Executive Director Mathieu Chantelois said an increased presence of uniformed officers is "not ideal." "We have to consider that many marginalized groups of our community have a very challenging relationship with police. So for us the solution is a very sophisticated plan. It's definitely not to just double the amount of police in uniforms," Chantelois said on Monday after meeting with Toronto Police, the RCMP and staff from the Prime Minister's office. Chantelois said the plan to not increase the number of uniformed officers was made mutually with Toronto police, the RCMP and the Prime Minister's Office, which took part in a Pride security review meeting because Justin Trudeau will march in the parade. CBC News (2016-06-13); * Globe and Mail; * Canadian Press (Daily Gleaner)

Tuerie d'Orlando : vaste rassemblement à la mémoire des victimes à Moncton
Plus de 200 personnes se sont rassemblées au parc Riverain de Moncton, au Nouveau-Brunswick, pour rendre hommage aux victimes de la tuerie d'Orlando. Des membres de la communauté LGBT de Moncton ont convié la population à ce grand rassemblement pour pleurer les 49 victimes du tueur, aider à guérir une profonde tristesse, partager des craintes et trouver une forme de réconfort en groupe. « On est tellement soulagé de voir autant de gens appuyer la communauté et les victimes d'Orlando. On fait du bien pour la terre. Il y a des gens partout dans le monde qui se rassemblent comme nous l'avons fait ici et c'est extraordinaire que Moncton contribue à ce mouvement-là », a déclaré le coordonnateur aux relations publiques de l'organisme Rivière de fierté du Grand Moncton, Charles MacDougall. (...)Par ailleurs, un membre de la GRC était présent sur les lieux, ce qui a surpris quelques participants. Ce dernier circulait en périphérie afin d'assurer la sécurité. Les organisateurs affirment ne pas avoir invité la GRC et que ces derniers se sont présentés de leur propre chef. « La GRC était bien gentille, elle restait autour, mais ça créait quand même une ambiance de "ils sont ici". Quand tu vois la GRC, tu réalises que

oui, peut-être qu'il peut se passer quelque chose, mais on ne peut pas vivre dans la peur », soutient Jason McGraw. Radio-Canada (2016-06-13)

Missing teen Montana Disbrowe could be in Winnipeg, RCMP say
Family of a Montana Disbrowe are worried for her well-being, Gimli RCMP say. The missing 17-year-old last contacted her family June 10. She is 5-foot-3 and weighs about 120 pounds. RCMP believe she could be in Winnipeg. Anyone with information that could help investigators is asked to contact Gimli RCMP at 204-642-5106 or Manitoba Crime Stoppers anonymously at 1-800-222-8477. CBC News

Shooting sparks gun laws debate
Every mass shooting in the United States carries another round of political rhetoric regarding gun ownership. While many gun owners cite their right to keep and bear arms as being fundamental to their American citizenship, this line of reasoning does not hold water in Canada. Here, "it's a privilege and not a right," Prince Albert Pistol and Rifle Club member James Brake said, clarifying that gun laws between our two countries are vastly different. It's not perfect in Canada, but it's better, he summarized. During the early morning hours of Sunday, a lone gunman opened fire on an Orlando, Florida, nightclub, killing at least 49 people and injuring 53. The gunman's weapon of choice was an AR semi-automatic rifle similar to a piece the Prince Albert Pistol and Rifle Club shot targets with during a recent open house at their gun range west of Prince Albert. In Canada, AR style rifles -- and any piece outside of regular hunting firearms -- are considered "restricted." Restricted weapons are not as easy to obtain in Canada as they are in the United States, Brake explained. Prince Albert Daily Herald (2016-06-13)

*** Killer's rifle very restricted here**
The semi-automatic rifle used in Sunday's deadly mass shooting in Florida is classified as a restricted weapon in Canada and most people can only use it at a gun range. The AR-15 is a civilian model of the M16 rifle used by the U.S. army and has been used to carry out other mass slayings in the past, including the 2012 killing of 20 children in Newtown, Conn. One of the top-selling rifles in the U.S., the AR-15 is also popular in Canada, according to Ontario provincial police. But while purchasing one doesn't require a licence in Florida, anyone looking to buy one here must have a firearms licence that includes restricted weapons, which involves passing two one-day safety courses. RCMP note that they need "a minimum of 45 days" to process an application. The form includes questions about the applicant's mental and emotional health and an RCMP report said 112 applications were denied last year due to mental health concerns. Authorities can request that someone provide information from their doctor to confirm they are not at risk to themselves or others if police have recorded an incident related to mental health, but privacy legislation makes it otherwise difficult to seek that information, another RCMP report said. "Considering almost three-quarters of the firearm deaths across Canada are attributable to suicide, there is little progress being made in developing better links with the mental health community as far as reporting obligations," said the 2010 report, an evaluation of the Canadian Firearms Program. "The exception being with the province of Quebec ... where more workable arrangements have been made with the mental health services to report on persons of risk." Canadian Press, A5 (Hamilton Spectator); La Tribune

*** Damage claims from RCMP's High River gun grab total $2.3 million**
The long arm of the law has nothing on the big boots of a police force overstepping its mandate to serve and protect. Now, thanks to the dogged persistence of an ex-Mountie and former National Firearms Association director working out of his Airdrie home, we know exactly how much damage those police boots caused, as RCMP kicked in thousands of High River doors in a massive gun seizure since condemned as a shameful abuse of power. "They shouldn't have been inside the homes at all, not even one," says Dennis Young, the former RCMP officer and firearms advocate that's been a massive thorn in the side of his former force, ever since the great flood of 2013, and the great gun grab that followed. "In all, 2,210 homes were left damaged by the RCMP, and they should not have gone into those homes in the first place. People's rights were violated, and that not only upsets me as a former member, I've heard from many RCMP veterans who are upset as well." Young's latest poke at the police force publicly rebuked last year for harming public trust through the improper seizure of 609 firearms from 105 homes, comes via a long list of numbers, all with a dollar sign attached. As Young says, the High River Mounties used the flood and evacuation of the town three years ago this month as an excuse to search most of High River's more than 4,000 homes, kicking in the doors of more than half. The list Young obtained, after

making a Freedom of Information request, shows at least $2.3 million in claims were paid out by the province to residents in High River as direct result of damage caused by the RCMP, with the average payout per home totalling $1,573. Postmedia Network (Ottawa Sun, Winnipeg Sun, Toronto Sun, Edmonton Sun); Canoe (2016-06-13)

*** High number of impaired drivers in Keswick and Nackawic areas arrested**

RCMP say some drivers still are getting behind the wheel after consuming alcohol. Police officers with the Keswick and Nackawic detachments of the West District RCMP stopped seven impaired drivers between Friday afternoon and early Sunday morning. The RCMP said four of the drivers were arrested for impaired driving, and are expected to face charges. It said three other drivers were issued seven-day licence suspensions for having a blood alcohol level of more than 0.05 but not above 0.08. Cpl. Peter Stubbs of the West District RCMP said some of the people were arrested as a result of police check stops that had been set up over the weekend, while others happened after the police received calls from people who reported drunk drivers. "Our main goal is to let people know that impaired driving is never acceptable and that it's easily preventable." He said anyone who's consuming alcohol or other substances needs to plan a safe way home. He said anyone who suspects a driver is impaired should call 911 immediately. The West District RCMP is focusing on reducing the number of impaired drivers on the road and will continue to carry out regular enforcement to find impaired drivers to ensure the public's safety. Daily Gleaner, A3

*** Innu police demand more funds at inquest**

When someone in Uashat takes his or her own life, a local police officer is often the first person at the scene. The frantic calls for help come directly onto their radio and they rush to a house on the Innu territory - walking past panicked, emotional loved ones before reaching the body of a person who, moments earlier, was still alive. "It takes a toll on us," said Raynald Malec, the chief of police in Uashat and neighbouring Maliotenam. "You often have to hold back relatives, to keep them away from the scene while paramedics and first responders do their work." To help fight the rash of suicides that rocked both Innu communities last year, Uashat's band council says police need better funding to keep up with the demands imposed on their officers. That was the first recommendation that the band council put before the Quebec coroner's office Monday during the public inquest into five suicides in Uashat and Maliotenam last year. (...)The department's $1.66 million budget can't keep up with equipment and training costs, according to police chief Malec. Last year, Malec's officers responded to 16 suicide attempts and 122 incidents of a "mentally perturbed" individual (someone in the throes of a psychiatric crisis that requires urgent intervention). Aboriginal police forces in 396 communities across Canada are financed by the First Nations Policing Program, which splits funding between the federal and provincial jurisdictions. Critics in six aboriginal police departments across Quebec told the Montreal Gazette the program can't keep pace with growing First Nations populations and the needs that come with systematic poverty and overcrowded housing conditions. The difficult nature of Uashat's police interventions requires additional training and resources, Malec said. Montreal Gazette, A4

*** Smith murder case remains open**

After nine long years, an investigation into finding the killer of an 89-year-old Westlock man remains ongoing. While technically considered a historical homicide, RCMP say the investigation into the unsolved murder of Doug Smith is active. “It’s quite a long time, but the investigation into any such matter never stops until we have identified a suspect and determined whether or not there is evidence sufficient for charges,” said RCMP ‘K’ Division strategic communications officer Cpl. Hal Turnbull. “Hopefully for the sake of the family and the community we will be able to identify a suspect or suspects in this particular matter.” It was in the early morning hours of June 14, 2007 when firefighters responded to a house fire at Doug Smith’s 108 Street home. As crews battled the blaze, they found a body inside, which was later confirmed to be Smith’s. The fire was immediately deemed suspicious and a homicide investigation was opened — the cause of death has never been publicly released. “Mr. Smith’s death was ruled suspicious and subsequent investigation from the medical examiner gave us definitely the cause and manner of death,” Turnbull said. Investigators determined a number of firearms and an unknown amount of Canadian and U.S. cash were taken from the home. Smith’s daughter Judy Burns said the family remains hopeful the killer will be brought to justice. Westlock News

*** RCMP focusing on domestic violence, chronic offenders**
An RCMP report before city council earmarked traffic offences, chronic offenders and domestic violence as key priorities for next year. Superintendent Warren Brown's presentation Monday showed a sharp dip in break and enters and assaults in the first five months of this year, compared to the two years previous. This year shows 195 break-ins compared to 269 the year before and 319 assaults, down more than 40 from the year before and following a dropping trend from the high of 403 in 2014. While Brown said this year's numbers for break and enters is better "it's an unacceptable number" Prince George has seen an increase in thefts this year. January to May had 945 files compared to 820 in 2014. Sexual assaults were up slightly from last year at 26 between January and May compared to 18 in 2015 over the same period, down from 2014, when there were 36 in the same time frame. The new domestic violence approach involve a safety plan for families and following up with offenders, Brown said. Prince George Citizen

*** Nanaimo RCMP bust "dumping ground" for stolen property**
RCMP in Nanaimo are sorting through a huge haul of stolen property after two raids on problem houses in that community. Police say the homes became "dumping grounds" for criminals with stolen property. Search warrants were executed on a home on the 700 block of Albert Street in Nanaimo's downtown, and the 400 block of Lambert Street in the University area last Thursday. Cst. Gary O'Brien says police recovered dozens of bikes, electric scooters, televisions and diving equipment as well as some property stolen in a recent rash of break and enters to local schools. "These were homes that were basically collecting spots for material across the city. They were causing a lot of distress to neighbours in the community in general. So what we found were about seven dozen bikes. A lot were disassembled. We found electronics, guitars diving equipment. Some of the material was stolen from the local schools. Unfortunately a lot of that is still outstanding." Five men and a woman between the ages of 21 and 56 were arrested on charges related to the stolen property. CHEK News (2016-06-13)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Harsh prison sentences are harder on women**
An editorial states, "Advocates of harsher criminal sentences commonly invoke the mantra of "truth in sentencing." This turn of phrase is meant to call out the perceived disconnect between the jail term handed down by the justice system and the sentence actually served by an offender. Those who call for "truth in sentencing" want to limit prisoners' eligibility for parole or reduce the time credited to prisoners to offset their time spent behind bars waiting for a trial or a sentencing hearing. So, is there truth in sentencing? No, not at all. There is no truth in sentencing because the criminal justice system does not account for the real, lived experience of time served behind bars. It should come as no surprise that incarceration is experienced differently by different people. Mandatory or prolonged prison sentences work a particular and disproportionate injustice on women. Their impact is harder still on indigenous women, who now appallingly make up over one third of all women in Canada's federal prisons. Tack on any number of intersecting disadvantages - poverty, mental illness, racialization - and the harms are further compounded. Many of us still believe that locking up prisoners and throwing away the key is the only means to a safer society. Yet harsh, one-size-fitsall sentencing comes at a price we collectively cannot afford. It blinds us to the disproportionately severe and harmful impacts of mandatory or prolonged imprisonment on historically disadvantaged groups at our own peril and nowhere is this more apparent than for female offenders. Imprisoned in one of the few prisons for female offenders, a woman will typically serve time far from her home community, leaving her without in-person contact or support from family or friends to aid in her rehabilitation. If she is among the 70 per cent of mothers in federal prison with minor children, her children were likely be apprehended by the state and put into care, severing the bond between mother and child." Province, A18

*** Making a difference by sending kids to camp**
An organization that works to improve the lives ex-cons in the community has another goal: to help kids who have parents who are behind bars, and it does so with its Bar None Camp. But to do so, it's turning to the community for help in the form of a benefit dinner and silent auction later this month. The summer camp, for 80 kids aged 10 to15 who have a mom or dad incarcerated, has been in operation for more than 20 years, says Misty McLaughlin, chief development officer with Bridges of Canada. "It was

recognized that these children didn't have a place to go in the summertime where they could just be kids, away from a stressful home environment where there are issues between Mom and Dad," she says. "A lot of times, [it's] addictions and substance abuse, then add in the fact that one parent is incarcerated, and it doubles the stress." Bridges of Canada founder Monty Lewis worked with inmates from Dorchester Penitentiary to build some of the cabins that are still on site at the camp. "His heart was to open this camp up in Boiestown and have it as a place that kids could come and be kids, and it's free of charge," says McLaughlin. "So all the money we raise on an annual basis goes directly to the operation of the camp." Lewis died in 2013, and up to that point, Bar None was a fun summer camp. It still is, McLaughlin says, but now they have implemented therapeutic community concepts. Daily Gleaner, C1

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Gays at increased risk of violence, stats show

Not only was Sunday's attack on the Pulse nightclub in Orlando the worst mass shooting in U.S. history, it was the deadliest single act of violence perpetrated against gays in modern history. Gay venues have been bombed, set on fire and even targeted by mass shootings before, but the death toll has never come close to the 49 killed at Pulse. What the Orlando attack brings home is that, even in an era of full legal equality and revolutionary HIV treatments, North American gays and lesbians are still disproportionately at risk of suffering a violent or premature death. "Acceptance of the LGBT community has not been universal and violence ... persists as a serious issue in the United States," reads a 2014 study sponsored by the U.S. Department of Homeland Security. (...) Among Canadian minority groups, the gay community remains a consistent target of random violence. In 2013, for instance, Canadian police recorded 186 hate crimes motivated by sexual orientation. Crimes against the LGBTQ community were only onefifth of the Canadian total, but are consistently more brutal. "These hate crimes were more likely to be violent than hate crimes targeting other groups," noted a Statistics Canada summary. Postmedia Network (Vancouver Sun, N4, Leader-Post, Ottawa Citizen, National Post, Edmonton Journal); Calgary Herald

*** Stats show handful commit over half of crimes in Sask**

A new Statistics Canada report shows that a small handful of Saskatchewan people are responsible for a disproportionate amount of crime in the province. The study tracked Saskatchewan offenders over a three-year period starting in 2009 and found that 21 per cent of accused individuals were responsible for more than half of the crimes. According to one of the lead researchers on the project, that is likely because the further along a person moves in the criminal justice system - from being questioned by police to getting arrested to appearing in court and serving a sentence - the more likely he or she is to reoffend. "The further you move through the system, the more likely it is you will have repeated contact with the justice system, particularly if you are an aboriginal person or a young person," said Shannon Brennan, a senior analyst with Statistics Canada. Brennan said the research shows that someone who only has contact with police but does not have to go to court or is not sentenced to any jail time is far less likely to be a repeat offender. On the other hand, those who are repeatedly sentenced to jail or probation are far more likely to reoffend and end up being sentenced again. In real numbers that means a small group - only 7,800 of the 37,054 people who came into contact with the Saskatchewan justice system in 2009-10 - were responsible for 57 per cent of all crimes committed in the province. StarPhoenix, A4 (Leader-Post)

Toronto police services board may overhaul TAVIS unit, sources say

Toronto's Police Services Board may be planning to overhaul a community policing unit set up 10 years ago to decrease violence and increase safety in high crime areas, sources have told CBC News. The police services board, which meets Friday, is expected to make an announcement about the future of TAVIS, the Toronto Anti-Violence Intervention Strategy. Sources said the unit could be renamed and made more community friendly in an effort to cut costs. TAVIS police program has dedicated funding cut. TAVIS, which was created in 2006, had its annual provincial funding cut nearly in half last September. The ministry of community safety and correctional services cut its budget from $5 million to $2.6 million, a cut that took effect at the beginning of this year. Community leaders say what is needed is appropriate, not extra, policing. They say TAVIS has created tension between police and residents of neighbourhoods where the unit has been deployed. There have been concerns about carding in areas where TAVIS was

working. Toronto Police Association President Mike McCormack said TAVIS has made a difference. "TAVIS is a unit that has been very effective, very efficient as far as surge policing is concerned, responding to different hot spots throughout the GTA. They have done some amazing work as far as reduction of crime and providing public safety." McCormack said the question remains what kind of resources the city will make available for crime prevention. CBC News

*** Gun amnesty program will actually save lives**

An opinion piece states, "It is unfortunate that the idea of a new gun surrender program has been envisioned and articulated by Councillor Giorgio Mammoliti in such a way that it has been met with derision and skepticism because to me, as a criminal defence lawyer, it is a very good idea. Anyone who finds such a concept that involves paying criminals to surrender firearms repugnant may not realize the Toronto Police Service already pays tens - if not hundreds - of thousands of dollars annually to criminals to inform upon illegal gun possessors. In fact, paying underworld informants is the main police weapon against illegal gun possession. Unfortunately, it is also an economically inefficient, unreliable weapon that causes tremendous collateral damage. It works like this: police offer individuals entrenched in the criminal subculture money (or, in some cases, a "walk" on outstanding charges) to tell them who has a gun and the place he or she keeps it. The outlay of taxpayer dollars to the criminal informant, however, is only the first expense required to remove a particular firearm off the streets. Dwarfing the initial outlay to the informant are the costs of the investigation to attempt to confirm some criminal aspect of the informant information - a prerequisite for a search warrant - the execution of the warrant, and the detention and prosecution of the alleged possessor. The dollar cost of the seizure of a gun through the search warrant process can be measured. What cannot be measured is the societal cost of the execution of search warrants where the informant has lied or been mistaken. The police are not required to publish how many times their affidavits sworn in support of search warrants applications proved to be inaccurate or untruthful, but my office gets multiple calls each week from people complaining their doors were smashed in, their homes ransacked and their children traumatized by the police and nothing illegal was alleged to be found. It is a devastatingly alienating experience." Toronto Star, A13

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

*** Ministers, indigenous representatives gather**

Ministers responsible for indigenous affairs in the territories and provinces, and leaders from national indigenous organizations met with the federal minister of Indigenous and Northern Affairs in Ottawa Friday to discuss how governments can improve the quality of life for indigenous peoples in Canada, and advance the process of reconciliation. The Federal, Provincial and Territorial Indigenous Forum, which will happen annually, replaces the Aboriginal Affairs Working Group. The major difference is that the federal government is now actively involved. Deputy premier Elaine Taylor was present on behalf of the Yukon, and called the meeting "historic," because it was the first time the federal government was at the table with ministers from the provinces and territories in charge of indigenous affairs in their respective jurisdictions. "Now the feds have come to the table, so this is an opportunity to really engage with Canada on issues important to indigenous peoples and all Canadians," said Taylor. The primary focus of the FPTIF is to find ways to close the socio-economic gaps between indigenous and non-indigenous peoples. This means reducing the number of indigenous children in the child welfare system, bringing down rates of poverty, improving the delivery of health services, and preventing violence against indigenous women and girls. The group discussed the Truth and Reconciliation Commission's 94 Calls to Action, which aim to redress harms caused by the legacy of the residential school system, and the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP), which Canada officially adopted last month. Under UNDRIP, governments are required to secure "free, prior and informed consent," for natural resource development on traditional territories. The group also agreed to work together on the National Inquiry of Missing and Murdered Indigenous Women and Girls. "The national inquiry that the federal government has committed to proceeding with is of utmost importance to Canada and of great importance to the Yukon," said Taylor, who has been in charge of this file as minister responsible for the Women's Directorate. Whitehorse Daily Star, 3 (2016-06-13)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Feds reject NDP motion to decriminalize marijuana for personal use
The federal Liberal government has no plans to decriminalize marijuana before legalizing it, Attorney General Jody Wilson-Raybould said Monday. "It would mean that marijuana would remain an illegal substance and that it would continue to be grown and distributed by organized crime networks," Wilson-Raybould told the House of Commons. "Canadians, both adults and youth, would continue to purchase a product of unknown potency and quality while fuelling the profits of organized crime." She said the Liberals would therefore not be supporting an NDP motion urging the federal government to immediately decriminalize simple possession of marijuana. Prime Minister Justin Trudeau campaigned on a promise to legalize, regulate and restrict access to marijuana, and his government plans to introduce legislation next spring. But New Democrat MP Murray Rankin said that could take two years to come into effect, leaving many Canadians at risk of criminal records for something the government doesn't believe should be a crime. The Guardian, A8 (Cape Breton Post, Telegram, National Post)

* **Marijuana producer eager to expand: Awaits legalization of recreational pot**
The politicking goes on in Ottawa about how and when to legalize recreational marijuana use. Meanwhile, existing licensed medical marijuana producers continue to operate within a costly compliance environment, and are forced to grapple with the challenges of being left outside of the mainstream of the capital markets. The industry is looking toward a massive increase in demand when recreational use is legalized, but its ability to scale up in anticipation of that demand can be challenging. Delta 9 Biotech, the only licensed producer in Manitoba, is a case in point. John Arbuthnot of Delta 9 said the company is on the verge of closing a financing, but has been struggling to come up with the right formula with which to approach investors. Delta 9 has been operating for more than two years, and was one of the original group of 13 producers Health Canada licensed in 2014 (there are now 31, with most of them in Ontario and British Columbia.) Prime Minister Justin Trudeau has promised to legalize marijuana and his government plans to introduce legislation next spring. In the House of Commons Monday, the government said it will not decriminalize it before a task force reports in the spring. It's just more uncertainty for an industry that was forced to invest heavily in security and standard operating procedures in order to comply with Health Canada standards to become licensed. But the ongoing uncertainty continues to create challenges. "Access to capital is difficult," said Arbuthnot, who is still weighing options that may include an initial public offering or a reverse takeover to get a public listing. Winnipeg Free Press, B8

* **Decriminalization of pot nixed**
The federal government will not decriminalize the possession of marijuana until it becomes law - with stringent regulations and restrictions in place, Attorney General Jody Wilson-Raybould said on Monday. "Our government's objectives in doing so are to protect young Canadians by keeping marijuana out of the hands of children and youth," said Wilson-Raybould. "We also want to keep profits out of the hands of criminals, particularly organized crime." The federal attorney general spoke against an Opposition Day motion introduced in Parliament on Monday by NDP justice critic Murray Rankin, who represents Victoria. The bill urges the government to decriminalize possession of personal amounts of pot before it's made legal. Prime Minister Justin Trudeau campaigned on a promise to legalize, regulate and restrict access to marijuana. "You can't have the prime minister announcing it's going to be legalized and then stand up and prosecute it," Rankin said in the House of Commons. "It's a ludicrous situation, ludicrous." The Liberal government says it plans to introduce legislation in the spring of 2017, after it has put together a task force to develop a comprehensive regime for controlling the safe production, distribution and consumption of cannabis products across Canada. "This task force will be set up very shortly and will have an ambitious timeline so that it can inform the government on its progress and complete its review in a timely and responsible way," Wilson-Raybould said. Decriminalizing possession of marijuana without ensuring the appropriate controls are in place would be giving a green light to dealers and criminal organizations to sell marijuana to Canadians, especially children and youth, she argued. Times Colonist, A5

PUBLIC SERVICE / FONCTION PUBLIQUE

Des experts examineront l'aide fédérale aux sciences
Le gouvernement Trudeau a annoncé, lundi, la création d'un groupe de travail pour faire l'examen des programmes fédéraux de soutien aux sciences fondamentales. Le Conseil consultatif pour l'examen du soutien fédéral à la recherche fondamentale sera chargé de faire des recommandations d'ici à la fin 2016 à la ministre fédérale des Sciences, Kirsty Duncan, pour améliorer les programmes axés sur les sciences. Le groupe formé de neuf experts sera présidé par le Dr David Naylor, ancien recteur de l'Université de Toronto, et compte parmi ses membres Art McDonald, ancien directeur de l'Observatoire de neutrinos de Sudbury et titulaire d'un prix Nobel, Rémi Quirion, scientifique en chef du Québec, et Robert Birgeneau, ancien chancelier de l'Université de la Californie. En plus de recueillir les commentaires du milieu de la recherche, le groupe devra analyser les pratiques exemplaires internationales touchant le financement de la science, et examinera les obstacles qui empêchent les jeunes chercheurs d'atteindre leurs objectifs de carrière et ce qui doit être fait pour les éliminer. Le milieu scientifique a connu des années difficiles pendant le règne du gouvernement Harper. Une campagne nationale en faveur de la science publique, menée par le principal syndicat des scientifiques, l'Institut professionnel de la fonction publique (IPFPC), a attiré l'attention à l'échelle nationale et internationale. Lors de la dernière campagne électorale, les libéraux avaient promis de redonner toute sa place à la science publique, et promis de mettre fin au musèlement des scientifiques fédéraux. Dans le cadre des présentes négociations, l'IPFPC demande la reconnaissance de l'intégrité scientifique dans la convention collective des scientifiques fédéraux. Le Droit, 9

Deux syndicats, deux strategies
Les deux principaux syndicats de la fonction publique ont décidé de stratégie différente, cette année, dans le cadre de la Semaine nationale de la fonction publique, qui a pris son envol lundi. Pendant que l'Alliance de la fonction publique du Canada (AFPC) invite ses membres à boycotter encore une fois les activités organisées par le gouvernement, l'Institut professionnel de la fonction publique du Canada (IPFPC) incite plutôt les siens à participer aux activités organisées par leur employeur en arborant des articles de visibilité appuyant les équipes de négociations. Pour la présidente de l'AFPC, Robyn Benson, le boycottage est encore nécessaire en raison de la lenteur des négociations. «Le gouvernement libéral n'a pas tenu parole, a-t-elle indiqué par voix de communiqué. Il avait pourtant promis de réparer les ponts avec les fonctionnaires et de faire preuve de respect envers eux. Compte tenu des négociations qui piétinent et de l'incertitude qui pèse sur les relations de travail, nous contestons la pertinence des activités qu'organise l'employeur à l'occasion de la Semaine de la fonction publique.» (…) Pour sa part, l'IPFPC a décidé de ne pas boycotter la Semaine cette année, afin de profiter de la fenêtre qui s'est ouverte avec l'arrivée du gouvernement libéral. La présidente de l'Institut professionnel, Debi Daviault, estime qu'il s'agit du «moment idéal» pour ses membres de montrer leur appui à leurs équipes de négociation, «pour que les choses bougent à la table de négociation». Les négociations doivent reprendre mardi et mercredi pour certaines équipes de l'Institut professionnel. (…) Lundi, le premier ministre Justin Trudeau a lancé la Semaine nationale de la fonction publique en participant à une rencontre avec de jeunes fonctionnaires fédéraux. Dans une déclaration, il a aussi salué le travail et le dévouement des fonctionnaires fédéraux en insistant sur l'importance de travailler dans «un milieu de travail sain, […] dynamique, stimulant et attirant». Le Droit, 9

Ottawa working on pay delays
A federal government spokesman says it is working to ensure that its employees receive accurate and timely pay after some workers in Sydney complaints of delays receiving their final pay and records of employment. Some casual employees with Immigration, Refugees and Citizenship Canada's office in Sydney said last week that more than a month after finishing their most recent stints there, they are still awaiting their final pay and haven't received their records of employment. In response to questions posed by the Cape Breton Post, Jean-François Létourneau, spokesman for Public Services and Procurement Canada, said in an email it is "working closely with all departments and agencies, to ensure that employee data is appropriately entered" into human resource systems and the Phoenix pay system. "We fully appreciate the challenges employees face any time pay is affected," Létourneau wrote. Among the steps that have been taken include hiring Phoenix experts on-site and online to answer questions from human resources advisers, and the pay centre has hired new compensation adviser trainees who have

started processing cases and "50 additional temporary resources" have been hired to answer calls. The workers who spoke with the Post indicated they believe the delays are being caused at the federal government's pay centre in Miramichi, N.B., which they have had difficulty reaching by phone. The Public Service Alliance of Canada, which represents many federal employees, issued a news release in April calling on the government to fix the relatively new Phoenix pay system. It blamed insufficient staff, training and what it believed to be flaws in the Phoenix system in preventing pay centre workers from ensuring people are paid accurately and on time. Cape Breton Post, A3

OTHER / AUTRE

Canada mourns slain hostage

Canada is mourning with the family of a Canadian man killed by a militant group in the Philippines, Prime Minister Justin Trudeau said Monday. Trudeau said Philippines President Benigno Aquino has offered his condolences and regrets over the murder of Robert Hall, who had been held hostage by Abu Sayyaf since September 2015. The prime minister praised Hall's family. "The Hall family has shown great strength of character in their resilience and are admirable in the face of this terrible situation," he said. "This is a grievous loss for them and their country mourns with them." The government is still seeking formal confirmation of Hall's death, Trudeau said during a brief news conference in the foyer of the House of Commons. However, "we have every reason to believe that the reports are unfortunately true." He said Canada holds Abu Sayyaf fully responsible for Hall's death. "We are more committed than ever to working with the government of the Philippines and international partners to pursue those responsible for these heinous acts and bring them to justice, however long it takes." He called terrorism "a scourge on the world." "Too many families have endured the unspeakable grief the Hall family is feeling today because of these senseless acts of hatred." "On behalf of them and all Canadians, we mourn their loss and reassert our resolve." (...) Trudeau has steadfastly refused to entertain the thought of paying ransom to hostage takers. He said after learning of Ridsdel's execution that Canada would never pay a ransom for the hostages in the Philippines and last month he persuaded leaders of the other G7 countries to reiterate their opposition to paying ransoms. Today, he repeated that paying ransoms would put more Canadians in danger. "Canada cannot and will not pay ransoms to terrorists," he said. "We will not turn the Maple Leaf worn with pride by over three million Canadians abroad into targets." Interim Conservative Leader Rona Ambrose also expressed shock and outrage at the news of Hall's execution. "The threat of radical and barbaric acts of terrorism remains very real. Canada is not immune to the danger presented by global terror networks," she said in a statement. Canadian Press (The Guardian, A8, Cape Breton Post, The Telegram, Times Colonist, Whitehorse Daily Star); * Presse canadienne (Voix de l'Est, Le Nouvelliste, Le Quotidien, La Tribune, Le Soleil, La Presse+); * Presse canadienne (Le Quotidien); * Le Devoir; * Journal de Montréal

*** Not paying ransom the right thing to do**

Justin Trudeau looked as pensive as Canadians have yet seen him, as he announced that a second hostage, Robert Hall, had been killed by his captors in the Philippines. The prime minister and many staff were working on only a few hours of sleep and, in the words of one senior staffer, were "emotionally devastated" by the outcome. The fatigue was likely compounded by a sense of guilt. After all, Hall's unimaginably grisly fate was sealed by the Canadian government's refusal to pay a ransom to the terrorist group, Abu Sayyaf. "We will not turn the Maple Leaf, worn with pride by over three million Canadians abroad, into targets," Trudeau said. It does not seem as if Hall and his friend John Ridsdel, and Norwegian Kjartan Sekkingstad and Filipino Teresita Flor, were targeted by Abu Sayyaf militants because of their nationality. (...) The real problem for Canadians unfortunate enough to be kidnapped abroad is not the no-ransom policy - it's the failure of successive governments to invest in the capacity to project this country's power beyond its borders. "Security is like an insurance policy - you get the coverage you pay for. And in Canada's case, we don't pay a lot," said Christian Leuprecht, a terrorism expert at Queen's University. Our intelligence and diplomatic capabilities in much of the world, particularly southeast Asia are limited. The decision by governments of all stripes not spend the $500 million necessary to set up a foreign intelligence service means that we rely on the goodwill of allies, whose priorities may not always dovetail with our own. "We don't have our own networks on the ground and once people have been kidnapped, it's too late," said Leuprecht. Canada has shown an increased interest in pursuing

extraterritorial prosecutions, such as in the case of Ali Omar Ader, who is accused of being one of the main negotiators in the 2008 kidnapping of Canadian journalist, Amanda Lindhout, in Somalia. Ader was lured to Canada by the RCMP with the offer of a book deal and arrested on landing. National Post, A6

*** So now what?**
An editorial states, "In what has already been a terrible week comes news that a second Canadian, Robert Hall, has been murdered by members of an Islamist criminal organization in the Philippines. Like the people slaughtered in Orlando, Mr. Hall must not be forgotten, and his death must lead to action to prevent further such tragedies. The thing is, what can Ottawa and the authorities in countries where kidnappers operate with near impunity do to stop this from happening again? Prime Minister Justin Trudeau's solution has been to state repeatedly that his government does not pay ransom to terrorists holding Canadians hostage. He first announced the policy after another Canadian, John Ridsdel, was murdered by the same Philippines-based thugs in April. His statement came as something of a surprise, as there was clear evidence that Ottawa had paid or facilitated ransoms in the past to other kidnappers in other countries. (...) There is little doubt that Mr. Trudeau is right that the citizens of a government that pays ransoms are more likely to be targeted. But Mr. Hall's killing is evidence that some Islamist kidnappers simply don't care; that they will grab anyone and, if they don't get the money they want, happily kill them. It is a game of chicken, and the pressure to blink will be greater on Mr. Trudeau than it ever will be on the terrorists. If Mr. Trudeau intends to uphold his no-ransom policy, he will have to demonstrate to the public that there is a viable alternative to that of helplessly watching as Canadian hostages are killed. He has vowed that Ottawa will work with the Philippine government to bring the killers to justice, "however long it takes." Show us some results, Mr. Trudeau, or your talk will look cheap." Globe and Mail, A12

*** Concordia community urges Iran to free academic**
Bring Homa home. That is the urgent message from colleagues at Concordia University and around the world as pressure mounts to secure the release of Concordia University professor emerita Homa Hoodfar, 65, who has been detained in a notorious Iranian prison since last Monday. A week after contact with Hoodfar was cut off, family, colleagues and friends are urging the Canadian government to use whatever means necessary to free the retired academic - who holds Canadian, Iranian and Irish citizenship - from Evin prison. Public pressure is also being exerted, with several petitions demanding to #Free-HomaNow, including one signed by 1,500 academics worldwide. Her friends are haunted by the knowledge that the respected anthropologist and scholar has already endured gruelling conditions since she was first detained in March (although subsequently released on bail), including ninehour interrogation sessions and being ordered to write essays on certain topics. Now they are worried she is sequestered in a prison known for torture, unable to take medication for a neurological illness (Myasthenia Gravis) and fear for her safety in a country with which Canada no longer has diplomatic ties. After being called for another interrogation session last Monday, she was incarcerated in Tehran. The petition by academics says "her academic research seems to have been interpreted as a threat to national security on the basis of her comparative research on women's status, law, development and the family in different Muslim contexts." It's a nightmare, said her niece, Amanda Ghahremani, who is studying international criminal law and describes this experience as a difficult merging of her professional and personal lives. Montreal Gazette, A3

*** MacKay regrets failure to buy Canada fighter jets**
Buying a fighter jet that's different from the one used by Canada's closest allies risks disconnecting the country from the global alliances it needs the most, a former Conservative defence minister said Monday. Peter MacKay told a Senate committee that in his mind, there's no question the Lockheed-Martin F-35 is the right plane for Canada - from defending the Far North to helping to confront the threat of terrorism around the world. MacKay's government tried to purchase that very plane but questions about its costs and capabilities forced a halt to the process - something MacKay said he regrets. "I'm very much lamenting some of the to-ing and fro-ing that's going on currently over the purchase of fighter aircraft," he said. "Do I regret that we did not make the final purchase of that aircraft? Absolutely. We need it, it's good for industry, it's good for interoperability, we need it at Norad." During the election campaign, the Liberals said they would not buy the F-35 and would instead open the process up to a competition. However, cabinet is now grappling with how to meet that commitment and Canada's defence needs at the

same time. "Our government is committed to making sure that we replace the fighters and we will do so and any procurement that takes place with our fighters will benefit Canada and make sure that our industry benefits as well," Defence Minister Harjit Sajjan said. Canadian Press (Red Deer Advocate, A8, Times & Transcript, Times Colonist)

*** Freedom to hate, freedom to kill**

An editorial states, "Once again, the world has witnessed an act of mass murder on American soil, perpetrated by an example of "home grown extremism", in the words of U.S. President Barack Obama. The massacre in Orlando raises a host of issues: gun violence, mental illness, homophobia, religious extremism and terrorism. Coming during Pride month, it strikes at the heart of not only the LGBTQ2S community, but at the fundamental belief that people in free societies have the right to live as they choose, with dignity and respect. Since the attack, we've been learning more about the perpetrator, Omar Mateen. His ex-wife paints a picture of a violent and unpredictable man she fled after only a few months of marriage. While he was an observant Muslim, he never expressed sympathies for radical Islam or terror groups during their relationship. His father has denounced his actions, saying he would have arrested his son himself had he known of his intentions. He claims his son was incensed when he and his three-year-old son saw two men kissing in Miami, and that the massacre may have been in reaction to this incident. At the same time, CBS News has reported that the elder Mateen hosted a television program in which he warned that "God will punish those involved in homosexuality". He also praises the Afghan Taliban, who seek to overthrow the Afghan government and introduce Sharia law, which criminalizes homosexuality. In 2011 and 2012, the younger Mateen made pilgrimages to Saudi Arabia, though it is not clear whom he met on these trips. In 2013, he was questioned by the FBI, and came under surveillance in 2014, due to a possible link with Moner Mohammad Abusalha, the first American suicide bomber in Syria. The FBI closed its inquiry after finding only "minimal contact" between the two men. Was Mateen influenced by his father's views? Was he mentally disturbed? Did he invoke ISIS in his 911 call because he supported them, or as a means of gaining notoriety for his crimes? He left no note, no video, no real explanation for his actions. He did, however, repeatedly voice his hatred for gay men - and it is that prejudice which lies at the root of this nightmare. The sad reality is that, despite thirty-seven years of Pride parades, public education campaigns, legalization of same-sex marriages in many western jurisdictions - and polls that show that seventy per cent of Americans born after 1980 support the institution - there are still young people like Mateen who not only hate, but choose to murder in obedience to that hate. At the same time, it's important to acknowledge that there are forces which *teach* people to hate. Religious extremism is one of those - whether it's in the form of anti-gay edicts from the Catholic Church, or a Canadian politician saying that homosexuals will burn for all eternity in "a lake of fire", or imams preaching that gays and lesbians should be put to death "out of compassion". iPolitics; La Presse (Le Droit); L'actualité (2016-06-13)

*** Terrorisme - Pourquoi les malfrats du monde musulman commettent-ils des attentats?**

Un article d'opinion déclare, « Omar Mateen, le meurtrier présumé des attentats d'Orlando, fut décrit par son ex-conjointe comme étant un mari violent qui la battait et une personne peu religieuse. Les principaux auteurs des attentats de Paris étaient aussi des malfrats : Abdelhamid Abaaoud était un délinquant ayant fait plusieurs séjours en prison et Salah Abdeslam fut décrit comme un consommateur de drogue peu religieux. Plus près de nous, Michael Zehaf-Bibeau était aussi un délinquant avec un historique de consommation de drogue, mais pas d'historique de religiosité. On peut tracer une constante : ce sont des individus n'ayant pas vécu selon les préceptes coraniques, qui, rapidement, passent à l'acte. Les psychologues pourront prendre des grilles d'analyse psychopathologique pour expliquer, mais mon expérience m'indique que c'est plutôt leur système de croyances qui est le moteur de leurs actions et qui explique pourquoi ce sont les malfrats plutôt que les personnes religieuses qui passent à l'acte. Le point de départ pour comprendre leurs actions, c'est leur système de croyances. Il faut entrer directement dans ces croyances pour expliquer leur influence sur les comportements. Ce système commence par les écrits coraniques et je synthétiserai principalement les écrits eschatologiques du monde musulman pour expliquer le soudain retour à la religiosité chez les malfrats. » Le Devoir, A9; Toronto Star

INTERNATIONAL

Double meurtre terroriste en France
Un policier a été tué de plusieurs coups de couteau lundi soir devant son domicile dans les Yvelines, près de Paris, où son agresseur se réclamant du groupe armé État islamique s'est retranché et où sa compagne a ensuite été retrouvée morte. L'assaillant a été abattu par les policiers du Raid, qui ont retrouvé le fils du couple, âgé de trois ans, sain et sauf. Le parquet antiterroriste s'est saisi de l'enquête. Selon des sources concordantes, l'homme s'est revendiqué du groupe djihadiste État islamique (EI) durant les négociations avec le Raid. L'information a été relayée par l'agence Amaq liée au groupe extrémiste, selon le centre américain de surveillance de sites djihadistes SITE. Des témoins ont rapporté aux enquêteurs qu'il aurait crié «Allah akbar » en attaquant le policier. «Toute la lumière sera faite » sur « la nature exacte » de « ce drame abominable », a promis le président français, François Hollande. Agence France-Presse (Le Devoir, A1); * Toronto Star; * Radio-Canada; * TVA Nouvelles

Gunman had 'talked about killing'
He was a body builder and a security guard, a religious man who attended the local mosque and wanted to become a police officer. Early Sunday, 29-year-old Omar Mateen opened fire at a gay nightclub in Orlando. Police said 49 victims died and 53 were wounded. Mateen was also killed. Mateen attended evening prayer services at Fort Pierce's Islamic centre three to four times a week, most recently with his young son, said Imam Syed Shafeeq Rahman. Although he was not very social, he also showed no signs of violence, Rahman said. He last saw Mateen on Friday, he said, two days before the massacre. "When he finished prayer, he would just leave," Rahman told The Associated Press. "He would not socialize with anybody. He would be quiet. He would be very peaceful." He was also bipolar, Mateen's former wife, Sitora Yusufiy, told reporters in Boulder, Colo. (…) Rahman agreed. "My personal opinion is that this has nothing to do with (the Islamic State of Iraq and the Levant)," he said. However, FBI director James Comey said Monday that Mateen had "strong indications of radicalization" and was likely inspired by foreign terrorist organizations. Authorities had immediately begun investigating Sunday's attack as a possible act of terrorism. A law enforcement official said the gunman had made a 911 call from the nightclub professing allegiance to the leader of the Islamic State, Abu Bakr al-Baghdadi. President Barack Obama said Monday that the killer had been inspired by extremist information over the Internet, calling it an apparent example of the "homegrown extremism" that U.S. officials have been fearing for years. Postmedia Network (Windsor Star, N1. StarPhoenix, Vancouver Sun, Leader-Post, Montreal Gazette, Edmonton Journal, Toronto Star, The Province); Associated Press (The Guardian, Whitehorse Daily Star, Cape Breton Post, The Telegram, Cape Breton Post)

* **Shooter cheered for 9/11 hijackers, ex-classmate claims**
At a Florida high school, students saw the horrors of 9/11 unfold on live TV. When the second hijacked airliner slammed into World Trade Center's south tower, the class watched in stunned disbelief. One student, however, "started jumping up and down cheering on the terrorist." That was Omar Mateen, according to one of the accounts from Martin County High School. It offers yet another stitch in the wider tapestry of the man's life and views before Sunday's rampage, which included his pledge of loyalty to the Islamic State of Iraq and the Levant. Robert Zirkle, then a freshman, said Mateen was excited and making fun of how America was being attacked on 9/11. "He was making plane noises on the bus, acting like he was running into a building," Zirkle recalled. "I don't really know if he was doing it cause he was being taught some of that stuff at home or just doing it for attention because he didn't have a lot of friends ... After 9/11 happened, he started changing and acting different." Mateen was suspended or expelled from the school soon after. Washington Post (Windsor Star, N3, Vancouver Sun, StarPhoenix, Ottawa Citizen, Leader-Post, Montreal Gazette, Calgary Herald, National Post, Edmonton Journal)

* **Mateen visited club, used gay dating app**
The gunman who attacked a Florida gay nightclub had attended the club before the attack and had used a gay dating and chat app, witnesses said. Kevin West, a regular at Pulse nightclub, said Omar Mateen messaged him on and off for a year before the shooting using the gay chat and dating app Jack'd. But they never met - until early Sunday morning. West was dropping off a friend at the club when he noticed Mateen - whom he knew by sight but not by name - crossing the street wearing a dark cap and carrying a black cellphone about 1 a.m., an hour before the shooting. "He walked directly past me. I said, 'Hey,' and he turned and said, 'Hey,' " and nodded his head, West said. "I could tell by the eyes." At least four regular customers of Pulse, the nightclub where the massacre took place, told the Orlando Sentinel on

Monday that they believed they had seen Mateen there before. "Sometimes he would go over in the corner and sit and drink by himself, and other times he would get so drunk he was loud and belligerent," said Ty Smith, who also uses the name Aries. He saw Mateen at the club at least a dozen times, he said. "We didn't really talk to him a lot, but I remember him saying things about his dad at times," Smith said. He told us he had a wife and child." As soon as West saw photos released of Mateen after the shooting, he said, he drove to his local police station, where officers summoned FBI officials, who showed him a photo of Mateen on a computer screen. "I said, 'That's him,' " West said, and turned over his phone and Jack'd log-in information to the FBI, which still had the phone late Monday, he said. Toronto Star, A9

*** ISIL is no army and it doesn't speak for Islam**

An opinion piece by Phil Gurski, CEO and president of Borealis Threat and Risk Consulting, states, "As we continue to get more information on the terrorist who killed 49 people and injured even more in Orlando Sunday, we find ourselves yet again in the murky world of "Why?" Why would someone kill dozens of innocent civilians? Why was he not being followed? Why was he able to get a gun given what the FBI knew about him? Why didn't others report his behaviour to authorities? Why are we incapable of getting beyond prayers for the victims and implementing real action that has a chance of preventing future tragedies? In all this maelstrom of information, the inevitable has happened: a terrorist group, Islamic State (ISIL), has claimed responsibility for the attack and Omar Mateen as one of their own. Fuelling this is the fact that Mateen called 911 just before his siege and pledged allegiance to the group (note, however, that allegiance - "bay'a" - is not pledged to an organization but to a person, showing that Mateen was not quite up on terrorist etiquette). Ergo, he was ISIL. Not so fast. Saying you are something does not mean you are. Anyone can pledge allegiance to anything whether or not that person has any real links, ties, relationship or communications with that group. Nothing to date suggests that Mateen had any of the above. He appears, so far, to be a young man inspired by the violent ideology promulgated by ISIL and others. Note that this does not mean he was self-radicalized, that meaningless term which has already been thrown about in this case. He was radicalized through the influence of others. Who those mentors were is impossible to say at this point, although his father's reported support of the Taliban is interesting. We will learn more, undoubtedly, and yet we may never figure out all the twists and turns of this man's path to violence. But back to Islamic State. The terrorist group has praised Mateen's actions and called him a "soldier of Islam." ISIL is quick to take advantage of terrorist acts carried out in its name, and its leadership regularly calls on Muslims to engage in "Nike terrorism": Just do it. No surprise there. Omar Mateen, however, is not a soldier of Islam. He is a terrorist, and a dead one. Islam does not condone the slaughter of innocents. Islam does not throw homosexuals off buildings." Ottawa Citizen, A9; Ottawa Citizen; Ottawa Citizen; StarPhoenix; Toronto Star

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
June 24, 2016 / le 24 juin 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

No plans to move cybersecurity jobs to province
There are no immediate plans to move federal government cybersecurity jobs from Ottawa to New Brunswick, says Beauséjour MP and House leader Dominic LeBlanc - despite a pitch made by Premier Brian Gallant on Parliament Hill last week. But LeBlanc says talks will continue on a role for the federal Liberals with Defence Minister Harjit Sajjan slated to visit New Brunswick later this week. In visiting Ottawa for meetings, Gallant said he asked the federal government to set up its cybersecurity infrastructure in New Brunswick as the province attempts to carve out a new niche as a centre of excellence in the emerging industry. The premier met with federal Innovation, Science and Economic Development Minister Navdeep Bains, as part of larger meetings with provincial and territorial counterparts responsible for economic development and innovation. Gallant then met with **Public Safety Minister Ralph Goodale**. The meetings come as the province attempts to grow its tech sector. "I made it very clear to **the minister** that one of the best things that government could do is actually set up some of their cybersecurity shops in New Brunswick," Gallant said. "They have a lot of cybersecurity within the defence sector or whether it's their IT sector, so we certainly believe that Fredericton, New Brunswick, and especially with [Base] Gagetown we have a lot to offer. "This would very much further help develop

the cluster that we have in cybersecurity [and] would allow for a lot of synergies and collaboration." He added: "I made that pitch to **the minister**." (…) "I was encouraged by the extent to which **Ralph Goodale** was aware of CyberNB, knew about the research that had been done by the University of New Brunswick, and is certainly anxious to see how the government of Canada can become a partner in a centre of excellence," LeBlanc said. LeBlanc said that both he and Gallant spoke to **Goodale** about the example of Israel. Telegraph-Journal, A1 (Times & Transcript, Daily Gleaner)

PM's CSIS oversight plan is, in reality, nearly toothless
An editorial states, "Will Justin Trudeau's government keep its pledge to undo the worst parts of Stephen Harper's wide-ranging anti-terror laws? The signs are not encouraging. To date, the Trudeau government has moved firmly on only one portion of that particular election promise: the formation of a parliamentary committee to oversee the country's various security agencies. But that proposed committee would be hedged in by so many restrictions as to render it almost toothless. Meanwhile, the substantive security amendments the Liberals promised in last year's election campaign are being put off until at least the fall. **Public Safety Minister Ralph Goodale** says he wants to consult first. That the new government is moving so hesitantly on its predecessor's anti-terrorism law should come as no surprise. When the Harper Conservatives introduced Bill C-51 last year, Trudeau's response was carefully inconsistent. He said his Liberals didn't like the bill but would vote for it anyway - and then amend it if they won power. In their election platform, the Liberals vowed to "repeal the problematic elements of Bill C-51" and introduce a new bill that better protected civil liberties. To that end, they made eight specific promises, ranging from establishment of a parliamentary oversight committee to partial repeal of a provision that, with judicial consent, allows the Canadian Security Intelligence Service to engage in any disruptive activity short of bodily harm, obstruction of justice or violation of a person's sexual integrity. In the latter case, the Liberals didn't promise to remove this disruptive power entirely. But they said they would insist that if CSIS broke the law it do so within the confines of the Constitution's Charter of Rights and Freedoms. In government, the Liberals have been even more cautious. (…) In short, even with the best of intentions, parliamentary oversight is not enough to curb too-powerful security services. The trick is to ensure that such services are not given excessive power in the first place. Some critics, including eventually the New Democrats, understood this when Bill C-51 was unveiled. I'm not sure the Liberals ever did." Toronto Star, A13

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

* **Fire prompts evacuation of two Manitoba communities**
A raging forest fire has forced the evacuation of more than 2,000 people from two northern Manitoba communities. The province's Sustainable Development department announced Thursday evening that evacuation orders had been issued for the communities of Easterville and the Chemawawin First Nation, due to smoke and threat from fires that have moved to within a half-kilometre of the communities. Officials said fire crews are working on three fires in the area, with a ground attack underway as well as aerial support in the form of two water bombers. Approximately 70 Easterville residents were being evacuated to The Pas, officials said, while up to 2,000 from the Chemawawin reserve were on their way to Winnipeg. The Canadian Red Cross is helping to co-ordinate the evacuation. Winnipeg Sun, A5; Canadian Press (Times Colonist)

* **B.C. preparing for another year of severe drought**
B.C.is preparing for another severe year of drought after an early start to hot weather has reduced the snow pack and water levels to rates far below normal. The province has registered 13 per cent of the normal amount of snowpack in the mountains after high temperatures in March, April and early May, said Dave Campbell of the government's River Forecast Centre. Vancouver Sun, A8 (The Province); Canadian Press (Times Colonist)

* **Threat of wildfire being reduced**
A little hard work can help minimize the threat of wildfire. Crews from the Vernon Fire Department and the B.C. Wildfire Service held FireSmart demonstrations at Canadian Lakeview Estates Monday and Tuesday. VernonMorningStar.com

* **First Nation flooding forces evacuation**
Flooding has forced 140 people from their homes on a northern Alberta First Nation, prompting a local state of emergency. Dene Tha' First Nation Chief Joe Pastion said Thursday that heavy rains last week dramatically raised water levels. Dene Tha' First Nation is about 750 kilometres north of Edmonton. The community has a population of about 1,200. Pastion said the community is accepting donations to help people get through the evacuation. Edmonton Journal, A2 (Edmonton Sun); Canadian Press (Whitehorse Daily Star, Red Deer Advocate)

* **New emergency radio system proven in wildfires launched**
First responders across the province will soon be able to tap into an Alberta-wide digitized radio communication system, one in the works for eight years and which played a "pivotal" role during the Fort McMurray wildfire crisis. The Alberta First Responders Radio Communications System (AFRRCS) will be activated July 1, allowing police, emergency medical services, fire departments and government agencies to access and communicate on the same network instead of the stand-alone systems they use now. Justice Minister Kathleen Ganley said the new system will improve co-ordination and response to emergencies between agencies, including those that cross jurisdictional boundaries, such as a police pursuit or natural disaster. Edmonton Journal, A3 (Calgary Herald, Edmonton Sun, Red Deer Advocate)

* **Feds to conduct environmental review of Springbank dry dam plan**
Opponents of a dry dam at Springbank are hoping Ottawa's decision to review the flood mitigation project will be a game-changer. On Thursday, the Canadian Environmental Assessment Agency announced it would review the project that's meant to divert the Elbow River and temporarily store its water to prevent the kind of flooding that ravaged Calgary in 2013. Those who've condemned the huge project as disruptive and costly, like local landowner Ryan Robinson, had been urging the federal agency to take action and say it's a move that could help them halt it in its tracks. Robinson, with the group Don't Damn Springbank, predicts federal involvement will also revisit an alternative the group has been pushing: a reservoir upstream of Bragg Creek at McLean Creek they insist will be less disruptive. The environmental agency is also accepting public input for its assessment with a deadline of July 25. Calgary Herald, A3

* **Rescue group looks to reel in funds**
When Cole Marsh slipped and fell into Lynn Creek this spring, North Shore Rescue put in 1,950 volunteer hours to recover the 17-yearold's body. And that was just one of 52 calls the group has responded to so far this year. It has been an unusually busy six months for the organization, following a record-breaking 139 calls in 2015. And those efforts don't come cheap. The volunteer group typically spends about $500,000 annually, according to team leader Mike Danks, and depends on an unreliable mix of community fundraising, provincial gaming grants and municipal grants. Search-and-rescue groups across the province have called for a stable source of funding for years. A $10-million contribution by the province to the B.C. Search and Rescue Association earlier this year added $100,000 to North Shore Rescue's pot, but it was just a temporary boost. Vancouver Sun, A7 (The Province)

* **Lessons learned in emergency planning**
The biggest mistake possible in disaster planning is to overlook the lessons of the past, says the specialist in charge of emergency planning for the City of Red Deer. "The worst thing you can do is watch somebody else go through an emergency and not learn anything from it," Karen Mann, emergency management co-ordinator for the city, told a small gathering of business leaders during a training session at the Red Deer Chamber of Commerce on Thursday. Within her presentation, Mann offered business leaders her insight into the variety of emergencies they could encounter along with advice on how to prepare for them. In recent weeks, Mann has toured the Fort McMurray region to inspect the devastation from forest fires and visited the Village of Bentley during a shutdown of local Internet services. Red Deer Advocate, D1

NATIONAL SECURITY / SÉCURITÉ NATIONALE

No telling how we're being watched

Canada's version of the Star Chamber is about to get another case - the B.C. Civil Liberties Association challenge of the mass interception of Canadians' international telephone and Internet use. The group claims the Communications Security Establishment is spying on citizens in violation of the charter's protections against unreasonable search and seizure, but needs to see secret material to make its case. "We believe this dragnet program is probably one of the largest surveillance efforts the Canadian government has ever launched against its own citizens," BCCLA litigation director Grace Pastine said outside the Federal Court in downtown Vancouver. This battle began in October 2014 after the disclosures of U.S. whistleblower Edward Snowden; the BCCLA filed suit demanding to know who the CSE was watching, what data it was collecting, how long it was storing the information and how it was protecting privacy. Under the National Defence Act and a secret ministerial directive, the agency is permitted to read Canadians' email and text messages as well as listen to their international phone calls. (…) Unsurprisingly, the federal government responded to the first legal challenge of the CSE's activities with heavily edited documents saying their contents could be injurious to the nation's security. The BCCLA says the court must order Ottawa to reveal the material being protected so its constitutional challenge can proceed. "Much of what is sought to be redacted is already in the public domain as a result of comparable litigation in other jurisdictions and as a result of the voluntary disclosures that the (Attorney General of Canada) has elected to make in this case," BCCLA lawyer David Martin said in his submission. "In addition, the (BCCLA) does not seek the disclosure of information that would tend to reveal sources, targets or the identity of national security or intelligence, nor does the respondent seek the granular details of specific operations or the specific no doubt evolving technologies that underpin investigative techniques." Full disclosure of the scope of the CSE's activities might be embarrassing to the government, he maintained, but that does not mean it is injurious to national security interests. In particular, Martin pointed out that judicial warrants are required by other government agencies, including the 16 others involved in national security. "(The Canadian Security Intelligence Service) is subject to judicial control and there is no reason why CSE should not be," he insisted. Vancouver Sun, A3; Globe and Mail; CBC News (2016-06-23)

Cirillo shooting search warrant to stay sealed

The Supreme Court of Canada has rejected an Ottawa man's bid to learn why the RCMP raided his south-side townhouse in its investigation into the 2014 Parliament Hill shootings. Mounties executed a warrant to search the Heatherington Road home of Farhan Nur in May 2015, looking for any evidence connected to Michael Zehaf-Bibeau, who gunned down National War Memorial sentry Cpl. Nathan Cirillo, 24, Oct. 22, 2014. Zehaf-Bibeau, 32, then stormed Centre Block with an old rifle, wounding a parliamentary security officer before being quickly killed in a wild shootout with police and security officers in the Hall of Honour. Shortly before, he recorded a cellphone video saying the attack was "in retaliation for Afghanistan and because (former prime minister Stephen) Harper wants to send his troops to Iraq." The RCMP has long suspected jihadi sympathizers exploited Zehaf-Bibeau's faltering mental state and influenced him to launch the armed attack. Nur and another man whose south-side Ottawa home was searched - police have never charged or named either as a suspect or material witness in the Hill attacks - asked an Ontario court to order the release of RCMP affidavits, called "Information to Obtain" (ITOs), setting out the confidential details police used to win judicial approval for the warrants. Postmedia Network (StarPhoenix, N5, Vancouver Sun, Ottawa Sun, London Free Press, Leader-Post, Calgary Herald, Ottawa Citizen, National Post, Kingston Whig-Standard)

Victims of Air India bombing remembered at 31st memorial service

With poetry, prayers and calls for justice, the 331 victims of the 1985 Air India terrorist bombings were remembered at a memorial in Stanley Park Thursday night. Gurdial Sidhu, who lost her sister-in-law Sukhwinder, niece Parminder, and nephew Kuldip in the terrorist attack, said all sense of normalcy in her family's life also died the day of the bombing. "We still did not get any justice," she told about 60 people gathered at the Air India memorial wall. "At the end, I am forced to think there is no justice for this criminal travesty. The terrorists are still alive. They're free and they enjoy their lives." Two B.C.-made suitcase bombs exploded on June 23, 1985. The first killed two Japanese baggage handlers who were transferring a bag onto an Air India flight. The second exploded aboard Air India Flight 182, killing all 329 aboard. Two B.C. men linked to the Sikh separatist movement were charged in 2000 and acquitted in 2005. A third, Inderjit Singh Reyat, pleaded guilty to manslaughter for helping to build the bomb. He was released on day parole earlier this year. Former Surrey-Newton MP Jinny Sims said it was shameful so few people

attended a memorial service for the victims of Canada's worst mass murder. "Where is everyone else today?" she asked. This was the largest act of terrorism against Canadians and we have to remember that it was against Canada and Canadians." She also said there are people in Metro Vancouver who have critical information that could lead to more charges in the case. "We know that out there are people who know exactly what happened. But they are not saying," she said. "Why is it there is a cone of silence? Why is it that people are not speaking up?" Vancouver Sun; * iNews880 (2016-06-23)

*** Toronto imam says he is a changed man despite homophobic comments on YouTube**
A prominent Toronto imam who has signed two declarations against the shootings in Orlando appears on a recently posted YouTube video saying gay men should be put to death. But Abdullah Hakim Quick, a teacher at the Islamic Institute of Toronto in Scarborough, said in a statement that he is a changed man. "Many years ago I made hurtful comments against homosexuals for which I have apologized. My views have evolved over the years. I am fully committed to peaceful coexistence and respect among all people," he said. "The video was made in 2000 and is totally unrepresentative of my present position," he added in a note after CBC News asked him for an interview, which he declined. (…) Raheel Raza, president of the Council for Muslims Facing Tomorrow, and an author who tries to fight hate in Islam, said the video is shocking and Quick's remarks dehumanize gay men. She said the comments do not reflect the teachings of Islam. (…) "If the imams are playing God," Raza said, it is disturbing and it shows that religious leaders may be the source of hate that is taught to young people. "No one is born a terrorist. No one is born a radical. Somebody teaches them and they teach them through hate. This is where it starts," Raza said. If he is truly apologetic, she said he needs to make it clear where he stands on certain issues. "He needs to stand up and condemn the Sharia and armed jihad and all these radical notions from the seventh century, which we don't want to perpetuate in the 21st century. CBC News (2016-06-23)

Terrorism in Canada
A letter to the editor states, "It is unbelievable so many individuals try to blind themselves to the fact some Muslims advocate hostility against those who are not in their particular faith group, and that includes other Muslims. From all evidence, it appears Omar Mateem was gay, that a local iman inspired Muslims to act compassionately toward gays by killing them, and that by doing so Mateem could erase his guilt of being gay. Barbara Kay is correct in pointing out the methods other than firearms, used by terrorists who were all motivated in some degree by their interpretation of Islam. It is not Islamophobic to face the facts there are such people in this country, as evidenced by attacks by Islamic-inspired terrorists and that the Mounties and the Canadian Security Intelligence Service are surveilling as many as their budgets and physical resources will allow. Fortunately, there are Muslims who advocate for a reformation in the interpreting of wording that might encourage those looking at terrorism to adopt a more tolerant approach to others." National Post, A9

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Groups call claims limit discriminatory
Canadian human-rights and refugee groups say the federal government's decision to limit the number of annual Mexican refugee claims is discriminatory, after federal officials had argued the move protects Canada from bogus refugees, many of whom are involved in organized crime syndicates. Since 2014, the Canada Border Services Agency agents have intercepted more than 100 fraudulently obtained Mexican passports, some of which were carried by members of South American criminal gangs, according to government sources. The Globe and Mail reported on Wednesday that the Liberal government will follow through on its promise to lift visa restrictions for Mexican travellers effective Dec. 1, but it's prepared to partially reimpose the measure if the number of Mexican asylum seekers surpasses 3,500 within any 12-month period. (…) Officials were concerned that the presence of Mexican organized crime groups in Canada would increase and human-smuggling networks would take advantage of Mexico's weak passport security system. The federal cabinet was told Canada would also face pressure to lift visa restrictions on Ukraine, Romania, Bulgaria and Costa Rica, sources say. Globe and Mail, A4

Roma family returns to Canada after Conservatives' deportation order reversed

When Georgia Brouwer, 11, hugged her friend Viktoria (Lulu) Pusuma, 7, goodbye at Toronto Pearson International Airport in 2014, neither of the girls wanted the moment to end. "We wouldn't let go of each other and it was really sad," Georgia said of their farewell two years ago. But her dad, Andrew Brouwer, also the Pusumas' lawyer, promised his daughter he'd keep fighting for the family until they came home. On Thursday, the family - deported from Canada in 2014 - did just that, returning to the country that was their sanctuary for nearly three years. "This is freedom's smell!" Lulu's mother, Timea, exclaimed, stepping outside the airport for the first time after their return. CBC News

*** Il a voulu fuir la prison, il y passera des mois**
Un Montréalais qui a fui en Italie en plein procès, par peur d'aller en prison, devra vraisemblablement passer plusieurs mois derrière les barreaux pour avoir tabassé une femme. (…) Expulsé du pays ? James Sartor pourrait avoir des problèmes avec l'immigration s'il était condamné à une longue peine de prison. «En raison de son statut de résident permanent, il est d'ores et déjà interdit de territoire. Il pourrait être expulsé du Canada à l'issue de sa peine», a précisé Me Robillard. Le quadragénaire risquerait aussi de perdre son entreprise de couvreur de toitures, a spécifié l'avocate de la défense. Journal de Montréal

*** Temporary foreign worker cap stays at 20%**
The federal government is freezing the 20 per cent cap on the number of low-wage temporary foreign workers a company can hire. Labour Minister MaryAnn Mihychuk said the controversial temporary foreign worker program needs an overhaul and will announce her plan for more changes later this year. But for now, the cap, which was set to go down to 10 per cent beginning July 1, will instead stay where it is. "I believe this is a prudent step to take as we work to develop a better temporary foreign worker policy and fix some of the problems with the program that emerged under the previous government," Mihychuk said. Employers who first began hiring low-wage temporary foreign workers before the previous Conservative government changed the program will still be able to use it for 20 per cent of their workforce. Those who started using the program after that point, or who are hiring temporary foreign workers for the first time, are subject to a 10-per-cent cap. All the other program requirements - including having employers ensuring that Canadians and permanent residents have the first opportunities to apply for available jobs - will remain in place while the cap is frozen. Canadian Press (Times Colonist, B5; Globe and Mail)

*** Local, state, Canadian lawmakers gathering Friday in Ogdensburg to support bill that would alleviate problems for boaters**
Local, state and Canadian lawmakers will gather in support of a bill that would ease laws for boaters crossing international waters. Under Canadian legislation introduced by Senator Bob Runciman (Ontario – Thousand Islands and Rideau Lakes), American boaters would no longer have to report to Canadian customs when passing through Canadian waters, as long as they do not disembark, anchor, moor, make contact with another vessel or import goods. The measure would also exempt Canadian boaters from reporting to Customs when they return from American to Canadian waters, as long as they meet these same conditions. NCNow News (2015-06-23)

Court turfs Howe bridge suit
The final piece of a lengthy lawsuit designed to stop construction of the Gordie Howe International Bridge has been dis- missed by a U.S. federal court judge in Washington. Lawyers for Ambassador Bridge owner Matty Moroun launched a sweeping lawsuit more than six years ago against the Canadian government, several ministries and U.S. federal departments to stop the Detroit River crossing project. (…) Inquires to the federal government for reaction to Collyer's decision were referred to Infrastructure Canada, which did not provide a response. At the Windsor-Detroit Bridge Authority, which is overseeing construction of the Howe span, an official did not wish to address the decision. "Windsor-Detroit Bridge Authority's focus is on delivering the Gordie Howe International Bridge project as expeditiously as possible," spokesperson Heather Grondin said. "We have been making significant process since shovels first went into the ground last fall for our early works activities." Windsor Star (London Free Press, A2)

4 ways Brexit could affect Canadians
The results of Thursday's "Brexit" referendum (…) Canada could also lose out on some of the benefits of the Comprehensive Economic and Trade Agreement (CETA), the country's trade agreement with the EU, which is under review. The deal removes most tariffs on Canadian goods entering Europe, a boon for

many Canadian businesses. Canada exported almost $16 billion worth of products to the U.K. in 2015, or about 3 per cent of total exports, according to Statistics Canada, which makes it Canada's third largest trading partner behind the U.S. and China. Toronto Star

Liberal immigration policy
An editorial states, "Our Liberal government intends to lift the visa requirement for Mexican citizens, and it is proceeding in the most Liberal way imaginable - which is to say, not all that unlike the Conservatives, while righteously claiming the opposite. Indeed, reports Thursday could hardly illustrate better the mostly cosmetic differences between the Liberals and the Harper-era Tories on the immigration file. The goal is simple enough: to eliminate a diplomatic irritant with one of our major trading partners. And the problem is simple as well, if large: in 2007-09, nearly 25,000 Mexican citizens applied for asylum in Canada, and most - well more than 90 per cent - were not granted it. In a world of limitless resources, that would be fine: everyone would get a hearing and we wouldn't turn away legitimate claimants, of whom Mexico produces a great many - 1,500 over that three-year-period, exceeded only by Sri Lanka, China and Colombia." National Post, A9

CYBER SECURITY / CYBERSÉCURITÉ

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Mike Duffy Investigation, Trial Cost RCMP $477,858**
The Royal Canadian Mounted Police spent nearly $478,000 investigating Sen. Mike Duffy and preparing for his trial, The Huffington Post Canada has learned. Documents released under the Access to Information Act show a total of $477,858.52 was spent on "Project AMBLE," the Mounties' probe of Duffy. The bulk of the money — $402,901.29 — was spent on the investigation itself: $320,039.80 on salaries and overtime and $82,861.49 on travel and forensic accountants. Court preparation accounted for $49,199.03 and the trial for $25,758.20. But that nearly half a million dollars in RCMP expenses comes on top of the tens of thousands of dollars spent by the province of Ontario in court costs. At least $60,000 was paid to the judge for overseeing the 62-day trial and deciding Duffy's fate — not to mention the rest of the court staff, the Crown attorneys, and security costs. The Senate also spent $137,784 on an audit looking into Duffy and fellow senators Patrick Brazeau and Mac Harb's travel and living expenses. HuffPost Politics (2016-06-23)

*** Duffy to Fight Senate over Repaying $16,995 in 'Ineligible Expenses'**
Sen. Mike Duffy will be fighting the Senate committee for its demand for him to repay $16,955 in expenses as he argues that the Upper Chamber unjustly denied him $155,867.56 in salary while he awaited his trial. The court acquitted Mr. Duffy of all 31 charges against him last spring and he started receiving his salary and benefits again on Aug. 1, 2015. Duffy's lawyer, Donald Bayne, wrote in a brief open letter to the Senate on late Wednesday night that "this unjust suspension and severe economic and reputational penalty was imposed on a man known to be confronting grave health issues exacerbated by stress," adding that "the Senate now seeks to compound that unjust and oppressive penalty already paid in full by Senator Duffy." Oye Times; Canadian Press (Castanet, Sudbury.com)

Evidence missing, say police
Halifax police admitted Thursday drugs, money and possibly weapons have gone missing from exhibit vaults, and say they plan a wider search to determine the full extent of the problem. Supt. Jim Perrin said an audit of a vault containing drug exhibits found 90 per cent of samples being sought last year couldn't be found, and the "alarming" result prompted a closer look this year. At a news conference Thursday, Perrin said the follow-up audit produced better results, but he said Halifax Regional Police are still looking for dozens of exhibits that may have been misplaced, destroyed or stolen. (...) "At the end of this, we may be able to account for where all those exhibits went," Perrin said. "Police officers make mistakes .... It happens." Canadian Press (Chronicle Herald, A1, Times & Transcript)

Two officers were hospitalized after collision
The RCMP have released a few more details about a collision involving one of its vehicles earlier this week. Three people are recovering after Monday morning's accident on the Alaska Highway at Wann Road in Porter Creek. At around 10:30 a.m., an RCMP emergency response team vehicle was travelling north along the highway when it was involved in the collision with a small car. According to the RCMP, the circumstances of the accident, which closed the highway to traffic for five hours, are still being investigated. Two RCMP officers were transported to Whitehorse General Hospital. One underwent surgery for injuries to his arm. The other was assessed and released. The driver of the second vehicle was assessed onsite by EMS. Whitehorse Daily Star

Sophie tours RCMP Heritage Centre
Who can resist two fine-looking horses ridden by Mounties in red serge? Not Sophie, Countess of Wessex. Accompanying Lt.-Gov. Vaughn Solomon Schofield into the RCMP Heritage Centre for breakfast Thursday, the countess stopped by Salute and Turbo, two former musical ride horses, and chatted with their riders, constables Dale Malbeuf and Carman Hunter. "She just wanted to know how old the horses were and if we were the only ones who rode them," Malbeuf said. "Salute is 17 and we let her know there's a group of about 20 of us that ride the horses here." The officers volunteered to pull royal duty; Malbeuf from the Morse RCMP detachment and Hunter from Shaunavon. Al Nicholson, CEO of the Heritage Centre, pointed out museum exhibits as he walked Sophie to the dining room. One display in particular caught her eye - a dress worn by Sitting Bull's daughter. "She stopped for the longest time in front of that exhibit and read all that was written there," Nicholson said. Leader-Post, A3

Three charged after weapons found in van
Three people have been charged after reports of rapid-fire automatic weapons in the Otter Point area of Sooke on Tuesday night. Kyle Fletcher, Michael Masson and Brady Shivak are charged with unlawfully being in a vehicle knowing there was a firearm, prohibited weapon, restricted weapon, prohibited device or magazine in the vehicle. Shivak is also charged with possessing a firearm when prohibited by a court order. Masson is also charged with possessing heroin. Sooke RCMP said they arrested five people who were seen driving away in a red minivan from Otter Point about 9 p.m. Tuesday. A search of the vehicle turned up a 12-gauge shotgun, a semi-automatic SKS assault rifle and ammunition. Officers also found bear spray, knives, a substance suspected to be methamphetamine, heroin, cocaine, marijuana and several cellphones. Sooke RCMP Staff Sgt. Jeff McArthur said he believed the people were involved in target shooting, honing their firearms skills. Times Colonist

Alleged drug kingpin had several legitimate businesses, lawyer says
The alleged kingpin of one of the two alleged drug organizations targeted in Operation J-Tornado had several legitimate businesses, according to his lawyer. Shane Stephen Williams' lawyer, Brian Munro, referenced several of his client's alleged ventures while cross-examining the RCMP officer who was responsible for the money used by police during the almost three-year investigation. Comments have been made multiple times throughout the trial, which began at the end of April, about BigShots Sports Bar being Williams' bar. Police searched the bar, which was located at Westmorland Place in east Saint John, as part of co-ordinated raids on Sept. 10, 2014. On Thursday morning, though, Munro alleged Williams also had a construction company, Port City Builders. In addition to this, he said Williams had a numbered company that supplied second mortgages. Sgt. Dustine Rodier said these ventures were investigated as part of the proceeds of crime portion of the operation. She denied ever telling any of Williams' clients after his arrest not to pay any outstanding loans or money, and rejected Munro's allegation that she had harassed Williams' clients. "As part of the proceeds of crime investigation, my role was to contact businesses and parties Mr. Williams had dealings with and determine if there's evidence to be gathered for the investigations," said Rodier. Telegraph-Journal, B2

*** Red Deer teen faces over a dozen charges after stolen truck crashes into townhouse steps**
An 18-year-old Red Deer man is facing numerous charges after RCMP allege he stole a truck before crashing into several vehicles and a townhouse on Wednesday. According to police, the stolen truck was seen driving westbound on Cornett Drive in Red Deer when it hit another pickup truck and a car before veering onto a townhouse's lawn and getting stuck on the front steps. Mounties said the suspect then

tried to run away on foot while carrying a shotgun in an unsecured case, along with ammunition. Police said about five witnesses were able to apprehend the suspect in a nearby park until officers arrived. In a release, police said while they "appreciate citizens' wish to help out" and were glad nobody was injured, they urge the public not to try making citizen's arrests. Global News

*** Pit bull involved in violent Surrey attack to be put down**
The pit bull that was involved in an attack on a woman in Surrey earlier this week will be put down, according to Surrey RCMP. The dog's owner voluntarily surrendered the dog to Animal Control to be put down, according to the City of Surrey. "While the Surrey RCMP's investigation remains open, officers have looked at the totality of the circumstances in this file and have deemed that there is insufficient evidence to proceed with criminal charges at this time," Sgt. Alanna Dunlop said in a statement. Surrey RCMP and the City of Surrey have been searching for the dog and its owner since it attacked a 65-year-old woman outside a convenience store on 120 Street on Monday. Police say the woman was walking in the area "when she was attacked, unprovoked, by an unleashed grey and white pit bull dog." CBC News; AM730; Castanet; Voice Online

*** RCMP searching for man who allegedly attempted to abduct a boy in Sylvan Lake**
RCMP are looking for a man who allegedly attempted to abduct a boy in Sylvan Lake on Wednesday. It happened around 4 o'clock in the afternoon, when a 12 year old boy was approached by a man in an older grey Honda 4-door, near Mother Theresa school. It's alleged the man drove up to the youth, grabbed him by the arm and tried to pull him into the vehicle. The youth was able to escape to safety. The suspect is described as a white male between 25 and 30 years of age, with a medium to heavy build, bald wearing a black hoodie pulled over his head. He was also wearing sunglasses. A composite sketch is on our website. iNews880; CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Les États-Unis peu enclins à transférer des détenus canadiens
Les probabilités qu'un Canadien incarcéré aux États-Unis soit transféré dans son pays sont équivalentes à celles de gagner à la loterie, et ce, même avec un gouvernement libéral qui a promis d'en faire plus pour les détenus à l'étranger. Des données obtenues par La Presse Canadienne grâce à différentes sources - notamment Affaires mondiales Canada, Service correctionnel Canada et, aux États-Unis, le Bureau des prisons et le département de Justice - démontrent que la plupart des Canadiens incarcérés au sud de la frontière se trouvent dans des établissements gérés par des États. Un total de 964 Canadiens avaient été emprisonnés aux États-Unis en date du 18 mai, de loin la plus grande proportion de citoyens canadiens détenus dans un autre pays. Parmi ceux-ci, 420 se trouvaient dans des établissements carcéraux étatiques, et 394, dans des prisons fédérales. Les États sont toutefois peu enclins à accepter les demandes de transferts de prisonniers désireux de purger leur peine au Canada, mettent en lumière les données compilées. Règle générale, les États sont responsables des personnes reconnues coupables de crimes violents. Entre 1978 - quand l'accord a été conclu - et 2014, 1256 détenus canadiens ont été retournés en sol canadien par les autorités américaines fédérales. Les États n'ont quant à eux accepté que 161 transferts. De nombreux Américains voient le système carcéral canadien comme n'étant pas suffisamment rigide, observe l'ex-responsable en chef du programme de transfert aux États-Unis, l'avocate Sylvia Royce. Presse canadienne (Acadie nouvelle)

*** Tories demand public inquiry after prisoner death**
Nova Scotia's Tory opposition is demanding a public inquiry in light of details revealed this week about the death of inmate Jason Marcel LeBlanc. Nova Scotia provincial jails have on-site nursing seven days a week but only from 8 a.m. to 8 p.m. There was no medical help on hand when LeBlanc suffered breathing trouble and died in the early hours of Jan. 31 at the Cape Breton Correctional Facility. He had previously ingested a lethal amount of methadone and bromezapan. That is because prison healthcare in Nova Scotia is not as extensive as in some other provinces. In Saskatchewan for example, prison nurses are available for 16 hours per day. Doctors in that province also offer weekly on-site clinics and are otherwise on call, according to the Human Rights in Action Handbook for Provincially Sentenced Prisoners in Saskatchewan. Tory leader Jamie Baillie said Thursday he can't be certain on-site medical care would

have saved LeBlanc. "That is one way. We need to find out the best way to provide medical assistance to people who enter our justice system as a result of mental illness or addictions like Jason," According to a Canadian Press report, LeBlanc was sent to jail on the afternoon of Jan. 30, after he was arrested for a parole violation. His blood pressure was already starting to go awry at that point and he managed to keep a bag of bromezapan pills in his pocket that were only found after he died. Chronicle Herald, A4

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Police can swab rape suspects, court rules
In a ruling that adds to police powers in investigating rape, the Supreme Court of Canada says police have the right to take a penile swab from suspected attackers, forcibly if necessary, as long as they do so in a private cell and have reasonable grounds to believe they will find relevant evidence. The new power is aimed not at gathering the suspect's DNA but the victim's. In that sense, it is, in a far more modest form, a male suspect's version of the rape kit, the highly intrusive examination of victims done in medical clinics, albeit with their consent, partly to recover DNA evidence to identify their assailant. Police will not need a warrant to obtain the swab from a suspect. His own DNA cannot be used in court unless police first obtain a warrant, or the suspect consents to the search, the court said. It is the first time the court has empowered police to take bodily samples without a warrant, according to Ottawa criminal lawyer Howard Krongold, who represented the Criminal Lawyers Association, which intervened in the case. Globe and Mail, A5

Arrest warrant issued for accused challenging minimum sentences
A judge has issued a warrant for the arrest of a man who was convicted of firearms offences and is challenging the constitutionality of mandatory minimum sentences for such crimes. On Thursday, B.C. Supreme Court Justice Stephen Kelleher was set to give his ruling on the constitutional application filed by Aosama Salim Hmod Al-Isawi, but instead issued the arrest warrant after the offender, who is out on bail, failed to show up in the Vancouver courtroom. Andrew Bonfield, Al-Isawi's lawyer, told the judge he had spoken to his client Wednesday night and told him to be in court Thursday. He said Al-Isawi had medical issues, but couldn't say why he was a no-show. Al-Isawi was convicted of using an imitation firearm to rob or try to rob 11 Lower Mainland pharmacies of the painkilling drug Percocet. The Province, A18

*** Crime prevention, victim services initiatives funded**
The Crime Prevention and Victim Services Trust is providing funding totalling $140,737 to eight community-led projects with a crime prevention or services for victims focus. The trust awards funds twice a year for eligible projects that are intended to: reduce crime; prevent violence against women and children; address the root causes of crime; provide services and information to victims of crime; or provide information about crime prevention and victimization. More than half the money ($72,064) is going to the Yukon Status of Women Council _ for Women and Girls: Sex Work and Trafficking in the Yukon. Whitehorse Daily Star, 4

*** Crime down across Durham Region, Oshawa**
It's official – crime was down in the region last year. According to the recently released annual report for 2015, Durham residents experienced less crime than the year before. The report – of which a preliminary version was presented to regional councillors earlier this year – highlights a 0.3 per cent drop in Criminal Code violations, not including traffic charges, with 23,202 known violations. On its own, Oshawa saw a 1.8 per cent drop in crimes not including traffic violations, including notable decreases in break and enters (24.6 per cent), motor vehicle thefts (33.7 per cent) and drug possession (20.8 per cent). The city, however, did see increases in fraud (27.6 per cent), arson (14.3 per cent) and drug production (20 per cent). For police chief Paul Martin, the general downward trend seen in Durham is similar to that across the country, but adds that may change in the future. Oshawa Express (2016-06-23)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

*** Advocate calls on Canada to remove sexism from Indian Act before MMIW inquiry**
A prominent Indigenous feminist says Canada's upcoming inquiry into missing and murdered Indigenous women can't be taken seriously until the federal government addresses sexism within its own legislation that's existed since 1876. Sharon McIvor said she was dismayed to find out recently that the federal government asked the United Nations Human Rights Committee to suspend consideration of a petition she launched aiming to stop gender inequality in Indian status designations. McIvor has been fighting for several decades against provisions in the Indian Act that stop Indigenous women from gaining Indian status and passing it along to their descendants on the same basis as men. "Because of this, Aboriginal women and their descendants have been separated from their families and communities, treated as less worthy, less human, less Indian, and not full members of their cultures and communities," McIvor said in a statement. The federal government's reason for blocking her petition to the UN is that it will be embarking on its own wider consultations in an effort to fix the problem. APTN (2016-06-23)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Underage access to marijuana a concern
Talk about a joint effort. There are bureaucrats from a dozen provincial departments working on an exhaustive cannabis strategy that will examine the impact of legalized recreational marijuana. As Prime Minister Justin Trudeau's government prepares to change federal laws next year, officials at Queen's Park are looking at everything from the effects on health and road safety to justice issues and fiscal implications. Public servants from the Ministries of Health, Education, Finance, Transportation, the Attorney General, Community Safety and Correctional Services, Municipal Affairs, Children and Youth Services, Indigenous Relations and Reconciliation, Community and Social Services, the Treasury Board secretariat, and the cabinet office are involved in the effort. Premier Kathleen Wynne emphasized Thursday that regulating the drug and limiting access for children and teenagers is a key concern no matter what the forthcoming federal legislation looks like. "I want there to be a controlling protocol in place. I think it is important in the same way that in Ontario we have controls on alcohol," Wynne told CBC Radio's Metro Morning. "We need to have some regulation of recreational marijuana. What I'm concerned about right now is that there hasn't been a clear delineation between recreational and medicinal marijuana," she said. While such marijuana is legal for those who have a prescription from a medical doctor, the storefront "dispensaries" sprouting up across Toronto are illegal. Wynne said the lack of legislative clarity from Ottawa has allowed the weed outlets to thrive to the point that there are more than 100 in the city even with the police cracking down. Toronto Star, A8

Future legalization of pot a factor in ruling
Former University of Saskatchewan football linebacker Seamus John Neary gave an audible sigh of relief when Queen's Bench Justice Shawn Smith sentenced him to two years of probation, but no jail time. Neary, 25, was convicted in November of trafficking marijuana and possessing the proceeds of crime, after 21 pounds of marijuana and $1,000 in cash were seized during an investigation in February 2014. Smith noted the Court of Appeal has ruled sentences of 15 to 18 months in jail are appropriate for marijuana trafficking involving amounts similar to Neary's case, but said the fact Canada is in a transition period with the federal government promising to legalize marijuana was a factor in his ruling. StarPhoenix, A11

*** We should legalize pot and move on**
A letter to the editor states, "Marijuana use carries a costly toll - June 23 Regarding Carol Mary Awrey's letter about the legalization of marijuana, I have some thoughts on her points. While I do agree that drug addiction is a real concern facing society today, I for one do not believe that simply legalizing marijuana will produce a whole (pardon the pun) crop of weed addicts. Personally, I have never been a pot smoker nor do I plan on becoming one. Does this writer really believe that, should it be legalized, thousands of

people who have never smoked marijuana before are suddenly going to run out and light up? Maybe it's time we stop putting people in jail for smoking a joint on Friday night after work and keep our jails for the real criminals." Waterloo Region Record, A8

*** Canada's drug policy is completely inadequate**
An opinion piece states, "The new government has promised to table a cannabis legalization bill in April 2017. This will "keep marijuana out of the hands of children, and the profits out of the hands of criminals." Due to this promise, Liberals now regard themselves as savants, leading a shining bastion of New Age drug laws. Why then, is Canada's current system so fucked up? Available treatment programs don't help, and the same policies that underpin the government's swank are being thwarted. Conservatives repeatedly bombarded policies hailed by the new Liberal platform, rendering them ineffective under their reign. Although Liberals won a majority, these policies remain as they were under the Harper government. Recently, this stagnation affected the Liberals' own kin**.** The ex-Liberal and now independent Honourable Hunter Tootoo resigned as Minister of Fisheries and Oceans after blaming an unspecified substance abuse problem. What else can be done for people — and public officials like Tootoo — if the resources that are available on a relatively consistent basis (unaffected by partisan politics) are a joke?" The Gateway (2016-06-23)

PUBLIC SERVICE / FONCTION PUBLIQUE

Fear that whistle blowing?
A fear of reprisals is the main reason why federal public servants are reluctant whistleblowers, says a report done for the Office of the Public Sector Integrity Commissioner. The report, Exploring the Culture of Whistleblowing in the Federal Public Sector, was prepared by Phoenix SPI, an Ottawa public opinion and market research firm. It summarizes the results of 10 focus groups of public servants - management and non-management - last November in Ottawa, Winnipeg, Regina, Quebec City and Moncton. The report says that, while more procedures are in place to facilitate whistle-blowing, some public servants were skeptical about the extent to which things had really changed. "Most participants believe that fear of reprisals for reporting wrongdoing is a real concern," the report says, though the extent to which the concern is real can vary. "For example, it was suggested that some departments are probably worse than others, given their internal culture," says the report. "In other words, the fear is justified, but to different degrees depending on context and circumstances." Moreover, a majority of managers in each focus group said concerns about reprisals for reporting wrongdoing "are as justified or more justified" for public service managers, in part because they have no union to support them. Ottawa Sun, A10 (Ottawa Citizen)

*** Federal workers sound off over payroll problems**
Unpaid bills, emergency loans, mortgages in default. Those are some of the hardships faced by a growing number of federal employees… all because of glitches with the government's new payroll system. It's short-changing everyone from prison guards to the coast guard. In a CKWS News exclusive — Newswatch's Morganne Campbell talks to some local workers who aren't getting the pay that's owed to them. Dealing with hardened criminals on the inside – a tough job for correctional officers. Bryan"/Correctional Guard: "The stress level is right through the roof. Everyone is on edge. But these days, much of the stress is coming from their employer…. the federal government. We've concealed the identity of this man, who's been told by Corrections Canada that he could face disciplinary action for speaking negatively about his employer. We've decided to call him "Bryan." Bryan is a correctional officer in the Kingston area — who's impacted by ongoing glitches with the Government's new "Phoenix automated payroll program". (…) Bryan figures he's been short-changed one-thousand dollars so far this month … plus overtime and other expenses. CKWS TV (2016-06-23)

OTHER / AUTRE

*** Abu Sayyaf frees Filipino woman kidnapped with Canadians Robert Hall, John Ridsdel**

Abu Sayyaf extremists on Friday freed a Filipino woman who was with two Canadian hostages beheaded by the militants in the southern Philippines after failing to get a huge ransom, officials said. Marites Flor was abandoned by the gunmen in front of the house of Sulu provincial Vice Governor Abdusakur Tan before dawn Friday. She was later turned over to the military for medical checkup, said police Superintendent Junpikar Sitin. Flor was abducted with two Canadians, John Ridsdel and Robert Hall, and Norwegian Kjartan Sekkingstad by the ransom-seeking militants from a resort on southern Samal island in September last year. Sekkingstad remains in captivity. It was not immediately clear if a ransom was paid to secure the freedom of Flor, who appeared in Abu Sayyaf videos tearfully pleading for her life and those of her companions. In a final video, she called on President-elect Rodrigo Duterte to save their lives before the extremists killed Hall a few days later. Associated Press (Global News); AAP

*** Do We Really Want a War With Russia?**
An opinion piece states, "No area of public policy is so shrouded in secrecy, obfuscation and outright deception than foreign policy. Most of the time it doesn't seem to matter much to the majority of voters who have more pressing things to worry about. But when Canadians read a headline that says "Russia mobilizing for war" one would hope they would take notice. A more absurd declaration is hard to imagine but there it was – coming out of the offices of CSIS, the Canadian Security and Intelligence Service. It was just the latest alarmist rhetoric in a steady stream of anti-Russian propaganda that coincided with the largest military build-up (a recent NATO military exercise called Anaconda) on Russia's borders since the German invasion of WW 2. As with almost every aspect of foreign policy, context is everything and this particular gem only begins to make sense if you go back to a February 1990 meeting between Soviet President Mikhail Gorbachev and the US Secretary of State, James Baker. That meeting saw a deal concluded (regrettably only with a handshake) whereby Gorbachev agreed to dismantle the Soviet Union and the Warsaw Pact (the NATO equivalent), in exchange for Baker's promise that NATO would not expand "one inch to the east."" Counter Punch

Is Iran holding a Canadian hostage?
An editorial states, "Homa Hoodfar, a 65-year-old Canadian-Iranian university professor, should be home in Montreal right now but is instead being held by the Iranian government in the country's most notorious jail - a place where prisoners are routinely tortured. She has not been allowed contact with her family or her lawyer since she was arrested on June 6 in Tehran by Iran's Revolutionary Guard. No official charges have been announced. The Canadian government does not have formal diplomatic relations with Iran. Officials say they don't know why Ms. Hoodfar was arrested, and that they are concerned for her health. Ms. Hoodfar suffers from a neurological disorder and is unlikely to have access to the medication she needs. This farce would be unacceptable under any circumstances, but it is even more appalling because it appears Ms. Hoodfar may have been taken prisoner in the hope of exchanging her for another Canadian-Iranian dual citizen living in Toronto. Iran has long wanted to get its hands on Mahmoud Reza Khavari, the former chief of the Melli Bank of Iran, who fled to Canada in 2011 after prosecutors tried to question him in connection with an alleged embezzlement and money-laundering scheme." Globe and Mail, A10; Kingston Whig-Standard (London Free Press)

Do something to stop ISIL
An editorial states, ""Is it better to not call a genocide 'genocide' and do nothing, or is it better to call a genocide 'genocide' and still do nothing?" - Payam Akhavan, former UN war crimes prosecutor. Remarkably, last week's parliamentary debate over whether to recognize that the Islamic State of Iraq and the Levant (ISIL) is committing genocide skirted one key question: how will declaring genocide affect what Canada is doing to prevent it? Perhaps this was an oversight. Perhaps the Tories really believed that calling a thing by its proper name is a triumph in its own right. If so, they were mistaken. Canada's recognition of this atrocity changes nothing on the ground. However, as the Liberals were right to note, genocide is a legal term. And it's one that triggers significant responsibilities. Now that the government has accepted that ISIL is trying to wipe out the Yazidi population, it should make clear how it intends to make good on its obligations. Specifically, under the Genocide Convention, Canada is now obliged to "prevent and punish" the perpetrators of this crime. This is not as pie-in-the-sky as it sounds. Canada is obviously not expected to solve this gargantuan problem alone. Rather, the obligation rests on all signatories to the convention, but to differing degrees, depending on each state's capacity to influence the perpetrators' actions, its geographical distance from the events and the strength of its political ties. So the

bar for Canada is not that high. But however low it may be, there can be no question that Canada has not yet crossed it. The Liberals will, of course, tell a different story. They will note that they have put in calls for the United Nations to take "urgent action" to investigate and prosecute ISIL. But we must be honest about where such efforts will lead, or more precisely, not lead." National Post, A8

INTERNATIONAL

Brexit: les Britanniques quittent l'UE et provoquent un séisme mondial
Les Britanniques ont décidé de quitter l'Union européenne, un désaveu pour la construction européenne qui a assommé les marchés mondiaux en ouvrant une ère d'incertitude sans précédent depuis des décennies, et dont David Cameron a tiré les conclusions en démissionnant. Selon les résultats définitifs publiés vendredi matin, 51,9% des électeurs ont voté pour le Brexit lors du référendum de la veille, marqué par une participation importante (72,2%). L'ensemble des marchés mondiaux a été gagné par la panique, les Bourses de Paris et Francfort plongeant d'environ 10% avec des valeurs bancaires en déroute. "C'est l'un des plus gros chocs sur les marchés de tous les temps", a estimé Joe Rundle, analyste chez ETX Capital. Les résultats montrent un pays divisé, avec Londres, l'Ecosse et l'Irlande du Nord qui voulaient rester, tandis que le nord de l'Angleterre ou le Pays de Galles ont largement voté contre. Partisan du maintien dans l'UE, en première ligne pendant la campagne, le Premier ministre conservateur David Cameron en a rapidement tiré les conclusions en annonçant sa prochaine démission lors d'une brève allocution devant le 10, Downing Street. "Les Britanniques ont pris une décision claire (...) et je pense que le pays a besoin d'un nouveau leader pour prendre cette direction", a déclaré M. Cameron, en précisant qu'il resterait en place jusqu'à l'automne et la désignation d'un nouveau leader par son parti. * Agence France-Presse (Huffington Post); Radio-Canada; * Associated Press (CBC News, CTV News)

*** Teacher recalls battle with tornado that killed 98 in China**
Teacher Guo Haimei said the ferocious wind, blacked with dust and debris, seemed to descend out of nowhere onto her kindergarten and its 120 pupils. Within minutes, the powerful tornado and its accompanying rain and hailstorm had scythed through the area of eastern China with merciless force, leaving almost 100 people dead and another 800 injured. "I was very scared. I had no idea what was happening," said Guo. "When I tried to close the door, my hand was injured by the wind pushing it back." Guo and her mostly 6-year-old pupils were among the lucky ones. Although the school was heavily damaged, just seven students were injured, two of them seriously. One day after the storm, rescuers on Friday continued searching for survivors in this densely populated area of farms and factories on the outskirts of the major city of Yancheng in Jiangsu province. The twister was one of the most extreme weather events witnessed by China in recent years, leaving a swath of destruction with destroyed buildings, smashed trees and flipped vehicles on their roofs. A sprawling solar panel factory was shredded, forcing fire crews to secure toxic materials before they leaked into neighbouring waterways. Associated Press (CTV News)

*** EgyptAir recorders to go to France after data downloads fail**
Initial attempts to download information from the flight data and voice recorders of an EgyptAir plane that crashed into the Mediterranean last month have failed, and key parts of the recorders are being sent to France for repairs, according to Egyptian and U.S. officials. The "electronic boards" of the recorders are being flown next week to the offices of the French aviation accident investigation bureau near Paris, authorities said. After the boards are repaired and salt removed, they will be sent back to Cairo for data analysis, Egypt's Investigation committee said in a statement late Thursday. The recorders, also known as black boxes, were extensively damaged when EgyptAir Flight 804 travelling from Paris to Cairo plunged into the sea on May 19, killing all 66 people on board. Associated Press (680 News) (2016-06-23)

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
July 9, 2016 / le 9 juillet 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Inquest needed into prison death
An editorial states, "How did it happen again? How did yet another woman with mental health issues choke herself to death while in a solitary confinement cell at Kitchener's Grand Valley Institution for Women? How and why did Terry Baker die in this terrible way this week? We thought Correctional Services Canada and the federal government had learned important lessons after all the lengthy investigations and earnest recommendations for change that followed the 2007 death of Ashley Smith, in the same prison, in what appear to be remarkably similar circumstances. We thought the serious systemic problems uncovered by a scathing report from the country's chief correctional investigator and then a coroner's inquest into Smith's death had already been dealt with. A deeply troubled 19-year-old, Smith was in prison for a series of minor offences when she choked herself to death in a segregated cell at Grand Valley prison while prison guards watched... Holding a coroner's inquest into Terry Baker's death would serve the public interest. There should be one. Yet we say this knowing we've been here before and that all the hard work done by the jury probing Ashley Smith's death was not enough to stop Baker from dying. However the federal government, which is responsible for the nation's prisons and ultimately for the conditions in which Baker found herself, need not wait for an inquest to act. **Public Safety Minister Ralph Goodale** said Thursday that the practice of segregation in women's prisons must

be addressed. That's a promising response but deeds, not words, are needed from this still young Liberal government." Waterloo Region Record, A6

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Firefighters holding their own against burning Wainfleet Bog
Firefighters are holding their own against a smouldering burn in the Wainfleet Bog. The fire had expanded from one hectare Tuesday to 6.4 hectares by Thursday morning. A Niagara Peninsula Conservation Authority news release said the blaze is now in the second phase of forest fire fighting: 'being held.' The four fire fighting phases are: not under control, being held, under control and out of control. Hamilton Spectator, A7

Another improperly-doused fire causes problems
One new wildfire was confirmed in the Southern Lakes fire region at 3 p.m. Thursday. The 0.01-hectare blaze began on a small island on the southeast side of Braeburn Lake. As with numerous other fires this season, Thursday's was caused by an abandoned campfire that was not properly extinguished. One crew and a helicopter responded with support from another crew, and the fire was quickly extinguished, Yukon Wildland Fire Management officials said today. Whitehorse Daily Star, 5

Quelque 14 000 canards atteints du virus H5N2 seront euthanasiés
Environ 14 000 canards d'une ferme ontarienne atteints du virus de l'influenza H5N2, mieux connu comme étant la grippe aviaire, seront euthanasiés. Les canards issus d'une ferme de St. Catharines, en Ontario, ont pour l'instant été placés en quarantaine.Ces oiseaux sont affectés par une sous-classe faiblement pathogène du virus qui provoque une maladie moins grave chez eux, a indiqué un vétérinaire en chef pour l'Agence canadienne d'inspection des aliments (ACIA), Harpreet Kochhar.Tous les canards affectés seront euthanasiés. La Presse Canadienne (Le Nouvelliste, 27); Canadian Press (Waterloo Region Record)

Trois ans après Lac-Mégantic
Un article d'opinion dit, « Il y a trois ans, le 6 juillet 2013 devenait une triste journée pour les Canadiens. A ce moment, personne ne se doutait qu'une tragédie allait secouer la municipalité de Lac-Mégantic dans la région de l'Estrie. Malheureusement, cette nuit-là, un train laissé à la dérive qui transportait du pétrole brut a déraillé en plein coeur du centre-ville et a emporté dans les flammes les vies de 47 personnes remplies d'avenir. Aujourd'hui, malgré la reconstruction de leur centre-ville, les citoyens de Lac-Mégantic sont toujours inquiets et préoccupés par les nombreux trains qui traversent leur ville. C'est avec raison qu'ils réclament l'implantation d'une voie de contournement afin d'éviter qu'un drame semblable ne se reproduise. » La Tribune, 16

Stampede begins: Ft. McMurray wildfire first responders honoured
The Calgary Stampede parade reserved a special spot for Fort McMurray on Friday, more than two months after a fierce wildfire forced everyone to flee the northeastern Alberta city. A contingent of first responders and staff from the Regional Municipality of Wood Buffalo marched directly behind the vintage car carrying the parade marshals and singers Jann Arden and Paul Brandt. The group carried a banner reading "Thank You Alberta" and wore T-shirts with "We are here. We are strong" printed on them. Canadian Press (Waterloo Region Record, B12, Chronicle-Herald, Red Deer Advocate)

UNB grad fighting 'the beast' in Alberta
It's a wildfire called 'the beast' and a University of New Brunswick graduate is using his brains and brawn to battle it. The massive Fort McMurray wildfire has burned 600,000 hectares of forest since it started in May - and it forced the evacuation of more than 80,000 people. Almost 15 years ago, Bathurst-born Alan Gammon was tree-planting in the forests of New Brunswick and studying for a bachelor of science and kinesiology at the University of New Brunswick. Now he's assessing wildfires and flying in helicopters over the wooded expanses of the Fort McMurray forest as a fire technologist for the government of Alberta. And while Gammon won't talk specifically about battling the beast - the blaze's firefighting efforts

are currently under review - he describes a life full of high-flying adrenaline as a front-line strategist planning attacks and techniques designed knock fires down. Daily Gleaner, A1 (Telegraph-Journal)

Fort McMurray fire seared in our memories
An editorial states, "It was neither the largest nor the hottest fire on record but it was the most traumatic. It destroyed some 2,400 buildings and threatened a major industrial complex. Perhaps more important, as Fire Chief Darby Allen said, was "the way this thing happened, the way it travelled, the way it behaved." The speed and intensity with which the fire grew and spread through town brought criticism that the emergency officials did not respond quickly enough. But that was also evidence of what Allen called "the overwhelming nature of the fire." Trauma and stress afflicted residents and firefighters alike." Waterloo Region Record, A6

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Ottawa braces for era of leaks
It's not a matter of if there will be another Edward Snowden, it's a matter of when, according to internal government documents obtained by the Star. Global Affairs officials warned minister Stéphane Dion in November an event on the scale of Snowden's disclosures about Internet surveillance is inevitable. "Incidents similar to the Snowden disclosures and the Sony hack will happen again and we can expect that sudden events will affect international debates on cyberspace," the document reads. The briefing note, prepared for Dion in November and obtained under access to information law, suggests that Snowden's disclosures about western mass surveillance "altered the tone" of the international discussion on cyberspace. In 2013 Snowden, a former employee of the U.S. National Security Agency (NSA), pulled back the curtain on mass surveillance online, detailing the capabilities of the "Five Eyes" countries - Canada, the United States, the U.K., Australia and New Zealand - to monitor activity online. His release of classified NSA documents triggered outrage among those who said he put lives at risk, and praise from others who argued he shed light on questionable practices. He was forced to flee the U.S. and was granted asylum in Russia. Toronto Star, A6

*** The developer, the fugitive and the feud**
Five years ago, Sam Mizrahi, one of Toronto's most ambitious real estate developers, found himself in a basement in the city's Bridle Path neighbourhood. It was there, he says, he began to fear for his safety. In a span of just a few hours, one of the main financial backers of two of his luxury condominium projects, Mahmoud Khavari, had become one of Iran's most wanted men, having left his position as the chairman of the country's largest bank and fled to Canada amid a corruption scandal. With Iran demanding Mr. Khavari's immediate return, Mr. Mizrahi feared being caught in the crossfire of a potentially violent international dispute as they debated the future of their business partnership inside the former banker's Toronto home. The agreement worked out in that basement in the hours that followed the frantic flight to Canada has become the subject of a multimilliondollar lawsuit before the Ontario Superior Court, and led to a feud between Mr. Mizrahi and the Khavari family of near-Shakespearian proportion, involving alleged death threats, international intrigue and some of the city's hottest real estate. Mr. Mizrahi, in his sworn statement, says the Khavari family and CSIS officials informed him in 2011 that the Iranian government was sending a "special force" to Toronto with the aim of spiriting the former banker back to Tehran. Iranian officials have also reportedly raised his name in discussions related to Saren Azer, an Iranian-Canadian doctor who is accused of abducting his four children and fleeing to Iran. In May, two former federal officials working on the file told the Globe that Mr. Khavari had been mentioned in back channels with Iranian officials, suggesting there's a deal to be made. All the while, Mr. Khavari has remained in Toronto, living in North York, as his family expands its real estate holdings across the city. Globe and Mail, M1

Government downplays terrorism threat
Re: "Terrorism: Is Canada ready?" July 2
A letter to the editor states, "This is a very thought-provoking column by Geoffrey Johnston, and anyone who thinks Canada is prepared to handle a major radical Islamist attack on a soft target like one of our

airports is dreaming. We have to give full marks to the RCMP and CSIS for their having thwarted numerous planned attacks on Canadian soil." Kingston Whig-Standard, A4

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Pair arrested in relation to fentanyl production bust
A search warrant executed last December in Red Deer County has been tied to a complicated investigation and two arrests this week related to largescale production of fentanyl pills. That search was carried out at a business in the county by police authorities who seized four barrels containing 100 kgs of N-phenethylpiperidinone (NPP), used to make fentanyl. The barrels were originally from China and had come to the attention of the Canada Border Services Agency in October at Edmonton International Airport. Red Deer Advocate, A3

Cloutier veut des actions rapides
Le candidat à la direction du Parti québécois (PQ), Alexandre Cloutier, a interpellé le premier ministre Justin Trudeau vendredi à propos du dossier du lait diafiltré. Le député réclame des actions rapides de la part du gouvernement fédéral. « C'est la survie de centaines de fermes familiales qui est en jeu en ce moment », a expliqué M. Cloutier par communiqué de presse. Selon lui, le gouvernement fédéral fait preuve de laxisme dans le dossier. Il a ajouté que les importations de lait diafiltré ont fait perdre 220 millions de dollars aux producteurs laitiers de la province en 2015. Alexandre Cloutier croit que le gouvernement Trudeau n'a aucune raison de ne pas régler tout de suite le dossier. D'après le député, l'Agence des services frontaliers du Canada devrait cesser de traiter le lait diafiltré comme un ingrédient, ce qui lui évite les tarifs imposés aux aliments sous la gestion de l'offre. Le Quotidien, 15

Tips for easier border crossings
Summer's here and many Canadians may be thinking of hitting the road for a much-needed vacation. The Canadian Border Services Agency is providing travel tips for those who choose to venture out of the country. They have issued several key tips... LethbridgeHerald.com

CYBER SECURITY / CYBERSÉCURITÉ

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Mounted Police Professional Association of Canada (MPPAC) Granted Intervener Status In RCMP's Appeal Re: St Albert Member Shooting**
The Mounted Police Professional Association of Canada (MPPAC) continues to stand up for the rights and interests of Royal Canadian Mounted Police (RCMP) members to ensure their employer complies with health and safety recommendations following a situation which resulted in the shooting and death of RCMP Constable David Wynn, and shooting injuries to Auxiliary Constable Derek Bond in January 2015. Earlier this year, RCMP management attempted to block MPPAC from having any status in the RCMP's appeal of the direction issued by Economic Skills and Development Canada (federal agency mandated for oversight of health and safety of federal employees) as a result of an investigation regarding this matter. However, this week the Occupational Health and Safety Tribunal of Canada ruled in favour of MPPAC being granted intervener status. Mounted Police Professional Association of Canada News Release (Newswire.ca)

*** Pint-sized crime fighter has dream visit by Mountie in Maple Ridge**
An accidental 9-1-1 call by his baby sister ended up being a dream come true for a pint-sized Albion crime fighter. On Wednesday evening, Tara Adamyk said her husband, Mathew, turned his head for a brief moment, just long enough for their one-year-old daughter Elizabeth to grab a phone and hit buttons. Unfortunately, those buttons were 9-1-1. Although Mathew took the phone away, a 9-1-1 operator called

back, making sure everything was okay, as they are required to do in the case of miss-dialed 9-1-1 calls. MRTimes.com

*** Secrecy shrouds deaths involving officers**

In 2015, five Alberta men were shot and killed by police: one in Grande Prairie, one in Calgary, one in Edmonton, one in Morinville, and one in Red Deer. A sixth man died in Edmonton after being Tasered by police. In addition, 12 people died while in police custody. Eight were shot and seriously injured by police, and another 11 were seriously injured by police due to physical force. Those numbers come from ASIRT, the Alberta Serious Incident Response Team, which investigates all police incidents that result in serious injury or death. Not all that data are publicly available on the ASIRT website. I had to obtain if through a series of access to information requests using Alberta's Freedom of Information and Protection of Privacy Act. But despite my repeated FOIP attempts, I can't tell you the names of those who were killed or seriously injured by police in Alberta last year. Despite FOIP, Alberta Justice won't make that information public. It says it has to protect the rights of those who've died and their families. And it insists the right to privacy extends 25 years after a death. Edmonton Journal, A4

*** Canadians lost $2 million to taxpayer scam in 2016**

The national RCMP and the Canada Revenue Agency (CRA) are again warning people of the "taxpayer scam" as Canadians continue to be victimized almost daily. In a news release issued Friday, the RCMP said "pushy scammers" impersonate CRA employees and demand either personal information or payment for a made-up fee or back taxes. They threaten arrest or worse if the fee is not paid immediately. Scammers also alter parts of their story in the hopes of victimizing more Canadians. In the latest variation, scammers ask that the payment be made via iTunes cards. Times & Transcript, A10; Leader-Post

*** Online story claiming man murdered family a virus: RCMP**

A fake news article posted on Facebook, claiming that a Moncton man shot and killed his wife and four children, works as a virus when users click on it; the story will be posted to your Facebook page without your permission. Sgt. Aurele Pelletier with Codiac RCMP confirmed Friday the incident the post describes did not happen. "I'm sure if it would have happened you would have heard about it," he said. The fake article originates from a website called reportletter.com and attached is a photo of Codiac RCMP members huddled behind a car, taken by Moncton freelance photographer Marc Grandmaison for The Canadian Press following the shooting of three Moncton Mounties in 2014. Grandmaison said Friday the image was used without his permission. Times & Transcript, A3

*** Mother makes tearful plea to missing teen**

There were emotional scenes at RCMP headquarters in Regina on Friday as the mother of missing Yorkton girl Mekayla Bali spoke of her love for the daughter she has not seen in almost three months. "I feel that I have failed you in my most important role of life as your mother, because I can't protect you now," Paula Bali said as she choked back tears. "We want you to know that you are not in trouble - we are worried about you. We love you to the moon and back, and that will never change." Bali - whose 17th birthday was this week - was reported missing after failing to return from school on April 12. She was last seen at the Yorkton bus depot at 1:45 p.m., and since then rumours have swirled of sightings in Regina and Saskatoon. The net has been widened into the U.S., but police say there is no evidence she has acquired a passport. Neither can they confirm any of the sightings in either city. StarPhoenix, A7 (Leader-Post)

*** Two men are dead in Ponteix after possible murder-suicide**

Two people are dead after a possible murder-suicide in the small community of Ponteix. "We're kind of like everybody else: We don't have a lot of details. We just know it's a murder-suicide. Two people are dead right now," said Tammie Norheim, an assistant town administrator. According to an RCMP news release, officers were called to the local dump, about six kilometres east of Ponteix, at 3:45 p.m. Thursday and located two dead men. Details about what transpired at the dump have not been released and police won't say any more about the case. Ponteix is 85 kilometres south of Swift Current. StarPhoenix, A10 (National Post); Canadian Press (CTVNews.ca)

*** Oversight, watchdogs & Ontario's thin blue line**

Andrew Loku lay on the floor dead. Near his body was the hammer the 45-year-old had been holding when police pumped two bullets into his chest. His death, in the hallway of a Toronto apartment building last July, had unfolded in a matter of moments - it was five minutes from the time a neighbour called police until the fatal confrontation with police. From there, the timeline stretches out. It would be eight days before Ontario's police watchdog, in search of answers, interviewed the officer who shot Loku. It would be nine more months before the public was told what had happened. Next March, eight months from now, Ontarians will find out whether the events of that night in Toronto will prompt a fundamental change to the oversight of police forces in this province. It is change, some say, that has been years in the making. Ottawa Citizen, B1

* **Police commission facing serious financial struggles due to rising investigative costs**
The New Brunswick Police Commission is dealing with a $243,000 deficit from the previous two fiscal years due to soaring investigative costs sparked by a string of complaints against New Brunswick police officers. The commission is an independent civilian body that oversees complaints from the public involving the conduct of police officers and reviews the quality of the services provided by municipal or regional police forces within the province. It's required to perform these duties in a transparent manner, ensuring that both the complainants and the police officers who are subjected to these complaints, are treated fairly and with respect. Steve Roberge, executive director of the New Brunswick Police Commission, said the costs associated with carrying out this work has spiked in recent years, exceeding the commission's allotted annual budgets. Daily Gleaner, A3

* **Charges laid after RCMP find stolen vehicles in Sylvan Lake**
Sylvan Lake Mounties have laid charges in two separate incidents involving stolen vehicles, including one case in which a driver tried to run over an officer and another where a man jumped out of a window to elude police. In the first incident, on Wednesday, police were conducting an investigation on Sylvan Drive when they noticed a suspicious truck around the corner on Parkland Drive with front-end damage to the front driver's side wheel. Officers determined the plate did not match the 2007 black Ford F350, which had been stolen out of the Rimbey area on July 2nd, and approached the lone male occupant of the vehicle. When the man saw police, he jumped into the driver's seat, fled the scene, and tried to hit one of the members standing beside the truck. That officer was able to jump out of harm's way. The driver then continued travelling in an erratic manner with no front driver's wheel through the central Alberta town, resulting in numerous complaints made to police by the public. Calgary Herald, A8

* **Six boys accused of cyberbullying**
Six male high school students in southwestern Nova Scotia are facing charges following an investigation into complaints that intimate images of at least 20 young female students were shared online without their consent. Bridgewater Police chief John Collyer said Friday the case marks one of the first in Canada that involves federal anti-cyberbullying legislation introduced in late 2013 after the high-profile death of Nova Scotia teen Rehtaeh Parsons. The bill became law in March 2015. After complaints came in from school officials, investigators seized a number of electronic devices - mainly cellphones - and handed them to the RCMP Technological Crime Unit for analysis. Canadian Press (Waterloo Region Record, A9, The Guardian, Cape Breton Post, Chronicle-Herald, London Free Press, Toronto Sun, Kingston Whig-Standard, Times Colonist, Windsor Star, Toronto Star, StarPhoenix, National Post, Leader-Post, Montreal Gazette, Calgary Herald)

* **Regina man charged with luring young teen girls over Internet**
A Regina man accused of child luring for allegedly seeking out teenage girls on the personals section of a website has been remanded in custody. Rodney Joseph Barras, 55, made his first appearance in Regina Provincial Court on Friday on two Internet-related child exploitation charges. After Barras sought the assistance of Legal Aid, the charges were put over to Wednesday for a possible bail hearing. The Saskatchewan Internet Child Exploitation Unit - known as ICE - began investigating Barras' online activities on June 16 in connection with Internet advertisements, according to an ICE news release issued Thursday. Officers searched Barras' Regina residence that same day. The Saskatchewan ICE unit comprises members of the RCMP and the Regina, Saskatoon and Prince Albert police services. Leader-Post, A3

*** Man arrested for child porn identified**
The Kingston man who has been charged by police with multiple child pornography-related offences has been identified as Matthew V. Sears. The 47-year-old was charged Thursday after more than a month-long investigation by the Kingston Police Internet Child Exploitation unit and a tip from the American Centre for Missing and Exploited Children. The RCMP National Child Exploitation Co-ordination Centre was told by its American counterpart in May that a resident had uploaded a digital image file that appeared to contain child pornography. On Thursday morning, officers executed a search warrant at a west-end residence where they arrested the accused and also seized electronic devices and media for analysis. Kingston Whig-Standard, A6

*** Nanton man faces 13 charges after fleeing from RCMP**
A 36-year-old Nanton man faces numerous charges after allegedly fleeing from Sylvan Lake RCMP in a stolen truck on Wednesday. RCMP said an officer noticed a damaged pickup truck with a licence plate that did not match the vehicle on Parkland Drive. The driver fled in the truck when he saw police and the officer had to jump out of the way to avoid injury. Red Deer Advocate, A3

*** Mounties raid suspected chop shop**
St. Albert RCMP are investigating a potential automobile chop shop after seizing a mini John Deere excavator, a Dodge pickup truck and drugs from a rural property. Edmonton Journal, A9 (Edmonton Sun)

*** Lawyer convicted in refugee claim case**
Windsor immigration lawyer Sandra Saccucci Zaher is guilty of a criminal offence for fabricating a refugee claim, a judge ruled Friday. Zaher was also found guilty of two Immigration and Refugee Protection Act offences for misrepresenting facts in a refugee claim and helping someone to make a false claim for refugee status. Zaher's legal assistant, Diana Al-Masalkhi, who had been facing identical charges, was found not guilty. She and Al-Masalkhi were arrested at the end of an RCMP sting operation. The investigation was launched after a local lawyer tipped off police that Zaher had allegedly filed a fraudulent refugee claim for a client. The RCMP investigation involved an officer posing as a Sikh man working illegally in Canada and a second officer posing as a translator. The two men met with Zaher on several occasions and each meeting was recorded. The RCMP also tapped Zaher's phones. Windsor Star, A6

Saskatoon police chief says Dallas shooting 'felt by every member of law enforcement'
Flags at the Saskatoon police headquarters were lowered to half-mast Friday to honour officers killed Thursday night in Dallas. Five officers were killed and seven others were wounded by sniper fire at a peaceful protest. Saskatoon police Chief Clive Weighill offered his condolences to the victims, saying the shooting highlights the dangers faced by police every day. "This is a tragedy felt by every member of law enforcement, not just in the United States but north of the border as well," Weighill, who is also the president of the Canadian Association of Chiefs of Police (CACP), said in a written statement. Weighill said Canadian officers are not immune to similar violence, referring to the shooting of two RCMP officers in Spiritwood a decade ago. StarPhoenix, A3

Support pours in for police 'in harm's way'
Windsor's police chief said the horrific killing of five Dallas officers is a grim reminder of how dangerous policing work can be, anywhere and at any time. "It's a reminder that each and every day when we suit up ... that the ultimate sacrifice could be expected or required of us," said Al Frederick. Friday began with a moment of silence at Windsor Police Service headquarters for the victims of the shooting ambush late Thursday on uniformed police in Texas, which included nine other officers injured. Frederick said front-line officers would be given the opportunity to express any thoughts or bring forward concerns during the day's three shift changes. Windsor Star, A1

Préserver le lien entre population et policiers
Le directeur du Service de police de la Ville de Gatineau (SPVG), Mario Harel, estime que les événements dramatiques qui se sont produits à Dallas, aux États-Unis, ont des répercussions de son côté de la frontière. Réagissant à cette tuerie d'au moins cinq policiers de la capitale texane, mercredi soir, M. Harel affirme que le SPVG est «conscient» de la situation délicate qui prévaut aux États-Unis. «Nous sommes conscients du fait que les gens parlent de profilage racial, dit-il. Chez nous, on dit à nos

agents de ne pas en faire. On peut parler de profilage criminel, mais pas de profilage social ou racial. Le lien de confiance entre la police et la population doit être préservé.» Le Droit, 2

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Dangereux mélange de détenus à Donnacona**
Échauffourées, bagarres, agressions. La prison de Donnacona a été le théâtre de nombreux incidents violents il y a quelques semaines, dont certains ont mis en danger la vie de détenus. Ce climat d'agressivité serait lié à la décision de l'administration de fermer une aile presque vide de l'établissement et d'intégrer 23 détenus dans les autres secteurs de la prison. Selon nos sources, des bagarres ont éclaté entre les nouveaux venus et leurs confrères de rangée et au moins deux détenus ont été plus gravement blessés. L'un d'eux a été agressé dans sa cellule par quatre détenus munis d'armes artisanales et a dû être transporté à l'hôpital. Le Service correctionnel du Canada (SCC) confirme qu'un incident est survenu le 14 juin impliquant un détenu qui avait été déplacé. " Le détenu a été vu par notre personnel de soins de santé. Il a été transporté dans un hôpital externe et est revenu à l'établissement la même journée. Aucune blessure grave n'est rapportée ", a-t-on informé Le Devoir par courriel. Aux premières loges, les agents du service correctionnel disent avoir effectivement dû intervenir pour des règlements de compte entre détenus, mais aucun " incident n'est tombé en dehors de notre contrôle ", a expliqué Frédérick Lebeau, président régional pour le Québec du Syndicat des agents correctionnels du Canada (UCCO-SACC). Pour lui, il est normal que, dans les changements de cellule, " ça brasse plus ". " Ce ne sont pas des enfants de choeur, vous savez ", a-t-il indiqué. Le risque que la violence éclate est plus grand lors de changements de secteur. Car, en milieu carcéral, ne cohabite pas qui veut. Règle générale, on sépare les prisonniers qui sont incompatibles. Par exemple, les agresseurs sexuels sont dans une aile, ensemble, et les membres de gangs criminalisés rivaux sont séparés. Le Devoir, A1

*** Louise Arbour, former Supreme Court justice, calls for end of segregation in prisons**
Louise Arbour, one of Canada's most renowned jurists and a human rights champion, is calling for the end of segregation in women's prisons following the death of an inmate at a federal women's institution in Kitchener, Ont., earlier this week. "I'm just outraged," she told CBC Radio's The House host Chris Hall. Terry Baker was found unresponsive in her cell at Grand Valley Institution for Women in Kitchener, Ont., Monday evening. She had been serving a sentence for first-degree murder. The Canadian Association of Elizabeth Fry Societies said the 30-year-old had been in segregation and had attempted suicide on Monday night. Baker's death has sparked comparisons to Ashley Smith, who died in 2007 at the same facility. Arbour — a former justice of the Supreme Court and one-time UN high commissioner for human rights — led an inquiry into the women's prison in Kingston back 1996, which called for limited use of segregation. "Frankly, at this point I don't think it should be used at all," she said. "A sentence of imprisonment, the punishment is the deprivation of liberty. It's not an opportunity for further abuse ... [Segregation] is extremely, extremely damaging." CBC.ca

*** Leone granted another parole hearing**
Sex offender Carl Leone has failed in his latest attempt to get out of prison, but he'll soon get another chance. The Parole Board of Canada shot down the Windsor man's appeal of an earlier ruling that denied him day parole, which would have seen him released from prison to live at a halfway house in the community. But in the same written decision, the board's appeal division stated it is ordering another hearing because it's possible one of the panel members who rejected his bid for day parole was biased against him. Windsor Star, A3

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Marijuana industry closely watches advertising rules**
As the Liberal government prepares to introduce legislation next spring to legalize cannabis, it has asked a nine-member task force to look at what restrictions should be in place when it comes to marketing marijuana. "Since marketing, advertising and promotion of marijuana would only serve to 'normalize' it in society and encourage and increase usage, it has been proposed that these should be strictly limited so as to dampen widespread use and reduce associated harms," reads the government's discussion paper on the issue. "Limitations could include products being sold in plain packaging." That's tough for the industry to inhale. CBC.ca

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

Canada to send 450 troops, armoured vehicles to Latvia for long-haul mission
Canada is sending hundreds of troops to Latvia for the long haul. Prime Minister Justin Trudeau announced at the NATO leaders' summit in Poland on Friday that Canada will take command of a 1,000-strong multinational force in Latvia, as the alliance beefs up its presence in the Baltics and Poland in response to recent Russian actions. Speaking on the sidelines of the summit, defence chief Gen. Jonathan Vance revealed that Canada will send about 450 soldiers along with armoured vehicles to the Baltic state as part of an "enduring" NATO presence in Eastern Europe. The Canadians will form the "nucleus" of a battle group in Latvia, Vance said, that with the addition of forces from other allies, is expected to grow to about 1,000 troops. Germany, the United States and Britain are leading similar forces in Lithuania, Poland and Estonia. Canadian Press (Times & Transcript, B2, The Guardian, Cape Breton Post, Chronicle-Herald, Toronto Sun, Times Colonist, Ottawa Sun, Edmonton Sun, Calgary Sun, Hamilton Spectator, Waterloo Region Record, Toronto Star, Telegraph-Journal, Daily Gleaner); National Post (Ottawa Citizen); La Presse Canadienne (Le Droit, La Voix de l'Est, L'Acadie Nouvelle)

Canada's return to NATO's front line has air of familiarity to it
An opinion piece states, "And so Canadian soldiers are heading back to Europe. Times change and the world, despite a steady drumbeat of appalling headlines, is safer for us than for our parents. So the deployment of 450 Canadian Forces troops to Latvia won't be nearly as formidable as the deployment to West Germany - often more than 10 times larger - that was Canada's defining military commitment for 42 years through the Cold War. But the purpose is wearyingly similar." Toronto Star, A1

Russian threats spark summit
NATO leaders geared up Friday for a long-term standoff with Russia, ordering multinational troops to Poland and the three Baltic states as Moscow moves forward with its own plans to station two new divisions along its western borders. Alliance Secretary-General Jens Stoltenberg said that on the first day of a landmark two-day summit, U.S. President Barack Obama and leaders of the 27 other NATO countries also declared the initial building blocks of a ballistic missile system operationally capable, recognized cyberspace as a domain for alliance operations, committed to boosting their countries' civil

preparedness, and renewed a pledge to spend a minimum of two per cent of their national incomes on defence. Chronicle-Herald, A12

*** Le Canada promet de verser 465 M $ à l'Afghanistan**
Le Canada a annoncé qu'il verserait un soutien financier plus généreux à l'Afghanistan tandis que certains de ses alliés ont promis de maintenir leurs troupes dans le pays qui fait face à une flambée de violence actuellement. Ottawa s'est engagé à offrir 465 millions $ qui seront répartis sur trois ans, à partir de 2018 — lorsque le financement promis par l'ancien gouvernement conservateur viendra à échéance. Le premier ministre Justin Trudeau en a fait l'annonce lors d'une rencontre spéciale des dirigeants de l'OTAN qui se tenait samedi, à Varsovie, en Pologne. M. Trudeau s'était entretenu vendredi avec le président afghan, Ashraf Ghani. La Presse Canadienne (Journal Métro); Canadian Press (iPolitics.ca)

INTERNATIONAL

First shot came as dusk fell
The murderous havoc unleashed on police at an anti-racism protest in Dallas Thursday night began with sniper fire. But at least one officer died in close quarters street combat. Dramatic footage taken by a civilian on a phone shows the entrance of El Centro College from a building rooftop across the street. A man with a rifle paced by the doors, shooting in both directions at police stationed around both street corners. An officer approached, also armed with a rifle, and took shelter behind a pillar. He fired on the gunman but missed, and stepped back behind the pillar. The gunman then appeared to run a fake, charging first to the side of the pillar where the officer fired from, then shifting to his right and coming around the other side, easily shooting the officer repeatedly in the back, and continuing to fire as he fell to the ground. The gunman then left the body where it lay and rounded the corner, as gunshots, presumably from police, kick up dust from the pillars and sidewalk around him. He did not appear to be hit. Panicked hours would pass before he was cornered on the second floor of a nearby parking garage and, after failed negotiations, killed by a remote control police bomb. He had shot 12 law enforcement officers, killing five. The mayhem and panic, charged through with racial tension, threatened to further divide a country already tormented by the killings of black men by white officers, nearly all of which have gone unpunished. The Dallas protest was in response two such killings in as many days, in Louisiana and Minnesota. National Post, A2 (Leader-Post)

Dallas gunman had bomb materials
The brazen attack in downtown Dallas that killed five police officers and injured nine other people was the act of a lone gunman, an Afghanistan veteran drawn to Black Power symbology and a determination to kill white people, authorities concluded. Investigators discovered bomb-making materials, rifles and a "personal journal of combat tactics" in the home of the black former Army reservist who struck during a demonstration against the shooting of two black men by police officers in Minnesota and Louisiana. Authorities identified the gunman as Micah Xavier Johnson, 25, a Dallas-area resident, a "loner" with no criminal history who "wanted to kill white people" and "especially white officers," police said. "He appears to have been a lone gunman, and at this point, we cannot see any connections to any foreign or international terrorist organization, or any inspiration from them," Homeland Security Secretary Jeh Johnson said. LA Times (Hamilton Spectator, A10); Globe and Mail

*** Islamic State's terrifying transition**
Massacres attributed to the Islamic State have struck on four continents this year, reflecting how the appeal of the group's ideology is growing even as the territory it controls in Iraq and Syria has receded, experts say. The slaughter of civilians in three large attacks in the past week alone - in Istanbul on Tuesday, in Dhaka, Bangladesh, on Friday, and in Baghdad on Sunday - suggests militant actions beyond the caliphate's borders are taking place more frequently and not necessarily with any overt direction from some caliphate headquarters. Even more alarmingly, a growing number of attacks, starting with those in Paris and Brussels, were conducted by gangs of assailants instead of by an individual gunman. Winnipeg Free Press, D5

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Sent to: !DMS External; PS.F DL DMS F.SP; CBSA Today's News; CSC & PBC Today's News; RCMP Today's News; RCMP Today's News 2

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
July 19, 2016 / le 19 juillet 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Police cleared in Somali detainee's death
More than a year after Abdurahman Ibrahim Hassan died in immigration custody, Ontario's police watchdog has cleared the officers responsible for guarding him at a hospital from any wrongdoing. On Friday, the Special Investigations Unit said there are "no reasonable grounds" to charge the two officers, one from Peterborough police, the other from the Ontario Provincial Police, who were watching the 39-year-old man at the Peterborough Regional Health Centre where he was under medical treatment in June 2015. (…)"We can't bring Abdurahman back, but Mr. **(Public Safety Minister Ralph) Goodale** can step in and stop future deaths by ending immigration detentions now. We can't wait for another two, three years for an inquest, which may turn out nothing." Hassan's family has declined to comment on the SIU and coroner's decisions. (…) **Scott Bardsley, Goodale's spokesperson**, said the minister is working on issues related to detention and hopes to put forward proposals in public later this year. In recent months, **Goodale** has already met with the United Nations High Commissioner for Refugees, the B.C. Civil Liberties Association, the Canadian Association of Refugee Lawyers and other groups working for reform, **Bardsley** said. ***"The government will consider how to strengthen the accountability and security of all our security, including Canada Border Services Agency. Our goal is to ensure our Canadian***

approach is world-class, including our methods of enforcement, with effective transparency and accountability," he said. Toronto Star, GT2

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Green and White team up with Red Cross to help flooded communities
The Saskatchewan Roughriders have had a couple of difficult weeks, but nothing compared to their fans in flood-ravaged communities. With that in mind, the Riders are teaming up with the Red Cross to help communities in need. Starting on Monday, the Riders announced that $5 from every ticket sold for Friday's game against the Ottawa Redblacks will go to the Red Cross "to help provide assistance in cleanup efforts." On Saturday, the province said there were 623 people forced to leave their homes because of flooding. Many of them, including 576 people from the Red Earth Cree Nation, have returned home. CBC News

Nuclear oversight challenged
The Ottawa-based Canadian Nuclear Safety Commission is investigating allegations, purportedly from an internal group of specialists, that CNSC commissioners are receiving "insufficient information" to make informed safety decisions about Ontario's nuclear power plants. In an unsigned letter to CNSC president Michael Binder, copied to the Citizen, the authors say their main concern is that the nuclear watchdog's commissioners "do not receive sufficient information to make balanced judgments (...)" The letter makes specific allegations involving CNSC oversight of Ontario's Darlington and Bruce nuclear power plants. In the case of Darlington, it says that CNSC granted the operator, Ontario Power Generation, a one year licence in 2014 on the understanding that it would provide the safety case for the refurbishment of the station. Ottawa Citizen, A1/FRONT

SGI prevails despite storms and wildfires
Mild winter weather and geographic diversification helped Saskatchewan Government Insurance (SGI) to increase profits in its general insurance business, SGI Canada, while Saskatchewan Auto Fund, the mandatory automobile accident insurance plan administered by SGI, hiked rates in late 2014, boosting its rate stabilization reserve to a record high in fiscal 2015-16 (...) Increased earnings were achieved, despite $55.1 million in claim losses due to summer storms and wildfires in Northern Saskatchewan. In fact, four of the last six years have seen major weather events, like $12 million in damages from a hailstorm in Kindersley last year, that have boosted catastrophe claims well above the 10-year average of $28.2 million. Leader-Post, B6 (StarPhoenix)

Plus d'outils et une meilleure connaissance
Au cours des deux dernières décennies, ce ne sont pas les occasions de bonifier ou de corriger les interventions qui ont manqué en matière de sécurité civile. Il y a eu la crise du verglas en 1998, le bogue de l'an 2000, Septembre-2001, la grippe A (H1N1), les inondations de Rivière-au-Renard, les tragédies de Lac-Mégantic et de L'Isle-Verte, etc. «Après chaque événement, on fait un « debriefing » avec les autorités municipales et on apprend. Ce qu'on a bien fait, on le garde et on améliore ce qui a cloché», explique Éric Houde, directeur aux opérations en sécurité civile. Grâce aux avancées technologiques, les systèmes d'alerte et de prévisions météorologiques se sont améliorés. Les différents paliers de gouvernement sont mieux équipés pour communiquer rapidement entre eux, ne serait-ce que grâce aux téléphones intelligents et aux systèmes de radiocommunications. Le Quotidien, X10

Wildfire smoke advisory issued for Northwest Territories
N.W.T.'s Chief Public Health Officer has issued a wildfire smoke advisory for the entire territory, saying many communities are experiencing varying levels of poor air quality. The advisory says exposure to smoke can result in sore eyes, tears, cough and runny nose and can cause worsening of pre-existing lung and heart disease. People at higher risk include young children, pregnant women, the elderly and people with chronic conditions such as diabetes, lung or heart conditions. CBC News

Tornado warnings ended for parts of southern Alberta
Tornado warnings were issued for parts of southern Alberta on Monday, but have now been lifted. The

areas around Lethbridge, Taber and Milk river areas were under a tornado warning, as was the area around Cypress Hills Provincial Park and Foremost. Tornado watches, a lesser level than a warning, were also in place for many other areas in southern Alberta. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Crashed drone found near Parliament Hill
A downed drone found near Parliament Hill has piqued the curiosity of at least one local couple. Melissa Presz and her boyfriend Luke Brimacombe found the crashed drone in a shrub at Nepean Point, near the statue of Samuel de Champlain, which overlooks the Alexandra Bridge, and is just steps from Parliament Hill, which is considered restricted airspace. Presz and a group of friends were playing bocce at Nepean Point on Sunday when she made the startling discovery. The drone – a Phantom 4K manufactured by DJI – is no cheap toy, either. It typically retails for between $1,000 and $2,000, depending on the model. (…) Transport Canada is revamping the laws around recreational drones as the "widespread public recreational use" can create a hazard for aviation safety. In May, the military scrambled CF-18 fighter jets after a drone was spotted by two passenger planes near the Ottawa airport. Under current regulations, drones cannot be flown within nine kilometres of airports, military bases or other restricted airspaces. Parliament Hill and Rideau Hall are both listed as "restricted" in NAV Canada's Designated Airspace Handbook. Ottawa Citizen (2016-07-18)

Terrorisme : jusqu'où l'hypocrisie ?
Un article d'opinion rapporte, « il faudrait être un parfait crétin pour nier que nous sommes en guerre. C'est certes une guerre d'un type nouveau, mais c'est une guerre quand même. Quand on veut gagner une guerre, il faut une compréhension lucide de nos forces et de nos faiblesses, autant que de celles de nos ennemis. Certaines de nos faiblesses crèvent les yeux. (…) La plus évidente est certainement l'incapacité de nos dirigeants à appeler un chat un chat. On préfère multiplier les boniments insignifiants sur l'«intégration ». Comment diable voulez-vous intégrer des gens qui souhaitent vivre comme au VIIe siècle ? Comment diable voulez-vous intégrer des gens qui pensent que leur religion doit être le socle indiscuté et indiscutable du fonctionnement de toutes les sociétés ? Une autre de nos faiblesses, au moins aussi débilitante mais dont on parle moins, est l'hypocrisie de nos dirigeants ou, si vous préférez, le fait de dire le contraire de ce que l'on sait être vrai. » Journal de Montréal, 8 (Journal de Québec)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Cuban ballplayers defect in Surrey: MISSING: Two women didn't show up Sunday for game at Women's World Softball Championship
Two Cuban ballplayers disappeared Sunday from the site of the Women's World Softball Championship in what organizers have taken to be a bid to defect. The Cuban team arrived in Canada last week, before the 31-country tournament started Friday, tournament spokesperson Laura Ballance said. The team played games Friday, Saturday and Sunday nights, and the two women didn't show up for the Sunday game, Ballance said. "We've been made aware that two of the Team Cuba players are not with the team," she said Monday as the remaining Cuban players prepared for a fourth game Monday night. The tournament wraps up July 24. Tournament organizers notified Surrey RCMP about the missing players Sunday, and RCMP passed the matter on to the Canada Border Services Agency. The Cuban players all had sixmonth tourist visas allowing them to attend the tournament, so the two women weren't breaking Canadian law by not showing up for their game at Softball City in south Surrey. Tournament players were staying at area hotels and school dormitories. Ballance wouldn't say specifically where the Cuban players were housed, nor would she release the missing women's names, saying only that they were adults. Cuban officials approached by Postmedia Sunday had no comment. The Communist government of Cuba, which recently liberalized relations with the U.S., has a long history of using international athletics as a means of promoting its political system, with elite athletes treated well back home. Despite that, the country also has a long history of its athletes defecting, with Canada and the U.S. among popular destinations. The Province, A6

Brothers accused of drug smuggling to be extradited

Two B.C. brothers accused of conspiring to smuggle large quantities of cocaine and ecstasy across the border have been ordered extradited to the U.S. Oscar Edgardo Mendoza and Rember Oswaldo Guevara-Mendoza were charged after authorities seized 54 kilograms of cocaine in the United States that was destined for Canada and 59 kg of ecstasy in Canada that was headed for the U.S. The drugs were seized following an elaborate undercover operation involving police and drug enforcement officials on both sides of the border. Evidence against the brothers consisted mainly of phone and text communications they had with a man in Washington state who was, unbeknownst to them, working with law enforcement. In July 2012, after communications between the accused and the man identified only as a "confidential witness," 29 kg of cocaine destined for Canada was seized in Bellingham, Wash. Authorities replaced a suitcase full of the 29 kg of cocaine they had seized with a substance resembling cocaine. The suitcase containing the sham cocaine was then smuggled across the border and later recovered by police and drug enforcement officials at an Abbotsford home. Apparently unaware one of their shipments had been seized, the brothers continued to conspire to traffic in drugs across the border, according to evidence presented in court. Two more shipments of cocaine - 14 kg in August 2012 and another 11 kg in December 2012 - allegedly linked to the brothers were seized by police in Washington. The Province, A4

Roma family in limbo as status reviewed: Mother, daughter risk deportation to Hungary unless permit approved

A Roma mother and daughter who risk being deported back to Hungary are waiting in limbo in Montreal to find out if they will be allowed to remain in Canada. Katalin Lakatos and her daughter Gilda, 17, applied for a permanent status permit on humanitarian grounds 10 months ago. They received a temporary residence permit in May, valid for two months, as they awaited the outcome of their application. That permit expired on Saturday. "We're kind of wondering why the minister gave them a two-month reprieve if it wasn't to respond to their permanent application," said Mary Foster of Solidarity Across Borders, who has been assisting the family through the application process. The family will be allowed to stay in Canada at least until their application for a renewal of their temporary residence permit is heard. Even with the permit, Gilda isn't allowed to go to school and Katalin can't work. They applied for permits separately, Foster said, but haven't received word on whether or not they will be accepted. Half of the family was deported in March, when Gilda's father and brother were sent back to Hungary. They said systemic racism against the Roma in the European country has made it impossible to live there. If the family's permanent permit is approved, the father and brother will be allowed to return. The family arrived in Canada in 2011. Montreal Gazette, A2

Tories draw fire after push for Yazidis

As the Conservatives push for more help for Yazidis fleeing persecution at the hands of Islamic militants, new information suggests their efforts to do so while in government were minimal. Data from a controversial audit of Syrian refugee cases ordered by former Prime Minister Stephen Harper late last spring reveals that, of 546 people reviewed, three identified as Yazidi, a Kurdish minority group that practises an ancient faith. Immigration officials also told a House of Commons committee Monday that Yazidis were never highlighted specifically by the Conservatives as a group that should be prioritized for resettlement, even with their targeted approach to resettlement. The data and the testimony Monday give both the Liberal and the Tory arguments over Canada's refugee policy some new energy after the file was a political flashpoint for most of 2015. The Conservatives' areas-of-focus policy drew heavy criticism, with many arguing it flew in the face of international obligations that see the UN choose who is resettled. The Tories argued they were using the UN criteria, but were drilling down within them to ensure the most vulnerable were helped. Canadian Press (National Post, A4, Record, Ottawa Citizen); Le Droit

Airport authority, union reach agreement

The Greater Moncton International Airport and the Public Service Alliance of Canada have inked a new collective agreement with the Union of Canadian Transportation Employees after four months of negotiations with Local 60605. The union, which represents 25 full-time airport administrative, maintenance and emergency response staff as well as 16 seasonal workers responsible for winter operations such as snow cleaning and one term employee, voted in favour of ratifying the agreement on March 15. Anna Goguen, who was team lead for the union in the talks, said both sides were able to work

together and left the table happy with what they got. "At the end of the day, [this agreement] is a win-win for everyone," she said. Airport president and CEO Bernard LeBlanc said he feels very lucky the talks went as well as they did. "When we get to the negotiation and everyone knows what the workplace environment is, we can come to the table with everyone being realistic," he said. "It means we'll have stability for the next five years." The previous contract expired on Dec. 31, 2015. This one will last for the next five years and includes an 11 per cent increase over the term. The agreement marks the fifth set of contract negotiations for the union and the airport authority since 1997. Times & Transcript, A4

Injured motorcyclist's family asks driver: 'Why?'
Ron Broda's family confronted the man who seriously injured the former Saanich police officer at Ogden Point three years ago, during an emotional sentencing hearing Monday in B.C. Supreme Court. In April, Justice Jennifer Power found Eric Gosse, 58, guilty of dangerous driving causing bodily harm. Broda lost his lower left leg and suffered life-threatening injuries when he was struck by Gosse's Toyota Highlander in the July 24, 2013, crash. Gosse, a pilot-boat operator, did not take the stand during the trial. Broda, 58, was not called as a witness because he has no memory of what happened that day. Broda, who works part time as a Canada Border Services officer, was on his way to the cruise-ship terminal at Ogden Point from his home in Central Saanich the morning of the crash. "All I want to know is why," said Broda's youngest daughter, Shayla, looking at Gosse. Daughter Janelle said she was "completely shattered" by the crash and described a night of terror, praying that her father would live. "You should be held accountable. You should tell them why it happened, at least apologize," said Janelle, looking directly at Gosse. Gosse appeared to redden slightly but held their gaze. Broda himself described the emotional, physical and financial impact of the crash and talked about his own experience running over a six-year-old boy with an 18-wheeler on Blanshard Street 10 years ago. "It was the worst day of my life. I co-operated with the police investigation. I reached out to the boy's family through the police to offer my sorry for the incident and best wishes for his recovery. I say this because I know how it feels to be in a situation of being responsible for the serious injury of another person," said Broda. Times Colonist, A3

West Vancouver property developers caught in cross-country lawsuit
A wealthy West Vancouver real estate developer faces an unusual lawsuit involving a $10 million loan which was advanced in China with the key term that it must be repaid in B.C. (…) China has strict rules barring citizens from transferring more than $50,000 out of the country. In Canada, funds over $10,000 must be reported to Canada's border agents and large cash transfers must be reported to the government. As tough as China's capital flight rules are, individuals and companies attempting to transfer money into Chinese banks face equally strict rules. The Financial Times noted some investors employ "underground banks" in China which provide "matchmaking services." These institutions connect Chinese citizens who want to move money abroad with offshore investors who want to move money into China, and no money crosses borders. According to Gui Hua Chen's claim, in June 2015 she loaned Chongye $10 million with a "promissory note" that stated "the borrower promises to pay the plaintiff in British Columbia," by May 1, 2016. Interest would be 10 per cent, with $875,000 interest due to be paid in December 2015. The Province

Australia and New Zealand sign new free trade deal
Customs authorities in Australia and New Zealand have signed a Mutual Recognition Agreement that accepts each other's supply chain security programmes and provides reciprocal benefits to the other country's trusted partners. (…) At the Council sessions, the Department also formally agreed to work towards mutual recognition of respective supply chain security programmes with the Canada Border Service Agency, Hong Kong Customs and Excise and Singapore Customs. These agreements were made through the signings of Statements of Intent and Action plans. The Department also reaffirmed Authorized Economic Operator cooperation with China with the signing of the latest schedule of the Strategic Partnership Program. Lloyd List Australia

CBP relocates NEXUS center to I Falls
U.S. Customs and Border Protection Office of Field Operations has moved the CBP Trusted Traveler Enrollment Center from Fort Frances to International Falls.The International Falls Enrollment Center will continue to support the NEXUS, FAST, and Global Entry Trusted Traveler Programs. The new enrollment center will be located at the U.S. Border Patrol station located on Highway 11 east, International Falls.

NEXUS is a joint program with the Canada Border Services Agency that provides prescreened, low-risk and approved travelers faster processing by U.S. and Canadian border officials. Approved applicants are issued a photo-identification/Radio Frequency Identification enabled card, which is valid for five years. Small boat operators who are NEXUS program participants may report their arrival by telephone, but may be selected for a more extensive examination. NEXUS also benefits CBP by allowing them to focus efforts on potentially higher risk travelers, thereby facilitating the movement of trusted travelers in a more efficient and effective manner. International Falls Journal

CYBER SECURITY / CYBERSÉCURITÉ

Hongkongers warned to avoid fake websites charging high fees for travel permits to Canada
Hongkongers who are required to apply for additional electronic authorisation when travelling to Canada have been warned to stay away from fake websites which scam travellers into paying additional fees costing up to 17 times the official charge. The warning from the Canadian government was issued after it reportedly received about 500 complaints from victims who had paid unnecessary fees or from people reporting suspicious websites. A statement from the Canadian government issued on Monday said several companies have set up websites since August 1 last year, when Electronic Travel Authorisation (eTA) was first phased in, to lure travellers into paying more than the official fee of C$7 (HK$ 41.92) to provide information and submit the applications on behalf of the applicants. South China Morning Post

LAW ENFORCEMENT / APPLICATION DE LA LOI

Cops warn of selfie risks for young people
Police fighting child exploitation are calling for reinforcements: from young people and their parents. Photos and videos of crimes against children form the bulk of the imagery found in child pornographers' collections, police say. But those investigators also say the public can help stop the proliferation of some illicit images: those created by young people. Created for perhaps a boyfriend or girlfriend, the images can be stolen or distributed illegally, at times ending up in child-pornographers' vast – and widely-traded – collections. (…)The RCMP centre handles 1,000 cases a year and the caseload is increasing, he said. (…) Canadian Internet service providers (ISPs) are bound by law to report suspected child exploitation. ***"The act also calls for ISPs to safeguard evidence if they believe an offence has been committed using an Internet service that they provide,"*** **Public Safety Canada spokesman Jean-Philippe Levert** wrote in an e-mail. Peterborough Examiner (Belleville Intelligencer) (2016-07-18)

Trial almost done for Mountie accused of abusing kid
The trial of a suspended Mountie accused of chaining his 11-year-old son naked in the basement of the family home and starving him has taken a sudden turn towards wrapping up. Closing arguments in the case were scheduled to begin Monday in an Ottawa courtroom. Instead, after a behind-the-scenes meeting with Crown prosecutors and lawyers for the Mountie and the boy's stepmother, Ontario Superior Court Justice Robert Maranger agreed to accept written submissions from all parties. Crown lawyer Mike Boyce said it's not an unusual move, but one that could result in the judge reaching a verdict sooner, possibly by early fall. The one-time officer with an RCMP anti-terrorism unit, now 44, as well as the boy's stepmother, were charged in February 2013 in what Ottawa police described as one of the worst cases of abuse they had seen. The couple, who cannot be named publicly under a court order to protect the boy's identity, face charges of aggravated assault, forcible confinement and failing to provide the necessaries of life. Canadian Press (Times & Transcript, B4, Red Deer Advocate)

CRA fraudsters scam Sask. residents out of $70K in 2016
RCMP in Saskatchewan say at least 17 people have been scammed out of a total of $70,000 this year by people posing as Canada Revenue Agency agents. RCMP have received 850 calls about the scams, where the caller pretends to be a CRA agent and demands payment over the phone, according to a news release. The callers often threaten legal action - threatening seizure of assets such as homes or vehicles - if people don't directly fork over cash over the phone. The fraudsters also often "spoof" local telephone

numbers and have even been known to imitate local police officers, using rank and badge numbers. RCMP are reminding the public that the CRA would not contact people by telephone this way and are asking any victims or anyone who receives the calls to get in touch with the authorities. People should take down the number and any names the callers give, RCMP said. StarPhoenix, A7; Canadian Press (Toronto Sun, Winnipeg Sun, Edmonton Sun, Ottawa Sun, Calgary Sun, Times Colonist); Leader-Post

Suspect pulls hand gun during high-risk arrest

A suspect armed with a skateboard and a handgun has been returned to custody after a tussle with police in downtown Red Deer on Thursday. Red Deer City RCMP allege that the 38-year-old Red Deer man had been wanted on outstanding warrants when he was seen walking along 50th Avenue, near 47th Street. Police allege that the suspect tried to run off, using his skateboard to ward them off, but found himself cornered. Police allege that he then produced a handgun, but dropped it during the high-risk arrest that followed. His weapons were seized and he was taken into custody on a variety of charges: Four counts of breaching release conditions, two counts of assaulting police, possessing a weapon for a dangerous purpose, possessing a stolen weapon, careless use of a firearm, carrying a concealed firearm, unauthorized possession of a loaded, restricted firearm, uttering threats, possession of stolen property worth less than $5,000. Red Deer Advocate, A2

When the trail runs cold

It was a cold Monday night in November 2012 when Alicia Dawn Boone stepped out onto George Street in Fredericton. Boone walked toward Brunswick Street, where she was planning on meeting someone. (...) Some 14 hours later, on the afternoon of Nov. 6, 2012, a Fredericton woman went out to collect mail from her roadside community mailbox on Killarney Road and came upon the body of Alicia Boone. She was naked, lifeless and alone. Boone's death was suspicious, police say, and it's one of 27 unsolved cold cases still under investigation by the RCMP in New Brunswick highlighted in the force's recent annual report. "All the evidence has been examined through the investigation, and there were no signs of foul play," Cpl. Chantal Farrah said in 2014. "She died, like we said, of exposure to the freezing temperatures." Const. Derek Black, a spokesperson for the RCMP, told The Daily Gleaner on Friday that because these cases are still open and ongoing, the RCMP won't comment on the techniques involved in solving or investigating cold cases. "Getting into details about our procedures and process is not something we do in the public," said Black. "We never have and we won't to protect investigations and individuals involved with the investigations." The 27 cases read like a dismal history of the province, each one poignant and sad. Sometimes, though, a case is solved. For example, investigations like the Kennedy Corrigan case sometimes get solved years later by the RCMP. (...) So why does the RCMP take such care to detail these cold cases on its website? The RCMP is adamant anyone with any information should come forward and contact the police. Forensic technology has come a long way for the RCMP, but it only helps solve the puzzle if the Mounties know where to look. "Obviously we want to do a good and thorough investigation on all our cases," Black said. "Sometimes we need to reach out to the public to ask for their assistance to provide anything that will help us with our investigation."Because of law like the privacy act there is only certain information that we can release and we can't jeopardize an investigation." Times & Transcript, A10

Du crack et de l'argent comptant saisis à Saint-Jean

Une opération policière qui s'est déroulée dimanche midi à Saint-Jean a mené à l'arrestation d'un individu âgé de 55 ans qui fait désormais face à des accusations de possession de crack en vue d'en faire le trafic et de recyclage des produits de la criminalité. L'Unité intégrée des crimes de rue, composée d'agents de la GRC, de la police régionale de Kennebecasis et du Service de police de Saint-Jean, a mené l'opération policière qui s'est déroulée aux abords de l'Hôtel Best Value Inn du Canada. Munis d'un mandat de perquisition, les policiers ont procédé à l'arrestation du suspect lorsque celui-ci s'apprêtait à quitter l'hôtel qui est situé sur la place Portland, à proximité du centre-ville de Saint-Jean. L'arrestation de l'individu a mené à la saisie relativement importante de 80,2 grammes de crack et d'une somme d'argent d'un peu moins de 3000$ en devises canadiennes. «La valeur de la drogue saisie par les policiers est estimée à 16 000$, une fois écoulée dans les rues de Saint-Jean», a indiqué Lori Magee, porte-parole du Service de police de Saint-Jean. La police a également indiqué que le suspect arrêté était incarcéré en attendant de comparaître en Cour provinciale à Saint-Jean. Acadie Nouvelle, 7; Telegraph-Journal

Health authorities seek safe inhalation site after overdoses
At least 43 overdoses in Surrey's Whalley area over the weekend are being attributed to crack cocaine being laced with the deadly opioid fentanyl. And as police and health care workers scramble to warn people of the unprecedented risks they face in using crack cocaine, those on the front lines think it is time to open up a safe inhalation site. At the Vancouver Area Network of Drug Users, spokesman Hugh Lampkin said they used to have a "consumption room" for both intravenous and crack cocaine users. But three years ago the facility was closed by Vancouver Coastal Health, with Insite now the only safe-injection facility in Vancouver's Downtown Eastside. "I'd like to see a sanctioned inhalation and consumption room where they could smoke or use a needle," Lampkin said Monday. Lampkin said having a safe, properly ventilated room to smoke crack would reduce the number of fatalities. "Staff would be in there monitoring people," he said. As for the risk on the street, Lampkin said any hard drug may be laced with fentanyl. "People have to be very, very careful right now," he said. Surrey RCMP Cpl. Scotty Schumann said police and health care providers have been warning Whalley's drug users that the crack cocaine sold on the street has high levels of fentanyl in it. "What we believe is happening is the crack cocaine is being cross-contaminated at the facility where they are packaging it up," Schumann said. "A minuscule amount is enough to cause an overdose." Despite the high number of overdoses, no one has died. Postmedia Network (Vancouver Sun, A8, The Province, C-FAX 1070)

Craven crime report: Calls for service down in 2016
A widespread animal cruelty case overshadowed what RCMP said was an otherwise more law-abiding Craven Country Jamboree. RCMP said they had fewer calls for assistance at the 2016 Craven Country Jamboree than a year ago. This year, there were 114 calls for service at the Craven site, which was down from 149 in 2015. CBC News (2016-07-18)

Summer program builds bridges between police, First Nations youth
As deadly encounters increase tension between police and visible minorities in the United States, some Edmonton officers hope a summer program will help First Nations teens see them as friends, not foes. At the Oskayak Police Academy, 25 teens scramble through obstacles courses, construct and decorate traditional drums and rattles, and tramp through the brush picking plants with medicinal properties. "The thing that surprised me is, (police are) human beings, too. They strap on the belt and they go out to work and they don't know exactly what's going to happen," said 14-year-old Theron Auigbelle. For three summers, organizers have brought teens and police together for two weeks of cultural and policing activities. A partnership between several organizations, Oskayak was created to mend relations by giving First Nations youth and police a glimpse into each other's lives. The teens earn three high school credits for completing the program. "A lot of our aboriginal community members, there's a stigma. A lot of bridges have been broken. There's no trust between our people and police," said Kari Thomason, a street outreach and street prostitution program coordinator with the Metis Child and Family Services Society. She's been involved with Oskayak from the get-go. Some children's first encounter with police may be when they arrest a family member, she said. After they get to know officers in the program, teens may go home and tell their friends and family the police aren't all that bad, she said. Police, meanwhile, benefit from getting to know the kids, hearing their stories, and learning that many want to live productive lives. Dispelling stereotypes would improve relationships between minorities and police, Auigbelle said. Postmedia Network (Edmonton Journal, A1, Edmonton Sun, Calgary Herald)

Sask. gamer's guide to Pokemon Go dos and don'ts
The continuing global roll out of Pokemon Go is taking the gaming world by storm. But as more and more potential Pokemon trainers download the app, concerns of public game play etiquette increasingly grows. (...) The Kindersley RCMP expressed their concerns for Pokemon trainers through a Facebook post Monday morning. The post read, "We love PokemonGo just as much as you and if you feel the need to run around playing it this summer, that's cool, just be smart about it." The officers stated, "Always be aware of your surroundings, this also includes looking both ways before crossing the street, respecting private property at all times and not playing the game while driving." CBC News

When people target police, all bets are off
An editorial states, "Police in Baton Rouge, La., held an emotional press conference Monday, just a day after an armed-to-the-teeth gunman killed three officers and wounded three others, one of whom remains

in hospital in critical condition after taking a shot to the head. As Col. Michael Edmonson of the Louisiana State Police, Sheriff Sid Gautreaux of the East Baton Rouge Parish and Chief Carl Dabadie of the Baton Rouge Police took their turns on the podium, they would then stand behind the next one at the microphone, eyes filling or blinking hard. They looked shattered, as indeed the Royal Canadian Mounted Police appeared two years ago, when a young man named Justin Bourque deliberately drew their members to a trailer park by walking down its main street, dressed in camouflage and openly carrying a rifle and a shotgun, never even pointing either at the civilians he passed. Unwilling pawns in an ambush they couldn't conceive, some of those civilians dutifully called 911 to report what they'd seen, just as police in Baton Rouge early Sunday morning began to receive calls about "a dude with a rifle," as Edmonson put it. The traps were duly set. Ditto Gavin Long, the 29-year-old who killed Montrell Jackson, with his big heart, and Brad Garafola, who died trying to get to the wounded Matthew Gerald (Long shot Garafola first, killing him, and then finished off Gerald with two more). Long wasn't after civilians, just cops, exactly as Bourque was. Their motivations may have been different and difficult to know, but they had that in common. (…) Police may expect to be occasionally shot at by criminals, particularly those they corner or catch in mid-crime; they don't expect it of ordinary citizens, and ordinary citizens don't expect or want it, either. No one should think otherwise, either in the United States or Canada. As then-PM Stephen Harper said at the regimental funeral for the three slain Mounties way back then, which is to say in 2014, "That is the understanding between us: Their service, and our support.'" Postmedia Network (Vancouver Sun, N5 StarPhoenix, Montreal Gazette, National Post, London Free Press, Calgary Herald, Windsor Star, Leader-Post, Ottawa Citizen)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Family of man who killed himself while in solitary wants answers

A coroner's inquest began Monday into the death of a man who committed suicide while in solitary confinement at Matsqui Institution. Christopher Robert Roy, 37, died on June 3, 2015, two days after he was found hanging from a ligature in his cell in the segregation unit of the Abbotsford prison. He had been in administrative segregation for two months. The inquest is expected to last five days. "It is expected that the jury will hear evidence indicating a direct correlation between Mr. Roy's suicide and his placement in segregation," Bibhas Vaze, lawyer for Roy's parents, Robert and Brenda Roy, said in a news release. Vaze said Roy's parents are seeking answers about whether there were concerns about Roy's mental health, what efforts were made to address any mental health concerns, and whether Roy was monitored in segregation. They also want to know if the Correctional Service of Canada is making any effort to end solitary confinement. "My son was not suicidal before he was placed into solitary confinement," Robert Roy said in a release. The Province, A10 (Vancouver Sun); CBC News (2016-07-18)

Delaying learning-disabled services are costly

An opinion piece states, “Saving money on public education is like saving money by using your credit card. You've still got plenty of cash for other things, and that minimum monthly payment is not really a problem. Until it is. (…)The cost of not providing adequate remedial support during an individual's public-school career far exceeds what it might have cost to provide those services. The Learning Disabilities Association of Vancouver reports that 35 per cent of students identified with a learning disability drop out of high school, twice the rate of non-disabled peers, and up to 70 per cent of inmates in Canadian prisons are learning disabled. A 2014 news article quotes a report from Correctional Services of Canada that estimated the cost in Canada of one year of incarceration for one person is $117,788, up 46 per cent from a decade ago.” Times Colonist, A10

Un meurtrier confiné en maison de transition

Le jeune homme condamné à cinq ans de pénitencier pour avoir causé la mort de son ami lors d'une beuverie qui a mal tourné au centre-ville de Jonquière en 2012 a récemment obtenu une semiliberté conditionnelle. Incarcéré depuis le 23 janvier 2015, Maxime Pelletier a pris le chemin d'une maison de transition le 6 juillet dernier après avoir reçu l'aval de la Commission des libérations conditionnelles du Canada. Celle-ci lui a octroyé une semi-liberté de quatre mois au cours de laquelle il devra éviter de consommer de l'alcool et des drogues en plus de se tenir loin des débits de boissons. Il pourra ensuite profiter d'une liberté conditionnelle complète par la suite. (…)Dans sa décision, la Commission des

libérations conditionnelles indique que Maxime Pelletier ne représente pas un risque pour la société et présente un potentiel de réinsertion élevé. Il a eu un comportement irréprochable depuis le début de son incarcération en janvier 2015. Journal de Québec, 2

Murder suspect 'no threat'
Parole board documents say a man accused of killing a Calgary mother and daughter had a 20-year criminal history but didn't pose a threat to society when he was granted full parole in 2010. Edward Delten Downey is facing two counts of first-degree murder in the deaths of Sara Baillie and her five-year-old daughter Taliyah Marsman. The 34-year-old waitress was found dead in her home on July 11 and an Amber Alert was issued for the little girl. Police found Taliyah's body late Thursday in a rural area just east of Calgary. Downey had not retained a lawyer when he was charged and is scheduled to appear in court Wednesday. None of the charges against him has been proven in court. Documents from the Parole Board of Canada granting Downey full parole in 2010 say the 46-yearold's criminal history began in 1990 with a series of convictions including possession of a credit card obtained by crime and possession of a restricted weapon. "It is evident that you have been involved in criminal activity over the years; however, it has been sporadic at times," said the parole board report dated May 2010. Canadian Press (Calgary Herald, A1, Edmonton Sun, Times Colonist, Calgary Sun, Edmonton Journal, Maclean's, National Post, Red Deer Advocate, Western Star, Prince Albert Daily Herald); Globe and Mail; Radio-Canada; CBC News

Il ne «se considère pas pédophile» malgré 26 ans de tourisme sexuel
Un octogénaire ayant fait du tourisme sexuel en République dominicaine pendant 26 ans ne croit toujours pas qu'il a une déviance, après plus de trois ans en prison. «Ce n'est pas une maladie que j'ai. C'est arrivé comme ça», a lancé d'emblée Joseph-Charles Côté, lors d'une audience des libérations conditionnelles. Condamné à sept ans de pénitencier en décembre 2014, le détenu de 85 ans a tenté en vain d'obtenir la permission de quitter le Centre fédéral de formation de Laval, hier. «Le risque de récidive est encore présent, autant pour les contacts sexuels sur des mineurs que la pornographie juvénile, ont statué les commissaires Michel Lafrenière et Richard Dupuis. Vu l'absence de changement et de progrès de votre part, une libération conditionnelle serait prématurée.» Journal de Montréal, 9 (Journal de Québec)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Sask. crime rate declined over decade, but many think it's rising
The long-term crime trend in Saskatchewan and the other provinces is downward — but public perception appears to be going the other way, an Angus Reid poll says. According to a recent survey by the pollster, 56 per cent of people surveyed in Saskatchewan say there has been an increase in crime in the province over the past five years or so. However, according to Statistics Canada, the evidence points the other way. The federal statistics agency produces a crime severity index report, which looks at numbers per capita but also factors in the severity of the crimes reported. StatsCan's most recent report on the index showed that from 2004 to 2014, there was a decline in all provinces, including Saskatchewan. However, Saskatchewan is the province with the highest crime severity index. CBC News (2016-07-18)

Black Lives Matter rally posters torn down in Peterborough
There's going to be a Black Lives Matter rally in Peterborough on Friday at 4 p.m. People will be invited to gather at Confederation Square to come and hear speakers such as Stephen Wright, the only black candidate to run for council in the last municipal election. You might not have seen much publicity, though. The organizers - Charmaine Magumbe and Niambi Leigh - say the posters downtown get ripped away by people as fast as they can post them. Why the vandalism? "Racism is real and alive - in Peterborough and everywhere," says Magumbe. Black Lives Matter is a grassroots movement that campaigns against violence toward black people. The movement has been around since 2013. Since then, participants have demonstrated against the deaths of several African-Americans in the U.S. by police action or while in custody of police. Magumbe, the chairwoman of the city's race relations

committee, got the local movement started here almost as soon as BLM began in the U.S. This will be the third local rally. Peterborough Examiner

James Forcillo Appeals Conviction in the Killing of Sammy Yatim
An opinion piece states, "Constable James Forcillo, the police officer who shot and killed Sammy Yatim on a TTC streetcar on July 27th, 2013 is now asking that his sentence be served under house-arrest instead of facing jail time. Constable Forcillo was convicted of attempted murder on January 25th, 2016. The fact that Forcillo was actually convicted, even of the lesser offence of attempted murder instead of second-degree murder, has surprised many. In the 23 year old history of the Special Investigations Unit (SIU), Forcillo is only the second cop in Toronto to be charged for murder. He is the first to ever be found guilty of even so much as a related charge. This exceptional event in the history of police self-investigations can be explained as a result of the public backlash against the police." Fightback

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Government's call for Manitoba commissioner on inquiry not a deal-breaker
Premier Brian Pallister says it's not an 'either or,' that a Manitoba commissioner be appointed to the inquiry into missing and murdered Indigenous women, but says it would be a "missed opportunity" if it didn't happen. The premier was responding to questions that the start to the MMIW inquiry was being delayed because of issues raised by Manitoba's Progressive Conservative government. The province is still in negotiations with the federal government over the terms of reference for the inquiry. Pallister and other Canadian premiers will meet the leaders of the five national Aboriginal organizations in Haines Junction, Yukon on July 20. Pallister says Manitoba has spent millions of dollars looking into issues such as the province's child welfare system's failure to protect Phoenix Sinclair and Brian Sinclair's 34 hour wait in a hospital emergency room. "Millions of dollars of money have been invested on behalf of taxpayers here in Manitoba to address finding solutions to these issues; curative solutions. That kind of healing has to happen nationally. Why wouldn't we want to benefit the country from our work?" Pallister said. Pallister told CBC News its imperative the MMIW inquiry doesn't "till the same fields again and again," and says he's been told the inquiry can't overlook work that is ongoing. "Indigenous people and non-Indigenous people are telling me and they are telling our members of the Legislature; our cabinet ministers, don't use this inquiry as a catch-all- as an excuse to delay other initiatives and other actions that have to be taken. Make sure you walk and chew gum at the same time here," Pallister said. Pallister says Manitoba can take a lead role both at the inquiry and when looking for solutions to problems facing Indigenous people. CBC News

Drag the Red sets out on new boat to search fast-moving waters
Behind weeds growing from the riverbank and in the heat of mid-July, Kyle Kematch unwinds rope from a four foot-wide bar to attach to Drag the Red's new boat. He is one of few community members that volunteer their time to drag the Red River for traces of missing and murdered people. "It eases my mind to know I'm doing the best to find my sister. She's been missing for six years now," he said. "In my eyes, everybody deserves to go home." The return home Kematch describes is synonymous with closure for families — particularly those with loved ones among 1,017 Indigenous women killed between 1980 and 2012 and 169 more listed as missing, the earliest case dating back to 1952. The new boat, which an Indigenous elder blessed in a smudging ceremony on Monday, brings about renewed hope that families will get that closure, Kematch said. "It's hard knowing those answers might be at the bottom of the river but if they're there, somebody has to go and try to find them," he said. CBC News (2016-07-18)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Marijuana task force faces 'fascinating journey' in making regulation decisions

Mark Ware was working with patients suffering from a painful blood disease in the late 1990s when he noticed that many of them were self-medicating. The sickle cell anemia research clinic where he was working was in Jamaica, and the pain reliever of choice for a growing number of his patients was cannabis. The episode put the Britishborn, Jamaica-raised doctor on the path that has made him a world-renowned expert on the use of cannabis in pain management. Now based at McGill University in Montreal, Dr. Ware will turn his attention in coming months to the use of marijuana for recreational purposes. As a key member of a new task force, he will help the federal government to create a legal regime for all adult pot users. "The next six months will be a fascinating journey in understanding a different aspect of cannabis regulation than the medical model," he said recently in his first media interview since being named vice-chair of the task force. The government called on former Liberal cabinet minister Anne McLellan last month to lead a nine-member task force on marijuana legalization and regulation. She was hired because of her political knowhow and the expertise she gained as a minister of health, justice and public safety in the 1990s and 2000s. The panel will provide its findings to the government and the public by November, with new legislation to come in the spring of 2017. Dr. Ware, who was brought in as one of Canada's foremost experts on the science behind marijuana, said he does not believe that cannabis is a "panacea" as a medical drug. He also said there should be strict controls on the quality and potency of recreational marijuana, especially as Canada starts research on the long-term impact of legalization. "Under a regulated, nonmedical model, the opportunity stands to learn in a much more informed way what is the true picture of cannabis use and its impact on health," Dr. Ware said. Globe and Mail, A4

Osoyoos debates banning all marijuana operations

Osoyoos boasts of having 'Canada's warmest welcome,' but not when it comes to marijuana retail shops. Instead those may continue getting a cold reception as the town considers passing a bylaw that would ban marijuana operations. A the last council meeting, mayor and council were split on the proposal. But in a 3-2 vote, they approved the initial readings of the bylaw. "If this bylaw gets passed, I don't think it is incredibly harmful, I just don't personally think it is necessary," said councillor Mike Campol, who voted against. "We have the right to refuse business licenses and the RCMP are, and have been, doing a great job with dealing with what we've been faced now with dispensaries trying to open here." The town said there's been growing business interests from marijuana dispensary owners. So it sought legal counsel, which recommended implementing a new zoning bylaw amendment. The town said this would be a 'short-term, interim measure' as officials wait for the federal government to introduce new regulations that would impact marijuana dispensaries. "Just because any zoning bylaw can be changed any time, it is just my feeling that we're discouraging something that we don't completely understand," Campol said. On Monday, people will be able to provide input at a public hearing before the issue goes for a third hearing. Global News (2016-07-18)

PUBLIC SERVICE / FONCTION PUBLIQUE

80 000 fonctionnaires touchés

Les témoignages se multipliaient et les différents syndicats de la fonction publique sonnaient l'alarme depuis plusieurs semaines. Lundi, Travaux publics et Services gouvernementaux Canada a confirmé l'ampleur des problèmes liés à l'implantation du système de paie Phénix. Au total, ce sont plus de 80000 fonctionnaires qui ont été touchés, d'une manière ou d'une autre, a confirmé la sous-ministre, Marie Lemay. «Je suis profondément inquiète de cette situation», affirmait Mme Lemay d'entrée de jeu lors d'une conférence de presse visant à faire le point sur les ratés de Phénix. «Cette situation est inacceptable et nous allons travailler sans relâche pour résoudre cette situation.» (...)Le vice-président exécutif régional de l'Alliance de la fonction publique du Canada, Larry Rousseau, se dit satisfait de voir le gouvernement admettre l'ampleur des problèmes liés à l'implantation de Phénix. M. Rousseau est toutefois sceptique quant à la capacité de Travaux publics et Services gouvernementaux Canada de rembourser rapidement tous les employés qui n'ont pas été payés à la hauteur de leur travail, malgré l'annonce de l'embauche d'employés supplémentaires à Miramichi et Gatineau pour résoudre la crise. «D'après moi, ce sera un travail de longue haleine», dit-il. La Presse Canadienne (Le Droit, 3); Postmedia Network (Ottawa Citizen, Times and Transcripts) La Tribune; Globe and Mail

StatsCan says government's IT agency providing 'slower, lower quality services'
Setbacks and shortcomings at the federal government's tech support agency could delay Statistics Canada's release of "mission critical" information required by the Bank of Canada, Department of Finance and commercial banks, according to a report. The document, submitted to Canada's chief statistician Wayne Smith, is one among more than a dozen reports, drafted at Smith's request from all of his directors general. Smith asked for the reports in an effort to fully understand the impact of Shared Services Canada (SSC) on his department. The memos, obtained by CBC News under access to information laws, detail how yet another federal ministry is embroiled in a dispute with SSC over services standards, red tape, billing and the capacity of IT infrastructure to keep up with departmental demands. CBC News

Salaries won't solve public servant crisis
If you don't already work for the public service, what would it take to get you to jump ship from your current gig and head for the sunny shores of government? The Professional Institute of the Public service of Canada is betting on money, asking for an ambitious 12 per cent raise over three years for the professional government employees it represents. The reason, apparently, is that salaries of federal government professionals are outstripped by the private sector. Crank up that pay cheque, and the employees will come. This is important, considering more than 25,000 of these folks will be looking to retire in the next five years. To modify the union's pitch slightly: Raise the salaries and the millennials will come. The concern is that the positions, at lower salaries, will still doubtless be filled, but the best and brightest will stay away unless compensated. There might be truth to that. But for a generation struggling with labour instability, the public service is already a relatively attractive employer. There are solid benefits, decent wages and long-term employment stability. Is money a factor? No doubt, but there are many other issues at play, including workplace culture; the public service has alarmingly high rates of depression and anxiety. Who wants to walk into that job? A salary hike is unlikely to compensate for these troubling issues. Postmedia Network (London Free Press, A5, Kingston Whig-Standard)

OTHER / AUTRE

The uncomfortable lesson of Nice and terrorism
Like magicians, spies are adept at creating illusions. Arguably, their biggest, most impressive trick, is convincing people they exist primarily to protect us from the infinitesimal prospect that we may, at some point in our lives, fall victim to terror. (Truth is, as whistleblower Edward Snowden and WikiLeaks have revealed, their most important job is, in fact, to spy on you and each other.) Of course, despite the tragic, unsettling times, the chances of you, me or our families being killed or maimed by a terrorist are still so remote that we are more likely to succumb to a rare brain infection than die at the murderous hands of a deranged zealot - whatever their equally deranged cause or motivation. But the fear industry, which undeniably includes the so-called "intelligence community" and their allies, enthusiastically gives sustenance to these irrational fears, rather than dampen them because it's in their institutional interest to do so. No matter. For interim Conservative leader, Rona Ambrose, the response to the mayhem in Nice was to rush onto Twitter and urge Canadians to "get serious" about terrorism. By employing this tired, meaningless bromide, Ambrose has confirmed yet again that she's more interested in cheap sloganeering than, you know, thinking. (…) One scribe suggested that the official response to Nice required "real and determined leadership." I have no idea what that tripe means, but it's intended, I suspect, to sound like we're doing something. Another high-profile pundit insisted, in effect, that Canada and the world should belatedly declare perpetual war. I don't know about you, but it certainly appears to me that the world is already in a state of perpetual war and has been for some time. Have the attacks miraculously stopped? Toronto Star, A11

Why France, over and over
An opinion piece states "On Bastille Day 2015, my family and I walked over to the banks of the Saône River in Lyon to watch the fireworks with thousands of the city's residents. I only briefly noticed the metal barricades blocking the street set up next to the french fry stands. France was still recovering from the Charlie Hebdo and Hyper Cacher massacres. The Lyon region had just been the site of a decapitation and a truck-based attack on a gas factory. In previous years, there had been attacks in cities such as Toulouse, Tours, Dijon and Nantes. But most were aimed at Jews or members of the police or military.

Most people in France still felt safe from direct violence. The events in Nice are a horrific reminder that, in reality, everyone in France is a target. While it is not the only country in the region to have experienced terrorist acts in recent years, France has suffered more frequently than neighbours like Britain, (...) The answer lies in three factors: the country's foreign and domestic policies, history and demography, and approach to citizenship and immigrant integration. The individual factors are not unique to France. It is the combination that makes France a focal point for violence." National Post

INTERNATIONAL

Attentat de Nice - Le profil "radical" du tueur se précise

Le tueur de Nice a marqué " un intérêt certain " pour le djihadisme dans les semaines précédant son carnage méticuleusement préparé, selon l'enquête sur l'attentat du 14 juillet, autour duquel le climat politique s'envenime en France. Quatre jours après l'attaque, la plus meurtrière en Europe depuis les attentats du 13 novembre à Paris et du 22 mars à Bruxelles, l'opposition de droite a réclamé lundi soir une commission d'enquête parlementaire sur la tragédie de la capitale de la Côte d'Azur. Dans la journée, le premier ministre socialiste, Manuel Valls, a été visé par quelques huées à Nice. L'exécutif se prépare à un débat houleux mardi et mercredi à l'Assemblée nationale puis au Sénat sur la prolongation de l'état d'urgence en vigueur depuis huit mois dans le pays. Si le tueur de Nice a été adoubé par le groupe État islamique (EI), qui a revendiqué l'attaque, " aucun élément de l'enquête ne démontre à ce stade une allégeance de Mohamed Lahouaiej Bouhlel à l'organisation terroriste ", a déclaré lundi le procureur de Paris, François Molins. Le magistrat, qui chapeaute l'enquête, a souligné en revanche que " l'exploitation de son ordinateur illustre un intérêt certain et récent pour la mouvance djihadiste radicale ". Ce Tunisien de 31 ans résidant à Nice depuis une dizaine d'années a ainsi multiplié entre le 1er et le 13 juillet les recherches de chants religieux utilisés comme outils de propagande par le groupe État islamique. La Presse canadienne (Le Devoir, A5)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
July 20, 2016 / le 20 juillet 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Canada's electronic spy agency won't reveal if shared info leads to torture overseas
Canada's electronic spy agency won't say how often it shares information that could lead to someone being tortured in an overseas prison. The Communications Security Establishment – which monitors threats from foreign terrorists and spies – has censored documents that spell out the figures, even though the RCMP and Canadian Security Intelligence Service have revealed such numbers in the past. The reticence prompted Amnesty International Canada to say "much greater transparency" is needed from the Ottawa-based CSE. "At stake is Canada's compliance with crucial international human rights obligations to prevent torture and ill-treatment," said Alex Neve, Amnesty's Canadian secretary general. The secretive CSE has been thrust into the national spotlight in recent years due to leaks by Edward Snowden, the former spy contractor who worked for the National Security Agency, CSE's American counterpart. It is also among a handful of Canadian agencies, including the RCMP, CSIS, the Canada Border Services Agency and National Defence, bound by a government instruction that allows it to share information with foreign partners – even when it means someone could be abused as a result of that exchange. **Public Safety Minister Ralph Goodale** said earlier this year the Liberals will review the

"troubling set of issues" raised by the foreign-sharing policy, enacted by the previous Conservative government. Canadian Press (Global News, News Review, Times Colonist, CTV News)

Protesters have Goodale listening
Controversy followed the federal **public safety minister** - right into the University of Regina. As **Ralph Goodale** rose to announce a bundle of research grants for U of R researchers, a small group of protesters from the Colonialism No More camp in downtown Regina appeared and unfurled a banner restating their opposition to the government's continuing use of detention for some people arriving in Canada. People in two Ontario federal detention centres recently began refusing food because they want to meet with **Goodale** about their imprisonment and conditions. Tuesday's protesters were polite, waiting until other speakers had finished, and presenting themselves only when **Goodale** began talking to reporters - and even then at low volume. Within minutes, **Goodale** was talking to them and agreeing to meet, a plan confirmed by his office later Tuesday. Coincidentally, his office had sent out a statement earlier Tuesday in which **Goodale** said only 400 persons - or about 0.01 per cent of all arrivals - are detained, as a last response, when there are problems identifying them with certainty, or because they are deemed a flight risk or to ***"threaten the safety of Canadians."*** He said they are given ***"immediate and regular legal review"*** by the independent Immigration and Refugee Board and have access to health, spiritual and legal help, plus visits by the UN High Commission for Refugees and the Red Cross. And though more money is needed to improve their lot even more, he hopes "to make specific announcements in the future." Leader-Post, A2

Winter traffic safety among U of R studies to get federal funding
Before Babrak Mehran came to Regina from balmy Ontario, he didn't know what a block heater was. But the assistant professor of environmental engineering at the U of R has thrown himself so thoroughly into his new home that he's studying traffic safety in winter and how to improve it. Insight into drivers' behaviour, speed limits that change with the weather via networked signs, amber lights that stay on longer (or shorter) because of the weather, and lane markings that are easier to see. They're all things that could emerge from his work, with possible testing on the South Regina Bypass, he said after a news conference announcing federal grants totalling $1.57 million to 16 U of R research projects at the University of Regina. These projects are in fields as varied as biology, physics, math and engineering ***"and will undoubtedly produce the next generation of smart, new ideas that will make the economy stronger and more successful,"*** said the man who brought the federal money, cabinet **minister Ralph Goodale**. Emphasizing the difference between fundamental science and ***"applied science",*** which he described as typically guided more by private interests than by a researcher's curiosity, he recalled what happened just over a halfcentury ago. Leader-Post, A2

Liberals promise plan to bolster emergency preparedness as extreme weather events surge
The Trudeau government says it will reach out to provincial, municipal and territorial governments and indigenous communities to improve disaster preparedness planning amid concerns that extreme weather events will become more frequent and severe in the coming years because of climate change. **Scott Bardsley**, **spokesperson to Public Safety Minister Ralph Goodale** (Regina-Wascana, Sask.), said department officials will work collaboratively with partners to help better ***"predict, prepare for, and respond to"*** weather-related emergencies and natural disasters. ***"Our government is determined to pay greater attention to emergency planning, preparedness and response, and that work is underway,"*** he said in an emailed message. Mr. Bardsley also noted that disaster mitigation and aid plans were major discussion points during the May 6 meeting of federal, provincial and territorial ministers responsible for emergency management. Hill Times

Reports could hide true police activity
"Clear gaps" in how the federal government reports invasive surveillance practices may hide the true scope of police activities, according to documents prepared for Canada's privacy watchdog. Although the number of authorized wiretaps has "plummeted" since 2002, a January briefing for Privacy Commissioner Daniel Therrien suggests those numbers may mask police surveillance practices. "It would be erroneous to infer from the drop in overall warrants issued that surveillance is affecting fewer individuals," reads the document, obtained under access to information law. "While federal authorities issued just over a hundred surveillance warrants last year (2014), they issued 792 notifications of surveillance to individuals

previously targeted. From this, one can conclude more and more individuals are being named as targets in a warrant application. "With a single warrant from the Federal Court (police) may list dozens of individuals for surveillance targeting." Public Safety is required to issue a report each year about the number of warrants sought to put individuals under surveillance - "wiretap" warrants that allow police extraordinary powers to keep tabs on individuals. (...) Canada has also seen confirmed uses of "Stingray" technology, a device, called an IMSI catcher, that simulates a cellphone tower to force any mobile device in the area to connect to it. A recent Vice News investigation reported the RCMP has used IMSI catchers in public places for more than a decade, citing court documents. The Star requested an interview with both Therrien and **Public Safety Minister Ralph Goodale** for this article. Neither was available Wednesday or Thursday. But in an emailed response to the Star, a **spokesman for Goodale** said the minister is open to changing the system. Guardian, A6 (Whitehorse Daily Star)

Howard Sapers urges legal limits on prison segregation

Canada's prison watchdog is calling for tighter legal restrictions and greater oversight over solitary confinement as two more cases of suicide in segregation hit the spotlight. Howard Sapers, Canada's correctional investigator, said he is "very concerned" that the circumstances around these deaths in custody had similar elements as those flagged years ago in the high-profile inquest into the death of teen prisoner Ashley Smith. "Simply leaving it to the Correctional Service of Canada (CSC) within the existing legal and policy framework is not producing an adequate response," he told CBC News. An inquest into the suicide death of 37-year-old Christopher Roy at British Columbia's Matsqui Institution began Monday — just weeks after 30-year-old Terry Baker took her own life at Grand Valley Institution for Women in Kitchener, Ont. That's the same facility where Smith died in a segregated prison cell in 2007. A coroner's jury ruled that her self-inflicted choking death was a homicide and made 104 recommendations to prevent similar deaths in future. (...) A spokesman for **Public Safety Minister Ralph Goodale**, who oversees Canada's prison system, said the government is making progress but promises to do more. Scott Bardsley said a framework developed by CSC in 2015 that strengthens rules and decision-making around placement and review has led to a "significant decrease" in the number of inmates in segregation. There was a 34 per cent decrease in the number of people in segregation in federal prisons last year. In March, there were 691 inmates in administrative segregation, compared to 454 in December, Bardsley said. There was also a 52 per cent decrease in the number of inmates in administrative segregation for 60 days or less. "***The government recognizes that the challenges raised by these issues are complex and require careful consideration,"*** Bardsley said. ***"We can and must do better. We will continue to strengthen the review process to ensure that alternatives to administrative segregation are considered for all offenders.***" CBC News

Time to fix a broken system

A hunger strike is a choice of last resort, something only the desperate attempt to draw attention to their plight. So we should listen to the message coming from 50 immigration detainees being held at the Toronto East Detention Centre in Scarborough and the Central East Correctional Centre in Lindsay, Ont. They have been on a hunger strike for more than a week to press their demand that they no longer be held indefinitely in facilities intended for criminals. Their health may already be threatened. According to scientific studies, by now they will have lost muscle mass and fat; important electrolytes, such as potassium, will have fallen to dangerous levels. But according to an advocacy group called the End Immigration Detention Network, they are intent on starving themselves until **Public Safety Minister Ralph Goodale** meets their demands. **Goodale** needs to resolve this situation urgently. The detainees are not alone in saying they should not be held indefinitely in maximum security prisons, in conditions that include lengthy lockdowns and solitary confinement. They are being supported by a host of organizations, including the United Nations, the Ontario Human Rights Commission, Amnesty International, the Canadian Council for Refugees and a group of 140 health-care professionals. As the University of Toronto's International Human Rights Program has said, housing immigration detainees in facilities intended for criminals violates international human rights law and constitutes "arbitrary detention and cruel, inhuman and degrading treatment." Still, it is all too common in Canada. Indeed, in 2013-14 the Canada Border Services Agency (CBSA) detained 10,088 migrants, with a third being held in provincial jails, even if they posed no danger to society. They may simply be failed refugee claimants, people without documents or those who have had their resident status revoked. Toronto Star, A10 (Our Windsor)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Busy agenda for Notley at premiers' meeting in Yukon
Premier Rachel Notley is scheduled to be in Whitehorse, Yukon, on Wednesday for the annual Council of the Federation meeting. Emma Graney looks at five items on the agenda (…) With memories of the Fort Mc-Murray wildfire still fresh, Notley added natural disaster preparedness to the meeting's agenda. Floods and fires affect all provinces, she said, and come with huge cost implications for all Canadians. Notley wants premiers to lobby the federal government for changes to the disaster relief program. Postmedia (Calgary Herald, A5; Edmonton Journal, Edmonton Sun); Canadian Press (St. John's Telegram); Radio-Canada

Atikamekw chief disillusioned by federal appeal
As the 2015 federal election campaign reached its climax in October, Christian Awashish was one of the few Quebec aboriginal chiefs to endorse a political party. The chief of Opitciwan's Atikamekw nation backed Justin Trudeau's Liberals because he believed they would fundamentally change the relationship between Canada and its indigenous people. Awashish says he now regrets that decision. Last month, the federal government appealed a tribunal ruling that would have awarded millions to the Atikamekw in Opitciwan - a First Nations reserve on the shores of the Gouin Reservoir (…) The legal decision could have granted the impoverished First Nation of 2,000 residents up to $150 million in compensation for flooding, contaminated drinking water and other damage caused by the creation of La Loutre dam in 1918 (…) The Liberals were swept into power in 2015 on a promise to help lift First Nations out of poverty, address historical injustices and speed up land claims negotiations. In their short time in government, they've committed to billions in new spending on education, housing and infrastructure on reserves. So when Judge Johanne Mainville of the Specific Claims Tribunal ruled on May 20 that the federal government failed in its duties to protect the Atikamekw from flooding and didn't properly compensate them for losing their homes as well as hunting and trapping revenue, Awashish was hopeful the government would "do the honourable thing." Postmedia (Montreal Gazette, A2; Kingston Whig-Standard, London Free Press, Vancouver Sun, Edmonton Journal)

Many Fort McMurray businesses struggle with serious lack of staff
Serving a beer within five minutes can be quite an accomplishment for some Fort Mc-Murray bars these days. It certainly was during the first few weeks of June at the East Village Pub. As the first restaurant to open following the wildfire, crowds usually seen on St. Patrick's Day became a daily occurrence. Yet, five kitchen and serving staff announced they were not returning. Others said they needed time to themselves before they could return to work. "We were the only place for people to come and the crowds reflected that," said Mike Lambert, the Eagle Ridge bar's manager (…)The Canadian Red Cross is offering financial relief to small businesses of up to $1,000, but Tatum said that only goes so far. Few employers, including Tatum, can afford the incentives of the halcyon boom days such as covering the first month's rent or travel expenses. Others have learned their commercial insurance policy does not include interruption coverage, which covers lost revenue during a disaster. Bryce Kumka, president of the Fort McMurray Chamber of Commerce, worries how a lagging economy will hit the staff, especially ones at businesses already struggling. Edmonton Journal, A2 (Edmonton Sun)

Tree Canada commits to Fort McMurray effort
After visiting the scorched areas of the Wood Buffalo region, Tree Canada is now committed to helping Fort McMurray rejuvenate its urban foliage. Following a helicopter tour of the area July 14, Tree Canada president Michael Rosen met with city officials, including Wood Buffalo Mayor Melissa Blake and urban forestry planner Stephen Fudge, to discuss how to go about replanting the 10,000 urban trees that the city lost during the wildfire. "Fire is a natural part of the boreal forest, so it regenerates naturally quite well," said Rosen, explaining why they won't be replanting trees in rural areas. "So we're looking more at people's residences, like the 2,000-plus homes that actually burnt. We're trying to give them that sense of normalcy when they finally come back and build their new homes." Postmedia (Edmonton Journal, A11; StarPhoenix)

'Last hurrah' of tsunami cash helps scour province's coast
A co-ordinated marine-debris cleanup described as the largest in Canadian history is underway all along B.C.'s west coast, from the remote wave-tossed beaches of Cape Scott and Haida Gwaii to the tourist-heavy Pacific Rim National Park Reserve. It is largely funded by the last of a $1-million package provided by the Japanese government in 2012 for tsunami debris cleanup in B.C. "This is the last hurrah," confirmed Karen Wristen, executivedirector of Living Oceans Society, the conservation group co-ordinating the effort on the western coast of Vancouver Island. "It will be the largest marine debris cleanup operation ever undertaken in Canada." Vancouver Sun, A1/FRONT

City to hire expert on climate change to help with future planning
With extreme weather patterns affecting both day-to-day operations and planning for the city, Calgary officials are looking to hire a fulltime climate change expert to better adapt to changing conditions. A job posting by the City of Calgary's water resources department says the climate change engineer will assess potential climate change risks for future infrastructure projects, as well as analyze any potential impact of climate change. Frank Frigo, senior planning engineer with water resources, said there's growing awareness about how climate change can affect city operations and it makes sense to have expertise when making decisions on new projects and ongoing operations. Calgary Herald, A6

Flood damage shifts SGI facility in Estevan, Sask., to temporary location
The SGI facility in Estevan, Sask. is moving to a temporary location after heavy rains and flash flooding damaged its building. The southeastern city of about 11,000 received 130 millimetres of rain on July 10. And while repairs are underway, claims, licence issuing, and driver examiner services are moving to 1210 7th St. The staff had previously been working out of the Estevan Claims Centre garage and at partner insurance broker offices. CBC News (2016-07-19)

Gloomy weather a mixed blessing for B.C.
Not everyone's feeling blue about B.C.'s recent grey skies. By Monday, 32.8 millimetres of rain had fallen at Vancouver airport this month, compared to last year's 1.4 mm, says Matt MacDonald, a meteorologist with Environment Canada. Vancouver had 11 days of rain by July 19, nearly twice the normal average of six days. Temperatures were about a degree cooler than normal, with an average high around 21.3 C. But this miserable month has so far proven a mixed blessing for the province. The rain has caused a downturn in wildfire activity after an early and active start to the season, particularly in northeastern B.C., said Claire Allen, an information officer with the B.C. Wildfire Service. "That's definitely slowed down with the June rains and with that kind of continuing into the July rains," said Allen, adding the fire danger rating is "significantly lower" than last season. This year, 545 wildfires burned 93,612 hectares by July 18, compared with the 1,141 wildfires that burned 293,664 hectares during the same period last year. Vancouver Province, A8

Baseball sized hail, tornado warning issued for south central Sask.
A tornado warning is in effect for the rural municipalities of Arm River and Willner, including Davidson and Girvin, Sask. According to Environment Canada, a sighting of a tornado was reported near Davidson at about 8:20 p.m. CST. A severe thunderstorm is moving east to southeast at 50 km/h. The weather agency warns that extreme hail the size of baseballs or larger are also possible along with damaging winds and intense rainfall. CBC News

Le Nouveau-Brunswick épargné par les tornades... mais pas par les rumeurs!
Les tornades qui ont durement frappé le Nord-est américain lundi soir n'ont finalement pas atteint le Nouveau-Brunswick. Environnement Canada a confirmé tôt mardi que la région de Grand-Sault n'a pas été balayée par une tornade, contrairement à des propos rapportés la veille par certains médias et réseaux sociaux. «Il y a eu des orages violents, une tornade rapportée du côté du Maine, mais pas de preuve et de trace de tornade au Nouveau-Brunswick sur nos radars», a indiqué Bob Robichaud, météorologue à Environnement Canada. «Environnement Canada est demeuré en contact lundi soir avec les agents américains de la National Weather Service, au Maine. La cellule orageuse qui se déplaçait vers l'est a été soigneusement observée, elle perdait au fur et à mesure sa capacité de produire une tornade en s'approchant du Nouveau-Brunswick», a-t-il expliqué. L'Acadie Nouvelle, 2

West Nile risk rises in province
As the mercury rises, so does the West Nile risk. With temperatures heating up, there has been an increase of Culex tarsalis mosquitoes - the species of skeeters that carry the West Nile virus (WNV). One pool of infected WNV mosquitoes has been found in southern Saskatchewan, where the risk is moderate, said Phil Curry, an entomologist and the provincial WNV co-ordinator with the Ministry of Health. "Ironically, that heavy rain event (earlier in the month) temporarily reduced Culex tarsalis activity," Curry said. "They're not flying on cold nights, either. Even in areas where they've experienced heavy flooding, that will actually reduce the habitat. It's really disruptive and everything really slows down. Leader-Post, A4

West Hants rafters lost, then found
Two missing female rafters in West Hants have been located near Scotch Village. RCMP confirmed that at 2:30 p.m. Tuesday that several local fire departments responded to reports of two missing female rafters, ages 29 and six years old. Emergency response crews, including a water rescue team equipped with a zodiac, EHS, RCMP were seen on the Kennetcook Bridge on Hwy 215 and then heading down Block Wharf Road in Summerville toward the Avon River. Cpl. Jennifer Clarke said a search and rescue Cormorant helicopter had also assisted in the search. Clarke said the two rafters from the Gore area were also wearing lifejackets. They were reported missing over an hour and were part of a larger group. Chronicle-Herald, A5

Search underway for missing boater on Lac La Martre
A search and rescue operation is underway near Whati, N.W.T., after a male boater was reported overdue. A spokesperson with the Department of Defence says a boat was found on the shore of Lac La Martre with no one inside it. A Twin Otter plane has been sent in from Yellowknife to help with the aerial search of the area. CBC News

Search to resume this morning for man missing in Lake Saint-Louis
Montreal firefighters and the Canadian Coast Guard will resume their search this morning for a 40-year-old man who went missing in the waters of Lake Saint-Louis near Beaconsfield Tuesday night. Fire department spokesman Bruno Ruscio said the man fell from the sailboat he was captaining around 8:30 p.m. while reaching for something in the water. "It was an accident... He wasn't wearing a life jacket. We searched all night and did not find him," Ruscio said. The man was accompanied by a friend with no experience steering the vessel. Ruscio said it's unclear why they were out on the water at night. CBC News

Search underway for Ulukhaktok father and daughter overdue from ATV trip
A search and rescue is underway for a father and his daughter from Ulukhaktok, N.W.T. Billy Joss and his young daughter were reported overdue after they failed to return to the community Sunday evening. The pair were last seen about 150 kilometres away from the hamlet. The pair were traveling by ATV. Dozens of local searchers are now out looking in known areas where Joss would typically be camping or hunting. "In addition to that there's actually a local pilot in Ulu who's conducting an initial flight around that area as well to help them out," said RCMP Const. Rob Frizzell. Joss is known to be an experienced hunter who frequently spends time on the land with his children, Frizzell said. According to Frizzell, there is now talk of bringing in Civil Air Search and Rescue Association volunteers from Inuvik to do a more extensive air search. It's currently 2 C in Ulukhaktok and foggy, with a chance of rain or flurries overnight. CBC News (2016-07-19)

The SQ's tips for safe outdoor adventuring
Thousands take advantage of Quebec's great outdoors every year, and provincial police are hoping to reduce the number who get into serious trouble while they do. The Sûreté du Québec issued comprehensive guidelines on Tuesday that are designed to help solo adventurers adequately prepare for their time in the province's more isolated areas. SQ search and rescue teams were called to more than 1,600 incidents last year, of which 200 required the deployment of teams to the field, said spokeswoman Sgt. Audrey-Anne Bilodeau. The cost of such operations are not cheap, but Bilodeau added "there's no cost that's as important as someone's life." CBC News

BlackBerry makes big sale for D.C. security
BlackBerry says it has received a multimillion-dollar order for secure software that would used in the U.S. Capitol complex in times of crisis. The order was awarded by the U.S. Senate Sergeant at Arms Office in Washington, D.C. BlackBerry says its AtHoc system will be fully implemented for the Capitol complex over the coming months. It didn't say how many millions of dollars the Senate contract will be worth over five years. The system will provide secure notification and communication for up to 50,000 people at the complex. CEO John Chen has shifted BlackBerry's focus more to software sales than its handsets, which have lost most of their market share. BlackBerry also says its AtHoc division will extend the capability of the U.S. Coast Guard's warning system to allow staffmembers in the National Capitol Region to receive and respond to emergency alerts through their computers. Canadian Press (Ottawa Citizen, BB6; National Post, Times Colonist, Hamilton Spectator); Agence QMI (Journal de Québec, Journal de Montréal)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Delays in refugee arrivals likely in wake of failed coup d'état
Delays in the resettlement of Syrian refugees from Turkey to Canada are likely to grow even longer after a failed coup attempted there. Securing exit permits for Syrians in Turkey has been a difficult process already, holding up the Liberal government's plans last fall to resettle thousands of people from there as part of their landmark program to bring 25,000 Syrians to Canada in a matter of months. Now, political instability in the country in the wake of the military's failed efforts to seize power July 15 is expected to delay things more. "We are continuing to work with the government of Turkey to obtain exit permits as quickly as possible and are continuing to monitor the situation," said Sonia Lesage, a spokesperson for the Immigration Department. "However, given recent events, we do expect delays." There are an estimated 549 Syrian refugees in Turkey who have been approved to come to Canada but haven't been cleared to travel, and a further 3,815 applications from that country are in progress. Among them are several Yazidi families, a Kurdish minority group whose plight is the subject this week of hearings at the House of Commons immigration committee. Canadian Press (Hamilton Spectator, A11, Telegram, Chronicle Herald, Ottawa Sun); Presse Canadienne (Le Droit, Le Quotidien)

Two Cuban defectors likely in U.S.: Lawyer thinks softball players crossed border
Cuban athletes who defect while at sporting events in Canada, such as the two softball players who disappeared from a tournament in Surrey over the weekend, almost always make a fast dash for the U.S. border, experts say. The whereabouts of the two softball players who disappeared Sunday are unknown, but "it would make sense for them to go to the U.S.," said Peter Edelmann, a Vancouver immigration lawyer who specializes in refugee law. This is because it is much easier for Cubans to obtain a green card in the U.S. than permanent residence in Canada. Jaime Ruiz, a Los Angeles-based spokesman with U.S. Customs and Border Protection, said he could not comment on specific cases of individuals seeking admission to the U.S. due to privacy laws. Generally speaking, if a Cuban national arrives at a U.S. port of entry and expresses fear of returning to Cuba, border patrol officers will check whether the person has a criminal or immigration history in the U.S., Ruiz said. If not, they are given a temporary residence permit that allows them to stay in the U.S. for one year. After that, they typically apply for permanent residence under the Cuban Adjustment Act of 1966. Vancouver Sun, A6 (The Province); CBC News

Texas man apologetic after failing to declare gun at border
A 69-year-old man from Texas was ordered to pay a $1,500 fine for failing to declare a gun at the St. Stephen border. Marwynne Garfield Khun from Webster, Texas, pleaded guilty to the charge when he appeared in provincial court in Saint John on Tuesday. He was charged under Section 160 of the Customs Act. Kuhn and his wife were stopped by customs officers at the Ferry Point border crossing between Maine and St. Stephen on July 15. They were travelling from Texas to New Brunswick. Federal

prosecutor Peter Thorn told the court the couple was greeted by the officers and asked if they had any weapons in their possession. Kuhn replied that he didn't have any weapons, the court heard. The officer noticed a "flushing" on Kuhn's wife's face so they asked the question again and received the same answer, the court heard. Kuhn's vehicle was referred for a secondary inspection. Upon investigation, officers found an empty gun holster in a storage compartment. They also found a .38-caliber pistol, in another holster, which is a prohibited weapon in Canada. Kuhn was interviewed by officers at the border and he admitted that he owned the pistol, but he had said he was confident that he didn't have any weapons. He said he had owned a .25-caliber pistol as well, but he had left the firearm at a gun shop in Maine, the court heard. Telegraph-Journal, B3

'Barbaric cultural practices' tip line dead, but other snitch lines have continued
The government is fielding hundreds of tips every month from Canadians standing on guard against immigration fraud. Most go nowhere. A small team in a secretive government office in the nation's capital stands ready, 24/7, to hear from Canadians who want to squeal on their neighbours. Working in 12-hour shifts, between two and four Canada Border Service Agency employees are assigned every day to monitor the agency's Border Watch Tip Line, a creation of the Paul Martin Liberal government that gives Canadians a chance to report "suspicious immigration activity" to the government around the clock, in either official language. "No information, however trivial it may seem, is too small," according to the CBSA webpage for the tip line. Most of those tips end up being deleted or filed away in government archives, as do those made to two of the government's other immigration-related tip lines, according to statistics provided to The Hill Times by the federal government. Many of the communications via the tip lines have actually been questions about how to file paperwork for visas or other routine and unrelated matters. Some are reports of illegal activity that falls outside of the CBSA's jurisdiction-for example, financial fraud. Others simply don't include enough information, or do include information "not substantiated" by database searches of CBSA officials, the agency says. Hill Times

B.C. couple must pay $111,000 for immigration fraud against 'friends' from China
A judge has ordered a Langley couple to pay a Chinese couple who were their friends more than $100,000 for committing civil fraud while helping them with immigration services. Bi He Zhao and Rui Du, a husband and wife whose home base is China, argued in court that Yubin Dong and Bing Ji of Langley offered to assist them as friends with their immigration to Canada. Dong and Ji claimed during a two-week trial in B.C. Supreme Court that they had an oral agreement to provide the services. Zhao, a lawyer with a successful practice in China, testified that sometime in late 2008, he was contacted by Dong, a former law school classmate in Beijing. That contact eventually led to Dong offering to help them come to Canada. Zhao testified that Dong said she would contact a friend who had an immigration consulting firm and that she would not charge him a fee; instead, she would be paid a commission by the company. Dong, who described herself as a businesswoman who had been working in the field of immigration services for several years, was neither a registered immigration consultant nor a lawyer in Canada. Instead, Dong had an association with a Vancouver-based immigration consultant business called Can Achieve Consultants, court heard. Vancouver Sun

La guerre de l'acier se joue aussi au Québec
ArcelorMittal sollicite l'appui du gouvernement provincial pour lutter contre le dumping d'acier au Canada, une pratique qui tire à la baisse le prix de cet alliage dans un marché déjà déprimé. L'entreprise souhaite que Québec fasse pression sur le gouvernement fédéral afin qu'il procède aux réformes promises. ArcelorMittal Produits Longs Canada s'est inscrite vendredi dernier au registre des lobbyistes du Québec dans le but « d'obtenir un appui politique pour demander au gouvernement fédéral de mettre en oeuvre les mécanismes de recours commerciaux proposés par l'Association canadienne des producteurs d'acier [ACPA] ». (…) Contourner les règles Selon l'Agence des services frontaliers du Canada (ASFC), le dumping consiste à « vendre des marchandises à des importateurs au Canada à des prix inférieurs aux prix de vente de marchandises similaires dans le pays d'exportation ou à des prix ne permettant pas de réaliser un bénéfice ». Le Devoir

Georgian national wanted in 3 provinces removed by ICE to Canada
A Georgian national and documented Russian mafia associate wanted for crimes committed in Canada was deported by U.S. Immigration and Customs Enforcement's (ICE) Enforcement and Removal

Operations (ERO) Tuesday and turned over to Canadian authorities to face criminal charges there. Alex Alexidze, 41, was repatriated to Canada via ground transportation under ICE escort July 19, from York County Prison and turned over without incident to the custody of the Canada Border Services Agency at the Niagara Falls International Rainbow Bridge. Provincial authorities in Alberta, Manitoba and Ontario have active warrants for Alexidze's arrest on multiple charges related to theft, identity fraud, false documentation and other charges, stemming from alleged crimes committed between 2013-2015 — some under the alias Alex Row. ICE confirmed his true identity with Canadian authorities using photos and biometric data. US Immigration and Custom Enforcement

U.S. tourist destinations try to counter weak loonie
Several American businesses are freezing their prices and trying to appeal to Canadians in a bid to have them cross the border this summer. The loonie's ongoing drop - which began in 2014 - has led to many people choosing places other than the U.S. for vacation. Last year, about 1.29 million people crossed the Quebec border into the U.S. for at least one night between June and August. This was a 13.6-per-cent drop compared with the same period the previous year, according to Statistics Canada. However, 686,000 American tourists spent more than a night in Quebec between June and August 2015 - an 11.8-per-cent increase over the year before. Suzanne Beaulieu, owner of Kebec 3 Motel in Old Orchard Beach, Maine, whose business is 90 per cent from Quebec, said the strength of the U.S. dollar has had a significant impact on her establishment. "Last week, over three days, it was clearly indicated that we had space here and no one stopped by," she said during a phone interview. "It's been years since this has happened." The 35-room motel is booked solid until Aug. 26, but Beaulieu said the peak season used to last until late September. Furthermore, she used to rent rooms in her motel for entire weeks, something that has changed in recent years. Canadian Press (Gazette, A3)

Persecuted Roma need protection
An editorial states, "Re: "Roma family in limbo as status reviewed" (Montreal Gazette, July 19) and "Roma family's deportation postponed" (Montreal Gazette, May 13) With Canada justifiably accepting thousands of Syrian refugees, it makes no sense to deport Katalin Lakatos and her daughter Gilda, back to Hungary, where the Roma are a persecuted minority. We need to welcome them with open arms. The Harper government's deportation of thousands of Roma, under the rationale that Hungary is safe for them, is a blot on our history. This policy needs to be eliminated. The Roma nation is one of the most oppressed in history. They were murdered by Nazi Germany in the hundreds of thousands and targeted for annihilation, like the Jewish people. Their ashes co-mingled in Auschwitz. In 1951, against the background of the Holocaust and the Second World War, the United Nations adopted its "Convention Relating to the Status of Refugees," which states that no signatory shall deport a refugee to a country where the person's life will be in danger. Our government breaks that commitment when it forces people back to countries where their lives will be in danger. We need to adopt Emma Lazarus's poem, The New Colossus, as our guiding spirit: "Send these, the homeless, tempest-tost to me /I lift my lamp beside the golden door!"" Gazette, A11

CYBER SECURITY / CYBERSÉCURITÉ

Cyber Security Threats
Cyber security threats because of employees' mobile gaming use are a concern for chief information officers (CIO). "There is ongoing conversation about what data is being collected with these sorts of interactive online games, so if employees are using their corporate mobile device, it's possible that it could create some vulnerabilities - though there is no talk of such a threat at the moment," says Nima Mirpourian, of Robert Half Technology. A recent survey of CIOs from Robert Half shows that keeping their organization's data safe is their top concern. In another one of their surveys, 54% cite plans to enhance employee training on IT security issues. Toronto Sun, A61

Exploit kits now adopting recent Office vulnerabilities: Report
Cyber security trends can be hard to nail down because attacker strategies constantly evolve. But a new report from Sophos suggests that criminals have finally turned away from an old Microsoft Office exploit and instead are favouring two new ones. However, the report also emphasizes the importance CISOs

have to put in their patching strategy because even the new exploits have fixes out for them. Sophos says that data gathered recently from customers shows the four-year old CVE-2012-0158 vulnerability, which allows remote attackers to execute arbitrary code via a crafted Web site, Office document, or .rtf file has been supplanted in exploit kits by CVE-2015-1641, also a remote execution attack and CVE-2015-2545, which allows remote attackers to execute arbitrary code via a crafted EPS image that would be embedded in a document or email. IT World Canada

LAW ENFORCEMENT / APPLICATION DE LA LOI

Hells Angels a major force in B.C. despite recent loss

As B.C. Hells Angels mourn the recent death of a member of the West Point chapter, police say the biker gang remains a significant criminal force in the province. Bjorn Sylvest died July 3 while on a houseboat on the Shuswap Lake, Barb McLintock, of the B.C. Coroners Service, confirmed. "The death of Mr. Sylvest was reported to us and we are investigating," she said. Sylvest was remembered last week by his fellow Hells Angels and other friends at a service in south Surrey. And they paid tribute to the 35-year-old heavy-duty mechanic Thursday with a procession of 200 to 300 bikers riding from the White Rock Hells Angels clubhouse to the Among the mourners were bikers wearing patches of the Hells Angels, the Throttle Lockers, the Shadow Club, the Jesters, the Devil's Army, the Castaways, the Ironworkers Motorcycle Club and the Horsemen Brotherhood. While Sylvest's West Point chapter has taken a hit with his death, the Hells Angels "remain active in British Columbia and overall membership appears to have remained consistent over the last few years," RCMP Supt. Sandro Colasacco said in an interview. He said the current membership of the HA in B.C. is about 120 in nine chapters. "This number does fluctuate based on factors such as police enforcement initiatives and criminal charges," said Colasacco, intelligence officer for the RCMP's E Division. "Previous investigations have made it clear that some members of the Hells Angels are involved in illicit drug, weapons and violencerelated offences, including murder. It is for this reason that the Hells Angels and other outlaw motorcycle gangs remain a priority for the RCMP and our law enforcement partners." Postmedia Network (The Province, A4, Vancouver Sun, Times Colonist)

Former Red Deer Mountie sentenced on assault charge

A Mountie whose career started in the Red Deer city detachment has been given a conditional discharge for punching a man he had arrested on suspicion of impaired driving. Const. Eric Pomerleau, currently on administrative duties with the Brooks RCMP, was tried and found guilty before Judge Gregory Lepp in Red Deer provincial court in June on an assault charge laid after the incident, which took place at the Red Deer city detachment on Nov. 7, 2012. Sentencing arguments were heard on Tuesday, with Calgary-based Crown prosecutor Photini Papadatou asking for a fine in the range of $500 to $1,000. Papadatou stressed that a police officer in charge of a prisoner is in a position of trust and that all police officers must be held to a higher standard than ordinary citizens. Defence counsel Robb Beeman, also from Calgary, asked for a conditional discharge, which would uphold the conviction without creating a criminal record for his client. Red Deer Advocate, A2; Radio-Canada (2016-07-20); CBC News (2016-06-19)

Conduct hearing for Mountie postponed again

A B.C. RCMP conduct hearing, which had been scheduled for Monday, was postponed for the fourth time leaving the former Osoyoos Mountie in his fourth year of paid suspension awaiting the rescheduled date. Const. Amit Goyal, who last served with the Osoyoos RCMP detachment, has been suspended with pay since at least June 2013. His hearing was originally set for 2015 before being rescheduled repeatedly, and as of Tuesday, the RCMP conduct hearing schedule website showed Goyal's hearing was set to begin in Federal Court in Vancouver on July 25. But Staff Sgt. Julie Gagnon, with the RCMP national communication service in Ottawa, confirmed Tuesday that Goyal's hearing had been adjourned again until Sept. 13. He remains suspended with pay, she said. "Every effort is made for adjudication board hearings to be scheduled in a timely manner," Gagnon wrote in an email. "However, these hearings are formal, court-like processes. Much like judicial proceedings, hearing dates, times and locations are subject to change for any number of reasons." Goyal faces five allegations under the 1988 RCMP Regulations, according to the RCMP hearing schedule. The allegations include three counts under Section 39, which prohibits members from engaging in "any disgraceful and disorderly act or conduct,"

and two counts of Section 45 (b), which says a member must not "knowingly or wilfully make a false, misleading or inaccurate statement or report" to a superior officer about an investigation. Goyal also faces a civil lawsuit, filed in B.C. Supreme Court last year by former Osoyoos resident Steve Condon. In the suit, Condon claimed he suffered harassment and left Osoyoos because of Goyal and the RCMP. Postmedia Network (The Province, A13, Vancouver Sun)

Boylston man charged after threatening RCMP with firearm

A 20-year-old man arrested after threatening citizens and RCMP officers in Guysborough District on July 13 has been remanded to the East Coast Forensic Hospital for assessment. William Anthony Pius George appeared in Port Hawkesbury Provincial Court on Friday. He is scheduled to be back in court on August 5 to answer to the charges. At 9 p.m. July 13, RCMP responded to a dispute on East Side Harbour Rd. where a man had broken the windows out of a residence and vehicles. Police arrived and were told by witnesses that he had threatened to kill individuals inside the residence and discharged a rifle multiple times prior to their arrival. According to RCMP, the man then threatened to kill police. RCMP officers moved the individuals inside the residence to a safe location and called in additional RCMP officers from neighbouring detachments and the Nova Scotia RCMP Emergency Response Team (ERT). The situation was resolved when the man surrendered to the RCMP just after 5 a.m., without incident. No one was injured. The individuals inside the residence and the accused are known to one another. George has been charged with uttering threats (8 counts), assault, careless use of a firearm, unauthorized possession of a firearm and mischief. Guysborough Journal

Police charge ex-boyfriend with murder

After Carol King's body was found in an abandoned farmyard near Herschel, Sask., her ex-boyfriend said he had nothing to do with her death. In an interview, he claimed he was "the fall guy" for the 2011 killing that rocked the small farming town. Almost five years later, that man, Joseph 'David' Caissie of Bluffton, Alta., is charged with first-degree murder. "We start with the people closest to the victim and attempt to clear them and work their way out. In this investigation, we were never able to clear Mr. Caissie," RCMP StaffSgt. Murray Chamberlin told reporters at a news conference announcing the arrest. Carol King went missing on Aug. 6, 2011. Chamberlin said Caissie was taken into custody in Saskatoon without incident. He is also charged with offering indignity to human remains. Caissie is scheduled to appear Wednesday in Saskatoon provincial court. "We are extremely sad but extremely happy at the same time, and have a sense of relief knowing that charges have been laid," Carol King's family said in a statement. Caissie had been under the microscope of RCMP investigators for years, but had long proclaimed his innocence. Postmedia Network (StarPhoenix, A1, Leader-Post); Canadian Press (Edmonton Journal, Toronto Star, Red Deer Advocate)

Une nouvelle fraude qui cible les immigrants

Pendant quelques minutes, la semaine dernière, Yoann a bien cru que le Canada allait l'expulser vers son pays d'origine, la France. Au bout du fil, un agent des services canadiens de l'immigration lui disait bel et bien que des policiers l'attendaient chez lui, prêts à l'embarquer dans le premier avion qui traverserait l'Atlantique. Sauf que Yoann a eu un doute quand il s'est rendu compte que l'employé en question ne parlait pas français et ne semblait avoir aucun collègue qui puisse s'exprimer dans cette langue. Son incertitude aura été bénéfique : le Français était bel et bien victime d'un type de fraude qui fait de plus en plus de victimes chez les immigrants installés au pays. De quatre plaintes en 2013, le nombre de signalements concernant la fraude d'immigration est passé à 1087 en 2015, selon des chiffres que le Centre canadien antifraude (CCAF) a transmis au Devoir. Depuis le début de l'année en cours, 554 Canadiens ont porté plainte pour cette raison, un chiffre qui laisse entendre que la quantité de signalements pourrait dépasser ceux compilés l'année précédente. En pertes, cela équivaut à plus de 416 000 $ depuis janvier. En général, le modus operandi des fraudeurs consiste à exiger des frais qui permettent d'éviter une prétendue expulsion du pays. " La fraude fonctionne. Les gens payent. C'est aussi simple que ça ", a répondu la caporale Josée Forest, de la Gendarmerie royale du Canada, quand on lui a demandé pourquoi les plaintes continuaient d'augmenter. Pire, les statistiques du CCAF montrent qu'environ 5 % de la population rapporte les cas de fraude. " Ce n'est pas beaucoup ", a commenté Mme Forest. Le Devoir, A3

Pot bust yields 400 plants

Police have seized five pounds of pot, 400 marijuana plants, growing equipment and cash after searching a Sturgeon County property this week. St. Albert RCMP say the amount of pot being grown could have produced hundreds of thousands of joints, which could have had a significant impact. Insp. Ken Foster said in a release he was concerned about the large amount of pot seized, noting it's indicative of a criminal trafficking operation rather than someone growing for personal use. "If these drugs were not seized, they would have impacted the well-being of our residents and our children in Morinville, Sturgeon County, St. Albert and throughout the Edmonton region," he said. Cpl. Laurel Kading said police wanted to make clear this was a commercial operation rather than anything personal or medicinal, emphasizing the danger associated with this kind of unregulated operation. "A concern raised to me by one of our experts is there aren't any controls around those kinds of operations," she said. "You don't know if stuff has been added to make the plant grow differently, or could potentially be health hazards growing plants." Officers from several agencies worked together on the bust: St. Albert RCMP, Morinville RCMP, Fort Saskatchewan RCMP, and the Alberta Law Enforcement Response Teams. The Edmonton Police helicopter helped survey the scene during the search for officer safety. St Albert Gazette

Épinglé avec 200 kg de cocaïne

Un résidant de la région de Québec est incarcéré depuis le début de février au Panama après avoir été arrêté en possession de plus de 200 kilos de cocaïne dans ce pays d'Amérique centrale. Le suspect, Steve Miller, a été appréhendé avec deux présumés complices, un Panaméen et un Colombien, lors d'une opération de la police nationale menée le 4 février dernier. L'affaire a fait les manchettes dans les journaux locaux, mais pas dans les médias québécois et canadiens. Lors de la frappe, les policiers panaméens ont découvert 212 kilos de cocaïne et quelques centaines de dollars en devises canadiennes et américaines. La drogue, qui était emballée dans des paquets d'un kilo chacun, avait été dissimulée dans un placard d'une résidence de Betania. Une camionnette, qui aurait servi à transporter la cocaïne, a aussi été saisie par les policiers. On ignore à quelle peine s'expose le présumé trafiquant québécois. La Presse a tenté plusieurs fois de communiquer avec une porte-parole du Ministère public panaméen, en vain. Ici, la Gendarmerie Royale du Canada a confirmé l'arrestation d'un Québécois pour une saisie de 212 kilos de cocaïne sans toutefois donner plus de détails. Selon nos sources, la drogue aurait été destinée aux Hells Angels québécois, en particulier ceux de la section de Trois-Rivières, une information qui n'a toutefois pas été confirmée par les principaux corps policiers du Québec. Au cours des dernières années, les Hells Angels du Québec ont planté leur drapeau ou renforcé leur influence en Amérique centrale, plaque tournante de l'importation de cocaïne vers le Canada, et dans les Antilles. En avril dernier, TVA a révélé que les Hells Angel du Québec auraient parrainé une nouvelle section que l'organisation internationale a fondée en Équateur. La Presse (La Tribune, 15, Le Nouvelliste, Le Soleil)

Father says daughter 'fell through the cracks'

Kent Robinson just wanted his daughter to come home. Cynder Robinson, 17, lived on a northern reserve, away from family, for nearly a year. By the time he convinced her to return, it was too late. "Obviously it was a dangerous situation. I knew that right away," Robinson said. "I don't want to let it rest. I don't think my daughter should have ever been there." Cynder was found dead inside a home on the Big Island Cree Nation on Friday. RCMP called the death suspicious, but would not confirm a homicide investigation is underway. An autopsy was scheduled for Tuesday in Saskatoon. Cynder's father said he tried to get her to come home to Taber, Alberta for months, but because she was over 16, the RCMP and social services workers could not force her to return. "Cynder was a beautiful, beautiful soul. She just made the one mistake and it cost her life," Robinson said. Few details have emerged about what happened inside the home, but Robinson said his eldest daughter suffered from an arachnoid cyst that made her more susceptible to fatal head injuries. (...) He said he doesn't know for sure if his daughter was killed or if she died of natural causes. If someone did kill her, he wants justice, he said. "She was not a violent person. She knew she couldn't be a violent person because of her condition," he said. (...) Trevor Kahpeepatow, a Big Island band councillor, said it's not uncommon for non-band members to spend time on the reserve, although it is usually temporary. He said Cynder was a well-known face around the reserve and that her death has hit hard. "It is a shock," he said He and the band council are working hard to make sure the reserve - which is technically a dry community - is a safe place, Kahpeepatow said, adding they are trying to get tough on the drinking rules and deal with some of the root problems in the community. StarPhoenix, A3

New Kelowna criminal gang is small but dangerous
When RCMP arrested a member of a new street gang in **Kelowna** this month, it was a significant blow to the organization. "They are what we consider a low level street gang (present) only in the immediate Kelowna area," Staff sgt. Lindsey Houghton of the B.C. Combined Forces Special Enforcement Unit says. "You can count their members on two hands." The gang came to light last week when a cache of guns, drugs and a vest bearing an unfamiliar crest was displayed to the media by local police after a warrant was executed at a home in West Kelowna. Two men and a woman were arrested and a seven-year-old child found inside the home was brought under the care of the Ministry of Child and Family Development. A 24-year-old West Kelowna woman was questioned and released. A 37-year-old West Kelowna man is expected to appear in court Oct. 13 on possible drug and firearms related charges and a 32-year-old West Kelowna man, Tyson Ashleigh Bone, remains in custody. Const. Jesse O'Donaghey said Bone is a member of a small, new gang called the Kelowna Warriors. "They've been around for about four years," Houghton confirmed on July 19. "Mostly street-level stuff like drugs but often times they are the most dangerous." Houghton says there are fewer than ten members and that membership changes quickly. "We see a lot of transiency at levels like this," he says. "They say they're in one group one day and then swear allegiance to another the next day." The vest taken from the West Kelowna home included three patches, a central logo and the name of the city and gang above and below. "In order to wear the three-piece patch you have to get the consent of whichever outlaw groups control the area. In Kelowna it's the Hells Angels." Houghton says although they likely have permission from the Angels to operate, there is no evidence of cooperation between the groups. InfoTel (2016-07-19)

Quarterly report: $155,770 in drugs seized by Valley police unit
The Valley Integrated Street Crime Enforcement Unit is taking thousands of dollars worth of drugs off of the streets. Kenneth Reade, acting chief of police for the Kentville Police Service, shared the unit's report for the quarter that concluded June 30 during a council advisory committee in Kentville July 11. In a three-month period, the unit executed 14 search warrants, and charged 16 people with 20 criminal code offences and 25 Narcotic Control Act violations. Twelve of the warrants were drug related and two were for Criminal Code matters. "There were $155,770 worth of drugs seized, $17,810 worth of other property seized, $22,007 in cash seized," said Reade.The quarterly report lists the drugs seized as: marijuana, cocaine, $137,000 worth of marijuana plants, hash, various prescription pills and Psilocybin. (…) The specialized law enforcement unit is comprised of members of the Kentville Police Service and Kings District RCMP and Windsor RCMP. Nova News Now

Burnaby 'demoviction' protesters continue fight for affordable housing
Protesters occupying a building slated for redevelopment in Burnaby, B.C., are renewing their call for affordable housing as the building approaches its demise. "I hope the politicians, you know, do something or take it serious," said a man who has been living in the building who referred to himself only as Mohammed. "These are people, they are not trash on the street. They're being treated like trash."The protesters have occupied the building at 5025 Imperial Street since July 9. They previously told CBC the developer, Amacon, would begin removing hazardous materials last Monday to prepare for demolition in August. Burnaby RCMP have obtained a court injunction to clear out the group, which is operating under the name Alliance Against Displacement. CBC News

Four suspects face charges after drug bust
Four people are facing charges after Mounties seized approximately 200 fentanyl pills and other drugs during a traffic stop in southern Alberta on Sunday afternoon. Pincher Creek RCMP said they stopped a vehicle for a "serious traffic violation" at around 4 p.m. in the town about 200 kilometres south of Calgary. Inside the vehicle, police found a backpack containing approximately 200 fentanyl pills, three ounces of methamphetamine, nearly two ounces of crack cocaine, a small amount of marijuana and a large amount of cash. RCMP say there was also open liquor in the vehicle. Sebastion Aranzalez, 21, of Calgary, Ruairi McGinnity, 22, of Lethbridge, Christie Reed, 39, of Pincher Creek, and Sherri Lagrandeur, 40, also of Pincher Creek, are charged with possession of a controlled substance for the purpose of trafficking. Police say Aranzalez was also charged with driving with no licence and careless driving. All four were released with conditions ahead of their court appearances. Calgary Herald, A10

La GRC invite à la prudence

La GRC a demandé aux joueurs de Pokémon Go de faire preuve de «gros bon sens». Des amateurs de l'application mobile l'utilisent en conduisant pour couvrir du terrain plus rapidement et ainsi attraper plus de Pokémon, au détriment de leur sécurité et de celle des autres. La gendarme Isabelle Beaulieu rappelle que l'utilisation du cellulaire au volant est interdite au N.-B. et souligne que les agents circulent sur les routes de la province, aux aguets pour repérer les conducteurs distraits. Toute personne arrêtée en train d'utiliser un appareil électronique au volant d'un véhicule à moteur s'expose à une amende de 172,50$, en plus de voir soustraire trois points d'inaptitude à son permis de conduire. Elle demande aussi aux utilisateurs de ne pas s'introduire sur des terrains privés. Acadie Nouvelle, 5

RCMP not letting youth off the hook following prank bomb threat at Vernon mall
Police are sending a message after the latest incident of swatting — deceiving law enforcement with a phoney call — led to major disruptions at a Vernon mall. The prank resulted in numerous employees and patrons being evacuated from the Landing Plaza for several hours while police investigated. But it's not the first time emergency officials have been 'swatted.' Last year in Kamloops, several schools were locked down due to swatting pranks involving fake bomb threats. The same thing happened in Toronto, and a host of other cities. Sgt. Mike Moyer of Vernon RCMP says a youth was identified as the source of the prank call in Vernon and won't be let off the hook for the crime. Given the seriousness of the incident, Moyer says they will be recommending criminal charges, including mischief and possibly more, to Crown counsel. "Obviously, it scares a lot of people, especially with what's going on worldwide," Moyer says. "We, as the police, take these calls very seriously." Significant resources were deployed to the incident, including specialized RCMP units, the Vernon Fire Department, B.C. Ambulance Services and bylaw. Numerous businesses were forced to shut down, equating to thousands of dollars lost, Moyer says. And while the threat was a hoax and no one was hurt, Moyer says they want to make it clear pranks like this one are a crime and will not be tolerated. "We want to send a strong message," Moyer says. InfoTel (2016-07-19)

RCMP nab alleged drug traffickers
The Wood Buffalo RCMP Drug Unit arrested two individuals on July 15 after receiving a tip through Crime Stoppers of a male and female selling drugs in a Thickwood apartment building. Tristen Bradbury, 19 and Jennie Podanovitch, 19, both of Fort McMurray, were arrested Friday when they were leaving their Signal Road residence. RCMP spokesperson Cpl. George Cameron said officers opened an investigation after receiving the tip at the beginning of June. "There was enough evidence in order for the courts to grant a search warrant," Cameron said. Officers located 144 grams of cocaine, 49 grams of marijuana and 1.5 fentanyl pills after searching the apartment. Cameron couldn't give an exact amount, but estimated the drugs to be worth "thousands of dollars." Also inside the residence was a shotgun and ammunition and approximately $35,000 in cash believed to be proceeds from selling drugs. Bradbury and Podanovitch were both charged with possession of cocaine and marijuana for the purpose of trafficking, possession of fentanyl, possession of property obtained by crime, unauthorized possession of a firearm and unsafe storage of a firearm. Fort McMurray Today (2016-07-19)

OPP charge two men in grow-op bust
Ontario Provincial Police have charged two Ottawa men after a raid on a commercial property in Beckwith, about 45 kilometres southwest of Ottawa, led to the discovery of a large-scale marijuana grow operation. According to police, an investigation into allegations of marijuana trafficking led to the July 11 raid when the two men were arrested. Police confiscated 2,012 plants in various stages of growth, 25 pounds of marijuana buds, 26 grams of cannabis resin (hash) and hydroponic growing equipment. Facing charges related to illegally growing marijuana are Adam Gunderson-Lord, 37, and John Armstrong, 36. Ottawa Citizen, A6

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Former Nfld. priest gets parole after serving one-third of sex abuse sentence
Roman Catholic priest George Ansel Smith abused more than a dozen boys over two decades, using alcohol, threats and bribes with children as young as 8 years old. In 2013, the judge who sentenced him to 11 years described him as a "predator." But in a decision this month, the Parole Board of Canada has

released the retired cleric on full parole after a third of his sentence, saying he is considered a low risk to reoffend. It noted that the Correctional Service of Canada rated Smith's potential for reintegration into society as high. "CSC is of the opinion that you have repeatedly demonstrated that you are fully committed to leading a pro-social life and are ready for a less structured release," the decision said. Smith was sentenced in March 2013 after he pleaded guilty in provincial Supreme Court to 41 charges, 38 of which resulted in a convictions for sexual assault, indecent assault and assault with intent. Canadian Press (CTV News, Toronto Sun, Ottawa Sun, Red Deer Advocate, Blackburn News, News 1130)

Rallo's claims of innocence slam door on parole
If ever there was going to be a time for Jon Rallo to confess to murdering his wife and children, this was it - his first parole hearing since his beloved mother's death. Yet despite the hopes and rumours that have churned around Hamilton in the 40 years since the killings, Rallo clung stubbornly to his "denial stance" Tuesday. "If my position doesn't change, am I never going to get full parole?" Rallo asked of the Parole Board of Canada (PBC) panel. "Because gentlemen, my position hasn't changed." It's that refusal to admit his guilt that has blocked him from full parole over and over again - this time being no different. And now, thanks to legislation championed by Flamborough-Glanbrook Conservative MP David Sweet, the convicted murderer may not get another chance for five years. Standing outside Beaver Creek Institution in Gravenhurst just moments after Rallo was denied his bid for full parole, his victims' family and Sweet wondered if this might be the last time they are dragged through this painful process. "Rallo will be 78 by then," said Janice Orovan, dabbing at her tears. "Imagine not coming back to this place?" Sweet's private member's bill calling for changes to the Corrections and Conditional Release Act was passed in April 2015, forcing offenders to wait longer for legislated full parole hearings. The change stretched from two years to five. Though offenders can apply before the five years is up, the PBC has the right to deny the application. Hamilton Spectator, A1

Adult sentence upheld in brothel murder case
A youth who was sentenced as an adult in the murder of a sex-trade worker has lost his appeal of his sentence. Peter Wong was five months short of his 18th birthday when he shot and killed Ping Li, a young woman, as she begged for her life in the Burnaby brothel where she worked. During the course of his attempted robbery of the brothel, Wong also shot Xing Li, the owner of the brothel. Li was placed in a medically induced coma for two weeks and survived. Wong was convicted by a B.C. Supreme Court jury of first-degree murder and discharging a firearm with intent to wound in connection with the March 2009 slaying. Following an application by the Crown, on the murder count Wong was sentenced as an adult to life in prison with no parole eligibility for 10 years. He was sentenced to four years in prison for the firearm count, to be served concurrently. Vancouver Sun, A3 (The Province)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Public has right to film officers on the job
A black man is wrestled to the ground and shot by a Louisiana police officer. The incident is caught on a bystander's camera. A day later, a Minnesota police officer shoots and kills a black man at a traffic stop. The incident is broadcast by the man's girlfriend using her smartphone. Those incidents - viewed by millions on social media - have underscored already strained race relations in the U.S. and spurred Black Lives Matter rallies throughout the United States. On Tuesday in Winnipeg, a teen girl wearing a mask and waving a replica gun at Portage and Main was caught on camera by a passerby just seconds before police officers ran into the intersection, tackled her and diffused a potentially escalating situation. The dramatic video was uploaded to Facebook and quickly watched by Winnipeggers and others. But can you automatically film and photograph police doing their jobs? Are there any rules? Winnipeg police spokesman Const. Rob Carver said if people want to pull out their smartphones to record officers performing their duties in public, police can't stop them. "There are no restrictions on people taking video of police officers in public," he said. "People have the right to record officers arresting somebody... by and large, there are no prohibitions whatsoever." However, Carver said police would be suspicious if people set up outside police headquarters with a video camera and targeted individual officers. "We've had gang members surveil us," he said. Police want the public to realize they shouldn't endanger themselves or

police while recording or getting too close to a potential crime scene, Carver said. Winnipeg Free Press, A3

Public help sought for anti-violence strategy
The federal government is turning to Canadians for their ideas on how to stamp out the "unacceptable" level of violence facing women and girls online. Status of Women Minister Patty Hajdu used a Toronto visit on Monday to launch consultations on a federal strategy to reduce gender-based violence and the first topic up for discussion is cyberviolence. "From my perspective, this is the Wild West of communication, where there are very few rules and very few avenues for people experiencing violence, women and girls in particular, who are disproportionately the victims of this type of violence online," Hajdu told the Toronto Star. The Internet and social media can be nasty forums for harassment, sexism and misogyny. In 2012, B.C. teen Amanda Todd took her life after becoming the target of cyberbullying. Hajdu said there is no doubt the abuse aimed at women and girls online should be branded as violence. "Language and abuse through the use of words is a form of violence. We take that very seriously and, quite frankly, think it's intolerable," Hajdu said. "We need to call out and condemn violent behaviour, sexism whenever it occurs. "Cyberspace is one of those areas that it's occurring at an astronomical rate. It seems like a logical place for us to start," she said last Friday in an interview from her Thunder Bay, Ont. riding. She said there is a role for Ottawa to act in this arena, but how remains a question. Whitehorse Daily Star, 7

Halton police praise Province's $72 million anti-human trafficking strategy
With Canadians being 93 per of Canada's sex trafficking victims, Ontario accounting for 65 per cent of police-reported human trafficking in Canada, and Halton's sex trade hidden behind closed doors along the QEW and Hwy. 401, a recently announced $72 million provincial anti-human trafficking strategy is a step in the right direction. That's according to a detective with the Halton Regional Police Service Human Trafficking and Vice Unit. "This is very positive and a step in the right direction in terms of addressing this issue," said Det. Sgt. Raf Skwarka, Halton police. The provincial government announced the investment in late June, stating the strategy is aimed at increasing awareness, coordination and enhancement of justice-sector initiatives and improving survivors' access to services. The provincial government, in announcing the strategy, admitted Ontario is a major centre for human trafficking in Canada — accounting for roughly 65 per cent of police-reported cases nationally. Inside Halton (2016-07-19)

Crime rates falling
Crime rates are higher in Western Canada than in the East of the country, according to an Angus Reid Institute survey. However crime decreased right across the nation, from 2000 to 2014, shows Statistics Canada's Crime Severity Index – used by the pollsters. The survey found that Canadians living west of Manitoba are much more likely than those living farther east to have reported falling victim to a crime over the last two years. British Columbia, Alberta and Saskatchewan residents are more than twice as likely as Ontarians or Quebecers to have experienced a crime. The east-west divide is also reflected in the perception that crime is on the rise in one's own community. Those in Western Canada are more likely to say crime has increased in recent years than respondents in the east. As might be expected, crime has fallen the most in the two provinces where Canadians are least likely to report having been the victim of a crime in the last two years – Ontario and Quebec. Only Quebecers seem be conscious of this fact, however. In Ontario, only seven per cent of respondents report that crime in their communities has been decreasing in the last five years. Five times that many (39 per cent) say crime has been on the rise. Castanet (2016-07-19)

Survey suggests Sask. residents believe crime on the rise; numbers show otherwise
Saskatchewan residents think crime is on the rise, even though crime numbers are dropping in the province, a new survey suggests. An online survey by Angus Reid shows 56 per cent of people in Saskatchewan believe crime has increased over the last five years in their communities, despite numbers from Statistics Canada showing crime and severe crime have dropped in the province. The belief is likely influenced by people being exposed to individual crime reports in the news, according to Angus Reid. More than 100 adults in Saskatchewan were surveyed by Angus Reid between May 30 and June 6. Four per cent indicated they thought crime had dropped during the last five years. CTV News (2016-07-19)

Opt for justice system that reduces crime, recidivism
An opinion piece states, "Monday City Views columnist Craig Babstock's column this week capably argued for establishing 'addiction courts,' much like we have 'youth courts' and 'family courts' to provide a justice system with specialized, focused expertise that aims to ensure rehabilitation and the minimizing of damage for all in society, including the guilty, rather than merely mete out punishment. That column was prompted by recent funding of a study to explore the practicality of such a court. Mr. Babstock, also a veteran Times & Transcript's court reporter, thinks our federal and provincial governments ought to forget more study and just knuckle down now to set up such a court. I second his notion. It's an issue worth informed public discussion. Unfortunately, too often discussion of our justice system isn't well informed. Too often it divides into the simplistic camps of 'law and order' versus 'rehabilitate and don't punish much, if at all.' (...)Why not an 'addictions court' too (including alcohol)? Addiction is illness. A court would help rehabilitate large numbers. It'd prevent repeat offences, saving money. It'd lower policing costs and add to economic productivity. It'd prevent impaired driving deaths, prevent other accidents due to impairment, and lower health care costs as long-term addictions decline. The more addicts an addiction court system can help, the more society saves. And even repeat offences are ironically a positive: it's common for addicts to try several times before successfully beating their addictions. Much violence in society, including domestic violence, is fueled by booze. Murders, assaults and other attacks would diminish noticeably. Impaired driving too." Times & Transcript, A8

The law needs to catch up on cyberbullying
An opinion piece states, "In 2014 I wrote a paper: "Cyberbullying: The Current State of Our Privacy and Technology Law". This report provided a review of cyberbullying legislation across Canada, including the relevant case law. This is a new, and fast-changing, area of the law. Since I wrote the paper, there have been new developments with the Nova Scotia Supreme Court, thus the striking down of that province's cyberbullying law. Striking it down for infringing privacy rights set out in the Charter of Rights and Freedoms, Nova Scotia's Cyber-Safety Act had been the most comprehensive among Canadian provinces. An article in Canadian Lawyer magazine by David Fraser of the law firm McInnes Cooper entitled: "Nova Scotia's cyberbullying law is a disaster" referring to the civil liberties infringements from the legislation's broad wording which captured activities that would be considered beyond cyberbullying. He argued in court this legislation should be struck down. Meanwhile, the problem of cyberbullying is hardly going away, with the increasing pervasiveness of social media platforms from Twitter to Facebook to SnapChat and many more. With laptops, tablets, and smartphones, the Internet is mobile, everywhere, creating a disturbing new dimension to cyberbullying. (...)Law enforcement needs to have the tools to deal appropriately with cyberbullying. Rather than using other legislative tools, such as child pornography laws, that could either be too strict, too lenient, or simply not capture the nature of the action. While effective laws capturing the problem of cyberbullying are needed, these laws must not be so overboard to capture forms of speech beyond cyberbullying." Telegraph-Journal, A9

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Zoe Saldana producing film on Canada's missing indigenous women
A new documentary by a team of Los Angeles-based filmmakers – including Avatar star Zoe Saldana – is hoping to shed light on the disappearance and murders of as many as 4,000 indigenous women across Canada. "If this exact same story were being told in a country in Africa, I think we would be paying attention to it and we would be donating money to it," said Leslie Owen, the American producer-director behind Gone Missing. "But because it's in Canada, a first world nation, we don't want to see it in our own backyard." She began researching the story in 2015, after stumbling across a news story highlighting 1,200 cases of murdered and missing women that had been compiled by police bodies from across the country. "I was like, what does that mean?" Recent months have seen the number revised upwards, with one government minister estimating the number of missing and murdered indigenous women could be as high as 4,000 women. The Guardian (UK)

Leaked document appears to give broad powers to MMIW national inquiry

There will be five commissioners sitting on a national inquiry into missing and murdered Indigenous women (MMIW) and they appear to have the power to run the inquiry as they see fit, according to the Terms of Reference (ToR) obtained by APTN National News. The document, watermarked "sensitive and confidential," appears to be a template for a final version. It does not name the five commissioners. The ToR document also appears to address a pivotal question asked by MMIW family members and their advocacy groups: how much power will the commission have. "Authorize the Commissioners to adopt any procedures that they consider expedient for the proper conduct of the inquiry," the ToR states. But it doesn't elaborate on how much power that is or whether the commissioners will have the power to compel people to testify. The ToR does call for the inquiry to bring the "ongoing national tragedy" of MMIW to an end and examine the "systemic causes of violence against Indigenous women and girls in Canada" and make recommendations. That means looking at the "underlying social, economic, cultural, institutional and historical causes" that have led to more than 1,200 Indigenous women and girls to be murdered or go missing in the last 30 years. APTN News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

City urged to act on pot shops

There are growing calls to shut down or regulate Ottawa's budding marijuana dispensary business, as new - and illegal - storefronts pop up around the city. Since the beginning of July, five more dispensaries have opened or plan to shortly, boosting the number in the city to nine. They are part of a wave of marijuana stores that have been opening across the country, in defiance of federal drug laws. Ottawa Coun. Mathieu Fleury says he has asked Ottawa's police chief to enforce the law and shut them down. He and other councillors who represent urban wards have also begun to discuss whether the city should regulate where the dispensaries operate. Coun. Riley Brockington, who is upset about a cannabis store about to open across the street from a school in his River Ward, said the city can't wait to act until the federal government makes recreational marijuana legal. The umbrella group for Ottawa's Business Improvement Areas invited two police officers to a recent meeting to provide information about the pot shops. The officers gave the same answer that a police spokesperson provided to the Citizen: They are aware of the dispensaries, and are investigating. With the legalization of recreational marijuana on the horizon, these businesses are "jumping the gun," says Christine Leadman, executive director of the Bank Street Business Improvement Area. Two marijuana shops have opened on Bank Street downtown, a situation that until recently would have "been unfathomable," Leadman said. "In my mind, the city police and bylaw should be shutting them down." But she's sympathetic about the difficulty the city may have in regulating the shops. "How do you build in (bylaw) planning for a business that's illegal?" The pot dispensaries are confounding police and municipal officials across the country. The federal government has promised to introduce legislation to legalize and "strictly regulate" recreational pot next spring. Ottawa Citizen, A1 (Ottawa Sun)

PUBLIC SERVICE / FONCTION PUBLIQUE

Minister says civil servants won't lose out for pay system problems
Civil servants who have been forced to max out credit cards or borrow money as a result of problems with the federal government's dysfunctional new pay system can expect to be compensated, says the minister responsible for the system. Public Services and Procurement Canada will review hardship cases one at a time, and make things right for anyone who has been placed in dire financial circumstances, minister Judy Foote told The Canadian Press on Tuesday. "Nobody should be out-of-pocket as a result of something over which they had no control," Foote said. Newly released documents obtained by the CBC also show that officials were warned as early as Jan. 18 that the new Phoenix system has a flaw that allows widespread access to employees' personnel records, including social insurance numbers. The minister told the CBC she learned only this week of the internal breach of private information. "I am aware of it, and I've been told that none of the information became public." She said she has turned the matter over to the privacy commissioner for investigation, and will focus on getting people paid. Heads could roll once the dust settles from investigations that have been launched into the new Phoenix pay system, Foote said. The government acknowledged Monday that nearly 82,000 public servants have had trouble getting the compensation they are owed because of major problems with what is the biggest pay system in the country, serving roughly 300,000 civil servants. (...) The Public Service Alliance of Canada has also called on the government to take Phoenix off-line and revert to the old system. Foote, however, says that's not possible. Canadian Press, (Record, A4, Times Colonist, Ottawa Citizen, Hamilton Spectator); Telegraph-Journal (Times and Transcript, Daily Gleaner); Le Droit (La Presse)

Phoenix flaw put PS personnel files at risk
The Public Service Alliance of Canada is renewing its call to scrap the government's Phoenix payroll system in light of newly released documents indicating that a flaw exposed the personal information of thousands of civil servants. "We knew this was going to be a disaster right from Day 1," PSAC executive vice-president Chris Aylward fumed Tuesday evening. "We knew this was going to be a Gong Show, and look where we are today," he said. "This is completely unacceptable. ... It's time to shut it down." Documents obtained by CBC News reportedly show officials were warned as early as Jan. 18 that the Phoenix system has a flaw that allows widespread access to employees' personnel records, including social insurance numbers. In an emailed statement to Postmedia, Public Service Minister Judy Foote's office confirmed government officials discovered the flaw early in the Phoenix rollout. Canadian Press (Ottawa Citizen, A2, Ottawa Sun); CBC News (2016-07-19)

Growing tech woes hinder Statscan's ability to meet mandate, chief says
Statistics Canada's technological troubles have become so acute that its chief statistician says they are hampering the agency's ability to carry out its mandate - and he places the blame squarely on one source: Shared Services Canada, the department now running the agency's informatics infrastructure. Statscan's website has for months been beset by crashes, delays and outages, most notably on July 8, when its main website was down for more than seven hours on the day of the release of the labour force survey. In an interview with The Globe and Mail at his Ottawa office, chief statistician Wayne Smith said that that outage - along with a long list of other information technology troubles - relates to problems with Shared Services. "It's had a significant impact on our operations," Mr. Smith said. "Our service to the public has suffered, clearly, in ways that we would rather not have happened. Some of our relationships have suffered. ... There's a frustration among our clients." Canada's statistical agency is tasked with producing quality data and analysis about the country on everything from oil exports to jobless rates, food prices and health outcomes. That mandate, Mr. Smith said, is at risk as tech glitches - stemming partly from a lack of maintenance at its data centre - have caused delayed releases, lost time in conducting quality assurance and higher costs. If the situation continues, he warned, data quality could be hurt and, if the agency incurs additional costs to boost muchneeded capacity at the data centre, it could result in cuts to surveys and programs. Mr. Smith said the frequency of incidents is growing. On July 8, the agency's main website was down for 7 hours 50 minutes when a power transfer switch failed. "The issue on July 8 was a pure informatics infrastructure issue, entirely under the responsibility of Shared Services," he said. Globe and Mail, A1

OTHER / AUTRE

U of T student interrogated in Bangladesh
Bangladeshi police have confirmed that a University of Toronto student is being interrogated, without clarifying his whereabouts or his condition, or saying whether he was being charged - escalating concerns over possible human-rights violations in his detention. Tahmid Hasib Khan, 22, and a fellow detainee, British citizen Hasnat Karim, 47, were among several hostages who survived a terrorist attack at a restaurant in Dhaka that left 23 people dead on July 1. They were then taken in by police for questioning. Family members have had no contact with Mr. Khan since July 3, aside from a phone call from an unknown agency confirming his detention. "We have to conduct the investigation through interrogation of witnesses, rescuers and others concerned. The puzzle cannot be solved without interrogation," the Dhaka Metropolitan Police commissioner said, according to a report in The Dhaka Tribune newspaper. Local outlets also reported that the commissioner evaded questions about the nature of the detention. The DMP's counter-terrorism and transnational crimes unit is said to be investigating. The commissioner's statement marks the first time law-enforcement authorities have acknowledged that Mr. Khan, a permanent resident of Canada, has been in custody since the attack. Last week, the deputy commissioner said everyone rescued had been "released." Globe and Mail, A7

No compromise with Iran
Iran's indictment of one foreigner and three Iranian dual-nationals, including Iranian-Canadian professor Homa Hoodfar, vindicates the Harper government's 2012 decision to sever ties with that country. Iranian prosecutors have not specified why Hoodfar and the others are being charged. Even Hoodfar's lawyer doesn't know what crimes have been alleged, having been denied access to the Canadian woman since June. Hoodfar, a professor at Concordia University, had been in Iran researching feminist activism when she was put in prison for interrogation last month. In some ways, the official charges hardly matter since everyone concerned knows the judicial case is little more than a grim charade - the sort we've seen before with Iranian-Canadian photojournalist Zahra Kazemi, who was tortured to death in Tehran's Evin prison after being arrested for allegedly taking photos of sensitive parts of the facility. (In reality, Kazemi, carrying an Iranian-government-issued press card, was documenting concerned family members of students who had gone missing after a massive police clampdown on demonstrations in the city. It was assumed the students had been jailed in Evin.) National Post, A7

Trudeau can and should bring home Canadian man trapped in Egypt
An opinion piece states" All three of us have spent substantial time in Egypt's most notorious prisons among thousands of people arbitrarily detained - activists, journalists and regular citizens, Egyptian and non-Egyptian. Tireless advocacy and political lobbying finally helped bring us home, but we left behind those who weren't as lucky. One of those prisoners is Canadian permanent resident Khaled Al-Qazzaz, a philanthropist, educator, husband and father, whose wife and four children are all Canadian citizens, and who now faces life-threatening injuries as a result of his imprisonment. We believe that the Liberal government under Prime Minister Justin Trudeau can bring him and his family home and bring their nightmare to an end. Like many people who are arbitrarily detained, Khaled was not charged with a crime. He was arrested in 2013 and spent hundreds of days in solitary confinement. He was kept in the adjacent cell to one of us, Mohamed Fahmy, a journalist with Al Jazeera at the time. As Khaled will surely tell you, it's the sheer physical loneliness that's toughest to deal with, the feeling of being cut off from family and friends. He and Mohamed tried their best to console each other as they dealt with this feeling." Toronto Star, A11

What to do about Turkey?
An opinion piece states, "These days, even the most forgiving observer of Turkish politics is having a difficult time glossing over the disturbing news coming out of Turkey. Certainly, the recent aborted coup attempt is important enough. But well before this, journalists, academics and activists critical of the government found themselves under arrest and their newspapers and television channels shut down. The net result is that Reporters Without Borders just listed Turkey in 151st place out of 180 countries in its 2016 World Press Freedom Index - lower even than Russia. (…) How, then, should Canada react to the current situation? We certainly shouldn't turn our backs on the Turkish people, who, during the past year, have faced continuous terrorist attacks and now an aborted coup attempt. However, the coup aside,

Canada needs to make clear that it does not condone the Turkish government's own assault on democracy, in which even those who dare to share a tweet can be branded as terrorists and traitors. Ottawa Citizen, A9 (London Free Press, Kingston Whig-Standard)

INTERNATIONAL

Daesh claims attack on German train

A 17-year-old Afghan asylum seeker who police say carried out an axe attack on a German commuter train had pledged loyalty to Daesh before slashing at least five people, in an incident that appeared likely to intensify opposition to Germany's influx of migrants. In a video issued by Daesh (also known as ISIS or ISIL), the teenager identifies himself as a "soldier of the caliphate" and threatens further attacks by the group "in every village, city and airport," according to a translation by the SITE intelligence group, which tracks jihadists. "I lived among you and in your houses," the Afghan said. "I will slaughter you in your houses and tear you apart. I will make you forget the horror of the France operation," a reference to an attack Thursday in Nice, France, that killed 85 people and injured more than 300. The authenticity of the video could not immediately be confirmed. More than two million people poured into Germany last year, many of them seeking asylum in a historic influx that was the largest since 1950. The migrant flows upended German institutions with sudden new demands and created the biggest political challenge for German Chancellor Angela Merkel in her 11-year rule. (...) Daesh earlier claimed that the teen was a "fighter" for the group, the Amaq agency said. It was not clear whether the video was evidence of a direct link to the man, or whether he posted it online without having arranged it with the group beforehand. The Daesh claim came just hours after the attack, in which at least five people were injured. Toronto Star, A8

Officer killed while looking for suspect

Kansas City, Kansas, police officer was shot and killed on Tuesday while searching for a suspect in a drive-by shooting, police said. Capt. Robert Melton was searching for the suspect when he drove up to someone who matched that person's description just before 2 p.m., police spokesman Tom Tomasic said. Before Melton could get out of his vehicle, the person opened fire, hitting the officer multiple times, Tomasic said. The alleged shooter was caught five minutes later about a block away, he said. A police spokeswoman said the suspect was being questioned Tuesday evening along with another person suspected in the initial drive-by shooting. Police weren't releasing the suspects' names because charges hadn't been filed. A third person who had been taken into custody was determined not to have been involved and was released, police said. It's the second time a Kansas City, Kansas, police officer has been shot and killed this year. In early May, detective Brad Lancaster was fatally shot near the Kansas Speedway, and Melton had served in the police honour guard at Lancaster's funeral. The shooting also comes as police departments across the country are on edge after ambush attacks left eight officers dead in Texas and Louisiana. "There's a lot of pain and brokenness in our community and our nation right now, and we just want to ask everyone to be prayerful and thoughtful right now," Mayor Mark Holland of the Unified Government of Wyandotte County said. Associated Press (Red Deer Advocate, A8, Edmonton Sun, Kingston Whig-Standard, Calgary Sun, Toronto Sun, London Free Press, Ottawa Sun, Winnipeg Sun, Times and Transcript, Hamilton Spectator, CBC News, Global News, St. Catherin Standard)

EU police agency warns of extremist threats to Europe

The number of people killed in attacks by extremists throughout Europe soared in 2015 from a year earlier, the European Union police agency reported Wednesday as it warned the Islamic State group may "put more emphasis on operations abroad" as a Western military alliance puts it under pressure in Syria and Iraq. The Europol report painted a worrying picture of an EU assailed by Islamic extremist threats that are unlikely to recede any time soon. It warned that Syrian asylum-seekers could be targeted and swiftly radicalized by IS recruiters while a new generation of fighters is being raised in IS territory in Syria and Iraq. The report also stated that IS appears to favour attacks against soft targets because they " instil more fear in the general public." That threat was horrifically underscored by the Bastille Day truck attack in Nice, France, that left 84 people dead. In a move that underscored the swiftly evolving nature of the extremist threat, Europol also issued a separate statement on recent attacks in Nice, Germany and the United States, saying they "highlight the operational difficulties in detecting and disrupting lone actor attacks." Associated Press (Metro Winnipeg)

The murky role of mental illness in extremism, terror

After family members of the driver who slammed a truck into a holiday crowd in the French city of Nice said he suffered from depression, questions have been raised again about the links between mental illness, extreme ideology and mass violence. Mental illness cannot be blamed for terror attacks, experts say. The overwhelming majority of people with mental illness never turn violent. But mental health disorders may make some people more susceptible to extremist ideology, and in rare cases that ideology can lead to horrific acts. "People who are loners and who become angry and resentful can easily be drawn to extremist ideologies," said Dr. Raj Persaud, a psychiatrist and professor at London's Gresham College. "They begin to dehumanize others and may not need much more motivation before deciding to commit a terrorist attack." It is not known for sure that the Nice attacker, 31-year-old Mohamed Lahouaiyej Bouhlel, was mentally ill. It is also unclear whether he was acting out of personal impulse or was driven by ideology. But the Nice attack and other recent ones, like the attack at a nightclub in Orlando, have involved a murky mix of extreme ideology and hints of mental illness. "Terrorist acts are not caused by mental illness but mental illness can provide a background that's receptive to terrorist activity," said Persaud. Canadian Press (Brando Sun)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
July 26, 2016 / le 26 juillet 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Trudeau's deafening silence on C-51
Thursday, June 21 passed with the usual run of crime, chaos and political lies we've come to know as "the news". But it was an important anniversary - and it went almost unnoticed. A year ago, the Canadian Journalists for Free Expression (CJFE), in partnership with the Canadian Civil Liberties Association, launched a Charter of Rights challenge of Stephen Harper's police state anti-terrorism act, Bill C-51. And not a moment too soon. C-51 handed Canada's spy service grotesque new powers that are unconstitutional, indefensible and unnecessary. Short of killing or sexually assaulting 'persons of interest' in its quest to disrupt activities deemed to be 'dangerous' to national security, CSIS was handed carte blanche by the Harper government. (...) Justin Trudeau did not offer blanket approval. Despite having helped to pass the bill, the Liberals vowed that they would amend it to ensure that it was Charter-compliant. Included in **Minister of Public Safety Ralph Goodale**'s mandate letter are explicit instructions to deal with the offensive sections of C-51. The Liberals promised to protect the rights of Canadians to lawful protest and advocacy, to require that government review all appeals by Canadians on the no-fly list, to rein in the Communications Security Establishment (CSE) by requiring a warrant to engage in surveillance of Canadians, and to hold a statutory review of the entire law after three years. When the

new government came to power after the October 2015 election, party officials assured the public that this deeply flawed "security bill" would be "overhauled without delay." A critical part of the Liberals' promise to amend C-51 was a pledge to hold public meetings to get citizen and expert input on what needed to be changed. Though the government announced the meetings, none have been held - and C-51 remains in force. While it's true that **Goodale** has a full plate in front of him - from prison reform to a broad-ranging national security review - critics of C-51 find the government's inaction disquieting and unacceptable. iPolitics

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Husky oil spill 'not a short-term event' for North Sask. River communities
Drinking water issues facing about 70,000 people along the North Saskatchewan River could persist for weeks and possibly months after a Husky Energy Inc. pipeline spilled more than 200,000 litres of oil near and into the fast-moving water. "It's not going to be a short-term event," said Sam Ferris, executive director of environmental and municipal management services at the Saskatchewan Water Security Agency, during a conference call with reporters on Monday afternoon. "We want to be certain that source water is safe and secure before it is reused for treatment for drinking water purposes ... We need further time just to assess the existence of any oil or globules of oil that may be suspended in the water column," he added. The leading edge of the oil plume passed Prince Albert early Monday afternoon, having travelled about 370 kilometres from the spill site near Maidstone, where the discharge was detected early Thursday morning. Postmedia (StarPhoenix, Leader-Post, Edmonton Sun, Calgary Sun); La Presse Canadienne (Le Devoir, Le Soleil); Canadian Press (Red Deer Advocate, Waterloo Region Record, Times-Colonist, Daily Gleaner, Charlottetown Guardian, Whitehorse Daily Star, St. John's Telegram, Cape Breton Post); Reuters (Globe and Mail)

Sask. oil regulator's budget slashed
The 2016-17 provincial budget in June cut funding of provincial offices tasked with enforcing oil and gas development in Saskatchewan. Government officials confirmed Monday that the Petroleum and Natural Gas branch, which serves as the province's main energy regulator, had its "budget reduced due to a reorganization." The branch got $2.7 million less than the $14.2 million it received in 2016-16. The province said the field staff complement has remained the same, but "we are unable to determine field office budget differences due to that organization." With about 118,000 kilometres of provincially regulated pipeline in the province, there is fewer than one inspector per 1,000 kilometres of pipeline (...) It remains unclear when the pipeline that leaked 200,000 litres of oil into the North Saskatchewan River was last inspected. The province said that, up until November, that data was kept by paper. By late Monday afternoon, the province was unable to track that information down and provide it to media. Government officials were able to confirm Monday that Husky Energy Inc., which owns the pipeline that leaked, had a required emergency response plan in place. The company was expected to file its initial incident report with the province on Monday. StarPhoenix, A5

Two oil-soaked birds pulled from spill site
Four birds, one fish and a frog are among the confirmed fatalities of the Husky Energy pipeline leak that sent more than 200,000 litres of oil pouring into the North Saskatchewan River near Maidstone. Another two oil-soaked birds have been rescued from the spill site and are being cared for by volunteers in Maidstone. Jan Shadick, who runs the Living Sky Wildlife Rehabilitation Centre in Saskatoon, said it's "shocking" how few oil-soaked animals have been found. "It's really quite hard to believe that they haven't found anything," Shadick said from Maidstone, where she is helping coordinate efforts to clean any rescued animals that come in. Leader-Post, A4

Elfros cleanup begins after flash flooding
Janice Schreiner panicked as a wave of water came over the hood of her Ford Focus. She'd been in Wadena when the rain began Saturday, but knew she had to make it to her home in flooding Elfros because her 11 Sheltie dogs were locked inside, she said (...) When she finally made it home, the water in her yard was up to her knees and rushing into her home through windows and any other "crack it could find," she said. She found her dog Brody in his kennel, which was floating, along with her deep-freeze, in

a basement that was filling fast. Brody was fine, other than being a bit wet, but the water was more than 1.8 metres high in her basement before she and her dogs were loaded into trucks and evacuated to Wadena, she said. Everything in her basement was destroyed. The flash flood put the village of less than 100 people onto a growing list of Saskatchewan communities that have fallen victim to severe flooding this summer. Leader-Post, A7

U of C prof gets five more years to predict forest fires
With the help of a NASA satellite, Quazi Hassan is working to anticipate dangerous forest fire conditions across Alberta - even the nooks and crannies of the province unable to be accurately watched in the past. The University of Calgary engineering professor has been at it for five years. And now, he's got the funding to push his project forward another five years. Postmedia (Calgary Herald, A3; Edmonton Journal)

Le ministre Garneau confirme que les DOT-111 ne transporteront plus de pétrole
L'Union des municipalités du Québec (UMQ) se réjouit de l'annonce d'Ottawa concernant les wagons-citernes DOT-111, mais elle estime que «beaucoup de travail reste encore à faire afin de réduire les risques liés au transport de matières dangereuses par train au Canada». Le ministre fédéral des Transports a confirmé, lundi, que les wagons-citernes DOT-111, comme ceux qui avaient explosé lors du déraillement à Lac-Mégantic, ne pourront plus transporter de pétrole brut dès le 1er novembre prochain. La Presse Canadienne (Le Nouvelliste, 15; Le Quotidien); Canadian Press (Times Colonist, B3, Times and Transcript, Daily Gleaner, Telegraph Journal,); Postmedia (Financial Post, National Post, Windsor Star, Calgary Herald, Edmonton Journal, Montreal Gazette, StarPhoenix, Leader-Post, Edmonton Journal, Ottawa Citizen); Agence QMI (Journal de Québec, Journal de Montréal)

Les Québécois inconscients des risques qu'ils courent
Inconscients, mal préparés... et donc, vulnérables. Même si les trois quarts des Québécois vivent dans des zones à risque moyen ou élevé de tremblements de terre, la grande majorité d'entre eux sous-estiment la menace. Pire : les Québécois ignorent non seulement comment réagir en cas de séisme, mais ils ont en plus des réflexes carrément dangereux (...) Les tremblements de terre, ça arrive en Californie et au Japon, mais pas au Québec ? Détrompez-vous. En vérité, les trois quarts des Québécois, dont les Montréalais, vivent dans des zones considérées comme à risque «moyen ou élevé». «C'est vrai qu'on ne parle pas de séismes de magnitude 8 au Québec comme on le fait à Vancouver ou en Californie, précise Maurice Lamontagne, séismologue à Ressources naturelles Canada. Mais ça peut monter à des magnitudes de 6 ou 7. Si ça survenait près d'une grande ville comme Montréal, Québec ou Ottawa-Gatineau, il n'y a aucun doute que ce serait assez pour causer des problèmes et des dommages importants.» La Presse (Le Quotidien, 18; La Tribune, Le Soleil, Le Nouvelliste); Le Devoir

Recovery operation
The search for a Calgary boy swept away by the Yoho River has changed from a rescue to a recovery operation. Behzad Ahmad, 11, fell into the river near the Takkakaw Falls Day Use Area about 7 p.m. Friday while visiting Yoho National Park with his family. Dwight Bourdin, acting resource conservation manager with Parks Canada, said regular monitoring searches with helicopters will take place until the boy is found. He said air searches are the best bet given current water levels. Calgary Sun, A3; Calgary Herald

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Alleged Surrey money launderer seeks bail
A Surrey man wanted in the U.S. for money laundering told an undercover American cop that some of the millions collected would be "wired to Afghanistan where it would potentially be used to fund terrorism," a federal prosecutor told B.C. Supreme Court Monday. Glenn Sheck also boasted during a 2012 meeting attended by the cop that he was "the fourth most wanted gangster in Vancouver," Federal Crown Diba B. Majzub told Associate Chief Justice Austin Cullen. Sheck wants to be released on bail pending his full extradition hearing scheduled for January 2017. But Majzub told Cullen that Sheck should remain in

custody because the U.S. case against him is "very strong." He said Sheck is alleged to have been involved in 23 transactions averaging $300,000 each between 2007 and 2011. One of his associates went to U.S. authorities and became a confidential witness against the Surrey man, Majzub said. Sheck was involved in a scheme known as "double exchanges" where he would direct couriers across the U.S. to pick up money owed for B.C. pot and have it delivered to Los Angeles for cocaine purchases, Majzub said. "The conduct here is very serious in that it involves international money laundering in the order of millions of dollars for the purpose of facilitating cross-border drug trafficking," Majzub said. (...) In another meeting a few days later, "Mr. Sheck talked about a friend who needed $800,000 moved to the Dominican Republic. "He expressed concern that the Dominican Republic was cracking down on money laundering. And he also explained that his friend wanted the money picked up in Toronto and then wired to Afghanistan where it would potentially be used to fund terrorism," Majzub said. "So not only is Mr. Sheck directing large-scale money laundering transactions, he is also involved by his own admission in the funding of international terrorism." Vancouver Sun, A5 (Province)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Brothers convicted in B.C. drug case
Two brothers from Bellingham have been convicted of various charges after attempting to smuggle more than 29 kilograms of cocaine into British Columbia. The U.S. Department of Justice said 46-year-old John Brown Jr. drove to Los Angeles in November 2014 to pick up cocaine, valued at more than $2 million US. The department said Brown contacted his 38-year-old brother, Derrick Carter, to help in the smuggling operation before the pair recruited a cousin and another man from Surrey to carry the cocaine over the border in backpacks. It said Carter was stopped for speeding near the border by a sheriff's deputy and that U.S. Border Patrol personnel later spotted three people running north from the border. Emily Langlie, a spokeswoman from the U.S. Attorney's Office, said RCMP arrested the cousin and the Canadian man with three backpacks containing items including cocaine, camouflage gear and a firearm. Brown and Carter are scheduled for a sentencing hearing in October and face mandatory minimum sentences of 10 years to life in prison. Associated Press (Times Colonist, B5)

Lait diafiltré
Les producteurs laitiers sont parvenus à récupérer une partie des revenus perdus depuis que les grandes entreprises de transformation importent des États-Unis des protéines contenues dans le lait diafiltré. Ce procédé leur permet de baisser les coûts de production dans la fabrication de fromage et autres produits dérivés nécessitant des protéines laitières. Le président du Syndicat régional des producteurs de lait, Daniel Côté, affirme qu'il sera difficile pour les fermes laitières de combler en totalité les écarts de prix entre ce que les producteurs obtenaient avant l'affaire du lait diafiltré et ce qu'ils recevront après la signature de l'entente de principe à l'automne. L'intervention du gouvernement fédéral aux frontières aurait été nécessaire pour réussir à combler les pertes et surtout freiner l'hémorragie. (...)«Quand il est aux États-Unis, il s'agit d'un produit qui peut traverser la frontière sans aucun problème. Quand il est introduit dans les usines de transformation au Canada, le produit qui est un concentré peut redevenir du lait même si les inspecteurs du gouvernement savent qu'il s'agit d'un concentré. Il redevient du lait», reprend Daniel Côté. Le Quotidien, 8

Property issues holding back start of work on Gordie Howe Bridge
Delays in buying properties in Detroit, Michigan, could hold up construction of the proposed 3.2km Gordie Howe International Bridge that will link the US city to Windsor in Canada. A report by the Detroit Free press said that around 30 of the estimated 900 parcels of land in the city's Delray district could pose potential problems if owners resist selling the sites to the bridge's developers. The newspaper noted that Dwight Duncan, interim chair of the Windsor-Detroit Bridge Authority - the Canadian entity managing the project - said about 20 of 30 parcels belong to businessman Manuel (Matty) Moroun, owner of the 2.3km Ambassador Bridge that already spans the Detroit River. Wold Highways

City legal fees come in at $1.3M more than expected
The City of Windsor will likely spend $1.3 million more than budgeted on lawyers' fees this year - three times what was forecast. The extra legal bills mainly represent fallout from battles over the bridge, bingo

and the 2014 election. "We see that legal expenses are increasing in general," Mayor Drew Dilkens said Monday. "We see that in the claims being made, that the slip and falls are a little more aggressive. Where people used to say, 'It was my fault,' now people will look to the city for some compensation. (…)The city also paid more than expected in legals costs for its challenge to the Ambassador Bridge's application to build a twin span, as well as heading to the Supreme Court to battle the bridge on its assertion that the Canadian Transit Company need not follow city bylaws since it is a federal entity. Finally, the city paid extra to defend two challenges alleging improprieties with the 2014 municipal election. One election challenge was dismissed in court while the other is ongoing. Windsor Star, A1

CYBER SECURITY / CYBERSÉCURITÉ

DNC email hack: A look at the theory Russian operatives led attack to boost Trump's bid
Days after a massive leak of hacked emails threatened to spoil the Democratic Party's convention kickoff, political operatives and assorted experts continue to debate whether the attack was a Russian plot to boost Donald Trump's presidential bid. Donald Jensen, a resident fellow at the Center for European Policy Analysis and expert on Russia, says the potential motive is obvious. "Certainly the Kremlin prefers Trump, there's no question about that at all," he said (…) A cybersecurity firm the Democrats hired reportedly found traces on the party's network of at least two sophisticated hacking groups that have ties to the Russian government. In an interview with Democracy Now, Wikileaks founder Julian Assange refused to reveal the source of the emails, but said when it comes to the DNC, "there's lots of consultants that have access, lots of programmers." "And the DNC has been hacked dozens and dozens of times. Even according to its own reports, it had been hacked extensively over the last few years." In a later interview with NBC, Assange said there's "no proof … whatsoever" that Russian intelligence was responsible for the hack. The FBI announced Monday it's investigating. CBC News; Washington Post (Leader-Post, StarPhoenix, Vancouver Sun, Montreal Gazette, Edmonton Journal, Calgary Herald, Windsor Star, National Post, Ottawa Citizen); Globe and Mail; AFP (Le Nouvelliste); Canadian Press (Telegraph-Journal, Winnipeg Sun, Edmonton Sun, Toronto Sun, Kingston Whig-Standard, Calgary Sun, Ottawa Sun, Waterloo Region Record)

Courriels démocrates - "La publication de WikiLeaks n'est pas un "scoop"
Un article d'opinion dit « pour WikiLeaks de publier ces courriels ? WikiLeaks a besoin d'exister et de publier régulièrement. Mais je ne suis pas sûr que cette publication leur profite, ni sur le crédit ni sur la confiance que l'on peut accorder à leurs publications. Le problème est que, contrairement à d'autres lanceurs d'alerte comme Edward Snowden [l'ex-consultant de la National Security Agency (NSA) à l'origine des révélations sur le programme de surveillance de la NSA], WikiLeaks est dépendant de ses sources et surtout de la qualité des informations que des tiers lui apportent. Il y a eu violation des correspondances, mais il n'y a pas en contrepartie le bénéfice de la désignation d'un péril supérieur, qui justifierait la violation du secret des correspondances. De plus, même si ce n'est pas systématique, WikiLeaks a pris l'habitude de s'adjoindre les médias, qui venaient mettre en perspective et raffiner leur matière brute. Ici, il y a juste la mise en ligne de données, mais pas de travail éditorial autour. On peut s'interroger sur le fait qu'il n'y ait pas eu de média qui ait été mis dans la boucle. Ont-ils estimé que le jeu n'en valait pas la chandelle ?» Le Devoir, B5

LAW ENFORCEMENT / APPLICATION DE LA LOI

Ottawa man Abdirahman Abdi dies after confrontation with police
Abdirahman Abdi died on Monday afternoon, a day after a confrontation between him and police prompted a Special Investigations Unit probe into how the 37-year-old Somali-Canadian man suffered fatal injuries during his arrest. In a statement, the SIU said Abdi attempted to elude arrest and led police on a foot chase through Hintonburg in the Wellington Street West and Fairmont Avenue area on Sunday morning, the SIU said in a release. The SIU said police confronted a man outside 55 Hilda St. and that "at some point during the confrontation, the man suffered medical distress." The SIU -- a civilian oversight agency -- investigates cases resulting in serious injury, death or sexual assault when police are involved. The details around what happened between Abdi and police remain scattershot and incomplete. The

Ottawa police and SIU have said little because the investigation is ongoing. However, witness accounts have shed some light on the events that led to Abdi's death. Witnesses who spoke with Postmedia said the man was beaten by multiple officers as he tried to run into an apartment building on Hilda Street. "You can't go against five cops at once," said witness Asli Mohamed. "It was unnecessary." Witnesses also said Abdi lay unconscious on the ground for about 10 minutes minutes before paramedics arrived and began administering CPR. However, on Monday, Ottawa police Chief Charles Bordeleau said officers called paramedics 23 seconds after Abdi collapsed. He said officers also administered CPR. Postmedia News (Calgary Sun, Edmonton Sun, Winnipeg Sun, Toronto Sun, Ottawa Sun)

Memorial plaque to be unveiled Wednesday

A bronze plaque marking the death of RCMP Const. Sarah Beckett will be formally unveiled at the West Shore detachment on Wednesday. The plaque reads "In honour of the memory of RCMP Constable Sarah Anne Beckett, regimental # 51939, perished in the line of duty April 5, 2016." Beckett, a 32-year-old mother of two children, died after a pickup collided with her vehicle in the intersection of Peatt Road and Goldstream Avenue. The driver of the pickup was taken into custody, but released the next day without charges. An investigation is ongoing. Beckett's family will be in attendance at the ceremony along with Langford Mayor Stew Young. The gathering will be held in front of the main entrance of the detachment at 698 Atkins Ave. Times Colonist, A5

Slain man 'not intended target': NO CRIMINAL RECORD: Police believe Surrey shooting victim was case of mistaken identity

A Surrey man with no links to an ongoing gang conflict has been identified as the victim of a fatal shooting Saturday. Staff Sgt. Jennifer Pound of the Integrated Homicide Investigation Team said Monday that Jatinder "Michael" Sandhu, 28, may not have been the intended target of the killer or killers who sprayed the vehicle he was in with gunfire about 10:20 p.m. on July 23. She said the shooting in the 14300-block 90A Avenue is believed to be part of an ongoing gang conflict involving street-level players in the drug trade. (...) "While the injured male does not possess a criminal record, he is related to an individual involved with the conflict and police continue to look into his direct involvement and/or connections to the current conflict," Pound said. She said investigators have done extensive canvassing in the area "and information from the public continues to be processed." "A suspect was witnessed fleeing the scene in a grey or silver Infiniti SUV (unknown year) and IHIT is asking for the public's assistance to locate this vehicle," Pound said in a news release. "Police would like to remind individuals that just because you're not directly involved in criminal activity or violence as a result of conflict, does not mean that you're immune to the associated risks. Province, A6 (Vancouver Sun)

Couple charged with attempted murder

Two Reginans appeared in court accused of a string of serious offences after RCMP officers were shot at during an evening of high drama near Punnichy. Kristin Marie Lerat, 32, is charged with attempted murder, fleeing from police, dangerous use of a motor vehicle, robbery with a firearm and other offences. Among other charges, Keli William Stonechild, 24, is accused of attempted murder as well as operating a vehicle while impaired and failure to comply with a recognizance. The sequence of events began after the Regina Police Service was called to a morning assault at the 1300 block of King Street on July 19, in which a 26-year-old woman was hospitalized with non-life threatening injuries. With police concerned that weapons were in the home, a SWAT team cleared the block but the house was found to be unoccupied. The next day at around 8:40 p.m., city police alerted the RCMP that a vehicle containing armed occupants was northbound on Highway 6 having fled an investigation. Regional RCMP teams then mounted a search for a white Dodge Caravan. After a motorist on Highway 6 north of Southey reported a gun being fired into a field from a matching van, at about 9:50 p.m. the Dodge was spotted in Punnichy, with local RCMP giving chase. Speaking Monday, Sgt. Craig Cleary of Punnichy RCMP described the scene's final moments, which included an alleged attempt to carjack a 65-year-old man, who suffered minor injuries after a long-barrelled firearm was drawn, but not fired. Star Phoenix, A3

Calves stolen from barn in Freetown

The East Prince RCMP is requesting the public's assistance regarding a theft of two calves that occurred overnight Saturday. The animals were taken from a barn on Route 8 in the Freetown area. The owner advised RCMP that a rope, which secured a fence on the property, was untied. "It appears the suspect

(or suspects) entered the property through an alternate driveway, and footprints and tire marks were located leading to the barn," said a statement issued Monday by the RCMP. "It is not something we see a lot of," said S/Sgt. Kevin Baillie. "The gentleman who owns them put the cows in the barn around 6 (p.m. Saturday), came out (Sunday) morning to feed them. The barn door was shut as it was the night before, but two calves were missing. "He went to a fence that leads out to a field, an alternate driveway, and the rope that secured the fence was not tied the way it is normally tied. "He noticed footprints and tire tracks," said Baillie. "We are quite confident they were stolen," he said. "It wasn't a case of them just getting loose in the barn." He said there is no bad blood among neighbours, no history of conflict, no land disputes. "There is nothing that could be a possible motive," said Baillie. Guardian, A3

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Inmate dies at Collins Bay institution
Correctional Service Canada has released a report on the death of an inmate. Christopher Leach, an inmate at Collins Bay Institution died at Bath regional hospital last week. He was 58 and had been serving an indeterminate sentence since September 19, 1997 for second degree murder. As in all cases involving the death of an inmate, the police and the coroner have been notified, and Correctional Service of Canada will review the circumstances. Napanee Today (2016-07-25)

Antigonish man who killed 2 teens while driving high granted parole
A Nova Scotia man serving a six-year prison sentence for killing two teenage boys in Antigonish County while driving impaired has been granted parole. On Nov. 24, 2011, William Lionel Edmund Byron Fogarty was driving a car on Highway 4 in Tracadie, N.S., when it crossed over the centre line and collided with another vehicle. The other car's driver, 16-year-old Kory Mattie, died at the scene. Seventeen-year-old Nicholas (Nico) Landry, a passenger in the vehicle, died of his injuries later in hospital. A drug test revealed Fogarty had methadone, several prescription drugs and Valium in his system at the time of the crash. Fogarty was convicted of two counts of dangerous driving causing death and two counts of impaired driving by drugs causing death. He was sentenced to six years in prison, less time served, in September 2013. Last week, the Parole Board of Canada granted Fogarty's parole. He will first be released on a six-month day parole program, and will live in a community-based residential facility. Fogarty will be released on full parole to live with family members once the six-month day parole is successfully completed. "The Board is of the opinion that, if released on day parole, you would not present an undue risk to society by reoffending, and that such a release would contribute to public protection by facilitating your reintegration into society as a law-abiding citizen," said parole documents released by the Parole Board of Canada. CBC News

Man exposes himself in Brunswick Square
A man was arrested Friday afternoon in Brunswick Square after exposing himself to a female sales clerk. Saint John Regional Police received a call from Brunswick Square security when the man who had committed the act the night before was spotted in the mall. The 33-year-old, who was on parole, was arrested at 2:41 p.m. on Friday. His parole was revoked. He was transported to provincial jail on a warrant and was released to appear in court on charges of committing an indecent act. Telegraph-Journal

Second sex assault gets 40 months
Jeffrey Lee Hogg sentenced by Provincial Court Judge Nancy Orr to 13 months longer than a similar conviction in 2012. Orr said the need for deterrence is "much more significant" in this case because Hogg was still on parole for second offence. The Guardian

Les Hells «purs et durs» de retour
«Les Hells Angels deviendront l'organisation criminelle la plus importante au Québec en 2016 et au cours des prochaines années», ont récemment confié à La Presse des sources policières spécialisées dans la lutte contre le crime organisé. Les membres québécois de cette organisation en ont peut-être donné un avant-goût en fin de semaine, dans la région d'Ottawa, alors qu'ils se sont rendus nombreux au Canada Run, le rassemblement de tous les Hells Angels canadiens qui a lieu tous les quatre ans, en alternance, dans les provinces canadiennes. Selon nos informations, au moins une trentaine de membres en règle

des sections de Montréal, South et Trois-Rivières ont pris part à l'événement, en compagnie de membres de leurs principaux clubs-écoles ou supporteurs : Red Devils, Devils Ghosts, Deïmos Crew et Beast Crew. L'absence de deux influents membres en règle Mario Brouillette et Michel Lajoie-Smith a toutefois été remarquée. Brouillette, que la police a déjà considéré comme un chef potentiel pour l'organisation au Québec, a déclaré devant les commissaires aux libérations conditionnelles avoir quitté les Hells Angels. Quant à Lajoie-Smith, certaines informations veulent qu'il se soit retiré lui aussi. Mais dans les deux cas, la police les considère comme faisant toujours partie de l'organisation, que ce soit avec des couleurs dans le dos d'une veste ou non. La Presse (Le Droit, 5, Le Nouvelliste, La Tribune, Le Quotidien)

Dauphin Correctional Centre inmate death under investigation
Corrections officials won't say how a man in custody at the Dauphin Correctional Centre died earlier this month. The inmate's name is not being released but Manitoba Corrections said he died July 14 and his family has been notified. "For privacy reasons, we are unable to provide additional information about the deceased person," Manitoba Corrections said. "We have launched an internal review and reported the death to the Office of the Chief Medical Examiner, as required by law," a spokesperson said. "We have also offered support and counselling to affected offenders and staff at DCC." It has not been made clear how the man died. RCMP have ruled out any likelihood it was the result of a crime. "Our investigation so far has not revealed any criminality to this incident, and no charges are expected," said RCMP spokesperson Sgt. Bert Paquet. Manitoba Corrections has launched an internal investigation. A spokesperson said there has not been a death at the facility in at least 28 years, which is as far back as records were readily available. CBC News (2016-07-25)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Sudbury safer, stats indicate
When it comes to crime, it appears Greater Sudbury is bucking a national trend. Last week, Statistics Canada released police-reported crime statistics for 2015. For the first time in 12 years, the Crime Severity Index and Crime Rate increased in Canada. Ontario's Crime Severity Index increased by 2 per cent; however, Greater Sudbury had the second largest percentage decreases in Ontario in both the crime severity index (-3 per cent) and crime rate (-5 per cent) in 2015. "The Greater Sudbury Police Service cannot take sole credit for the decrease in the crime severity index and the crime rate here in Greater Sudbury," Greater Sudbury Police Chief Pedersen said in a release. "It is a team-based approach to safety, security and wellness that could not be achieved without the support of our community."The citizens of the City of Greater Sudbury continue to demonstrate a commitment to community safety and well-being by showing respect, vigilance and tranquility." The statistics are based on the crime severity index and crime rates broken down by province and by census metropolitan area. Sudbury Star

Les 150 ans du Canada risquent de coûter cher à la police d'Ottawa
Le Service de police d'Ottawa prévoit terminer 2016 avec un budget équilibré malgré les pressions fianncières causées par le nombre élevé de meurtres et de fusillades dans les six premiers mois de l'année. Mais 2017 s'avère déjà un défi, alors que les nombreuses activités entourant les festivités du 150^{e} anniversaire de la Confédération lui entraîneront d'importantes dépenses. «Si les festivités de la fête du Canada durent deux semaines, ce sera un énorme défi pour nous, un défi très coûteux pour nous», a illustré le chef de la police d'Ottawa, Charles Bordeleau, lundi, devant le comité des finances et de la vérification des services policiers de la Ville d'Ottawa. Le gouvernement fédéral verse une somme de 2 millions $ par année au Service de police d'Ottawa (SPO) afin d'éponger certaines dépenses encourues lors d'événements comme la fête du Canada, le 1er juillet. Le problème pour le SPO est qu'il ne connaît pas encore toutes les activités que le fédéral organise dans la capitale, des activités qui seront différentes de celles que prévoit Ottawa 2017, avec qui la police travaille présentement pour se préparer dans sa gestion des effectifs. «Tout dépendamment de la grosseur et de la fréquence des événements, nous pourrions devoir examiner la possibilité d'imposer des restrictions additionnelles sur les congés de nos membres en 2017», a prévenu le chef Bordeleau. La Presse (2016-07-25)

Northern plights

An editorial states, "The 134 members of Canada's largest First Nations police force are threatening to go on strike in August, and the ultimatums are flying. Alvin Fiddler, Grand Chief of the Nishnawbe-Aski Nation, says he will disband the Nishnawbe-Aski Police Service (NAPS) unless it is properly funded by the Ontario and federal governments, which hold the purse strings. He wants officials from both governments at the bargaining table. But Ontario and Ottawa are balking. Officials from both levels of government say the labour dispute is between the officers' union and their employer. They have no interest in taking part in the negotiations. But they add that they are prepared to have the Ontario Provincial Police step in to provide coverage, should NAPS officers walk off the job. The Chief's demand that Ottawa and Ontario get involved directly is reasonable. NAPS was created by the federal and provincial governments in 1994 to provide culturally sensitive policing to 200,000 square kilometres of territory in northern Ontario. The force's 134 officers and 30 civilian employees serve 23,000 people across 35 remote communities, many of which are afflicted by chronic alcohol and substance abuse and concomitant problems of family violence and suicide. NAPS officers often patrol alone, a dangerous practice. They work out of plywood shacks heated by oil drums. There is no running water in some of these so-called detachments. Prisoner cells in many are made of plywood. Two prisoners burned to death and one officer was injured when a detachment caught fire in 2006. Ottawa and Queen's Park promised in the past to improve conditions but did nothing." Globe and Mail, A10

Political will needed to rein in price of policing

An editorial states, "When the Winnipeg Police Service released its 2015 annual report last week, the headline and key concern it reported was obvious - the crime rate had climbed for the first time in a decade. There was an equally or even more important trend hiding in plain sight on the report's first page. It was a dollar figure that, when compared with a decade of declining crime stats, put last year's $261-million cost of supporting public safety through our police service in a personal perspective. In 2005, the so-called "tax supported cost" of policing was $195.40 per citizen. Last year, it was $363.45. That's with a 2015 population of 718,000, and a full 67,000 citizens more to be factored into the per capita cost since 2005. It's not as if Winnipeg is the only Canadian city with a police budget problem. Three years ago, the per capita cost of policing in Toronto was $352 , about $11 less than Winnipeg's this year. Ballooning police budgets - Winnipeg's is $280.7 million this year - are a well-documented national problem. So, for that matter, is the price of the fire and paramedic service, which amounted to a $190 million allocation for this year. Last March - when the 2016 budget was being debated - politicians finally signalled they were ready to begin addressing the out-of-control costs of policing in our city. There was serious talk of police layoffs. No one wanted that, and with some non-core cutting - $1 million for the introduction of body-cameras, for example - the police budget was passed and the service's 1,916 total cop and staff body count - up by more than 350 since 2005 - held steady." Winnipeg Free Press, B1

New police must count

An editorial states, "Facing a massive city hall agenda before summer break, councillors had myriad topics to wade through Monday, such as the never-ending secondary suite issue, transit passes and the ethics report into the mayor's comments on Uber. But one item that took no time at all was the Calgary Police Service's request for 50 more officers at a cost of $7.5 million. The manpower was proposed to be funded by the increase in revenue that has occurred since the provincial government raised fines for speeding, running red lights and other offences in the spring of 2015. With soaring city crime figures, which coincidentally came out last week, it was a hard argument to reject. And council didn't, voting unanimously to hire the crimefighters. And that's what we hope they will be - officers assigned to tackle the burgeoning thefts and robberies and break and enters afflicting our city. We expect they won't be out en masse nabbing speeders to generate more revenue to pay for even more police in a self-fulfilling scenario. We expect these additional officers on the street will make a difference in the numbers and types of crime being committed in our city. Statistics Canada numbers released July 20 show that a growing number of thefts - including robberies and stolen cars - has pushed the city's Crime Severity Index (or CSI), to its highest level since 2009. That increase, at 29 per cent, is the largest of any municipality across the country. Crime in Calgary had dropped for 11 consecutive years before 2015. The police attributed the numbers to a struggling provincial economy and the prevalence of highly addictive drugs such as fentanyl and methamphetamine. Whether it's due to addicts needing to feed their addiction or homeless individuals needing to feed themselves, the crimes on the rise affect us all. Police Chief

Roger Chaffin is correct in saying, "These are the crime trends that tend to affect public confidence.'" Calgary Herald, A9

Pokemon Go can be good for your mental health
An opinion piece states, "We're hitting the middle of the summer this week. July is almost over and we're heading into the long hot days of August. The kids are having fun, playing the new Pokemon Go game, getting out and about in groups, exploring the city. But all is not as well as it seems. Last week, the Centre for Addiction and Mental Health reported that one-third, 34 per cent, of Ontario students experience increased levels of psychological distress. That's an estimated 328,000 kids. That's a lot of kids. And more disturbing is that this is a 10 per cent increase over the 2013 number. The situation, it seems, is getting worse. (…) Social media has had a huge impact on society. Over the past 10 years, we've seen technological innovations that have put a computer in almost everyone's pocket. The development of applications has exploded as developers find ever new and amazing ways to make our lives easier and keep us constantly entertained. Got a problem, I bet there's an app for that. Bored? Angry Birds, Candy Crush, and Farmville to the rescue. But the downside is not pretty. Dr. Hayley Hamilton, co-investigator of the study, highlighted the connection between time spent on social media and the increased risk of cyberbullying. We've seen the real life impacts over the past few years in the cases of Rehtaeh Parsons and Amanda Todd, to name just two Canadian kids who killed themselves over cyberbullying. The number of American examples is much greater." Hamilton Spectator, A13

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Road warriors: Epic journeys raise funds, awareness
Mark Quattrocchi rode up a rough, dusty path into the small village of El Trapiche on a bicycle laden with bags. The 28-year-old Ontario teacher had pedalled more than 20,000 kilometres from China to Nicaragua. A group of local boys on bikes watched the stranger approach, and fell in beside Quattrocchi as he headed down the last hill. (…)Then there's Gwich'in First Nation native Brad Firth (who is also known as Caribou Legs.) He is running along the Trans-Canada Highway from Vancouver to St. John's in an epic effort to get more people to pay attention to the issue of missing and murdered indigenous women. Quattrocchi says by the time he had biked through China, he had raised enough to build a school room. Rather than stopping at the border, he plotted a new route that allowed him to visit all of the other communities in India, Kenya, Ecuador and Nicaragua where he wanted to build school rooms. Postmedia Network (Calgary Herald, C1, Leader-Post, Starphoenix, Montreal Gazette, Edmonton Journal, Windsor Star, Vancouver Sun, Ottawa Citizen)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Premiers push for pot policy
An opinion piece states "Canada's premiers are signaling they need swift action from Ottawa on recreational marijuana legalization to keep cannabis away from kids, motorists and criminals. With a federal panel set to deliver a report this November that will be the blueprint for legislation next spring, the provincial leaders say time is of the essence. "There's real concerns, there's concerns on so many levels," Manitoba Premier Brian Pallister said Thursday at the annual Council of the Federation meeting. "I would hope that we can develop a national approach, a co-operative approach, rather than each of us going in our own separate ways. (…) "Young people should not have access to marijuana before they're of age. People should know - if they're consumers of it - that the product that they're getting is what they expect and the criminal element must be kept out," Clark said. "Those are the three things I'm most concerned about. We need to see the federal legislation. Then once we get through that we will build a system … that complies completely, but it will be focused on safety." Guardian

Let lounges sell pot like bars sell alcohol, forum told

Marijuana bars that sell pot rather than alcohol should be licensed to operate in Toronto, a city councillor's forum on marijuana distribution heard Monday. Coun. Jim Karygiannis, who represents Ward 39 Scarborough-Agincourt, called the meeting to give frustrated medical marijuana distributors and their supporters a chance to air their thoughts, after controversial police raids in May led to hundreds of charges against owners and employees at 43 Toronto marijuana dispensaries. (...) The federal government has promised to legalize and regulate recreational marijuana use in 2017. But some dispensaries are already selling marijuana from storefront operations, mainly to medicinal users. CBC News (2016-07-25)

PUBLIC SERVICE / FONCTION PUBLIQUE

Opposition parties want probe of Phoenix 'debacle'

As the federal government was scrambling to make sure hundreds of civil servants get paid this week, the opposition parties joined forces Monday to call for emergency hearings into the government's problem-plagued new payroll system. Newly released documents from one of the government's biggest departments show that questions about "critical defects" in the so-called Phoenix system were going unanswered just weeks before its scheduled launch. Both the Conservatives and New Democrats demanded the government operations committee be recalled to talk about how Phoenix has resulted in tens of thousands of civil servants being improperly paid -or not paid at all. "I would hope that Liberal committee members would welcome an opportunity to examine what lead to this fiasco, why it has taken so long to get clear answers, and why we have yet to receive clear timelines for resolution of numerous problems," NDP public works critic Erin Weir said in a statement. (...) "We are truly disappointed to see the Liberal members of this committee ignore our request to convene an emergency meeting," said Conservative public services critic Steven Blaney. "After reaching out to their offices, and receiving no response, it is clear that this issue is not a priority for them." Prime Minister Justin Trudeau said last week that the clerk of the Privy Council, which advises him and his cabinet on government operations, would head up efforts to fix the system, which has left more than 80,000 civil servants facing pay issues. Canadian Press (Red Deer Advocate, A5, Whitehorse Daily Star, Telegraph-Journal, Waterloo Region Record, Hamilton Spectator, Globe and Mail); Presse canadienne (Le Droit, 7, Le Nouvelliste); Ottawa Citizen, A8; La Presse

OTHER / AUTRE

Wife of Calgarian held captive in Turkey allowed brief visit

Friends and relatives say a Calgary man being detained in Turkey has been allowed to see his wife, but the visit was too brief to glean much information about how Davud Hanci is faring and what might happen next. Hanci's wife, Rumeysa, called from a police station in Turkey on Monday to say she was able to see her husband for between 30 seconds and a minute, said her brother Selman Durmus, who lives in Toronto. "All she could ask is, 'How are you?' to my brother-in-law and that was pretty much it," said Durmus, relaying what another sister, who also lives in Toronto, told him about the call. "He said he was doing all right. He was stressed out. That was pretty much it." Hanci, an imam who provides spiritual counselling to prisoners, is being held on accusations he was involved in a July 15 coup attempt in Turkey, Durmus said. Pictures are being circulated in Turkish media showing a man purported to be Hanci with U.S.-based cleric Fethullah Gulen, a critic and former ally of Turkish President Recep Tayyip Erdogan. "They do look alike, but they're not the same person at all," said Durmus. Hanci's family members are waiting to hear from Turkish prosecutors about what happens next. Hanci, his wife and two sons, 8 and 9, left for Turkey on July 7 to visit his ailing father. Had the father not been so gravely ill, it's likely they would have opted to take the trip another time, given the political instability in the country, said Durmus. He fears for the safety of his sister and nephews if they stay in Turkey. He said Canadian government officials have told the family they can help get Hanci's wife and children out of the country, but cannot provide security while they're there. A spokeswoman for Global Affairs said in an email Saturday night that the department is "aware of a Canadian dual-citizen detained in Turkey" and that Canadian consular officials are ready to assist if needed. Canadian Press (Calgary Herald, A10, Winnipeg Sun, Calgary Sun, Daily Gleaner)

Canadien détenu
L'ambassadeur de la Turquie à Ottawa a été convoqué à une rencontre avec les autorités canadiennes à la suite d'informations selon lesquelles le gouvernement turc a arrêté un homme de Calgary relativement à la tentative de coup d'État avorté dans ce pays. Des médias turcs ont soutenu que Davud Hanci a aidé à orchestrer la tentative de coup du 15 juillet, au cours de laquelle plus de 200 personnes ont été tuées. Des photos semblant montrer M. Hanci avec Fethullah Gülen, un religieux musulman établi aux États-Unis accusé par le régime du président Recep Tayyip Erdogan d'avoir organisé le soulèvement, se retrouvent un peu partout dans les journaux en Turquie. Presse canadienne (Acadie Nouvelle, 15, Le Nouvelliste); Canadian Press (Ottawa Citizen, Vancouver Sun)

INTERNATIONAL

Church hostage situation in France ends with priest, 2 attackers dead
Two attackers killed a priest with a blade and seriously wounded another hostage in a church in northern France on Tuesday before being shot dead by French police. Another person inside the church was seriously injured and is hovering between life and death, Interior Ministry spokesman Pierre-Henry Brandet said. Police managed to rescue three people from the church in the small northwestern town of Saint-Etienne-du-Rouvray, Brandet said. The hostage-taking occurred during morning mass, he told reporters. There were no immediate details on the identity or motives of the two assailants, but the investigation was handed to the anti-terrorist unit of the Paris prosecutor's office. Associated Press (CBC News, CFRA News); Daily Mail

Une attaque au couteau fait 19 morts
Dix-neuf personnes ont été tuées et 25 blessées lors d'une attaque au couteau dans un centre pour handicapés mentaux au Japon, perpétrée aux premières heures mardi par un ancien employé. «Les médecins ont confirmé la mort de 19 personnes», a déclaré à l'AFP un porte-parole du département des pompiers. Parmi les blessés, 20 sont gravement touchés, a-t-il précisé. La police avait fait état un peu plus tôt de plus de 10 morts. Un homme âgé d'une vingtaine d'années s'est rendu à la police après 3 h mardi (18 h GMT lundi), disant être l'auteur de la tuerie, a indiqué à l'AFP un porte-parole de la police de la préfecture de Kanagawa, dans la région de Tokyo. «Nous sommes en train d'essayer de déterminer les détails de l'affaire», a ajouté le porte-parole. La police avait auparavant reçu un appel du centre les alertant de l'agression, qui s'est déroulée à Sagamihara, une ville de plus de 700000 habitants située à une cinquantaine de kilomètres de Tokyo. Le meurtrier présumé, identifié comme Satoshi Uematsu, 26 ans, a affirmé être un ancien employé, selon l'agence de presse Kyodo. Agence France-Presse (Le Droit, 3, Le Soleil, Voix de l'Est, Le Devoir)); Associated Press (Times Colonist, B5, CBC News); Canadian Press (Cape Breton Post, B4)

German officials vow more checking of refugees after attacks
Top security officials in Germany called Tuesday for tougher security screening of asylum-seekers and also announced that more police officers will be hired following four attacks in the country — two of them claimed by the extremist ISIS group. Horst Seehofer, the interior minister of Bavaria — where three of last week's attacks took place — told the daily Sueddeutsche Zeitung Tuesday: "We must know who is in our country." Thomas Strobl, the interior minister of Baden-Wuerttemberg — where a woman was killed by a Syrian attacker Sunday — also demanded a tougher stance toward asylum-seekers. "Those who abuse the right to hospitality must go back to their home countries — make no mistake about it," Strobl told Funke media group. Three of the attacks were carried out by recent immigrants, rekindling concerns about Germany's ability to cope with the estimated 1 million refugees registered entering the country last year. Associated Press (CBC News); Bloomberg (Toronto Star, A4)

Brazil police arrest last suspect in Olympics terror case
Police arrested the last suspect sought in the case of a group of Islamic State sympathizers who allegedly discussed attacking the Olympics in Rio de Janeiro. The Federal Police said in a statement late Sunday that the man was caught in the city of Comodoro, in the central west region of Brazil. Police said he was taken to a federal prison but didn't reveal his name, citing security reasons. The anti-terror probe was

announced by authorities last week when 10 Brazilians were arrested in different states of Brazil. Another man turned himself in on Friday. Justice Minister Alexandre de Moraes said some of the men had pledged allegiance to the IS without having any personal contact with members of the terrorism group. The suspects also didn't know each other and only communicated via WhatsApp and Telegram. Moraes said the group was amateur and ill-prepared. The closest it got to planning an attack was an alleged attempt via email to buy an AK-47 assault rifle in a store in Paraguay. Associated Press (Waterloo Region Record, Globe and Mail) (2016-07-25)

Did Saudi Arabia play role in 9/11?

An opinion piece states, "In the Middle East, it can be difficult to tell the difference between a friend and an enemy. For decades, the United States treated Saudi Arabia as a friend and ally, while the Saudis treated America as an enemy. A newly declassified report highlights this betrayal. In 2002, the United States Congress released its inquiry into the 9/11 attacks. But for 14 years, it kept 28 pages hidden from the public. Those pages were finally released last week. They outline possible connections between al-Qaida terrorists, Saudi spies in the U.S. and members of the Saudi royal family. While the Obama administration and Saudi Arabia's rulers insist the pages provide no conclusive evidence of official Saudi involvement in 9/11 - a view repeated by mainstream media - the report itself offers a somewhat different perspective." Winnipeg Sun, A9

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
July 31, 2016 / le 31 juillet 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Up to 100 homes evacuated near Vernon due to wildfire
Vernon Fire and Rescue Services says it is battling a wildfire in the Adventure Bay area near the city on the west side of Okanagan Lake above Tronson Road. Captain Trevor Keenan says RCMP officers are assisting in getting residents from 100 homes out of the area. CBC News

Crews dig up breached oil pipeline
The Saskatchewan government says the breach that leaked up to 250,000 litres of oil and other material into a river earlier this month has finally been found, but word on what caused it will have to wait. Laurie Pushor, the deputy minister of the economy, says the section of the Husky Energy pipeline where the spill

occurred into the North Saskatchewan River near Maidstone, Sask. on July 20 was dug up Friday. Canadian Press (Edmonton Sun, A7)

Storm wallops city again
Another storm rolled through Edmonton Saturday evening flooding Whitemud Drive and stranding motorists for the second time this week. The storm also forced the early closure of the Heritage Festival. K-Days, meanwhile, pushed on despite the weather... Emergency services were deployed to help stranded motorists under both the 106 Street and 111 Street overpasses on Whitemud Drive and portions of the highway were closed as a result of the flooding around 6 p.m. Edmonton Sun, A5

NATIONAL SECURITY / SÉCURITÉ NATIONALE

LE QUÉBEC EST UN MODÈLE À SUIVRE
Une sommité française en matière de lutte contre la radicalisation soutient que le Québec est un modèle à suivre en la matière pour la France, ciblée par de nombreux attentats récemment. «Le Québec et le Canada sont en avance sur la France, notamment en ce qui concerne la réflexion et les indicateurs d'alerte. Ils sont aussi en avance sur le processus de déradicalisation», avance Dounia Bouzar, une anthropologue française et fondatrice du Centre de prévention contre les dérives sectaires liées à l'Islam (CPDSI). Agence QMI (Journal de Québec, 16)

Snowden made Canadian spies review contractor policy
When Edward Snowden begin leaking secrets about mass surveillance in the United States, Canada's electronic spy agency quietly wondered if their security screening was sufficient to stop a copycat. Newly released documents show some of the behind-the-scenes actions taken by the Communications Security Establishment (CSE) three years ago, when contractor Snowden first pulled back the curtain on the West's pervasive mass surveillance capabilities. Toronto Star, A4

Canada's electronic spies revealed
EONBLUE: The Communications Security Establishment's EONBLUE program tapped into the physical infrastructure of the Internet, collecting data at real-world choke points, according to documents published by Der Spiegel newspaper. The program reportedly allows CSE to collect vast amounts of information, as well as conduct cyberdefence and potentially offensive actions. Levitation: Another tool in CSE's mass surveillance box, Levitation tracked between 10 million and 15 million downloads and uploads to popular file-sharing sites per day, according to documents reviewed by CBC. Of the hundreds of millions of interactions tracked, CSE found approximately 350 "interesting downloads" per month, the outlet reported. Toronto Star, A4

'They were out of their league'
A retired RCMP inspector who helped develop the 'Mr. Big' sting tactic in B.C. believes the officers in the Canada Day terror probe were "out of their league" while investigating John Nuttall and Amanda Korody. "The police that were engaged in this particular investigation never had the experience to be running something of this nature," former Mountie Al Haslett said. "They were not experts in undercover work and they were out of their league." Nuttall and Korody were arrested in July 2013 as part of a police sting after planting what they believed were pressure-cooker bombs at the B.C. legislature on Canada Day. Canadian Press (The Province, A4)

Impact on RCMP unclear after entrapment ruling in B.C. terror trial: lawyer
It's unclear what the impact on law enforcement will be in the wake of a landmark court decision that slammed the RCMP for investigative methods it used during an elaborate undercover operation into two terrorist suspects, a legal expert says. Micheal Vonn of the B.C. Civil Liberties Association said police would do well to reconsider their anti-terrorism tactics after Friday's B.C. Supreme Court ruling tossed out guilty verdicts against John Nuttall and Amanda Korody. Canadian Press (Times Colonist, A6; Ottawa Sun)

Des méthodes de la GRC remises en question
Le jugement rendu vendredi reprochant à des agents de la Gendarmerie royale du Canada (GRC) d'avoir piégé un couple pour que celui-ci soit ensuite accusé de terrorisme créera un précédent qui, selon plusieurs experts, demeure vague. Le directeur général de l'Association des libertés civiles de la Colombie-Britannique, Micheal Vonn, estime que la police devrait reconsidérer ses tactiques antiterroristes. Presse Canadienne (Le Soleil, 16)

Syrian refugees
A letter to the editor states, "Kudos to Anthony Furey for questioning Canada's fast-tracking 30,000 Syrian refugees into Canada ("Life is anything but a cabaret," July 23). Of course, officials screen the adult refugees who pass, but it is their children who may grow up to be indoctrinated by radical Islam. After all, Jihadi John, who was killed last November by an American drone in Syria, was raised in Britain, and many of the Toronto 18 terrorists were born in Canada or immigrated here as children. Let us also not forget the hundreds of millions of dollars..." Toronto Sun, A19

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Major investigation into cocaine smuggling from Mexico to Canada brings arrests
Mounties say they have arrested people from Manitoba and Ontario after a two-year investigation into a criminal group moving large amounts of cocaine into Canada from Mexico. RCMP said during the course of their investigation, they seized more than two kilograms of cocaine. Times Colonist, A8

L'homme qui fuit
Marie-Hélène Girard croyait marier un juriste spécialisé en droit pénal international. C'était plutôt un homme en fuite, soupçonné d'avoir enlevé sa propre fille au Guatemala. Comment les autorités canadiennes ont-elles pu laisser filer Carlos Arnoldo Reyes Rivas aussi longtemps ? Marie-Hélène Girard avait des idéaux plein la tête. En ce mois de septembre 2009, elle rentrait d'un voyage au Guatemala et voulait s'impliquer pour ce pays d'Amérique latine. Alors, elle a cogné à la porte d'Amnistie internationale, à Montréal. C'est là qu'on lui a présenté Carlos Reyes, coordonnateur pour le Guatemala au sein de l'organisme de défense des droits de l'homme... Carlos Arnoldo Reyes Rivas était cultivé, séduisant et doté d'une intelligence exceptionnelle. Avocat spécialisé en droit pénal international, il était observateur de l'ONU au procès du criminel de guerre rwandais Désiré Munyaneza. Il côtoyait des professeurs de renom de l'UQAM, de McGill et de l'Université Laval. Il était le père dévoué d'une fille de 11 ans, Michelle. Pour couronner le tout, il était le richissime héritier d'oligarques guatémaltèques. Tout le monde y a cru. Les militants d'Amnistie, trop heureux de pouvoir compter sur le travail bénévole d'un tel cerveau. Les juristes québécois, impressionnés par la feuille de route de leur distingué confrère. Et Marie-Hélène Girard, bien sûr. Conquise par ce brillant humaniste, elle lui a passé la bague au doigt huit mois après l'avoir rencontré, le 8 mai 2010. Ce jour-là, elle ne se doutait pas que le piège tendu par Carlos venait de se refermer sur elle ; qu'en l'épousant, elle avait aidé un présumé criminel, recherché par la police guatémaltèque, à fuir la justice de son pays ; que l'Agence des services frontaliers du Canada (ASFC) était à ses trousses ; que la GRC faisait enquête pour enlèvement d'enfant ; que d'autres femmes étaient tombées dans ses filets. La Presse (Le Soleil, 18)

Attrape-moi si tu peux
Ciudad de Guatemala, Guatemala. Carlos Arnoldo Reyes Rivas est né le 11 décembre 1969, à Guatemala. Il a été élevé dans un quartier très modeste. Sa mère avait réussi à l'inscrire dans une école située dans un secteur plus riche de la capitale. Mais le jeune Carlos avait honte de ses origines et s'était inventé un personnage de riche héritier auprès de ses camarades, selon son ancienne femme, la Française Isabelle Auclair. Le couple a eu deux enfants au Guatemala : Michelle et Nicolas... Carlos Reyes a demandé le statut de réfugié lors de son arrivée au Canada, le 8 septembre 2002. Le processus s'est étiré pendant des années. Il avait épuisé tous ses recours lorsqu'il s'est marié, en 2010, avec Marie-Hélène Girard, qui a accepté de le parrainer. C'est ainsi que Carlos Reyes a obtenu sa résidence permanente en juin 2013_ tout en étant visé par un avis d'expulsion de l'Agence des services frontaliers du Canada (ASFC). La Presse, 2,3

Que font les autorités ?
Carlos Arnoldo Reyes Rivas a obtenu sa résidence permanente au Canada en juin 2013, alors même qu'il était visé par une mesure de renvoi dans son pays d'origine, le Guatemala. Comment expliquer cette incohérence ? « Le problème, c'est que personne ne se parle, dit Marie-Hélène Girard, qui a mené sa propre enquête sur son ex-mari. Un tas d'organismes publics ont des dossiers contre Carlos, mais ne se partagent pas l'information : l'Agence des services frontaliers du Canada, Citoyenneté et Immigration Canada, la GRC, le SPVM_ » Dans ce dossier, Marie-Hélène Girard a eu l'impression que les différents organismes « ne connaissaient pas toute l'histoire » au moment de rendre leurs décisions. Un travail en vase clos qui semble avoir joué en faveur de Carlos Reyes. Voici les principales étapes de son parcours au Canada. La Presse, 2, 5

Cross-border co-operation needed to halt march of opioid drugs
A letter to the editor states, "In 2011, there were six. Only five years later, and there are 274. That's the number of lives lost to the deadly drug fentanyl last year in Alberta. With an increase of nearly 46 times the amount of deaths, we are seeing a public health crisis impact every community in our province. Alberta is leading the nation in the fight against opioid drugs. The Progressive Conservatives were strong advocates for additional funding for the Alberta Law Enforcement Response Team (ALERT) that cracks down on illicit drugs flooding our communities. I also received unanimous support for Bill 205, the Pharmacy and Drug Amendment Act, 2016. This bill regulates the ownership of pill presses used to create fentanyl tablets..." Calgary Sun, A16

CYBER SECURITY / CYBERSÉCURITÉ

Cyberattaque contre des organismes publics
Les services russes de renseignement ont annoncé samedi avoir mis au jour une attaque informatique «planifiée» visant à espionner une vingtaine d'organisations, dont des agences publiques et industries militaires. Le FSB, l'héritier du KGB soviétique, explique avoir détecté des cas d'infection par un logiciel malveillant «destiné au cyberespionnage dans les réseaux informatiques d'environ 20 organisations sur le territoire de la Russie». Agence France-Presse (Journal de Montréal, Journal de Québec)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Mountie injured in traffic stop
A Mountie was sent to hospital with minor injuries and three police cruisers damaged when Blackfalds RCMP tried to stop a stolen pickup truck in the central Alberta town. RCMP received a tip from the public on Thursday afternoon that a black Dodge Ram previously reported stolen in Red Deer was parked in an alley behind a home in Blackfalds. Three RCMP cars attempted a traffic stop. Postmedia Network (Edmonton Sun, A6; Calgary Sun)

Les Hells Angels encore une fois à Saint-Gédéon
Lors du passage du Progrès-Dimanche en début d'avant-midi, un barrage policier était érigé comme l'an dernier près de l'établissement hôtelier, dans le rang des Îles. Plusieurs patrouilles de la MRC Lac-Saint-Jean Est de la police provinciale étaient sur place, avec des agents spécialisés pour les interventions liées au crime organisé. La Presse

Il venait de devenir un Hells
Le plus récent motard à être devenu membre en règle des hells angels est mort dans un accident spectaculaire survenu au nouveau- Brunswick. Kenny Bédard, 51 ans, est mort dans une collision impliquant neuf motos et un véhicule récréatif, dans le secteur de Saint-Basile, à Edmundston, dans le nord-ouest du Nouveau- Brunswick, vendredi soir. Selon les informations obtenues par TVA Nouvelles, Kenny Bédard était le tout dernier venu chez les Hells Angels. Agence QMI (Journal de Montréal, 3, Journal de Québec)

Quebec man dies in N.B. pileup involving members of biker groups
An employee at a New Brunswick campsite said the highway "looked like it had blown up" after a pileup involving nine motorcycles and an RV that left one man dead. Edmundston police said eight men and a woman, all of whom were travelling on motorcycles, also suffered injuries in the crash Friday night and are in hospital. Police said the male motorcyclists involved in the crash were members of various biker groups such as Hells Angels, Red Devils and Darksiders. Times Colonist, A7

Ruling to come Sept. 30 as Hells Angels cocaine conspiracy trial ends
The months-long cocaine conspiracy trial of two Kelowna Hells Angels and three of their associates wrapped up Wednesday in B.C. Supreme Court. Justice Carol Ross said she would hand down her ruling in the judge-only case Sept. 30. Hells Angels David Giles and Brian Oldham and associates James Howard, Michael Read and Shawn Womacks were charged with conspiracy to import cocaine following a 2012 reverse sting by Mounties posing as members of a South American drug cartel. Three other co-accused have already pleaded guilty in the case. The Province, A22

Crime Stoppers turns 40
"Michael Carmen never intended to become part of a legend. "Neither did Thomas Charles Boone nor Lawrence Edward Tate. "But they did on a July night in 1976 when evil brought them together." Postmedia Network (Toronto Sun, A22; Ottawa Sun)

Most wanted
NAME: CONOR D'MONTE. AGE: 38 DESCRIPTION: Black hair (if not shaved), brown eyes, 201 pounds, 6 feet 1, heavily tattooed, left-eye piercing. BACKGROUND: A member of Vancouver's United Nations gang, D'Monte is wanted for first-degree murder in the gangland execution of rival Kevin LeClair. He's also wanted for conspiracy to murder the notorious Bacon brothers. He's linked to a Mexico-based drug network and hasn't been seen in Vancouver since January 2011. POSSIBLE LOCATION: Mexico, Spain, Asia, Vancouver. Toronto Sun, A26

Ex-gang leader shot in fitness class
A self-described former gang leader who was trying to start his life over after being convicted in a drug-trafficking investigation in 2007, was shot and seriously wounded while teaching a fitness class in Christie Pits Park. Toronto Star, A2; Toronto Sun, A6

Time for cop cameras
An opinion piece states, “The public's confidence in the administration of justice has been shaken in the past week by two high-profile incidents. Both of the cases involved show the power and the importance of video in seeking truth and justice…” Postmedia Network (Ottawa Sun, A4; Toronto Sun)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Three most wanted
Police warn that all three subjects are considered violent. Kathryn Hill: 26, 5'8", 130 lbs., brown hair, brown eyes, wanted for Canada-wide parole violation. Michael Taypayosatum: 25, 5'2", 120 lbs., shaved hair, brown eyes, wanted for violating parole. Jonathan Michael Burgoyne: 36, 6'5", 230 lbs., black hair, brown eyes, wanted for violating parole. The Province, A23

The hunt for the Balaclava Rapist
The search for Larry Takahashi was a long one. Suspected of nearly a decade of sex-related offences in Edmonton, including the rape of more than 100 women in their homes, two fingerprints led to his arrest. Postmedia Network (Edmonton Sun, A16; Toronto Sun, Ottawa Sun, Winnipeg Sun, Calgary Sun)

Rapist denied parole
The man who brutally raped and nearly killed a young, pregnant woman in Banffmore than a decade ago will remain behind bars. Albert Muckle was declared a dangerous offender after being found guilty of sexual assault and attempted murder...Since being handed an indeterminate sentence with the

dangerous offender designation in 2006, Muckle has had his case reviewed by the Parole Board twice. Canadian Press (Calgary Sun, A6)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

High court judge denies bail to UN gangster charged with plotting to kill rivals
A B.C. Supreme Court judge has denied a bail application from a United Nations gangster charged with plotting to kill the Bacon brothers and their Red Scorpion associates. Troy Tran, 33, and his gang-mate Billy Ly, 32, were arrested in January following a lengthy investigation by law enforcement agencies in B.C. and Alberta. Postmedia Network (The Province, A23; Calgary Sun)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

Travel insurance tip
You've booked a trip from Canada to Istanbul but you're worried about political unrest or terrorism and want to cancel. You can always cancel a flight, of course, but you might have to pay a steep penalty and may not get any or very little of your money back. Experts say most travel insurance policies will cover you if you're heading out to a trouble spot where terrorism has just happened or is on high alert. But most policies won't cover you if your trip is months out or if you're flying to an area where you simply are afraid of problems. Toronto Sun, A59

INTERNATIONAL

Investigate Muslims
A letter to the editor states, "Germany is now paying the price for Chancellor Angela Merkel's foolish decision to allow its immigration system to go unchecked. The same is likely in store for Canada. The immigration system is wrought with ineptitude, incompetence and constantly under pressure from politicians demanding security checks to be lowered to the point where they are irrelevant. Tens of thousands of German women have been sexually assaulted by Syrian refugees and now the cancer of radical Islam is causing terror to run rampant..." Winnipeg Sun, A11

Skewed message on terror in Israel
A letter to the editor states, "From Israel: lessons on living with terror, Insight July 23. This article implies that Palestinians are a constant source of terrorism. Of course, some Palestinians have committed horrific

acts. But they did not terrorize thousands of Israelis to flee their homes in 1948 and 1967 and then obliterate their villages. Nor have they systematically bulldozed thousands of Israeli olive groves to clear the land for Palestinian settlements. They have not used Palestinian armed forces to assist in removing Israelis from their homes in East Jerusalem and Hebron so that they can be occupied by their own people. And they have not built a wall through Israeli villages and separated people from their families and fields..." Toronto Star, A10

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
August 16, 2016 / le 16 août 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Government to rebuild immigration detention facilities

Immigration holding facilities in Vancouver and Laval, Que., will be replaced as part of a $138-million overhaul intended to improve detention conditions for newcomers to Canada. The federal government will also move ahead with plans to ***expand the range of alternatives to locking up immigrants, with the aim of making detention a last resort***, said **Public Safety Minister Ralph Goodale**. In addition, a community supervision program will be developed for released detainees. **Goodale** announced the details Monday during a visit to the aging Laval facility. The Canada Border Services Agency holds people who are considered a flight risk or a danger to the public and those whose identities cannot be confirmed. The Canadian Red Cross Society has found numerous shortcomings at facilities for immigrant detainees, including overcrowding and lack of mental health care. Newcomers are often held in provincial jails or police facilities alongside suspected gang members and violent offenders. There are three federal immigration holding centres and the government has flagged the Vancouver and Laval facilities as most in need of attention. One in Toronto is considered to be in better shape. The planned improvements are designed to reduce reliance on provincial facilities. Some of the new money will go to mental health and

medical services for detainees in federal holding centres. Canadian Press (Guardian, A5, Red Deer Advocate, Cape Breton Post, Chronicle Herald, Telegram); * Postmedia News (London Free Press, N4)

La détention des immigrants remise en question
L'annonce de la réfection des centres de détention canadiens doit relancer la réflexion, jugent des groupes. Le **ministre de la Sécurité publique, Ralph Goodale**, a annoncé lundi des investissements de 138 millions de dollars, principalement pour moderniser les centres de détention d'immigrants à Laval et en banlieue de Vancouver. Des voix s'élèvent pour réclamer la fin de cette pratique, digne d'un traitement réservé aux criminels dans certains cas. En mai dernier, Carmelo Monge s'est présenté aux bureaux de Citoyenneté et immigration Canada 1010 à Montréal, croyant qu'il repartirait avec un permis de travail renouvelé. Il a plutôt été arrêté. " Ils m'ont mis les menottes et alors je me suis senti comme si j'avais fait quelque chose de très grave ", relate-t-il, encore sous le choc. " Je ne suis pas un criminel, je suis ici pour travailler, pour aider ma famille restée au Mexique ", dit l'homme de 45 ans. Il est au Canada depuis huit ans, en attente d'une demande de résidence permanente fondée sur des considérations humanitaires, après avoir vu sa demande d'asile déboutée. A son arrivée au centre de détention de Laval, des bâtiments entourés de barbelés, c'est la surveillance constante qui l'a marqué. " J'ai vu une femme du Pakistan avec son enfant à l'entrée, avec des gardes autour d'eux ", rapporte M. Monge. Circonstances : En 2014-2015, l'Agence des services frontaliers du Canada (ASFC) a détenu 6800 personnes. Si un agent de l'ASFC doute de l'identité d'un ressortissant étranger, s'il croit que celui-ci se soustraira aux procédures d'immigration ou encore s'il considère que sa demande est inadmissible, il a le pouvoir de le détenir. Le Devoir, A1, A8; Presse Canadienne (Acadie Nouvelle, 14, Quotidien, Voix de l'Est, Tribune, Soleil)

* **Critics slam oversight on immigration detention reforms**
Migrants advocates welcome Ottawa's reforms of the immigration detention system, but say the government is falling short on creating proper oversight of the agency responsible for the enforcement operations. "It is encouraging the federal government is promising actions and reforms to the immigration detention system. Detention of immigrants needs to be absolutely the last resort and the government recognizes that," said Josh Paterson of the British Colombia Civil Liberties Association. "The thing is, we need to put an end to housing migrants in criminal population. The money dedicated to the immigration infrastructure must not become the reason to detain more migrants and for longer period of time." **Public Safety Minister Ralph Goodale** announced on Monday that $138 million would be invested to ***"enhance alternatives to detention"*** and invest in rebuilding immigration holding facilities. He also plans a series of community consultations. **Goodale** has been under fire after a series of deaths of detainees held in immigration custody this year. A United Nations human rights report last year also raised alarm over Canada's lengthy immigration detention and lack of medical support for inmates. Anthony Navaneelan of the Canadian Association for Refugee Lawyers said what was missing in **Goodale**'s announcement was creating an independent oversight of the Canada Border Services Agency, which is responsible for enforcement of immigration laws including immigration detention. Toronto Star, A7

* **Feds move to reassure Canadians on terrorism**
The governing Liberals are moving further to reassure Canadians that they have a grip on combating the threat of terrorism in the wake of last week's death of a man suspected of plotting an attack. **Public Safety Minister Ralph Goodale** was in Montreal Monday where he was expected to give a talk about how the government is moving ahead with a program designed to reach out to those who are vulnerable to radicalization in order to nip in the bud suspected terrorist plots like the one in southern Ontario last week. **Goodale** was expected to visit a Montreal centre devoted to preventing radicalization that leads to violence. Details about the program aren't expected until a later date. Last week, he stressed the importance of identifying those who are open to radicalization and finding the right way to prevent situations such as the death of a man in Strathroy, Ont., who was suspected of planning a terrorist attack. **Goodale** will announce the government will replace immigration detention facilities in Laval, Que., and Vancouver. (...) In his statement, **Goodale** suggested that a free flow of information between Canadian and U.S. intelligence and law enforcement agencies is the norm***. "Consistent with the robust security alliance that we have with the U.S., the Americans passed that material to the RCMP,"*** said **Goodale**'s statement, which prominently mentioned the context of the FBI contribution. ***"It's important for Canadians to know that our agencies and their global partners are monitoring potential risks***

and threats all the time - 24-7, 365 days a year." Last week's incident, as well as the attack on Parliament Hill in 2014, have led to an appetite among Canadians to examine current national security measures and look at how they can be improved to better protect Canadians while safeguarding civil liberties, **Goodale** said. Canadian Press (Waterloo Region Record, A8, Times Colonist, Hamilton Spectator, Red Deer Advocate)

*** Canada to launch counter-radicalisation office**

The Canadian government announced plans for a specialised centre to fight radicalisation of its citizens following a police shooting death of a suspected jihadist last week and lone-wolf attacks. **Public Safety Minister Ralph Goodale** said Ottawa would combine a patchwork of counter-radicalisation efforts launched by cities and universities under a new federal office. ***"We pride ourselves on being a generous and diverse society," Goodale*** said. ***"If we want to keep it that way, we have to be among the best in the world in dealing with radicalisation and trying to head off these tragedies before they happen."*** Last week's foiled terror plot, and two separate lone-wolf attacks in October 2014 that resulted in the deaths of two Canadian soldiers have led to demands for a review of Canada's national security framework. ***"The largest concern," Goodale*** said in a statement, ***"is about lone wolves who get sucked into perverse and extreme ideologies that promote violence."*** A new national centre for 'community outreach and counter-radicalisation' will be modelled on existing centres in Montreal and Calgary. Pakistan Today

The RCMP needs to arrest terrorists

Public safety minister Ralph Goodale is either pulling our leg or we've got a very serious problem in the upper ranks of Canada's policing and intelligence services. For the past couple of days, **Goodale's** been highlighting the need for counterradicalization. But somehow he missed the glaringly obvious anti-terror measure that's already at our disposal: That the RCMP need to do their job and arrest terrorists. In March, RCMP commissioner Bob Paulson told a Senate committee that for some of the Canadians who've gone abroad to participate in terror-related activities "we've assessed that they're back, they're sorry, they're working to try to get their heads straight and we're relying on family members or other professionals." Yup. That's right. If terrorists say they're sorry the RCMP doesn't charge them. What the heck kind of policing is this? It's already illegal, according to the Criminal Code, to leave the country or attempt to leave to participate in terror. Yet there are dozens of jihadists returned from abroad the RCMP knows about who haven't been charged. (…) If the Liberals want to spend a few dollars on community outreach, go ahead. But police aren't social workers. And **Goodale** isn't running a daycare. The cops need to enforce the law. It must be their top priority. ***"We need to know how to intervene with the right tools at the right time in the right way -all to head-offtragedies before they happen, as much as humanly possible," Goodale*** wrote in a statement released on Sunday. We already have the right tool though. It's the law. And we're opting not to use it. Prime Minister Justin Trudeau and **Goodale** either aren't aware of this or they're choosing to ignore it. Either way, it's a big problem. Postmedia Network (Winnipeg Sun, A10, Edmonton Sun, Calgary Sun)

*** Trudeau, Trump go opposite ways on homegrown terror**

Compare and contrast. ***"Canada is an open, pluralistic democratic society and if we want to maintain those qualities and values then we have to become among the best in the world at dealing with radicalization to violence."*** That was Canada's **Public Safety Minister Ralph Goodale** speaking Monday morning about some new approaches his government will take in the coming months to combat domestic terrorism. Now contrast. "Our country has enough problems. We don't need more." That's Donald Trump, the Republican nominee for president, a few hours after **Goodale**, talking about how new barriers to immigration will protect America from terrorism. "I call it extreme vetting," he said. Trump wants new barriers and actual real walls put up in the belief that it's bad guys from somewhere else who are threatening American security. He said he'll set up a screening system for immigrants which will detect danger to America from any children those immigrants might one day have. Canada, by contrast, will continue to accept thousands of Syrian refugees in addition to broadening the kinds and types of immigrants the country will accept. That's because the Trudeau government believes fighting terrorism is not done by shutting borders. Trump believes the opposite. And yet, immigration could cut to zero tomorrow and there would still be young, disaffected Canadians and Americans watching ISIS propaganda online and signing up to do harm. Calgary Sun, A18

*** Mosque lauds feds' radicalization fight**

The London Muslim Mosque welcomed news from Ottawa that the government is moving ahead with a nationwide program to combat radicalization. "This is in line with what we've been talking about," mosque spokesperson Nawaz Tahir said Monday. "We'd be happy to lend any support we can. This is a multi-disciplinary issue. It's not a London issue, it's a macro issue and it requires a national response." His comments came after **Public Security Minister Ralph Goodale** spoke about plans for Ottawa to spend $35 million during five years to fund programs that reach out to vulnerable people open to radicalization in a bid to prevent terror attacks in Canada. ***The federal government will establish a national centre for deradicalization that will co-ordinate efforts across Canada to fight extremism***, **Goodale** said. ***"The events of the last week or so have demonstrated in Canada that we need to get better and better at understanding and dealing with the serious issue of radicalization."*** **Goodale** was referring to a situation that unfolded in the London region last Wednesday, after the FBI tipped off the by Strathroy resident Aaron Driver. Police tracked down Driver, who was killed after getting into a Strathroy taxi believed to be headed for London. **Goodale** said most of the money will go to groups and organizations at the community level that are best equipped ***"to intervene in the right way, with the right tools and at the right time."*** Postmedia News (National Post, A1, London Free Press)

Single bullet killed terror suspect, dad says

Father says son's death was 'gut-wrenching,' but doesn't blame police for lethal takedown. The suspected terrorist who allegedly planned an attack on a major Canadian urban centre last week was killed by a bullet as Mounties descended upon him outside his sister's home, according to his family. Wayne Driver, a retired military officer whose youngest son Aaron Driver died after detonating an explosive device inside a taxi during the confrontation with police in Strathroy, Ont., told the Star that the family also plans to give him an Islamic funeral Thursday - on what would have been his 25th birthday. "We're going to respect his beliefs," Wayne Driver said, shortly after arriving in London, Ont., Monday to plan his son's burial. Both Driver and Aaron's older brother, Rob, say they were told by the RCMP that an autopsy concluded the 24-year-old died from one of two gunshots wounds. Driver said he was told that one bullet pierced his son's spleen, and another went through his heart and liver. (…) **Public Safety Minister Ralph Goodale** was in Montreal Monday, where he was expected to talk about how the Liberal government in Ottawa is preparing a program designed to reach out to people who are vulnerable to radicalization, The Canadian Press reported. Details aren't expected until a later date. In a statement Sunday, **Goodale** said ***co-operation between agencies like the FBI and the RCMP are "consistent with the robust security alliance" between Canada and the U.S. "It's important for Canadians to know that our agencies and their global partners are monitoring potential risks and threats all the time - 24/7, 365 days a year,"*** he said. Canadian Press (Toronto Star, A1)

La mère d'un djihadiste dénonce le gouvernement

Une mère de famille de Calgary dont le fils djihadiste de 22 ans a été tué en Syrie il y a deux ans croit que le gouvernement a laissé tomber Aaron Driver et sa famille. Aaron Driver, 24 ans, est mort la semaine dernière lors d'un affrontement avec la police à Strathroy, en Ontario, après avoir apparemment réalisé une vidéo suggérant qu'il allait commettre un attentat-suicide dans un centre urbain du pays. La mère du jeune radicalisé Damian Clairmont, Christianne Boudreau, dit avoir pleuré lorsqu'elle a appris la nouvelle. Mme Boudreau, qui vit maintenant à Eymet, en France, a ajouté qu'elle avait le coeur brisé de constater que tant d'agences et d'organisations n'avaient pas pu aider sa famille. (…) «Il aurait dû fournir un suivi psychologique pour lui et sa famille afin de s'assurer qu'ils s'occupent de ce qui le troublait, ce qui le dérangeait; de prendre toute cette motivation émotionnelle et ces croyances qui le poussaient dans cette direction et d'utiliser cette énergie pour quelque chose de positif», a-t-elle ajouté. **Le ministre de la Sécurité publique Ralph Goodale** a dit jeudi que son gouvernement avait consacré 500 millions $ pour assurer la sécurité au pays et pour contrer la radicalisation. Presse Canadienne (Acadie Nouvelle, 12)

Canada approves transfer of Florida lifer but state mum on approval

The federal government has approved the transfer of a Canadian jailed for 30 years in Florida prisons for a murder committed when he was 18 years old. However, there was no immediate word whether the state, which has previously blocked William (Russell) Davies from serving out his life sentence in Canada, will let him go. "Canada will bring Russell back but we have to go through the States yet," Davies's

mother, Carol Davies, said. **Public Safety Minister Ralph Goodale** had no immediate comment while a spokeswoman for Florida Gov. Rick Scott said she was looking for information on the case. In an investigative series in June, The Canadian Press chronicled the events leading to Davies's conviction for first-degree murder following a trial in Daytona Beach that essentially lasted only seven hours and which some legal experts have denounced as a sham. Now 48, Davies was then an 18-year-old runaway misfit from Richmond Hill, Ont., when he and five others were charged with gunning down a seventh member of their group in June 1986. His co-accused - initially represented by the same lawyer - quickly pleaded out in return for testifying against him, and were given probation or short sentences. Red Deer Advocate, A7

*** I'm very glad the Mounties got their man**

An opinion piece states, "The biggest story in Canada this weekend was the triumph of Penny Oleksiak, the dazzling young Canadian who took the swimming world by storm. Lucky us. The biggest story could have been the triumph of Aaron Driver, the Islamist-inspired jihadi warrior, if he had blown himself up at a train station in Southern Ontario and taken a dozen innocent people with him. We'll never know, of course. Just as Mr. Driver stepped into a taxi, police opened fire and he detonated a bomb. Officially, we don't know what killed him, but either way, the Mounties got their man. I'm sorry they had to do it, but I don't have a shred of sympathy for him - only for his family, who saw him going to the dark side and were helpless to prevent it. Mr. Driver had rejected help. He sought out martyrdom. All the evidence indicates that he was a traitor to his country. The RCMP don't get much good press these days. They're usually portrayed as the gang that can't shoot straight. Most stories about the Mounties are meant to tell us how sexist, racist and incompetent they are. They deserve a lot of credit for getting this one right. Around 8:30 a.m. last Wednesday, the FBI sent them a screen shot of a man with his face masked, taken from a homemade "martyrdom" video. By 11 a.m., Canadian authorities had identified the suspect. At 4:30 p.m., when the man got into a taxi outside his house in Strathroy, Ont., police were waiting for him. (…) **Ralph Goodale**, the minister of public safety, says Canada needs to step up its counter-radicalization efforts. I'm all for that. The trouble is, nobody knows what works. And nobody will ever devise the perfect combination of police powers and social intervention that will keep us completely safe. Like it or not, sometimes the only solution is the violent one." Globe and Mail, A11

*** Canada, it's time we discussed the Islamic reformation**

An opinion piece states, "We need to get really good at counter-radicalization, **Public Safety Minister Ralph Goodale** recently argued. And he's right. But we won't succeed at that until we add talk about the Islamic reformation into the mix. Yet media and politicians here never even reference the phrase. And what is it? It's the idea that Islam needs to "jump from totalitarian fundamentalism to enlightened, liberal religion," as Foreign Policy magazine describes it. Sort of like the 16th century Christian reformation. We need to talk about it in the wake of Aaron Driver. We need to talk about it because almost 200 Canadians are now abroad training or fighting armed jihad. Dozens more have already returned. And we need to talk about it because Muslims in Canada, according to a recent Environics Institute report, are becoming more observant. The 18-34-year-olds are the most observant and "they identify primarily as Muslim rather than as Canadian," the report notes. Now, you can bet the politically correct will be resistant. They'll plug their ears. They'll look the other way. Or, worse, they'll call anyone who brings it up "Islamophobic." But they'll be speaking out of ignorance. Because the conversation's already happening. In journals, at think-tanks and during conferences. It just hasn't made its way into daily conversation yet. It will soon. Even the leader of the free world talks about it." Toronto Sun, A15

TOP STORIES / MANCHETTES

*** Feds want RCMP to look into Canadian firm's armoured car shipments to war-torn Libya**

The Liberal government has asked the Mounties to look into a UN report that found a Canadian-owned company shipped dozens of armoured personnel carriers into the chaos of Libya, possibly in violation of an arms embargo. In a statement released late Monday, the Global Affairs Department said a copy of the UN panel's findings about the Streit Group has been handed to the Mounties. There's no indication at the moment whether the RCMP intends to launch a full-blown investigation. The Liberal government says it will leave the matter up to law enforcement. "It is the role of the RCMP to investigate potential offences under Canadian law, while the prosecution of offences under federal jurisdiction is the responsibility of the

Public Prosecution Service of Canada who will determine if Canada has jurisdiction to prosecute based on the facts of the case," spokesman Francois Lasalle said in a statement. The department didn't say when the UN report, which was released in March, was shared with the Mounties. But the handover of the file to the RCMP comes less than a week after CBC News published a series of stories about the activities of Streit in both Libya and South Sudan. CBC News (2016-08-15)

*** Prisoner on the lam was deemed a low risk to the public**
A man deemed a dangerous offender by the provincial justice system was determined to be a low risk to public safety prior to his escape from the Pe Sakastew federal prison in Maskwacis over the weekend. Darell Moosomin, 54, was on an escorted temporary absence from Pe Sakastew on Sunday, where he was serving an indeterminate sentence, when he escaped. He was on a leave to attend the Samson Powwow when the elder who was supposed to be with him lost sight of him. A Canada-wide warrant was issued for his arrest, but Moosomin remained at large Monday. (…) Correctional Service Canada spokesman Jeff Campbell said inmates are evaluated before being granted permission to go on these types of outings, which can include excursions to complete community service, attend family functions or to access resources such as a doctor or a hospital. Campbell said there are also conditions that must be followed when the leave is granted. Edmonton Sun, A4 (Edmonton Journal, Calgary Sun); Red Deer Advocate

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Wildfires torch province's firefighting budget**
Nova Scotia's firefighting budget is up in smoke, thanks to the worst wildfires in years. Spending is already three times the 2016 provincial firefighting allocation of $686,000 battling 10 wildfires across Nova Scotia, according to estimates from the Natural Resources Department. Spokesman Andrew Preeper said this year's provincial firefighting budget is $686,000 and actual expenditures as of Aug. 8 were $520,000. Chronicle-Herald, A1

*** Officials worry about fracking risks**
BC Hydro officials have worried that earthquakes triggered by fracking could damage or destroy some of the utility's dams in the province's north, an issue that has been a point of discussion among staff over recent years, documents show. Globe and Mail, S1

*** Sweet ending in the search for missing three-year-old boy**
Rescuers say a three-year-old boy who wandered away from his Vancouver Island home Sunday evening has been found safe - and covered in berry juice. Constable Rob Gardner with the Comox Valley RCMP said Lochlan McKenzie was playing in the yard of his home near Union Bay, south of Courtenay on Sunday evening, when he went missing. It appears as though the little boy simply decided to ride his scooter bike further than he was supposed to, Constable Gardner said. A significant effort was mounted to find the boy, including eight search-and-rescue teams from across Vancouver Island, said Paul Berry, commander of the Comox Valley Ground Search and Rescue. A large contingent of RCMP officers also assisted in the search, along with the Mounties' air and marine services, a drone, dog teams and crews on horseback. Globe and Mail, S2; Canadian Press (Toronto Sun, Ottawa Sun, The Telegram, Cape Breton Post, The Guardian)

*** 'It was a win, win'**
Cape Breton Regional Police North Division will move into its new headquarters in the historic former town hall in Sydney Mines next week. During a tour of the new station Monday morning, Chief Peter McIsaac admitted initially he was a little reluctant to consider moving into another old building. Mayor Cecil Clarke said with Central Division being upgraded this year, by 2017 the budget process will include a new police station for East Division and within two years all of the police facilities across the regional municipality will be upgraded. "This will allow us to focus on the fire and emergency service review long term, along with ground search and rescue." Cape Breton Post, A6

*** Les juges comprennent-ils le terrorisme ?**
C'est la vigilance du FBI qui a permis à la GRC d'intercepter Aaron Driver, le plus récent djihadiste «made in Canada» avant qu'il ne commette un attentat-suicide. Bravo et merci! Mais que faisait ce jeune homme, connu des autorités pour ses positions pro-État islamique, en liberté à peine surveillée? L'étude du dossier d'Aaron Driver révèle que l'homme de 24 ans a passé une bonne par-tie de 2015 entre la prison et les salles d'audience du palais de justice de Winnipeg. On lui reprochait, outre sa proximité intellectuelle avec le groupe État islamique, d'avoir exprimé son admiration pour le salaud qui a tué le caporal Nathan Cirillo sur la colline du Parlement en octobre 2014. Mais, aux yeux de la justice, il n'avait commis aucun crime. De plus, son casier judiciaire était vierge. Impossible donc de le garder en prison, mais les avocats du jeune homme et la Couronne s'étaient entendus sur l'imposition d'engagements à ne pas troubler l'ordre public parce qu'il existait «des raisons de croire qu'il pourrait participer ou contribuer directement ou indirectement aux activités d'un groupe terroriste». Parmi les conditions qui ont rendu possible sa libération, Aaron Driver devait porter un bracelet électronique avec GPS à la cheville. La Commission des droits de la personne du Manitoba a poussé les hauts cris, repris en choeur par tout ce que le Canada anglais peut contenir de bonnes âmes opposées à tout raffermissement des lois antiterrorisme: «On ne peut soumettre une personne qui n'a commis aucun crime à une surveillance 24 jours par jour.» Journal de Montréal, 8 (Journal de Québec)

*** ISIL happy to get know-nothing new recruits**
An analysis of thousands of leaked Islamic State documents reveals most of its recruits from its earliest days came with only the most basic knowledge of Islam. A little more than 3,000 of these documents included the recruit's knowledge of Shariah, the system that interprets into law verses from the Qur'an and "hadith" - the sayings and actions of the Prophet Muhammad. LITTLE OR NO KNOWLEDGE According to the documents, 70 per cent of recruits were listed as having just "basic" knowledge of Shariah - the lowest possible choice. Around 24 per cent were categorized as having an "intermediate" knowledge, with just five per cent considered advanced students of Islam. IGNORANCE PREFERRED Are disaffected people who understand Shariah more prone to radicalization? Or are those with little knowledge of Islam more susceptible to the group's radical ideas that promote violence? The documents suggest the latter. The group preys on this religious ignorance, allowing extremists to impose a brand of Islam constructed to suit its goal of maximum territorial expansion and carnage as soon as recruits come under its sway. Those who've claimed advanced knowledge in Shariah on the ISIL entry documents were less likely to want to become suicide bombers, according to a study by the U.S. military's Combating Terrorism Center, an academic institution at the United States Military Academy. "If martyrdom is seen as the highest religious calling, then a reasonable expectation would be that the people with the most knowledge about Islamic law (Shariah) would desire to carry out these operations with greater frequency," said the report. However, despite the religious justification that ISIL uses for suicide missions, "those with the most religious knowledge within the organization itself are the least likely to volunteer to be suicide bombers," the study found. Associated Press (StarPhoenix, N2, London Free Press, Edmonton Journal, Windsor Star, Montreal Gazette, National Post, Ottawa Citizen, Vancouver Sun, Calgary Herald)

*** Timely police work**
An opinion piece states, “Canada came close to suffering a terrorist attack last week, but countless lives were saved when police disrupted the plan. The would-be terrorist, Aaron Driver, who was living in Strathroy, Ont., under what's basically a restraining order, was killed. How he died isn't yet clear. The Ontario Provincial Police are investigating whether he died by police gunfire or from a bomb that went off in the back of a taxi, injuring the cabbie who had picked up Driver at the house where he lived. The RCMP acknowledged the tragic outcome, but noted correctly that, had Driver not been stopped, the carnage would have been far, far worse. So let's take a moment to give our police and security authorities - whose actions are often challenged - full credit. In a fine example of cross-border co-operation, the operation began with a tip from the FBI, which had come across a martyrdom video Wednesday. By afternoon, Canadian police had identified and were swooping in on Driver. It's something of a miracle they were able to figure out so quickly who the ISIL video star was. Self-radicalized, homegrown terrorists are elusive. It appears officials at a local mosque had been attempting to break through to Driver; the Muslim community is an important ally in the fight against terror, and this event shows the difficulty in actually

talking sense into radicalized people. The Liberals remain committed to reforming the Tories' anti-terrorism bill, C-51 - rightly, in our view - but this incident adds complications. And the task has barely begun, although a bill to create a new national security oversight committee has been tabled." Times Colonist, A8

*** Co-operation, outreach best terrorism defence**
An opinion piece states, "By its nature, terrorism targets innocent people and seeks to create distrust among citizens through shock, panic and fear. This is what makes it the weapon of the ignorant and of the cowardly. And last week, our region and city felt its impact. What is the way forward and how should we respond? By keeping in mind a few important truths about what keeps societies secure. The first of these is the need to remain vigilant, yet reasonable. Questions will be asked about whether more could have been done to keep us safe from the likes of Aaron Driver. This is appropriate, but unless the conversation is measured, we might end up trying to fix what is not broken. The result will be that important resources needed to maintain public safety - time, energy and money - could be used ineffectively. Avoiding this problem requires us to search first for lessons, not in what went wrong, but in what went right. Last Wednesday, various agencies - the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, the London Police Service, Strathroy-Caradoc and the Ontario Provincial Police - worked together to thwart an act of terrorism. The importance of this cannot be overstated. When the RCMP was informed about an imminent attack, they acted swiftly and were successful. Local forces were involved and engaged. Partnership, rather than rivalry, is what defined this effort and we are all safer because of it. This example, in fact, provides a model as we move forward. Some may ask why the U.S. Federal Bureau of Investigation identified the threat instead of the RCMP. This is beside the point. What matters much more is that the information was discovered and shared. This happens between the FBI and the RCMP on a regular basis and last week provided another example of the importance of co-operation. The second need is to pursue proactive policies that offer reassurance in the face of unpredictability. This is why a counter-radicalization policy is important and why the federal government is right to direct funding - $35 million during the next five years - to the office of a new Community Outreach and Counterradicalization Co-ordinator." London Free Press, A5

*** Former Islamist discusses how to end spread of terrorist ideology**
An opinion piece states, "Canada needs to revamp its approach to Islamic extremism if it hopes to prevent another homegrown radical from setting off a bomb, says the founder of an international anti-radicalization think tank. In an exclusive interview with Postmedia, Maajid Nawaz - a former Islamist radical and founder of the U.K.-based Quilliam Foundation - called for a societywide effort to undercut the intellectual and theological planks of Islamist and jihadist ideology. "There certainly needs to be training. Counter-radicalization training involves de-radicalization training on how to disengage somebody from the theory of violence, and it involves taking them beyond that actually and discrediting the theory of Islamism in their minds," said Nawaz. "A lot of this, Muslims simply don't know." Nawaz was in Niagara Falls Saturday to address the third annual Non-Conference at the Americana hotel as the keynote speaker. Although the event was billed as a conference for non-believers, Nawaz, a Muslim seeking to reform the faith, told his audience he looked upon them as allies in combating radicalization. "You are more my brothers and sisters than anyone who ever joined ISIS," Nawaz said. "Islam needs to reform. And Islamism needs to be intellectually terminated," Nawaz's address comes only days after headlines were dominated by a jihadist incident in Strathroy. On Wednesday, RCMP counterterrorism officers shot and killed Aaron Driver, a declared ISIS supporter. According to news reports, Driver regularly attended a London-area mosque. The mosque's leaders were aware of Driver's radical views and believed if they kept him as a member they might be able to pull him away from Islamist ideology. Nawaz said most mosques are ill-equipped to counter radical ideology." Postmedia Network (Toronto Sun, A9, Ottawa Sun, Edmonton Sun, Kingston Whig-Standard, Calgary Sun)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Plea ends potential test of privacy rights
A Quebec man arrested last year at the Halifax airport for refusing to provide border officers with the password for his cellphone pleaded guilty Monday and was ordered to pay a $500 fine. Alain Philippon's

plea on the eve of a scheduled trial brought an abrupt end to a case that was being watched closely as a test of the line between privacy rights and the state's power to control its borders. Robert Currie, director of Dalhousie University's Law and Technology Institute, said the plea deal represents a "missed opportunity" to explore an emerging legal question. "We've got case law around the Customs Act, going back in time, which says essentially that you have next to no privacy at the border," Currie said in an interview. "On the other hand, we've got very recent case law from the Supreme Court of Canada, starting in about 2010, that says you've got an intense amount of privacy in your electronic devices. "What we have not seen to date is a case where a court has really wrestled with all of this and tried to put it all together." Philippon, 39, was returning to Canada from the Dominican Republic in March 2015 when he was pulled aside by the Canada Border Services Agency and as part of a search asked to provide access to his BlackBerry. He refused to give the password and was charged under the federal Customs Act with hindering or preventing an officer from doing his job. Postmedia Network (Ottawa Citizen, N1, Edmonton Journal, London Free Press, Starphoenix, Windsor Star, Leader-Post, Montreal Gazette, National Post, Vancouver Sun, Calgary Herald); * Radio-Canada (2016-08-15)

Un véritable arsenal confisqué
Un couteau format carte de crédit, des arbalètes miniatures, des poings américains, des pistolets paralyseurs et des vaporisateurs de gaz irritants ne sont là que quelques exemples d'armes prohibées saisies par les agents des services frontaliers du Canada à trois points d'entrée de la région d'Ottawa au cours des 18 derniers mois. Une liste des armes illégales interceptées par les douaniers canadiens à Prescott, à Cornwall et à l'aéroport international Macdonald-Cartier d'Ottawa en 2015 et jusqu'à présent en 2016 fait état d'une variété d'articles saisis. C'est le cas à Prescott, un petit poste douanier situé à une soixantaine de minutes de voiture au sud d'Ottawa. (…) Les douaniers de Prescott ont aussi mis la main depuis janvier 2015 sur deux arbalètes miniatures, deux pistolets paralyseurs, quatre vaporisateurs de gaz poivré, deux pistolets à impulsion électrique (Taser), deux nunchakus, huit armes de poing et trois couteaux à ouverture automatique. Une interception menée le 16 juin 2015 a d'ailleurs permis aux douaniers de mettre la main sur 33 armes prohibées, dont des poings américains et des poings américains munis d'un canif. Du côté de Cornwall, les agents de l'Agence des services frontaliers du Canada (ASFC) ont saisi une dague à pousser (poignard), huit couteaux à ouverture automatique, une arme de poing, une sarbacane avec des fléchettes, un Taser, deux vaporisateurs de gaz poivré, une réplique d'une arme à poing et une matraque rigide à ressort. A l'aéroport international Macdonald-Cartier, seul un vaporisateur de poivre a été intercepté par les douaniers depuis le début de 2015, selon les données fournies par l'ASFC. Le Droit, 2

* **Passenger denied boarding over travelling with only a Nexus card**
A Washington state man was recently denied boarding for a flight from Newark to Toronto after only presenting his Nexus card, thinking it was the only documentation he needed. Justin Thompson is a U.S. citizen and was travelling on Porter Airlines from Newark Airport to Billy Bishop Airport in Toronto in July. Thompson was travelling with his Nexus card and did not have his passport. When he tried to board the flight, the Porter Airlines gate agent refused to allow him on. (…)There are eight designated Canadian cities with Nexus kiosks. While Billy Bishop Airport isn't on the list, CBSA's website says there is a "trusted traveller kiosk" for Nexus members at that airport for incoming flights. In a statement to CTV News, Canada Border Services Agency (CBSA) said that a Nexus card can be used in lieu of a passport for "Canadian and American citizens who are Nexus members entering Canada from the U.S." (…) Porter Airlines told CTV News that it's in the "best interest of all international travellers to carry a valid passport" and "the language on our website and flight reminder is explicit noting the requirement for a passport, which is supported by CBSA indicating that an airline may do so." CBSA's website also states that a passport may be required by an airline or alternative transportation authority. CTV News (2016-08-15)

Deportation overturned
Media attention, including a recent Vancouver Sun column, has helped a man thrown out of Canada because of a wrongful sexual assault conviction obtain a permit to return and seek redress. Vancouver lawyer Jason Gratl said his client, Gurdev Dhillon, was ecstatic after the immigration department did an about-face late Friday afternoon and said the subsistence farmer in Punjab could come back. He was wrongly convicted in October 2005 of participating in a July 2004 Surrey gang rape at his apartment and

served four years in prison before deportation. The convictions were set aside in December, 2014. Postmedia Network (Vancouver Sun, A6) * Voice Online (2016-08-15)

Cimenterie
La Caisse de dépôt et placement du Québec (CDPQ) ne croit pas que la nouvelle ronde de financement réalisée pour compléter le projet de cimenterie de Port-Daniel ravivera les menaces de barrières tarifaires aux États-Unis. Son président et chef de la direction, Michael Sabia, a voulu se montrer clair vendredi, en marge de la mise à jour semestrielle, en affirmant qu'il ne s'agissait pas de fonds publics. Le projet de cimenterie, dont le principal marché d'exportation sera les États-Unis, a fait l'objet de critiques au sud de la frontière, où des membres de l'industrie et certains élus crient à la concurrence déloyale. Questionné à ce sujet, M. Sabia a affirmé que la CDPQ était un investisseur privé qui a pris une décision d'affaires afin de générer du «rendement pour ses clients». Il n'a pas semblé craindre que le dossier puisse prendre une ampleur similaire à celui du bois d'oeuvre canadien, qui a fait l'objet de barrières tarifaires à la frontière étant donné que les Américains estimaient que l'industrie était subventionnée. Selon M. Sabia, il n'y a «pas un soupçon» de subvention dans le financement de 250 millions $ auquel contribue la CDPQ dans une proportion de 125 millions $. Le dossier de la cimenterie, qui fait face à des dépassements de coûts de l'ordre de 450 millions $. La Presse Canadienne (Le Soleil, 37, La Tribune, La Voix de L'est)

Halifax port boom tops all across North America
Container traffic at the Port of Halifax is spiking this year as it grabs a growing share of the market due to its newfound ability to receive bigger cargo ships coming through the new Suez and Panama Canals. (…) And while there has been growth at some ports, like Miami which saw an increase of 5.5 per cent, the biggest percentage jump so far this year has been in Halifax. Industry insiders are chalking it up to three things: a low Canadian dollar; fast and efficient turnaround of container cargo in Halifax; and the port being ready to handle the new, big ships coming from Asia through the newly-widened and lengthened Suez and Panama canals. (…) When the Canadian Border Services Agency needs to inspect a container, that extra space makes things easier for the Port of Halifax where these inspections are done more quickly than in Vancouver, said Snowden. The executive director of the national freight forwarders thinks the time lost at the Port of Vancouver, compared with Halifax, may be encouraging companies to use the Atlantic seaport. Chronicle Herald, B1

*** Masse politicizes Ambassador Bridge debate**
An opinion piece by Doug Sartori states, "I find it neither "troubling" or "alarming" that Dwight Duncan is diligently pursuing all options with respect to the current and future crossing. Government ownership of the Ambassador Bridge would address many issues faced by residents of Windsor West, particularly the residents of Sandwich Town who have been caught in the crossfire between the City of Windsor and the Ambassador Bridge Company. It's absurd to suggest that it is not in the best interests of our community to explore this option. I find it troubling that the Windsor West Member of Parliament has chosen a needlessly aggressive approach in requesting answers from the government. Surely, if Mr. Masse was sincere about his concerns, he would see that over-the-top accusations are a counter-productive way to engage with the government." Windsor Star

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Nil

LAW ENFORCEMENT / APPLICATION DE LA LOI

Why did cops target city home?
Five days after swooping down on a northwest London home in the dark of night as part of a terrorism probe, the RCMP still won't say why the place is under investigation. But the family who lives there has had "no communication" from the RCMP since their home was searched - without a warrant - and cleared the night terrorism suspect Aaron Driver died in a confrontation with police in Strathroy, their lawyer said Monday. "My understanding is they are not suspects," said Gord Cudmore, who is acting as a lawyer for

the London Muslim Mosque and, by extension, the family who lives at 43 Blanchard Cres. because they are members of the mosque. London police and officers with the RCMP searched the home Wednesday and Thursday, hours after Driver was killed in a confrontation with police after detonating a bomb in a Strathroy cab. (...) Hours after police had left the property and released it to the owners, the RCMP announced the address at a news conference in Ottawa, and said the property was still under investigation. "I was concerned the address was released," Cudmore said. Asked about that probe Monday, an RCMP spokesperson said via email "the RCMP is not answering any other questions at this time." (...) Told he was not doing anything illegal, a group in the community set out to try to change him by teaching him, "about warmth, about peace, about community engagement," a spokesperson said. "There is no formal program to do this thing, so it was informal people in our community." But despite their best efforts, Driver remained a firm supporter of the Islamic State. RCMP said they were alerted by the U.S. Federal Bureau of Investigation at 8:30 a.m. Wednesday that an individual was planning to bomb an urban centre during morning or afternoon rush hour in the next 24 hours. London Free Press, A1, Front

*** Agir après les faits**

Plus on en apprend sur aaron driver, l'islamiste qui a été neutralisé par la grc alors qu'il s'apprêtait à commettre un attentat suicide, plus on se pose des questions... En juin 2015, Driver (qui avait été arrêté pour «activités suspectes» sur les réseaux sociaux) a été remis en liberté sous conditions. On lui demandait, entre autres, de s'engager à ne pas troubler l'ordre public , d'assister à «des séances de counseling religieux » et de porter un bracelet électronique. À l'annonce de ces conditions, l'Association manitobaine des droits et libertés (AMDL) s'était immédiatement portée à la défense d'Aaron Driver. «On parle d'un citoyen canadien qui n'a pas été inculpé d'un crime, mais qui sera surveillé grâce à un bracelet de surveillance chaque heure du jour, a lancé le directeur de l'AMDL, Corey Shefman. C'est franchement inacceptable .» Je sais qu'il est facile de jouer au gérant d'estrade une fois qu'on sait comment les choses ont tourné... Mais je me demande si, à la lumière des événements récents, le directeur de l'AMDL dirait la même chose aujourd'hui. Défendrait-il encore les droits d'Aaron Driver sachant que le gars était aussi dangereux? «La GRC demande à M. Driver de promettre qu'il va bien se comporter, a dit Corey Shefman. Le problème c'est qu'aux yeux de la loi, M. Driver ne s'est jamais mal comporté...» Ah oui? Affirmer ses sympathies envers l'État islamique n'est pas «mal se comporter»? Entretenir des liens avec des djihadistes qui veulent massacrer des innocents pour déstabiliser le pays n'est pas «mal se comporter»? Journal de Québec, 6 (Journal de Montréal)

*** Police appeal for help after four shootings**

In three decades of policing in Ottawa, Supt. Don Sweet says he doesn't think he's seen any other day quite like Sunday: four shootings in the city in just 13 hours, including the nightclub killing of a known gang member. Police say they're mobilizing every available resource to investigate the killing and the gun violence, but they are also turning to the public for help. Potential links between the shootings are being investigated and police are asking anyone with information to come forward - while promising to protect them from any retaliation - and reassuring all Ottawans that the city remains safe. Within hours on Sunday, police rallied officers from forensics, guns and gangs, general investigations and patrol over multiple scenes with lots of evidence and witnesses, Sweet said. He said he's confident there will be an arrest soon in the slaying of Omar Rashid-Ghader, 33, who was shot multiple times inside the Sentral nightclub in the ByWard Market at about 3:20 a.m. Sunday. (...) Chief Charles Bordeleau said that while he understands residents are concerned, the incidents were targeted shootings involving criminal activity and gang members. "They are not random," Bordeleau said at the Shaw Centre, where the Canadian Association of Chiefs of Police is holding its national meeting. Bordeleau said that Ottawa is not alone as urban police forces see an increase in gang-related shootings. Ottawa police are working with the RCMP and border forces to stem the flow of smuggled handguns, such as a recent arrest of someone bringing the illegal guns through Cornwall to Ottawa. Bordeleau urged witnesses to come forward despite what he called legitimate concerns about retribution for going to police. Ottawa Citizen, A3 (Ottawa Sun)

Children bitten at former daycare, trial told

The former owner of a Memramcook daycare was accused by a former employee of biting some of her young charges as a form of discipline, a Moncton courtroom heard on Monday. The trial for Celine Lang, 56, who is accused of assaulting her young charges and an employee, opened on Monday in Moncton Court of Queen's Bench with testimony from five witnesses. Lang is standing trial on 13 counts of assault,

one count of assault with a weapon and breach of an undertaking. Her judge-only trial is scheduled to last for 13 days before Judge Jean-Paul Ouellette. The opening day of the trial featured testimony from five witnesses: two RCMP officers, two Francophone Sud school district officials and the former employee that Lang is accused of assaulting. (…) When she got home, de la Rosvil called the police. RCMP Const. Kevin Tremblay arrived at her home in Memramcook, where she was with three other daycare workers prepared to talk about what they believed was abuse occurring at the daycare. "They talked about the young kids that were submitted to physical punishment that the women didn't think was safe," Tremblay, who at the time was with the Sackville RCMP detachment, said while testifying on Monday. "In the next few days, I got a list from the daycare with all the people who worked or had worked there. I called them to learn about Ms. Lang. "I also met with parents to take statements, and after all the statements, we determined the incidents to be illegal." Times & Transcript, A1 (Daily Gleaner, Telegraph-Journal)

Distrust, racism loom over probe into farm shooting

Even before a murder charge was laid against Gerald Stanley, a 54-yearold Saskatchewan farmer, for the shooting death of Colten Boushie, a 22-year-old First Nations man whose friends drove a truck on to Stanley's property, the incident became symbolic of a deep social divide. Just as recent police shootings in the U.S. fit an increasingly obvious pattern of official racism, and have drawn more attention because of it, so has Boushie's killing come to seem like the inevitable result of distrust, racism and antipathy between Saskatchewan's white and indigenous people. Dangerously for dispassionate justice, that political weight will hang on the police investigation, the public reaction and any eventual prosecution. "In too many ways, this is a sad day for Saskatchewan," said National Chief Perry Bellegarde of the Assembly of First Nations. (…) Colten Boushie, 22, of the Red Pheasant First Nation died at the scene. He was in the back seat of the truck and was shot in the head, his uncle, Alvin Baptiste, said. His mother, Debbie Baptiste, showed media cherished diplomas and awards, and the boots and helmet her son got for volunteer firefighting work. In their early press statements, police said three people from the vehicle, one woman, one girl and one man, were taken into custody as part of a theft investigation, and they were still looking for another man. The next day, Thursday, when Stanley made an appearance in court in North Battleford, police said "charges are still being considered with respect to some property-related offences pending further investigation." The three were released without charge. Even the police description of the investigation into "the events leading up to the arrival of the vehicle to the yard, the circumstances involving the death, and the actions following," seemed to suggest doubt of the accidental flat tire story. This, at least, is how it seemed to Chief Bobby Cameron of the FSIN, who told The Canadian Press the RCMP statement "provided just enough prejudicial information for the average reader to draw their own conclusions that the shooting was somehow justified. The messaging in an RCMP news release should not fuel racial tensions." Chief Clint Wuttunee of the Red Pheasant First Nation likewise said the resulting stories made it sound like the truck was on the property to commit a crime. Postmedia Network (National Post, A1, Front, London Free Press, Vancouver Sun, Edmonton Journal, Windsor Star, Montreal Gazette, Ottawa Citizen, Calgary Herald); * National Post

'I went a far way, way from home'

When three-year-old Lochlan McKenzie was finally found by searchers on Monday morning, after wandering away from his home the evening before, his face was purple and blue from eating berries. Lochlan, who disappeared while playing outside on his bike, was found safe on a logging road about 10:30 a.m. Monday - nearly 14 hours after he went missing. He was discovered, still with his bicycle, by a team on an ATV after an overnight search in Union Bay, a community of about 1,200 south of Courtenay. (…) The RCMP had a helicopter, a drone, police dogs and a vessel patrolling the shoreline. "We used a lot of resources, put as many people in there as we could," Comox RCMP Const. Rob Gardner said. Gardner said the boy was found near Langley Lake. While the lake is only about two kilometres from his home, the boy likely travelled about five or six kilometres "when you add in all the logging roads," he said. Times Colonist, A1, Front

Teen involved in crash driving with suspended licence

The 16-year-old driver of the vehicle that was involved in a single-vehicle collision Friday that sent four teens to hospital was driving when he wasn't supposed to be. RCMP confirmed Monday that the driver was, in fact, driving while his learner's licence had already been suspended. RCMP were called to the scene at 5:56 a.m. following reports that a vehicle had left the roadway on Brackley Point Road near

Harrington. Four occupants - two boys aged 16 and 15, and two girls aged 17 and 16 - were taken to the Queen Elizabeth Hospital in Charlottetown with serious and potentially life-threatening injuries. At least one of the people in that car, a female, is still in hospital. She was transferred to a hospital in Halifax for treatment. A blood demand was given to the 16-year-old driver who showed signs of impairment. Alcohol was seized from the vehicle. "He was already suspended. He should not have been driving according to the law," said RCMP Staff Sgt. Mark Crowther. Guardian, A4, Front

* **Company believed to be a scam operation**
Police are investigating a possible fraud scheme that cost at least one person thousands of dollars. RCMP said over the course of two weeks, a St. Albert resident transferred money to a company named Option Giant, which police believe is a scam. Police said the resident believed the company traded foreign currencies and there would be a return on investment within 90 days. Slave Lake RCMP had a similar case earlier this summer with the same alleged company. In both cases, funds were sent outside the country so the money wasn't recovered. Police are warning people not to invest in companies without doing prior research. Edmonton Journal, A5 (Edmonton Sun)

Crime top of mind among residents
Crime is increasingly on the minds of Red Deer residents, the City of Red Deer's 2016 Citizen Satisfaction Survey shows. The survey, which cost $21,500 and was released on Monday, shows that 28 per cent of those surveyed named crime as top-of-mind and the most important issue facing the community. That compares with 25 per cent in 2015 and 22 per cent in 2014. Crime also became the top priority this year when respondents were asked what were the top three priorities they felt the city should address over the next 12 months. Those top three priorities are crime (38 per cent); transportation (32 per cent); and municipal government services (26 per cent). Crime surpassed last year's top three - where transportation came in as tops in the May 2015 satisfaction survey - 22 per cent compared with second place crime at 18 per cent. (…) On Thursday Red Deer RCMP will be outline the impact its new crime reduction strategy has had since it came into affect on April 1, along with crime statistics for the second quarter. The worsening economy is reflected in the 2016 satisfaction survey when compared to 2015. Red Deer Advocate, A1, A8

Woman wins battle over security clearance
After a two-year battle with Transport Canada, Ayaan Farah could have her security clearance and job restored. A Federal Court judge quashed the decision to revoke the US Airways employee's security clearance, because Transport Canada failed to give her enough information to defend herself against allegations of links to individuals with criminal records. The decision was "both procedurally unfair and substantively unreasonable," Justice Susan Elliott wrote in a ruling released Monday. Elliott sent the matter back to the federal Minister of Transport Marc Garneau to be considered again in light of her ruling. (…) Elliott criticized Transport Canada for an "improper blanket reliance on the Privacy Act" when responding to Farah's request to know who Subject A was and the date and location of the interaction. In fact, Transport Canada fundamentally changed Farah's questions when they passed on her request to the RCMP, instead asking for "any further information related to the method by which this information was received by police," Elliott found. As a result, the RCMP's answer did not address Farah's questions. Transport Canada then gave Farah a "somewhat misleading" response, blaming the Privacy Act for being unable to provide names of details of third party individuals or sources, Elliott wrote. Toronto Star, A1

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Prison locked down as staff look for contraband items
A federal prison near Moncton is in lockdown while staff search for contraband. On Aug. 11, at about 11:30 a.m., a lockdown was put in place in the medium-security unit at Dorchester Penitentiary to enable staff members to conduct a search. The search was ordered to ensure the safety and security of the institution, its staff and inmates. Normal operations will resume as soon as it is considered safe to do so. Visits have been suspended until the search is completed. The Correctional Service of Canada said in a news release that it is committed to preventing the entry of contraband into its institutions. CSC also

works in partnership with the police to take action against those who attempt to introduce contraband into correctional institutions. Times & Transcript

Prisoner on the lam was deemed a low risk to the public
A man deemed a dangerous offender by the provincial justice system was determined to be a low risk to public safety prior to his escape from the Pe Sakastew federal prison in Maskwacis over the weekend. Darell Moosomin, 54, was on an escorted temporary absence from Pe Sakastew on Sunday, where he was serving an indeterminate sentence, when he escaped. He was on a leave to attend the Samson Powwow when the elder who was supposed to be with him lost sight of him. A Canada-wide warrant was issued for his arrest, but Moosomin remained at large Monday. (…)Correctional Service Canada spokesman Jeff Campbell said inmates are evaluated before being granted permission to go on these types of outings, which can include excursions to complete community service, attend family functions or to access resources such as a doctor or a hospital. Campbell said there are also conditions that must be followed when the leave is granted. Edmonton Sun, A4 (Edmonton Journal, Calgary Sun); Red Deer Advocate

Police say Bedford '100%' likely to reoffend
Internet predator Mark Bedford is contesting an effort by Kingston Police to have him placed on twoyear peace bond meant to keep him offthe Internet and away from children, adolescents and young teens. Det. Brian McCormick, manager of the sexual offender registry for the Kingston Police Force, testified Monday on the first of what is scheduled to be a two-day hearing this week that he made the application based on a series of reports and assessments of Bedford by Correctional Service Canada and the National Parole Board. (…)He was sentenced to three years in prison and ended up serving every day of it after the National Parole Board denied him early statutory release. The board determined that he remained a high risk to re-offend sexually against children. His sentence expired in March 2011, however. (…)He was later found to have violated both those conditions and, after nine months in pretrial custody, was sent back to prison in June 2013 for a further 27 months. The hearing is to continue Wednesday with testimony from two CSC staff. Kingston Whig-Standard, A1

Couple 'reel' busy with derby
Saskia and Mike Deslauriers discovered one drawback when it came to organizing this year's annual Kingston Kids Perch Derby: it didn't leave them any time this summer to do any fishing themselves. (…)Mike Deslauriers is also a correctional service officer at Joyceville Institution and has been involved in the derby since 2013 when he and other officers stepped in with some financial assistance to keep it going after a Ministry of Natural Resources grant was cancelled. At the time, he was president of the correctional officers' union, and its involvement continued in subsequent years. (…)Things looked OK until this past winter when, in a conversation with fish and game club executive member Jim Muir, Deslauriers learned the club membership had dwindled to such a point it didn't have enough bodies to do all the work needed to run a good derby. So he considered taking it on himself. Deslauriers got some unexpected backing from Don Head, commissioner of corrections, who was willing to support what he believed to be a worthwhile community endeavour with resources and manpower. (…)The number of loaner rods traditionally available to any kids who don't already have their own were down this year, so CSC used an inmate work program to help fill the void. Inmates at Joyceville Institution made fishing rod handles and put the rods together before sending them to Bath Institution to be painted. Kingston Whig-Standard, A2

Privacy: subverting good laws for no good purpose
An opinion piece states, "I hadn't paid much attention to stories about the 'departure' of Dieppe's fire chief, but last week a story indicated there's considerable upset over it, including among firefighters who call him a great leader. (…)That said, these cases do not negate the fact that privacy legislation has often proven highly problematic. (…)Correctional Services Canada is notoriously bad for this. They won't tell the public where specific prisoners are jailed, or details of serious incidents inside prison walls. In the tragic case of Moncton teenager Ashley Smith, who hung herself while guards refused to intervene, CSC did everything possible to withhold evidence from a coroner's jury although findings led to some guards being charged with 'negligent homicide,' the charges later withdrawn. And this in a penal system that has repeatedly been exposed as less enlightened than it might be." Times & Transcript, A8

*** Mariage sans contact pour un détenu**
Privé de contact physique avec celle qu'il désire épouser le 12 septembre, un détenu de Portcartier poursuit l'établissement carcéral et le procureur général du Canada pour la somme de 30 000 $. Selon la poursuite déposée devant la Cour fédérale, ces refus de donner à Dominic Delisle accès à l'élue de son coeur «lui causent préjudice». (...)En novembre 2015, alors que les deux tiers de sa peine étaient purgés, la Commission des libérations conditionnelles refusait que Delisle soit remis en liberté, dans une décision considérée comme «exceptionnelle ». (...)Dans le cadre de sa décision, la Commission avait également fait savoir que le détenu avait traité sa conjointe «comme un bien et service ne servant qu'à rapporter financièrement» et en août de la même an-née, une accusation de menace avait été déposée, qui, finalement, s'était soldée par la signature d'un document où il s'engageait à ne pas «harasser, molester, harceler, importuner et épier» sa conjointe. Journal de Québec, 5 (Journal de Montréal)

Abuser doc's victims go after MD watchdog
Some former patients of disgraced ex-psychiatrist Stanley Dobrowolski have lined up to sue him, but their bigger civil target is the governing body for doctors across Ontario. It's the legal actions against the College of Physicians and Surgeons of Ontario that could attract the most scrutiny and debate, says a London civil lawyer who has seven clients who were sexually abused by the former London psychiatrist. The cases, said London lawyer Robert Talach, could end up in the Ontario Court of Appeal to determine whether the college can be held judged for decisions it made to allow Dobrowolski to keep his medical licence while the accusations of sexual abuse kept piling up. (...)Dobrowolski, 69, is serving a four-year sentence after pleading guilty two years ago to 18 charges: 16 counts of sexual assault, one of voyeurism and one of disobeying a court order. He recently was denied parole after it was found he still posed a risk to the community and that he asked his in-prison probation officer when she last had a breast exam. London Free Press, A1

*** Un Canadien détenu en Floride sera rapatrié**
Le Canada a donné son accord au rapatriement de William Russel Davies, un Ontarien détenu en Floride depuis 30 ans après avoir été reconnu coupable d'homicide volontaire. L'État américain où le Canadien purge sa peine depuis ses 18 ans n'a toutefois pas indiqué, pour l'instant, s'il autorisera le transfert. William Russel Davies a été condamné à la prison à vie. Presse canadienne (Le Soleil, 18)

*** Parole denied for man convicted in Sask.'s largest fraud case**
The Saskatchewan man convicted in the biggest fraud case in the province's history has been denied early release from prison. Ronald Jerry Fast, 73, is serving a seven-year sentence after pleading guilty to fraud over $5,000 and possession of property obtained by crime. He was arrested in 2012 following a two-year police investigation that revealed Fast had defrauded more than 200 investors of $16.7 million. Fast used his company, Marathon Leasing Corporation, in a Ponzi scheme, promising high interest rates through the infusion of money from new investors, court heard at his sentencing in 2014. During a parole hearing earlier this month, Fast sought either day parole or full parole, citing his remorse, lack of criminal record and family support. The parole board ruled there is no evidence Fast has addressed any of his risk factors over the course of his sentence, thus denying him both parole options. StarPhoenix, A2

*** Serial rapist released, police warn**
Vancouver police are warning residents that "compelling circumstances exist" to warn the public that Larry John Takahashi, a high-risk sexual offender, is now living in the city. Notoriously known as the 'Balaclava Rapist,' Takahashi was released on day parole in the Vancouver area last month, following a previously shortened 2013 release in Victoria. It remains unknown exactly where Takahashi, now 63, will reside, but police said Monday that he will stay at a correctional halfway house. The Province, A4 (Vancouver Sun); CBC News (2016-08-15)

*** Pimp gets three years for attempt at bribery**
A Vancouver pimp who tried to bribe a Crown witness not to testify against him has been sentenced to three years in jail. The sentence imposed Monday on Reza Moazami will run consecutively to a 23-year jail term he is currently serving for running a prostitution ring of underage girls. Moazami persuaded his co-accused, Babak Najafi-Chaghabouri, to contact a friend outside prison to approach the Crown witness,

who can only be identified by the initials S.W. due to a publication ban. S.W. was told that Moazami was prepared to pay a $5,000 bribe for her to approach his lawyer and recant her evidence against him. He was ready to pay another $5,000 for her not to testify at trial and more money if other witnesses could be convinced not to testify. Vancouver Sun, A4 (The Province, National Post)

*** What is the purpose of an official apology?**
An opinion piece states, "The Globe and Mail reported last week that the Liberal government is set to apologize for the historic persecution of gay Canadians. Their sources suggest an announcement may come as early as the fall. For decades, discrimination based on sexual orientation was built into Canada's legal structure. Beginning in the 1950s, sexual minorities in Canada were prohibited by law from working in the public service and serving in the military. Many were fired from their jobs as a result. Prior to 1969 when then-prime minister Pierre Trudeau's amendments to the Criminal Code came into effect and homosexuality was decriminalized, people who engaged in same-sex acts could be convicted of gross indecency and imprisoned. Homosexuals were classified as "inadmissible" under Canada's Immigration Act until 1978. The list goes on. If it moves forward, this will be the latest in a string of government apologies. (...)In 1967, Everett Klippert, a gay man from the Northwest Territories, was imprisoned as a "dangerous sex offender." It was a legal decision upheld by the Supreme Court of Canada. A mere 38 years later in 2005, same-sex marriage was legalized in Canada." Kingston Whig-Standard, A4 (London Free Press)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Ottawa seen as safe - and stats say it's true**
Ottawa is considered the safest city in Canada, according to a Mainstreet/Postmedia poll to be released Tuesday. It's also one of the rare cases in which the perception almost matches reality as measured by Statistics Canada's Crime Severity Index, said Quito Maggi, president of Mainstreet Research, which conducted the automated telephone poll of 4,213 Canadians about their perceptions of safety in 15 cities. Almost three-quarters of the respondents said Ottawa was safe or very safe. Charlottetown, Moncton, St. John's and Quebec City rounded out the top five "safest" cities, according to the survey respondents. Toronto, Montreal, Saskatoon and Edmonton were in the bottom five. Regina, Halifax, Victoria, Vancouver and Calgary were perceived to be in the middle of the pack. According to the Crime Severity Index, which takes into account both the volume and the severity of crime, Ottawa is actually the thirdsafest city of the 15 on the list, after Quebec City and Toronto, said Maggi. A lot of the public perceptions about a city's relative safety are based on its media exposure, especially on a national level, he said. "When people read about Ottawa, it's not about crime. It's about the prime minister or politics." But some cities got an unfair bad rap in the survey. Winnipeg, for example, was ranked as the most dangerous city in Canada by the respondents - 35 per cent said it was safe or very safe, compared with 56 per cent who said it was unsafe. Ottawa Citizen, A2

*** Plurality of Canadians view Toronto as unsafe: poll**
Canadians view Toronto as one of the most dangerous cities in the country despite a crime rate that actually places it among the safest, a new poll has found. Mainstreet Research asked 4,231 Canadians for their opinion on whether 15 major cities are safe or unsafe. The poll revealed that 47 per cent of respondents view Toronto as unsafe compared to 46 per cent who view it as safe and seven per cent who weren't sure. Only Winnipeg had a less favourable rating (56 per cent viewed it as unsafe). Montreal was the other city in the bottom three (44 per cent viewed it as unsafe). Meanwhile, Ottawa topped the list with 72 per cent of respondents viewing the capital city as safe and just 16 per cent perceiving it as unsafe. Charlottetown (65 per cent viewed it as safe) and Moncton (64 per cent viewed it as safe) rounded out the top three. The results contrast with Statistics Canada's Crime Severity Index, which takes into account the total number of crimes in a given city as well as the severity. CP24

*** New poll ranks Winnipeg as the most unsafe city in the country**
A new Mainstreet/Postmedia poll of 4231 Canadians has found among 15 major cities surveyed, Winnipeg is seen as the most dangerous and Ottawa is seen as the safest. In a news release, Mainstreet/Postmedia says while Winnipeg is seen as the most unsafe, crime statistics recently released

by Stats Canada show Saskatoon actually has the highest crime rate in the country. Toronto, Montreal, Saskatoon and Edmonton were the bottom five most unsafe. Only Toronto joined Winnipeg with a negative score with 46% saying it was unsafe. CTV News

* **Crime-plagued city a 'myth'**
Edmonton is perceived as the fifth most dangerous city in Canada, outranked by Winnipeg, Toronto, Montreal and Saskatoon, a new poll suggests. Winnipeg is considered the least safe place. Ottawa is ranked as the safest city. More than 4,200 Canadians across the country were surveyed and asked to rank 15 cities in terms of safety, regardless of crime statistics, for a poll released Tuesday. Fifty-two percentofthose polled believed Edmonton to be safe, compared to 41 per cent who believed it was unsafe. Seven per cent said they weren't sure. Women were slightly more likely to believe Edmonton was dangerous than men. Seventy-two per cent of Canadians said Ottawa is safe or very safe, compared to 16 per cent who believe it is unsafe. "Perceptions compared to Statistics Canada's Crime Severity Index yields some interesting comparisons," Quito Maggi, president of Mainstreet Research, said in a written statement. "Winnipeg, which is ranked at the bottom by Canadians has a Crime Severity Index lower than Vancouver, Edmonton, Regina and Saskatoon." Edmonton 's Crime Severity Index, which measures the volume of reports and how serious they are, put it as the 13th safest city in Canada in 2015, ahead of Regina and Saskatoon. Edmonton Sun, A4 (Edmonton Journal)

* **Education the best prevention when dealing with bullying**
Education is one of the most imperative tools for preventing bullying. Northern Lights Public Schools (NLPS – formerly Northern Lights School Division) superintendent Rick Cusson suggests sitting down with your children and reminding them to speak to an adult if they are faced with conflict. (…) Cyberbullying adds another platform for bullies, and is defined on the RCMP website as "involving the use of communications technologies, such as the internet, social networking sites, websites, email, text messages and instant messaging to repeatedly intimidate or harass others." Years ago, when you were bullied you would go home and the bullying would stop, said Skinner, however with phones, computers and social media, bullying now follows students home. Cusson recommends having an open relationship with you children in regards to social media. Bonnyville Nouvelle

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

* **Justice for Canada's indigenous women**
An opinion piece states, "Each number has a name, a family, a life story and, tragically, an unresolved ending. One of those stories belongs to Danita Faith BigEagle. The youngest of six children, Danita was born in Arcola, a tiny town known as the "city of angels" that sits in the southeast corner of the Canadian prairie province of Saskatchewan. Like her ancestors, Danita is part of the Ocean Man First Nation, just one among the countless indigenous communities that was a fixture on the prairie long before European settlers arrived and remains an essential part of the Canadian mosaic. On February 14, 2007, the 32-year-old mother of two was, Danita was reported missing after she didn't show up for a visit to her mother who was "caretaker" to her young son and daughter while she got help for drug and alcohol addiction. Her whereabouts and fate are unknown. Sadly, Danita's story is far from unique. In 2014, Canada's national police first revealed that between 1980 and 2012, 1,017 Aboriginal women and girls were murdered across the country and another 164 were missing. These appalling figures continue to climb. (…)But the conscience of Canada and Canadians may be in for a sharp reckoning following the Liberal government's decision earlier this month to launch a commission of inquiry to address belatedly what has been appropriately described by Amnesty International as a "national human rights crisis". (…)Whatever the inquiry's ultimate recommendations, the institutional efforts to finally find the missing women and girls must be redoubled and the perpetrators must - if possible - be apprehended. Only then, will Canadians be able to right, in part, the injustice visited upon their indigenous neighbours for generations." Al Jazeera

* **Making progress with First Nations**

An opinion piece states, "The Canadian Government announced the official launch of a national inquiry into missing and murdered indigenous women (MMIW) on Aug. 3. It's about time, given the RCMP report stating there are a total of 164 missing women and 1,017 homicide victims in Canada — a total of 1,181 MMIW — between 1980 and 2012. Those are staggering numbers, especially if we assume they have gone up since 2013. To those who say, 'Violence in the indigenous community is indigenous-on-indigenous violence, therefore it's an indigenous problem' — I have a response. (…)So, to the people with the aforementioned mentality: the way I see it, any problem within the indigenous community isn't just an indigenous problem — it's a Canadian problem — a problem for us all to rectify." Rocky Mountain Goat News (2016-08-15)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Calgary Police Commission push for roadside drug testing device ahead of marijuana legalization**

Driving impaired is driving impaired - it doesn't matter what substance a person's on, but Calgary police and their overseeing commission wants to be ready when one in particular is legalized. This weekend in Ottawa, at a Canadian Association of Police Governance Conference, the Calgary Police Commission put forward a resolution to continue pressure on the federal government to identify and approve a roadside drug screening device, in light of the feds' commitment to legalize and regulate marijuana by 2017. "Currently, when police suspect a driver of being impaired by drugs, a drug recognition expert is called to the scene to administer a field sobriety test. A roadside drug screening device would greatly improve the ability of police officers to detect drug impaired driving and provide objective and efficient means of enforcing drug impaired driving laws," the commission's resolution read, in part. "A roadside drug testing regime would be similar to roadside breath testing for alcohol. "This capability would simplify the current investigative process for drug-impaired driving, including potentially reducing the time a motorist is detained." "Given the imminent legalization of marijuana and its proven negative effect on drivers, there is now urgency around acquiring appropriate tools in Canada to enable police to detect drug-impaired drivers roadside so they can effectively enforce road safety laws, especially the stricter punishments for marijuana-impaired drivers that government intends to introduce," the resolution read. Calgary Herald

*** As Canada Moves to Legalize Marijuana, Shop Owners Ask: Why Wait?**

The Cannabis Culture Lounge has everything a pothead might need to feel right at home: $3 marijuana buds, bongs for rent, bags of Skittles and Doritos for sale, and black leather couches where customers can recline in zoned-out contemplation in a pungent haze. Never mind that it is all technically prohibited by Canadian law. Still, some enthusiasts have higher hopes for the business, which opened more than a decade ago as a kind of speakeasy for marijuana smoking — long tolerated by the city's authorities. The lounge began selling marijuana after Justin Trudeau was elected prime minister in November. "This is what recreational marijuana legalization in Canada looks like," said Jodie Emery, an activist and the co-owner of the lounge and several medical marijuana dispensaries across Canada. Mr. Trudeau has promised to make recreational marijuana legal in Canada as soon as next year, bypassing the nation's strict medical marijuana regulations. Under the latest rules for medical use, announced last week, patients must be registered, have a prescription and obtain their supplies only by mail from a government-licensed producer or by growing a limited amount privately. New York Times (2016-08-15)

PUBLIC SERVICE / FONCTION PUBLIQUE

Nil

OTHER / AUTRE

Nil

INTERNATIONAL

Nil

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
August 17, 2016 / le 17 août 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Goodale contradicted over detainee claim: 17 responded to minister's request for details on why detention was unfair
Advocates for a group of hunger-striking immigration detainees were shocked Monday to hear **Public Safety Minister Ralph Goodale** say none had replied to his request for details of why their detention was unfair. In fact, 17 of 50 detainees in two Ontario jails who ended a hunger strike in July responded to **Goodale**'s invitation conveyed to them by Canada Border Services Agency officials. Syed Hussan, a member of the End Immigration Detention Network, told the Star that many wrote **Goodale** to make their individual case, and others did not. "Many of the detainees refused to participate. They didn't know what it was for. They didn't know it came from **Goodale**'s office," Hussan said, adding many felt that, "the onus is not on the detainee to prove why he shouldn't be in there. "The onus is on the government to explain why someone is in prison without trial or charges, in the case of the people we work with, mostly for two-plus years." Scott Bardsley, a spokesman for **Goodale**, told the Star Tuesday that the minister was not fully briefed with the latest information on the hunger strikers' file prior to a news conference in Laval, Que., Monday. Toronto Star, A11

Prison farm proponents make their case

Correctional Service Canada finally hosted its town hall meeting Tuesday night at City Hall surrounding the reinstatement of prison farms at the Joyceville and Collins Bay institutions, a gathering anticipated since July 13 by the Save Our Prison Farms (SOPF) committee. Between 2009 and 2013, six federally run prison farms across the country, two of which were in Kingston, were closed by the Conservative government. The farms were closed as a cost-cutting measure. The government also claimed, at the time, that offenders were not being prepared to enter the workforce, as "very few ex-inmates were obtaining work in agriculture." Frontenac institution was the only farm to earn limited revenue, being the largest at 900 acres and housing a dairy operation, egg production, fruit and vegetables and a prizewinning breed of heritage cattle, the last of which were shipped out in August 2010 before hundreds of protesters. **Ralph Goodale, the minister of public safety and emergency preparedness** was in attendance at the town hall meeting. A couple of hours earlier, he took a tour of the Collins Bay facility, saying, "***I know the issue [of reopening the prison farms] is close to many in Kingston and the Islands***." He deemed the tour of the penitentiary's long unused farm facility "***largely a learning experience***" for him. (...) "***There are certain values and morals that you gain doing farm work***," he said in response to the question of why the government is regaining interest in a program it had earlier rejected. "***I can't discuss specific cases, but we're looking at minor offenders who sincerely want to reintegrate into society, and we can help them do that***." Goondale suggested the town hall meeting as part of a larger feasibility study to assess the viability of re-establishing the "***agri-food employment initiatives for offenders***" that organizations like Save Our Prison Farms have been pushing for the past six years. (...) **Goodale** seemed to be in agreement with the positive results of farming programs. "***Effective rehabilitation and integration programming for inmates are absolutely fundamental in successfully achieving that goal of public safety,"*** he said. ***"Part of that is making sure they have the right skills, the right qualities, the right attitudes, to maintain employment and be constructive to society.***" Kingston Whig-Standard, A1

Driver killed by gunfire: Father: ISIS supporter's funeral won't be held at mosque in London, spokesperson says

An ISIS supporter who died during a confrontation with an RCMP tactical team outside his home in Strathroy, Ont. was killed by a police bullet, his family said Tuesday. Wayne Driver said an autopsy had determined that his son Aaron had been shot two times and that one of the bullets had struck his liver and travelled to his heart. The other hit his spleen, he said. The 24-year-old was allegedly in the final stages of preparing a terrorist attack on Aug. 10 when a police Emergency Response Team surrounded him. He detonated an explosive device and police opened fire. Following the incident, the RCMP said it was unsure whether Driver had died as a result of his own bomb or police bullets but the father said the autopsy had put that question to rest. "It was the police officer's bullet that killed him," the father told the National Post. "The bomb that exploded he could have walked away from with minor to severe injuries they said." (...) In his first reaction to the alleged terror plot, Prime Minister Justin Trudeau said a wider response to domestic terrorism would be rolled out by **Public Safety Minister Ralph Goodale**. "All Canadians expect their government to do two things: To keep Canadians safe and to defend and uphold the values and rights that all Canadians hold dear," he said during a stop in Bridgetown, N.S. "Getting that balance right isn't always easy in the challenging situation we now live in but it's extremely important." Kingston Whig-Standard, B1/FRONT; * Canadian Press (Times Colonist, A7)

Change terror tactics

The RCMP thought Martin Couture-Rouleau was on the right track when officers met the 25-year-old radicalized convert on Oct. 9, 2014. Despite a failed attempt to travel to Syria, he seemed to be coming around. Eleven days later, he drove to a strip mall frequented by uniformed soldiers in Saint-Jean-sur-Richelieu, Que., and killed Warrant Officer Patrice Vincent. Chased by police, he crashed his car and charged officers with a knife before he was shot dead. Following a similar scenario in Strathroy, Ont., on Aug. 10, which ended with the shooting death of ISIL supporter Aaron Driver as he was allegedly about to conduct a bombing, some experts are calling for changes to the way extremists are assessed. In the Couture-Rouleau and Driver cases, the assessments were ultimately wrong. Both men had come to the attention of the RCMP but were apparently thought to have softened their views and were not being closely monitored. (...) The Violent Extremist Risk Assessment tool currently used is a guide that rates

extremists based on whether they score low, medium or high on 25 categories such as use of extremist websites, direct contact with extremists and military training. But it "has some weaknesses," Prof. Dawson said. "It shows some potential but it's got some real limitations. ... Everyone recognizes that we really need to get serious about developing better assessment mechanisms." He said the office of community outreach and counter-radicalization that **Public Safety Minister Ralph Goodale** has announced would likely take on the task. "They're aware of this and this is probably one of the things they're going to be pouring a lot of resources into." Postmedia Network (National Post, A1, Front, Vancouver Sun, Windsor Star, Kingston Whig-Standard, StarPhoenix, Leader-Post, Montreal Gazette, Ottawa Citizen, London Free Press, Edmonton Journal, Calgary Herald)

How will PM tackle terror? Just watch him

An opinion piece states, "So far on terrorism, Justin Trudeau is more or less the prime minister Stephen Harper told us he would be. On the very day Trudeau became leader of the Liberal Party of Canada, in April 2013, he sat in Ottawa for an interview with Peter Mansbridge of the CBC. Two bombers had just detonated their home-brew contraptions at the Boston Marathon, killing three and wounding hundreds. How would you respond if you were prime minister, Mansbridge asked. "Over the coming days," Trudeau replied, "we have to look at the root causes." That language seemed custom- designed to ruffle Conservative feathers. But Trudeau was not done. "There is no question that this happened because there is someone who feels completely excluded. Completely at war with innocents . . . And our approach has to be, where do those tensions come from?" (...) In a long weekend news release, **Goodale** first reassured Canadians that the police had done their job well and that Canada's threat level is no higher than it has been for a year and a half. Then he added: ***"We have also budgeted for a new national office and centre of excellence for community outreach and counter-radicalization. "We need to get really good at this - to preserve our diversity and pluralism as unique national strengths."*** So if you want a government that conveys any view other than utter condemnation, this new Liberal government's language will seem wildly complicated. **Goodale** remains unbowed. ***"We need to know how to identify those who could be vulnerable to insidious influences that draw certain people - especially young people - toward extremism leading to violence,"*** he wrote. ***"We need to understand what positive messages can counteract that poison."*** Toronto Star, A1

A question of balance: CIVIL LIBERTIES, SECURITY EQUAL IN BATTLE AGAINST TERRORISM: PM

An alleged terrorist plot in Ontario that created anxieties over police monitoring of suspects hasn't shaken Prime Minister Justin Trudeau's emphasis on balancing civil liberties with public safety. In his first reaction to an alleged plot that led to the death of Aaron Driver in Strathroy, Ont., Trudeau said Tuesday that balancing individual rights with keeping Canadians secure from bombing threats has to be handled with care. "Canada is a country that values its freedom (and) its basic charter rights," he said during a stop in Bridgetown, N.S., for an infrastructure funding announcement. "All Canadians expect their government to do two things: to keep Canadians safe and to defend and uphold the values and rights that all Canadians hold dear." "Getting that balance right isn't always easy in the challenging situation we now live in but it's extremely important." (...) During the news conference, the prime minister said the wider response against domestic terrorism will be rolled out by **Public Safety Minister Ralph Goodale** as the Liberals continue plans to reform Bill C-51. During the last federal election, the Liberals pledged to guarantee that all Canadian Security Intelligence Service warrants respect the charter, that the right to lawful protests and advocacy aren't violated, and they pledged to "narrow overly broad definitions (in Bill C-51), such as defining 'terrorist propaganda' more clearly." They also said a Liberal government would limit the Communications Security Establishment's powers by requiring a warrant to engage in the surveillance of Canadians and emphasize community outreach to battle radicalization of youths. Canadian Press (Red Deer Advocate, A8, Cape Breton Post, Telegraph-Journal); Postmedia News (Ottawa Sun, A9, Winnipeg Sun, Toronto Sun, Edmonton Sun, Calgary Sun)

*** Review of Harper's Anti-Terrorism Bill Likely to Launch End of Summer**

Long anticipated look at C-51, national security starts 'soon,' official says. The government's highly anticipated review of its national security framework, including the Harper government's controversial anti-terrorism legislation C-51, is expected to start before parliamentarians return from summer break***. "Yes, it will be soon — so most likely before Parliament resumes,"*** said **Scott Bardsley**, press secretary for

Public Safety Minister Ralph Goodale. Prime Minister Justin Trudeau campaigned on a promise to "repeal the problematic elements of Bill C-51, and introduce new legislation that better balances our collective security with our rights and freedoms." But so far, he has not provided details on when he envisions starting that process despite pressure from critics of the law. (…) As well, the government has moved ahead on a promise to help those whose names match those on the no-fly list and who face travel delays during the extra time needed to clear their name in the system.In June, **Goodale** announced the creation of a new government office to support those travellers, with the eventual goal of allowing those travellers to apply for a unique identification number to distinguish them in aviation systems. iPolitics (The Tyee)

*** Border phone search case raises thorny issues: lawyers**
Several thorny questions still haven't been answered in the case of a Quebec man who refused to give border officers his cellphone pass code, say privacy and technology lawyers. Alain Philippon had said he would fight a charge of obstructing border officials but pleaded guilty Monday in Dartmouth, N.S., and was fined $500. He was charged when he refused to unlock his cellphone in March 2015 after flying to Halifax from the Dominican Republic. David Fraser, a privacy lawyer with McInnes Cooper in Halifax, says that because the case didn't go to trial there are still serious doubts about phone searches. (…) "A phone really is a portal that goes well beyond the sorts of things that have been traditionally searched at the border." In an email, a spokesman for **Public Safety Minister Ralph Goodale** said the government wants to hear from experts and the general public on how to ensure safety while protecting rights during upcoming consultations on national security. **Scott Bardsley** said those consultations would include border security policies. ***"Canadians need to reflect on new and emerging areas of law, privacy and public safety," he said. "We all need to think this through carefully. There are no easy answers."*** Canadian Press (Times & Transcript, B4, Record, Hamilton Spectator, Chronicle Herald, Cape Breton Post)

TOP STORIES / MANCHETTES

*** Trudeau se tourne vers le comité parlementaire**
Le premier ministre Justin Trudeau estime que le comité parlementaire créé pour surveiller les activités des agences de renseignement aura à évaluer l'efficacité du travail de ces agences. La semaine dernière, la Gendarmerie royale du Canada (GRC) a intercepté un jeune Canadien qui préparait une attaque terroriste. Le jeune homme était connu des autorités canadiennes, mais c'est le FBI qui a alerté la GRC alors que l'homme préparait un attentat imminent. (…) «Cette situation de la semaine dernière et des situations semblables, c'est exactement le genre de choses sur lesquelles le comité de parlementaires aura à s'exprimer, aura à réfléchir», a-t-il ajouté. Le premier ministre s'attend à ce que ce comité offre «des conseils sur la manière dont on peut encore mieux assurer la sécurité des Canadiens, comme nous avons pu le faire la semaine dernière». Presse canadienne (Le Droit, 15, La Presse+, Le Soleil) (2016-08-16); ***** Agence QMI (Journal de Montréal)

Funeral for terrorist sympathizer will not be held at mosque
Muslim institutions in London, Ont., are keeping their distance as funeral arrangements are underway for a terrorist sympathizer killed in a high-stakes police standoff in a nearby community. A spokesman for the London Muslim Mosque says the organization is offering support to Aaron Driver's family and advice on planning the service according to Islamic traditions, which is expected to be held Thursday. But Nawaz Tahir says the ceremony will not be held at any Muslim institution in the city, nor will any local imam preside, acknowledging there were concerns over appearing to be associated with someone linked to terrorism. In a statement issued after last week's takedown, the mosque said it had taken notice of Driver and his views more than a year ago and had tried to steer him away from extremism. "We engaged him with the hope of changing his views on Islam and to show him the true, peaceful nature of our religion," the statement read. "We constantly monitored his activities within the mosque and did our best to keep the authorities engaged with our activities. Driver, 24, died during a confrontation with RCMP in Strathroy, Ont., last Wednesday after making a martyrdom video that suggested he was planning to detonate a homemade bomb in an urban centre. Ontario Provincial Police, who took over the investigation into his death, said Tuesday he died from a gunshot wound, but gave no other details. The investigation into the

incident is also ongoing. (...) Aaron Driver's father has said his son was a troubled child but appeared to have turned his life around after converting to Islam. But then the father said CSIS contacted him in January 2015 about disturbing posts his son had made on social media. Canadian Press (Red Deer Advocate, A8, Winnipeg Sun, Ottawa Sun, Toronto Sun, Times Colonist, Edmonton Sun, Calgary Sun, Daily Gleaner, Times & Transcript, CTV News); * Presse canadienne (Le Droit) ; * Radio-Canada

*** Les chefs de police réclament l'accès légal aux mots de passe**
Les chefs de police canadiens réclament une loi pour contraindre les gens à révéler leurs mots de passe aux forces de l'ordre s'ils ont obtenu l'approbation d'un juge. L'Association canadienne des chefs de police (ACCP) a adopté une résolution incitant le gouvernement à prendre des mesures législatives pour faciliter l'obtention de preuves électroniques. L'ACCP estime que les criminels ont de plus en plus recours au chiffrement pour dissimuler leurs activités illicites en ligne. Le commissaire adjoint de la Gendarmerie royale du Canada (GRC), Joe Oliver, a déclaré qu'aucune loi canadienne ne contraignait actuellement le détenteur d'un mot de passe à le révéler aux policiers dans le cadre d'une enquête. Lors d'une conférence de presse mardi, M. Oliver a soutenu que les criminels, qu'ils soient membres de la mafia ou pédophiles, bénéficient d'un anonymat quasi absolu grâce à des outils en ligne qui camouflent leur identité, de même que leurs communications. «Les victimes dans l'espace numérique sont réelles, a rappelé M. Oliver. Les lois du Canada et sa capacité à maintenir l'ordre doivent suivre le rythme de l'évolution technologique.» Cette résolution de l'ACCP survient alors que le gouvernement fédéral entame ses consultations en matière de cybersécurité, notamment par rapport à l'équilibre entre les besoins des policiers et les libertés fondamentales. Ces consultations se poursuivront jusqu'au 15 octobre. La Presse Canadienne (Le Quotidien, 17, Le Soleil); Canadian Press (Times & Transcript, Calgary Herald, National Post, Ottawa Citizen, Leader-Post, Edmonton Journal, Waterloo Region Record, Toronto Star, Hamilton Spectator, Edmonton Sun, Toronto Sun, Cape Breton Post, Chronicle-Herald, The Telegram, The Guardian)

*** Calgary police push for right to access digital passwords**
Calgary police are supporting calls for a new law that would force civilians to hand over electronic passwords to investigators with a judge's permission. Calgary police Chief Roger Chaffin was among those at the Canadian Association of Chiefs of Police who voted Tuesday to ask for legal means to obtain such digital evidence, saying it would help law enforcement keep pace with cybercrime. But civil liberties advocates say such a law would be highly problematic, and might even clash with the Charter of Rights and Freedoms. "When the chiefs of police want this sort of self-incrimination and openness, will it apply to them as well?" said Rocky Mountain Civil Liberties Association director Sharon Polsky, insisting it would be "flagrantly in violation" of Canadians' privacy rights. Current laws don't allow police to compel someone to give them a password. Deputy Chief Sat Parhar, who was in Ottawa with Chaffin to vote on the resolution, said the new legislation would be a guide for law enforcement, outlining when it is and isn't OK to access certain data. "There's a rule book, the rule book is the criminal code," said Parhar. "We're just saying this needs to be represented in the rule book. You don't want the police doing things without some sort of guidance through the law." Calgary Herald, A1

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Up to 47,000 houses face flood risk**
The Insurance Bureau of Canada wants a new deal for people who live in the riskiest, most flood-prone areas. On Tuesday, the association that represents most insurance companies in the country told the legislature's climate change committee it wasn't fair for taxpayers to keep subsidizing people who live in floodplains or along coastal areas. "I hate to say this, but in the industry we now call water the new fire," said Amanda Dean, a vice-president with the bureau. Thanks to torrential downpours, flooding has become the biggest insurance claim in recent years, outstripping the former number 1 claim, for fire damage. Over the last 20 years, property claims have doubled in New Brunswick, most of them due to water damage. Across Canada, annual insured losses from catastrophic events are now close to $1 billion, with 2013 the high-water mark, when insurers paid out a record-high $3.2 billion. In June, the association submitted a proposal for a national flood strategy to Ottawa. It spent more than $1 million mapping out areas in Canada that are prone to flooding from rivers, and is about to do the same for

coastal areas. According to its analysis, about 90 per cent of the country's homeowners live in areas that are not at high risk of flooding, and are insurable. The other 10 per cent live in areas such as floodplains that are just too risky to insure. Although there's a perception many of these people are wealthier people with waterfront homes, most of them are actually low-income or middle class. Typically, when these uninsurable properties are inundated, the federal and provincial governments step in to help. Over the last decade in New Brunswick, the government payouts have been $135 million - about $100 million covered by Ottawa and $35 million by the province. Times & Transcript, B1 (Daily Gleaner, Telegraph-Journal)

*** Storm damage hits $48 million**

The Insurance Bureau of Canada says severe storms that swept across the Prairies last month caused more than $48 million in insured damage. Intense thunderstorms between July 8 and 11 produced strong winds, hail, lightning, heavy rain and funnel clouds in Alberta, Saskatchewan and Manitoba. Most property damage was reported in Saskatchewan, where up to 130 millimetres of rain in a short period resulted in significant flooding in Estevan. The downpour overwhelmed the local stormwater network and caused streets to flood and sewers to back up. Bill Adams, a vice-president with the insurance bureau, says severe storms are happening more often and with greater intensity across the Prairies. He advises people to understand their insurance policies and be prepared for an emergency. Canadian Press (Calgary Herald, B12, StarPhoenix, Edmonton Journal)

*** Firefighters keep watch after rain**

While the recent precipitation in western Nova Scotia was enough for firefighting crews to get a toehold on blazes around Seven Mile Lake, it's not over until it's over, say provincial officials. "You can never say things are good when it comes to wildfires because things change so quickly," said Department of Natural Resources forest technician Dave Steeves. "Where we are sitting with it now is much more favourable than where we were three days ago." Having 100 per cent containment doesn't mean the fire is completely extinguished, it just means crews have a perimeter around the area of the fire, he said. Chronicle-Herald, A3

*** Smoke from B.C. fire may enter Yukon**

The BC Wildfire Service in Dease Lake is cautioning the public to be aware of smoky conditions on Highway 37 from Wheeler Lake to the Yukon border and along the Alaska Highway. It's due to a Blue River wildfire. Smoke may also be visible from Upper Liard, Watson Lake, and Lower Post. Warm temperatures and gusty wind conditions have increased fire growth and hampered visibility. Drivers are advised to drive cautiously and should not stop between Blue River and One Ace FSR. The Blue River wildfire was started by lightning on July 17. It is approximately 1,846 hectares in size and is located about 22 kilometres south of the Yukon border. The fire is burning within an area where a wildfire occurred in 2010 and there are no structures or communities threatened. The wildfire is currently in "modified response" status. Whitehorse Daily Star, 5

*** BC Hydro emails show concern for fracking**

Officials at British Columbia's public power utility have been raising concerns as early as 2009 that earthquakes caused by a controversial gas-extraction method used in the mining industry may put the province's largest hydroelectric dams at risk, internal documents reveal. Emails obtained through an access-to-information request by the Canadian Centre for Policy Alternatives show BC Hydro discussing the possible threat posed by hydraulic fracturing, or fracking, a mining technique that involves injecting high-pressure fluid deep underground in order to extract either natural gas or coal-bed methane. Critics have slammed fracking as a poorly understood and risky industrial activity that contributes to increased seismic activity and risks contaminating nearby aquifers. In one BC Hydro email exchange dated Dec. 3, 2009, safety officer Ray Stewart expresses his unease to water rights comptroller Glen Davidson over the risks of a particular methane-extraction project near the Peace Canyon Dam. Canadian Press (Chronicle-Herald, A6, Red Deer Advocate)

*** Fort Mac residents plagued by sleepless nights**

Geneviève Belleville is struck most about the many Fort McMurray residents who are having nightmares and trouble sleeping. The psychology professor at Université Laval in Quebec City is heading a mental-

health study of people from the northern Alberta city who were forced to flee a voracious wildfire in May. Two of her research assistants were returning Tuesday after spending three weeks in the community. They conducted clinical interviews with about 50 residents and another 300 people completed an online questionnaire. Analysis is to begin soon on whether some are suffering from post-traumatic stress disorder, Belleville said. A preliminary look at the data shows many in the group aren't sleeping well. Canadian Press (Toronto Star, A9, Edmonton Journal)

* **Mayor pans Kinder Morgan's 'risky' pipeline expansion**
Vancouver Mayor Gregor Robertson has told a federal panel on the proposed Kinder Morgan pipeline expansion that the project could be catastrophic to the city. The Province, A10

* **Local search and rescue group helps member repair fire damages to home**
Darleen Steeves woke Aug. 11 to snapping noises and a glow coming into her window. When she looked out of the window she was shocked to see the trailer next door on fire. She called 911 and proceeded to get out of the house. So before waiting for the investigation to be concluded, volunteers at the York Sunbury Search and Rescue (YSSR) group she belongs to rallied together to repair the damages to the side of her home Sunday. Daily Gleaner, A4

* **N.-B.: un petit hydravion s'écrase au décollage**
Un petit hydravion s'est écrasé dans le fleuve Saint-Jean près de Woodman's Point, au cours du décollage, samedi vers 14 h. L'aéronef avait auparavant amerri sans problème. Les deux passagers ont réussi à sortir de l'aéronef d'eux-mêmes. Plusieurs embarcations se trouvant dans le secteur, entre autres une embarcation de l'équipe locale de recherche et sauvetage, se sont rendues sur les lieux pour venir en aide aux passagers. L'Acadie Nouvelle, 6

* **Grimsby volunteer marine rescuers lose boat during mission**
A volunteer marine rescue unit that lost its "workhorse" boat during a weekend call is trying to chart a way forward during the busiest time of the season. The crew discovered the fibreglass hull of the 22-foot Zodiac had cracked while towing a 42-foot boat to safety in Hamilton Saturday. Whether it can be fixed is uncertain. TheSpec.com

* **Lost boy survives on berries**
A three-year-old boy who got lost in the bush overnight on Vancouver Island did a good job of taking care of himself - feasting on berries until authorities found him. The tot slipped out of his home near Union Bay early Sunday evening, crossed a highway on an overpass and went down a logging road. Six search teams, including Mounties, dogs and even a drone - covered the area for 14 hours before locating the boy at 11 a.m. Paul Berry, with Comox Valley Ground Search and Rescue, said, "He was feeding himself on berries. He had a face full of blue and purple from eating berries, but otherwise, in good shape." Canadian Press (Edmonton Sun, A78)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

* **Trudeau se tourne vers le comité parlementaire**
Le premier ministre Justin Trudeau estime que le comité parlementaire créé pour surveiller les activités des agences de renseignement aura à évaluer l'efficacité du travail de ces agences. La semaine dernière, la Gendarmerie royale du Canada (GRC) a intercepté un jeune Canadien qui préparait une attaque terroriste. Le jeune homme était connu des autorités canadiennes, mais c'est le FBI qui a alerté la GRC alors que l'homme préparait un attentat imminent. (...) «Cette situation de la semaine dernière et des situations semblables, c'est exactement le genre de choses sur lesquelles le comité de parlementaires aura à s'exprimer, aura à réfléchir», a-t-il ajouté. Le premier ministre s'attend à ce que ce comité offre «des conseils sur la manière dont on peut encore mieux assurer la sécurité des Canadiens, comme nous avons pu le faire la semaine dernière». Presse canadienne (Le Droit, 15, La Presse+, Le Soleil) (2016-08-16); * Agence QMI (Journal de Montréal)

Funeral for terrorist sympathizer will not be held at mosque

Muslim institutions in London, Ont., are keeping their distance as funeral arrangements are underway for a terrorist sympathizer killed in a high-stakes police standoff in a nearby community. A spokesman for the London Muslim Mosque says the organization is offering support to Aaron Driver's family and advice on planning the service according to Islamic traditions, which is expected to be held Thursday. But Nawaz Tahir says the ceremony will not be held at any Muslim institution in the city, nor will any local imam preside, acknowledging there were concerns over appearing to be associated with someone linked to terrorism. In a statement issued after last week's takedown, the mosque said it had taken notice of Driver and his views more than a year ago and had tried to steer him away from extremism. "We engaged him with the hope of changing his views on Islam and to show him the true, peaceful nature of our religion," the statement read. "We constantly monitored his activities within the mosque and did our best to keep the authorities engaged with our activities. Driver, 24, died during a confrontation with RCMP in Strathroy, Ont., last Wednesday after making a martyrdom video that suggested he was planning to detonate a homemade bomb in an urban centre. Ontario Provincial Police, who took over the investigation into his death, said Tuesday he died from a gunshot wound, but gave no other details. The investigation into the incident is also ongoing. (…) Aaron Driver's father has said his son was a troubled child but appeared to have turned his life around after converting to Islam. But then the father said CSIS contacted him in January 2015 about disturbing posts his son had made on social media. Canadian Press (Red Deer Advocate, A8, Winnipeg Sun, Ottawa Sun, Toronto Sun, Times Colonist, Edmonton Sun, Calgary Sun, Daily Gleaner, Times & Transcript, CTV News); * Presse canadienne (Le Droit) ; * Radio-Canada

Expansion urged for programs that combat radicalization

After RCMP thwarted a major terror threat in Ontario last week, Mohamed El-Rafih knew that his community anti-radicalization initiatives were more urgently needed than ever. El-Rafih is best known in Calgary's Muslim community as the creator of an anti-radicalization program that he calls Fostering Youth Inclusiveness (or FYI). The program is a day camp for children aged five to 12 that aims to fight radicalization by tackling the feeling of isolation that some Muslim children experience while trying to integrate into Western society. Now, El-Rafih is gathering a group of local politicians, police, religious leaders and Muslim community members on Thursday to see how his programs can be expanded and brought to high schoolage youth. "The purpose behind this meeting is to look at the messaging (we've come up with), and to get everybody's opinion on … whether it is going to help us against radicalization," said El-Rafih. "There's messaging for Muslims and there's a message for non-Muslims. The message for Muslims is on how there could be misinterpretations on misguided imams and misguided leaders that could make youth vulnerable to radicalization." (…)El-Rafih expects the Calgary police, RCMP and Darshan Kang, Liberal MP in the Calgary SkyView riding, to attend Thursday's meeting, and hopes their input can help craft an effective message that will help to prevent the radicalization of teenage Muslims. Postmedia Network (Calgary Herald, A11, Edmonton Journal, Calgary Sun)

Terrorism propaganda case referred straight to trial

The Public Prosecution Service of Canada says the case against a Fort St. John man charged with four terrorism-related offences will go directly to trial. Spokeswoman Elizabeth Armitage said the case of Othman Ayed Hamdan will proceed by direct indictment, meaning there will not be a preliminary inquiry. Hamdan was arrested in July 2015 and accused of posting Islamic State propaganda online. An RCMP statement at the time alleged the propaganda included inducement and instructions to commit murder in the name of jihad. None of the allegations has been proven in court. Hamdan was originally charged with three terrorism related charges in provincial court, but Armitage said those charges have been stayed. B.C. Supreme Court documents show he is now charged with counselling to commit murder for a terrorist group, counselling to commit assault causing bodily harm for a terrorist group, counselling to commit mischief for a terrorist group and instructing a person to carry out a terrorist activity. Canadian Press (Times Colonist, A5)

*** American Involvement In Canadian Terror Cases Must Be Questioned**

While watching last week's RCMP press conference in the aftermath of Aaron Driver's death, many questions invaded my mind but were left unanswered. The RCMP's narrative of the events that transpired was repeated over and over in the media with very little questioning. Mike Cabana -- the deputy commissioner of the RCMP who stood alongside his colleagues in the conference room at the RCMP headquarters, apparently nervous and uncomfortable answering some questions -- is the same Mike

Cabana that was involved in the case of Maher Arar. (…) By contrast, Ottawa resident Mohamed Harkat has been the object of a security certificate due to suspicions that he is an Al-Qaeda sleeper agent for more than a decade. Today, he continues to face the threat of being deported to torture by the Canadian government, and has worn a GPS electronic bracelet for more than six years while living under what amounts to house arrest. All his visitors must report to Canada Borders Services Agency (CBSA) and he must obtain the authorization of the CBSA to leave his house. For years, he couldn't use the Internet or even get near a computer. Huffington Post (2016-08-16)

Kudos and questions in terrorist takedown
An editorial states, "Canada came very close to suffering a terrorist attack last week, but countless lives were saved when police disrupted the plan. The wouldbe terrorist, Aaron Driver, who was living in Strathroy under what was basically a restraining order, was killed. How he died isn't yet clear. The Ontario Provincial Police are investigating whether he died by police gunfire or from a bomb that went offin the back of a taxi, injuring the cabbie who had picked up Driver at the house in which he lived. The RCMP acknowledged the tragic outcome but noted correctly that had Driver not been stopped, the carnage would have been far, far worse. So let's take a moment to give our police and security authorities - whose actions are often challenged - full credit. In a fine example of cross-border co-operation, the operation began with a tip from the FBI, which had come across a martyrdom video. (…) Questions remain, of course. We don't know how the FBI got the video, for example. Some wonder about the peace bond Driver was under and why an electronic monitoring bracelet had been removed. There's a tricky balance between monitoring for terrorism and respecting civil liberties; he had never been charged or convicted of a dangerous crime. Even if he had, severe conditions, particularly imprisonment, can further fast-track extremist tendencies. There are dicey political and policy issues ahead. The Liberals remain committed to reforming the Tories' anti-terrorism bill, C-51, but this incident adds complications. And the task has barely begun, although a bill to create a new national security oversight committee has been tabled." Kingston Whig-Standard, A4

Don't overestimate terrorist threat to Canada
An opinion piece states, "Last Wednesday Canada experienced another brush with global terrorism, when Aaron Driver was killed during a violent encounter with police in the sleepy southern Ontario town of Strathroy. No one but Driver was killed in the incident, but the fear-mongers were quick to tell Canadians that the intent of this deranged Islamic supporter of Daesh (also known as Islamic State, ISIS, and ISIL) was to commit mass murder during a workday rush hour. Scary stuff. According to the official version of events, it was the FBI that first discovered that Driver had made a recent martyrdom video and was about to launch an attack. It had to be the FBI because the Canadian Security Intelligence Service insists that it does not spy on Canadians. Driver had long publicly declared his sympathy for the Daesh cause and, as a result, had been arrested prior to signing a peace bond to secure his release. (…) First of all, Driver was a troubled youth who found popularity among Daesh sympathizers online. He was not a hard-core member of the Daesh evildoers. He had never even been to the Middle East, and the congregation at his local mosque tried to correct his skewed take on the Islamic faith. He did make some sort of bomb, but if the result was that exploding it in his own lap failed to kill him and left the taxi driver largely unhurt, it really wasn't much of a bomb. The intelligence and security services-both Canadian and American in this case (because Canadians don't spy on Canadians)-worked efficiently together. Driver did not get to carry out a terror attack. He was killed before he could even attempt the attack. No one was terrorized by his actions. Yet after Driver's death we were told of all the carnage he "would have" created, therefore making it imperative to impose stricter security measures and better monitoring to keep the public safe. (…) Canada remains very, very safe." Hill Times

*** How much do we really know about the Canadian intelligence community?**
An opinion piece states, "Last year American whistle-blower Edward Snowden proclaimed that Canadian intelligence agencies have the "weakest oversight" in the Western world and compared the Canadian government's Bill C-51 to George W. Bush's post-9-11 *U.S. Patriot Act*. Canada became a surveillance state under the Stephen Harper Conservatives. In 2014, for example, it came to light that the Government Operations Centre was monitoring residents of Newfoundland and Labrador, including Indigenous Peoples, residents of the Island's west coast who opposed fracking, and fishermen who were protesting shrimp quotas. This ongoing problem is further complicated by multiple transnational intelligence sharing

agreements, in place since World War II, that remain largely unknown to the general public. Indeed, the rise of the surveillance state is a global phenomenon that cannot be separated from the rise of the internet. But in Canada, because of the lack of any credible oversight, it has played out in a very specific way. This has everything to do with what the Canadian public knows—and more importantly, *does not know*—about Canadian intelligence agencies. Canada's new and highly invasive so-called anti-terror legislation came into force last year with the support of then-Opposition Leader Justin Trudeau and the Liberal caucus. The Trudeau Liberals knew that in order to win the election they would need to undo—or at least promise to undo—much of the damage done by their predecessors. They would have to address the alienation felt by Canadians from having a government that used national security as an excuse to trade away its citizens' freedom and civil liberties. Unfortunately, they have yet to repeal or even reform Bill C-51, and recent terrorist attacks in Europe, the U.S, and here at home in Canada have provided the perfect backdrop against which to further delay the process. On August 10, for example Aaron Driver, a 24-year-old Canadian citizen who was allegedly plotting a terrorist attack in the southern Ontario town of Strathroy, died in a confrontation with police who were following up on a tip from the FBI." The Independent (2016-08-16)

Trump's jihad against jihad deserves support

An opinion piece states, "It didn't take long for critics of Donald Trump to cry foul when the Republican presidential candidate announced his plans to "temporarily suspend immigration from some of the most dangerous and volatile regions of the world that have a history of exporting (Islamic) terrorism." (...)But Trump is not the first to propose such a policy. A Muslim group in Canada, in the wake of the failed "Toronto 18' terror plot, called for a similar suspension. In 2006, the Muslim Canadian Congress (MCC) suggested to Prime Minister Stephen Harper that he suspend immigration from Pakistan, Saudi Arabia, Iran and Somalia, until Canadians officials did thorough security checks of prospective immigrants from these countries. Unknown to many is the fact that security checks of wouldbe immigrants to Canada are not done solely by Canadian (or U.S.) officials, but also rely on information from foreign security agencies that may themselves be infiltrated by terrorist sympathizers. In 2015, I was invited to make a submission to Canada's Senate committee studying the rise of Islamic radicalism. As part of my submission, I suggested a plan akin to what Trump has proposed. I testified that, "We (should) suspend immigration from Somalia, Iran, Pakistan and Saudi Arabia until we are assured that the men and women coming here are committed not to the Muslim Brotherhood, al-Shabaab, Hamas, Hezbollah, and Jamaat-e-Islami, but to a separation of religion and state, gender equality, liberal democracy.'" Toronto Sun, A17 (Ottawa Sun, Edmonton Sun, Calgary Sun)

'Rising threat'

A letter to the editor states, "Not only is there no national deradicalization plan to deal with radical Islamists, the Trudeau Liberals are sending mixed messages. From naively saying we are not at war with the Islamic State of Iraq and the Levant - even though this murderous group has called Canada a legitimate target and claimed last week's thwarted terrorist as its operative - to still planning to remove several provisions from Bill C-51, this government has a disjointed approach to tackling this rising threat. We cannot count on our ability to deradicalize individuals, or on the ability of the RCMP and CSIS to stop future attacks on our soil. Without the timely intelligence from the FBI, we could have had more Canadian casualties last week." National Post, A7

Arrest The Terrorists

A letter to the editor states, "Our prime minister needs to pull his head out the sand. Like his father before him, he needs to re-introduce the War Measures Act so potential terrorists can be arrested and locked up without being charged before more innocent people are injured or killed here in Canada. A wise person who once said "those that fail to learn from history are doomed to repeat it," wasn't far off with what is occurring in the world today. We can't afford to sit on the sidelines any longer." Ottawa Sun, A18

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Privacy and border phone search

Several thorny questions still haven't been answered in the case of a Quebec man who refused to give border officers his cellphone pass code, say privacy and technology lawyers. Alain Philippon had said he would fight a charge of obstructing border officials but pleaded guilty Monday in Dartmouth, N.S., and was fined $500. He was charged when he refused to unlock his cellphone in March 2015 after flying to Halifax from the Dominican Republic. (...)Smartphones typically contain reams of data that go far beyond what could be physically carried in hard copy in any piece of luggage as now defined under an outmoded Customs Act, he said. "I totally understand the law enforcement desire to search devices under certain circumstances. "But what I'm most interested in would be a judge saying, under the Charter of Rights and Freedoms, where that line is and what the proper procedures are." Rob Currie, director of the Law and Technology Institute at the Schulich School of Law at Dalhousie University, said the case highlights legal and regulatory gaps. "The powers that the Canada Border Services Agency have under the act - both to search your things and to make you open them - really only apply to luggage, and also things that you import," he said in an interview. "The Supreme Court of Canada has been quite clear that our electronic devices are not comparable to luggage." (...) There has so far been no constitutional challenge, however, that would clarify what's expected at border crossings. (...) Still, the border agency has been clear that it believes its officers have the authority to search cellphones, Currie said. "The CBSA feels that it has the authority to search your electronic device and they've shown that they will indeed charge you with hindering or preventing customs officers from doing their jobs if you don't unlock the device when you are asked to." Canadian Press (Waterloo Region Record, A3, Hamilton Spectator, Chronicle Herald, Cape Breton Post, Global News, Sudbury.com, Times and Transcripts); *La Presse Canadienne (L'actualité)

Texans hiding guns learn that the fines for firearms can be big in New Brunswick

Vacation trips to Canada for two Texas men ended in provincial court on Tuesday because they lied about guns at the border. Than Jeffrey Do, 56, of Murphy, Texas., pleaded guilty to denying that he had weapons on board when he and his wife Van Bich Pham pulled up to the primary inspection booth at the Canadian end of the Ferry Point Bridge in St. Stephen at about 9:30 a.m. on Saturday. The officers conducting the secondary inspection found three handguns, a shot gun and pepper spray in their camper trailer, federal Crown prosecutor Peter Thorn related in court. Do, a retired engineer, intended to travel across Canada and the United States, defence counsel Rod Macdonald said. He noted that, in Texas, his client could have worn these guns publicly strapped to his waist. They brought the guns for personal protection, the lawyer said. Judge Henrik Tonning agreed, but said that Canada has strict gun laws. He said that this couple could have saved legal trouble by simply answering truthfully when the Canadian border agent asked if they had weapons on board. Tonning fined him $1,700 on top of the $3,500 civil penalty levied by the Canada Border Services Agency for the return of their vehicle. The Crown withdrew charges against Pham. Lloyd Norman Chaffin, 57, Aurora, Texas, failed to declare a 40-calibre Glock handgun at the same bridge in St Stephen at about 2 p.m. on Sunday. Telegraph-Journal, B6

Abbotsford police warn of immigration phone scam

Abbotsford police are warning the public about a phone fraudster who appears to be targeting the South Asian community. Const. Ian MacDonald says the scam artist presents himself as a police officer and uses caller ID 'spoofing' to display the APD phone number. The suspect then suggests the victim has immigration issues, and requests personal and family information - and eventually looks for payment. "The cash could take the form of a wire transfer, it could be a breach of your credit card information, or they might even try to compel you to buy gift cards for them," MacDonald said. MacDonald says there have been similar scams where a caller poses as a Canada Revenue Agency officer. "They prey on people who might be vulnerable, in the sense that they might be immigrants to Canada - new and old - and suggests that they could be deported or they could be in trouble with Immigration Canada," MacDonald said. Four complaints in one day. MacDonald says police received four complaints on Monday. The victim who picked up the call said a man identified himself as "Steve Miller" and told the victim the family failed to fill out proper paper work when they immigrated to Canada several years ago. The fraudster also threatened deportation if the person didn't co-operate in answering questions about the names and birth dates of family members. CBC News (2016-08-16); Postmedia Network (Province, A8, Vancouver Sun)

* **Revocation of airport-security clearance was unfair**

A government decision that stripped a woman of her airport-security clearance and put her out of work more than two years ago was unfair, incomprehensible and unreasonable, a Federal Court judge has ruled. In ordering the minister of transport to take another look at the case, Judge Susan Elliott slammed the government for treating Ayaan Farah in a shoddy fashion. The advisory group that recommended revoking the clearance did not carefully review documents, Elliott said in her written decision, while the director general of aviation security failed to "ensure the critical facts upon which she relies are very clear." Elliott quashed the revocation, saying the government had hidden behind the Privacy Act and failed Farah badly - especially in light of the "gravity of the consequences" to her. Farah expressed delight with the ruling, saying she hopes it will help others caught in a similar situation. Canadian Press (Times Colonist. A8)

*** Canada Should Not Follow Europe's Example In Taxing Online Purchases**

There has been some debate in Canada recently over the issue of sales taxes when making purchases on the Internet from abroad. Right now, when Canadians buy products and services, such as clothes or movie streaming subscriptions, from online vendors located abroad, it is the consumers who are responsible for declaring sales taxes. Very few do so, however, or are even aware that they are supposed to. To remedy this fiscal gap, the Canadian Border Services Agency filters packages, applying taxes and an extra handling fee, but many packages get through untaxed. Beyond this fiscal gap, Canadian sales taxes, both federal and provincial, give foreign vendors an advantage over Canadian retailers. However, the search for an alternative to current policies should not neglect consumers' interests. Huffington Post (2016-08-16)

Immigration detention reform a chance to lead

An opinion piece by Madeline Ashby states, "The government of Canada has announced an investment of up to $138 million in a "better, fairer immigration detention system for the humane and dignified treatment of individuals." It has been a long time coming. According to the Canadian Council for Refugees, Canada is one of the few nations that still detains immigrants, refugees, foreign nationals and permanent residents alongside convicted criminals in prisons. Those in detention, including minors, can wait for the Canada Border Services Agency to review their cases alongside people already convicted of a violent crime like murder, rape, assault or armed robbery. (…) But let's think bigger: in what ways can the CBSA and the Canadian government as a whole change immigration detention itself? Since the 9/11 attacks, immigration norms have taken on an antiterrorist flavour. According the Global Detention Project, the Immigration and Refugee Protection Act (passed in 2001) pulls focus away. (…) Since 2002, the laws regarding immigrants and refugees have grown more strict and more punitive: The 2012 Protecting Canada's Immigration System Act allowed deportations of refugees seeking asylum on humanitarian grounds and cut offany avenues of appeal to the Immigration and Refugee Board for those refugees who had already been rejected. It also mandated biometric identification procedures for those applying for a Canadian visa. The legislation drew criticism from Human Rights Watch, Amnesty International and the Canadian Civil Liberties Association." Postmedia Network (Kingston Whig-Standard, A4, Ottawa Citizen, London Free Press)

Now serving cups of Discontent

An opinion piece states, ' Peter O'Neil's article on our labour shortage and the supposed need for temporary foreign workers fails to address a crucially important point. The Trudeau government has now set our annual intake of immigrants at the absurdly high level of 300,000. This figure is unjustifiable, but surely in this human tsunami there should be enough workers to meet our labour needs three times over. Isn't that what immigration is supposed to be for? If this isn't the case, then not only are we bringing in far too many immigrants, we're bringing in the wrong kind." Vancouver Sun , A11

Le gouvernement contrevient à ses propres règles

Une article d'opinion mentionne, « Lettre adressée au premier ministre du Canada, Justin Trudeau. Monsieur le premier ministre, Depuis quelques années, un de vos ministères ne respecte pas les règles au niveau de l'importation des produits laitiers au Canada en laissant passer à sa frontière du lait diafiltré. Il contrevient donc à une règle canadienne très simple à faire respecter. Il n'est pas normal que dans une agence, le lait ne soit pas du lait et soit dédouané, et que pour une autre agence canadienne, le lait redevienne du lait! L'agriculture en général au Canada, mais particulièrement la

production laitière au Québec, est souvent le principal levier économique de nos régions. Depuis la baisse du prix du lait payé aux agriculteurs, causée par l'importation illégale de lait diafiltré, plusieurs d'entre eux ont décidé de reporter des projets ou même de les abandonner. » Le Nouvelliste (La Presse)

Out of touch and out of gas: where are post-Harper Conservatives headed?
An opinion piece states, -"I always thought Preston Manning was done as champion of the restive western-driven Reform party the day he changed his mind and decided to move into Stornoway, the official opposition leader's residence. (…) Tony Clement has lots of government experience and is the only remaining big-name Mike Harris acolyte among those who jumped to Ottawa from Ontario in 2006. But Tony isn't exactly lighting up the scoreboard. Beyond his social media expertise, he brings little that is new or compelling to the race. And his credibility as a fiscal hawk went south after he secretly shifted $50 million in border infrastructure money to his Muskoka region for a lavish G8 spending spree on a gazebo, public washrooms, and other facilities." Hill Times

* **US Customs and Border Protection hosts Trade Day in Detroit**
The U.S. Customs and Border Protection's Detroit Field Office is hosting its 5th annual Trade Day. The event takes place Wednesday at the Patrick V. McNamara Building in Detroit. Those involved in Trade Day say that it offers the chance for U.S. and Canadian importers, brokers and other trade groups to network with officials from the U.S. and Canada. Participants include Immigration and Customs Enforcement, the U.S. Department of Agriculture, the U.S. Fish and Wildlife Service, the Consumer Product Safety Commission, the Environmental Protection Agency and the U.S. Patent and Trademark Office. Others include the U.S. Food and Drug Administration, the Canadian Border Services Agency and the Canadian Food Inspection Service. Click on Detroit

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Nil

LAW ENFORCEMENT / APPLICATION DE LA LOI

* **Police chiefs want access to passwords**
Canada's police chiefs want a new law that would force people to hand over their electronic passwords with a judge's consent. The Canadian Association of Chiefs of Police has passed a resolution calling for the legal measure to unlock digital evidence, saying criminals increasingly use encryption to hide illicit activities. There is nothing currently in Canadian law that would compel someone to provide a password to police during an investigation, RCMP Assistant Commissioner Joe Oliver told a news conference Tuesday. Oliver said criminals - from child abusers to mobsters - are operating online in almost complete anonymity with the help of tools that mask identities and messages, a phenomenon police call "going dark." "The victims in the digital space are real," Oliver said. "Canada's law and policing capabilities must keep pace with the evolution of technology." The chiefs' proposed password scheme is "wildly disproportionate," because in the case of a laptop computer it would mean handing over the "key to your whole personal life," said David Christopher, a spokesman for OpenMedia, a group that works to keep the Internet surveillance-free. "On the face of it, this seems like it's clearly unconstitutional." The police chiefs' resolution comes as the federal government begins a consultation on cybersecurity that will look at issues including the best way to balance online freedoms with the needs of police. The consultation runs until Oct. 15. Police demands for access to online communications and the concerns of civil libertarians about privacy rights have created tensions around the globe in recent years. The issue came to fore last year when the U.S. Federal Bureau of Investigation went to court in a bid to crack the password of a terror suspect's iPhone following a mass shooting in San Bernardino, Calif. Canadian Press (Red Deer Advocate, A7, Guardian, Telegram, Chronicle-Herald, Cape Breton Post, Toronto Sun, Hamilton Spectator, Waterloo Region Record, Edmonton Sun, Toronto Star, Edmonton Journal, Leader-Post, Ottawa Citizen, National Post, times & Transcript); Canadian Press (Calgary Sun,A3, Calgary Herald); Presse canadienne (Acadie-Nouvelle, 12, Le Quotidien, La voix de l'est, Le Soleil)

*** Transfert d'armes en Libye**
Le gouvernement fédéral a transmis à la Gendarmerie royale du Canada (GRC) les conclusions d'un rapport de l'Organisation des Nations unies (ONU), qui révèle qu'une entreprise canadienne aurait opéré le transfert illicite de véhicules blindés vers la Libye. En mars, un rapport de l'ONU a avancé que l'entreprise ontarienne Streit aurait transféré en 2012 des véhicules blindés de ses installations des Émirats arabes unis vers la Libye, pourtant sous un embargo commercial qui y interdit la vente d'armements. Selon le comité de l'ONU concernant la Libye, tout transfert de véhicule blindé vers le pays de l'Afrique du Nord devrait être interdit. En 2014, des membres de ce comité ont rencontré des représentants de Streit, qui se sont défendus d'avoir agi illégalement. Or, selon la CBC, qui a eu accès à des avis de livraison et des reçus de vente, l'entreprise canadienne aurait continué de vendre des véhicules blindés à la Libye et au Soudan du Sud après avoir été avertie par l'ONU. Le Devoir, A5

*** King may have been on the move**
Denecho King is believed to have hid in several locations throughout the city prior to being found in a housing unit on Sissons Court Saturday morning, police say. "We can confirm that we suspect he was moving to different locations during the three-day search, thus the police activity that was all over Yellowknife," RCMP civilian member Marie York-Condon stated in an e-mail Tuesday. The force declined an interview request. King, 23, had escaped Wednesday from the North Slave Correctional Centre. He was found in a home on Sissons, an area with multiple rowhouses, by police through "investigational techniques" and tips from the public. Between 25 to 30 RCMP officers were involved at the height of the search, police have stated. "We followed up on any and all sightings reported around the city, and followed the investigational leads," York-Condon stated. "Ultimately, this led us to King at the residence where he was apprehended." RCMP officers were going door to door around 8 a.m., Sissons Court resident Leroy Mantla said. Police confirmed King was in a unit and a crisis negotiator established contact with the occupants. How many people were inside remains unclear. By 9 a.m., officers with weapons drawn could be seen around the buildings as more officers arrived. About 30 minutes later, an officer began giving instructions to King over a loudspeaker. After about 30 minutes more, King left the unit through the front door and was led away in handcuffs to a waiting police truck. "Through the hard work and professional conduct of our RCMP members, we were able to bring this search to a successful conclusion without incident," Yellowknife RCMP detachment commander Insp. Matt Peggs stated in a news release. Northern News; Yellowknifer; Yellowknifer

*** Revocation of airport-security clearance was unfair**
A government decision that stripped a woman of her airport-security clearance and put her out of work more than two years ago was unfair, incomprehensible and unreasonable, a Federal Court judge has ruled. In ordering the minister of transport to take another look at the case, Judge Susan Elliott slammed the government for treating Ayaan Farah in a shoddy fashion. The advisory group that recommended revoking the clearance did not carefully review documents, Elliott said in her written decision, while the director general of aviation security failed to "ensure the critical facts upon which she relies are very clear." Elliott quashed the revocation, saying the government had hidden behind the Privacy Act and failed Farah badly - especially in light of the "gravity of the consequences" to her. Farah expressed delight with the ruling, saying she hopes it will help others caught in a similar situation. "I hope this brings light to the fact that Transport Canada needs to do a better job regarding security-clearance decisions - cancelling people's clearance," Farah said in an interview Tuesday. "Transport Canada needs to change its policy." In April 2014, Transport Canada told Farah the RCMP had reported her having contact with criminals only identified as subjects A, B, and C. Police claimed that two of the individuals used Farah's car to go to a funeral for a known gang member - although she was not in the car and did not attend the service. RCMP also said police interacted with her while she was in A's company, but she said she had no memory of being stopped by police. She also said she did not know who the criminals were, although her lawyer suggested one might have been her brother. Canadian Press (Times Colonist, A8, Chronicle-Herald, Kingston Whig-Standard, Waterloo Region Record, Leader-Post, Ottawa Citizen, Calgary Herald)

Mario Harel s'affaire déjà à la tâche
Le directeur du Service de police de la Ville de Gatineau, Mario Harel, est devenu le «chef des chefs» de police, d'un océan à l'autre. A peine 24 heures après son élection unanime à la tête de l'Association canadienne des chefs de police (ACCP), M. Harel s'est prononcé mardi sur les enjeux qui marqueront

son mandat de deux ans, se réjouissant au passage de l'oreille attentive du nouveau gouvernement fédéral. M. Harel est passé de vice-président à numéro un de l'organisme représentant plus de 1000 membres, lors du congrès de l'ACCP, qui se termine à Ottawa ce mercredi. Il compte profiter de son siège pour marquer des points sur la colline parlementaire. «Avec l'arrivée du nouveau gouvernement, dit M. Harel, il y a un dialogue avec l'ensemble des décideurs qui touchent la sécurité publique. (Le gouvernement) écoute nos enjeux et on écoute ceux du gouvernement. Il y a une bonne communication avec les autorités. On sent qu'il y a une écoute et on sent un désir d'améliorer le cadre législatif dans le but d'améliorer la sécurité publique.» M. Harel sera président lorsque le gouvernement Trudeau légalisera la marijuana, l'an prochain. Ce dossier fait partie des préoccupations à court terme de l'ACCP. Le Droit, 5

*** Rift between Muslims and police deepens**

An opinion piece by Amira Elghawaby, the communications director at the National Council of Canadian Muslims, states, "The past few weeks have deeply shaken whatever trust exists between Canadian Muslim communities and law enforcement agencies. First, news and video footage of the heartbreaking and unjustifiable death of a mentally ill Canadian-Somali man in Ottawa as a result of a police intervention. Then, a B.C. Supreme Court judge ruled that the RCMP were the key architects of a terrorism plot that was used to entrap two marginalized individuals who had recently converted to Islam. Both of these cases have spotlighted some troubling excesses in our country's security establishments. They further underscore the need for Canadians to continually question the unequal power balances in our society that can and do sometimes lead to violations of the human rights and dignity of fellow community members. (...) "We need a fundamental and transformative cultural change to policing attitudes and practices," argued criminology professor and policing expert Darryl Davies in a recent Ottawa Life Magazine article. The same conclusion might be drawn from the RCMP's role in manufacturing a terrorist plot, which points to deep flaws in how security agencies operate. Justice Catherine Bruce's ruling in the case against John Nuttall and Amanda Korody should serve as a wake-up call for our elected leaders. "There must be a balance between the need to protect the public from crime and what is tolerable police conduct in a free and democratic society," wrote Justice Bruce. There is clearly an urgent need for adequate checks, balances, and oversight of those who hold incredible power and authority. With the federal government's current consultations on the Anti-terrorism Act, the time for Canada to properly balance civil liberties with public safety is now. Trust is fundamental to our collective well-being. We need more of it, not less. As the authors of a 2016 Kanishka research study of Canadian Muslim concerns around counterterrorism policies discovered in their interviews, citizens are losing faith in the state." Toronto Star, A13

*** Fighting crime in the digital age**

An opinion piece states, "This week, top police officials from coast to coast have descended on our nation's capital for the 111th annual Canadian Association of Chiefs of Police conference. The topic that will shape their discussion, Public Safety in a Digital Age: Real Victims - Real Crime, is timely, given that we're at an important societal juncture. So much of our daily lives now take place online: our wealth passes through jurisdictions in the form of ones and zeros; the most intimate details of our lives, whether they are held by government or industry, rest on servers located somewhere around the globe; and our critical infrastructure, whether it is managed by the public or private sector, is operated digitally. Given the recent media coverage of data breaches and many people's personal experiences with fraudulent phishing schemes, it's understandable that we, as consumers and citizens, want to erect the highest walls possible around our valuable digital assets. This is a natural human reaction, but it isn't a realistic societal response, given the magnitude of our online world." National Post, A8

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Contraband search done, prison back to normal operations

The lockdown at Dorchester Penitentiary's medium-security unit has now ended, prison management announced on Tuesday. On Aug. 11, at about 11:30 a.m., a lockdown was put in place at Dorchester to enable staff members to conduct a search for contraband items, to ensure the safety and security of the

institution, its staff and inmates. As of Tuesday, the institution returned to normal operations and visits to the institution have resumed. Times & Transcript, A7

Court to consider convicted bomber's appeal next month
In less than a month, the financial advisor convicted of setting a bomb on the doorstep and ultimately killing a former client will have his appeal heard. Brian Andrew Malley, 59, of Innisfail will go before the Calgary Court of Appeal on Sept. 14. He was convicted of first-degree murder on Feb. 24, 2014 by a jury and sentenced to life in prison, without the possibility of parole for 25 years, by Justice Kirk Sisson. Victoria Shachtay, 23, was killed on Nov. 25, 2011 opening a gift left on her doorstep. The paraplegic single mother opened the gift disguised as a bomb, it went off and killed her instantly. (...)Malley's counsel has maintained throughout the proceedings that investigators had tunnel vision and focused in on Malley without considering other alternatives. After the conviction defence counsel Bob Aloneissi, of Edmonton, said his client was wrongfully convicted and compared it to the convictions of Guy Paul Morin and David Milgaard. Red Deer Advocate, A1

Forcillo appeal up next
Const. James Forcillo's police disciplinary hearing will begin after his appeal for the attempted murder of Sammy Yatim is finished. Forcillo is suspended with pay and on bail pending appeal of his conviction and six-year prison sentence. (...)A judge sentenced him to six years in jail. Forcillo was granted bail pending appeal of the conviction and sentence. Toronto Sun, A5 (Ottawa Sun, Winnipeg Sun, Calgary Sun, Edmonton Sun)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Deux fois plus de crimes contre des groupes religieux
Graffitis nazis sur une synagogue, tête de porc devant une mosquée, homosexuels agressés : plus de 250 crimes haineux ont été commis au Québec en 2014, dont près d'une centaine à Montréal. En un an, les crimes ciblant un groupe religieux ont doublé dans la province. Les communautés juive et musulmane sont préoccupées par le phénomène, mais n'observent pas de flambée sur le terrain. Le nombre de crimes haineux perpétrés au Québec était relativement stable dans les dernières années, et même en baisse au Canada. Or, 257 délits haineux ont été rapportés en 2014, un bond de 39 % par rapport à l'année précédente, a révélé le ministère de la Sécurité publique (MSP) dans un volumineux document rendu public lors de l'étude des crédits, en avril dernier. Depuis 2010, il n'y avait jamais eu plus de 200 crimes haineux pendant une année. Cette récente augmentation est « majoritairement attribuable à la hausse des délits motivés par la haine contre certaines religions », selon le MSP. En effet, ces crimes ont doublé entre 2013 et 2014 (48 contre 94). D'autre part, 80 crimes étaient guidés par la haine contre la « race ou l'ethnie » et 27 par l'orientation sexuelle de la personne. Le Ministère prévient toutefois qu'une « grande prudence est de mise dans l'interprétation des données [_] considérant qu'il est parfois complexe d'établir le caractère haineux d'un délit ». Les données de 2015 n'ont pas été compilées. À Montréal, 113 crimes haineux ont été répertoriés l'an dernier, une hausse de 24 % en un an. Pourtant, au moment de présenter la nouvelle escouade vouée aux crimes et incidents haineux, en mai dernier, le chef Philippe Pichet évoquait plutôt une moyenne d'environ 70 crimes haineux chaque année dans la métropole. Il avait aussi spécifié que le phénomène n'était pas en hausse. La Presse+

Les verdicts de non-responsabilité criminelle en légère baisse au Canada
Alors que Richard Henry Bain connaîtra bientôt son verdict, certains se demandent si le tireur de la soirée électorale québécoise de 2012 ajoutera son nom à la liste de ceux qui ont invoqué avec succès la défense de non-responsabilité criminelle pour cause de troubles mentaux. Si les procès lors desquels ce moyen de défense a été invoqué font souvent beaucoup parler et remplissent les pages des journaux, le nombre de causes où un tel verdict est rendu demeure stable et est même légèrement en baisse ces trois dernières années au pays, selon de récentes données de Statistique Canada. Il s'agit d'une «faible proportion» du total des causes criminelles au pays, ajoute l'agence fédérale. Selon ses données, 230 verdicts de non-responsabilité criminelle pour cause de troubles mentaux ont été rendus au Canada lors de la dernière année compilée par l'agence fédérale, soit 2013-2014, sur un total de 295 116 affaires

criminelles. Elle a donc été utilisée avec succès par les accusés dans moins d'un pour cent des causes criminelles, note Statistique Canada. Moins de 0,08 pour cent, pour être plus précis. Il est toutefois important de noter que les chiffres du Québec ne sont pas inclus dans l'étude de Statistique Canada, qui a compilé les données de 2005-2006 à 2011-2012, puis jusqu'à 2013-2014 à la demande de La Presse canadienne, qui vient d'obtenir la mise à jour. Le ministère de la Justice du Québec ne recense pas ces données, pas plus que l'Institut de la statistique du Québec. (...)C'est toutefois au Québec que deux des causes hautement médiatisées sur ce type de verdict se sont déroulées, soit les affaires Guy Turcotte et Luka Rocco Magnotta. Presse canadienne (Le Quotidien, 14, Le Droit, Le Soleil)

*** Poll finds Moncton third-safest Canadian city**
A national survey focusing on which cities Canadians consider safe and unsafe has produced some flattering results for New Brunswick. Although Fredericton wasn't included in the just released Mainstreet/Postmedia poll of 4,231 Canadians, much can be interpreted from the results, David Valentin, executive vice-president of Mainstreet Research, said Tuesday. Moncton ranked third nationally and was considered safe by 63 per cent of respondents. I think if we had asked about Fredericton, we would probably have gotten a very similar score to Moncton," Valentin said in an interview. Charlottetown ranked second and St. John's, N.L., fourth in the survey and were considered safe by 68 per cent and 58 per cent of respondents from across Canada. Halifax, ranked seventh, was perceived safe by a majority at 53 per cent. Only Ottawa was considered safe by more people at 72 per cent. Daily Gleaner, A5

*** John Howard Society exec director downplays poll results**
The perception that Winnipeg is Canada's unsafest city is simply wrong, asserted the executive director of the John Howard Society of Manitoba. "I don't care what people in Vancouver and Toronto think," John Hutton said Tuesday. "It's more important what we think in Winnipeg." Hutton was responding to a Mainstreet Research/Postmedia poll that shows that 56% of Canadians surveyed consider the Manitoba capital unsafe. "It 's certainly not as dangerous as Vancouver, Regina or Saskatoon - and I pulled that out of that poll," Hutton said. "It's not a perception that's based on reality." The problem is that the perception is partly fuelled by politicians who are always pushing for more police out of fear, Hutton said. Winnipeg Sun, A4; 1; 2; Winnipeg Free Press; 1; CBC News

*** Canadians see city as less safe**
Canadians perceive Calgary to be one of the country's less safe cities, ranking it 10th out of 15 major centres in a new poll. The poll comes after last month's release of Statistics Canada crime stats, which showed a 29% increase in the severity of crime in Calgary. Based on StatsCan's Crime Severity Index, Calgary ranks ninth among the 15 cities covered by the poll (it ranks seventh for overall crime rate, regardless of severity). Winnipeg was seen as Canada's least safe city by poll respondents, followed by Toronto and Montreal. Calgary Sun, A18

*** Les politiques doivent être revues, dit un expert**
Les quatre fusillades survenues en l'espace d'une quinzaine d'heures dimanche à Ottawa devraient inciter les autorités municipales d'Ottawa à bonifier les programmes de prévention pour lutter contre les gangs de rue, croit un professeur en criminologie à l'Université d'Ottawa. «Ottawa peut faire beaucoup plus pour prévenir ce genre de violence», a lancé le professeur Irvin Waller, affirmant notamment que les 400000 $ annuels qu'a budgété la Ville d'Ottawa pour les stratégies de sortie pour les membres de gang, d'aide à l'emploi et de formation sont insuffisants. «C'est un investissement minuscule, a déploré M. Waller. J'ai écouté le maire (Jim Watson) qui a dit qu'il y avait récemment eu le recrutement de 25 policiers additionnels. Je ne crois pas que c'était pour l'escouade antigang. Vingt-cinq policiers de plus, c'est minimum 2,5 millions $. Ce n'est pas une politique de prévention, c'est une politique de réaction». Augmenter le nombre de policiers sans investir davantage dans les programmes de prévention ne règle pas la situation, a-t-il ajouté. Le Droit, 6

*** Forum targets sex slavery**
Police, social service groups and others in the battle against human trafficking emerged from a roundtable discussion in Windsor Tuesday calling for a provincewide task force to fight the growing scourge. Progressive Conservative MPP Laurie Scott from Haliburton-Kawartha Lakes-Brock, who introduced the private member's bill known as Saving the Girl Next Door Act, said there are victims in

virtually every city, neighbourhood and high school. "This is one of the largest growing crimes in Ontario, Canada and globally," said Scott, who travelled to Windsor for the discussion. "We have to recognize it's happening in our neighbourhoods and we have to help our children from these horrific situations." Windsor police hosted the roundtable, which brought together officers, community organizations and others with a stake in the fight against human trafficking. Scott, whose Bill 158 has passed second reading, said more than 90 per cent of victims in this country are Canadian-born. Scott added that Ontario has been designated as a hub for human trafficking in Canada, with 65 per cent of all cases occurring in the province. Windsor Star, A3

*** Human trafficking survivor lured by gifts, fake affection**
Human trafficking survivor Caroline Pugh-Roberts of London wants to tell her story with the hope of preventing young women from experiencing the nightmare she lived. "What they [the predators] do is something called 'love bombarding'," explained Pugh-Roberts. "They tend to shower the girl with gifts, designer clothes, nails, make-up, jewellery, take the girls out for meals and get the girls to fall in love with them." Often the girls are young, vulnerable and come from a difficult family background. Pugh-Roberts was 35 and at a vulnerable stage in her life. Her mother, husband and two friends had all died within six months of each other. She said she loved him. But the 'love bombarding' turned into commands to work and help support what he described as "the family." That support meant being forced to work as a stripper in various clubs along the 401 highway corridor in southwestern Ontario. Sometimes, she made extra money from prostitution. He kept all of the money she made over the eight years she was with him. (...)Pugh-Roberts entered counselling and received help for seven years. Now, when she is not speaking to high school students or helping other women escape from from trafficking, she's at school, entering her final year studying social services. CBC News

*** Ontario on right path in fighting human trafficking**
An opinion piece by Tracy MacCharles, Ontario's Minister responsible for Women's Issues, states, "Human trafficking is a deplorable activity that robs the safety, livelihood and dignity of those being exploited and abused. Our government is aware of the devastating effects that human trafficking can have on individuals, families and communities across Ontario, and is deeply committed to protecting and supporting survivors. That is why our government brought forward a comprehensive strategy to end human trafficking in Ontario in June, with dedicated funding of up to $72 million to fight back against this heinous crime. We have clearly heard from those on the front lines of this issue, and have incorporated their feedback into an approach that we believe to be truly responsive to needs on the ground. Our approach is a survivor-centred approach, one that both provides sustained and meaningful supports for survivors but also gives police, intelligence services and the justice sector the resources they require to combat and prosecute traffickers. These are long-term, sustainable solutions aimed to end human trafficking in Ontario. However, such solutions don't happen overnight. Work is set to begin on a number of the initiatives below: The development of an anti-human trafficking co-ordination office to help collaboration across law enforcement, justice, social, health, education, and the child welfare sectors. Establishing a provincial human trafficking prosecution team, composed of a provincial coordinator and specialized, trained Crowns to effectively prosecute human trafficking cases and ensure consistency across the province. The creation of an anti-human trafficking intelligence team in the Criminal Intelligence Service Ontario (CISO). The team will include a provincial human trafficking intelligence co-ordinator, an intelligence training co-ordinator and an intelligence analyst." Waterloo Region Record, A8

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

MMIW Red Dress Campaign heading to Prince George
There will be empty red dresses hanging in parts of the city on October 2nd, honouring missing and murdered indigenous women. Local organizer Tammy Meise saw the Red Dress display while in Vancouver in 2014. She wants to give a voice back to local women who've gone missing, especially one. "One of my childhood best friends, Kari Anne Gordon, she was murdered and she has become a statistic. When I saw the red dress project it impacted me, it literally took my breath away ... us that are mothers,

that are sisters, that are daughters, that are aunties, have family and friends that have gone missing. When you actually talk to people and start making connections, it's actually amazing how it affects so many people." Meise presented the event to Council on Monday night. Councillors unanimously supported the event and met her request of waiving the Lheidli T'enneh Memorial Park liability costs and covering the Park rental fees. Council also gave Meise permission to hold a candlelit vigil at the Park that night and many, including Councillor Terri McConnachie, promised to be there. My Prince George Now (2016-08-16)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Liberals failing Canadians on marijuana reform
An opinion piece states, "The Liberal government does not seem to be taking too seriously its promise to regulate and legalize marijuana. Sure, the federal party is looking at ways to reform obsolete and arguably draconian drug laws. After all, a permanent criminal record and jail time is rather heavy handed for a non-violent act and use of a substance that indigenous cultures around the world have used for millennia. But as authorities are still throwing the proverbial book at Canadians whose only "crime" was being in possession of a substance that the government is working to legalize, lives continue to be ruined. This might not seem like a serious issue to some voters, many of whom were outright dismissive about it before, during and since the election, but it should be a concern to every Canadian." Sundre Roundup (2016-08-16)

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Workers plan protest to crank up pressure on Foote to fix Phoenix**
The giant Public Service Alliance of Canada is cranking up the pressure on Public Services Minister Judy Foote to fix the troubled Phoenix pay system by staging a public protest by workers in her home province. Employee frustration over the malfunctioning pay system has escalated in recent weeks as new cases of public servants being unpaid, overpaid or not paid at all keep cropping up, but Thursday's planned demonstration is the first political action against the Liberals since PSAC first sounded the alarm about the massive project more than a year ago. The rally will be held at Harbourside Park in St John's NL, drawing public servants from federal offices there as well as from Quebec, Nova Scotia and New Brunswick. Until now, the unions have been working with senior bureaucrats at Treasury Board and Public Services and Procurement Canada to try and resolve mushrooming pay problems caused by Phoenix which appear to be getting more complicated. It also comes the day before Foote is expected to have her first face-to-face meeting with PSAC President Robyn Benson and Debi Daviau, president of the Professional Institute of the Public Service of Canada. Unions have complained that Foote has dodged responsibility for the fiasco and let her senior bureaucrats take the heat. She didn't appear as a witness at the government operations committee meeting that was hastily called last month to discuss Phoenix. John MacLennan, president of the Union of National Defence Employees whose members are among the hardest hit by Phoenix foulups, said public servants want more urgent action. He said workers feel the Oct. 31 deadline Foote's department promised to clear the backlog is too far away. Postmedia Network (Ottawa Citizen, Ottawa Sun)

OTHER / AUTRE

Nil

INTERNATIONAL

*** Security concerns prompt backpack ban at Oktoberfest in Munich**

Munich city officials say they're banning backpacks from this year's Oktoberfest and plan to erect a fence in an effort to increase security after recent attacks rattled Germany. Deputy mayor Josef Schmid said Wednesday that bags of more than 3 litres (0.8 gallons) in capacity won't be allowed into the annual beer celebration, which runs Sept. 17-Oct. 3. The number of security staff also will be increased. Schmid said a 350-meter (380-yard) fence will be put up to secure a previously open entrance to the festival grounds. Bavaria was shaken last month by three attacks in a week. Two were carried out by asylum-seekers and claimed by the Islamic State group. Only the attackers were killed. Unrelatedly, a teenager killed nine people in a shooting rampage in Munich. Associated Press (Global News)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
September 7, 2016 / le 7 septembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

U of S leads major water project
A new $143.7-million water research program could have "vast" economic benefits for Saskatchewan by allowing scientists to predict and citizens to prepare for floods, droughts and towering summer storms, according to its associate director. "If we go back in history, every civilization has been built upon its ability to manage its water successfully, and when civilizations have collapsed, it's because they failed to do so," University of Saskatchewan hydrologist John Pomeroy told reporters. (…) **Public Safety and Emergency Preparedness Minister Ralph Goodale** - whose arrival at the announcement was ironically delayed by fog - said severe weather driven by climate change means research into water and weather systems is crucial. ***"The damages that we will save by better controlling the water flow and the profit that we can make in a more diversified agricultural sector, the payback will dwarf the initial investment (and) return it to Saskatchewan, to Canada many, times over,"*** he said. Since its launch, CFREF has handed out 13 grants, of which two have gone to the U of S. The first, a $37.2 million

package announced last month, will fund the university's new Designing Crops for Global Food Security program. Postmedia Network (Starphoenix, A1, Leader-Post)

Universities take lead on flooding research
Southern Alberta's 2013 flood - which claimed five lives and caused billions of dollars in damage - has prompted researchers to launch the largest university led water project in the world. On Tuesday morning, the federal government announced the Global Water Futures: Solutions to Water Threats in an Era of Global Climate Change initiative in Saskatoon. (…) The project will position Canada ***"as a global hub for leading-edge, user-driven water science for the world's cold regions,"*** **Ralph Goodale**, **minister of public safety and emergency preparedness**, said in a news release. Postmedia Network (Edmonton Journal, A12, Calgary Herald); 650 CKOM (2016-09-06)

Time to talk about electoral reform across the country
It must be important: two meetings in Regina across only five days on how to overhaul the way we Canadians elect our House of Commons. The meetings were requested by the federal Liberals, who, during last autumn's election campaign, pledged the 2015 federal election would be the last one using the familiar first-past-the-post system. (…) Weir was first out of the organizational gate back in June when he began planning a local meeting, but he complained last week that neither of the two other MPs representing the Regina area - Liberal **Ralph Goodale** and Conservative Andrew Scheer - would attend it. **Goodale, the federal public safety and emergency preparedness minister**, cited a busy schedule and conflicts with his work as a minister. Weir claimed **Goodale** indicated he'd be available only on the two days when Weir was expected to be in a national NDP caucus meeting. Postmedia Network (Starphoenix, A4, Leader-Post)

Ottawa ditches ISIL, will call group Daesh
The federal government will no longer refer to the Islamic State of Iraq and the Levant and will instead call the group by a different, potentially insulting name: Daesh. **Public Safety Minister Ralph Goodale** revealed the change in a report on terrorism released last month, saying ISIL is neither Islamic nor a state and that the report would instead use the group's Arabic acronym. Global Affairs Canada and the Department of National Defence also say they are adopting Daesh to refer to the group. The decision continues a trend that has been sweeping through western governments. France and the United Kingdom are among those that have adopted the term in recent years. But while the term has long been used by Arabic speakers and comes from the group's Arabic acronym, it can also be considered an insult, with some translations meaning to tread underfoot or crush. The group has forbidden use of the term Daesh within its territory. Canadian Press (Times Colonist, A9, Red Deer Advocate, Toronto Sun, Hamilton Spectator, Vancouver Sun, Ottawa Sun, Waterloo Region Record, Edmonton Sun, Montreal Gazette, Ottawa Citizen, National Post, London Free Press, Kingston Whig-Standard, Winnipeg Sun, Calgary Sun, Times Colonist)

TOP STORIES / MANCHETTES

*** Canadian Firearms Institute Offers To Help Americans Bring Guns to Canada**
An open letter from the CEO of the Canadian Firearms Institute states, "Dear American Friends, As a Canadian Firearms owner that has enjoyed the hospitality of your country many, many, times, I'd like to offer an explanation of why our Border guards are asking you to leave your guns at home. After spending years enjoying the company of American shooters, I now think I understand the difference between us with respect to firearms and perhaps why it exists. (…) All of the details of how this can be done can be found on the RCMP Canadian Firearms Program website. The address is: (…). If you need help, or have questions, they are happy to help you through the paperwork." Editors Note: Recently the Canadian Border Services Agency issued a warning in the form of a public awareness campaign to tell Americans not to bring their guns to Canada, after seeing a seven per cent increase in the number of firearms seizures at the boarder. Ammoland (2016-09-06)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Flood sparks global initiative**
Southern Alberta's 2013 flood - which claimed five lives and caused billions of dollars in damage - has prompted researchers to launch the largest universityled water project in the world. On Tuesday morning, the federal government announced the "GlobalWater Futures: Solutions to Water Threats in an Era of Global Climate Change" initiative in Saskatoon. The water research project will be funded with a $77.8-million grant to the University of Saskatchewan. The seven-year program, one of 13 projects being funded Tuesday through a $900 million investment from the Canada First Research Excellence Fund, will grow to $143.7 million with additional money fromother universities and industry partners. Calgary Sun, A12

*** Coast guard fleet deteriorated under Tories and Liberals, report says**
The majority of the Canadian Coast Guard fleet is so old that its book value is almost worthless, says an independent report presented to the Liberal government. A third-party analysis was commissioned by the agency, which has for the last 20 years fallen under the responsibility of the Fisheries Department. A heavily censored copy of the report, which was included in a briefing package for former fisheries minister Hunter Tootoo, was obtained by CBC News under the Access to Information Act. It pulls no punches when it comes to the state of the fleet that performs vital ice-breaking and life-saving search and rescue functions on all three coasts. CBC.ca

*** No summer floodway use to control Winnipeg river levels: report**
The Red River Floodway should not be used during the summer to control water levels in Winnipeg, according to a report commissioned by the former NDP government and made public after the Progressive Conservatives took power. A review of provincial flood-control infrastructure operating guidelines, ordered up by the Selinger government in 2013 and completed in 2015, concludes the floodway should not be used to prevent the Assiniboine riverwalk and other riverbank recreational amenities in Winnipeg from being submerged during the summer. The document, authored by a panel of high-profile consultants, was published with zero fanfare after the Pallister government took power and was made aware of its existence, said a spokesman for Manitoba Infrastructure Minister Blaine Pedersen. CBC.ca

*** Presque toutes les familles ont été indemnisées**
Un montant avoisinant les 114 millions $ a été distribué aux réclamations en cas de décès dans le cadre du Fonds d'indemnisation des victimes de la tragédie ferroviaire du 6 juillet 2013 à Lac-Mégantic. Le 23e rapport du contrôleur déposé à la Cour supérieure en vertu de la Loi sur les arrangements avec les créanciers des compagnies (LACC) révèle que près de la totalité de la somme remise au fiduciaire a été distribuée aux familles des 48 personnes décédées en lien avec les tragiques événements. Le Tribune, 8

*** Canadians stepped up to help lead Ebola fight**
Ottawa's Dr. Mélissa Langevin stepped forward when the federal government and the Red Cross launched an extraordinary recruitment drive in late 2014, asking doctors, nurses and others to "join the fight against Ebola." Langevin, who spent a month working in an Ebola treatment centre in Sierra Leone, was one of 900 Canadians to do so. Ottawa Citizen, A9

*** Major oil spill response improvements planned for B.C.**
The organization responsible for cleaning up oil spills around Vancouver and B.C.'s South Coast has plans for major improvements to its facilities and spill response times - but the $200 million upgrades come with a catch: they won't go ahead if the Kinder Morgan Trans Mountain pipeline expansion project isn't approved. Western Canada Marine Response Corporation (WCMRC) currently has about 17 vessels ready for duty around Vancouver's harbour. The proposed upgrades include a new $10-million spill response base a little west of the Iron Workers Memorial Bridge in Burrard Inlet. CBC.ca

*** B.C. search-and-rescue teams renew call for new funding model**

All over British Columbia, search crews are being pressed for resources as call volumes increase. The provincial government has increased funding for the teams, but many say it's not enough to support B.C.'s 80 search-and-rescue groups. At a press conference Tuesday, BC Premier Christy Clark said the government is aware of the issue. "I think we have the best funded volunteer search and rescue anywhere in the country by a long shot, but we know we need to change the funding model, we need to chance some of the ways that it's run," BC Premier Christy Clark said Tuesday. While some argue people should be charged for the cost of their rescue, search-and-rescue teams have said they do not want go down that path. GlobalNews.ca

* **Sask. woman Sheree Fertuck still missing after 9 months**
It's been nine months since RCMP began investigating the disappearance and suspected homicide of a missing Kenaston, Sask., woman Sheree Fertuck, 51. On Dec. 8, 2015, Fertuck's semi was found abandoned at a gravel pit near Kenaston, about 80 kilometres south of Saskatoon. She was last seen wearing a grey sweater, grey pants, white running shoes and glasses. Since then police said there has been no banking activity, use of her passport or cellular phone. Fertuck also hasn't made contact with any family. She's described as being five-foot-four and 250 pounds, with greying brown hair and blue eyes. CBC.ca

* **Helicopter wreckage pulled from Restigouche River**
The wreckage of a helicopter that crashed on Sunday, killing two and injuring one, was pulled from the Restigouche River at Flatlands near Campbellton early Tuesday afternoon. Federal Transportation Safety Board officials oversaw the operation. Times & Transcript, B1

* **Boat carrying 4 missing fishermen discovered off St. John's harbour**
Officials from the Joint Rescue Coordination Centre (JRCC) in Halifax say a boat carrying four missing fishermen outside St. John's habour has been located by search and rescue crews. According to JRCC, the 6.7-metre open boat was found near their fishing nets. Air efforts were stalled overnight due to poor visibility, but are expected to resume Wednesday morning as weather conditions improve. JRCC said the boat had been overdue since Tuesday. A Cormorant helicopter from Gander, a Hercules aircraft from Greenwood, N.S., several fishing boats and the Royal Newfoundland Constabulary have also been involved in the search. Air searches are expected to resume Wednesday morning. CBC.ca

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Bridge lane closure causes concern about economy, commuting
Windsor's local economy and commuter travel time will feel the pinch if Ambassador Bridge owner Matty Moroun doesn't move quickly to address "safety deficiencies" that have indefinitely closed down a curb lane on the 87-year-old crossing, said local leaders on Tuesday. Transport Canada and federal Transport Minister Marc Garneau announced a section of the bridge will be blocked with concrete barriers near the entrance to Windsor where there is a crumbling sidewalk and rusted-out railings. Due to the shutdown of a traffic lane entering Canada, lineups are expected for both trucks carrying cross-border goods and vehicle traffic that each weekday includes a few thousand commuters travelling across the Windsor-Detroit border. "The sooner we can add capacity at the Windsor-Detroit border the better for business and for trade," said Matt Marchand, CEO for the Windsor-Essex Regional Chamber. "This certainly highlights the need for redundancy and need for the (planned Gordie Howe International Bridge) to move forward in a timely manner. I understand infrastructure and international projects are complex, but the sooner we can add more lanes, the better." It has been estimated up to 25 per cent of the local economy is linked to the movement of cross-border goods and trade, most notably within the auto and agricultural sectors. Windsor Star, A4

*** Accusé à 71 ans d'exportation de marijuana aux États-Unis**
Le doyen d'un «club de l'âge d'or» d'exportateurs québécois de pot ne pourra esquiver la justice américaine, qui risque de l'envoyer finir ses jours en prison. Yvan Chandler, 71 ans, sera jugé dans l'État de New York face à des accusations de complot pour trafic de plus de 1000 kilos de marijuana et pour blanchiment d'argent, vient de trancher la Cour d'appel du Québec. (...)Une dizaine d'autres «old timers » québécois croyant que leur âge n'attirerait pas les soupçons ont été épinglés dans cette enquête. Parmi eux, Monique Storie, une sexagénaire de Saint-Jean-sur-Richelieu, cachait un magot de 212 485 $ US dans des couches pour adultes quand les douaniers du poste frontalier de Champlain ont fouillé sa voiture, en juillet 2010. Journal de Montréal, 23

*** Police blotter**
(...) Kenento Boots, 62, of Akwesasne, was arrested on Sept. 5 at the port of entry. Police alleged Boots was found to be in breach of his conditions while at the port of entry and police were called. Police also alleged Boots kicked a CBSA officer in the leg and refused to provide a breath sample. He was taken into custody and charged with refusing to provide a breath sample, assault and breach of undertaking for operating a vehicle while under the influence of alcohol. He is scheduled to appear in court on Sept. 13. Cornwall Standard-Freeholder (2016-09-06)

*** Interactive Advance Passenger Information Initiative: coming soon**
On September 30 2016 changes relating to the government's collection of information regarding all passengers and crews aboard commercial air carriers destined for Canada will come into effect. Over the past few months the Canada Border Services Agency (CBSA) has been working with the more than 200 foreign air carriers that operate in Canada to transition them to the Interactive Advance Passenger Information Initiative (IAPI). This regime replaces the Advance Passenger Information/Passenger Name Record Programme (API/PNR). Air carriers must provide information to the federal government under two pieces of legislation: the Customs Act and the Immigration and Refugee Protection Act. Regulations setting out the prescribed information have been made under each act, but the information prescribed is the same under both. (...)The Canadian government has stated that the IAPI initiative will "contribute to preventing prescribed persons and improperly documented foreign nationals from reaching Canadian ports of entry, thereby protecting the integrity of Canada's immigration program and enhancing public safety" – a virtual wall of sorts. Interactive systems that allow or require earlier transmission of PNR data are also said to "facilitate faster clearance of international passengers and [to] reduce examination time upon arrival". International Law Office

*** Frustrations et préoccupation sécuritaire**
Le temps d'attente dépasse parfois les deux heures à la douane internationale. Le syndicat des agents frontaliers redoute des failles de sécurité résultant du surnombre de voyageurs. Des milliers de voyageurs ont dû patienter pendant deux heures, voire davantage, hier après-midi, pour franchir la douane internationale de l'aéroport Pierre-Elliott-Trudeau, submergée de vacanciers et d'étudiants étrangers depuis trois semaines. Le « manque chronique » de douaniers est tel que le président du syndicat des agents frontaliers craint qu'on ne puisse « échapper » des personnes suspectes à la frontière. « C'est présentement une de mes craintes qu'on puisse laisser passer des gens dans ce maillon-là parce qu'il y a un manque d'employés et que la pression est très forte », s'inquiète Jean-Pierre Fortin, président national du Syndicat des douanes et de l'immigration. Il craint que les agents frontaliers ne soient tentés d'« aller dans la facilitation » en raison de la grande pression à laquelle ils sont soumis. Le syndicaliste assure néanmoins que ses membres font leur travail méticuleusement, même en période de congestion. (...) Un nombre très important de vols internationaux a atterri à l'aéroport Montréal-Trudeau entre 15 h et 18 h hier, provoquant un déferlement de 6100 personnes à la douane. L'objectif opérationnel de 20 minutes de l'Agence des services frontaliers du Canada (ASFC) a ainsi été dépassé par cet afflux de voyageurs. « Les délais d'attente ont été causés principalement par une convergence de vols internationaux ayant occasionné un temps d'attente de plus de 60 minutes », a indiqué par courriel hier soir Stéphane Malépart, directeur régional adjoint des communications de l'ASFC au Québec. La Presse +; CJAD

*** Encore moins de vols vers les États-Unis**

L'offre de vols vers les États-Unis diminue encore à l'aéroport international Jean-Lesage, cet automne, alors même que l'établissement peaufine son projet de centre de prédédouanement américain. Trois transporteurs ont réduit la cadence vers les États-Unis ou s'apprêtent à le faire. Depuis la fin d'août, Delta Airlines n'offre plus qu'un vol quotidien vers l'aéroport John-F. Kennedy à New York. La construction en cours est évoquée comme raison à court terme. Une demande insuffisante durant la saison creuse constitue toutefois la véritable raison à long terme, indique le porte-parole Anthony Black. United abandonne pour sa part son service annuel vers Chicago pour le rendre saisonnier. Les voyageurs peuvent encore profiter d'un vol par jour d'ici la fin du mois d'octobre, à défaut de quoi il faudra attendre le mois de juin. (…)En mars, les gouvernements canadien et américain sont parvenus à une entente diplomatique sur le prédédouanement qui accorde un centre à Québec. Cela fait plus de 10 ans que l'aéroport de Québec souhaite obtenir cette infrastructure qui devrait coûter autour de 30 millions $. Dans un centre de prédédouanement, les voyageurs en direction des États-Unis ou qui y font escale passent les douanes américaines avant l'embarquement, ce qui réduit l'attente à l'arrivée ou entre deux vols. Le Quotidien, 18 (La Presse, Le Soleil)

New Chinese visa offices could spur more tourism to Canada
The opening of several new offices in China where citizens can apply for visas to visit Canada could be a boon for travel operators in this country, if Chinese tourism surges as a result. Among the deals signed by Prime Minister Justin Trudeau during his state visit to China was an agreement to allow Canada to open seven new visa application centres, in addition to the five already there. Until now, the Chinese government has permitted visa offices only in cities where Canada has an embassy or a consulate. The new offices are expected to open in 2017. With more Chinese people heading out on travels from secondary cities, smoothing the visa application process could sharpen Canada's competitive edge as a travel destination. (…)Rob Taylor, vice-president of the Tourism Industry Association of Canada (TIAC), said that in the long term, the new offices will also help deal with a new technical requirement: After 2018, tourists coming to Canada will have to provide "biometric" data with their visa applications, which might include electronic fingerprints or retinal scans. That can only be done in person, so having more offices will help prevent roadblocks. Canada has become a key destination for Chinese tourists, with close to 500,000 visiting in 2015. Globe and Mail, B5

Province in a better position to accept intake of refugees
The B.C. government and settlement groups are bracing for a new wave of roughly 1,500 government-assisted refugees from the Middle East before the end of this year. Another 750 privately-sponsored newcomers to the region are expected before next spring. That rough estimate of 2,250, provided Tuesday by the Immigrant Services Society of B.C., compares with the more than 3,000 government and privately-sponsored Syrian refugees welcomed to the province since the program began in November of 2015. The national total is slightly over 30,000. Vancouver Sun, A3 (The Province)

Report to EU threatens $200M lobster industry
Federal Fisheries Minister Dominic LeBlanc says Canada will partner with the United States to vigorously oppose any and all efforts to have live American lobsters banned from the European Union. The EU moved a step closer to a ban on Tuesday following a report that says there's enough scientific evidence to proceed with a review of Sweden's request to declare the American lobster an invasive species. (…)Some observers have wondered if the proposed lobster ban is an attempt in Europe to erect a non-tariff barrier to free trade and head off Canadian and U.S. live lobster imports, now worth $200 million annually. "I hope not," LeBlanc said. "We believe a free trade agreement with Europe is in the economic interests of Canada and the EU." Lobstermen in the U.S. and Canada had hoped to stop the proposal before it moved any further. Telegraph-Journal, A1 (Times & Transcript, Daily Gleaner); * Associated Press (Ottawa Citizen, Cape Breton Post)

*** Keep compassion for Syria alive**
An editorial states, "It's been one year since three-year-old Alan Kurdi's lifeless body was lifted from a Turkish beach. The photo of the toddler, one of thousands fleeing the war in Syria, hit the front pages of newspapers around the world and touched a nerve. In Canada amid a federal election campaign, it prompted all political parties to take a hard look at their refugee resettlement promises and see what more they could do. After the Liberals were brought to power, they mounted an exceptional campaign to

resettle thousands of Syrian refugees in Canada. Faith and community groups banded together to raise money and other resources to host refugees in dozens of communities across the country. The UN's refugee agency says that since Alan Kurdi's death, "4,176 people have died or gone missing on the Mediterranean-an average of 11 men, women, and children perishing every single day over the last 12 months." The world, including Canada, must not forget about the Syrian refugees looking for resettlement in safer places. Canada has resettled more than 30,000 Syrian refugees since the Liberals began their campaign last November. But they're still a ways off of meeting their goal of bringing in 25,000 government-assisted refugees by the end of this year. They had brought in just over 19,000 from this category as of Aug. 28. The Canadian Press reported Aug. 29 that the government has learned from the first wave and is preparing to welcome a second influx to meet the end-of-year goal. Let's hope it does." Hill Times

Canadian Firearms Institute Offers To Help Americans Bring Guns to Canada
An open letter from the CEO of the Canadian Firearms Institute states, "Dear American Friends, As a Canadian Firearms owner that has enjoyed the hospitality of your country many, many, times, I'd like to offer an explanation of why our Border guards are asking you to leave your guns at home. After spending years enjoying the company of American shooters, I now think I understand the difference between us with respect to firearms and perhaps why it exists. (…) All of the details of how this can be done can be found on the RCMP Canadian Firearms Program website. The address is (…). If you need help, or have questions, they are happy to help you through the paperwork." Editors Note: Recently the Canadian Border Services Agency issued a warning in the form of a public awareness campaign to tell Americans not to bring their guns to Canada, after seeing a seven per cent increase in the number of firearms seizures at the boarder. Ammoland (2016-09-06)

*** No match for China**
An opinion piece states, "This week, China indicated its interest in a free-trade agreement (FTA) with Canada through the removal of tariffs and some non-tariff barriers. Will Canada be able to respond appropriately? Australia, a country that mirrors Canada in many respects, already has a freetrade agreement with China that began Dec. 20, 2015. The agreement sets out reductions on tariffs on coal, copper alloys, pharmaceuticals, car parts and agriculture goods (dairy, beef, wine and wool) and will ensure free access to the Chinese market for iron ore and energy. There will be greater access for services, like financial industries, telecommunications, tourism and education. A mechanism will be in place to challenge non-tariff barriers and settle investmentstate disputes. Restrictions on foreign direct investment are to be eased, with Australia still screening all investments by Chinese stateowned enterprise (SOE), regardless of their size. Presumably, Canada should learn from Australia's negotiation with China. However, we should not fool ourselves. Gains from free trade may not be sufficient to overcome our discomfort with China's human rights, espionage and environmental practices, subsidies and non-tariff protectionism and other policies aimed at gaining global market share. Even if a good FTA is in the making, it is unclear that Canada has much to offer, given our proximity to the United States and our inability to get key resources to tidewater." National Post, FP9

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Watch How Government Spyware Infects a Computer in This Leaked Demo Video**
Just like any regular tech company, vendors such as Hacking Team or NSO Group, which sell software designed to spy on computers and cellphones, have to convince potential customers that their product is worth the thousands of dollars, or sometimes millions, that it costs. For that, companies often set up controlled live demos, showing the potential buyers, usually police departments and intelligence agencies, how their technology works and just how great their spyware is. Unless you are a police agent, a middleman who resells this type of software, or you've worked in one of these companies, you've probably never seen one of these demos—until today. Motherboard has obtained a never-before-seen 10-minute video showing a live demo for a spyware solution made by a little known Italian surveillance contractor called RCS Lab. Unlike Hacking Team, RCS Lab has been able to fly under the radar for years, and very little is known about its products, or its customers. Motherboard.vice.com

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Canadian Firearms Institute Offers To Help Americans Bring Guns to Canada**
An open letter from the CEO of the Canadian Firearms Institute states, "Dear American Friends, As a Canadian Firearms owner that has enjoyed the hospitality of your country many, many, times, I'd like to offer an explanation of why our Border guards are asking you to leave your guns at home. After spending years enjoying the company of American shooters, I now think I understand the difference between us with respect to firearms and perhaps why it exists. (…) All of the details of how this can be done can be found on the RCMP Canadian Firearms Program website. The address is: (…). If you need help, or have questions, they are happy to help you through the paperwork." Editors Note: Recently the Canadian Border Services Agency issued a warning in the form of a public awareness campaign to tell Americans not to bring their guns to Canada, after seeing a seven per cent increase in the number of firearms seizures at the boarder. Ammoland (2016-09-06)

Edmonton police allow Mill Woods residents to return to homes after bomb investigation
Police said residents of Mill Woods who were forced out of their homes by the potential discovery of an improvised explosive device (IED) Tuesday, were told they could return to their homes shortly after 10 p.m. after officers "concluded investigations of the IED." Police also said two people had been taken into custody in connection with their investigation and that charges were pending. They did not provide details about the suspects or what type of charges might be laid. Earlier in the day, police said officers were evacuating residents within a one-block radius of a home at 20 Avenue and 46 Street while they conducted their investigation. "There was an investigation that brought us to the address today… at approximately 4 p.m. today," said Insp. Gary Godziuk with the Edmonton Police Service. "The search warrant that we were conducting discovered a quantity of improvised explosive devices which needed to be dealt with in a safe and reliable manner." Global News

Charges withdrawn: Teen agrees to peace bond in case involving lyrics and death threats
The Crown has withdrawn death-threat charges against a Cape Breton teenager who posted online a song he wrote that included lyrics suggesting a school shooting "sounds like bliss." The RCMP said the lyrics, written by 18-year-old Nelson Fletcher Rudderham, represented a threat against students and staff at the Inverness Education Centre Academy. His trial was due to begin Tuesday, but the Crown withdrew the charge when the Inverness teenager agreed to sign a peace bond. Defence lawyer Kevin Patriquin said he was happy with the outcome. "I think it's a good resolution. It's one where you know what the outcome is going to be in terms of not having a criminal record, as long as he complies with the terms, and that is one of the most important aspects of it," he said. Under the terms of the 12-month recognizance, Rudderham is required to keep the peace, stay away from the Inverness school, and not own or possess any firearms or explosives. Crown attorney Herman Felderhof told the court he would drop the charge if Rudderham signed a bond, but did not elaborate. He would not comment afterward. Patriquin said the peace bond conditions were all standard, and his client will have no problem complying with the firearms condition, which the Crown wanted because of the perceived threat conveyed in the song. "That was a pretty easy one because Mr. Rudderham doesn't own any firearms anyways," he said. "It's almost a non-issue from his point of view." Canadian Press (Cape Breton Post, A3, Calgary Sun, Times Colonist)

*** Youth who escaped from Dojack centre remains at large**
A youth who escaped from the Paul Dojack Centre last week remains at large, and the province hopes to be granted an extension of a court order that allows for the publication of his name. The youth escaped from the Regina-based youth correctional facility Thursday. The Ministry of Justice received a five-day exemption so it could release the boy's name and photo in hopes of it leading to his apprehension. That exemption expired at midnight Tuesday and the ministry cannot reapply until Wednesday morning. A justice ministry official said last week that the young man - whose age and offences are still protected by a publication ban under federal legislation - was in custody for reasons that were "violent in nature." Names of youth offenders are normally protected under the Youth Criminal Justice Act. Whatever the specific reasons for his custody is, it was enough to prompt the government to seek a rare court order

allowing for his name and photo to be released to the public. A judge agreed there was enough of a threat to public safety to warrant the approval, and allowed the boy's name to be published for five days. The boy is five-foot-11, 145 pounds with a slim build. He has brown eyes and brown hair. Anyone with information about his location is asked to contact local police or the RCMP. Leader-Post, A6

*** La GRC veut mettre la main sur du matériel de l'émission *Enquête***
La GRC tente de forcer Radio-Canada à lui remettre des extraits jamais diffusés d'entrevues réalisées par l'animateur Alain Gravel à l'époque où il travaillait à l'émission Enquête, a appris La Presse. Déjà, la société publique a mobilisé son service juridique pour bloquer la manoeuvre des policiers et protéger ce que son directeur général de l'information décrit comme un «principe sacré»: l'assurance que le matériel amassé par des journalistes servira uniquement à informer le public, pas à compléter par la bande le travail des autorités. Le dossier qui intéresse la GRC est celui de la corruption à l'Agence du revenu du Canada, qui avait fait l'objet d'une fouille approfondie à l'émission Enquête. Plusieurs personnes ont été accusées au criminel dans cette affaire, dont deux intervenants avec qui Alain Gravel avait réalisé des entrevues: Francesco Bertucci, propriétaire de l'entreprise Thomson Tremblay, et Adriano Furgiuele, vérificateur du fisc congédié en 2009. La Presse

Accused reporter awaits ruling: Crown argues journalist sought confrontation with police defence says RCMP exaggerated on stand
A judge will issue a ruling in October on whether a Yellowknifer reporter obstructed police officers last year while taking photos of them searching a van downtown. A three-day trial of John McFadden, 53, ended Friday with Crown prosecutor Annie Piche questioning the reporter followed by closing arguments from Piche and defence lawyer Peter Harte. McFadden was arrested on July 5, 2015 just before 1 a.m. in front of Shoppers Drug Mart on 49 Street after taking 20 photos over 3.5 minutes of four RCMP officers searching a van for ownership information. The van had licence plates reported as stolen in Alberta and police wanted to confirm a drunken man seen climbing into the driver's seat was its owner, according to testimony from officers. The testimony of three RCMP officers formed the basis of the Crown case when the trial began June 22 in territorial court before Judge Garth Malakoe. It had been adjourned after the first day until it resumed Thursday afternoon with cross examination of the last officer to take the stand. Sarah Heaton, a friend of McFadden, testified in his defence. She said McFadden joined a family dinner at her home July 4 before they went to the Black Knight Pub. They had two rounds and had ordered a third when McFadden had left the bar to smoke, Heaton and McFadden testified. While outside, he saw police vehicles blocking part of the roadway with their emergency lights on. He walked toward the vehicles where McFadden said Const. Christopher Hipolito told him, "What the f--- do you want? You shouldn't be here, get the f--- out of here." McFadden testified that he walked back toward the bar, muttered that he would get his "f---ing camera." The remark from the officer, the reporter said, left him frustrated and heartbroken because it came after a period of acrimonious relations with RCMP, including him being barred from a press conference in April 2015. Northern News Service (Yellowknifer)

RCMP end probe into Senate expenses
Mounties drop cases of 30 current, former senators as source cites lack of evidence, says investigation no longer in the public interest. The RCMP will not launch any further criminal investigations into the remaining Senate expense files, officially closing the book on one of this decade's biggest political scandals without a conviction. Sources say the Mounties have reviewed 30 cases of current and former senators that were flagged by Auditor-General Michael Ferguson in his June, 2015, report and decided none warrant a criminal investigation. The decision comes after Senator Mike Duffy, the only member of the Senate whose case made it to trial, was exonerated last April on 31 charges of fraud, breach of trust and bribery relating to his Senate spending. He has since returned to work. A source close to the RCMP files cited lack of evidence and said it was no longer in the public interest to pursue investigations. The Mounties also shut down their nearly three-year investigation into Senator Pamela Wallin in May without laying charges, and fraud and breach of trust charges against Senator Patrick Brazeau were withdrawn in July. Both are now back in the Senate. Globe and Mail, A14

*** Condamnation d'un prêcheur islamiste bien connu de la GRC**
L'un des prêcheurs radicaux les plus influents d'Occident, suivi sur les réseaux sociaux par les terroristes canadiens Martin Couture-Rouleau et Michael Zehaf Bibeau, vient d'être condamné à plus de cinq ans de

prison au Royaume-Uni pour avoir soutenu le groupe armé État islamique (EI). En 2013, il avait prédit un attentat au Canada. Les Anglais le surnomment «l'homme le plus détesté» de leur pays, le «prêcheur de haine». Anjem Choudary, avocat de 49 ans d'origine pakistanaise, prédicateur emblématique dans les milieux islamistes britanniques, marchait sur une fine ligne depuis plusieurs années. Il s'était fait «le porte-parole des extrémistes, faisant des commentaires des plus déplaisants, mais sans jamais franchir le seuil de la criminalité», comme l'a expliqué au Guardian le commandant Dean Haydon, chef de l'escouade antiterroriste de Scotland Yard. La Presse

* **Racism lesson of the day**
Students returning to class in Surrey Tuesday got a lesson in racism. Police were called to Johnston Heights Secondary because of a large swastika and a racial slur that had been spray-painted on the outside wall. By the afternoon, someone had turned the swastika into a flower and covered up the slur, but students and parents said the damage was already done. "I saw this disgusting language and it really hurt me," one student told CTV News. A cleanup crew was also called to the school grounds in the mid-afternoon. It's unclear who is responsible for the spray-painted vandalism. Another student said she believes it was likely the work of "stupid kids." "Obviously they're stupid enough to write things like a swastika on the school," she said. The RCMP said investigators take cases like these very seriously. If the vandal is identified, Mounties said it's possible the individual will be charged with mischief, and that the incident could be treated as a hate crime. Castanet

* **Arrest leads Penticton police to cache of stolen mountain bikes**
Penticton RCMP's Targetted Enforcement Unit was successful in recovering a number of stolen bikes last week. Cpl. Don Wrigglesworth says the enforcement team arrested a 30-year-old Penticton man for possession of a high-end mountain bike stolen out of Kelowna last Tuesday, Aug. 27. That arrest led police to a downtown residence where police found $14,000 worth of stolen high-end mountain bikes. While making patrols on Van Horne Street Tuesday, police witnessed two men and a woman in front of a Van Horne residence with three expensive mountain bikes. The Van Horne residence was known to police, who were also looking for four mountain bikes reported stolen the previous night. A red Specialized Crave mountain bike was in possession of one of the men, which was found to have been stolen from Peachland on Aug.12. The man was also found to be in possession of methamphetamine and heroin. He was released on a promise to appear. Police then attended the residence of the man in possession of the stolen bike, leading them to Eckhardt Avenue where they found several high end mountain bikes in a shed. The bikes came from all over the Okanagan Valley, Wrigglesworth says. Infotel

* **La Loche, Sask., staff and students return to school where shooting took place**
Tuesday morning marks back to school for staff and students in La Loche, Sask. It has been nearly nine months since a horrific shooting rocked the northern Saskatchewan village. On Jan. 22, two staff members were killed and seven people were wounded in a shooting that took place at the community school. In a home nearby, two brothers were found dead. A 17-year-old is charged in connection with the shooting. At the time, officials were calling for the school to be torn down. (…) La Loche RCMP have confirmed that a school resource officer will be posted in the building. In addition to the RCMP officer at the school, officials have said the school division has hired a security service. The high school and Ducharme Elementary School will both have three security staff working in the buildings from morning to evening. The health region has also hired a suicide prevention worker who will also provide services through the Friendship Centre. Currently, there are two mental health counsellors and two addictions workers that are providing services in the community of La Loche. CBC News

West Shore RCMP identify man arrested after standoff
West Shore RCMP have released the name of the man arrested after shots were fired during an armed standoff in Langford on Saturday. Michael Godolphin, 36, is now in custody. West Shore court officials said Godolphin is facing at least two charges, possession of a weapon and two counts of possession of a controlled substance, and is scheduled to appear in court on Thursday. RCMP received a report of an agitated male in the 800 block of Langford Parkway just after 5 p.m. Saturday. Minutes later, responding officers found a man waving a handgun while standing on the side of the road near Langford Parkway and Veterans Memorial Parkway. A witness reported hearing two shots fired. Nobody was injured. Streets were blocked and the nearby Rona store was evacuated. Emergency responders, including Vancouver

Island and Greater Victoria emergency response teams, crisis negotiators and B.C. Ambulance paramedics, were on scene. Negotiators made contact with the man and talked to him for just under three hours until he surrendered shortly after 8 p.m. The handgun was recovered and sent for forensic tests. Times Colonist, A4; * Check News

RCMP Report: Thief gets away with $4,000 cash from Reddi Mart
The Golden-Field RCMP responded to 184 calls for service in the last two weeks, an average for this time of year. Calls for service included, but weren't limited to, 43 traffic complaints, 16 collisions, 14 abandoned 911's, 4 reported thefts, and 6 disturbances. (...)Local RCMP assisted the CP Police Service and Canadian Border Services Agency on August 31 after two males were located riding a train near the Beaverfoot, east of Golden. Further investigation by police determined that the males were US Citizens who had not reported their entry into Canada. The males were then detained and lodged in cells awaiting an immigration hearing which resulted in CBSA agents escorting the two back to the United States. Golden Star (2016-09-06)

*** Police believe 3 Burnaby sex attacks are related**
Burnaby RCMP is investigating three apparent sexual assaults against women between Sept. 1 and 3. Police said that on Sept. 1, they received two reports of women being followed as they walked along Mary Avenue and 16th Street. The women said the unknown male approached them from behind and pulled their pants down to the ground. When the women turned around, he fled the area on foot. The incidents happened within 20 minutes of each other and the suspect's description was similar in both cases. He is medium-skinned and in his late teens or early 20s, 5-foot-7 to 5-foot-10 with a thin build and prominent dark eyebrows. He wore a black baseball hat, black hoody and dark jeans. On Sept. 3 at 7:50 a.m., a woman reported that she'd been grabbed by a male on the 7400 block of Kingsway Avenue. The woman was walking down an alley when he approached her from behind and grabbed her buttocks. When she turned around the man ran away. The suspect was described as light-skinned with a thin build and 5-foot-7 to 5-foot-10. He wore a red jacket and blue jeans. RCMP, which believes the three incidents are related, said extensive patrols have been undertaken. None of the three women were injured. Burnaby RCMP caution people to be vigilant when walking alone, and to walk in pairs or groups if possible. Vancouver Sun, A6

Langford RCMP deserve kudos
An opinion piece states, "The incident in Langford Saturday could have so easily turned out differently, but because police officers did their job - and did it well - a dangerous situation was resolved with no one getting hurt. West Shore RCMP got a report at about 5:20 p.m. Saturday of an agitated man with a gun along the road near the intersection of Veterans Memorial Parkway and Langford Parkway. When officers arrived, the man fired two shots with a pistol. It would be hard to criticize officers if they had fired back. There was a serious threat to the lives of the police officers and to many civilians at a busy intersection at a busy time of the day. It was a tense situation. Yet the officers handled it with patience. Despite the man's highly agitated state, despite the fact that he set the gun down and picked it up several times, waving it around, officers waited him out. Instead of shooting him, they talked to him. They answered his agitation with calmness and it paid off. He gave himself up about 8 p.m. Police-involved shootings are in the news with distressing regularity these days, but the Langford incident won't make headlines outside of the region. Move on, folks, nothing to see here. But in reality, there was something to see: commendable professionalism and remarkable restraint. Witnesses, some of whom were trapped in their cars as police stopped traffic for understandable reasons, noted how calm the police were, not an easy task in such a high pressure situation. Officers had to weigh the welfare of the man with the gun with the safety of the public - the lives of innocent people were at risk. It was a situation for which police are trained, but one that most officers hope they never confront." Times Colonist, A10

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Rapist sightings false, say police
Vancouver police say convicted rapist Larry Takahashi has not been seen in an east Vancouver neighbourhood. Someone has posted leaflets claiming to have seen the 63-year-old in the neighbourhood

but Acting Sgt. Brian Montague says the sightings are false. Takahashi is staying at a halfway house in an unknown location in Vancouver but Montague says he has not yet left that facility. In 1984, Takahashi was sentenced to three life terms after admitting to raping at least 30 women in Edmonton in the 1970s and 1980s. He was recently granted parole, even though a Parole Board report found he poses a moderate to high risk to reoffend and is a danger to teen girls and women. Privacy laws prevent officials from naming where Takahashi is staying. Canadian Press (The Province, A9, Vancouver Sun, Waterloo Region Record)

Un procès devant juge seul pour une affaire de maltraitance d'enfant
Un couple de Sherbrooke accusé de maltraitance envers son enfant et qui devait subir son procès devant jury retourne devant juge seul. (...) Les accusations portées contre le père de famille sont plus imposantes que celles qui pèsent contre la mère. Le père a été condamné le printemps dernier de gestes à caractère sexuel sur deux filles sous sa garde. (...) Dans le dossier complémentaire de cette affaire, le père a été condamné à 12 ans de prison en mai dernier pour les gestes à caractère sexuel sur deux de ses filles. Il a porté la peine en appel et la permission d'en appeler doit être entendue le 14 septembre prochain à Montréal. La Tribune, 11

*** Former Quebec judge Jacques Delisle, convicted of murdering wife, applies for release from prison**
The only judge in Canada to ever have served time for a murder conviction is filing for bail as he waits for a ministerial review of his case. The lawyer for former Quebec judge Jacques Delisle, who was convicted in 2012 of first-degree murder in the death of his wife, filed an application for bail in Quebec Superior Court today. Delisle was sentenced to life in prison with no chance of parole for 25 years in the shooting death of his wife. (...) In Canada, convicted prisoners who have lost all legal appeals are allowed by law to ask the government to reopen the case by making a direct appeal to the federal justice minister. The Department of Justice`s Criminal Conviction Review Group has advanced the application for review to the Investigation stage, the second of four stages in a ministerial review. Lockyer said that means Justice Minister Jody Wilson-Raybould "is saying that she has determined that there may be a reasonable basis to conclude that a miscarriage of justice likely occurred." "Having done that, Mr. Delisle is entitled to bring a bail application, pending the minister's final decision," Lockyer said. The review is the final recourse for Delisle, who has maintained his innocence since his wife's death. CBC News (2016-09-06)

*** Kevin McMurrer, convicted of second-degree murder, granted full parole**
A Prince County man, convicted and sentenced in the murder of his estranged wife, has been granted full parole. Kevin Kenneth McMurrer, now in his mid 50s, had been serving a life sentence for second-degree murder of his ex-wife, Carrie Ellen (Crossman) McMurrer. (...) In August 2015, his case was again reviewed and he was granted a six-month day parole, which was extended another six months in February. At that time, leave privileges were authorized and special conditions imposed “to protect society” and assist with his reintegration. The board wrote that during this release McMurrer “met and exceeded expectations” of his supervision plan; maintained regular counselling with different supports; obtained employment; participated in programming, community groups related to combating domestic violence; and attended Alcoholics Anoymous meetings and psychological counselling. Journal Pioneer (2016-09-06)

*** Routine patrol results in drug charges**
A Grande Prairie man is facing drug charges after being caught with what is believed to be cocaine in his mouth during routine patrols on Saturday, south of Grande Prairie. At about 3 a.m., RCMP patrolling the area near the County Industrial Park saw a man walking south on 93 Street near 42 Avenue. During questioning, police determined the man was hiding a small amount of what is believed to be cocaine in his mouth and was arrested without incident. Blake Dean Murphy, 29, of Grande Prairie has been charged with possession of a controlled substance and obstructing a Peace Officer. Murphy is currently on parole but remains in police custody. Daily Herald Tribune (2016-09-06)

*** Dartmouth woman gets almost 6 years in prison for prolonged attack on ex-lover**
A Dartmouth woman who confined her former lover, threatened to kill her and repeatedly stabbed her with a steak knife has been sentenced to five years and 10 months in prison. Diane Lynn Pothier, 37, pleaded

guilty in June to a charge of aggravated assault and was sentenced Tuesday in Halifax provincial court. (…) The judge made Pothier's sentence consecutive to a three-year term she is already serving for an attack on an Elizabeth Fry Society employee in Ontario. That incident happened while Pothier was on bail on the charges involving her ex-lover. Last summer, while in a federal facility in Kitchener, Ont., she threatened to kill a corrections officer, an offence that drew a one-month sentence. Local Xpress (2016-09-06)

*** La Fête des pères**
Une lettre à l'éditeur déclare, « Je suis détenu à la prison de Cowansville. On m'a faussement accusé de tentative de meurtre. La lenteur des délais pour aller à procès au provincial ainsi que les conditions inhumaines de détention m'ont emmené à plaider coupable pour limiter ma peine à 6 ans. J'ai pris cette décision pour éviter le suicide et faire du meilleur temps au fédéral. Les conditions de détention au provincial sont invivables, incluant les préjudices et injustices causés, tant par les agents correctionnels que les autres détenus. Personne ne peut comprendre la réalité du milieu carcéral s'il n'a pas le malheur d'y avoir séjourné. J'écris un Journal au quotidien pour éventuellement dénoncer la vie en milieu carcéral dans un livre à publier pour conscientiser les citoyens sur la réalité d'ici. Je suis un homme avec de belles valeurs et une bonne éducation. Même si je souffrais dans certains aspects de ma vie d'avant, jamais je n'aurais pu imaginer les pressions psychologiques que j'allais subir en dedans. Je termine un DEC en sciences humaine et j'étudie par correspondance en gestion des ressources humaines. Pourriez-vous me référer à une personne qui serait intéressée à me publier. Il est important que les gens sachent que les détenus, victimes du système, payent 100 fois plus cher au niveau des conséquences, que l'importance véritable de ce qui les a mené en prison. » Journal de Montréal, 47 (Journal de Québec)

Buzz kill
An editorial states, "There goes another Harper tough-on-crime law out the judicial window. Because, of course, we wouldn't want to be too hard on a woman farming 1,100 pot plants in the middle of a Jane St. highrise apartment building. In a landmark ruling, an Ontario judge has struck down yet another of the former Conservative government's mandatory minimum sentences as unconstitutional, this time the two-year minimum jail term - with an extra year for endangering public safety - for growing more than 500 marijuana plants. In 2015, Hai Thi Pham was convicted of tending an elaborate commercial pot grow-up in a three-bedroom apartment at 2755 Jane St. Toronto Police found 1,110 plants being grown under 19 high-pressure sodium lights connected to 20 ballasts that made them compatible with 1,000-watt lightbulbs. (…)10 Months Pham's lawyers argued the 45-year-old mother of two shouldn't be sentenced to the mandatory minimum mandated in the 2012 amendments to the Controlled Drugs and Substances Act. They challenged the law not because a three-year sentence would be "grossly disproportionate" in her particular case - they actually agreed it wouldn't be - but because it could possibly affect other, less blameworthy offenders where it would amount to cruel and unusual punishment. (…) Mandatory minimum sentences were championed by the former Conservative government as a legislated way to curtail courts too often seen as soft on crime. But now that Harper-era agenda is being systematically dismantled by a judiciary which never liked being told what to do." Toronto Sun, A5

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Court reviewing acquittal in death**
The Alberta Court of Appeal is hearing arguments on whether to overturn a controversial acquittal of an Ontario trucker charged with killing an indigenous woman. Last year, a jury found Bradley Barton not guilty of first-degree murder in the death of Cindy Gladue, a 36-year-old sex-trade worker who was found dead in a bathtub in an Edmonton motel room in 2011. Gladue bled to death after a night of what Barton called consensual, rough sex. (…) In a submission to the court, the Women's Legal Education and Action Fund criticized the way the trial was conducted. The brief said Gladue was consistently dehumanized and stereotyped. "The characterization of Ms. Gladue as 'native, ' coupled with the characterization of her as a prostitute, created a heightened risk that the jury would bring to the fact-finding process discriminating beliefs, misconceptions or biases about the sexual availability of indigenous women. Canadian Press

(Edmonton Sun, A5, Red Deer Advocate, Edmonton Journal); Globe and Mail (2016-09-07); Metro News (2016-09-06)

*** SaskTel's 'I Am Stronger' returns to help youth tackle bullying**
As students head back to school this week, SaskTel is ramping up its program designed to help youth put an end to bullying. In partnership with the Ministry of Education, the I Am Stronger program offers grants of up to $1,000 for youth-led initiatives that promote kindness and address the issue of bullying and cyber-bullying both online and in local communities. In addition, the website offers dedicated to resources for kids, teenagers, families, and educators, plus assists victims of bullying or cyber-bullying in getting help and reporting bullying activity safely. SaskTel said that it acknowledges that the products and services it sells may be used to conduct bullying activities. "Since the program launched in 2014, we are excited to have offered 27 grants to date totaling $25,735," said SaskTel president and CEO Ron Styles, in the news release. "We are pleased to assist with empowering our youth to turn their ideas into actions that positively influence social change in schools, communities, and online." SaskTel (2016-09-06)

*** Opioid addiction 'epidemic' in N.L. says U-Turn founder**
The founder of the U-Turn Drop in Centre in Carbonear says that opiate abuse in Newfondland and Labrador has reached "epidemic" levels. In an interview with the *St. John's Morning Show*, Jeff Bourne said that in his region, opioids used as pain medication and as street drugs are a problem just like everywhere else in the province. "I say we're into an epidemic right now," said Bourne. He said that fentanyl – a drug that can be up to 100 times stronger than morphine – has been showing up around Carbonear, first as a slow-release patch and lately as a pill. CBC News (2016-09-06)

*** Drug education upgraded in schools amid B.C. overdose crisis**
Educators are working diligently to warn youth about the inherent dangers of fentanyl as the death toll from B.C.'s overdose crisis shows little sign of receding. According to the B.C. Coroners Service, 433 people died in B.C. of illicit-drug overdose between Jan. 1 and July 31. Fentanyl, a potent synthetic opioid increasingly being cut into street drugs and counterfeit opioids, was detected in 62 per cent of cases in the first half of 2016. The vast majority of those who died — 235 people — were between the ages 20 and 39, but 11 were between 10 and 19. To protect children from fentanyl — which police and health authorities have detected in heroin, cocaine, crack, amphetamines and counterfeit prescription pills — educators are bolstering their outreach in schools. Rob Rai, director of school and community connections for Surrey School District 36, said his district is working closely with the City of Surrey and Fraser Health to obtain updates on fentanyl's presence in the community. Since last year, the district has distributed such information to counsellors, administrators and youth-care workers, who then work with students to answer their questions and clarify misconceptions about fentanyl and other toxic adulterants. "One of the things the kids have shared with us is that they don't see pill drugs as a hard drug," Rai said. "We're working hard to educate the kids that just because it's not a pipe or not a needle, doesn't mean that you're any less at risk." Vancouver Sun (2016-09-06)

*** New addictions treatment program for women opens as demand soars**
A new addictions treatment program designed specifically for women has opened its doors as the province grapples with a growing demand for services to help individuals with drug and alcohol abuse problems. On Tuesday, the Recovery Acres Society unveiled its CARE (Co-occurring Addiction Recovery Essentials) for Women office next door to its existing treatment facility for men in Marda Loop. Janine Copeland, program director for CARE for Women, said the short-term, outpatient-only program will "fill a gap." "I've always suspected that there has been missing pieces when it comes to programming for women. Historically, I'd always been told that addiction is addiction and recovery is recovery. That never sat right with me," she told the crowd gathered for the grand opening. (…) The government has acknowledged Alberta is facing an "opioid crisis," as it deals with a rising death toll from illicit fentanyl that reached 153 fatalities in the first six months of this year. On Wednesday, Liberal Leader David Swann will renew his call for the provincial government to declare a public health emergency to deal with fentanyl. The provincial government provides about 40 per cent of the funding to the Recovery Acres Society but did not put dollars specifically toward the CARE for Women program. Calgary Herald (2016-09-06)

*** Crown seeks 'incredibly harsh' sentence for B.C. fentanyl trafficker**

Does the dire nature of the deadly fentanyl epidemic demand extreme punishment for the drug's dealers? That's the question facing a B.C. provincial court judge this week as she considers the Crown's call for an unprecedented 18-year jail sentence for Walter James McCormick, a fentanyl trafficker arrested in a Vancouver police investigation. Crown counsel Oren Bick is calling for 10 years for the initial charges and eight for a subsequent fentanyl-related offence that occurred while McCormick was on bail. He wants the two terms served consecutively. "This is an incredibly harsh and high sentence," Bick told Judge Bonnie Craig during the first day of sentencing last week. But Bick said the circumstances demand action. "Mr. McCormick is and has been a high-level drug trafficker in fentanyl, which is a drug that is extremely dangerous, and he and other high-level fentanyl dealers bear personal significant responsibility for hundreds of fentanyl-detected deaths in British Columbia," he said. (…) In calling for a tough sentence, Bick entered into evidence a series of reports about the scope of the fentanyl crisis currently facing British Columbia and other provinces. He also called Dr. James Kennedy, an expert on internal medicine from St. Paul's Hospital in Vancouver, as a witness to talk about the effects of fentanyl on the brain and the rise of the drug in both the worlds of medicine and illicit drug use. On cross-examination, Kennedy agreed with the defence's suggestion that over-prescribing doctors and pharmaceutical companies have contributed to an epidemic that has ravaged communities and killed hundreds. Bick didn't disagree. But he said dealers like McCormick are taking advantage of the bigger problem of opioid dependence to introduce dangerous new drugs onto the illicit market. CBC News

* **Draft Police Budget Approved**
The draft budget was passed by the board at a special meeting last Tuesday. The budget sees board expenditures total $103,378. Board Chair Pat Hehn says they worked really hard to find efficiencies and savings this year. She says the projected budget for 2017 will be less than the 2016 budget. The OPP portion of the budget works out to be close to $8.3 Million. Hehn says the OPP is in salary negotiations with the union and it could see the budget go up by as much as $250,000 due to salaries and wages. She says that is one component in the budget that the board has no control over. Bayshore Broadcasting

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

* **Attorney joins national inquiry**
The art piece that will hang in Mary Potter' s new Toronto office was created to remember Canada ' s missing and murdered aboriginal women and girls. A print of Not Forgotten , by Manitoba artist Maxine Noel, was Potter ' s going-away gift from the Middlesex County Crown ' s office where she made history as the first woman to hold the top job. Potter will be part of national history in her new post as a member of the legal team heading up the Ontario leg of the National Inquiry into Missing and Murdered Aboriginal Women. "When I saw they were looking for experienced Crown counsel to be part of this team, I thought it ' s something that ' s worthwhile, fulfilling work. It ' s definitely my niche ," Potter said. " This is something that I feel deeply committed to, and if I can be part of this nationwide inquiry, even the smallest part into reviewing what happened in the past and exploring what can be done to stop us from going down this road in the future, then I will be able to feel I have done something rewarding with my legal career ." The inquiry began its two-year probe Sept. 1 into the deaths of 1,200 women across Canada between 1980 and 2012. London Free Press, A3

* **A conversation with the minister for the status of women**
Federal status of women minister Patricia Hajdu is no stranger to the struggles of being a woman working in volatile environments. Prior being elected to Parliament in the Liberal return to power in the fall of 2015, Hajdu worked as executive director of a Thunder Bay homeless shelter. Before that, she raised two sons as a single mother while attending university. Last week, Hajdu was in Winnipeg to attend a roundtable discussion on gender-based violence as part of a cross-Canada tour on the issue. Hajdu played a major role in organizing an inquiry into missing and murdered indigenous women (MMIW) and has been travelling country-wide to speak at and attend roundtables, town halls, and conferences covering everything from the inquiry – which began its mandate Sept. 1 – to physical and sexual violence against women and international women's issues. While in Winnipeg, Hajdu spoke with the *Manitoban* about the

MMIW inquiry and a broad range of issues facing women both within Canada and internationally, including campus sexual assault and pay equity. (…) "The government's role in the [MMIW inquiry] is pretty much complete. We were responsible for choosing commissioners and making sure that the inquiry was designed and planned. We also made sure that the inquiry was funded and launched. Now the inquiry becomes an independent process and the commissioners take over and decide exactly how they will move forward." Manitoban

* **Reconciliation takes leadership**
An opinion piece states, "Is reconciliation between indigenous and nonindigenous peoples going where it needs to go? Reconciliation has taken the road of least resistance. Sure, residential schools were awful, but they were symptomatic of a larger problem - colonialism. Colonialism was supported by mid-19th-century racist scientific ideas of alleged aboriginal inferiority, which allowed Canadians to believe they should control the lives of First Nations. Real leadership is personified by people like Gitxsan Cindy Blackstock and Anishinabe John Borrows. Ms. Blackstock has forced the federal government to rectify its discriminatory underfunding of on-reserve social services. Mr. Borrows argues cogently that Canada needs to accept indigenous legal systems. In addition, the inquiry on missing and murdered indigenous women and girls needs our attention." Vancouver Sun, A11

* **Vancouver aboriginal men don high heels**
Curtis Ahenakew will walk in high heels this weekend to urge a stop to gender violence and sexual assault. Ahenakew is one of the organizers of Walk a Mile In Her Shoes: Aboriginal Men Against Violence Against Women. The march calls on indigenous men to walk in high heels as an act of raising awareness. "We're doing this as men to speak out openly about it," he said. "We could have called it walk a mile in their moccasins, but walking in a pair of heels is the symbol or the metaphor of the pain they've experienced." (…) The walk's opening speaker is Musqueam elder Shane Pointe. Ahenakew said speakers will also talk about the National Inquiry into Missing and Murdered Indigenous Women and Girls. 24 Hrs Vancouver (2016-09-06)

* **Explore the city with Vancouver Book Award finalists**
When was the last time you saw your city through someone else's eyes? Three provocative books shortlisted for the City of Vancouver Book Award encourage readers to do just that. This year's finalists include *The Revolving City: 51 Poems and the Stories Behind Them*, an anthology of poetry edited by Wayde Compton and Renee Sarojini Saklikar; *That Lonely Section of Hell*, a memoir of Vancouver's Missing and Murdered Women Investigation by Lorimer Shenher; and *Lawrence Paul Yuxweluptun: Unceded Territories*, the catalogue for an art exhibition currently on display at the Museum of Anthropology, by Karen Duffek and Tania Willard. (…) *That Lonely Section of Hell: The Botched Investigation of a Serial Killer Who Almost Got Away*, published by Greystone Books, is Shenher's first book, and it's been shortlisted for several awards. The moving first-person account of the Vancouver police investigation into missing women in the Downtown Eastside in the 2000s is also a call for change in what he calls a "toxic" police culture. "I have felt like, while this issue has been an important issue, I've felt that to some degree it's been ignored," Shenher said. "So I'm thrilled that the City of Vancouver, the people there have read it, and I hope that the Vancouver Police will take their lead and read the book." Metro News (2016-09-06)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

N.B. government has high hopes in economic return of marijuana legalization
Medical marijuana is a rapidly growing industry, and with the federal government looking into legalization, the potentially enormous economic return is something the province of New Brunswick is counting on. The Gallant government has recently announced a $4 million investment for Zenabis, a marijuana production facility in Atholville, and has given previous money to medical marijuana producer Organigram in Moncton. "We see it as a huge opportunity both in the growth of medical marijuana and the impending legalization," said Susan Holt, New Brunswick's chief of business relationships. Global News (2016-09-06)

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Federal workplace charity donations delayed over Phoenix fears**
When the federal government rolls out its annual workplace charitable campaign this morning, it will advise departments to delay collecting pledges from employees until the dust from the Phoenix pay system fiasco settles. The precaution — a first in the campaign's history — comes as some public servants say they're afraid to sign up for automatic payroll deductions over fears it could lead to other problems with their pay. Since January, more than 80,000 public servants have reported being overpaid, underpaid or not paid at all during the government's transition to the new Phoenix pay system. Some said they've maxed out credit cards, taken out loans, gone on stress leave or even quit their jobs entirely over the debacle. CBC News; Radio-Canada

*** Canadians lack faith in upper ranks of public service: survey**
Canadians don't have a lot of trust in senior bureaucrats to "do the right thing" in managing federal operations and delivering services. The findings of a survey, conducted by Environics Institute and the Institute on Governance, into how Canadians view accountability and oversight in government underscore a troubling level of mistrust among Canadians in their government, both elected officials and public servants. Canadians put more faith in front-line public servants delivering services — as long as they have the resources and authority to do the right thing — than they do for MPs and senior bureaucrats. The majority have at least some trust in front-line workers and MPs, but views of senior public servants are almost equally divided between some trust and little or no trust. At the same time, Canadians overall perceptions about government and its effectiveness — even among its harshest critics who believe government is broken — improved significantly since a similar survey in 2014, which some attribute to the "Trudeau Effect." Ottawa Citizen (2016-09-06)

*** Les étudiants, victimes oubliées du système de paie Phénix ?**
Le nouveau système de paie de la fonction publique, le système Phénix, connaît de nombreux ratés depuis sa mise en place en février dernier. Des dizaines de milliers de fonctionnaires fédéraux rencontrent des difficultés à percevoir l'intégralité de leurs paies, lorsqu'ils ont la chance de recevoir un salaire. Entre 3000 et 5000 étudiants de l'Université d'Ottawa (U d'O) auraient travaillé pour le gouvernement cet été. En raison de la nature et des particularités de leurs contrats, ces derniers seraient pour la plupart concernés par les erreurs du système Phénix. **(…)** Dans un communiqué publié la semaine dernière sur le portail uoZone, l'U d'O annonçait avoir pris des mesures pour venir en aide aux étudiants employés par le gouvernement. Concrètement, les personnes concernées sont invitées à prendre contact avec le bureau des Comptes étudiant afin d'établir des ententes de paiements pour la session d'automne. La Rotonde (2016-09-06)

OTHER / AUTRE

Canadian military aircraft playing 'critical' role in anti-ISIL fight
Despite the withdrawal of Canada's fighter jets from Iraq and Syria last spring, a senior officer says Canadian military aircraft are providing vital intelligence to allies for air strikes and other operations against the Islamic State of Iraq and the Levant. The Liberal government announced in February that it was ending Canadian combat operations in Iraq by withdrawing six CF-18s that had been part of the U.S.-led bombing campaign against ISIL since October 2014. But the Liberals left behind a Polaris air-to-air refueller and two Aurora surveillance aircraft. Those aircraft have continued to support the bombing campaign against ISIL, also known as Daesh, even as public attention has turned to the role of Canadian special forces operatives in northern Iraq. Canadian Press, (Telegram, A6, Cape Breton Post, London Free Press, Vancouver Sun, National Post, Montreal Gazette, Ottawa Citizen, Telegraph-Journal, Guardian, Province, Waterloo Region Record, Kingston Whig-Standard, Hamilton Spectator, Times and Transcripts)

*** Turkey's Victory Day has new meaning in light of coup attempt**

Turkish Ambassador Selçuk Ünal welcomed guests to his beautiful Rockcliffe home on Aug. 30 to celebrate Turkey's Victory Day. The celebration commemorates the Turkish victory over Greek forces in the Battle of Dumlupinar in 1922, a fight instrumental in the Turkish War of Independence. (…) The tone of the event was sombre while the president's message, one delivered at all Turkish embassies around the world on that day, was delivered by Hakan Cengiz, counsellor at the embassy. (…) Since July 15, the Turkish government has labelled the coup as the work of what it calls the terrorist organization of Fethullah Gulen, a Turkish cleric living in the United States who denies involvement in the coup. The Turkish government has detained thousands of judges, public servants, academics, journalists, and others, including two Turkish-Canadians and Turkey's former ambassador to Canada, Tuncay Babali, many for suspicion of collaborating with the coup plotters. Turkey has been widely criticized for its actions after the coup attempt, including by Canadian Parliamentarians Judy Sgro, a Liberal MP and chair of the Canada-Turkey Parliamentary Friendship Group, and Foreign Minister Stéphane Dion. Hill Times

*** The untold story of the two weeks when Edward Snowden was the world's most wanted man**
The tall, lanky American dressed in all black looked familiar. But Ajith, a 44-year-old Sri Lankan refugee seeking asylum in Hong Kong figured the nervous-looking man with the red-rimmed eyes fidgeting in the darkness outside the United Nations building in the Tsim Sha Tsui district of Kowloon was a U.S. army dodger. Summoned by his immigration lawyer in the late evening of June 10, 2013, Ajith (last names of the refugees in this story have been withheld), a former soldier in the Sri Lankan military, was told the unidentified man was "famous" and needed "protection." Little else was revealed except that he would be responsible for covertly moving the American around at a moment's notice. (…) To escape the long arm of American justice, the man responsible for the largest national security breach in U.S. history retained a Canadian lawyer in Hong Kong who hatched a plan that included a visit to the United Nations sub-office where the North Carolina native applied for refugee status to avoid extradition. (…) Supun wasn't told that Snowden had earlier that day escaped his hotel room where he had been holed up with Poitras and felllow journalist Glenn Greenwald leaking classified documents he had stolen from the National Security Agency's Threat Operations Centre in Hawaii where he worked as an outside contractor for Booz Allen Hamilton Inc. The media's explosive reporting captivated the world, and infuriated and embarrassed the U.S. government. Postmedia Network (Vancouver Sun, N1/FRONT, National Post, Starphoenix, Leader-Post, Montreal Gazette, Calgary Herald, Windsor Star, Ottawa Citizen, London Free Press, Edmonton Journal, Windsor Star); Canadian Press (Hamilton Spectator, Waterloo Region Record)

*** Defend our own interests through universal rights**
An opinion piece states, "Another meeting between a powerful dictatorship and a liberal democracy, another chance to pretend that by defending universal values, governments unavoidably hurt their countries' own interests. China has perfected the art of censoring speech, repressing minorities, jailing critics and flouting the rule of law at home. The consequences of its abuse extend beyond the mainland, though. (…) Don't expect these indignities to remain local. They humiliate and terrify a group so intolerably as to foment violent terrorism in China, and violent terrorism doesn't tend to stay put. Well over 100 Uighurs have travelled to Syria and joined jihadist movements; many bring their wives and kids because they believe it better to live in a war zone than back home. And it's not as if China reserves repression for minority groups. It detains and tortures critics without anything approaching due process. We might think this a tragic violation of the rights of Chinese citizens, and perhaps we could leave it there, were China not jailing citizens of other countries, too, including our own. Foreign governments can't console themselves with the knowledge that the only way people will get thrown in a Chinese prison cell is if they travel to the Chinese mainland. China allegedly sent special agents into Hong Kong and Thailand, kidnapped some booksellers, and whisked them back for a bit of detention and forced confession. If political dissidents won't go to China, China might come to them." Kingston Whig-Standard, A4, (London Free Press)

INTERNATIONAL

*** Paris police discover car with gas cylinders near Notre Dame**
Peugeot owned by man on terror watchlist found near cathedral on Saturday night. A car containing several gas cylinders was discovered close to the Notre-Dame cathedral in central Paris last Saturday

night and its owner, now in custody, is on an intelligence services watchlist of people suspected of religious radicalisation, police officials said. The Peugeot 607, which had no registration plates, contained seven gas cylinders, one of them empty on the front passenger seat. It was found with its hazard lights flashing, as if to attract attention, two police officials said on Wednesday. "We think he may have been trying to carry out a test-run," one of the officials said. There was no detonating device present in the car, found on a Seine riverside stretch called the Quai de Montebello, metres from the Notre-Dame cathedral. Documents with writing in Arabic were also found in the car. More than 200 people have been killed in terror attacks over the past year and a half in France. France remains on maximum alert after calls by the Islamic State group for followers to attack the country, which is bombing the militant group's bases in Iraq and Syria. Irish Times

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
October 10, 2016 / le 10 octobre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Erosion of trust threatens to ravage internet, 'eighth wonder of the modern world,' say authors
An interview between Kate Malloy of the Hill Times and Fen Hampson states, "When former CIA computer specialist Edward Snowden leaked classified information in 2013 revealing the United States National Security Agency and other government agencies were using global surveillance programs to spy on internet users, Fen Olser Hampson and Eric Jardine started thinking about how a worldwide lack of trust could destroy the internet. So they wrote a book about it, Look Who's Watching: Surveillance, Treachery, and Trust Online, published by the Centre for International Governance Innovation. [Malloy] What is your message to Canadian federal lawmakers and to the **federal minister responsible for public safety** in Canada, specifically? What can the government do? [Hampson] "The Canadian government and indeed all governments have a major, fiduciary responsibility to respect and ensure the privacy and security of their citizens online, not to compromise that trust through their actions, and to

ensure that private corporations do the same. As we say in the book, without trust the internet won't be an effective tool of prosperity, growth, communication, and innovation. We also argue that internet policy in all of its aspects, not just public safety, is too important to be left solely in the hands of governments or, for that matter, private corporations... The public believes that there is a role for surveillance, but, at the same time, they don't want governments snooping into their own private communications. As authors, we believe that there should be no back doors to end-to-end encrypted data and communications for the simple reason that governments are not very good at keeping secrets and if the good guys have encryption keys, the bad guys will eventually get their hands on them too..."" The Hill Times

'Deep concerns' over proposed security panel

Battle lines are being drawn in the House of Commons over the Liberal government's proposed new National Security and Intelligence Committee of Parliamentarians. The Conservatives and NDP expressed qualified support for the committee's creation during second reading debate on Bill C-22 that began Sept. 27, but both parties zoomed in on what they said were serious flaws, such as too much governmental control over the committee's membership and direction and too little secret information the security-cleared committee of seven MPs and two Senators will be allowed see... However, Saskatchewan lawyer and **Public Safety Minister Ralph Goodale** said if committee members were to uncover something they considered problematic — that their oath of confidentiality prohibited them from disclosing — they would have recourse, without disclosing any classified information. ***"Without getting into specifics, committee members would command a great deal of attention and put a great deal of pressure on the government of the day if they were to tell Parliament and the public that there was something going on within the realm of security and intelligence activities that they believed was improper,"*** he assured the Commons Sept. 27. ***"The committee would be able to outline the problem in detail in its report to the prime minister, and the prime minister would be accountable to Canadians. Subsequently, the committee would be able to tell Canadians whether the problem had been adequately addressed, and the pressure would not go away until the committee gave the all clear. That public pressure would be a powerful tool, and only a committee of parliamentarians could bring it to bear."*** **Goodale** said C-22 aims to help create a national security framework that makes Canada "a world leader in both effectiveness and accountability." The Lawyers Weekly

Defending the damned

For Howard Sapers, one of the most striking moments of the last decade came soon after he released a damning report on racism and discrimination in Canada's prisons. By any reasonable standard, the 2013 report by Sapers, the country's correctional Investigator, should have given pause to every Canadian. It found that black and indigenous people were being thrown in jail at alarmingly accelerated rates, far out of proportion with their numbers in Canadian society. Moreover, once inside, their treatment seemed to suggest particular scorn... Instead, the response from the Conservative government and its members of Parliament landed somewhere between mockery and dismissal. 'The only identifiable group that our justice system is targeting is criminals," said **Steven Blaney, then-public safety minister,** when the report came up during Question Period on Nov. 26, 2013... Soon after, the Conservatives called an election, and lost power. This spring, the new Liberal government gave him another year. Sapers says rather than seeing it as a second chance, he just sees a continuation of the work that needs to be done. And there's a lot of that work to do. Justice Minister Jody Wilson-Raybould's mandate letter from Prime Minister Justin Trudeau, for example, specifically calls for the implementation of recommendations from the inquest into the death of Ashley Smith. Hill Times

Climate change 'issue of the century,' ministers should be demanding environmental assessments from their departments, says environment commish

Calling climate change "the issue of the century," Canada's federal Environment and Sustainable Development Commissioner Julie Gelfand says federal departments must do more to help the government realize its sustainable development goals, and ministers and cabinet should refuse to consider their proposals until they are accompanied by assessments of the environmental impacts of their plans. With this being the fourth year the audit has been done, her office has now reported on 21 departments with five left to do next year: **Public Safety Canada**, Western Economic Diversification Canada, Atlantic Canada Opportunities Agency, the Public Health Agency, and Canada Economic Development for Quebec Regions. Hill Times

TOP STORIES / MANCHETTES

CSIS, Bill C-51 and Canada's growing metadata collection mess
An opinion piece states, “Much has been made over whether the Canadian Security Intelligence Service, Canada's spy agency, should be armed with broader powers to "disrupt" what it perceives as terrorist plots. A report tabled this month by the Security Intelligence Review Committee, which watches over CSIS's work, notes that while the spy agency hasn't abused its new powers of disruption, its bulk data collection program needs to be scaled back. It's easy to think of CSIS and other spy agencies as shadowy organizations that carry out James Bond-like "missions" involving cool gadgets and high-tech weaponry, but the Snowden leaks, among other revelations, have shown the public that metadata collection (online communications, phone logs and other electronic exchanges that can be intercepted in enormous amounts) now constitutes the state's primary instrument of control. Privacy Commissioner Daniel Therrien recently called upon legislators (the Liberals in particular) to amend certain aspects of Canada's national security laws in order to address the issue of metadata collection…” CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort Mac residents say thanks
As Canadians count the reasons they have to be grateful this Thanksgiving, Fort McMurray, Alta. is expressing its own thanks to Canada with a special video. The Regional Municipality of Wood Buffalo has posted a video on its Facebook page expressing the gratitude residents have for the help and support they received in the spring when a massive wildfire forced everyone to flee the city for weeks. The video begins with scenes of smoke and flames, along with accounts from residents about what they went through as they left. It then shifts to talk of the rebuilding effort, as well as the help that came from the rest of Canada… "Thanksgiving is a time to reflect on what we are thankful for, and this weekend we are thankful for the support of Canadians. Your thoughts, prayers, donations, volunteer hours, hand-made gifts, shipments of supplies and kind words are a constant reminder of the care the residents of Wood Buffalo received in their time of need," the post states. The fire in May forced over 80,000 people out of the northeastern Alberta city for a month and destroyed 10 per cent of its structures. In August, the Canadian Red Cross said $299 million had been raised to help with recovery from the Fort McMurray wildfire. Red Cross CEO Conrad Sauve said that included $165 million donated by Canadians to the charity. The federal government contributed $104 million to match funds donated made by individual Canadians and the province matched $30 million given by individual Albertans. Canadian Press (Whig Standard, Toronto Star, For McMurray Toda, Owen Sound Sun Times, Brantford Expositor, Chatham Daily News, North Bay Nugget, Sault Star, Cornwall Standard Freeholder, London Free Press, Chronicle-Journal)

Paying the piper
When Saleemul Huq gets into a room with negotiators to hash out climate change agreements, he prefers not to mince words in making his point about compensating developing countries for loss and damage… There are two elements to the conversation about loss and damage: scientific and political. On the science side, there isn't much disagreement. If no one does anything about climate change… the planet Earth and its inhabitants are in for a rough ride. Finding examples of climate change-induced loss and damage doesn't even require looking beyond North America's borders. The Alberta government's website lists increased forest fires, droughts, and "heavy precipitation with associated increased risk of flooding" as examples of extreme weather events brought about by climate change… The Canadian government, which as of publication, had yet to ratify the Paris Agreement, says it's a proponent of supporting efforts to minimize loss and damage… But the Canadian government draws the line at shouldering the blame. "Canada encourages and supports all countries to put in place frameworks or strategies that will allow them to undertake effective adaptation actions that would also increase resilience to prevent or minimize loss or damage," the email says. "These strategies may be developed at the country or community-level. Linking loss and damage to liability could inhibit a country-driven approach to adaptation. Hill Times

Plane crash survival story recounted
A short flight ended up as a long night for two men after their Maule M-4 float plane flipped upside down into the frigid waters of Gordon Lake on Sept. 29. The lake is about 100 kilometres northeast of Yellowknife. When the private plane carrying Shariff Adam, piloted by his friend Ken Quackenbush, didn't make it back to Sandy Point Lodge on the lake, his father Hassan Adam and others in the party grew anxious as hours ticked by... Hassan, who recounted for News/North his son's story about the crash, said the two were landing in the northwestern part of the lake when the engine cut out... Several hours after the plane failed to return to the lodge, Hassan called his friend Adam Bembridge who owns a helicopter company. Bembridge said he knew it would take time for search and rescue efforts to get underway and reach the area... He called one of his pilots at Acasta HeliFlight Inc., John Buckland. Within 30 minutes Hassan heard the helicopter at the lodge. The search of the edge of the lake that evening included help from float plane pilot Ray Decorby and a Royal Canadian Air Force Twin Otter but nothing was spotted. Without a cache of fuel at the lodge, the helicopter had to return to the city. For several hours overnight, Hassan said he heard the C-130 Hercules from Winnipeg circle. On the island, the two could see and hear the search but without fire or lights had no way to signal the aircraft... Not long after the search resumed, Beck was peering out the chopper's window when he spotted Hassan's bright blue jacket. He was waving his arms on a high spot on the island. NWT News/North

'I want to change my life'
Lanny Stewart says one of the hardest things about being lost in the bush for nearly a week was hearing helicopters flying overhead looking for him - and then hearing them fly away. The 37-year-old Fort McPherson man was lost in the wilderness from Sept. 5 to Sept. 10... He was wearing a hoodie and jacket, jeans, a ball cap and boots. Stewart told his hunting companions that he would be back by about supper time that evening, but he didn't return. His friends searched for him through the night and called the RCMP early the next morning... A search and rescue helicopter saw his fire and landed.
He was flown back to to camp after declining medical assistance. Though his ordeal didn't cause any lasting physical damage, Stewart said it has impacted him mentally... Stewart said he is grateful to everyone who participated in his search, which was comprised of members from the Civil Aviation Search and Rescue (CASARA), Canadian Helicopters, Gwich'in Helicopters and North-Wright Airways, in addition to Fort McPherson residents, search and rescue workers and hunters at James Creek Camp. NWT News/North

Winter gifts to Resolute
Children in Resolute will have new books, winter clothes and sports equipment this winter, thanks to a donation from a Grade 12 class at an Ontario high school. The Civil Air Search and Rescue Association (CASARA) delivered 1,000 lbs. of goods Oct. 4. Mayor Ross Pudluk accepted the gift at a presentation ceremony at the Kenn Borek hangar. NWT News/North

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CSIS, Bill C-51 and Canada's growing metadata collection mess
An opinion piece states, “Much has been made over whether the Canadian Security Intelligence Service, Canada's spy agency, should be armed with broader powers to "disrupt" what it perceives as terrorist plots. A report tabled this month by the Security Intelligence Review Committee, which watches over CSIS's work, notes that while the spy agency hasn't abused its new powers of disruption, its bulk data collection program needs to be scaled back. It's easy to think of CSIS and other spy agencies as shadowy organizations that carry out James Bond-like "missions" involving cool gadgets and high-tech weaponry, but the Snowden leaks, among other revelations, have shown the public that metadata collection (online communications, phone logs and other electronic exchanges that can be intercepted in

enormous amounts) now constitutes the state's primary instrument of control. Privacy Commissioner Daniel Therrien recently called upon legislators (the Liberals in particular) to amend certain aspects of Canada's national security laws in order to address the issue of metadata collection..." CBC News

Survivre à la prison d'Evin
C'était à la fin du mois d'août. L'anthropologue montréalaise, qui était détenue depuis le 6 juin dans la prison même où la photojournaliste canado-iranienne Zahra Kazemi avait été torturée à mort en 2003, souffrait alors d'une infection aux poumons et de sévères problèmes respiratoires. Sa maladie auto-immune (la myasthénie grave) et le manque de sommeil - elle dormait à peine deux heures par nuit - la rendaient de plus en plus faible. « Il n'y avait pas assez d'air dans ma cellule », raconte-t-elle... Pour survivre à la prison d'Evin, Homa Hoodfar devait rester forte moralement, quitte à souffrir davantage sur le plan physique. Ses geôliers avaient déjà tenté de la briser et de l'intimider en utilisant toutes sortes de techniques de torture psychologique. La Press

Nightmare in notorious Egyptian prison
When the Arab Spring came to Egypt in 2011, Khaled Al-Qazzaz was full of hope for the country's future. Instead, he and his wife, Sarah Attia, were caught up in a three-year nightmare that left them and their four young children struggling to recover from emotional scars - and Al-Qazzaz from serious physical injuries that may require years of rehabilitation. A Canadian permanent resident and University of Toronto engineering graduate, he was arrested while serving as an aide to Egyptian president Mohamed Morsi, who was ousted in a military-backed coup in July 2013. Now back home in Mississauga, 37-year-old Al-Qazzaz recounted the ordeal that continued even after his release without charge in January 2015. Toronto Star, A6

All alone on the West's front
What makes a Canadian join forces fighting in a war zone? The Mounties put that question to Dillon Hillier, 28, after he got back from Iraqi Kurdistan last year. At the time, he had just spent three months fighting alongside factions out to reclaim territory seized by the Islamic State group. Prior to that, Mr. Hillier, the son of rural Ontario MPP Randy Hillier, had spent five relatively uneventful years with the Canadian Forces. He was only getting reacquainted with a workaday life as a civilian when the terror group known as IS - also referred to as ISIS - started capturing swaths of Iraq and Syria. Then, in October, 2014, the Canadian sympathizers of IS killed two Canadian Forces soldiers. Weeks later, Mr. Hillier was on a plane overseas hoping to battle the terror group... Making a name for himself as a new breed of vigilante soldier savvy in social media, he became something of a controversial cause célèbre for publicly encouraging other veterans to join him. Now, comes his memoir, One Soldier. Globe and Mail, A11

E-petition condemning all forms of Islamophobia attracts highest number of signatures in a year, fails to receive unanimous House consent
Rookie Liberal MP Frank Baylis's e-petition condemning all forms of Islamophobia in the country failed to receive unanimous consent in the House last week, despite having garnered the highest number of signatures of any e-petition on the parliamentary website since the e-petition system began last year. The non-partisan e-petition, numbered 411 and sponsored by Mr. Baylis (Pierrefonds-Dollard, Que.), opened up for signatures on June 8 and closed Oct. 6. In total 70,317 Canadians signed the petition. The petition received support from Canadians across the country, but most came from Ontario, Quebec, and Alberta... Meanwhile, Mr. Baylis' e-petition calls upon the House of Commons to join Canadians in condemning all forms of Islamophobia. "We, the undersigned, citizens and residents of Canada, call upon the House of Commons to join us in recognizing that extremist individuals do not represent the religion of Islam, and in condemning all forms of Islamophobia," reads the last part of the 179-word-long petition... The petition says that a small number of extremist individuals have undertaken terrorist activities in the name of Islam, which has caused anti-Muslim sentiments in Canada. But these individuals do not speak for Islam, the petition says... On Wednesday, NDP Leader Tom Mulcair (Outremont, Que.) rose in the House to seek unanimous consent in the Commons but failed. It was an oral vote, and the Speaker heard at least one MP or more opposing it. Liberal and NDP MPs say some Conservative MPs opposed it but did not know who. Hill Times

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

HIS DYING WISH IS TO LEAVE THE PSYCH WARD

Facing deportation is the least of Hassan Ason Mazinani's problems. Three years ago, the 42-year-old refugee from Iran was diagnosed with the debilitating and usually fatal Lou Gehrig's disease. In despair, he says he made three failed suicide attempts before being admitted to the psychiatric ward at St. Michael's Hospital. Three years later, he's still on the ward - and his dying wish is to get out... Mazinani has had several run-ins with the law over the years, including convictions for possession of narcotics, drug trafficking and firearms charges between 1993 and 2007. He was ordered deported in 2000 and later immigration officials twice assessed him and deemed him a danger to the public, in 2002 and 2008, according to the Canada Border Services Agency. However, he cannot be removed from Canada because Tehran has refused to issue him a travel document. A CBSA spokesperson confirmed Mazinani is still under a removal order but stressed he is not being detained under the Immigration and Refugee Protection Act... Ottawa does cover the health care of refugees, failed refugees and migrants facing removal like Mazinani under its interim federal health program. However, the federal program only covers medical expenses and losing OHIP will put his access to a long-term care facility in jeopardy. A homeless shelter may now be the only option for him if he leaves the hospital. Toronto Star

The Great Debates: advisory groups and a new NAFTA

An interview between the Hill Times and Patrick Leblond, Senior Fellow at the Centre for International Governance Innovation at the University of Ottawa states, "Our experts go head-to-head to debate two hot topics: the probable renegotiation of NAFTA and the high number of consultations being undertaken by the Liberal government. Q: Would a renegotiation of NAFTA be a blow to Canada's economy or an opportunity to make improvements? [A]... Since the 9/11 attacks, there have been calls in Canada to deepen NAFTA through a grand bargain: deeper trade integration with the U.S. in return for more security in Canada. This logic led to the Security and Prosperity Partnership (SPP), agreed to in Waco, Texas in 2005 by then-Prime Minister Paul Martin, U.S. President George W. Bush and Mexican President Vicente Fox. Unfortunately, the SPP was quietly abandoned five years later, owing in large part to insufficient political support from former Prime Minister Stephen Harper and U.S. President Barack Obama. Instead of a trilateral approach to North American economic and security collaboration, a double bilateral one was adopted. For instance, in 2011, Canada and the U.S. negotiated a Beyond the Border agreement that aimed to make the border both more secure and more fluid in order to facilitate trade between the two countries. Mexico and the U.S. negotiated a similar agreement. Although welcome, given that the border had become "thicker" since the 9/11 attacks, these new measures were much less ambitious than the SPP. Moreover, they did not amount to a modernization of NAFTA. They were administrative in nature and targeted a very specific, even if crucial, issue: border security and fluidity. Hill Times

Dion's candour

An opinion piece states, "The successive visits of Prime Minister Justin Trudeau to China and Premier Li Keqiang to Ottawa in September carried some overtones of naiveté on Canada's part - perhaps most notably, the agreement to begin negotiations toward an bilateral extradition treaty, with an apparent emphasis on supposed economic crimes of Chinese citizens to be shipped back to China.So it is reassuring, and indeed encouraging, that Foreign Affairs Minister Stéphane Dion answered questions in late September about Tibet with considerable candour..." Globe and Mail, A8

The softwood war is poised to reignite

Canada and the United States are about to find themselves in a very familiar place - quarrelling over softwood lumber. The U.S. lumber industry will be in a legal position to file a potentially damaging trade case against Canada at midnight Oct. 12, when a decade-long truce between the countries ends. If the United States launches a challenge - as widely expected - Canada and the United States will be locked in a lumber trade war for the fifth time since the 1980s. Globe and Mail, B1

Angus Reid's survey actually shows high level of support for our diverse society

An opinion piece states, "Much is being made of a new Angus Reid poll on the attitudes of Canadians towards minorities, coming out as it does on the heels of Kellie Leitch's plan to test immigrants on "anti-

Canadian" values. Polling people's attitudes on diversity is always a good thing as the mood does change from time to time, depending on the issues that face us… There were two sets of questions on diversity in the poll. Interestingly, the first did not receive coverage-not even in Reid's own article on the CBC News website-while the second, the more sensational one, garnered all the coverage. Surprising! Respondents were asked to first comment on: "How well immigrants are integrating into society." A full 67 per cent said they were satisfied and 33 per cent said they were dissatisfied. (The report does not reveal how many had no opinion, which seems odd. Not even one per cent? But I digress.) This is a good news story, no? Two to one, Canadians believe immigrants are integrating well. Not many government policies or societal trends get that kind of support…" Hill Times; Toronto Star

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Cold case leads police to alleged Sask. grow-op
The case of a missing Edmonton doctor led police recently to an alleged marijuana grow-op east of Regina. Dr. Patrick Cyril Thauberger, a 53-year-old clinical psychologist with a doctorate in pharmacology, was on leave from his job when he disappeared on Sept. 3, 1997… As the unsolved file grew older, it eventually became what's termed a "cold case." The Regina Police Service has continued to investigate and, recently, that investigation reportedly led investigators to what was described as a large, outdoor marijuana grow-op in the RMs of Indian Head and South Qu'Appelle. The grow-op reportedly contained more than 300 plants, police reported. A news release from the RPS indicated the grow-op was discovered by its members, along with members of the RCMP, during the execution of a search warrant under the Controlled Drugs and Substances Act. Although police didn't provide additional details, the release said the warrant "was obtained as part of the investigation" into the Thauberger case. Postmedia News (Leader-Post)

Pesky drone annoys people in Oakbank, but RCMP can do little to stop buzz
Curt Danners couldn't believe it when a drone buzzed by him in his backyard while he was cleaning his pool recently. The wind generated by the propellers fanned down on him, and it wasn't the first time. A week earlier, Danners and his wife were coming home from work when he got out of his car in the garage and spotted the device for the first time… People in Oakbank have been complaining on social media about a persistent drone that has been flying very close to people's homes since the end of September. The City of Winnipeg is considering a bylaw to regulate the use and the sale of drones… Danners said RCMP told him and other neighbours there is little they can do. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Patrick Côté a eu un poumon perforé
Patrick Coté, cet ancien joueur de la Ligue nationale de hockey (LNH) qui a été blessé par balle jeudi, au pénitencier de Donnacona, a eu un poumon perforé. Selon son père, Gilles Côté, l'ex-joueur de hockey serait maintenu dans un coma artificiel, mais on ne craint pas pour sa vie. « Ils lui ont tiré dans le dos. La balle a performé son poumon », a déclaré Gilles Côté à Radio-Canada en entrevue téléphonique. Le père du prisonnier déplore n'avoir recu aucune information du pénitenicer. Il a finalement obtenu des informations de l'Hôpital de l'Enfant-Jésus. Patrick Côté a été gravement blessé jeudi soir lors d'une violente bagarre avec un autre détenu de la prison de Donnacona Incapables de le maîtriser, les agents correctionnels ont utilisé du gaz irritant, sans succès, avant de tirer des coups de semonce avec leurs armes de service. Un des gardiens l'aurait finalement atteint d'un tir pour le neutraliser. Radio Canada

Songs for women prisoners

Nancy Gallant of Cole Harbour is a passionate ministry worker and speaker, and she made correctional and local music history Oct. 4 as the first musician to hold a CD release party inside a federal prison... The idea stemmed from her work with Royce Harris of Daybreak Prison Ministry and was inspired after six years of monthly musical and biblical counsel, song, and discussion with inmates at Truro's Nova Institution for Women. Her motives are simple: to give hope and peace to those confined - and defined - by the walls of the prison they find themselves in. Chronicle Herald

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Search for slain teen Cooper Nemeth inspires Winnipeg homeless initiative
The family of slain 17-year-old Cooper Nemeth is giving back to a Winnipeg street patrol group that played a significant role in searching for the teen in February — and brought together Indigenous and non-Indigenous communities in the process. The Nemeth Initiative is supplying Bear Clan Patrol with care packs for community members in need that they come across. The goal of the initiative is to give people on the streets hope and keep Cooper Nemeth's spirit alive. Nemeth, 17, was found dead on Feb. 20, 2016, after a high-profile six-day search for the teen. Nicholas Bell-Wright was charged with second-degree murder in the case. Police have said the incident was drug-related. CBC News

Province, police want help cracking down on crimes involving illegal tobacco
Crime Stoppers and the Department of Public Safety want the public's help to stop crimes involving illegal tobacco. New Brunswickers are asked to report anything involving the use, sale, transportation, and distribution of tobacco that's not purchased from a licensed retailer. Times & Transcript, A10

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Shepherds of Good Hope launches fundraising appeal to help Pootoogook's brother attend her Nunavut funeral
The Shepherds of Good Hope has launched a fundraising appeal to help the brother of renowned Inuit artist Annie Pootoogook with the purchase of a plane ticket to attend her burial... Pootoogook's body was in the hands of the Ontario's Coroner's Office until a few days ago as Ottawa police continue to investigate her death as suspicious. Ottawa Citizen

Walk for murdered, missing women ends awareness week
A 5-kilometre walk for murdered and missing indigenous women has wrapped up an awareness week aimed at educating and engaging people across the country. Wolastoqiyik Sisters in Spirit hosted the awareness events throughout the week, which included a vigil, poetry slam and panel discussion, along with Saturday's walk... Among Saturday's runners was Brad Firth, also known as Caribou Legs, who is currently finishing his cross-Canada marathon in support of missing and murdered women. Telegraph Journal, A5

It's Canada's time to lead on women's rights at home, abroad
An opinion piece states, “Maybe it takes a rock star to remind us of who we are as Canadians and what we are capable of. At the recent meeting of the Global Fund to fight AIDS, tuberculosis and malaria, U2 lead singer Bono declared "the world needs more Canada." These words were spoken at an urgent time for many of the world's women and girls, and while laudatory, should be taken as a challenge to our nation to do more to help end gender inequality and violence. The attention being afforded Canada must be used wisely. We should leverage this moment to do three things: Lead by example. Income equality, sexual violence, and gender discrimination are not foreign ills. They infect Canada too. We need look no further than our shamefully delayed response to missing and murdered indigenous women. We are taking

action now, but from how we treat survivors of sexual assault to female representation in government and on corporate boards, Canada can do more..." Hill Times

Senator dishonours Inuit experience
An opinion piece states, "Nunavut's only Senator seems to have forgotten the people he is representing in Ottawa. In a Sept. 21 opinion piece for the National Observer, Senator Dennis Patterson said "racism ... is motivating Pauktuutit, Canada's national Inuit women's association, and the Qulliit Nunavut Status of Women Council to condemn" the choice of an Iglulik-born non-Inuk woman, Qajaq Robinson, as a commissioner to the inquiry into Missing and Murdered Indigenous Women and Girls. We do not doubt that Robinson is qualified for the role. A graduate of Nunavut's Akitsiraq Law School, Robinson is a successful lawyer in Ottawa and her Inuk husband is an RCMP officer on Parliament Hill. She speaks Inuktitut and Patterson points to her work defending the interests of indigenous people. The problem is not with the appointee, but with Sen. Patterson's belief that he is right to question Pauktuutit's and Qulliit's motives. They are right to want an Inuk commissioner. The four other commissioners are indigenous: a judge from the Mistawasis First Nation in Saskatchewan; a former Quebec deputy minister and activist from the Innu community of Mani Utenam; a Metis law professor - who taught at Akitsiraq - from Saskatchewan; and a First Nations lawyer from Ontario..." NWT News/North

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

All you need to know about marijuana legalization in Canada
An opinion piece states, "...Welcome to the world of marijuana spot checks, a hypothetical place that may soon become a reality in Canada... But we do know the RCMP confirmed this spring that it planned on field testing oral fluid screening devices similar to breathalyzers-which could detect marijuana-at roadside stops. Plus, a new handheld device has been developed at the University of British Columbia that can detect the primary ingredient of marijuana in the breath up to 12 hours after consumption. Lastly, the Liberals under Prime Minister Justin Trudeau, who have promised to introduce a bill to legalize and regulate maryjane next spring, said in their election platform they would "create new, stronger laws to punish more severely those who...operate a motor vehicle while under [marijuana's] influence." So the elements are all there... A related issue for legalization is deciding which places in Canada should be 420 friendly, and which should ban the bud... Along with where it should be smoked, there's also the questions of private cultivation and commercial sales. In Canada's most populous province, stars seem to be aligning in favour of Ontario Premier Kathleen Wynne's plan. She has been planting the seeds for months, trying to grow the idea in Ontarians' minds that the LCBO, the Crown corporation that sells booze across the province, would be the natural place to sell marijuana...Not everyone agrees. The head of the largest food retailer in Canada, Loblaw Companies, which also owns Canada's largest pharmacy chain Shoppers Drug Mart, wants to sell marijuana through its pharmacies... Still, others think legalized marijuana shouldn't be sold in storefronts at all, rather that it should replicate the existing medical marijuana regime by allowing Canadians to order their weed directly from licensed producers and have it delivered to them through the mail... With any of these systems, there is still the question of whether individual Canadians will be allowed to grow their own..." Hill Times

College should wait for clarity
An opinion piece states, "Even if the New Brunswick Community College network is an arm's-length provincial government learning institution, it appears ready to join with the rest of New Brunswick government groupthink in embracing reefer madness. The French sector of the community college system is ready to offer specialized training in marijuana production, even if some of the basic skills needed for marijuana cultivation (such as growing crops, or laboratory analysis) are already offered in public institutions in the region. Let's refrain from further inflation of the speculative New Brunswick marijuana bubble - because if we don't stop, taxpayers will have a real hangover when it eventually pops..." Telegraph-Journal, A6

LE CANADA POURRAIT S'INSPIRER DE LA SUISSE
Substance psychoactive la plus consommée au monde, le cannabis fait l'objet de débats depuis des années dans la Confédération helvétique. En 2008, la proposition de dépénaliser la marijuana a été

rejetée par 63% de la population lors d'un référendum. Presque 10 ans plus tard, la question revient sur la table. «Le problème qu'on a aujourd'hui est que dans la mesure où le cannabis est illégal, on a quand même 600 à 700000 personnes dans notre pays qui, chaque année, en fument. Et on ne sait pas exactement ce qu'ils consomment», statue Alain Berset, ministre de la Santé en Suisse. D'où l'initiative des villes de Berne et de Genève, qui ont mandaté des chercheurs universitaires afin d'élaborer des projets pilotes qui pourraient permettre une vente ou une remise légale de cannabis. La Presse (Journal de Québec, 6; Journal de Montréal)

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

Refugees take in Caliph talk after fleeing persecution
Hundreds of refugees from Syria were able to experience religious freedom for the first time in years as they gathered at a conference of 25,000 Ahmadiyya Muslims in Mississauga this weekend. Wissam Alburaki, 41, brought his wife and three children to Canada as refugees last month, landing in Calgary by way of Kuwait and Dubai. And while Calgary is where his family intends to stay, Alburaki was west of Toronto over the weekend, attending Canada's Jalsa Salana - an annual meeting of the Ahmadiyya Muslim Jama'at. He was one of hundreds of Syrian refugees attending the conference, according to Safwan Choudhry, a spokesperson for the Canadian chapter of the group... And this year marks the 40th anniversary of the convention in Canada, which was attended by the community's spiritual leader, Caliph Hazrat Mirza Masroor Ahmad, who is from Pakistan. Canadian Press (Toronto Star, Chronicle Herald); Globe and Mail; CBC News

Admit it. Canadian troops in Iraq aren't just advising. They're fighting
An opinion piece states, "It has always been a myth that Canada's soldiers in Iraq don't do combat. Now the myth is even harder to sustain. On Thursday, a senior general acknowledged that, over the last few months, Canadian special forces operating in northern Iraq have become increasingly involved in front-line skirmishes against Daesh fighters. "The mission has changed," said Brig.-Gen. Peter Dawe. "We are more engaged on the line ... the risk has increased.'" Toronto Star

INTERNATIONAL

One man in custody as part of manhunt for German bomb plot suspect
German police searched nationwide Sunday for a 22-year-old Syrian man believed to have been preparing a bombing attack, who slipped through their fingers as they were closing in on him, and were questioning a second Syrian man on suspicion he was involved in the plot. The man in custody was one of three apprehended in the eastern city of Chemnitz on Saturday. He was the renter of the apartment that police raided in their search for the main suspect, Jaber Albakr from the Damascus area of Syria, Saxony police spokesman Tom Bernhardt told The Associated Press. The other two men have been released... The raid came after Saxony police were given a tip from Germany's domestic intelligence service that Albakr may be planning an attack. He had been on the agency's radar, but Bernhardt said it was not clear how long. German media have reported that Albakr is believed to be connected to Islamic extremist groups, but Saxony police have not commented on his possible motivation or the bomb plot's target. Federal police have increased security around the country, particularly around "critical infrastructure" like train stations and airports, as authorities search for Albakr. Associated Press (Times & Transcript, Yahoo)

Matthew downgraded, but still dangerous

When Hurricane Matthew dumped torrential rains on North Carolina, thousands of people found themselves suddenly trapped in homes and cars. Rescuers in Coast Guard helicopters plucked some of them from rooftops and used military vehicles to reach others, including a woman who held onto a tree for three hours after her car was overrun by floodwaters. The storm killed more than 500 people in Haiti and at least 17 in the U.S. - nearly half of them in North Carolina. Gov. Pat McCrory said authorities were searching for five people and feared they may find more victims. The problems were far from over as all that rain - more than 30 centimetres in places - flows into rivers and downstream, likely causing days of flooding in many of the same places devastated by a similar deluge from Hurricane Floyd in 1999. "Hurricane Matthew is off the map. But it is still with us. And it is still deadly," McCrory said. More than a million people in South Carolina and North Carolina were without power, and at least four separate sections of Interstate 95 - the main artery linking the East Coast from Florida to Maine - were closed in North Carolina. Reuters (Toronto Star, A2)

Bellingham, Wash. airport evacuation called off

An evacuation at the Bellingham International Airport in Washington state has been called off. Bellingham police said a piece of luggage that had tested positive for explosives was empty. Police deployed a bomb robot to X-ray the suitcase shortly after it was reported about 3 p.m. PT. on Sunday. CBC News

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 5, 2016 / le 5 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Feds to review CSIS powers in the digital age
A federal review of national security will consider whether Canada's spy service should be able to sift through the kind of personal data it kept illegally for years, says **Public Safety Minister Ralph Goodale**. **Goodale** said Friday the notion that the Canadian Security Intelligence Service should avoid stashing away information about innocent people is a ***"fundamental principle of Canadian privacy."*** But **the minister** appeared to leave the door open to one day giving CSIS the legal authority to keep and analyze electronic data about individuals who do not pose a security threat. ***"I want to hear the professional advice on both sides,"*** **Goodale** told a news conference in the foyer of the House of Commons. ***"I'm not pre-empting the consultation."***... **Goodale said** he became aware of the ***"full scope of the issue"*** when the court judgment was made available to him in preliminary form a couple of weeks ago. **He said he took** the immediate step of informing the Security Intelligence Review Committee, the watchdog over

CSIS, and asked the review committee to supervise management of the data and ensure full compliance with the judgment. Coulombe ***"understands my expectations here,"*** **Goodale added.** ***"A serious error has been made. This situation needs to be remedied. It has to be remedied quickly."*** The NDP said Friday the revelations underscore the need for stronger parliamentary oversight. Canadian Press (Cape Breton Post, A10; The Telegram, Chronicle Herald, Red Deer Advocate, Charlottetown Guardian, Whig-Standard, Edmonton Sun, Calgary Sun, Times Colonist, Hamilton Spectator, Times Colonist, The Record, iPolitics, Times & Transcript, Daily Gleaner); Presse Canadienne (Le Droit, 21 ; Le Devoir, L'Acadie Nouvelle)

Espionnage de journalistes - Ottawa ferme les yeux sur le passé
Aucun journaliste n'est actuellement surveillé par la GRC et le SCRS... mais Ottawa n'a pas idée si cette situation a pu se produire dans un passé récent. **Le ministre de la Sécurité publique, Ralph Goodale**, ne l'a pas demandé. Et **il n'a pas** l'intention de le faire : c'est le présent qui compte, dit-il. **Pour M. Goodale,** ***" la question porte sur ce qui se passe maintenant et nous pouvons offrir l'assurance que ce genre d'activité n'a pas lieu. Je ne sais rien sur les événements qui se sont produits lorsque nous [les libéraux] ne formions pas le gouvernement "***, **a indiqué le ministre** en point de presse. Questionné à savoir s'il demanderait directement au patron du Service canadien du renseignement de sécurité (SCRS) si des mandats de surveillance ont pu être lancés dans les cinq dernières années, **Ralph Goodale** a répondu que c'était précisément la ***" responsabilité du directeur de répondre aux questions opérationnelles "***... Lors de la période de questions, **M. Goodale a indiqué** trouver ***" très inquiétantes "*** les révélations qui ont marqué la semaine au Québec -- l'espionnage de plusieurs journalistes par le Service de police de la Ville de Montréal (SPVM) ou la Sûreté du Québec (SQ). Le Devoir, A7

Advocates urge Liberal government to reduce number of women in prison
Sometimes when she goes to the grocery store, all Alia Pierini can do is sit in the parking lot, unable to bear the idea of going inside. She tries a different store, but Pierini, 31, often ends up coming home without the food she had planned to buy for lunch. "I feel like a big loser, to be honest, but I can't help it," the former prisoner told a news conference Thursday as she described the lingering anxiety, panic and fear she still feels as a result of months spent alone in solitary confinement... Now a regional advocate for female prisoners in federal custody, Pierini joined the Canadian Association of Elizabeth Fry Societies, which provides support for women and girls in the justice system, in calling on the Liberal government to reduce the number of women behind bars. The association's longtime executive director, Kim Pate - newly recommended for the Senate by Prime Minister Justin Trudeau - urged the government to give judges the discretion to overturn or alter the mandatory minimum sentences brought in by the previous Conservative government... Pate also said she was "heartened" to see Justice Minister Jody Wilson-Raybould given a mandate to restrict the use of solitary confinement and improve the treatment of prisoners with mental illness by implementing recommendations from the Ashley Smith inquest... **Public Safety Minister Ralph Goodale**, who is working with Wilson-Raybould on reviewing the inquest recommendations, has said that when it comes to administrative segregation, the government is looking at reforms that touch on everything from policy and programs to physical infrastructure and hopes to have specific proposals sometime this winter. ***"We need to dramatically change the scenario, and we're working at that,"*** **Goodale said** last week. Daily Star, 25

Spies could be left out in the cold
" Trust, but verify ." Academics Craig Forcese and Kent Roach argue that this should be the maxim in the security sector when dealing with powerful state agencies like the Canadian Security Intelligence Service and the RCMP. But trust in Canada ' s security services is thin on the ground, after the news Thursday that a CSIS unit illegally kept data deemed unrelated to national security threats. **Public Safety Minister Ralph Goodale said** Friday that a Federal Court decision by Justice Simon Noel, who found CSIS has ***"breached, again, the duty of candour it owes the court,"*** is timely because the Liberals are in the midst of reviewing the national security laws... Even before that, both Mosley and Noel had lambasted CSIS for providing inaccurate information to the court. In the Mohamed Harkat case, Noel criticized the agency ' s lack of candour... **Yet Goodale** did not rule out a change to the law to allow CSIS to keep the information ruled offside by the court. "***This is an issue that I think needs to be examined in the context of our national security review,"*** **he said**. ***"I want to hear the professional advice on both***

sides...Our security agencies to be effective in keeping Canadians safe. At the same time, what the agencies do needs to be in accord with the law and with the Constitution." Phil Gurski, a former CSIS analyst, said the metadata were retained for a rea-son - to identify people involved with, or sympathetic to, terror groups. Postmedia News (London Free Press, N6; Vancouver Sun, Calgary Herald, Leader-Post, Montreal Gazette, The Record, Ottawa Citizen, National Post)

Feds to look at border-crossing challenges for First Nations
The federal government will appoint a special ministerial representative to look at border crossing issues faced by First Nations. In a joint letter written in response to a Senate committee study, Indigenous Affairs Minister Carolyn Bennett, Immigration Minister John McCallum and **Public Safety Minister Ralph Goodale** say the adviser and First Nations will discuss significant and complex challenges. The letter said the resolution of these issues will require a ***"horizontal approach"*** involving several departments and agencies. ***"This will be necessary in order for the government of Canada to arrive at workable and sustainable solutions that facilitate the ability of First Nation community members to cross the U.S.-Canada border and, at the same time, take into consideration issues such as status, international sovereignty and security,"*** it said. Canadian Press (Whig-Standard, B2; Daily Gleaner, Telegraph-Journal, Times & Transcript)

Spy watchdog that triggered scathing rebuke of illegal CSIS activities facing job cuts
The federal watchdog that triggered this week's scathing judicial rebuke of Canada's spy service for illegal activities faces significant job cuts because of a chronic lack of sustained government funding, even as the Liberals hinted Friday the agency could be asked to do more to police federal spies. The Security Intelligence Review Committee (SIRC), the independent agency that reports to Parliament on the operations of the Canadian Security Intelligence Service (CSIS), says the equivalent of at least 11 full-time positions will disappear March 31 unless the Liberal government delivers millions more dollars under a sustained, multi-year funding plan announced by the previous Conservative government. "We don't know if we're getting any more funding," SIRC spokeswoman Sabrine Barakat said Friday. "SIRC has been actively working to access that money on a permanent basis but we're still waiting to see." The government has offered no explanation, she said. **The office of Public Safety Minister Ralph Goodale was unable** Friday to explain the funding confusion. Treasury Board officials could not explain either when asked the same question by the Ottawa Citizen last March... **Goodale repeated the pledge** for robust oversight again Friday in the swirling aftermath of the Federal Court ruling that CSIS illegally retained a decade's worth of metadata gleaned from Canadians' electronic communications that had nothing to do with threats to national security. Questions about the activity were first raised by SIRC in its 2014-15 annual report... Speaking with reporters, **Goodale said** the length of time it took for the decade of CSIS metadata misconduct to surface is of ***"critical concern."***... Paul Cavalluzzo, counsel for the Maher Arar commission, said SIRC is not in a position to adequately deal with CSIS. National Post (2016-11-04); Postmedia Network (London Free Press, N6; Calgary Herald, Vancouver Sun, Leader-Post, Montreal Gazette, Ottawa Citizen)

Watchdog defends CSIS, its director
Michel Coulombe, Canada's top spy, is in deep trouble with the courts and his political boss, **Public Safety Minister Ralph Goodale**, over revelations CSIS kept a decade's worth of data on Canadians who are no threat to national security. But Pierre Blais, head of the civilian watchdog agency over CSIS, says Coulombe "acted in good faith" and should not lose his job over the affair... Still, the judge said CSIS breached its "duty of candour" when it failed to reveal what it was up to. Goodale said Friday the first he learned of it was two weeks ago when an unredacted copy of the pending judgment reached his desk. Asked if he still has confidence in Coulombe, **Goodale said** only that he has made his expectations to the director clear. ***"A serious error has been made. (Coulombe) maintains that in his view, and in the view of the advice he got from the Department of Justice over the course of the last number of years, that the course of conduct by CSIS was within the parameters of law,"*** **Goodale told** reporters. ***"The court has now said very clearly and unequivocally that it was not. This situation needs to be remedied. It has to be remedied quickly ... CSIS must be forthcoming and candid with the court. That will happen."***... **But Goodale** was adamant Friday that innocent people should not have their information tracked and stored by Canada's spies. ***"That's a fundamental principle of Canadian privacy,"*** **he said.** Toronto Star, A10

Pas d'assurances pour le passé à Ottawa
S'il a obtenu l'assurance qu'aucune surveillance de journalistes ne se produit «actuellement» au niveau fédéral, le gouvernement Trudeau n'a pas demandé à la Gendarmerie royale du Canada (GRC) et au Service canadien du renseignement de sécurité (SCRS) s'ils ont mis des journalistes sous surveillance au cours des cinq dernières années. ***«L'enjeu, c'est ce qui se passe maintenant et nous pouvons offrir l'assurance que ce genre d'activités ne se produit pas actuellement. Je n'ai pas connaissance de choses qui se sont produites quand nous ne formions pas le gouvernement du Canada»*, a dit le ministre Ralph Goodale**, qui n'a pas l'intention de demander à la GRC ou au SCRS si des mandats de surveillance ont été lancés à l'égard de journalistes au cours des cinq dernières années. ***«La réponse, autant de la GRC que du SCRS, est que rien de la sorte ne se produit actuellement. [...] C'est la responsabilité du directeur du SCRS de répondre aux questions opérationnelles. Vous allez sur une pente très dangereuse quand vous invitez les politiciens à aller dans ce domaine»,* dit le ministre Goodale.** La Presse, A12

Minister vows action on CSIS
Public Safety Minister Ralph Goodale says he will make sure Canada's spy agency takes action after a Federal Court found that its officials have misled justices and unlawfully amassed data about people not suspected of being threats... On Friday, **Mr. Goodale said he** intends to ensure that CSIS follows the Federal Court's directive to stop the controversial practices. Pressed on whether he plans to fire anyone now, **Mr. Goodale said** only that **he** wants to have words with CSIS officials. ***"I will discuss with the executive management of the service how they plan to respond to this judgment,"* he said**. **The minister told** reporters that CSIS director Michel Coulombe has told him that CSIS lacks records that indicate whether it briefed previous ministers on the programs. ***"I take that as a pretty serious defect in the record keeping of the organization. "That is one of the things that absolutely needs to be rectified," he said***. Globe and Mail, A9

It's not easy being a journalist's unnamed source in the Information Age
An opinion piece states, "Were I in a position of authority, I would probably hang up if contacted by a journalist. Not because I don't think people in positions of authority should speak to journalists - I do, and I'm grateful to all the people in positions of authority who haven't hung up on me over the years... In Canada, Mounties investigating a document leak have targeted journalists, and last week, reporters at La Presse in Montreal and at Radio-Canada discovered Quebec police, hunting for leakers in their own ranks, have been tracking and tapping their communications. (We have no idea how many other journalists have been surveilled, but it's safe to assume it happens.)... Glenn Cowan, GRA Quantum's Canadian CEO, says such software allows phone, video or email communication without leaving any record: no metadata, no communications link to analyze, no tracking log, nothing... Cowan stresses that his firm does not regard law enforcement as a "threat actor," to use the language employed by the super-secret Communications Security Establishment in its advice to government employees on how to protect their communications..." CBC News

The worst part about the spying spree - it was legal
An opinion piece states, "Connect the dots between Quebec's police corps and the half-dozen or more investigative journalists who were put under surveillance over the past decade and you will find a gaggle of judges potentially derelict in their gatekeeping duties. In each of the spying episodes that have come to light over the past week, the police had to convince a judge to sanction the surveillance and, in some cases, to do so more than once..." Toronto Star

Spying eyes
An editorial states, "Taken in isolation, either case is concerning. But this week, we actually had two major law enforcement misconduct issues surface. The Canadian Security Intelligence Service, it turns out, has been collecting unrelated information it received as part of terrorism investigations (and was supposed to destroy), and instead loaded it into database systems that its legal overseers weren't even told existed. Meanwhile, in Quebec, police services were tracking some reporters' calls and texts for periods as long as five years, in an effort to catch and punish police whistleblowers. There's a huge problem here. And it's an oversight problem..." The Telegram, A15

Clean up spy agency
An editorial states, "So, Canada's spy agency has gobs of people's metadata in a secret database. Well, it's just numbers, isn't it? You know, telephone numbers and Internet IP addresses and so forth. Who cares? The justice system, to begin with. On Thursday, the Federal Court released a ruling saying that the Canadian Security Intelligence Service's retention and analysis of wide swaths of data, which had been going on for 10 years, was illegal. And CSIS hadn't bothered to inform the court of what it was doing... **Public Safety Minister Ralph Goodale was shifty** on Friday when asked if the Liberals' planned security oversight committee would have stopped this sort of spying; instead he repeated talking points. **He also refused** to say how many Canadians had their data captured. Reassuringly, though, the government won't appeal the court ruling..." Ottawa Citizen, B5

Surveillance des journalistes - La nouvelle chasse aux sorcières
Un article d'opinion déclare, « Le professeur Stéphane Leman-Langlois est un spécialiste de la police, du renseignement, du terrorisme, des technologies et du contrôle social. Il a récemment collaboré au livre "Transparent Lives" sur la surveillance au Canada. Il enseigne à l'Université Laval.\r\nAvez-vous été surpris par les récentes révélations sur l'ampleur de l'espionnage des journalistes québécois ? Pas du tout. Chaque fois que je parle de surveillance depuis des années et que je dis aux journalistes qu'ils sont les premières cibles, la plupart d'entre eux lèvent les yeux au plafond parce qu'ils n'y croient pas. Ils me traitent de parano parce que je suis dans les études de la surveillance. Je suis certain que le phénomène est d'une ampleur bien supérieure à ce qui vient d'être dévoilé. Je pense que les révélations de la SQ -- arrivées très, très rapidement et concernant, comme par hasard, des écoutes datant d'anciens directeurs de ce corps de police -- sont faites pour détourner l'attention. Mais bon, il va y avoir une commission d'enquête et, si elle peut lever des pierres, on va en trouver bien plus, de ces histoires de surveillance... » Le Devoir, B1

Surveillance - La confiance ébranlée
Un article d'opinion déclare, « Pendant dix ans, le Service canadien du renseignement de sécurité (SCRS) a conservé et analysé des données associées à des personnes qui n'étaient soupçonnées de rien, mais qui avaient eu le malheur de communiquer avec des personnes légalement surveillées. Et le service l'a fait sans en informer la Cour fédérale, un des rares garde-fous contre d'éventuels abus de nos espions. Le gouvernement doit serrer la vis et vite ; la confiance des citoyens et la protection de leur vie privée en dépendent... Le Tribunal rappelle que le SCRS doit, en vertu de la loi, conserver les données uniquement " dans la mesure strictement nécessaire ", ce qui n'était pas le cas. Lors d'une conférence de presse convoquée en toute hâte, le directeur du SCRS, Michel Coulombe, a dit que le service avait cessé toute analyse et verrouillé l'accès aux données en question. **Le ministre de la Sécurité publique, Ralph Goodale**, a précisé que le gouvernement n'interjetterait pas appel et a déploré le manque de franchise du SCRS devant la Cour. Mais ensuite ? La Cour n'a pas demandé de détruire ces données et personne ne sait trop ce qu'on en fera. Le plus préoccupant est que M. Coulombe espère pouvoir les conserver et que **le ministre de la Sécurité publique, Ralph Goodale**, n'a pas fermé la porte. **Il a noté** que cette question serait mieux débattue lors des consultations publiques en cours sur ***" le cadre de sécurité nationale "***. **Le ministre** a d'ailleurs **relevé** que le juge Noël avait suggéré de revoir la loi sur le SCRS et de l'adapter à la réalité des nouvelles technologies... » Le Devoir, B4

TOP STORIES / MANCHETTES

*** Alberni flooding may shut highway for days**
Flooding near Port Alberni has the potential to close Highway 4, the only highway link to Ucluelet and Tofino, for five or six days, says the emergency preparedness co-ordinator of the Tseshaht First Nation. Times Colonist, A1

*** Complaints skyrocket at women's prison**
The number of complaints to the Correctional Investigator from women at the federal women's prison in Kitchener has skyrocketed in the past three years, Correctional Investigator Howard Sapers received 344 complaints from Grand Valley Institution in 2015-16 — about 41 per cent of all complaints from women in federal prisons anywhere in Canada. Of the 45 federal prisons across the country, only one other was the

subject of more complaints. The number of complaints at Grand Valley has increased each year for the past several years, from 144 in 2013, to 193 in 2014, to 218 in 2015 — a 139 per cent increase in three years. "I think the numbers (of complaints) going up is indicative of how desperate some of the women are," said Kim Pate, executive director of the Canadian Association of Elizabeth Fry Societies, who added that her agency has encouraged women to complain more in an effort to get their concerns addressed. The Record, A1

* **Health Canada disputes police story on fentanyl**
Police were alerted by both phone and mail in July that there was liquid fentanyl in Hamilton, says Health Canada. The statement is in direct contradiction to police claims that the vice and drug unit were notified the week of Oct. 31 about the lab results and that they were not physical documents that landed on an officer's desk. Torstar (Hamilton Spectator, A1; The Record)

Pregnant killer Kelly Ellard's boyfriend a 'person of interest' in drug dealer disappearance
The boyfriend of pregnant killer Kelly Ellard is a "person of interest" in the May 2016 disappearance of a low-level drug dealer, according to Parole Board of Canada documents. Darwin Dorozan, 42, had his parole revoked after Correctional Services of Canada officials were made aware of the investigation into the missing dealer, the just-released documents say. "On the same date full parole was granted, police advised CSC that you were a person of interest in the suspicious disappearance of a low-level drug dealer in May 2016," the parole board said in its Oct. 27 ruling...She was denied day parole in May despite the Parole Board of Canada noting that she was finally taking some responsibility for the murder and had made strides in her rehabilitation. Postmedia Network (Edmonton Sun, Ottawa Sun, Calgary Sun, Vancouver Sun, Winnipeg Sun)

Retour sur une semaine sombre pour la liberté de presse
Pour les trois journalistes de Radio-Canada, il s'agit de tous leurs appels de novembre 2008 à octobre 2013, confirme la SQ. Cette procédure ne prévoyait pas d'écoute électronique. La SQ cherchait à faire la lumière sur des fuites d'éléments d'enquête provenant de l'écoute électronique en 2008 et 2009 du président de la Fédération des travailleurs du Québec (FTQ) de l'époque, Michel Arsenault - qui s'est plaint en 2013 de ces divulgations dans les médias... Jeudi, il a dit s'être assuré auprès de la Gendarmerie royale du Canada (GRC) et du Service canadien du renseignement de sécurité (SCRS) que de telles « activités » ne se passent pas « au niveau fédéral ». Rappelons que deux journalistes de La Presse ont été espionnés en 2007 par des agents de la GRC. Radio-Canada

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

* **Climate change: What does it mean for Canada and how can we respond?**
Canada has already seen smoke-related health impacts and stressful evacuations as the result of increased wildfires; the spread of Lyme disease; and food security and mental health challenges related to rapid changes in the Far North, which is two to three degrees Celsius warmer than it was in the 1950s. Here's How Canada's Provinces Are Responding To Climate Change. New Brunswick banned fracking. Last month, lawmakers in New Brunswick voted to place a moratorium on fracking within the province. Canada Journal

* **Alberni flooding may shut highway for days**
Flooding near Port Alberni has the potential to close Highway 4, the only highway link to Ucluelet and Tofino, for five or six days, says the emergency preparedness co-ordinator of the Tseshaht First Nation. Times Colonist, A1

* **Winter gear guide**
El Nino is famous for weather media headlines. But its sister act - La Nina - is known to be pretty frosty and forecasted to slam the Canadian Rockies with a good old-fashioned winter, full of what skiers and snowboarders love, cooler temperatures and above-average moisture. Calgary Herald, G10

* **Tornado-damaged homes still waiting to be repaired**
Some of the of roofs, siding and porches wrecked in just four seconds when a tornado touched down on Riberdy Road Aug. 24 remain unfixed 10 weeks later, and resident Greg Tremblay says he's had enough. Windsor Star, A5

* **Une heure de plus... pour vérifier son détecteur de fumée**
Le changement d'heure, dimanche, est le moment idéal pour faire penser de vérifier son avertisseur de fumée et en remplacer la pile. La remarque vient du Service de protection contre les incendies de la Ville de Sherbrooke. La Tribune, 10

* **CBRM phases out storm help line**
Assistance will continue for residents reeling from October flood. The Cape Breton Regional Municipality shut down its emergency telephone help line for residents affected by the Thanksgiving Day flood. The provincial government issued a news release Friday indicating that while the help line is being phased out, the municipality will follow up with anyone who has called for assistance. Cape Breton Post, A3

* **Les municipalités veulent plus de sécurité**
Le monde municipal n'a pas oublié la tragédie de Lac-Mégantic. Réunis à l'occasion d'une rencontre spéciale à Edmundston au Nouveau-Brunswick vendredi, quelques dizaines de représentants municipaux ont discuté de sécurité ferroviaire en compagnie de divers intervenants. Ils ont réclamé l'adoption d'une série de mesures pour accroître la sécurité des communautés à l'issue de leurs discussions. La Tribune, 9

* **High hopes for Elbow River brown trout after devastating 2013 flood**
River watchers are hoping this year's brown trout count in the Elbow River continues to show growth after the 2013 Alberta flood had a devastating effect on the population. Chris Bjornson, a senior fisheries biologist with Golder Associates, says the flood three years ago continues to affect the population. CBC News

* **Springbank dam raises concerns for environment**
An opinion piece states, "It has now been one year since the Alberta government flip-flopped on its election promise to scrap the Springbank dam project in favour of the McLean Creek dam. I remember watching the news conference - led by the environment minister, flanked by the mayor of Calgary - but with no one there from Springbank, Rocky View County or the impacted First Nations..." Calgary Herald, A13

* **Letters to the Editor**
A letter to the editor states, "Independent probe needed. Husky Energy was supposed to file a major and conclusive report on the disastrous oil spill in the North Saskatchewan River to the provincial government. Instead, it filed a one pager and asked the government for an extension later into November. This request was granted..." StarPhoenix

The beast is still alive
Six months after it sent the population of Fort McMurray fleeing, the wildfire known as MWF-009 is still burning. The fire can no longer be seen; there is no smoke or open flames. But in a remote section of Alberta and Saskatchewan far from the city it nearly destroyed, the blaze is still being carefully watched. Postmedia Network (London Free Press, N5; Windsor Star, Vancouver Sun, Edmonton Journal, Calgary Herald, National Post, Ottawa Citizen)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Attack on a free press a strike against us all**
An opinion piece states, "For some Canadian readers, this column may sound, at best, like an objection worthy of little notice. At worst, it may read like a series of trivial complaints - bellyaching, even - from a journalist with oh-so-precious sensibilities when it comes to press freedoms..." London Free Press, A12

Retour sur une semaine sombre pour la liberté de presse
Pour les trois journalistes de Radio-Canada, il s'agit de tous leurs appels de novembre 2008 à octobre 2013, confirme la SQ. Cette procédure ne prévoyait pas d'écoute électronique. La SQ cherchait à faire la lumière sur des fuites d'éléments d'enquête provenant de l'écoute électronique en 2008 et 2009 du président de la Fédération des travailleurs du Québec (FTQ) de l'époque, Michel Arsenault - qui s'est plaint en 2013 de ces divulgations dans les médias... Jeudi, il a dit s'être assuré auprès de la Gendarmerie royale du Canada (GRC) et du Service canadien du renseignement de sécurité (SCRS) que de telles « activités » ne se passent pas « au niveau fédéral ». Rappelons que deux journalistes de La Presse ont été espionnés en 2007 par des agents de la GRC. Radio-Canada

Why spying on the press hurts democracy
An opinion piece states, "Revelations this week that two Quebec police forces spied on journalists by secretly monitoring their smartphones was widely condemned in Canada and abroad as an outrageous attack on press freedom. Critics from Edward Snowden to domestic and international media groups decried the police tactics as a spectacular assault in a country that is widely considered to be a gold standard for democracy..." Ottawa Citizen, B5

Important questions
An editorial states, "Quebecers are on the verge of another potentially explosive public inquiry, this one sparked by revelations about police spying on journalists. The need for a full inquiry became rapidly apparent as the snooping scandal that broke Monday widened, from Montreal police tracking one columnist for months, to the Sûreté du Québec peering into five years' worth of phone records belonging to six top investigative journalists. To its credit, the Couillard government, which first had announced more limited measures, was quick to see the broader need..." Montreal Gazette, A14

Police spying threatens freedom of the press
"An editorial from the Toronto Star, published Oct. 31: "Are you a journalist?" tweeted American whistleblower Edward Snowden on Monday. "The police spying on you specifically to ID your sources isn't a hypothetical," he warned. "This is today."..." Hamilton Spectator, A14

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Deportation order for men linked to human smuggling put on hold
Two men caught trying to bring people into Canada from the United States across the St. Lawrence River on an inflatable raft had their deportation orders put on hold in the wake of last year's landmark Supreme Court of Canada ruling on human smuggling. The two cases not only highlight the top court's reversal on what is considered criminal human smuggling, but also reveals rich details on what authorities said was a crew moving people back and forth across the Canada-U.S. border along the Thousand Islands archipelago. Whig-Standard, A1

Canadians charged in cross-border fraud
Four Canadians facing charges they crossed into the United States to fraudulently skim money from ATM machines in Vermont could have stolen almost $250,000 US, court documents say. A federal grand jury in Burlington, Vermont, indicted the men Thursday on a charge they acquired bank account information belonging to others and put it on the magnetic strips of gift cards that were then used at ATMs in the Burlington area to get cash advances. Times Colonist, A9

Whoever wins the presidency will have a big impact on B.C.
British Columbians don't get to vote in the U.S. election although the results are likely to have a major impact on varied issues germane to the province. Here are a few ways the outcome of Tuesday's vote could affect B.C.: Softwood lumber and trade. A 2006 agreement to manage the trade of softwood lumber, which is crucial to the B.C. economy, expired in October of last year, and so far there is no replacement. While the future of the softwood agreement hasn't factored significantly in the campaign, the larger issue of trade has - with Donald Trump railing against the North American free-trade agreement and the Trans-Pacific Partnership... The border. Another concern is a "thickening" of the Canadian-U.S. border under a Trump presidency that could complicate things for Canadian professionals who need to spend time in the United States, the board of trade's Mr. Black said. While Mr. Trump has talked about a wall between Mexico and the United States, the board fears a "spillover" into relations with Canada although Mr. Trump has been more focused on the southern U.S. border than the Canadian border. Globe and Mail, S4

Trade deal affects how Canadian firms do business
An opinion piece states, "The Comprehensive Economic Trade Agreement that Canada recently signed with the European Union is Canada's most important trade deal since the North American Free Trade Agreement. CETA is likely to transform Canada much more than NAFTA has, and has already had a significant impact on provincial-federal relations in Canada..." Times Colonist

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

* **Security matters**
The Canadian Centre For ethics in Sport has shut down its email and internet systems after an october cyberattack that mirrors similar security breaches against the World anti-doping agency and the u.S. antidoping agency, the Canadian Cyber Incident response Centre detected the attack that might have involved the theft of confidential information of some athletes. Cyber security experts are investigating the breach in hopes of discovering what, if anything, was stolen and how the hackers got in. "We are looking at how we can ensure this doesn't happen again," Paul melia, president and chief executive officer of the CCeS, told Postmedia on Friday. "We've been told our system is a very secure one, but these cyber-attacks are very sophisticated and very difficult to defend against. Postmedia Network (Winnipeg Sun, S10; Edmonton Sun, Ottawa Sun, Toronto Sun)

* **Commissioner wants mandatory privacy breach reporting**
New Brunswick's privacy commissioner is calling for tougher legislation to force government departments to report breaches of personal information. Anne Bertrand's call comes as the Liberal government plans to introduce changes next year to the province's right to information and privacy legislation. According to one cyber security expert, the call also comes at a time when public bodies are facing more complex and serious security threats...As director of strategic initiatives in information technology services, David Shipley works to protect the university from cyber attacks and other threats. He said encryption is important, but the cost can discourage public bodies from taking that step. CBC News

* **Russia likely can't hack polls, but still a threat**
U.S. intelligence agencies do not think Russia is capable of using cyber-espionage to alter the outcome of Tuesday's presidential election, but they warn that Moscow could continue meddling after the voting has ended to sow doubts about the legitimacy of the result, U.S. officials said. Washington Post (Toronto Star, A14)

* **Ashley Madison gets an 'open-minded' facelift**
Ashley Madison - or just "Ashley," as the hookup website's new management team calls "her" - has more users now than before last year's infamous cyber attack, according to the men brought in for her massive makeover. Torstar (Hamilton Spectator, Toronto Star)

*** The hacking saga**
2002: Ashley Madison is founded. July 2015: Ashley Madison claims to have some 36.5 million users. July 12: Hackers threaten to release client information from Ashley Madison and Established Men unless both sites are taken down. Toronto Star

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Police arrest man after indecent act complaints**
A Lawrencetown man has been arrested and charged after RCMP received complaints about a man committing indecent acts in front of children. Annapolis County District RCMP started an investigation after receiving a complaint Tuesday afternoon about a man masturbating while fully undressed in front of a window as children walked by. A second similar complaint was received at about 8:30 a.m. the next morning. Chronicle Herald, A5

*** Pas de retraite**
Avec l'accord des Hells Angels, Richard «Bob» Hudon disait avoir pris sa retraite comme membre en règle à l'automne 2010. Pourtant, un an plus tard, c'est dans le local du club-école des Dark Souls à Scott en Beauce que les policiers de l'escouade régionale mixte sont allés le cueillir. Le Soleil, 8

*** Police expect to roll out new dispatch system on Nov. 15**
Lacombe Police Service expects to roll out a new dispatch system designed to speed up response times on Nov. 15. Barring any last-minute snags, in mid-November 911 calls will be passed directly from the 911 centre to Lacombe police without first going through the RCMP's communication centre in Red Deer. Red Deer Advocate, A4

*** Charge pending for officer who stopped Green**
A provincial police oversight agency has directed Hamilton police to lay a disciplinary charge against one of its officers accused of "carding" a black city councillor. The Police Services Act charge will be officially laid when the officer makes his first appearance on Dec. 15, says Clint Twolan, president of the Hamilton Police Association. The officer has continued to perform his regular duties throughout the complaint process. Hamilton Spectator, A3

*** Retirement number forces police budget tweak**
Winnipeg Police find themselves $2 million over budget on salaries and expenses this year. Acting chief Art Stannard told the Winnipeg Police Board Friday retirement numbers have fallen short of WPS projections for the year. Winnipeg Free Press, 1

*** Working on use-of-force policy**
The Winnipeg Police Board is prioritizing the establishment of a use-offorce policy for the Winnipeg Police Service and will seek public feedback on the issue. The board announced Friday it has approved a draft for a policy on use of force in shaping how WPS members conduct themselves in the line of duty. A repor t that went before the board Friday morning said the intent is to "promote officer and community safety, effective policing, accountability and trust between the public, the board and the service." Winnipeg Sun

*** Board formalizes appointment; WPS salary budget topped up**
The Winnipeg police board has confirmed the appointment of Danny Smyth as the next police chief. Board members voted unanimously on the recommendation from the board's recruitment committee. The move wasn't a surprise given all members of the board were members of the recruitment committee. Winnipeg Free Press, B1

Kinder Morgan braces for Standing Rock-type protests
A person only has to read a few of the stories about the Standing Rock protest or see some of the pictures and videos to get a sense of the hostile stalemate over the construction of the new Dakota Access pipeline. The protests in North Dakota began small and peaceful, but grew in support and captured the attention of the continent... "I'd be naive if I didn't expect that," said CEO Ian Anderson told

reporters recently in Calgary... Meetings with RCMP. The preparations involve meeting with law enforcement. "We've been in deep conversations with policing authorities, RCMP in the planning for our project - what can we anticipate and what their role needs to be," said Anderson. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Complaints skyrocket at women's prison**
The number of complaints to the Correctional Investigator from women at the federal women's prison in Kitchener has skyrocketed in the past three years, Correctional Investigator Howard Sapers received 344 complaints from Grand Valley Institution in 2015-16 — about 41 per cent of all complaints from women in federal prisons anywhere in Canada. Of the 45 federal prisons across the country, only one other was the subject of more complaints. The number of complaints at Grand Valley has increased each year for the past several years, from 144 in 2013, to 193 in 2014, to 218 in 2015 — a 139 per cent increase in three years. "I think the numbers (of complaints) going up is indicative of how desperate some of the women are," said Kim Pate, executive director of the Canadian Association of Elizabeth Fry Societies, who added that her agency has encouraged women to complain more in an effort to get their concerns addressed. The Record, A1

*** Liberals outline mental health, justice priorities**
A Liberal government would refocus the implementation of the Yukon Mental Wellness Strategy and include comprehensive after-care services in the communities. Liberal Leader Sandy Silver and Jeanie Dendys, the party's Mountainview candidate in Monday's election, outlined their plan to improve mental health, justice and health care services Tuesday... Dendys, who is the Kwanlin Dun First Nation's justice director, said improved mental health services are just one part of a larger plan to improve the justice system. "A responsive and culturally relevant justice system will help protect all Yukoners, respect the human rights of incarcerated individuals and provide for rehabilitation that reduces the recidivism rates in the correctional system," she said. Daily Star, 10

*** Judge denies charter application for killer**
A criminal court is not the proper venue to award constitutional damages to someone who suffered a psychotic breakdown after spending 18 consecutive months in solitary confinement, a judge has ruled. Ottawa defence lawyer Dominic Lamb filed a charter application Friday in the hopes that Ontario Superior Court Justice Robert Maranger would make a declaration that Mutiur Rehman's constitutional rights were violated in jail and award damages for those breaches, but he left the courthouse with neither. Ottawa Citizen, A5

Pregnant killer Kelly Ellard's boyfriend a 'person of interest' in drug dealer disappearance
The boyfriend of pregnant killer Kelly Ellard is a "person of interest" in the May 2016 disappearance of a low-level drug dealer, according to Parole Board of Canada documents. Darwin Dorozan, 42, had his parole revoked after Correctional Services of Canada officials were made aware of the investigation into the missing dealer, the just-released documents say. "On the same date full parole was granted, police advised CSC that you were a person of interest in the suspicious disappearance of a low-level drug dealer in May 2016," the parole board said in its Oct. 27 ruling... She was denied day parole in May despite the Parole Board of Canada noting that she was finally taking some responsibility for the murder and had made strides in her rehabilitation. Postmedia Network (Edmonton Sun, Ottawa Sun, Calgary Sun, Vancouver Sun, Winnipeg Sun, * Toronto Sun, * The Province)

Torture in our jails
An opinion piece states, "Humans are social animals. We need to interact with other humans merely to exist. Otherwise, we can perish. We may kill ourselves. We may be so emotionally shattered that we lose all sense of who we are... The British Columbia Civil Liberties Association has launched a constitutional challenge to the use of solitary confinement in Canadian federal prisons. The BCCLA says that in Canada one out of every four federal prisoners has spent some time in solitary. At any moment, in federal or provincial prisons, up to 1,800 people are confined in solitary..." National Post, A15

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Health Canada disputes police story on fentanyl**
Police were alerted by both phone and mail in July that there was liquid fentanyl in Hamilton, says Health Canada. The statement is in direct contradiction to police claims that the vice and drug unit were notified the week of Oct. 31 about the lab results and that they were not physical documents that landed on an officer's desk. Torstar (Hamilton Spectator, A1; The Record)

*** Une année meurtrière à Ottawa**
Ottawa pourrait supplanter Montréal au chapitre du nombre d'homicides en 2016. Malgré une population deux fois moins importante, la capitale fédérale affiche un bilan semblable à celui de la métropole québécoise. Vendredi, le Service de police de la Ville de Montréal (SPVM) comptait 18 homicides sur son territoire, depuis le début de l'année. Au même moment, le Service de police d'Ottawa (SPO) en dénombrait 16. Le Droit, 3 / Front

*** Prudence avec les comparaisons**
Un professeur en criminologie de l'Université d'Ottawa privilégie la prudence avec les statistiques qui tendent à démontrer qu'Ottawa connaît plus d'homicides per capita que Montréal. «Mais je demeure quand même impressionné par la chute vertigineuse des homicides à Montréal», dit Ronald-Frans Melchers de l'Université d'Ottawa. Selon lui, il vaut mieux être prudent avec les données brutes concernant les homicides rapportés à Ottawa et Montréal, en 2016. Bien que les deux villes aient une certaine parité en 2016, le criminologue préfère comparer les statistiques sur les Régions métropolitaines de recensement (RMR) et se fier aux taux d'homicides calculés par Statistique Canada. Le Droit, 2

*** So many cops aren't neighbours**
An opinion piece states, "The irony made me smile. On Sunday, in the midst of getting ready to negotiate a new contract with the city, the Winnipeg Police Association is conducting a door-to-door public relations campaign they're calling Neighbour to Neighbour Outreach. On Tuesday - two days before the Neighbour to Neighbour news release - I had called police union president Moe Sabourin to inquire about how many of his membership aren't really neighbours. I wanted to know how many live outside the city. For years, it's been well-known that when large numbers of city police officers leave work, they head home to neighbourhoods or acreages outside the city that pays them so handsomely..." Winnipeg Free Press

What happens when our schools aren't safe for all students?
An opinion piece states, "Imagine videos purportedly showing violent "Jewish takeovers" or "homosexual takeovers" of Paris and London, or a video headlined: "Must see: Dutch mayor tells fellow Jews they can f------ if they don't like freedom." To some it may be just the simple exercise of free speech rights. Others will argue that as distasteful as they are, a person must have the right to express such views. Yet others may feel that these cross the line into hate..." Toronto Star

Religious neutrality bill comes in for embarrassing criticism
An editorial states, "The Couillard government's legislative venture into identity politics is not going well. Last year, to keep an election promise made under pressure from the nationalist opposition parties, the Liberal government introduced an anti-"radicalization" package of measures aimed at Muslims in particular..." Montreal Gazette, A14

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Call for peace**
It's a call for justice. And, it's a call for healing, said Catherine Dickson one of the leaders for the recent CGIT and explorers pilgrimage walk. "This is a response to the call from the aboriginal community to

make a change," she said. Dickson, and about 30 others, participated in the walk in October to raise awareness about murdered and missing aboriginal women in Canada. Charlottetown Guardian, C4

*** We can't afford to ignore indigenous women and girls**
Before providing aid money to support resource-development projects in other countries, Canadian policy requires a careful examination of how the project might affect the lives and safety of women and girls... In 2004, Amnesty International published a report called Stolen Sisters, which demonstrated that the economic marginalization of indigenous women and the discrimination they face in Canadian society are critical factors putting them in positions of increased risk, fuelling violence against them, and denying them the protections and support they deserve. At the time, we noted that indigenous women had long struggled to draw public attention to these issues and that there was already, at that point, a significant body of government reports and other studies pointing to the need for action. Yet it is only now, with the launch of a national inquiry on missing and murdered indigenous women and girls, that we begin to see real government acknowledgment of the scale and urgency of this crisis. Globe and Mail, S2

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Police hope pot shop raids**
Ottawa police raided six marijuana dispensaries Friday morning, closing a big chunk of the city's pot shops in one fell swoop... The targeted shops are operated by a B.C.-based outfit that moved into Ottawa this summer, opening dispensaries called Green Tree, WeeMedical and CannaGreen. Ottawa Citizen, A2

*** Local Ottawa politicians applaud raids on marijuana dispensaries**
Local politicians in Ottawa are applauding the closure of a string of marijuana dispensaries operating illegally in the city. Police arrested nine people and raided seven pot shops this week after mounting complaints from community members and councillors. "I'm happy with the level of response that OPS has put in," said Jody Mitic. "We were kind of tightening the screws a little bit on the [police] chief." CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

Feds' payroll system a nightmare
An opinion piece states, "Over 30,000 workers are waiting to have their paycheques fixed, many haven't been paid in months, due to the federal government's new pay system, Phoenix. Phoenix was rolled out in February of 2015, despite being warned by the Public Service Alliance of Canada (its largest union), that the system was flawed..." Windsor Star, A6

OTHER / AUTRE

NIL

INTERNATIONAL

*** Paris pour un "meilleur encadrement" des armes à feu**
Le ministre français de l'Intérieur, Bernard Cazeneuve, a appelé vendredi l'Union européenne à un " meilleur encadrement " de la circulation des armes à feu dans le cadre de la lutte contre le terrorisme. " Nous devons avancer " et " être fermes " sur l'adoption par le Parlement européen d'une nouvelle directive sur les armes à feu, a insisté le ministre qui recevait le Britannique Julian King, nouveau commissaire européen en charge de la sécurité et de la lutte contre le terrorisme. Les États membres de l'UE se sont mis d'accord en juin sur un renforcement des règles de contrôle des armes à feu au terme d'une négociation difficile. Mais l'adoption définitive de la directive requiert désormais un vote favorable du Parlement européen. Pour M. Cazeneuve, il s'agit de " permettre un meilleur encadrement et une

meilleure traçabilité des armes à feu au niveau européen '', une priorité de la France. Agence France-Presse (Le Devoir, C6)

Les déplacés de Boko Haram - Venir en aide malgré le silence médiatique
Dans l'Extrême-Nord du Cameroun, l'organisme de bienfaisance L'Oeuvre Léger offre depuis six mois une aide humanitaire d'urgence aux déplacés internes du groupe terroriste Boko Haram. Un aspect du conflit peu médiatisé, alors que des milliers de Camerounais souffrent de malnutrition et n'ont accès ni à des soins de santé ni à de l'eau potable.\r\n'' Les 31 500 personnes à qui le projet vient en aide sont victimes de violation grave des droits de la personne, en vertu du droit humanitaire international '', lance d'emblée Chanèle Boulet-Gauthier, coordonnatrice de l'action humanitaire à L'Oeuvre Léger et responsable du projet. En partenariat avec une ONG locale, le Comité diocésain de développement (CDD) -- Caritas du Cameroun, et avec le soutien d'Affaires mondiales Canada, ce projet vise à aider les déplacés dans la région de l'Extrême-Nord ainsi que les membres des communautés hôtes. '' Le projet vient casser le cycle de vulnérabilité de ces personnes '', présente la coordonnatrice, précisant que dans cette région, la plus pauvre du pays, les déplacements de population provoquent des situations particulièrement difficiles. Le Devoir, I4

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 5, 2016 / le 5 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Feds to review CSIS powers in the digital age
A federal review of national security will consider whether Canada's spy service should be able to sift through the kind of personal data it kept illegally for years, says **Public Safety Minister Ralph Goodale**. **Goodale** said Friday the notion that the Canadian Security Intelligence Service should avoid stashing away information about innocent people is a ***"fundamental principle of Canadian privacy."*** But **the minister** appeared to leave the door open to one day giving CSIS the legal authority to keep and analyze electronic data about individuals who do not pose a security threat. ***"I want to hear the professional advice on both sides,"*** **Goodale** told a news conference in the foyer of the House of Commons. ***"I'm not pre-empting the consultation."***... **Goodale said** he became aware of the ***"full scope of the issue"*** when the court judgment was made available to him in preliminary form a couple of weeks ago. **He said he took** the immediate step of informing the Security Intelligence Review Committee, the watchdog over

CSIS, and asked the review committee to supervise management of the data and ensure full compliance with the judgment. Coulombe ***"understands my expectations here,"*** **Goodale added.** ***"A serious error has been made. This situation needs to be remedied. It has to be remedied quickly."*** The NDP said Friday the revelations underscore the need for stronger parliamentary oversight. Canadian Press (Cape Breton Post, A10; The Telegram, Chronicle Herald, Red Deer Advocate, Charlottetown Guardian, Whig-Standard, Edmonton Sun, Calgary Sun, Times Colonist, Hamilton Spectator, Times Colonist, The Record, iPolitics, Times & Transcript, Daily Gleaner); Presse Canadienne (Le Droit, 21 ; Le Devoir, L'Acadie Nouvelle)

Espionnage de journalistes - Ottawa ferme les yeux sur le passé
Aucun journaliste n'est actuellement surveillé par la GRC et le SCRS... mais Ottawa n'a pas idée si cette situation a pu se produire dans un passé récent. **Le ministre de la Sécurité publique, Ralph Goodale**, ne l'a pas demandé. Et **il n'a pas** l'intention de le faire : c'est le présent qui compte, dit-il. **Pour M. Goodale,** ***" la question porte sur ce qui se passe maintenant et nous pouvons offrir l'assurance que ce genre d'activité n'a pas lieu. Je ne sais rien sur les événements qui se sont produits lorsque nous [les libéraux] ne formions pas le gouvernement "***, **a indiqué le ministre** en point de presse. Questionné à savoir s'il demanderait directement au patron du Service canadien du renseignement de sécurité (SCRS) si des mandats de surveillance ont pu être lancés dans les cinq dernières années, **Ralph Goodale** a répondu que c'était précisément la ***" responsabilité du directeur de répondre aux questions opérationnelles "***... Lors de la période de questions, **M. Goodale a indiqué** trouver ***" très inquiétantes "*** les révélations qui ont marqué la semaine au Québec -- l'espionnage de plusieurs journalistes par le Service de police de la Ville de Montréal (SPVM) ou la Sûreté du Québec (SQ). Le Devoir, A7

Advocates urge Liberal government to reduce number of women in prison
Sometimes when she goes to the grocery store, all Alia Pierini can do is sit in the parking lot, unable to bear the idea of going inside. She tries a different store, but Pierini, 31, often ends up coming home without the food she had planned to buy for lunch. "I feel like a big loser, to be honest, but I can't help it," the former prisoner told a news conference Thursday as she described the lingering anxiety, panic and fear she still feels as a result of months spent alone in solitary confinement... Now a regional advocate for female prisoners in federal custody, Pierini joined the Canadian Association of Elizabeth Fry Societies, which provides support for women and girls in the justice system, in calling on the Liberal government to reduce the number of women behind bars. The association's longtime executive director, Kim Pate - newly recommended for the Senate by Prime Minister Justin Trudeau - urged the government to give judges the discretion to overturn or alter the mandatory minimum sentences brought in by the previous Conservative government... Pate also said she was "heartened" to see Justice Minister Jody Wilson-Raybould given a mandate to restrict the use of solitary confinement and improve the treatment of prisoners with mental illness by implementing recommendations from the Ashley Smith inquest... **Public Safety Minister Ralph Goodale**, who is working with Wilson-Raybould on reviewing the inquest recommendations, has said that when it comes to administrative segregation, the government is looking at reforms that touch on everything from policy and programs to physical infrastructure and hopes to have specific proposals sometime this winter. ***"We need to dramatically change the scenario, and we're working at that,"*** **Goodale said** last week. Daily Star, 25

Spies could be left out in the cold
" Trust, but verify ." Academics Craig Forcese and Kent Roach argue that this should be the maxim in the security sector when dealing with powerful state agencies like the Canadian Security Intelligence Service and the RCMP. But trust in Canada ' s security services is thin on the ground, after the news Thursday that a CSIS unit illegally kept data deemed unrelated to national security threats. **Public Safety Minister Ralph Goodale said** Friday that a Federal Court decision by Justice Simon Noel, who found CSIS has ***"breached, again, the duty of candour it owes the court,"*** is timely because the Liberals are in the midst of reviewing the national security laws... Even before that, both Mosley and Noel had lambasted CSIS for providing inaccurate information to the court. In the Mohamed Harkat case, Noel criticized the agency ' s lack of candour... **Yet Goodale** did not rule out a change to the law to allow CSIS to keep the information ruled offside by the court. "***This is an issue that I think needs to be examined in the context of our national security review,"*** **he said**. ***"I want to hear the professional advice on both***

sides...Our security agencies to be effective in keeping Canadians safe. At the same time, what the agencies do needs to be in accord with the law and with the Constitution." Phil Gurski, a former CSIS analyst, said the metadata were retained for a rea-son - to identify people involved with, or sympathetic to, terror groups. Postmedia News (London Free Press, N6; Vancouver Sun, Calgary Herald, Leader-Post, Montreal Gazette, The Record, Ottawa Citizen, National Post)

Feds to look at border-crossing challenges for First Nations
The federal government will appoint a special ministerial representative to look at border crossing issues faced by First Nations. In a joint letter written in response to a Senate committee study, Indigenous Affairs Minister Carolyn Bennett, Immigration Minister John McCallum and **Public Safety Minister Ralph Goodale** say the adviser and First Nations will discuss significant and complex challenges. The letter said the resolution of these issues will require a ***"horizontal approach"*** involving several departments and agencies. ***"This will be necessary in order for the government of Canada to arrive at workable and sustainable solutions that facilitate the ability of First Nation community members to cross the U.S.-Canada border and, at the same time, take into consideration issues such as status, international sovereignty and security,"*** it said. Canadian Press (Whig-Standard, B2; Daily Gleaner, Telegraph-Journal, Times & Transcript)

Spy watchdog that triggered scathing rebuke of illegal CSIS activities facing job cuts
The federal watchdog that triggered this week's scathing judicial rebuke of Canada's spy service for illegal activities faces significant job cuts because of a chronic lack of sustained government funding, even as the Liberals hinted Friday the agency could be asked to do more to police federal spies. The Security Intelligence Review Committee (SIRC), the independent agency that reports to Parliament on the operations of the Canadian Security Intelligence Service (CSIS), says the equivalent of at least 11 full-time positions will disappear March 31 unless the Liberal government delivers millions more dollars under a sustained, multi-year funding plan announced by the previous Conservative government. "We don't know if we're getting any more funding," SIRC spokeswoman Sabrine Barakat said Friday. "SIRC has been actively working to access that money on a permanent basis but we're still waiting to see." The government has offered no explanation, she said. **The office of Public Safety Minister Ralph Goodale was unable** Friday to explain the funding confusion. Treasury Board officials could not explain either when asked the same question by the Ottawa Citizen last March... **Goodale repeated the pledge** for robust oversight again Friday in the swirling aftermath of the Federal Court ruling that CSIS illegally retained a decade's worth of metadata gleaned from Canadians' electronic communications that had nothing to do with threats to national security. Questions about the activity were first raised by SIRC in its 2014-15 annual report... Speaking with reporters, **Goodale said** the length of time it took for the decade of CSIS metadata misconduct to surface is of ***"critical concern."***... Paul Cavalluzzo, counsel for the Maher Arar commission, said SIRC is not in a position to adequately deal with CSIS. National Post (2016-11-04); Postmedia Network (London Free Press, N6; Calgary Herald, Vancouver Sun, Leader-Post, Montreal Gazette, Ottawa Citizen)

Watchdog defends CSIS, its director
Michel Coulombe, Canada's top spy, is in deep trouble with the courts and his political boss, **Public Safety Minister Ralph Goodale**, over revelations CSIS kept a decade's worth of data on Canadians who are no threat to national security. But Pierre Blais, head of the civilian watchdog agency over CSIS, says Coulombe "acted in good faith" and should not lose his job over the affair... Still, the judge said CSIS breached its "duty of candour" when it failed to reveal what it was up to. Goodale said Friday the first he learned of it was two weeks ago when an unredacted copy of the pending judgment reached his desk. Asked if he still has confidence in Coulombe, **Goodale said** only that he has made his expectations to the director clear. ***"A serious error has been made. (Coulombe) maintains that in his view, and in the view of the advice he got from the Department of Justice over the course of the last number of years, that the course of conduct by CSIS was within the parameters of law,"*** **Goodale told** reporters. ***"The court has now said very clearly and unequivocally that it was not. This situation needs to be remedied. It has to be remedied quickly ... CSIS must be forthcoming and candid with the court. That will happen."***... **But Goodale** was adamant Friday that innocent people should not have their information tracked and stored by Canada's spies. ***"That's a fundamental principle of Canadian privacy,"*** **he said.** Toronto Star, A10

Pas d'assurances pour le passé à Ottawa
S'il a obtenu l'assurance qu'aucune surveillance de journalistes ne se produit «actuellement» au niveau fédéral, le gouvernement Trudeau n'a pas demandé à la Gendarmerie royale du Canada (GRC) et au Service canadien du renseignement de sécurité (SCRS) s'ils ont mis des journalistes sous surveillance au cours des cinq dernières années. ***«L'enjeu, c'est ce qui se passe maintenant et nous pouvons offrir l'assurance que ce genre d'activités ne se produit pas actuellement. Je n'ai pas connaissance de choses qui se sont produites quand nous ne formions pas le gouvernement du Canada»*, a dit le ministre Ralph Goodale**, qui n'a pas l'intention de demander à la GRC ou au SCRS si des mandats de surveillance ont été lancés à l'égard de journalistes au cours des cinq dernières années. ***«La réponse, autant de la GRC que du SCRS, est que rien de la sorte ne se produit actuellement. [...] C'est la responsabilité du directeur du SCRS de répondre aux questions opérationnelles. Vous allez sur une pente très dangereuse quand vous invitez les politiciens à aller dans ce domaine»,* dit le ministre Goodale.** La Presse, A12

Minister vows action on CSIS
Public Safety Minister Ralph Goodale says he will make sure Canada's spy agency takes action after a Federal Court found that its officials have misled justices and unlawfully amassed data about people not suspected of being threats... On Friday, **Mr. Goodale said he** intends to ensure that CSIS follows the Federal Court's directive to stop the controversial practices. Pressed on whether he plans to fire anyone now, **Mr. Goodale said** only that **he** wants to have words with CSIS officials. ***"I will discuss with the executive management of the service how they plan to respond to this judgment,"* he said**. **The minister told** reporters that CSIS director Michel Coulombe has told him that CSIS lacks records that indicate whether it briefed previous ministers on the programs. ***"I take that as a pretty serious defect in the record keeping of the organization. "That is one of the things that absolutely needs to be rectified," he said***. Globe and Mail, A9

It's not easy being a journalist's unnamed source in the Information Age
An opinion piece states, "Were I in a position of authority, I would probably hang up if contacted by a journalist. Not because I don't think people in positions of authority should speak to journalists - I do, and I'm grateful to all the people in positions of authority who haven't hung up on me over the years... In Canada, Mounties investigating a document leak have targeted journalists, and last week, reporters at La Presse in Montreal and at Radio-Canada discovered Quebec police, hunting for leakers in their own ranks, have been tracking and tapping their communications. (We have no idea how many other journalists have been surveilled, but it's safe to assume it happens.)... Glenn Cowan, GRA Quantum's Canadian CEO, says such software allows phone, video or email communication without leaving any record: no metadata, no communications link to analyze, no tracking log, nothing... Cowan stresses that his firm does not regard law enforcement as a "threat actor," to use the language employed by the super-secret Communications Security Establishment in its advice to government employees on how to protect their communications..." CBC News

The worst part about the spying spree - it was legal
An opinion piece states, "Connect the dots between Quebec's police corps and the half-dozen or more investigative journalists who were put under surveillance over the past decade and you will find a gaggle of judges potentially derelict in their gatekeeping duties. In each of the spying episodes that have come to light over the past week, the police had to convince a judge to sanction the surveillance and, in some cases, to do so more than once..." Toronto Star

Spying eyes
An editorial states, "Taken in isolation, either case is concerning. But this week, we actually had two major law enforcement misconduct issues surface. The Canadian Security Intelligence Service, it turns out, has been collecting unrelated information it received as part of terrorism investigations (and was supposed to destroy), and instead loaded it into database systems that its legal overseers weren't even told existed. Meanwhile, in Quebec, police services were tracking some reporters' calls and texts for periods as long as five years, in an effort to catch and punish police whistleblowers. There's a huge problem here. And it's an oversight problem..." The Telegram, A15

Clean up spy agency
An editorial states, "So, Canada's spy agency has gobs of people's metadata in a secret database. Well, it's just numbers, isn't it? You know, telephone numbers and Internet IP addresses and so forth. Who cares? The justice system, to begin with. On Thursday, the Federal Court released a ruling saying that the Canadian Security Intelligence Service's retention and analysis of wide swaths of data, which had been going on for 10 years, was illegal. And CSIS hadn't bothered to inform the court of what it was doing... **Public Safety Minister Ralph Goodale was shifty** on Friday when asked if the Liberals' planned security oversight committee would have stopped this sort of spying; instead he repeated talking points. **He also refused** to say how many Canadians had their data captured. Reassuringly, though, the government won't appeal the court ruling..." Ottawa Citizen, B5

Surveillance des journalistes - La nouvelle chasse aux sorcières
Un article d'opinion déclare, « Le professeur Stéphane Leman-Langlois est un spécialiste de la police, du renseignement, du terrorisme, des technologies et du contrôle social. Il a récemment collaboré au livre "Transparent Lives" sur la surveillance au Canada. Il enseigne à l'Université Laval.\r\nAvez-vous été surpris par les récentes révélations sur l'ampleur de l'espionnage des journalistes québécois ? Pas du tout. Chaque fois que je parle de surveillance depuis des années et que je dis aux journalistes qu'ils sont les premières cibles, la plupart d'entre eux lèvent les yeux au plafond parce qu'ils n'y croient pas. Ils me traitent de parano parce que je suis dans les études de la surveillance. Je suis certain que le phénomène est d'une ampleur bien supérieure à ce qui vient d'être dévoilé. Je pense que les révélations de la SQ -- arrivées très, très rapidement et concernant, comme par hasard, des écoutes datant d'anciens directeurs de ce corps de police -- sont faites pour détourner l'attention. Mais bon, il va y avoir une commission d'enquête et, si elle peut lever des pierres, on va en trouver bien plus, de ces histoires de surveillance... » Le Devoir, B1

Surveillance - La confiance ébranlée
Un article d'opinion déclare, « Pendant dix ans, le Service canadien du renseignement de sécurité (SCRS) a conservé et analysé des données associées à des personnes qui n'étaient soupçonnées de rien, mais qui avaient eu le malheur de communiquer avec des personnes légalement surveillées. Et le service l'a fait sans en informer la Cour fédérale, un des rares garde-fous contre d'éventuels abus de nos espions. Le gouvernement doit serrer la vis et vite ; la confiance des citoyens et la protection de leur vie privée en dépendent... Le Tribunal rappelle que le SCRS doit, en vertu de la loi, conserver les données uniquement " dans la mesure strictement nécessaire ", ce qui n'était pas le cas. Lors d'une conférence de presse convoquée en toute hâte, le directeur du SCRS, Michel Coulombe, a dit que le service avait cessé toute analyse et verrouillé l'accès aux données en question. **Le ministre de la Sécurité publique, Ralph Goodale**, a précisé que le gouvernement n'interjetterait pas appel et a déploré le manque de franchise du SCRS devant la Cour. Mais ensuite ? La Cour n'a pas demandé de détruire ces données et personne ne sait trop ce qu'on en fera. Le plus préoccupant est que M. Coulombe espère pouvoir les conserver et que **le ministre de la Sécurité publique, Ralph Goodale**, n'a pas fermé la porte. **Il a noté** que cette question serait mieux débattue lors des consultations publiques en cours sur ***" le cadre de sécurité nationale "***. **Le ministre** a d'ailleurs **relevé** que le juge Noël avait suggéré de revoir la loi sur le SCRS et de l'adapter à la réalité des nouvelles technologies... » Le Devoir, B4

TOP STORIES / MANCHETTES

*** Alberni flooding may shut highway for days**
Flooding near Port Alberni has the potential to close Highway 4, the only highway link to Ucluelet and Tofino, for five or six days, says the emergency preparedness co-ordinator of the Tseshaht First Nation. Times Colonist, A1

*** Complaints skyrocket at women's prison**
The number of complaints to the Correctional Investigator from women at the federal women's prison in Kitchener has skyrocketed in the past three years, Correctional Investigator Howard Sapers received 344 complaints from Grand Valley Institution in 2015-16 — about 41 per cent of all complaints from women in federal prisons anywhere in Canada. Of the 45 federal prisons across the country, only one other was the

subject of more complaints. The number of complaints at Grand Valley has increased each year for the past several years, from 144 in 2013, to 193 in 2014, to 218 in 2015 — a 139 per cent increase in three years. "I think the numbers (of complaints) going up is indicative of how desperate some of the women are," said Kim Pate, executive director of the Canadian Association of Elizabeth Fry Societies, who added that her agency has encouraged women to complain more in an effort to get their concerns addressed. The Record, A1

* **Health Canada disputes police story on fentanyl**
Police were alerted by both phone and mail in July that there was liquid fentanyl in Hamilton, says Health Canada. The statement is in direct contradiction to police claims that the vice and drug unit were notified the week of Oct. 31 about the lab results and that they were not physical documents that landed on an officer's desk. Torstar (Hamilton Spectator, A1; The Record)

Pregnant killer Kelly Ellard's boyfriend a 'person of interest' in drug dealer disappearance
The boyfriend of pregnant killer Kelly Ellard is a "person of interest" in the May 2016 disappearance of a low-level drug dealer, according to Parole Board of Canada documents. Darwin Dorozan, 42, had his parole revoked after Correctional Services of Canada officials were made aware of the investigation into the missing dealer, the just-released documents say. "On the same date full parole was granted, police advised CSC that you were a person of interest in the suspicious disappearance of a low-level drug dealer in May 2016," the parole board said in its Oct. 27 ruling...She was denied day parole in May despite the Parole Board of Canada noting that she was finally taking some responsibility for the murder and had made strides in her rehabilitation. Postmedia Network (Edmonton Sun, Ottawa Sun, Calgary Sun, Vancouver Sun, Winnipeg Sun)

Retour sur une semaine sombre pour la liberté de presse
Pour les trois journalistes de Radio-Canada, il s'agit de tous leurs appels de novembre 2008 à octobre 2013, confirme la SQ. Cette procédure ne prévoyait pas d'écoute électronique. La SQ cherchait à faire la lumière sur des fuites d'éléments d'enquête provenant de l'écoute électronique en 2008 et 2009 du président de la Fédération des travailleurs du Québec (FTQ) de l'époque, Michel Arsenault - qui s'est plaint en 2013 de ces divulgations dans les médias... Jeudi, il a dit s'être assuré auprès de la Gendarmerie royale du Canada (GRC) et du Service canadien du renseignement de sécurité (SCRS) que de telles « activités » ne se passent pas « au niveau fédéral ». Rappelons que deux journalistes de La Presse ont été espionnés en 2007 par des agents de la GRC. Radio-Canada

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

* **Climate change: What does it mean for Canada and how can we respond?**
Canada has already seen smoke-related health impacts and stressful evacuations as the result of increased wildfires; the spread of Lyme disease; and food security and mental health challenges related to rapid changes in the Far North, which is two to three degrees Celsius warmer than it was in the 1950s. Here's How Canada's Provinces Are Responding To Climate Change. New Brunswick banned fracking. Last month, lawmakers in New Brunswick voted to place a moratorium on fracking within the province. Canada Journal

* **Alberni flooding may shut highway for days**
Flooding near Port Alberni has the potential to close Highway 4, the only highway link to Ucluelet and Tofino, for five or six days, says the emergency preparedness co-ordinator of the Tseshaht First Nation. Times Colonist, A1

* **Winter gear guide**
El Nino is famous for weather media headlines. But its sister act - La Nina - is known to be pretty frosty and forecasted to slam the Canadian Rockies with a good old-fashioned winter, full of what skiers and snowboarders love, cooler temperatures and above-average moisture. Calgary Herald, G10

* **Tornado-damaged homes still waiting to be repaired**
Some of the of roofs, siding and porches wrecked in just four seconds when a tornado touched down on Riberdy Road Aug. 24 remain unfixed 10 weeks later, and resident Greg Tremblay says he's had enough. Windsor Star, A5

* **Une heure de plus... pour vérifier son détecteur de fumée**
Le changement d'heure, dimanche, est le moment idéal pour faire penser de vérifier son avertisseur de fumée et en remplacer la pile. La remarque vient du Service de protection contre les incendies de la Ville de Sherbrooke. La Tribune, 10

* **CBRM phases out storm help line**
Assistance will continue for residents reeling from October flood. The Cape Breton Regional Municipality shut down its emergency telephone help line for residents affected by the Thanksgiving Day flood. The provincial government issued a news release Friday indicating that while the help line is being phased out, the municipality will follow up with anyone who has called for assistance. Cape Breton Post, A3

* **Les municipalités veulent plus de sécurité**
Le monde municipal n'a pas oublié la tragédie de Lac-Mégantic. Réunis à l'occasion d'une rencontre spéciale à Edmundston au Nouveau-Brunswick vendredi, quelques dizaines de représentants municipaux ont discuté de sécurité ferroviaire en compagnie de divers intervenants. Ils ont réclamé l'adoption d'une série de mesures pour accroître la sécurité des communautés à l'issue de leurs discussions. La Tribune, 9

* **High hopes for Elbow River brown trout after devastating 2013 flood**
River watchers are hoping this year's brown trout count in the Elbow River continues to show growth after the 2013 Alberta flood had a devastating effect on the population. Chris Bjornson, a senior fisheries biologist with Golder Associates, says the flood three years ago continues to affect the population. CBC News

* **Springbank dam raises concerns for environment**
An opinion piece states, "It has now been one year since the Alberta government flip-flopped on its election promise to scrap the Springbank dam project in favour of the McLean Creek dam. I remember watching the news conference - led by the environment minister, flanked by the mayor of Calgary - but with no one there from Springbank, Rocky View County or the impacted First Nations..." Calgary Herald, A13

* **Letters to the Editor**
A letter to the editor states, "Independent probe needed. Husky Energy was supposed to file a major and conclusive report on the disastrous oil spill in the North Saskatchewan River to the provincial government. Instead, it filed a one pager and asked the government for an extension later into November. This request was granted..." StarPhoenix

The beast is still alive
Six months after it sent the population of Fort McMurray fleeing, the wildfire known as MWF-009 is still burning. The fire can no longer be seen; there is no smoke or open flames. But in a remote section of Alberta and Saskatchewan far from the city it nearly destroyed, the blaze is still being carefully watched. Postmedia Network (London Free Press, N5; Windsor Star, Vancouver Sun, Edmonton Journal, Calgary Herald, National Post, Ottawa Citizen)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Attack on a free press a strike against us all**
An opinion piece states, "For some Canadian readers, this column may sound, at best, like an objection worthy of little notice. At worst, it may read like a series of trivial complaints - bellyaching, even - from a journalist with oh-so-precious sensibilities when it comes to press freedoms..." London Free Press, A12

Retour sur une semaine sombre pour la liberté de presse
Pour les trois journalistes de Radio-Canada, il s'agit de tous leurs appels de novembre 2008 à octobre 2013, confirme la SQ. Cette procédure ne prévoyait pas d'écoute électronique. La SQ cherchait à faire la lumière sur des fuites d'éléments d'enquête provenant de l'écoute électronique en 2008 et 2009 du président de la Fédération des travailleurs du Québec (FTQ) de l'époque, Michel Arsenault - qui s'est plaint en 2013 de ces divulgations dans les médias... Jeudi, il a dit s'être assuré auprès de la Gendarmerie royale du Canada (GRC) et du Service canadien du renseignement de sécurité (SCRS) que de telles « activités » ne se passent pas « au niveau fédéral ». Rappelons que deux journalistes de La Presse ont été espionnés en 2007 par des agents de la GRC. Radio-Canada

Why spying on the press hurts democracy
An opinion piece states, "Revelations this week that two Quebec police forces spied on journalists by secretly monitoring their smartphones was widely condemned in Canada and abroad as an outrageous attack on press freedom. Critics from Edward Snowden to domestic and international media groups decried the police tactics as a spectacular assault in a country that is widely considered to be a gold standard for democracy..." Ottawa Citizen, B5

Important questions
An editorial states, "Quebecers are on the verge of another potentially explosive public inquiry, this one sparked by revelations about police spying on journalists. The need for a full inquiry became rapidly apparent as the snooping scandal that broke Monday widened, from Montreal police tracking one columnist for months, to the Sûreté du Québec peering into five years' worth of phone records belonging to six top investigative journalists. To its credit, the Couillard government, which first had announced more limited measures, was quick to see the broader need..." Montreal Gazette, A14

Police spying threatens freedom of the press
"An editorial from the Toronto Star, published Oct. 31: "Are you a journalist?" tweeted American whistleblower Edward Snowden on Monday. "The police spying on you specifically to ID your sources isn't a hypothetical," he warned. "This is today."..." Hamilton Spectator, A14

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Deportation order for men linked to human smuggling put on hold
Two men caught trying to bring people into Canada from the United States across the St. Lawrence River on an inflatable raft had their deportation orders put on hold in the wake of last year's landmark Supreme Court of Canada ruling on human smuggling. The two cases not only highlight the top court's reversal on what is considered criminal human smuggling, but also reveals rich details on what authorities said was a crew moving people back and forth across the Canada-U.S. border along the Thousand Islands archipelago. Whig-Standard, A1

Canadians charged in cross-border fraud
Four Canadians facing charges they crossed into the United States to fraudulently skim money from ATM machines in Vermont could have stolen almost $250,000 US, court documents say. A federal grand jury in Burlington, Vermont, indicted the men Thursday on a charge they acquired bank account information belonging to others and put it on the magnetic strips of gift cards that were then used at ATMs in the Burlington area to get cash advances. Times Colonist, A9

Whoever wins the presidency will have a big impact on B.C.
British Columbians don't get to vote in the U.S. election although the results are likely to have a major impact on varied issues germane to the province. Here are a few ways the outcome of Tuesday's vote could affect B.C.: Softwood lumber and trade. A 2006 agreement to manage the trade of softwood lumber, which is crucial to the B.C. economy, expired in October of last year, and so far there is no replacement. While the future of the softwood agreement hasn't factored significantly in the campaign, the larger issue of trade has - with Donald Trump railing against the North American free-trade agreement and the Trans-Pacific Partnership... The border. Another concern is a "thickening" of the Canadian-U.S. border under a Trump presidency that could complicate things for Canadian professionals who need to spend time in the United States, the board of trade's Mr. Black said. While Mr. Trump has talked about a wall between Mexico and the United States, the board fears a "spillover" into relations with Canada although Mr. Trump has been more focused on the southern U.S. border than the Canadian border. Globe and Mail, S4

Trade deal affects how Canadian firms do business
An opinion piece states, "The Comprehensive Economic Trade Agreement that Canada recently signed with the European Union is Canada's most important trade deal since the North American Free Trade Agreement. CETA is likely to transform Canada much more than NAFTA has, and has already had a significant impact on provincial-federal relations in Canada..." Times Colonist

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

* **Security matters**
The Canadian Centre For ethics in Sport has shut down its email and internet systems after an october cyberattack that mirrors similar security breaches against the World anti-doping agency and the u.S. antidoping agency, the Canadian Cyber Incident response Centre detected the attack that might have involved the theft of confidential information of some athletes. Cyber security experts are investigating the breach in hopes of discovering what, if anything, was stolen and how the hackers got in. "We are looking at how we can ensure this doesn't happen again," Paul melia, president and chief executive officer of the CCeS, told Postmedia on Friday. "We've been told our system is a very secure one, but these cyber-attacks are very sophisticated and very difficult to defend against. Postmedia Network (Winnipeg Sun, S10; Edmonton Sun, Ottawa Sun, Toronto Sun)

* **Commissioner wants mandatory privacy breach reporting**
New Brunswick's privacy commissioner is calling for tougher legislation to force government departments to report breaches of personal information. Anne Bertrand's call comes as the Liberal government plans to introduce changes next year to the province's right to information and privacy legislation. According to one cyber security expert, the call also comes at a time when public bodies are facing more complex and serious security threats...As director of strategic initiatives in information technology services, David Shipley works to protect the university from cyber attacks and other threats. He said encryption is important, but the cost can discourage public bodies from taking that step. CBC News

* **Russia likely can't hack polls, but still a threat**
U.S. intelligence agencies do not think Russia is capable of using cyber-espionage to alter the outcome of Tuesday's presidential election, but they warn that Moscow could continue meddling after the voting has ended to sow doubts about the legitimacy of the result, U.S. officials said. Washington Post (Toronto Star, A14)

* **Ashley Madison gets an 'open-minded' facelift**
Ashley Madison - or just "Ashley," as the hookup website's new management team calls "her" - has more users now than before last year's infamous cyber attack, according to the men brought in for her massive makeover. Torstar (Hamilton Spectator, Toronto Star)

*** The hacking saga**
2002: Ashley Madison is founded. July 2015: Ashley Madison claims to have some 36.5 million users. July 12: Hackers threaten to release client information from Ashley Madison and Established Men unless both sites are taken down. Toronto Star

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Police arrest man after indecent act complaints**
A Lawrencetown man has been arrested and charged after RCMP received complaints about a man committing indecent acts in front of children. Annapolis County District RCMP started an investigation after receiving a complaint Tuesday afternoon about a man masturbating while fully undressed in front of a window as children walked by. A second similar complaint was received at about 8:30 a.m. the next morning. Chronicle Herald, A5

*** Pas de retraite**
Avec l'accord des Hells Angels, Richard «Bob» Hudon disait avoir pris sa retraite comme membre en règle à l'automne 2010. Pourtant, un an plus tard, c'est dans le local du club-école des Dark Souls à Scott en Beauce que les policiers de l'escouade régionale mixte sont allés le cueillir. Le Soleil, 8

*** Police expect to roll out new dispatch system on Nov. 15**
Lacombe Police Service expects to roll out a new dispatch system designed to speed up response times on Nov. 15. Barring any last-minute snags, in mid-November 911 calls will be passed directly from the 911 centre to Lacombe police without first going through the RCMP's communication centre in Red Deer. Red Deer Advocate, A4

*** Charge pending for officer who stopped Green**
A provincial police oversight agency has directed Hamilton police to lay a disciplinary charge against one of its officers accused of "carding" a black city councillor. The Police Services Act charge will be officially laid when the officer makes his first appearance on Dec. 15, says Clint Twolan, president of the Hamilton Police Association. The officer has continued to perform his regular duties throughout the complaint process. Hamilton Spectator, A3

*** Retirement number forces police budget tweak**
Winnipeg Police find themselves $2 million over budget on salaries and expenses this year. Acting chief Art Stannard told the Winnipeg Police Board Friday retirement numbers have fallen short of WPS projections for the year. Winnipeg Free Press, 1

*** Working on use-of-force policy**
The Winnipeg Police Board is prioritizing the establishment of a use-offorce policy for the Winnipeg Police Service and will seek public feedback on the issue. The board announced Friday it has approved a draft for a policy on use of force in shaping how WPS members conduct themselves in the line of duty. A repor t that went before the board Friday morning said the intent is to "promote officer and community safety, effective policing, accountability and trust between the public, the board and the service." Winnipeg Sun

*** Board formalizes appointment; WPS salary budget topped up**
The Winnipeg police board has confirmed the appointment of Danny Smyth as the next police chief. Board members voted unanimously on the recommendation from the board's recruitment committee. The move wasn't a surprise given all members of the board were members of the recruitment committee. Winnipeg Free Press, B1

Kinder Morgan braces for Standing Rock-type protests
A person only has to read a few of the stories about the Standing Rock protest or see some of the pictures and videos to get a sense of the hostile stalemate over the construction of the new Dakota Access pipeline. The protests in North Dakota began small and peaceful, but grew in support and captured the attention of the continent... "I'd be naive if I didn't expect that," said CEO Ian Anderson told

reporters recently in Calgary... Meetings with RCMP. The preparations involve meeting with law enforcement. "We've been in deep conversations with policing authorities, RCMP in the planning for our project - what can we anticipate and what their role needs to be," said Anderson. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Complaints skyrocket at women's prison**
The number of complaints to the Correctional Investigator from women at the federal women's prison in Kitchener has skyrocketed in the past three years, Correctional Investigator Howard Sapers received 344 complaints from Grand Valley Institution in 2015-16 — about 41 per cent of all complaints from women in federal prisons anywhere in Canada. Of the 45 federal prisons across the country, only one other was the subject of more complaints. The number of complaints at Grand Valley has increased each year for the past several years, from 144 in 2013, to 193 in 2014, to 218 in 2015 — a 139 per cent increase in three years. "I think the numbers (of complaints) going up is indicative of how desperate some of the women are," said Kim Pate, executive director of the Canadian Association of Elizabeth Fry Societies, who added that her agency has encouraged women to complain more in an effort to get their concerns addressed. The Record, A1

*** Liberals outline mental health, justice priorities**
A Liberal government would refocus the implementation of the Yukon Mental Wellness Strategy and include comprehensive after-care services in the communities. Liberal Leader Sandy Silver and Jeanie Dendys, the party's Mountainview candidate in Monday's election, outlined their plan to improve mental health, justice and health care services Tuesday... Dendys, who is the Kwanlin Dun First Nation's justice director, said improved mental health services are just one part of a larger plan to improve the justice system. "A responsive and culturally relevant justice system will help protect all Yukoners, respect the human rights of incarcerated individuals and provide for rehabilitation that reduces the recidivism rates in the correctional system," she said. Daily Star, 10

*** Judge denies charter application for killer**
A criminal court is not the proper venue to award constitutional damages to someone who suffered a psychotic breakdown after spending 18 consecutive months in solitary confinement, a judge has ruled. Ottawa defence lawyer Dominic Lamb filed a charter application Friday in the hopes that Ontario Superior Court Justice Robert Maranger would make a declaration that Mutiur Rehman's constitutional rights were violated in jail and award damages for those breaches, but he left the courthouse with neither. Ottawa Citizen, A5

Pregnant killer Kelly Ellard's boyfriend a 'person of interest' in drug dealer disappearance
The boyfriend of pregnant killer Kelly Ellard is a "person of interest" in the May 2016 disappearance of a low-level drug dealer, according to Parole Board of Canada documents. Darwin Dorozan, 42, had his parole revoked after Correctional Services of Canada officials were made aware of the investigation into the missing dealer, the just-released documents say. "On the same date full parole was granted, police advised CSC that you were a person of interest in the suspicious disappearance of a low-level drug dealer in May 2016," the parole board said in its Oct. 27 ruling... She was denied day parole in May despite the Parole Board of Canada noting that she was finally taking some responsibility for the murder and had made strides in her rehabilitation. Postmedia Network (Edmonton Sun, Ottawa Sun, Calgary Sun, Vancouver Sun, Winnipeg Sun, * Toronto Sun, * The Province)

Torture in our jails
An opinion piece states, "Humans are social animals. We need to interact with other humans merely to exist. Otherwise, we can perish. We may kill ourselves. We may be so emotionally shattered that we lose all sense of who we are... The British Columbia Civil Liberties Association has launched a constitutional challenge to the use of solitary confinement in Canadian federal prisons. The BCCLA says that in Canada one out of every four federal prisoners has spent some time in solitary. At any moment, in federal or provincial prisons, up to 1,800 people are confined in solitary..." National Post, A15

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Health Canada disputes police story on fentanyl**
Police were alerted by both phone and mail in July that there was liquid fentanyl in Hamilton, says Health Canada. The statement is in direct contradiction to police claims that the vice and drug unit were notified the week of Oct. 31 about the lab results and that they were not physical documents that landed on an officer's desk. Torstar (Hamilton Spectator, A1; The Record)

*** Une année meurtrière à Ottawa**
Ottawa pourrait supplanter Montréal au chapitre du nombre d'homicides en 2016. Malgré une population deux fois moins importante, la capitale fédérale affiche un bilan semblable à celui de la métropole québécoise. Vendredi, le Service de police de la Ville de Montréal (SPVM) comptait 18 homicides sur son territoire, depuis le début de l'année. Au même moment, le Service de police d'Ottawa (SPO) en dénombrait 16. Le Droit, 3 / Front

*** Prudence avec les comparaisons**
Un professeur en criminologie de l'Université d'Ottawa privilégie la prudence avec les statistiques qui tendent à démontrer qu'Ottawa connaît plus d'homicides per capita que Montréal. «Mais je demeure quand même impressionné par la chute vertigineuse des homicides à Montréal», dit Ronald-Frans Melchers de l'Université d'Ottawa. Selon lui, il vaut mieux être prudent avec les données brutes concernant les homicides rapportés à Ottawa et Montréal, en 2016. Bien que les deux villes aient une certaine parité en 2016, le criminologue préfère comparer les statistiques sur les Régions métropolitaines de recensement (RMR) et se fier aux taux d'homicides calculés par Statistique Canada. Le Droit, 2

*** So many cops aren't neighbours**
An opinion piece states, "The irony made me smile. On Sunday, in the midst of getting ready to negotiate a new contract with the city, the Winnipeg Police Association is conducting a door-to-door public relations campaign they're calling Neighbour to Neighbour Outreach. On Tuesday - two days before the Neighbour to Neighbour news release - I had called police union president Moe Sabourin to inquire about how many of his membership aren't really neighbours. I wanted to know how many live outside the city. For years, it's been well-known that when large numbers of city police officers leave work, they head home to neighbourhoods or acreages outside the city that pays them so handsomely..." Winnipeg Free Press

What happens when our schools aren't safe for all students?
An opinion piece states, "Imagine videos purportedly showing violent "Jewish takeovers" or "homosexual takeovers" of Paris and London, or a video headlined: "Must see: Dutch mayor tells fellow Jews they can f------ if they don't like freedom." To some it may be just the simple exercise of free speech rights. Others will argue that as distasteful as they are, a person must have the right to express such views. Yet others may feel that these cross the line into hate..." Toronto Star

Religious neutrality bill comes in for embarrassing criticism
An editorial states, "The Couillard government's legislative venture into identity politics is not going well. Last year, to keep an election promise made under pressure from the nationalist opposition parties, the Liberal government introduced an anti-"radicalization" package of measures aimed at Muslims in particular..." Montreal Gazette, A14

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Call for peace**
It's a call for justice. And, it's a call for healing, said Catherine Dickson one of the leaders for the recent CGIT and explorers pilgrimage walk. "This is a response to the call from the aboriginal community to

make a change," she said. Dickson, and about 30 others, participated in the walk in October to raise awareness about murdered and missing aboriginal women in Canada. Charlottetown Guardian, C4

*** We can't afford to ignore indigenous women and girls**
Before providing aid money to support resource-development projects in other countries, Canadian policy requires a careful examination of how the project might affect the lives and safety of women and girls... In 2004, Amnesty International published a report called Stolen Sisters, which demonstrated that the economic marginalization of indigenous women and the discrimination they face in Canadian society are critical factors putting them in positions of increased risk, fuelling violence against them, and denying them the protections and support they deserve. At the time, we noted that indigenous women had long struggled to draw public attention to these issues and that there was already, at that point, a significant body of government reports and other studies pointing to the need for action. Yet it is only now, with the launch of a national inquiry on missing and murdered indigenous women and girls, that we begin to see real government acknowledgment of the scale and urgency of this crisis. Globe and Mail, S2

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Police hope pot shop raids**
Ottawa police raided six marijuana dispensaries Friday morning, closing a big chunk of the city's pot shops in one fell swoop... The targeted shops are operated by a B.C.-based outfit that moved into Ottawa this summer, opening dispensaries called Green Tree, WeeMedical and CannaGreen. Ottawa Citizen, A2

*** Local Ottawa politicians applaud raids on marijuana dispensaries**
Local politicians in Ottawa are applauding the closure of a string of marijuana dispensaries operating illegally in the city. Police arrested nine people and raided seven pot shops this week after mounting complaints from community members and councillors. "I'm happy with the level of response that OPS has put in," said Jody Mitic. "We were kind of tightening the screws a little bit on the [police] chief." CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

Feds' payroll system a nightmare
An opinion piece states, "Over 30,000 workers are waiting to have their paycheques fixed, many haven't been paid in months, due to the federal government's new pay system, Phoenix. Phoenix was rolled out in February of 2015, despite being warned by the Public Service Alliance of Canada (its largest union), that the system was flawed..." Windsor Star, A6

OTHER / AUTRE

NIL

INTERNATIONAL

*** Paris pour un "meilleur encadrement" des armes à feu**
Le ministre français de l'Intérieur, Bernard Cazeneuve, a appelé vendredi l'Union européenne à un " meilleur encadrement " de la circulation des armes à feu dans le cadre de la lutte contre le terrorisme. " Nous devons avancer " et " être fermes " sur l'adoption par le Parlement européen d'une nouvelle directive sur les armes à feu, a insisté le ministre qui recevait le Britannique Julian King, nouveau commissaire européen en charge de la sécurité et de la lutte contre le terrorisme. Les États membres de l'UE se sont mis d'accord en juin sur un renforcement des règles de contrôle des armes à feu au terme d'une négociation difficile. Mais l'adoption définitive de la directive requiert désormais un vote favorable du Parlement européen. Pour M. Cazeneuve, il s'agit de " permettre un meilleur encadrement et une

meilleure traçabilité des armes à feu au niveau européen '', une priorité de la France. Agence France-Presse (Le Devoir, C6)

Les déplacés de Boko Haram - Venir en aide malgré le silence médiatique
Dans l'Extrême-Nord du Cameroun, l'organisme de bienfaisance L'Oeuvre Léger offre depuis six mois une aide humanitaire d'urgence aux déplacés internes du groupe terroriste Boko Haram. Un aspect du conflit peu médiatisé, alors que des milliers de Camerounais souffrent de malnutrition et n'ont accès ni à des soins de santé ni à de l'eau potable.\r\n'' Les 31 500 personnes à qui le projet vient en aide sont victimes de violation grave des droits de la personne, en vertu du droit humanitaire international '', lance d'emblée Chanèle Boulet-Gauthier, coordonnatrice de l'action humanitaire à L'Oeuvre Léger et responsable du projet. En partenariat avec une ONG locale, le Comité diocésain de développement (CDD) -- Caritas du Cameroun, et avec le soutien d'Affaires mondiales Canada, ce projet vise à aider les déplacés dans la région de l'Extrême-Nord ainsi que les membres des communautés hôtes. '' Le projet vient casser le cycle de vulnérabilité de ces personnes '', présente la coordonnatrice, précisant que dans cette région, la plus pauvre du pays, les déplacements de population provoquent des situations particulièrement difficiles. Le Devoir, I4

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
December 15, 2016 / le 15 décembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Un projet pour détecter les fautifs
Les automobilistes de plusieurs provinces et territoires canadiens pourraient bientôt se faire demander par des policiers de se soumettre à un test de salive sur une base volontaire et ainsi participer à un projet pilote visant à mieux détecter la conduite affaiblie par la consommation de drogue. L'initiative menée par le gouvernement fédéral, la Gendarmerie royale du Canada (GRC) et plusieurs services de police du pays vise à déterminer quels appareils fonctionnent le mieux pour détecter la présence de drogue dans la salive. Le **ministre de la Sécurité publique, Ralph Goodale**, a indiqué que son ministère et le Conseil canadien des administrateurs en transport motorisé (CCATM) travailleront en collaboration avec les forces policières pour tester deux systèmes de détection différents. De tels appareils permettent de déceler la présence de cannabis, de cocaïne, de méthamphétamine et d'opioïdes. (…) Les services de police des villes de Gatineau, Toronto, Vancouver et Halifax participeront au projet pilote, de même que la Police provinciale de l'Ontario et les détachements de la GRC à North Battleford, en Saskatchewan, et

à Yellowknife. (…) ***«La mise à l'essai de ces nouveaux appareils de détection de drogues constitue une étape importante de nos efforts soutenus visant à renforcer l'application des lois sur la conduite avec les facultés affaiblies par la drogue, à réduire la conduite avec les facultés affaiblies par la drogue et à améliorer la sécurité de tous les Canadiens»,*** a soutenu **le ministre Goodale** dans un communiqué. Le Nouvelliste, 24 (Voix de l'Est, Le Quotidien); Canadian Press (Chronicle Herald, Waterloo Record, Hamilton Spectator, Cape Breton Post); Postmedia Network (Leader-Post, Star Phoenix); Journal de Montréal; Radio-Canada

Spies and lies, but no lost jobs
An editorial states, "This goes from the sublime to the bizarre - and beyond. Back in November, the Canadian Security Intelligence Service found itself in the hottest of hot water: a Federal Court judge ruled that the spy agency had broken the law by collecting and storing information it was not legally entitled to gather - in particular, metadata on innocent Canadians unconnected in any way with legal investigations. The judge ruled, in fact, that CSIS misled the court when the agency had applied for special warrants to collect documents. It was a huge embarrassment for the spies, especially when the federal government would not appeal the ruling. The information was collected starting in 2006, and processed through the secretive Operational Data Analysis Centre. But things are twistier than just a decade's worth of private information unlawfully held by the agency. Last week, a federal committee was told that the spy agency hasn't gotten rid of the material it was never supposed to have, even though it was illegally collected in the first place. CSIS director Michel Coulombe told the committee that it should know, within six months or so, what it will do with the data. And federal **Public Safety Minister Ralph Goodale** told the committee that he's still deciding whether the spy agency should be allowed to retain and process such information." Waterloo Record, A10 (Hamilton Spectator)

Canada's top spy "watchdog" says Edward Snowden should be shot
An opinion piece states, "Michael Doucet—the director of the government "watchdog" agency tasked with ensuring the Canadian Security Intelligence Service (CSIS) doesn't violate Canadians' rights—has publicly declared that US National Security Agency (NSA) whistleblower Edward Snowden should be shot. Far from being an individual outburst, Doucet's remarks exemplify broad sentiments within establishment circles. More than three years after Snowden lifted the veil on the NSA's illegal activities, including the major role that Canada plays in the NSA-led "Five Eyes" global spy network, the Canadian ruling elite remains outraged at his exposures. The head of the Security Intelligence Review Committee (SIRC), Doucet responded to a question at a recent talk he gave at Toronto's Ryerson University on what Snowden's fate would have been had he been Canadian by saying, "Do you want my opinion on that? Do you really want it? I'll give it to you. If Edward Snowden had worked for CSIS and did what he did, he should be shot." Doucet's outburst underscores the fraudulent character of the SIRC and like government "oversight" bodies charged with ensuring CSIS, Canada's premier intelligence agency, and other parts of the national-security apparatus don't violate Canadians' civil liberties. (…) The Liberal government response to Doucet's inflammatory comments is no less revealing. Asked about them, **Public Safety Minister Ralph Goodale** noted blandly, ***"That remark strikes me as highly inappropriate."*** Beyond this, there has been no official government response, let alone any suggestion that Doucet should be removed or otherwise sanctioned. Nor have the opposition parties seen fit to raise the issue. As for the corporate media, only the *Globe and Mail* reported Doucet's remarks and **Goodale's** tepid criticism of them." World Socialist Web Site

TOP STORIES / MANCHETTES

*** Assaults, violence leading causes of injury for Mounties**
More than 530 Mounties were injured on the job last year while being subjected to assaults and other violent acts - usually during incidents where officers had to use force to subdue someone. The information is contained in the RCMP's 2015 report on occupational health and safety, obtained by CBC News, which looks at everything from ergonomics at employees' desks to on-the-job injuries and fatalities. The report notes that physical control is more effective in subduing a suspect than using current "intermediate weapons," such as a baton or a stun gun. No one from the RCMP responded to CBC's request for information or an interview. CBC News

*** Operation Picnic was secret phone-tapping feast for RCMP, historian discovers**
The federal government secretly gave RCMP security officials the authority to tap telephone calls without court oversight during the Cold War, newly unearthed archival documents show. The surveillance program, codenamed "Picnic," began as an emergency effort during the Korean War, but federal agencies collaborated with telephone companies in 1954 to continue the wiretaps, says Dennis Molinaro, who teaches history at Ontario's Trent University. Molinaro's research indicates the RCMP security branch was listening in on the embassies of East Bloc countries, "certain unfriendly organizations" and individuals suspected of disloyalty. It has long been known the Mounties kept an eye on a wide array of people and organizations — from church and gay rights groups to Quebec separatists and Communists — in the name of national security, amassing hundreds of thousands of dossiers. Mountie scandals in the 1970s led to a royal commission, the demise of the RCMP security service and creation in 1984 of the civilian Canadian Security Intelligence Service. Molinaro believes the documentation he has uncovered with the help of tenacious staff at Library and Archives Canada helps flesh out how the RCMP surveillance of Canadians took place and implicates federal politicians and bureaucrats in making it happen. Canadian Press (Truro Daily); CBC News; 1

*** Police may soon ask you to spit for them for pilot project**
Drivers in some jurisdictions may soon find themselves asked by police to volunteer for a saliva test, part of a pilot project aimed at detecting drug-impaired drivers. The "oral fluid" screening systems test saliva for the presence of drugs, including cannabis, cocaine, methamphetamine and opioids. Police forces in Toronto, Vancouver, Halifax and Gatineau, Que., will take part in the project, along with the Ontario Provincial Police and RCMP detachments in North Battleford, Sask., and Yellowknife. Police officers will be trained in the use of two types of screening devices, but only with drivers and passengers who volunteer to provide a sample anonymously. Toronto Star

Inmates sue Ottawa over solitary confinement
A $600-million class action lawsuit was certified in an Ontario court this week, opening the door for thousands of prison inmates with diagnosed mental illnesses to seek compensation for their alleged mistreatment in federal jails. The lawsuit alleges Canada's federal prison agency fails to properly care for mentally ill inmates, relies too much on the "cruel and unusual punishment" of solitary confinement and neglects to adequately train its staff. Superior Court Justice Paul Perell ruled that the lawsuit should go ahead in a decision released Wednesday. (...) A spokesperson for the Justice Ministry referred questions on the lawsuit to the Correctional Service of Canada, the agency responsible for federal prisons. In an emailed statement, Corrections spokesperson Véronique Rioux said "effective and timely" treatment for inmates with mental illness is a priority for the agency. Front-line staff are trained to "understand the mental health needs of offenders," and $77 million was "invested" to address the needs of these inmates during the 2015-16 fiscal year, she said. Rioux added that segregation - the term the government uses for solitary confinement - is a legally available tool that is used to "manage risk," either to the inmate or staff, and is not a punitive measure. She said there are ongoing reviews of an inmate's placement in solitary confinement, including physical and mental health, and the agency is legally required to remove them from segregation "at the earliest time." She would not discuss the newly certified lawsuit, because it "is currently before the courts." Toronto Star, A1

Saskatchewan Penitentiary locked down in Prince Albert after 'major disturbance'
A lockdown was put in place Wednesday at the Saskatchewan Penitentiary following what Corrections Canada was calling "a major disturbance" and what the union representing guards was calling "a riot." "It was a flat-out riot," said James Bloomfield of the Union of Canadian Correctional Officers. "There are serious injuries and several inmates at outside hospitals right now. "There's been no staff hurt. Control has been gained at the institution. We're working through how we're going to be operating from here going forward." The lockdown was first instituted in the medium-security unit at about 1 p.m. Wednesday, and then expanded to the maximum-security unit at 3:30 p.m. as a precautionary measure. Visits to the prison in Prince Albert, Sask., were suspended. "It's still locked down," Jeff Campbell, spokesman for the Correctional Service of Canada, said late Wednesday. "It's been the scene of a major disturbance, so as I say, we're locked down in the interests, of course, of safety and security at the institution for the staff and inmates and the general public as well." He said to his knowledge, the involved prisoners had been

confined to their cells. "A lockdown takes place when there's a clear and substantial danger to safety and security at an institution," Campbell said. "Normal operations are suspended for the moment but they're going to be resumed as soon as it's considered safe to do that." Canadian Press (CTV News, Castanet, Global News, Times Colonist); CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

* **Du froid extrême s'amène sur les Maritimes et un blizzard à Terre-Neuve-et-Labrador**
Les résidents des Maritimes doivent s'attendre à du temps glacial accompagné de vent fort à compter de jeudi soir, tandis que ceux de certaines régions de Terre-Neuve-et-Labrador doivent se préparer à un blizzard. Environnement Canada estime que la température va chuter sous la barre de - 20 degrés Celsius dans l'ensemble du Nouveau-Brunswick. Le refroidissement éolien sera de - 35 vendredi. Les autorités recommandent aux gens de porter plusieurs couches de vêtements, des chaussettes chaudes, des gants, une tuque et un foulard. À l'Île-du-Prince-Édouard, Environnement Canada prévoit des rafales à 90 km/h avec des averses de neige et de la poudrerie, de jeudi soir à vendredi. La température pourrait chuter à - 20 degrés Celsius avec refroidissement éolien de - 30 vendredi matin. Radio-Canada

* **Messy morning for much of Newfoundland Thursday**
For the second morning this week, people in Newfoundland woke up to snow-covered roads Thursday morning as schools, government buildings and businesses have delayed openings with updates scheduled before noon. Check out the following links for a complete list of storm-affected openings in each area: Newfoundland East Storm Centre, Newfoundland Central Storm Centre and Newfoundland West Storm Centre. A snowfall warning is in effect for the eastern region of Newfoundland Thursday morning, with wind warnings for the east and south by evening and Friday morning. CBC News

* **'Significant precipitation' could develop over southern Ontario Friday evening - Environment Canada says snow or a mix of snow and rain may continue straight through Saturday**
Environment Canada has issued a special weather statement for much of southern Ontario in anticipation of "significant precipitation" starting Friday evening. The federal agency also issued a winter travel advisory Thursday for much of the Greater Toronto Area, warning that bands of snow coming inland from Lake Huron will bring brief periods of heavy snowfall and blowing snow. The weather "will make travel hazardous at times," and "brief whiteouts may occur," the advisory said. It covers Toronto and Hamilton, as well as parts of Halton, Peel, York and Durham regions. CBC News

* **Residents unaccounted for after fire at First Nation near London, Ont.**
Ontario Provincial Police say the residents of a home engulfed in flames on a southern Ontario First Nation remain unaccounted for. Emergency crews were called to the home on the Oneida Nation of the Thames, southwest of London, at about 11 a.m. Wednesday. Police, however, have not yet indicated how many people are unaccounted for, nor have they released any information on their ages of genders. There was also no immediate information on what caused the blaze. The Ontario Fire Marshal's Office has been called in to investigate. Canadian Press (Truro Daily News); Windsor Star

* **Letter on flood dam investigation rankles Springbank landowners**
The province's letter on a review of a contentious flood mitigation project has angered some opponents of a dry dam planned for Springbank. In a Dec. 9 email sent to Rocky View County residents, an impending engineering and environmental review of the McLean Creek site is described partly as a means to confirm the merits of the Springbank location for a dry dam to which the province has committed. "This additional work is intended to further demonstrate the essential nature of this project and support the position that SR1 is the best course of action - environmentally, financially and in the best location - to protect communities downstream," it states... Opponents, primarily some area landowners, argue the Springbank proposal to divert the Elbow River during a time of extreme flooding would disrupt their lives and be environmentally and financially costly. Proponents in Calgary say it's the best way to protect far more people from 2013-scale flooding downstream. Calgary Herald, A10

*** B.C. wants Ottawa to reopen Comox centre in its marine safety plan**
B.C. wants the federal government to reopen the coast guard marine communications centre in Comox, as part of Ottawa's recently announced $1.5-billion ocean-protection plan. Naomi Yamamoto, Minister of State for Emergency Preparedness, wrote to Federal Fisheries Minister Dominic LeBlanc on Tuesday "to express my continued concern" about the Comox closure and request it be reopened in the federal plan. "British Columbians need to know they can rely on assistance from the Canadian Coast Guard during emergencies," wrote Yamamoto. "Recent events have highlighted the need to maintain reliable communications to support a swift marine response. "I am asking that the safety and protection of our marine users, coastal communities and environment continue to be given the highest priority and that due consideration be given specifically to the reopening of the Canadian Coast Guard Comox Marine Communications and Traffic Services Centre." The Comox centre was closed in May. A similar closure at Vancouver's Kitsilano Coast Guard Station was subsequently reversed by Prime Minister Justin Trudeau. But the Comox station remained closed, after a parliamentary committee concluded it wouldn't affect emergency response on the West Coast. Vancouver Sun

*** Small earthquake rattles nerves of some homeowners in southwestern Nova Scotia**
A small earthquake rattled some nerves on Nova Scotia's south shore on Tuesday. Earthquakes Canada said the 3.0-magnitude earthquake was reported around 10:40 a.m. and was centered about 42 kilometres southwest of Digby, between Weymouth and Meteghan. The Earthquakes Canada website says more than a dozen people have reported feeling the earthquake. Canadian Press (Times and Transcript, B6)

*** Warship crew helped out in quake**
The commanding officer of the warship that helped with relief efforts after a major earthquake in New Zealand said the mission offered a valuable learning experience for the Royal Canadian Navy, which would be called into action in the event of a major earthquake on the West Coast. The crew of HMCS Vancouver spent five days delivering humanitarian aid to Kaikoura, a small coastal town 180 kilometres north of Christchurch, which was cut off after a 7.8-magnitude earthquake on Nov. 14 caused landslides and damaged roads. "It was an excellent opportunity to practise some things we probably need to do if we have a similar event here, so it was great training," Cmdr. Clive Butler said from a jetty at CFB Esquimalt during the ship's homecoming ceremony Wednesday. "A number of government departments will have a role to play if there's an event like that here, and that's what struck me, it was really an all-government effort there. [There were] civilian emergency-response folks working, police, fire, ambulance and navies from four countries." Times-Colonist, A4

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Operation Picnic was secret phone-tapping feast for RCMP, historian discovers
The federal government secretly gave RCMP security officials the authority to tap telephone calls without court oversight during the Cold War, newly unearthed archival documents show. The surveillance program, codenamed "Picnic," began as an emergency effort during the Korean War, but federal agencies collaborated with telephone companies in 1954 to continue the wiretaps, says Dennis Molinaro, who teaches history at Ontario's Trent University. Molinaro's research indicates the RCMP security branch was listening in on the embassies of East Bloc countries, "certain unfriendly organizations" and individuals suspected of disloyalty. It has long been known the Mounties kept an eye on a wide array of people and organizations — from church and gay rights groups to Quebec separatists and Communists — in the name of national security, amassing hundreds of thousands of dossiers. Mountie scandals in the 1970s led to a royal commission, the demise of the RCMP security service and creation in 1984 of the civilian Canadian Security Intelligence Service. Molinaro believes the documentation he has uncovered

with the help of tenacious staff at Library and Archives Canada helps flesh out how the RCMP surveillance of Canadians took place and implicates federal politicians and bureaucrats in making it happen. Canadian Press (Truro Daily, Chronicle Herald, CTV News); CBC News

Police seek terrorism peace bond for B.C. man
A British Columbia man has been arrested on a terrorism peace bond, officials said Wednesday, marking the 19th time since last year police have used the legal tool against suspected extremists. Khalid Ahmed Ibrahim was to appear in provincial court in New Westminster, B.C. on Dec. 20. Police told the court on Dec. 8 there were reasonable grounds Ibrahim "may" commit a terrorism offence. He has also been charged with uttering threats, court staff said. The threatening charge dates to July 19 and was to return to court Dec. 21. No further details about Ibrahim or the allegations were available. The arrest was made by RCMP in B.C., according to the Public Prosecution Service of Canada. Postmedia Network (Vancouver Sun, N6, The Province, National Post, Calgary Sun) (2016-12-15); * Vice News (2016-12-14)

*** Canadian man arrested over fears he might commit act of terrorism**
25 conditions - Canadian cops arrested, and released, a man over fears he may commit an act of terrorism. Now he's living with his mother and facing 24 other restrictions on his freedom. Police are pursuing a terrorism-related peace bond against a 39-year-old man from British Columbia, who has since been released from custody under at least 25 bail conditions. Police believe Khalid Ahmad Ibrahim "did cause fear of terrorism" on December 8, according to court documents obtained by VICE News. A peace bond is not a formal criminal charge, but can allow police to restrict someone's movement and activities and is easier to obtain than criminal charges. Ibrahim's case is the 19th time that police have pursued the controversial tool meant to deter terror over the last year. But as the National Post first reported Wednesday, Ibrahim was also formally charged with uttering threats in July of this year... Ibrahim is the third person from BC to face a terror-related peace bond, according to a list provided to VICE News from the Public Prosecution Service of Canada. John Nuttall and Amanda Korody, of Victoria, are waiting for the outcome of their terrorism-related peace bond applications. The couple had their terrorism criminal charges stayed this summer after a BC judge ruled they had been entrapped by the RCMP. Vice News (2016-12-14)

*** Who speaks for Muslims?**
A letter to the editor from Martin Collacott, former Canadian ambassador to Syria and Lebanon, states "Ihsaan Gardee, the executive director of the National Council of Canadian Muslims, criticizes columnist Barbara Kay for suggesting that his organization has to be treated with considerable caution. Among other things, Kay points out in her column that the group has a history of threatening legal action against those who level charges of worrisome connections against them. In his rejoinder, Gardee chooses not to mention that the FBI ceased working with the NCCM's parent organization, the Council on American-Islamic Relations, in 2008 after evidence emerged that linked the group to support for questionable causes. He also fails to note that in 2014 the RCMP withdrew its support for a handbook titled United Against Terror prepared in part by the NCCM due to its adversarial tone including, according to media reports, counselling Canadian Muslims to limit the extent of their co-operation with Canadian security and intelligence agencies." National Post, A12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Number of asylum-seekers crossing illegally into Quebec from U.S. spikes
823 caught crossing Quebec's border between April 1 and Nov. 30, 2016, compared to 166 two years ago. The number of asylum-seekers entering Quebec illegally from the United States has more than quadrupled in the last three years, according to an exclusive report by Radio-Canada. According to the Canada Border Services Agency, 823 refugee claimants were taken into custody by the RCMP between April 1 and Nov. 30, 2016, after illegally crossing into Quebec. By comparison, the RCMP detained 166 asylum-seekers for entering Quebec illegally in the year between April 1, 2014, and March 31, 2015, and another 315 between April 1, 2015, and March 31, 2016. Last month alone, 273 asylum-seekers entered Quebec illegally — by far the highest one-month total for the three years. "They come regularly every week," said retired police officer Francois Doré, who lives near the Roxham Road crossgin near

Hemmingford, about 70 kilometres south of Montreal. Doré said the migrants cross the Canadian border easily enough, passing under yellow tape that divides the two countries. "Sometimes you see whole families with babies and suitcases," Doré said, adding that many arrive by taxi. CBC News

*** A Trump bump? American refugee claims in Canada increased last month**
The number of Americans seeking refugee status in Canada has experienced a significant bump this year, increasing more than five times in November 2016 from the same period a year earlier. The overall numbers, however, remain tiny. Few people seek to flee the world's largest economy, and one of its oldest democracies, on humanitarian grounds: A mere 170 Americans claimed asylum at Canada's land borders through the first 11 months of this year. Yet that was more than twice the total from 2015 — and it was led by a noticeable five-fold increase in the month of November, with 28 people claiming refugee status last month compared with merely five in November 2015. Was any of this driven by politics — and Donald Trump's Nov. 8 election? The Canadian government won't touch that question. "Refugee claims are protected under the Privacy Act," said Nicholas Dorion, a spokesman for the Canada Border Services Agency, which supplied the figures to The Canadian Press. "Therefore the CBSA will not discuss specifics of asylum cases." Canadian Press (Metro News)

Le fédéral confirme qu'il bannit l'utilisation et l'importation d'amiante au Canada
L'utilisation de l'amiante dans toute nouvelle construction au pays, et son importation, seront interdites par le gouvernement fédéral. Ces mesures entreront en vigueur d'ici 2018. Comme Radio-Canada l'annonçait la semaine dernière, Ottawa ne prend pas la chose à la légère. Quatre ministres libéraux présentent, jeudi matin, une stratégie nationale au Centre de cancérologie de l'Hôpital d'Ottawa. Ils seront accompagnés de personnes souffrant de problèmes de santé à la suite d'une inhalation prolongée d'amiante. La raison fondamentale, c'est vraiment pour la sécurité des travailleurs et la sécurité des citoyens. Marie-Claude Bibeau, ministre du Développement international et de la Francophonie Le gouvernement fédéral lancera donc prochainement un processus de modification de la Loi sur la protection de l'environnement, afin d'y inclure une interdiction d'utiliser de l'amiante. Une série de mesures L'Organisation mondiale de la santé (OMS) a condamné ce produit dès 1987, puisqu'il est cancérigène et peut entraîner des problèmes pulmonaires. Pourtant, l'amiante n'a jamais été entièrement proscrite dans le Code national du bâtiment du Canada, alors que plus d'une cinquantaine de pays l'ont fait. Radio-Canada

Fin du principe de « premier arrivé, premier servi »
Ottawa change les règles d'immigration en matière de réunification familiale afin de privilégier le hasard plutôt que la ruse ou l'argent. Jusqu'à présent, certains Canadiens pouvaient payer des centaines de dollars pour s'assurer que le dossier des proches qu'ils souhaitaient parrainer se retrouve au sommet de la pile évaluée par les fonctionnaires fédéraux. Mercredi, le ministre de l'Immigration, des Réfugiés et de la Citoyenneté, John McCallum, a annoncé un changement des règles pour 2017. Ceux qui veulent faire venir un parent ou un grand-parent au pays auront 30 jours à compter du 3 janvier pour remplir un simple formulaire en ligne. Le ministère sélectionnera au hasard 10 000 personnes, qui seront alors appelées à envoyer par la poste une trousse de demande complète. Jusqu'à cette année, le fédéral fonctionnait selon le principe du premier arrivé, premier servi. En conséquence, des demandeurs se prévalaient de coûteux services de courrier, qui gonflaient leur prix pour l'occasion. D'autres faisaient le pied de grue devant l'unique bureau d'immigration qui acceptait les formulaires, à Mississauga, en banlieue de Toronto. Selon M. McCallum, cette nouvelle façon de faire assurera que « tout le monde aura la même chance ». La semaine dernière, le ministre avait annoncé qu'il prendrait des mesures pour accélérer les demandes de réunifications familiales, et abaisser les délais à 12 mois. Voix de L'Est

U.S. border cities fear ending NAFTA would hurt economies
Donald Trump's only visit to the U.S.-Mexico border while running for president was a stop in Laredo that lasted less than three hours. On some days, that's not long enough for 18-wheelers hauling foreign-made dishwashers and car batteries to lurch through the gridlocked crossing. Trump's campaign promise to tear apart the North American Free Trade Agreement helped win over Rust Belt voters who felt left behind by globalization. But the idea is unnerving to many people in border cities such as Laredo and El Paso or Nogales in Arizona, which have boomed under the 1994 treaty. About 14,000 tractor-trailers cross the border daily in Laredo, the nation's busiest inland port. Local officials say roughly 1 in every 3 jobs

benefits from international trade. "We are NAFTA on wheels," Mayor Pete Saenz said. Free trade across the border, he explained, is the "backbone" of this city of 255,000 people. The Democrat endured a backlash from his party for welcoming Trump in July 2015 after the then-candidate called immigrants from Mexico criminals and rapists. Trump described NAFTA as "the worst single trade deal ever approved in this country." That kind of talk resonated in hard-hit industrial towns such as Greenville, Michigan, where Electrolux shut down a factory a decade ago and moved jobs to the Mexican border city of Ciduad Juarez. CTV News

Glib talk about NAFTA won't help Canada
Suggestions that we could still thrive without the North American free-trade agreement ignore the realities of our relationship with Mexico. The election of Donald Trump as president of the United States has prompted a flurry of speculation about what his campaign pledge to renegotiate or withdraw from the North American free-trade agreement might actually mean. A number of commentators have been quick to suggest that if Mr. Trump tore up NAFTA it would be no big deal, because we could just fall back on the Canada-U.S. free-trade agreement (FTA). Part of this narrative then becomes that our relationship with Mexico doesn't really matter much. I strongly disagree on both counts. Here are two points of advice for Canada: One, let's wait to see what Mr. Trump as president actually decides to do about NAFTA, rather than react publicly to his campaign rhetoric; and two, given the seriousness of the situation, the government should urgently, but quietly, begin preparations for a possible renegotiation of NAFTA. Given the primordial importance of our trade relationship with the United States, some Canadians might be forgiven for occasionally forgetting about the importance for Canada of our other NAFTA partner. (…) Under the influence of NAFTA Mexico has become our fifth-largest export market and our third-largest supplier. Trade between Mexico and Canada has grown by more than 800 per cent since NAFTA came into force. Much of the trade with Mexico is inputs to North American supply chains, inputs that help make North American companies more competitive on a global basis. Globe and Mail

*** Piant ne sera jamais remis en liberté au Canada**
Si l'on se base sur les lois canadiennes, Claude-Auguste Piant sera pris en charge par l'Agence des services frontaliers du Canada (ASFC) dès sa sortie de prison avant d'être expulsé du pays. Ce ressortissant français de 62 ans a été condamné en début de semaine à 30 mois de prison pour avoir trempé dans une affaire d'inconduite sexuelle avec une adolescente de 15 ans à Sherbrooke. Sans commenter ce cas précis, l'ASFC explique que « les étrangers reconnus coupables d'avoir commis des actes criminels ont droit à une application régulière de la loi. Ils doivent purger leur peine avant d'être renvoyés du Canada », explique l'Agence des services frontaliers du Canada. Piant devra donc régulariser sa situation criminelle en purgeant sa peine avant que soient appliquées les affaires d'immigration. « Il y a sursis de la mesure de renvoi tant que n'est pas purgée la peine d'emprisonnement infligée au Canada à l'étranger », stipule la loi sur l'immigration et la protection des réfugiés du Canada. Pour le moment, l'ASFC ne peut expulser Claude-Auguste Piant du Canada tant que sa peine de prison ne sera pas expirée. Une fois la peine terminée, Piant ne sera pas remis en liberté. Un renvoi du Canada sera alors exécuté. Pour le moment, Claude-Auguste Piant purgera sa peine au Canada. Tribune

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** More than just hacks: Russia's 'hybrid warfare' has been targeting western Europe for months**
One might wonder whether the suspected Russian cyberattacks during the U.S. election were serious enough to warrant all the calls for investigation - an argument that could be made, were it not for all the other cases worrying Western governments.Start with remarkably similar warnings of Moscow's interference and cyber-sabotage voiced by Germany, France, Britain, Poland and Sweden, along with much of NATO and even the security committee of the European Union. To view the cyberattacks on Hillary Clinton's campaign, then, as a unique offence - as many Americans seem to do - is to miss the full picture. Western Europe has been a far more consistent target of what some intelligence chiefs now see as "hybrid warfare" emanating from the Kremlin. European spymasters have repeatedly expressed alarm over the years about a sharp rise in Russian espionage under Vladimir Putin. But what is far more worrisome are the attempts to destabilize Western governments through the same cocktail of political interference. CBC News

*** Poutine aurait été impliquédirectement dans le piratage des démocrates américains**
Des responsables américains du renseignement estiment que le président russe Vladimir Poutine s'est personnellement impliqué dans les piratages informatiques qui ont marqué l'élection présidentielle américaine, motivé par un désir de revanche contre Hillary Clinton, avançait la chaîne NBC. Vladimir Poutine aurait lui-même donné les instructions sur la façon de filtrer et d'utiliser les messages dérobés aux démocrates après les piratages informatiques, affirmait la chaîne américaine mercredi soir, en citant deux hauts responsables ayant eu connaissance de cette information Les responsables disent avoir un «haut degré de confiance» dans ces conclusions. «Les absurdités ne peuvent reposer sur aucun fondement», a rétorqué jeudi le porte-parole du Kremlin Dmitri Peskov, balayant ces allégations. La CIA a conclu dans un rapport secret révélé la semaine dernière par le *Washington Post* que la Russie était intervenue par ses cyberattaques dans la campagne électorale dans le but précis d'aider Donald Trump à être élu, et non dans le but plus général de troubler le bon déroulement de l'élection. Le président élu a rejeté avec virulence ces allégations. Agence France-Presse (Journal de Montréal, Journal de Québec)

*** Georgia asks Trump to investigate 'failed cyber-attacks'**
The state of Georgia is asking President-elect Donald Trump to investigate what it described as "failed cyberattacks" on its secretary of state's network that it traced to the U.S. Homeland Security Department. In a letter Tuesday, Georgia Secretary of State Brian Kemp said his staff has uncovered nine more instances this year in which computers they traced back to the Homeland Security Department apparently attempted to infiltrate the state's network between Feb. 2 and Nov. 8. His letter followed earlier complaints that his office had detected what it called "a large attack on our system" one week after the presidential election. Trump's transition team did not immediately respond to a request for comment. Chronicle Herald, A10

*** Cyberaggression is the 'new normal' Trump can't ignore**
An opinion piece by Wesley Wark states, "The furor over allegations of Russian meddling in the U.S. election continues to grow and poses one of the first big tests for the incoming Trump administration. The story has a long trail, leading back to the summer of 2016, when FBI investigations into Russian hacking targeted at the presidential election began in earnest. Media reporting suggests the growing body of intelligence on Russian involvement in U.S. domestic politics even made its way into President Barack Obama's top level intelligence report - the President's Daily Brief - during the campaign. Very recently, the CIA reached a judgment, according to intelligence sources tapped by The Washington Post, that Russian hacking had a very specific aim - not just to undermine confidence in the U.S. electoral system, but to help Donald Trump win the election. This is an explosive charge, but one not limited to the U.S. arena. Concerns about Russian cyberaggression caused the head of Britain's Secret Intelligence Service, Alex Younger, to make a rare public speech, delivered from SIS headquarters on the Thames, charging that cyberattacks and information warfare represent "a fundamental threat to our sovereignty; they should be a concern to all those who share democratic values."" Globe and Mail, A13

*** Yahoo reveals hack affecting 1B users**
Yahoo has discovered a 3-year-old security breach that enabled a hacker to compromise more than 1 billion user accounts, breaking the company's own humiliating record for the biggest security breach in history. The digital heist disclosed Wednesday occurred in August 2013, more than a year before a separate hack that Yahoo announced nearly three months ago that affected at least 500 million users. Toronto Star

*** Yahoo's Big Breach Helps Usher in an Age of Hacker Anxiety**
Yahoo has become the worst-case example of an unnerving but increasingly common phenomenon — massive hacks that steal secrets and other potentially revealing information from our personal digital accounts, or from big organizations that hold sensitive data on our behalf. On Wednesday, Yahoo disclosed a gargantuan breach affecting more than a billion user accounts, the largest such attack in history. (...) "The lesson is clear: no organization is immune to compromise," said Jeff Hill, director of product management for cybersecurity consultant Prevalent. And since most of us are dependent on big organizations that hold our digital lives in their hands, in a broad sense that effectively means no one is safe. ABC News

*** Were Yahoo hackers state-sponsored?**
Yahoo has said more than one billion user accounts may have been affected in a hacking attack dating back to 2013. Names, phone numbers, passwords and email addresses were stolen, but not bank and payment data. Professor Peter Sommer, a cyber security expert, told the Today programme he questions "what on earth" would motivate a state to want details of ordinary users. BBC News

*** Ashley Madison pays $1.6M to settle hack probes**
The parent company of adultery website AshleyMadison.com, based in Toronto, has agreed to pay a steeply discounted $1.65 million (U.S.) settlement to resolve U.S. state and federal probes into a 2015 hack that exposed personal data of 37 million users of the site, whose slogan was "Life is Short. Have an Affair." The company, which changed its name to Ruby Corp. from Avid Life Media Inc. after the breach, agreed to a $17.5 million penalty to resolve the multi-state investigation, New York Attorney General Eric Schneiderman said in a statement. The amount was reduced by about 90 per cent due to an "inability to pay," and the rest was suspended. "Reckless disregard for data security will not be tolerated," Schneiderman, who joined with 12 other U.S. states and the U.S. Federal Trade Commission to announce the settlement. Hackers dumped almost 10 gigabytes of data on the Internet. Toronto Star

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Assaults, violence leading causes of injury for Mounties**
More than 530 Mounties were injured on the job last year while being subjected to assaults and other violent acts - usually during incidents where officers had to use force to subdue someone. The information is contained in the RCMP's 2015 report on occupational health and safety, obtained by CBC News, which looks at everything from ergonomics at employees' desks to on-the-job injuries and fatalities. The report notes that physical control is more effective in subduing a suspect than using current "intermediate weapons," such as a baton or a stun gun. No one from the RCMP responded to CBC's request for information or an interview. CBC News

*** Police may soon ask you to spit for them for pilot project**
Drivers in some jurisdictions may soon find themselves asked by police to volunteer for a saliva test, part of a pilot project aimed at detecting drug-impaired drivers. The "oral fluid" screening systems test saliva for the presence of drugs, including cannabis, cocaine, methamphetamine and opioids. Police forces in Toronto, Vancouver, Halifax and Gatineau, Que., will take part in the project, along with the Ontario Provincial Police and RCMP detachments in North Battleford, Sask., and Yellowknife. Police officers will be trained in the use of two types of screening devices, but only with drivers and passengers who volunteer to provide a sample anonymously. Toronto Star

*** Defence argues Travis Vader should serve no more jail time after claims of pre-trial abuse**
Travis Vader's lawyer is asking a judge to let his client go without serving more jail time or drop the case altogether. In a notice of motion filed in court, Nate Whitling argued that Vader's constitutional rights were violated following his arrest and during his lengthy imprisonment leading up to the trial. He argued Justice Denny Thomas should either impose a sentence equivalent to the time Vader has already served or impose a stay of proceedings, which would essentially drop the case. The document was filed Wednesday on the third day of Vader's sentencing hearing for two manslaughter convictions for the killings of Lyle and Marie McCann. A manslaughter conviction can result in a sentence ranging from probation to life in prison. During the sentencing hearing, which started Monday, Vader has testified he was subjected to a humiliating, recorded strip search after his arrest in 2010, was constantly harassed by remand centre guards, and endured abuse from other inmates. "The applicant was subjected to cruel and unusual conditions in pre-trial custody," according to the notice of motion. It also claimed the strip search was illegal and that RCMP denied Vader's right to seek legal advice when he was arrested six and a half years ago. But an extended audio recording played in court appeared to show that RCMP officers gave Vader all night to reach his defence lawyer after his arrest. When Vader finally reached the law office just after 9 a.m. the day after he was taken into custody, an RCMP officer could be heard saying, "The door is closed. I can't hear the conversation. I can see Mr. Vader talking to somebody, but I can't

hear the conversations they're having." CBC News (2016-12-14); Calgary Herald (Edmonton Journal, Edmonton Sun) (2016-12-15)

*** Police force needs more cops to maintain service: chief**
The current level of city policing is "not sustainable" without more officers and is taking a toll on members, according to Fredericton Police Chief Leanne Fitch. "We have been making it work for the last four years only because of the hard work, commitment and dedication of our officers," Fitch said in an interview with The Daily Gleaner earlier this week. "The city is still in good hands, has been in good hands, but I know the toll it is taking on our staff. "I have done my best to educate council to these realities." Fitch's comments came after council's rejection of a request from the force for an extra $440,000 to hire two police officers and several civilian employees in 2017. Councillors did, however, approve an extra $60,000 a year for the police to lease a new light armoured vehicle. In 2016, the police force budget was about $15.3 million. Council approved a 2017 police budget of $15.8 million, an increase of 3.63 per cent, compared to an overall municipal budget increase of 1.34 per cent. Most of that jump is a result of a newly negotiated police union contract, the city said. The force has 103 officers, including the chief and deputy chief. Fitch believes those officers will log about 10,000 hours of overtime this year at a cost of about $500,000. That translates into a lot of time where officers are away from home and working when they should be resting, she said. Daily Gleaner, A1 (Telegraph-Journal)

*** Arson with possible Mafia link probed**
Police are investigating an eastend arson with possible links to the Montreal Mafia. They opened the investigation early Wednesday after a used-car lot in Pointeaux-Trembles was apparently the target of a firebombing. Though his name does not appear in any of the business's paperwork, the car lot has links to alleged mobster Marco Pizzi, according to a report by La Presse. Pizzi, 46, survived an attempt on his life in August after two men tried to gun him down in his car on Grande-Allée St. He escaped on foot. He was arrested last May after an RCMP investigation into an alleged international cocaine trafficking ring. He was released on bail while awaiting his trial. Montreal Gazette, A8

*** 'Those Kugs' donate to Tuk A group...**
A group of Inuvialuit men who have formed "Those Kugs" gave a Christmas hamper donation of three turkeys and three hams to the community feast in Tuktoyaktuk. They organized the donation with the Tuktoyaktuk recreation department and RCMP to make the delivery. Inuvik Drum

*** RCMP may charge teen for sharing photo**
Queens County RCMP are considering laying charges against a 16-year-old boy relating to the sharing of an intimate photo. He allegedly sent a 12-year-old girl an image of himself through Snapchat. The boy reportedly asked for an image in return but the girl refused and reported the incident. "The investigation is ongoing and we will do a media release if and when we lay charges," RCMP spokeswoman Cpl. Jennifer Clarke wrote in an email. Chronicle-Herald, A3

*** Warrants to tell tale of 'scandalous' probe**
She is a TV reporter who exposed the rot in Quebec's construction industry; he is a print journalist known as much for his hard-news scoops as his opinion columns. Marie-Maude Denis and Patrick Lagacé are among at least eight journalists who were recently spied upon by either the provincial Sûreté du Québec or the Montreal Police Service. The first clear sense of what happened is set to come out soon in Montreal, where a court will release the first of dozens of warrants that targeted some of Quebec's best-known journalists. The disclosure could come as early as Thursday, or in ensuing days, depending on the ruling. The search warrants gave police unprecedented access to journalists' cellphones to track their movements and calls. They raise troubling questions about the relationships among officers, politicians and the judges who are supposed to keep the authorities in check. The Quebec government has launched a public inquiry into the surveillance, and the ramifications will go on for years. Globe and Mail, A3

*** Hells Angels bring trouble**
An editorial states, "The arrival of the Hells Angels on Prince Edward Island is a disturbing development. Motorcycle gang members are not the kind of newcomers we want to see in this province. They are

unwelcome visitors at any time, but especially around Christmas when expressions of peace and goodwill are on most lips. The Angels is the most notorious motorcycle gang in Canada. Wherever they set up, illegal activity follows. In some jurisdictions, violence is commonplace. The only reason the club has arrived on P.E.I. is to make money through criminal activity - likely drugs. Police seem powerless to stop them. All our law enforcement agencies can do is watch and let Islanders know what's going on." The Guardian, A6

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Inmates sue Ottawa over solitary confinement
A $600-million class action lawsuit was certified in an Ontario court this week, opening the door for thousands of prison inmates with diagnosed mental illnesses to seek compensation for their alleged mistreatment in federal jails. The lawsuit alleges Canada's federal prison agency fails to properly care for mentally ill inmates, relies too much on the "cruel and unusual punishment" of solitary confinement and neglects to adequately train its staff. Superior Court Justice Paul Perell ruled that the lawsuit should go ahead in a decision released Wednesday. (...) A spokesperson for the Justice Ministry referred questions on the lawsuit to the Correctional Service of Canada, the agency responsible for federal prisons. In an emailed statement, Corrections spokesperson Véronique Rioux said "effective and timely" treatment for inmates with mental illness is a priority for the agency. Front-line staff are trained to "understand the mental health needs of offenders," and $77 million was "invested" to address the needs of these inmates during the 2015-16 fiscal year, she said. Rioux added that segregation - the term the government uses for solitary confinement - is a legally available tool that is used to "manage risk," either to the inmate or staff, and is not a punitive measure. She said there are ongoing reviews of an inmate's placement in solitary confinement, including physical and mental health, and the agency is legally required to remove them from segregation "at the earliest time." She would not discuss the newly certified lawsuit, because it "is currently before the courts." Toronto Star, A1

Fentanyl puts prisoners and guards at risk
Correctional officers at the Bowden Institution rushed to the aid of one of their peers this week after a guard collapsed due to suspected fentanyl exposure. James Bloomfield, regional president of the Union of Canadian Correctional Officers, said staff at the medium-security facility immediately applied first aid and administered naloxone, a medication used to reverse the effects of opioids. The officer had been in the process of conducting a search for suspected drugs in the institution. "The officers that responded to this situation - they really did save this officer's life," said Bloomfield. (...) On Tuesday, the Bowden Institution announced that a lockdown was in effect to allow staff to conduct an "exceptional search." Bloomfield said the institution is currently under an "adjusted routine" due to the incident involving the officer. "We are currently under a searching protocol at the institution and trying to ensure we don't have any further drugs that we're going to be coming across, so we're taking all precautions necessary in that searching and just working our best through a tough situation," he said. The officer who collapsed Tuesday was taken to hospital and is now recovering well at home. Bloomfield noted the correctional facilities have various drug interdiction and searching strategies in an effort to keep the institutions drug free. However, despite those efforts, there are "so many different ways to bring drugs into an institution," he said. "It comes in everywhere - through visits, through getting thrown over the fences, to drone drops. Everything and anything you can imagine - when someone sits inside for 24/7 and tries to figure out how they're going to get their next hit, they come up with some pretty creative ways to bring stuff in." Correctional Service Canada has various programs to treat addictions among inmates, including a methadone program, he added. A spokesperson from Correctional Service Canada was not available to comment Wednesday. Calgary Herald, A3

Saskatchewan Penitentiary locked down in Prince Albert after 'major disturbance'
A lockdown was put in place Wednesday at the Saskatchewan Penitentiary following what Corrections Canada was calling "a major disturbance" and what the union representing guards was calling "a riot." "It was a flat-out riot," said James Bloomfield of the Union of Canadian Correctional Officers. "There are serious injuries and several inmates at outside hospitals right now. "There's been no staff hurt. Control has been gained at the institution. We're working through how we're going to be operating from here

going forward." The lockdown was first instituted in the medium-security unit at about 1 p.m. Wednesday, and then expanded to the maximum-security unit at 3:30 p.m. as a precautionary measure. Visits to the prison in Prince Albert, Sask., were suspended. "It's still locked down," Jeff Campbell, spokesman for the Correctional Service of Canada, said late Wednesday. "It's been the scene of a major disturbance, so as I say, we're locked down in the interests, of course, of safety and security at the institution for the staff and inmates and the general public as well." He said to his knowledge, the involved prisoners had been confined to their cells. "A lockdown takes place when there's a clear and substantial danger to safety and security at an institution," Campbell said. "Normal operations are suspended for the moment but they're going to be resumed as soon as it's considered safe to do that." Canadian Press (CTV News, Castanet, Global News, Times Colonist); CBC News

Les coûts d'incarcération presque deux fois plus élevés à la prison Leclerc qu'à Bordeaux
Le coût d'incarcération par détenu est presque deux fois plus élevé à l'établissement Leclerc, loué depuis deux ans au gouvernement fédéral, qu'à la prison de Bordeaux, révèlent des documents du ministère de la Sécurité publique. Chaque détenu coûte 299 $ par jour à la prison Leclerc, comparativement à 159 $ à la prison de Bordeaux, indique la Direction générale des services correctionnels. Ces coûts ont été estimés en date du 31 décembre 2015, avant le transfert à Leclerc de 248 détenues de la prison Tanguay. Il s'agit d'une comparaison des coûts de deux prisons provinciales pour hommes (à l'époque) de la région de Montréal. La prison Leclerc héberge des hommes et des femmes depuis février dernier. Les coûts de l'établissement depuis qu'il est devenu mixte n'ont pas été précisés, mais la seule autre prison hébergeant des détenus des deux sexes, celle de Québec, signale des coûts par détenu de 213 $ par jour -- nettement moins que les 299 $ par jour à Leclerc. Le Devoir, A3

* **Le délateur Stéphane Gagné débouté**
Le délateur Stéphane Gagné aurait échoué dans sa tentative de convaincre les commissaires aux libérations conditionnelles de lui permettre d'effectuer ses premières sorties du pénitencier avec escorte policière, a appris La Presse de diverses sources. La Commission des libérations conditionnelles n'a toutefois pas voulu confirmer l'information puisqu'il aurait fallu que les commissaires rendent leur décision séance tenante lundi pour qu'elle devienne publique. Gagné, alias Godasse, est détenu depuis près de 20 ans. Il a été condamné à la prison à vie en 1998 pour le meurtre de la gardienne de prison Diane Lavigne, commis un an plus tôt, à la demande de l'ancien chef guerrier des Hells Angels Maurice Boucher. Gagné a témoigné dans le procès pour les meurtres des gardiens de prison intenté contre Boucher à la fin des années 90 et au début des années 2000 et a contribué à faire condamner l'ancien chef des Hells Angels. La Presse, 12

City keeps 'door open for other' KP plans
A group of five prominent Kingston citizens on Tuesday disclosed their vision for the mothballed Kingston Penitentiary property and Portsmouth Olympic Harbour site. But their vision may not jibe with a consultant's report, which is currently being prepared for the city. In a telephone interview on Wednesday, Kingston Mayor Bryan Paterson said there will be time over the next few months to discuss various proposals once the consultant releases its recommendations. "We're looking forward to, some time early in the new year, a concept that will come to city council for approval, and once that concept has been approved, certainly we look forward to interested parties coming forward with proposals that would align with that final vision," Paterson said. The citizens group consists of George Hood, a former viceprincipal at Queen's University; George Jackson, a Kingston business consultant; lawyer and former Olympic sailor John Curtis; former Kingston mayor Harvey Rosen; and Dr. Michael de la Roche. They also have dozens of local citizens working behind the scenes on what they call the Hatter's Bay project. (...) "I'm certainly pleased to see there's interest in developing Kingston Penitentiary," Paterson said. The mayor also said the city doesn't own the property but is appreciative with the partnership it has developed with Canada Lands, the Crown corporation in charge of disposing of the property, and Correctional Service Canada. Kingston Whig-Standard, A1/Front

* **Moms Make Noise**
Supporters of an inmate who took his own life while at the Ottawa-Carleton Detention Centre held a vigil outside the jail Wednesday evening to send a message: that mentally ill inmates should be in treatment centres, not prisons. Justin St. Amour, who had been diagnosed with schizophrenia, hanged himself in

his segregation cell at OCDC on Nov. 30. He died eight days later at The Ottawa Hospital, one day after he was removed from life support. His death came just months after another man, Yousef Mohammed Hussein, hanged himself while on suicide watch at OCDC. "We shouldn't be warehousing our mentally ill sons and daughter and brothers and sisters, they should be in treatment centres, in healthcare facilities," said Irene Mathias of Mothers Offering Mutual Support (MOMS), a group that advocates for the humane treatment of prisoners. Members gathered outside OCDC Wednesday to share experiences, observe a minute of silence for St. Amour and lay flowers near the gate. Farhat Rehman, a member of MOMS, was there on behalf of her son, who had been jailed at OCDC and is currently serving time at a federal prison. Ottawa Sun, A5 (Ottawa Citizen)

* **Première peine spécifique aux Autochtones à Québec**
Pratique courante dans le Nord, c'est la première fois, dans le district judiciaire de Québec, qu'un avocat demande la confection d'un rapport présentenciel spécifique aux Autochtones, une disposition législative disponible depuis l'arrêt Gladue, rendu par la Cour suprême du Canada en 1999. Sans réduire la peine imposée à une jeune Autochtone de Colombie-Britannique, le plus haut tribunal du pays avait alors tranché qu'il fallait changer d'approche pour déterminer les peines afin de contrer la surincarcération des membres des Premières Nations. Le Code criminel a été modifié afin d'obliger les juges à travers le pays à ordonner la confection de ce type de rapport spécifique aux Autochtones. La Presse (2016-12-14)

* **Advocate encouraged but challenges remain in mental health system**
Roughly half of young people in New Brunswick with mental health disorders have to wait more than 30 days to get help, and the rate of hospitalization for troubled youngsters is significantly higher than the national rate, a new report shows. But Norm Bossé, the province's Child and Youth Advocate, says in his latest state of the child report he is encouraged by the new focus the provincial government and communities are placing on identifying and helping troubled young people. "There are so many ways in which New Brunswickers are developing innovative programs and interventions to support children and youth with mental health needs that it is, in fact, possible to be optimistic about the future," the advocate states in his report. The issue of mental health in children has been a concern in New Brunswick since the case of Ashley Smith and her tragic death in prison highlighted shortcomings in the mental health system in the province and across Canada. Smith, a native of Moncton, died by self-inflicted strangulation in 2007 in an Ontario women's prison while under suicide watch. She was 19. Smith's short, troubled life and sad death have become a lightning rod for improved mental health treatment for children and youth. Daily Gleaner, B1 (Telegraph-Journal, Times & Transcript)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

* **Alberta and Saskatchewan lead country in drinking and driving**
A new report from Statistics Canada breaks down drunk driving numbers from across the country, and Alberta does not fare well. Overall, drunk driving numbers are down in Canada. Last year there were 72,039 incidents, an average of 201 per 100,000 people. But Alberta had 314 incidents per 100,000, and in Saskatchewan, it's even higher. (…) "This province and city are going through some very difficult times," said Chief Roger Chaffin, Calgary Police Service. "It's not surprising at all to see alcohol really fueling people out in the community right now, people medicating through alcohol not a surprise, I think impaired driving is still something the city is very alive to." (…) The RCMP is teaming up with **Public Safety Canada** to run a pilot project to test new roadside drug testing devices, but police say that is putting the cart before the horse. "How is it going to be operationalized, and that's one of the aspects is that there isn't any particular per se limits set yet, there aren't any devices yet we can use to help identify when impairment occurs," said Chaffin. "I think as we are racing along to this, chances are legalization is going to occur before we've even begun to answer those questions." CTV News (2016-12-14)

* **'Not surprising' province has highest impaired rate in country, MADD says**
Saskatchewan is 30 years behind the rest of Canada when it comes to rates of impaired driving. Figures released by Statistics Canada Wednesday show that Saskatchewan had the highest provincial rate of police-reported impaired driving in 2015, with 575 incidents per 100,000 of population. Rates include drug

and alcohol impairment. Among the more startling figures is that Saskatchewan's 2015 impaired driving rate is almost exactly what the national average was in 1986, when comparable statistics were first made available. Thirty years ago the national average was 577 per 100,000, but Saskatchewan's rate today is just two lower at 575. The province's rate has decreased by 37 per cent since 1986, but the national drop has been 65 per cent - to 201 per 100,000 - over the same period. Saskatchewan's rate is almost double that of Alberta, which had a rate of 314 per 100,000 last year and ranks second among all provinces. The lowest-rated province, Ontario, had just 111 incidents per 100,000. StarPhoenix, A1 (Leader-Post)

* **Impaired Driving by the Numbers**
1986: The year comparable impaired driving data was first gathered. The national rate of impaired driving then was 577 incidents per 100,000, which mirrors Saskatchewan's rate in 2016. 72,039: The total number of police-reported impaired driving incidents nationwide in 2015, which is a rate of 201 incidents per 100,000 of population. 122: Countrywide incidents of impaired driving causing death in 2015. There were 596 cases of impaired driving causing bodily harm. Leader-Post, A5

* **Edmonton amongst worst Canadian cities for impaired driving**
Edmonton ranked in Canada's 10 worst cities for impaired driving as reported by police in 2015, according to a Statistics Canada report. Police filed 226 reports of impaired driving per 100,000 Edmontonians last year. In a city of nearly 900,000 people, that number translates to about 2,000 reports overall-or roughly five every day. That rate made Edmonton the seventh-worst city for impaired driving in Canada. Edmonton's rate is nearly four times higher than in Kingston, Ont., the city with the lowest rate of impaired driving. CBC News (2016-12-14)

* **Victoria has fourth highest rate of impaired-driving incidents in Canada**
Victoria had the fourth highest rate of impaired-driving incidents in Canada, according to a Statistics Canada report released Wednesday. The report also found that while drunk driving is steadily declining, drug-impaired driving, which is harder to detect, is on the rise. Victoria had 271 impaired driving incidents per 100,000 population in 2015, which was behind Kelowna and Regina with 323 and 311 impaired incidents, respectively. St. John's, N.L., had 411 impaired-driving incidents, the highest rate in the country. Times Colonist, A6

* **Impaired driving rate among lowest**
The London area had one of the lowest rates of impaired driving of major centres in Canada last year, new figures show. But as the federal government moves toward legalizing recreational marijuana use, police warn they could see increases in drug-impaired driving charges. Only four other census metropolitan areas in Canada had a lower rate of alcohol-impaired driving than the London area in 2015, Statistics Canada reports. With a total of 444 cases of impaired driving in 2015, the London area's rate of impaired driving per 100,000 people was 87 cases. London Free Press, A2

* **Cape Breton police order 250 naloxone kits amid fentanyl crisis**
The Cape Breton Regional Police Service recently ordered 250 naloxone kits - one for each of its officers and jailers - as one measure to protect its workers from exposure to fentanyl. Naloxone can temporarily reverse the effects of an overdose from opioid drugs, including fentanyl, which has been responsible for hundreds of deaths across Canada. While the Cape Breton Regional Municipality has not yet seen a major influx of fentanyl, police are sure it's on its way. 1 confirmed fentanyl overdose in CBRM "There's probably been some form of it come back from out west. We have a large population of people that travel out west for work and come back. So we do think that there has been some here," said Staff Sgt. Paul Muise, one of two senior officers taking the lead on fentanyl for the police service. Muise said he's been told there has already been one confirmed overdose death in the area as a result of fentanyl. Safety for first responders When it comes to fentanyl, the safety of first responders such as police and EHS is a major concern given that as little as two milligrams of the drug can kill a person, said Muise. CBC News

*** Safe injection bill 'welcome news' for Hamilton**
In the face of a deadly opioid crisis, the federal government is hoping to speed up the process for cities like Hamilton to open safe injection sites. It was just last week that public health was given the green light by city councillors to launch its study into the feasibility of bringing safe injection sites to town. At last Friday's general issues committee meeting, associate medical officer of health Dr. Jessica Hopkins estimated it would be early 2018 before the "onerous and time-consuming" application could be completed. But the federal government has announced a bill that would trim the to-do list for communities looking to apply for an injection site, simplifying the required criteria from 26 items to five. It's a "timely" move - and "welcome news" for Hamilton, Hopkins says. Opioid overdoses are up across the country, with an increasing number of deaths being attributed to fentanyl, a potent painkiller 100 times stronger than morphine. Of the province's staggering 685 opioid-related deaths last year, 162 of them were specifically linked to fentanyl. In Hamilton alone, there were 19 fentanyl deaths last year (up from 10 in 2014). And just this week, the presence of carfentanil - a drug 100 times more potent than fentanyl - has been confirmed in four provinces including Ontario. Hamilton Spectator

*** Inside Quebec's far right: At the crossroads with Soldiers of Odin**
In the early evening darkness, four figures huddled in the parking lot of a Quebec City arena, all wearing black sweatshirts emblazoned with a drawing of Odin, the Norse god of war. One was a professional hunter, another a wood-factory worker. They stomped their boots in the cold, shared a cigarette or two, then set off to patrol the historic streets of the city, armed only with a flashlight and the belief they were protecting Quebecers from a vague but dangerous threat. (…) In Canada, the Soldiers of Odin met with criticism as they established themselves across the country. Its patrols in Edmonton, for instance, were described as "troubling" by the National Council of Canadian Muslims. A city councillor in Hamilton accused them of spreading hate speech. (…)And it has teamed up on a number of occasions with Atalante Québec, an openly neo-fascist organization that speaks of protecting the "neo-French." The two groups joined forces for a food drive last month and jointly patrolled the Laval University campus after a spate of sexual assaults there in October. CBC News (2016-12-14)

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** PM meets indigenous leaders a year after Truth and Reconciliation report release**
Prime Minister Justin Trudeau is scheduled to sit down with indigenous leaders today, the one-year anniversary of the Truth and Reconciliation Commission's final report. The commission, led by Murray Sinclair, Manitoba's first indigenous judge, issued 94 sweeping recommendations after six years spent examining the legacy of Canada's residential school system. (...) Trudeau says progress is underway on 36 of the 45 calls to action in the report that are under federal jurisdiction. Hearings are expected to begin next spring in the inquiry into missing and murdered aboriginal women and girls — one of the recommendations enacted by the Liberal government. Canadian Press (570 News)

*** Kamloops woman teaches modelling to help keep Indigenous women safe**
Kim Coltman is teaching Indigenous women how to walk tall in the hope it will protect them. When Tanya Pellett walks down the street, she makes sure to walk tall and make eye contact with the people she passes. But theTk'emlups te Secwepemc band member didn't always do that. "I would always look down," she said. "I felt like I was always vunerable." Pellett made the change after taking a training course offered by Fashion Speaks International. The Kamloops-based agency was founded by Kim Coltman. She's hoping to use fashion to help raise awareness about the issue of murdered and missing Indigenous women. Coltman is teaching women, especially Indigenous women, how changing the way you walk can change the way people perceive you. CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Police will need more resources for legal pot
Saskatoon police Chief Clive Weighill says he expects marijuana legalization will require more resources from the police force. The work will include training and enforcing new regulations, and he also expects the black market will maintain some of its hold over the industry, he said. "Through what we learned from Colorado and Washington, the people who are moving marijuana illegally have undercut the selling price at the dispensary and are still doing quite a bit of business." Recommendations from the federal task force suggest recreational marijuana sales should be conducted through a mail-order system or from designated stores, with the added suggestion that higher-potency marijuana should be taxed at a higher rate than weaker strains. Police are not the only ones who will require more resources after legalization, Mayor Charlie Clark said, noting city hall will likely require additional funds, especially if new technology is needed to determine if someone is driving under the influence. Clark said the federal government should consider helping with some of the new costs. Leader-Post, A3 (StarPhoenix)

Top pot dispensaries plan to expand before legalization
The entrepreneurs behind Canada's two biggest chains of illegal marijuana dispensaries say they will continue to expand the number of their storefronts aggressively across the country while the federal and provincial governments take the next two years to fine-tune new laws to legalize the substance. A day after an independent panel provided Ottawa with a road map for ending the prohibition on recreational marijuana that could include dispensaries, MP Bill Blair, the government's point person on the issue, warned that, in the meantime, anyone selling marijuana outside the federal mail-order system is breaking the law and police could raid their stores. But those behind two Vancouver-based chains say the new report indicates they will have two years of challenging the existing cannabis laws - and police departments' appetite for enforcing them - during which they plan to open more than 100 new stores across Canada. They say they are willing to comply with future regulations and hope to join the regulated sector once the federal laws change, but Mr. Blair said it is too early to say whether the new legal system will allow dispensaries to participate. Globe and Mail, A6

Top doctor says province may set age to buy marijuana at 21
New Brunswick's top doctor says the province may set a minimum age of 21 to buy marijuana. Jennifer Russell, New Brunswick's acting chief medical officer of health, says an internal working group, set up by government in the wake of Ottawa's move toward legalization, has landed on that age as a balance between access and impacts on health. Meanwhile, a new report ordered by Ottawa on legalizing and regulating pot has recommended that federal government set a minimum age of 18, and then leave it to the provinces to set a higher minimum age if they want to. "Our discussions have revolved around the age of 21," Russell said in an interview with the Telegraph-Journal. "Some of the things that we have discussed would be balancing the risk to people's health with the practical aspects of implementation and the black market issue. "Some of the evidence suggests that we wait until 25, so we have to compromise somewhere." Russell said that a final decision on setting the legal age at 21 has not been made and is still subject to internal debate within government. Telegraph-Journal, A3 (Times & Transcript, Daily Gleaner)

N.S. among top supporters of marijuana legalization
Nova Scotia has the highest support for the legalization of marijuana in the Atlantic Provinces, a new public opinion poll says. The Corporate Research Associates survey of 1,502 Atlantic Canadians showed the vast majority, 82 per cent, support the legalization of marijuana for medical purposes - compared with 84 per cent one year ago - while 53 per cent support legalizing it for personal use, compared to 49 per cent in 2015. Conversely, 41 per cent of Atlantic Canadians oppose recreational marijuana legalization while only 13 per cent oppose it for medical purposes. In Nova Scotia, however, 86 per cent support legalization for medical purposes while 57 per cent support legalization for personal use. P.E.I. has the lowest support for recreational legalization, at 46 per cent. The survey also also notes that support for legalization of marijuana for personal use is stronger among younger residents, with 70 per cent of 18-34 years old expressing support. Chronicle-Herald, A5

*** Victoria's pot rules backed in task force report**
For Victoria mayor Lisa Helps, this week's federal task force recommendations on marijuana sales look a lot like the regulations her own city council approved in September. Age restrictions, a ban on advertising

and buffer zones to keep shops far from schools and parks are among the measures urged by the panel appointed to advise Justin Trudeau's Liberal government on legalizing pot. "We're not way out there in terms of our approach. That's a good thing," Helps told On the Island host Gregor Craigie. Even with this first step towards a national framework for legalized marijuana, Helps said Victoria remains on its own in enforcing regulations. "Until legislation passes there's still a vacuum," she said. "We couldn't wait for something to be done, in terms of the proliferation of these cannabis dispensaries." For existing marijuana storefronts in Victoria, the city now requires a lengthy rezoning process that costs $7,500 and could take seven or eight months. If successful, the business is then allowed to purchase a $5,000 business license. "We've put a regulatory regime in place. That will stay in place until we get further direction from the federal government and the province," Helps said. "That couldn't come soon enough." While the task force urged distribution of legal pot through stand-alone dispensaries or by mail-order, Helps said she thought it would recommend the sale of cannabis through pharmacies. CBC News (2016-12-14)

Marijuana : où et à quel âge pourra-t-on s'en procurer?
Au lendemain de la présentation du rapport du Groupe fédéral de travail sur la légalisation et la réglementation du cannabis, il est toujours impossible de savoir avec exactitude à quel endroit et à quel âge il sera possible de se procurer de la marijuana. Les opinions des spécialistes et des intervenants concernés divergent quand il est temps d'aborder ces deux questions cruciales. Le gouvernement provincial a indiqué mercredi que la légalisation est une initiative fédérale, tout en soulignant que les répercussions sont importantes pour les gouvernements provinciaux. «Le gouvernement du Nouveau-Brunswick accueille favorablement le rapport rendu public mardi par le Groupe de travail sur la légalisation et la réglementation du cannabis. Il s'agit d'une étape importante pour définir l'orientation que prendra le gouvernement fédéral dans le dossier de la légalisation», a indiqué à l'Acadie Nouvelle Cathy Rogers, la ministre des Finances. «Nous attendons avec intérêt la réponse du gouvernement fédéral à ce rapport, car il aidera le Nouveau-Brunswick ainsi que les autres provinces et territoires à prendre les dispositions nécessaires en vue de la légalisation de la marijuana», de poursuivre la ministre. L'Association des pharmaciens du Nouveau-Brunswick demeure pour sa part sur sa position. Selon elle, quelle que soit la classification gouvernementale de la marijuana lorsqu'elle est utilisée de façon thérapeutique, elle peut avoir un impact sur les fonctions physiologiques du patient et sur les effets d'autres médicaments. L'Acadie Nouvelle, 3

Canadian parents prepare for realities of legalized marijuana
B.C. mom Scarlett Ballantyne wonders if Ottawa's plans to legalize marijuana will make her 14- and 16-year-old daughters more inclined to try it. But she's not waiting to find out. Ballantyne says her family has been discussing the dangers of drug use since the girls were 13 - a pre-emptive strike as pot shops and marijuana headlines have been popping up everywhere they turn. She's proud to say they are athletic, self-confident kids, but she also gets the impression that their generation sees marijuana as "not that big of a deal." Telegraph-Journal, C1

Councillors weigh in on marijuana in Saskatoon
Before the civic election, The Star-Phoenix asked councillors their opinions on how Saskatoon should prepare for marijuana legalization. These are their responses... StarPhoenix, A3

Entre deux joints
Un article d'opinion note, « Justin Trudeau avait promis de légaliser la marijuana récréative au Canada : les recommandations du groupe de travail présidé par l'ancienne ministre libérale Anne McLellan lui donnent maintenant les balises pour aller de l'avant. Et c'est là que ça va se compliquer. La consommation de marijuana fait pratiquement partie des moeurs au Canada. Or son commerce profite exclusivement au crime organisé qui n'a rien à faire de l'impact social et sanitaire de cette drogue « douce » qui ne l'est plus vraiment puisque la concentration de sa principale composante psychotrope, le THC (tétrahydrocannabinol), a augmenté de 300 à 400 pour cent depuis les années 70. Bizarrement, le rapport du groupe de travail ne se prononce pas sur la teneur en THC, pas plus que sur l'impact de cette drogue sur la maturation cérébrale des adolescents. » La Tribune, 10

* **Free-market buzzkill**

An opinion piece states, "What were they smoking? Actually, the report of the federal government's task force on how to legalize and regulate marijuana isn't all that bad, as these things go. I just couldn't resist that line. One part of the report that seemed remarkably clear-headed was its recounting that: "The vast majority of respondents to the (task force's) online consultation expressed a preference for a competitive private-sector production model, noting that this would allow for a greater variety and diversity of products with fair pricing." National Post, FP9

* **Liberals must get it right on pot**

An editorial states, "Prime Minister Justin Trudeau campaigned to legalize pot in the 2015 election campaign. This federal task force report on the subject released this week offered no quick fix to the complex issues surrounding legalization, and the sensible recommendation that the Liberals proceed slowly. The 106-page report made more than 80 recommendations - including restricting pot sales to those 18 and older, banning sales near schools, banning pot advertising and branding (similar to tobacco products) and a new, proposed Cannabis Control Act to police illegal production and trafficking. Marijuana consumption is an estimated $7 billion-a-year underground business in Canada, and that market could grow to $10 billion to $20 billion with legalization. Legalization is also broadly supported by the Canadian public. Meanwhile, the case for criminalization is increasingly difficult to support. Canada needs to reconcile the agreements it made via international treaties to criminalize and prosecute drug possession and production with legalization in this country. But our decades old "war on drugs" has failed miserably to deter drug use or abuse." Edmonton Sun, A16 (Winnipeg Sun, Toronto Sun, Calgary Sun, Ottawa Sun)

Pot report on the hazy side

An opinion piece states, "The federal government has just released the report of its special advisory task force on marijuana legalization. While the report lays out broad strokes, key decisions remain on retail distribution, legal age limit, and taxation that Ottawa and the provinces should agree on soon. The report recommends that provinces be given the jurisdiction to determine the precise mechanism of retail distribution. However, the report has also recommended against allowing the sale of marijuana in stores that also offer liquor and/or cigarettes. This is consistent with my own study that was released by the C.D. Howe Institute, in which I recommended retail sales through stand-alone stores as opposed to government-owned retail outlets, as is the case in Ontario. Ontario Premier Kathleen Wynne has supported the idea of the provincially owned LCBO distributing marijuana. The idea has also received considerable support from the trade unions representing LCBO employees. A supporting argument is that selling marijuana through LCBO outlets reduces the possibility of underage consumption. In this respect, the task force has certainly made a sound economic and health policy recommendation... However, the task force's proposed legal age limit of 18 raises some valid concerns. The task force has acknowledged that a higher age limit of 19 is possible if a province wishes to harmonize marijuana regulation with corresponding alcohol minimum ages. On the other hand, the federal government should consider an even higher national legal consumption age for marijuana, possibly at 21 years of age." National Post, FP9

* **Happy daze?**

Re Ottawa Plans To Open Up Legal Market For Cannabis By Early 2019 (Dec. 14)

A letter to the editor states, "The personal use limits proposed by the marijuana task force make sense - 19 or older to buy it, can't carry more than 30 grams, can't grow more than four plants at home. The task force seems to have walked a line between trying to discourage a market for organized crime and throwing the door wide open. The issue now will be how to discourage the 18- to 25-year-olds from heavy use, since those young brains of theirs are still developing. The forbidden is always more attractive." Globe and Mail, A12

* **Big Changes**

A letter to the editor states, "As Canada is about to join Uruguay as one of two countries to legalize marijuana, we are in for major changes in our culture, plus added pressure on our ailing health care. It is most disturbing that the Trudeau Liberals are rushing ahead with legalization before a simple roadside test is available to test for driver pot-smoking impairment. The government is ignoring the Canadian Medical Association's recommendation to raise the age for purchase to at least 21. Police better get

ready for the entry of organized crime groups, which will surely take advantage of black market pot sales." Ottawa Sun, A20

Huit boutiques de pot ouvrent aujourd'hui à Montréal
Les proprios de huit boutiques illégales de marijuana qui ouvrent leurs portes aujourd'hui se croisent les doigts pour que la police de Montréal n'intervienne pas. «Nous ne savons pas ce qui va arriver, a avoué hier Jodie Emery, copropriétaire de la marque Cannabis Culture, dont des franchises s'installent dans la métropole. On espère que la population va nous soutenir et que nous pourrons servir de modèle pour démontrer de quoi la légalisation devrait avoir l'air à Montréal et au Québec.» L'activiste de longue date croit que les autorités policières peuvent choisir d'intervenir ou non. Dès 10h ce matin, huit boutiques vendront de la marijuana récréative aux adultes de 19 ans et plus, même si employés et clients risquent d'être arrêtés. Dans les prochaines semaines, ce nombre grimpera à 10 commerces, a confirmé Mme Emery. Pour l'instant, Cannabis Culture s'installe dans les secteurs d'Hochelaga, de Ville-Marie, du Plateau- Mont-Royal, de Rosemont, de Villeray et de Côte-des-Neiges-Notre-Dame-de-Grâce. Le Journal de Montréal, 7; Canadian Press (Chronicle-Herald) (2016-12-14)

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Privacy watchdog investigating Liberals' survey**
The federal privacy commissioner is investigating the Liberals' new online survey about Canadians' feelings toward electoral reform. Privacy commissioner Daniel Therrien's office said it is looking into the government's mydemocracy.ca site, which asks for highly personal information such as household income, education and employment status, and for postal codes. The survey lists the information as "optional," but it's actually required if respondents want their views meaningfully counted in a final report for Democratic Institutions Minister Maryam Monsef. A spokesperson for Therrien's office said it has already recommended improvements to the government to "better protect" respondents' privacy. But because the commissioner received a formal complaint about the website, Therrien will open an investigation. "Our goal is to have these issues resolved as quickly as possible," wrote spokesperson Valerie Lawton in an email to the Star. Toronto Star, A6

*** Public servants urged to donate**
Ottawa community groups are urging federal public servants to donate to a massive United Way workplace campaign that's "at risk" of falling short of its $19-million fundraising goal - something the groups say could have a "devastating impact on our city's most vulnerable people." The plea is contained in an open letter to public servants co-authored by Susan Ingram of Big Brothers Big Sisters of Ottawa and Kathryn Hill of Family Services Ottawa. The letter was penned on behalf of the 25 agencies supported by the United Way charity organization that distributes the proceeds of the annual campaign. The current total of donations sits at $14.6 million, Ingram told the Sun. The deadline for donating is March 31, 2017. "We are able to provide vital programs and services because of your generous donations to United Way Ottawa through your annual workplace campaign," the letter reads. "This year, our ability to support those who need it most is at risk." Marie Lemay, a campaign co-chair AD{NS50921906} and deputy minister of Public Services and Procurement Canada, confirmed the campaign will fall short of its goal but said "below target is still a big amount of money." "It's still a very positive contribution that federal public servants are making to the community." Ottawa Sun, A16

*** Fiasco du système de paye: encore 10 000 fonctionnaires fédéraux touchés**
«Nous progressons lentement en raison de la complexité de ces cas, a admis la sous-ministre du ministère des Services publics et de l'Approvisionnement, Marie Lemay, mercredi. Mais nous nous approchons d'un objectif important, a-t-elle ajouté au sujet du seuil des 10 000 cas encore non résolus. Ottawa avait promis de régler les ratés de son système de paye Phénix avant le 1er novembre. Depuis cet échec, le ministère n'ose plus s'enfermer dans un nouvel échéancier. Mme Lemay a concédé que «l'année qui se termine a été très éprouvante» pour bon nombre de fonctionnaires qui n'ont pas reçu leur dû. «En particulier avec la période des Fêtes qui approche, votre patience et votre tolérance sont extrêmement appréciées», a-t-elle dit, s'adressant aux employés du gouvernement federal. Agence QMI

*** Phoenix system will not cause tax problems: LeMay**
The federal government is assuring public servants they won't have tax trouble because of the Phoenix pay system, despite thousands of over-payments and other delays. Deputy Minister Marie LeMay gave another update Wednesday on the troubled pay system, reporting that there are still 10,000 cases in the backlog the government first identified in July. Another 200,000-230,000 cases are outside of the government's standards for processing but have come in since July. LeMay said the government was addressing the problem and was seeing steady and continued improvement. "Our processing capacity will further increase once we have cleared the backlog," she said. She said she was confident that over-payments would not show up on T4 tax statements. Metro News

OTHER / AUTRE

La preuve contre les deux Québécoises emprisonnées en Australie devrait être révélée
Mélina Roberge et Isabelle Lagacé, originaires de Granby et Longueuil, ont été arrêtées le 28 août dans le port de Sydney en compagnie d'André Jorge Tamine, avec 95 kg de cocaïne dans leurs valises. Les deux Québécoises emprisonnées en Australie, Mélina Roberge et Isabelle Lagacé, devraient prendre connaissance des éléments de preuve amassés contre elle, lors de leur retour en cour, jeudi soir, à Sydney. Mélina Roberge, 23 ans de Granby, et Isabelle Lagacé, 28 ans de Longueuil, doivent subir leur enquête préliminaire à 17h30, jeudi, heure du Québec. À l'heure locale de Sydney, en Australie, l'audience se tiendra à 9h30, le 16 décembre. Il est prévu que la Couronne y dévoile sa preuve. Le juge de la cour criminelle locale de Sydney devra alors conclure si les éléments sont suffisants pour justifier la tenue d'un procès. (...) Les deux Québécoises, ainsi que leur complice André Tamine, âgé de 64 ans, ont été arrêtés au port de Sydney, en Australie, le 28 août dernier. Petite-Nation

*** Battle for Mosul will shape Canada's ground commitment in Iraq**
Anti-ISIS coalition members meet in London to review progress and chart future course. Canada will continue to have a military mission in Iraq through 2017, but the size and scope of it have yet to be determined, the country's defence minister said in advance of an international meeting with allies battling ISIS. Defence planners have been spinning various scenarios for months, but the Liberal government committed — when it overhauled the mission against ISIS last February — to reviewing the deployment of special forces, helicopters, surveillance planes, an air-to-air refueling jet and a military field hospital. The assessment is due by March of next year, but the last budget numbers put before Parliament have set aside only $41 million for the operation, less than one-third of what's being spent in the current budget year. CBC News

INTERNATIONAL

Medical convoy trying to leave Aleppo comes under fire
An attempt to evacuate people in need of medical attention from rebel-held eastern Aleppo stalled on Thursday when fighters loyal to the Syrian government fired on the convoy, wounding three, the head of the ambulance service said. The vehicles had intended to leave under a deal to evacuate people from rebel areas following rapid advances in Aleppo by government forces. The evacuation of the last rebel enclave would end years of fighting for the city and mark a major victory for Syrian President Bashar al-Assad. "The convoy was shot at by regime forces and we have three injured, one of them from civil defense ... They were brought back to besieged areas," ambulance service Ahmed Sweid told the pro-opposition Orient TV. A Reuters witness in nearby government-held territory heard a burst of gunfire that lasted several minutes. An official with an Aleppo rebel group said the medical convoy had stopped before clearing the besieged eastern part of the city. A Syrian official source told Reuters earlier on Thursday that efforts to organize the departure of fighters from east Aleppo had begun and the International Committee of the Red Cross said it had been asked to assist with the evacuation. Globe and Mail; * Acadie Nouvelle

J'Accuse

Aleppo has fallen. The last and sturdiest bastion of the Syrian uprising is gone. The Battle of Aleppo is over, the revolution is finished, and the Syrian mass murderer Bashar al-Assad has won. Russia has won. Iran has won. Hezbollah has won. The United States has lost. The United Nations has lost, and the bloody war in Syria, already having taken nearly half a million lives, goes on. Aleppo mattered, it should go without saying, but it's worthwhile enumerating what did not matter. You can start with Aleppo's 31,000 dead and proceed from there through each and every statutory war crime codified by the International Criminal Court. (...) And now Aleppo is undergoing what UN humanitarian spokesman Jens Laerke calls "a complete meltdown of humanity." The still-living lie with dead in the rubble of bombed out buildings. You can hear them screaming. Regime militias are carrying out mass executions of civilians. In one case, 11 women and 13 children were shot "on the spot." Women are committing suicide rather than face the prospect of rape and murder. A planned evacuation of perhaps 100,000 civilians and rebel fighters from East Aleppo was heralded as a breakthrough on Tuesday, following the abject surrender by all of Aleppo's remaining rebels - hardline Islamists and democratic patriots alike. Postmedia Network (National Post, A1, Montreal Gazette, Vancouver Sun, Windsor Star, Leader-Post, Star Phoenix, Ottawa Citizen, London Free Press, Edmonton Journal, Calgary Herald)

*** Evacuation of eastern Aleppo underway, aid workers say: Buses move into rebel-held territory after earlier coming under fire**

Efforts to evacuate people from the rebel-held eastern areas of Aleppo are underway, according to aid workers, after a convoy came under fire earlier Thursday. The International Committee of the Red Cross said in a Tweet shortly after noon local time that the operation to evacuate around 200 wounded people from rebel-held areas, part of a wider ceasefire deal, was under way. The Britain-based Syrian Observatory for Human Rights monitoring group said ambulances and municipal buses had crossed from government territory. Those same buses were seen on webcams, set up by the Russian military, as they rolled through the besieged city. Evacuation efforts stalled earlier in the day when pro-Syrian forces opened fire on a convoy as it prepared to leave eastern Aleppo. Three people were wounded according to the head of the ambulance service in the district. "The convoy was shot at by regime forces and we have three injured, one of them from civil defence ... They were brought back to besieged areas," Ahmed Sweid told the pro-opposition Orient TV. (...) The rebels have held to the eastern part of the city for four years but their enclave rapidly evaporated in the past days in the face of a fierce Syrian government onslaught. CBC News

*** Un djihadiste reconnaît son implication dans l'attaque du Thalys**

Près de 18 mois après l'attentat raté contre un Thalys, en août 2015, le tireur présumé Ayoub El Khazzani a reconnu pour la première fois son implication dans l'attaque djihadiste, tout en réfutant avoir voulu commettre un «massacre de masse». Entendu pendant plus de cinq heures devant un juge d'instruction antiterroriste, ce Marocain de 27 ans est revenu sur son parcours jusqu'à cette journée du 21 août 2015 lorsque muni d'une kalachnikov et de neuf chargeurs pleins, il a ouvert le feu dans un Thalys Amsterdam-Paris, peu après son entrée en France, dans le Pas-de-Calais. Il avait grièvement blessé un passager avant l'intervention de plusieurs voyageurs qui l'avaient maîtrisé, mettant ainsi en échec un potentiel carnage, sept mois après les attentats de janvier à l'Hyper cacher, Montrouge et *Charlie Hebdo* et trois mois avant ceux de Paris, le 13 novembre. «Maintenant il assume, il prend ses responsabilités. Il explique que c'est en tant que djihadiste qu'il est monté dans ce Thalys (...) mais ce qu'il comptait faire savoir, c'est qu'il n'était pas là pour faire un massacre de masse et tuer n'importe qui (...) Pas du tout», a déclaré à la presse son avocate Sarah Mauger-Poliak à l'issue de l'audition. Agence France-Presse (La Presse) (2016-12-14)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
December 22, 2016 / le 22 décembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

*** Ottawa veut une révision en profondeur du financement des services policiers pour les Premières Nations**

Le gouvernement fédéral promet de revoir la façon dont il finance les services de police dans les communautés autochtones. **Le ministre de la Sécurité publique, Ralph Goodale**, dit que le Programme des services de police des Premières Nations est dépassé et aurait besoin d'être réformé. ***« Il est en place depuis le début des années 1990. Ça va prendre plus de fonds, mais également une restructuration »*** - **Ralph Goodale, ministre de la Sécurité publique du Canada.** Les commentaires du **ministre** ont été faits en réaction à un rapport interne de **Sécurité publique Canada** qui explique en détail les problèmes persistants du programme qui finance les services de police dans plus de 450 communautés inuites et des Premières Nations au Canada. Le statu quo n'est plus une option viable, conclut en substance le rapport qui a été publié le mois dernier. Radio-Canada

Trudeau hopes to rein in spy agencies

Justin Trudeau says his government will ensure security and spy agencies follow the "letter and spirit" of the law, amid mounting concerns they have trampled the privacy of journalists and other Canadians. In a roundtable interview this week with The Canadian Press, the prime minister stressed that national security agencies must protect Canadians but also safeguard the laws and values the public cherishes. Trudeau's words come as the Liberal government wraps up a national consultation on federal security policy and they follow two recent episodes that heightened public concern about unwarranted surveillance. It emerged last month that the Montreal and Quebec provincial police forces had been tracking the communications of several journalists. Only days later, a Federal Court judge found the Canadian Security Intelligence Service had broken the law by keeping and analyzing information about the communications of innocent people - potentially revealing data that was collected during investigations into actual suspects. (…) **Public Safety Minister Ralph Goodale** told MPs at a House of Commons committee this month he was keeping an open mind as to whether CSIS should be allowed to retain and use the incidentally gathered data trails - such as phone numbers and email addresses. Canadian Press (Ottawa Sun, A9, Red Deer Advocate, Montreal Gazette, Ottawa Citizen, Vancouver Sun, Edmonton Journal, Calgary Herald, Times Colonist, London Free Press, Star Phoenix)

Change will require 'diplomatic skills'

Their position on marijuana is hardly the only difference between Canada's prime minister and the president-elect of the United States. But when Justin Trudeau's government introduces legislation to legalize cannabis this spring, it could spark problems between Canada and the U.S., particularly since Donald Trump has indicated he will keep pot illegal at the federal level. Here's a look at what could change in Canada-U.S. relations once Canadians start lighting up legally. Border control Len Saunders, an immigration lawyer in Blaine, Wash., predicts a boom in his business after Canada legalizes marijuana - though it's one he has a hard time feeling happy about. Saunders represents Canadians who have been banned from entering the U.S. after admitting they have smoked marijuana in the past. Every year, he files as many as 30 costly waivers for people who've made this admission and hope to regain access. (…) Earlier this year, **Public Safety Minister Ralph Goodale** said Canadians banned from entering the U.S. because they've admitted to using pot was a ***"ludicrous situation"*** that needed to be addressed. **Scott Bardsley, a spokesman for the minister**, said **Goodale** will continue to discuss with American officials the need for Canadians to be treated appropriately when they are entering the U.S. Canadian Press (Kingston Whig-Standard, B3, Chronicle Herald); Agence France-Presse (Le Droit, Huffington Post Québec) (2016-12-22); * Les Affaires (2016-12-21)

Toughen gun laws

An editorial states, "Canada may pride itself on not being the Wild West of gun violence, like its neighbour to the south. But it can still do better. The reality is Toronto police are concerned about gaps in gun control laws that they say are putting more legally purchased Canadian guns into the hands of dangerous criminals. That's not their only worry. They have also seen a spike in criminals using rifles and shotguns for crimes since the former Harper government shut down the long gun registry in 2012. Now their concerns are rightly being taken up by Mayor John Tory, who shared them in a letter last week with **Public Safety Minister Ralph Goodale**. As Tory put it, he wants only one thing: 'To get the guns out of the hands of those who choose to do harm and are hell-bent on disrupting our peaceful city.'" Toronto Star, A22

*** Trudeau is his Person of the Year**

A letter to the editor states, "Because it's 2016, Dec 15 Even if Justin Trudeau accomplishes nothing more, he has already launched two mighty waves that are unlikely to be reversed, namely the empowerment of women in politics and a change in the ways in which we view and negotiate with our indigenous brothers and sisters. That already makes him Person of the Year. Areas of Liberal government weakness remain, such as the unseemly issue of money for access, wavering around electoral reform and compromises struck on pipelines that call into question this government's determination to combat climate change. And I would argue that Mr. Trudeau and **Ralph Goodale** have not yet awakened to what it has meant to have had no genuine **public safety minister** for 10 years, i.e. someone beholden more to their job than to the gun lobby." Toronto Star (2016-12-21)

TOP STORIES / MANCHETTES

*** Des dizaines d'agents de la GRC ont fouillé dans la vie privée de Canadiens sans permission**
Des documents obtenus par Radio-Canada révèlent que des dizaines d'agents de la Gendarmerie royale du Canada (GRC) se sont servis de bases de données policières pour chercher des informations sur la vie privée de Canadiens sans autorisation. Selon des documents obtenus grâce à la Loi sur l'accès à l'information, de 2010 à 2015, 62 agents de la GRC se seraient servis sans permission de bases de données policières pour fouiller dans la vie privée de proches ou de citoyens. De ce nombre, 34 plaintes ont été jugées fondées. Notons par exemple celle d'un agent du Manitoba reconnu responsable d'avoir cherché sans autorisation le numéro d'une plaque d'immatriculation dans la base de données du Centre d'information de la police canadienne (CIPC). D'autres cas sont beaucoup plus inquiétants : en 2012, un agent a été reconnu responsable d'avoir recueilli de l'information sans autorisation d'une base de données de la GRC, en plus d'avoir entretenu des liens avec un criminel connu. Sa sanction? Une simple réprimande informelle. Une plainte déposée en février 2015 accuse un agent de s'être servi d'une base de données de façon inappropriée, d'avoir envoyé des photos à caractère sexuel à un mineur et d'avoir utilisé sa position en tant que policier pour entretenir une relation avec cette personne. L'information ne précise pas quelle sanction a été appliquée et la GRC a refusé de nous dévoiler plus de détails sur cette plainte sans une autre demande d'accès à l'information. Dans un courriel, une porte-parole de la GRC affirme que « la GRC prend très au sérieux les contraventions au code de déontologie, et elle s'emploie résolument à gérer les affaires disciplinaires avec diligence, efficacité et équité ». Elle ajoute que les employés de la GRC « doivent se comporter de façon non seulement à satisfaire, mais à dépasser les attentes élevées et justifiées des Canadiens. » Radio-Canada; Le Journal de Montréal

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** No quick end to disaster despite lack of new cases**
The Canadian Food Inspection Agency says it has not found any new cases of bovine tuberculosis in the past week, though it could take several more months to sound the all clear. Cattle ranchers in parts of Alberta, and Saskatchewan, have been rocked after a cow from Alberta that was slaughtered in the U.S. in October was found to have the disease. About 26,000 cows have been quarantined on dozens of ranches, and around 10,000 are set to be slaughtered to ensure the disease doesn't spread. Any animal that shows a sign of the disease is destroyed, and the meat cannot be eaten. CFIA chief veterinary officer Harpreet Kochhar told reporters on Wednesday that testing continues on thousands of animals, but the number of confirmed cases is unchanged from the six reported last week. Postmedia (Red Deer Advocate, A6; StarPhoenix, Edmonton Sun, Calgary Sun, Edmonton Journal)

*** Canada launches hotline to report bad drone drivers**
The government wants bad drone drivers reported. Expecting a spike in drone sales for Christmas, the transportation ministry on Wednesday launched an online hotline to report bad drone pilots. The new "incident-reporting tool," according to Transport Canada, aims to keep Canadians "safe from reckless drone use." The ministry urges Canadians to go to its website and fill out a report if they believe someone is flying a drone "in an irresponsible manner without a permit." Complaints would be reviewed by officials and if an operator is found to have broken the rules, he or she would be fined up to $25,000 or jailed. Agence France Presse (CTV News); Canadian Underwriter

*** Search for missing man suspended**
Eskasoni RCMP have suspended the search for 79-year-old Camillius Alex after five days. They were unable to find Alex, despite help from Ground Search and Rescue, volunteers in Cape Breton and area, and the Eskasoni fire department. The RCMP provided a helicopter, a fixed-wing plane, all-terrain vehicles, police dogs and UAV services. Chronicle-Herald, A5; Canadian Press (CTV News)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

La vigilance est de mise pour le 375e de Montréal

Si les Montréalais ne devraient pas nécessairement craindre des actes de terrorisme pendant les célébrations du 375e anniversaire, des experts soulignent l'importance de rester vigilant. «Tout grand évènement peut être une cible potentielle, parce que c'est une opportunité pour les terroristes. Le défi[en matière de sécurité], c'est un terrorisme improvisé, des loups solitaires qui agissent à la dernière minute», dit Michel Juneau Katsuya, ancien agent du Service canadien du renseignement de sécurité (SCRS). «Compte tenu que la menace est extrêmement évolutive et versatile, [...] ça pourrait contourner les dispositifs de sécurité mis en place», ajoute Stéphane Berthomet, codirecteur de l'Observatoire sur la radicalisation et l'extrémisme violent. Une dizaine de rassemblements de plus de 10 000 personnes sont prévus dans le cadre du 375e anniversaire, en plus des festivals habituels. Le Québec a toutefois beaucoup moins de risques d'être touché par le terrorisme que l'Europe et les États-Unis. «Malheureusement, Montréal a été le théâtre d'activités favorisant la montée d'un certain radicalisme. [...] Statistiquement, on a eu un taux disproportionné, par rapport au reste du Canada, de jeunes qui ont voulu partir ou qui sont partis faire le djihad», nuance M. Juneau Katsuya. Journal de Montréal, 14 (TVA Nouvelles)

Digitally secure, but private
An opinion piece states, "Historically, liberaldemocratic societies have tried to balance security challenges and reconcile the limits on civil liberties required to maintain the peace. In the 1950s, in an effort to curb the growing number of drunk drivers, Canadians became subject to breath tests and subsequently random spot checks without a reasonable doubt of guilt. (...) Police agencies, both in Canada and abroad, have looked for leadership from their governments since investigations into major crimes such as human-trafficking, terrorism, murder and the sexual abuse of children have been enabled by digital devices or the internet. The magnitude of the challenge was highlighted by the Royal Canadian Mounted Police's unprecedented looks into the challenges they face in securing Canadians in the digital age. Law enforcement agencies largely have the legal framework they need to investigate digital devices that enable crimes. However, the increasing levels of encryption that now exist on commonly used smartphones and applications will render these authorities borderline toothless. Here in Canada, privacy commissioners from around the country came together recently to caution lawmakers against legislating against encryption. Their argument is that any weakening of encryption would result in both risks to our civil liberties and unintended security challenges as we weaken the security architecture of commonly used platforms. The civil liberties argument against providing police the powers to collect and share the private data of citizens is not misguided. Security agencies around the world were alleged to have violated civil liberties in the name of national security by former U.S. National Security Agency contractor, Edward Snowden." National Post, FP7

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Man accused of killing Groton good Samaritan back in Conn. after fleeing to Canada
A man who ran from Groton, Connecticut, all the way to Canada was returned to the United States on Tuesday, and arrived back in the United States on Wednesday after an extradition process. Dante Hughes, 30, of Groton, is suspected of shooting and killing Joseph "Joey" Gingerella, 24, also of Groton, on December 11 around 1:30 a.m. after Gingerella tried to intervene when he allegedly saw Hughes beating a woman in a restaurant parking lot. It's been reported that she was Hughes' girlfriend. Gingerella was shot multiple times and died, and an arrest warrant charging Hughes with murder was issued. Groton Police told FOX 61 that on Wednesday, Hughes appeared at Niagara County Court in Lockport, New York, on charges of being a fugitive from justice. He had been deported there from Canada. At the hearing Hughes waived extradition, and was returned to Groton police. He will appear in court on December 22 to be arraigned for the murder charge. Fox 61

* **Canada-U.S. trade not broken: Freeland**
Donald Trump has pledged to fix a lot of broken things when he becomes U.S. president. But Canada's trade minister says the world leading trade relationship between Canada and the United States need not be on the president-elect's to-do list. "I think the reality is the trading relationship with Canada is the farthest possible thing from being broken. It is very balanced and mutually beneficial," Chrystia Freeland told The Canadian Press. That's the message she said she has been actively spreading to Republicans and others in Washington during the presidential transition period. Freeland visited Washington last week

and met with some senior Trump advisers and Republican senators. She had get-acquainted meetings with former House Speaker Newt Gingrich, now a Trump adviser, and Stephen Schwarzman, the CEO of the Blackstone Group investment firm, who was appointed earlier this month to lead the President's Strategic and Policy Forum. Trump has said the collection of 16 CEOs and business leaders will provide him what it takes to create jobs and drive growth. Freeland also met with the Republican chairs of two powerful committees - Sen. Pat Roberts of the agriculture committee and Sen. Orrin Hatch of the finance committee. Freeland reminded them the $2.4 billion a day that crosses the border is good for both countries. She hauled out some other well-worn statistics: nine million Americans depend directly on exports to Canada while 35 states have Canada as their top customer. London Free Press

High prices force millions to buy medicine outside U.S.
As drug prices have spiraled upward in the past decade, tens of millions of generally law-abiding Americans have committed an illegal act in response: They have bought prescriptions outside the U.S. and imported them. (…) The Food and Drug Administration has cautioned that many online pharmacies aren't what they seem. An international crackdown in 2014 found that many packages of medicines purportedly from Australia, Canada, New Zealand and the United Kingdom contained drugs from other countries, including India, China and Laos. (…) When purchased outside the country, many prescription medicines cost half or less than they do in the states. According to the FDA's website, it is generally illegal for Americans to import drugs into the states for personal use. The law isn't rigorously enforced, in part because it is difficult to monitor the entry of medicine in suitcases and small packages. But in 2015 the FDA implemented a rule that would give government border inspectors expanded authority to destroy drugs imported for personal use at their point of entry. Detroit News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

* **Cybersecurity firm finds evidence that Russian military unit was behind DNC hack**
A cybersecurity firm has uncovered strong proof of the tie between the group that hacked the Democratic National Committee and Russia's military intelligence arm — the primary agency behind the Kremlin's interference in the 2016 election. The firm CrowdStrike linked malware used in the DNC intrusion to malware used to hack and track an Android phone app used by the Ukrainian army in its battle against pro-Russia separatists in eastern Ukraine from late 2014 through 2016. While CrowdStrike, which was hired by the DNC to investigate the intrusions and whose findings are described in a new report, had always suspected that one of the two hacker groups that struck the DNC was the GRU, Russia's military intelligence agency, it had only medium confidence. Washington Post; Reuters (New York Times); Wall Street Journal

* **Don't get cyber-Scrooged!**
Tis the season to be jolly - but it's also the season for identity theft, phishing and credit card fraud. With Christmas just days away, people are using their smartphones and other devices to get a handle on their last-minute shopping. Hackers are on the hunt as well, looking to steal personal information from easy targets. "People just need to have their radar up, so that when they're trying to get their perfect gift to grandma's house in time for Christmas day, they're not clicking on things they shouldn't," says Michael Kaiser, executive director of the National Cyber Security Alliance. Here are some tips for staying safe this holiday season: You'd better watch out Make sure your phone's operating system and all the apps you use to shop are up to date. That way you'll have the fixes for any recently discovered security problems. You should also enable multifactor authentication in the settings on your important accounts. This is a security measure that requires you to enter a temporary code in addition to your password when signing in; services often text this code to your phone. It complicates life for hackers should they somehow manage to get your password. Improvements in credit card fraud detection have pushed hackers to focus on stealing legitimate login credentials, so adding an extra layer of protection to these accounts is a must, says John Dickson with the cybersecurity firm Denim Group. And while some cybersecurity experts question the value of changing your password frequently, Dickson says it's not a bad idea this time of year. Associated Press (Kingston Whig Standard, D5; Whitehorse Daily Star)

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Des dizaines d'agents de la GRC ont fouillé dans la vie privée de Canadiens sans permission**
Des documents obtenus par Radio-Canada révèlent que des dizaines d'agents de la Gendarmerie royale du Canada (GRC) se sont servis de bases de données policières pour chercher des informations sur la vie privée de Canadiens sans autorisation. Selon des documents obtenus grâce à la Loi sur l'accès à l'information, de 2010 à 2015, 62 agents de la GRC se seraient servis sans permission de bases de données policières pour fouiller dans la vie privée de proches ou de citoyens. De ce nombre, 34 plaintes ont été jugées fondées. Notons par exemple celle d'un agent du Manitoba reconnu responsable d'avoir cherché sans autorisation le numéro d'une plaque d'immatriculation dans la base de données du Centre d'information de la police canadienne (CIPC). D'autres cas sont beaucoup plus inquiétants : en 2012, un agent a été reconnu responsable d'avoir recueilli de l'information sans autorisation d'une base de données de la GRC, en plus d'avoir entretenu des liens avec un criminel connu. Sa sanction? Une simple réprimande informelle. Une plainte déposée en février 2015 accuse un agent de s'être servi d'une base de données de façon inappropriée, d'avoir envoyé des photos à caractère sexuel à un mineur et d'avoir utilisé sa position en tant que policier pour entretenir une relation avec cette personne. L'information ne précise pas quelle sanction a été appliquée et la GRC a refusé de nous dévoiler plus de détails sur cette plainte sans une autre demande d'accès à l'information. Dans un courriel, une porte-parole de la GRC affirme que « la GRC prend très au sérieux les contraventions au code de déontologie, et elle s'emploie résolument à gérer les affaires disciplinaires avec diligence, efficacité et équité ». Elle ajoute que les employés de la GRC « doivent se comporter de façon non seulement à satisfaire, mais à dépasser les attentes élevées et justifiées des Canadiens. » Radio-Canada; Le Journal de Montréal

*** Sharing RCMP social media posts helps solve crimes**
An opinion piece written by RCMP Assistant Commissioner Larry Tremblay states, "As 2016 comes to a close and we begin to look forward to a new year, I wanted to take this opportunity to thank the people of New Brunswick for the support enjoyed by the RCMP in this province. Many may not realize what an important role they play in helping to keep our communities safe, be it by consistently making responsible decisions, ensuring the safety of others, reporting impaired drivers, sharing RCMP messages on social media, or providing police or Crime Stoppers with information that might help solve a crime... In the past year, people sharing our posts has helped us to solve crimes, bring guilty parties to justice, and find missing people. One of the most memorable examples is perhaps the case of Marissa Shephard and Tyler Noel, who were wanted in connection with the December 2015 murder of Baylee Wylie in Moncton. Mr. Noel evaded police for three weeks, while Ms. Shephard remained a fugitive for two and a half months. Throughout the investigation, we saw thousands of people sharing our calls for information about Ms. Shephard's whereabouts, and keeping the case in the public eye until she was apprehended." Daily Gleaner, A7

*** This bill will save lives. Why are the Liberals against it?**
An opinion piece states, "Constable David Wynn died on duty, but it didn't have to be that way. It happened in January 2015, when Wynn and Auxiliary Constable Derek Bond were at a casino in St. Alberta, Alta., confronting a suspect about a stolen vehicle. The suspect, Shawn Rehn, shot both officers and fled the scene, later committing suicide. Bond survived his injuries; Wynn did not. Rehn never should have been at the casino that night, much less out on the streets. Months earlier, he was released on bail despite facing 29 outstanding Criminal Code charges. Rehn was a poster boy for the "revolving door" criminal, with a record spanning 20 years and 206 charges. Yet the court consented to his release on a cash bail and a number of conditions, which he subsequently broke. We know how that ended: with a widow, three children without a father and a family changed forever. The problem was that the court never heard Rehn's criminal history during his bail hearing — an oversight that makes entirely no sense. Indeed, risk assessment 101 dictates that past negative behaviour is the best predictor of similar future behaviour. But courts can't make proper assessments unless they actually hear about a bail applicant's past criminal activity. That's where Bill S-217 comes in. Proposed by Conservative Senator Bob Runciman, the bill proposes a simple amendment to the Criminal Code that would change the word "may" to "shall." That move would require the prosecutor or police representing the Crown to put an accused's criminal record, recent charges and/or "breach of trust" offences before the court. The judge still

maintains absolute independence, and the decision to release or detain remains his or hers alone. Yet for some unconscionable reason, the Liberals seem determined to kill the bill." CBC News

*** Amanda Lindhout kidnapping: Accused to face trial next October**
A man charged with taking journalist Amanda Lindhout hostage in Somalia is slated to face trial by judge alone next October. Three weeks have been set aside for the trial of Ali Omar Ader, which will come more than two years after he was arrested and over nine years after the abduction. Lindhout and Australian photographer Nigel Brennan were seized by masked gunmen near strife-scarred Mogadishu in August 2008. Both were released on Nov. 25, 2009. Ader, a Somalian national, faces a criminal charge of hostage-taking for his purported role as a negotiator. He was arrested by the RCMP in Ottawa in June 2015. The Mounties said Ader, 39, had been in town for a few days but the national police force has not publicly confirmed how he arrived in Canada. At the time, RCMP Asst. Commissioner James Malizia said successfully prosecuting such a case "depends on a certain level of discretion." Canadian Press (Global News)

*** Death in disguise: Seized pills confirmed to be fentanyl masquerading as Oxycontin**
On the street, they have a few nicknames: green monsters, greenies, green beans, green apples. They're 100 times stronger than morphine, and have caused an increasing number of deaths in Newfoundland and Labrador in recent years. It's fentanyl, an extremely potent synthetic pain medication, and it doesn't just come from pharmaceutical companies. Drug dealers are cooking them up in home labs and selling them disguised as less-potent Oxycontin pills and other drugs. On Wednesday, police said "Oxycontin" pills seized by the RNC/RCMP's Combine Forces Special Enforcement Unit (CFSEU) last month as part of Operation Titanium have been confirmed by Health Canada to be fentanyl. Police believe the pills were made in a clandestine lab and not by a pharmaceutical company, since they look identical to Oxycontin 80s - green with the number 80 stamped on one side and "CDN" on the other. Tree Walsh, co-ordinator of the AIDS Committee of Newfoundland and Labrador's Safe Works Access Program (SWAP), says the disguised fentanyl isn't a new thing in this province. "Even cocaine is laced with fentanyl now," she says. "It's in essentially everything." The homemade pills are especially deadly since their fentanyl content is never consistent, Walsh says. There could be none in one pill and an excessive amount in another, leading to an almost instant death. Walsh is confident if those 252 pills seized by police had made their way to the street, it would have resulted in multiple overdoses. The Telegram, A1/A3

*** More police presence needed in Hanwell**
Hanwell Mayor Chris Melvin says it's time for the community to come together to protect itself from an increased number of crimes. Thieves have been helping themselves to items left in unlocked vehicles, sheds, garages and houses. "It's not a sharp spike in crime but there has been an increase in thefts over the past couple of months. Other communities are also seeing the same thing," he said. According to the Keswick RCMP detachment, the thefts have occurred throughout the community, but especially in the Brookdale and Starlite subdivisions. Daily Gleaner, A2

*** Kelowna RCMP detachment commander announced**
Kelowna RCMP have announced Insp. Brent Mundle will officially take the reins as their detachment commander in the new year. The announcement was made on Wednesday by Chief Supt. Brad Haugli, commander of the B.C. RCMP's Southeast District, in consultation with Kelowna City Manager Ron Mattiussi. Global News (2016-12-21)

*** Surrey RCMP release 10 most wanted list**
These folks are on the naughty list, but you could get on the nice list if you have information that leads to an arrest. Surrey RCMP have released their wish list this year, naming the top ten most wanted criminals, along with a public call for tips. Each of the offenders are wanted for "numerous charges." The Province, A10

*** Terrace Mountie gets suspended sentence for assaulting teen**
A veteran B.C. Mountie convicted of assaulting an Indigenous teenager in Terrace, B.C., has been handed a suspended sentence with 12 months probation. RCMP Const. Bruce Lofroth was charged after

video surfaced in 2014 of a violent arrest of a teenage boy on a Terrace sidewalk Lofroth was sentenced Wednesday afternoon in a Terrace court. Provincial judge Edmond de Walle, who was brought in from Salmon Arm, also ordered Lofroth to perform 100 hours of community service and pay a $200 fine. In the video, played at Lofroth's sentencing hearing in October, a Mountie in black leather gloves appears to punch the youth's body and head. After the boy is handcuffed, the officer then appears to strike him in the face The video sparked two investigations. One was an RCMP code of conduct review. The second was a probe by the Independent Investigations Office of B.C. Lofroth was charged with one count of assault and placed on administrative desk leave. He pleaded guilty in August. CBC News (2016-12-21); Times Colonist (2016-12-22)

*** Police raid leads to couch fire in Moncton home**
The RCMP's tactical unit wound up in a literal firefight this week when a "flash-bang" device tossed into a home during a raid accidentally set a couch ablaze. The Emergency Response Team ended up carrying the couch outside where the fire was extinguished by police. The police team was called Tuesday to help detain people in a one-storey home on Shirley Avenue, between John and York Streets, in downtown Moncton. As part of the raid, police used a "flash bang, a non-lethal explosive device" that creates a burst of light and sound to disorient people and help the officers enter the house. The device landed on a couch in the home, setting it on fire as it discharged. Mounties were able to extinguish the fire before the Moncton Fire Department arrived. No one was injured in the incident. Telegraph-Journal, A4 (Times & Transcript)

*** Surrey's singing Mounties spread Christmas cheer**
Their shifts are spent patrolling a city plagued by gunfire and gang violence. With some 60 shootings in 2016, Surrey RCMP have no shortage of crimes to solve. Still, a few busy Mounties are finding time to continue a decade-old Surrey RCMP holiday tradition. "It's just another thing, another gesture of just giving," Const. Parnelli Parnes said. This year, the three-year Mountie is leading a team of more than a dozen caroling cops, who are lending their voices to spread Christmas cheer at local seniors' homes. Global News

*** RCMP extended family answers call**
Ever since her son Zachary was born, Heidi Hessing has never spent his birthday or Christmas away from him. So when Hessing, who is the spouse of an RCMP officer stationed in Lillooet, B.C., learned she wouldn't be able to see Zachary for his 20th birthday on Wednesday, she enlisted the help of some local "angels" to ensure he wouldn't feel alone. A few days ago, Hessing turned to a Facebook group for spouses of RCMP officers with a simple request. Could someone in Lethbridge please bring Zach some balloons? Her request resulted in an outpouring of support. Although they have never met Hessing, about two dozen local RCMP members, spouses and their children took up her call. Their mission was dubbed "Operation: Hug My Child," and they went above and beyond her request. Lethbrdge Herald (2016-12-21)

*** La GRC sauve un homme qui s'était effondré sur la glace d'une rivière**
En fin de semaine, des agents de la GRC et d'autres premiers intervenants ont sauvé un homme qui s'était aventuré sur les glaces de la rivière Saint-Jean. Samedi, vers 11h30, la GRC a reçu un appel l'informant qu'un homme de la Première Nation de Tobique s'était aventuré sur les glaces et qu'il s'y était effondré, inconscient. Les policiers ont réussi à atteindre l'homme et à le transporter près de la berge pour lui donner les premiers soins. L'Acadie Nouvelle, 8

*** Police, firefighters get together to put on big blood drive in Metro Moncton**
With days to go before Christmas, Metro Moncton firefighters and police joined forces to give the best gift they could think of: life. On Wednesday, the Codiac Regional RCMP and the Moncton Fire Department held Guns and Hoses, a bi-annual blood drive. Times & Transcript, A6

*** Rescued bald eagle on the mend**
An injured eagle that was coaxed to safety in southeastern B.C. with the help of a hockey stick and a chunk of salmon appears to be on the mend. The juvenile male bald eagle, dubbed Lily, appeared to have a broken wing when it was spotted in Revelstoke on Friday. But with no trained wildlife officers

nearby, it was up to two passing RCMP officers to use Canadian ingenuity to nab the bird. The officers used a hockey stick to extend a chunk of salmon to the starving bird, and it followed the fish to a spot where rescuers could cover and gently restrain him. Calgary Sun, A35 (Times Colonist, Calgary Herald)

*** Shediac holds property tax rate steady**
Shediac will maintain its property tax rate at $1.4784 per $100 of assessment for a 16th consecutive year. In a news release, Mayor Jacques LeBlanc says the town's 2017 operating budget of $11.5 million reflects 3.09 per cent growth in the town's tax base, to $655 million from $635.2 million, but also a decrease in its unconditional grant from the province to $148,500 from $214,000. Also, a 4.6 per cent jump in RCMP costs, to $1.3 million from $1.24 million comes on the heels of an increase the previous year of 5.8 per cent. Times & Transcript, A3

Drugs, Cash Seized
After six months of investigation, Edmonton police drug and gang investigators raided three homes, seizing hundreds of thousands of dollars worth of drugs and cash, and arrested three men with alleged ties to organized crime. More than $108,000 in Canadian currency was seized during the warrant executions, along with variety of illegal drugs including: Two kg of cocaine with a street value up to $110,000; 10 kg of marijuana with a street value up to $50,000; 357 grams of psilocybin with a street value up to $3,570; 103 grams of hashish with a street value up to $1,550; 84 grams of ketamine with a street value up to $4,210; 13 grams of shatter with a street value up to $965; and 44 kilograms of phenacetin with a street value up to $154,000. Edmonton Sun, A7 (Edmonton Journal)

*** Investigation launched into foster-care death**
Circumstances surrounding the death of an 18-year-old woman in foster care, in a home in Oakbank, will be subject to an external investigation requested by Sandy Bay Child and Family Services. Lydia Whitford was found dead in a licensed foster home last summer in Oakbank, in the rural municipality of Springfield, but her death was ruled a homicide only this week. Oakbank RCMP said Tuesday they responded on July 14 to the home where Whitford's body was found. The RCMP's major crime and serious crime units also are investigating. Winnipeg Free Press, B3 (2016-12-22); CBC News (2016-12-21)

*** Regina police renew rewards for information on cold cases**
The rewards for the Tamra Keepness disappearance and a 2011 triple homicide were renewed for another year at the monthly Regina board of police commissioners meeting Wednesday. Keepness was last seen at her home in Regina on the evening of July 5, 2004. She was reported missing the next morning. On July 13 that year, a $25,000 reward for information about Keepness' location was made. Ten years later, the reward was increased to $50,000. On Aug. 6, 2010, the bodies of Gray Nay Htoo, his wife Maw Maw, and their three year-old son Seven June were found at a home in Regina. The family were Karen refugees from a Thailand refugee camp and had lived in Regina for approximately two years. Since the beginning of the investigation, the RPS has worked with an RCMP member of Karen descent in order to communicate with the Karen community. StarPhoenix, A6 (Leader-Post)

*** Remains of missing Red Deer woman found on rural property**
A Red Deer woman, who went missing in February, has been confirmed dead after human remains were discovered on a rural property. Lorie Nichols, who was 49, was last seen in the Michener area in Red Deer on the evening of Feb. 23. She was reported missing that evening by her family. Blackfalds RCMP said in a statement on Wednesday that they were alerted to the discovery of human remains last Friday. Red Deer RCMP Forensic Identification Section, and Major Crimes South, completed an examination of the scene and investigated the circumstances of the discovery of the remains. Red Deer Advocate, A6

*** OPP back fentanyl awareness initiative**
Ontario Provincial Police are joining the fight to educate the public about the dangers of fentanyl, which has been linked to more than 500 deaths in the province over the past five years. The force is releasing public service announcements and says it will post or link content to its Facebook and Twitter accounts in an effort to make the public aware of the threats posed by fentanyl and similar opioids. RCMP

Commissioner Bob Paulson and Chen Zhimin, the vice-minister of China's public security ministry, have agreed to boost efforts to disrupt the flow of the drug and other opioids. British Columbia has been hard-hit by the opioid crisis - fentanyl was detected in 374 overdose deaths during the first 10 months of 2016. Waterloo Region Record, B5

*** 'He Had Four Months With Them And He Took Them Away'**
The mother of two boys killed by their father in a double-murder suicide said Wednesday her sons only moved in with their father this year so that they could play hockey in Spruce Grove. Ryder MacDougall, 13, and Radek MacDougall, 11, and their father Corry MacDougall, 39, were found dead in MacDougall's Spruce Grove home Monday morning. The boys moved to Spruce Grove this past summer after living in Whitecourt, where their mother and stepfather still live. RCMP have since confirmed the triple death was a double homicide-suicide and gunshots were the boys' cause of death. Calgary Sun, A7 (Edmonton Sun, Calgary Herald, National Post) (2016-12-22); CBC News (2016-12-21)

*** Man accused of sexual communications with minor**
A man in Dallas, Texas, is accused of having sexual communications over the Internet with an underage person in the Indian Head area. Indian Head's RCMP detachment received the complaint on Nov. 21, 2015. Police said the complaint concerned inappropriate online communication that was sexual in nature between an adult man and a minor in the Indian Head area. Police would not specify the age or gender of the victim. An investigation was carried out with the assistance of the Saskatchewan Internet Child Exploitation Unit (ICE), and police later determined the male suspect was located in the United States. Since the suspect was in the U.S. and the communication originated from that country, police passed the information along to the Department of Homeland Security. Last week, a man in Dallas was identified and arrested in connection with the investigation. Leader-Post, A3

*** Credit card scam widespread**
The RCMP is warning businesses throughout the province to be on the alert for a credit card scam targeting merchants. Const. Jeremiah Donahue of the RCMP's Gander detachment said new evidence shows that the recent fraudulent credit card activity reported in Gander is much more widespread than previously thought. He also noted that the pattern of criminal activity suggests more than one culprit may be involved. The Telegram, A3

*** RCMP officers conducting checkstops over holidays**
December is Impaired Driving Awareness Month in Alberta and Corporal Curtis Peters, media relations officer with the RCMP K Division, said checkstops will be conducted across the province throughout the month of December. Alberta RCMP has partnered with Mothers Against Drunk Driving (MADD) to promote Impaired Driving Awareness Month through the media and social media. The most recent statistics on MADD Canada's website show 1,497 out of 2,546 fatal collisions across the country in 2012 involved drivers who had some sort of alcohol or drug presence in their systems. Airdrie City View

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** How bad is Canada's recidivism problem? Nobody knows.**
Numbers matter in banking, golf and lotteries — and no less in the murky world of crime and punishment. By the numbers, crime in Canada is a swamp of confounding data. According to recent statistics, a little over two million incidents were reported to police in Canada in 2014. As a result of those reports, there were 228,328 guilty findings in adult criminal courts. Of those, 64,604 resulted in admissions to provincial or territorial custody and 4,781 to federal prisons — where those who commit the more serious crimes are sent if they receive a sentence of two years or more. Try to figure out how many of those people reoffend, however, and the numbers start to baffle. Consider recidivism rates in the federal system (federal and provincial jurisdictions overlap, of course). According to the 2014 Correctional Service of Canada (CSC) offender population profile, about eight out of 10 male and seven out of 10 female offenders have previous convictions. In the 2013 report, the stats were nine out of 10 men and eight out of 10 women. (…) A significant portion of the prison population suffers from serious mental disorders. According to a 2015 Correctional Service Canada report, 'National Prevalence of Mental Disorders Among Incoming

Federally-Sentenced Men', 44.1 per cent of inmates have antisocial personality disorder, 15.9 per cent have borderline personality disorder, 29.5 per cent suffer from anxiety disorders and 3.3 per cent are classified as "primary psychotic". iPolitics

Justice - L'ex-juge Jacques Delisle ne sera pas remis en liberté
L'ex-juge de la Cour d'appel Jacques Delisle, qui purge une peine de prison à perpétuité pour le meurtre de sa femme, va demeurer derrière les barreaux en attendant le résultat de sa demande de révision judiciaire du verdict auprès de la ministre fédérale de la Justice, a tranché un juge mercredi. Jacques Delisle se dit victime d'une erreur judiciaire, et il a demandé à être libéré pendant que sa demande est étudiée à Ottawa. Mais le juge Benoit Moulin, de la Cour supérieure, a refusé que l'homme de 81 ans soit remis en liberté, car il estime que cela pourrait miner la confiance du public envers le système de justice. Il a rendu sa décision mercredi matin après avoir entendu cet automne les arguments du procureur de la Couronne et des avocats de l'ex-juge. " La confiance du public dans l'administration de la justice commande que M. Delisle continue de purger sa peine : un public formé de personnes raisonnables, bien informées des dispositions législatives et des circonstances réelles de l'affaire, qui apprécient les fondements de notre système de justice criminelle et qui ne sont pas mues par la passion mais par la raison, n'accepteraient pas la mise en liberté, à ce stade des procédures ", écrit le magistrat dans sa décision. Presse canadienne (Le Devoir, A5, Le Droit, Le Soleil, La Tribune, Le Nouvelliste); Canadian Press (Chronicle-Herald, A8); Postmedia Network (London Free Press, StarPhoenix, Leader-Post, National Post, Ottawa Citizen, Windsor Star, Vancouver Sun, Edmonton Journal, Calgary Herald, Montreal Gazette, Province); Agence QMI (Journal de Québec, Journal de Montréal)

* **NS man convicted of child luring, child porn offences granted day parole**
A Nova Scotia man convicted of child luring and accessing child pornography has been granted day parole. Alexander John Ernst was sentenced to three years in prison in June 2015. Parole Board of Canada documents obtained by Global News show that Ernst used social media to attempt to lure underage females, and one of the potential victims turned out to be an undercover police officer. A search of his computer following his arrest also turned up 250 deleted images of child pornography. Global News (2016-12-21)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

* **Saskatoon police carding practice evolves in face of criticism**
Saskatoon's police chief says officers are changing the way they approach street checks. The police practice of stopping and quizzing individuals at random emerged as a hot button issue this year. Critics characterized it as thinly-veiled racism. Police chief Clive Weighill said he appreciates the concerns of people who feel racially targetted. To that end, police now explain to a person why they are being stopped. "I think the good compromise is, and we've already told our officers to do this, if you do stop somebody the very first thing out of your mouth should be the reason why you're stopping that person," he said in a recent interview. But Weighill said it's counterproductive for officers to begin an exchange explaining that a person does not need to answer any questions. CBC News

* **B.C.'s first responders at the breaking point: MENTAL HEALTH CRISIS**
Incessant overdose calls and multiple drug deaths during shifts are taking a serious toll on the mental health of B.C. paramedics, according to their union. Bob Parkinson, director of health and wellness for the Ambulance Paramedics and Emergency Dispatchers of B.C., said even before the current fentanyl-related overdose crisis, paramedics were feeling strained while responding daily to life-and-death situations. (...) With an overdose crisis across the province, paramedics in small communities are responding to calls and reviving friends' kids or handling multiple overdoses involving casual drug users at parties, Parkinson said. Parkinson said depression and anxiety are the most common mental health issues among paramedics, but some are dealing with post-traumatic stress disorder or struggling with family problems and their own addiction issues. He's worried the workforce will lose quality women and men. "You know how we cope as a first responder or a paramedic or a dispatcher - we go 'til we break and then it's too late," he said. Both Parkinson and Bronwyn Barter, president of the union, are pleading

for more resource support and for government to quickly respond to an ORH report recommending an increase in B.C. Emergency Health Services' fleet size. (...) Barter said paramedics are accustomed to responding to life-and death situations, but the overdose crisis has changed the nature of their work. Province, A14 (Vancouver Sun)

*** Fentanyl campaign begins with arrests**

Talk about underlining a point. Just as Ontario Provincial Police launched a public relations offensive Wednesday against the growing scourge of fentanyl and similar opioid drugs, London police were wrapping up the seizure of 30 fentanyl patches of various dosages. The OPP said it's moving ahead with public service announcements and links to its Facebook and Twitter accounts in a bid to make the public better aware of the dangers of fentanyl, a powerful painkiller whose use has led to a dramatic spike in overdose deaths across the country. In London, advocates for the drug-addicted say misuse of another drug, the stimulant crystal meth, is much higher than the misuse of fentanyl. The local crisis is so bad the city's homeless coalition is launching its own awareness campaign next year. London police say fentanyl seizures have not become common in London. still, the city has not been immune from the fallout of the drug's abuse. dozens of vials of the potent drug in liquid form went missing from a London hospital five years ago, as the drug's street crisis in canada began. At the time, local outreach workers blamed up to 30 deaths in the previous two years on fentanyl overdoses. Wednesday, London police said they arrested two people and seized prescription fentanyl patches - used to administer the drug through the skin - after investigating a vehicle in the Millbank drive area. London Free Press

*** For addicts, road to recovery starts with a wait: At Royal Jubilee, 45 people are on list for treatment at its 21-bed detox unit**

While officials scramble to set up places where illicit drugs can be safely injected, addicts wanting to get clean and sober are looking at wait-lists for detox - the first step on the road to recovery. It makes no sense whatsoever, said Carole James, B.C. NDP MLA for Victoria-Beacon Hill. "We're hearing that the fentanyl crisis has people who are ready, ready to go to detox," James said. "Everyone who works in the addictions field knows that in order to be successful, you have to grab someone when they are ready." Island Health is applying to open three supervised injection sites in Victoria. Such sites offer a hygenic place in which users can inject drugs under the supervision of health professionals. In the meantime, it plans to open temporary overdose-prevention sites. There were 755 fatal drug overdoses in B.C. between January and November, an increase of more than 70 per cent increase over the same period in 2015. The opioid fentanyl has been linked to about 60 per cent of drug deaths in B.C. this year. Island Health spokeswoman Kellie Hudson said 45 people are on a wait-list for the 21-bed detox unit at Royal Jubilee Hospital. That is more than double the usual number, but isn't out of the norm for the Christmas season, especially given the cold weather, she said. Times Colonist, A3

*** Naloxone saved pup from drug overdose**

Two doses of naloxone saved a six-month-old puppy from an overdose after it ingested drugs in Mount Douglas Park. Veterinarian Helen Rae said Chico was brought to the McKenzie Veterinary Hospital on Friday evening after her owners noticed she was wobbly and appeared to be under the influence of drugs. The owners knew the puppy had eaten something while on leash in the Saanich park but didn't know what. Rae noticed the dog, a pug cross, couldn't walk straight, seemed sedated and had constricted pupils. "We thought it was marijuana at first, because we see so many of those [cases], but she didn't quite fit the picture," she said. Rae made the dog vomit and gave her activated charcoal to stop further absorption of the drug, but Chico's condition continued to deteriorate. The vet decided to administer two low doses of naloxone. Naloxone reverses the effects of opioid drugs such as heroin, fentanyl, oxycodone and morphine. "She went from being flat on the table, unable to lift her head, to lifting her head and responding to voice and stimulation," Rae said. While pets are often brought to the vet after consuming marijuana, Rae said this is the second time she has seen a dog overdose from opioids in her 18-year career. A public health crisis has been declared because of a rise in deaths linked to fentanyl, an opioid that is 50 to 100 times more powerful than heroin. Times Colonist, A1/Front

*** Transit Police to get more Tasers**

Transit Police Chief Doug LePard is ordering a three-fold increase in the number of officers equipped with Tasers as a way of providing an alternative to using guns during critical incidents. LePard said

Wednesday that there are currently about 20 officers trained and equipped with Tasers among the force's 120 front-line officers. That number should reach 60 during the coming year. "I want police officers to have that option if it's appropriate," he said. "You never want to be forced to use deadly force if there is an option." The directive would mean one officer in every pair would be equipped with a Taser that could be used to subdue a person acting dangerously, while the other officer would stand "lethal overwatch" with a standard-issue Glock handgun. LePard made the comment in response to the shooting earlier this week of a man armed with a machete-like weapon at the 29th Avenue SkyTrain Station. Transit officers had locked the man inside a train, but he escaped after kicking out a window and was shot by Vancouver police. The man remains in serious condition in hospital but is expected to survive. Metro Vancouver is the only region in Canada with dedicated transit police. The shooting provides a window into the unique role of transit police and their relationship with other municipal and RCMP forces in the region. Province, A3

*** 'It's just tragic': Therapist concerned about treatment programs in Cape Breton**
A 70 per cent increase in the number of suicides from 2014 to 2015 has a local clinical therapist questioning the present state of mental health and addictions treatment programs in Cape Breton. "People want help," says Todd Vassallo, a psychotherapist based in Sydney. "But we need to be human about this." Vassallo said he became increasingly concerned when he read data from the Nova Scotia Medical Examiner's office indicating that suicide deaths in Cape Breton (including acute drug toxicity suicide deaths) had risen from 14 in 2014 to 24 in 2015. That figure could be even higher since the data for 2015 was incomplete. In 2009, the number of suicide deaths in Cape Breton was 25. In 2010, it declined to 11. The following two years it increased again to 21 deaths in 2011 and 22 deaths in 2012. In 2013, the number of suicides island-wide dropped to 17. As for acute drug toxicity deaths last year, it was determined that suicide was the cause of death in seven cases and nine were accidental in nature. Vassallo began to notice the increasing suicide rate last year but the provincial numbers didn't seem to mirror what he saw happening around him. Cape Breton Post, A1

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Quebec calls public inquiry into systemic racism**
Premier Philippe Couillard has launched a public inquiry into the treatment of aboriginals, acquiescing to a long-time demand of indigenous chiefs and women's groups. The announcement drew cheers and tears of joy at the Val-d'Or native friendship centre, where women had gathered to watch the news conference on Wednesday. "We experience many things - racism, injustice, so ... we are very relieved that there's a public inquiry. For once, we'll be treated as equals," Cherilyn Papatie told Radio-Canada. Calls for an independent inquiry grew louder this fall after an investigation into allegations that provincial police abused indigenous women in Val-d'Or concluded there was not enough evidence to lay charges. Quebec's director of penal and criminal prosecutions (DPCP) did not charge officers in Val-d'Or, but charged two retired SQ officers from Schefferville for sexual assault alleged to have occurred in the 1980s and 90s. "The impact of these denunciations is that other women and men in Quebec now have a forum to tell their stories," said Édith Cloutier, executive director of the Val-d'Or native friendship centre. "We are celebrating the moment; these women know they just made history." The Couillard government had been opposed to holding an independent public inquiry, saying concerns would be investigated as part of the federal inquiry into missing and murdered indigenous women. Gazette; Globe and Mail; CBC News

*** Racisme systémique - Le Québec s'ouvre à la critique : Le gouvernement Couillard lance l'enquête publique que réclamaient les autochtones**
Après bien des réticences, le premier ministre Philippe Couillard a annoncé la tenue d'une commission d'enquête québécoise sur les relations entre les services publics et les autochtones sous le titre " Écoute, réconciliation et progrès ". Présidé par le juge à la retraite de la Cour supérieure Jacques Viens, la commission d'enquête visera non seulement les corps policiers, mais aussi les services sociaux, la protection de la jeunesse, les services correctionnels et le système de justice. Alors que jusqu'ici, tant le

premier ministre que ses ministres avaient évité de parler de racisme systémique en ce qui a trait aux autochtones, Philippe Couillard a reconnu, mercredi, le phénomène. " Ce que nous voulons accomplir, c'est d'examiner les enjeux systémiques, incluant le cas du racisme, a-t-il affirmé en réponse à une question d'une journaliste. Je veux le dire ouvertement : le Québec n'est pas différent d'autres sociétés. Une des causes qui rassemble les Québécois, " c'est notre désir de lutter contre l'intolérance, la discrimination, l'exclusion et la stigmatisation ", a déclaré Philippe Couillard dans sa présentation. " Parce que peu importe la couleur de notre peau, nos croyances ou qui nous aimons, personne ne mérite d'être humilié, diminué ou exclu. " Le premier ministre était accompagné de quatre de ses ministres -- Stéphanie Vallée (Justice), Martin Coiteux (Sécurité publique), Geoffrey Kelley (Affaires autochtones) et Lucie Charlebois (Protection de la jeunesse et Santé publique) --, ainsi que du chef de l'Assemblée des Premières Nations du Québec et du Labrador (APNQL), Ghislain Picard, et du grand chef des Cris, Matthew Coon Come. Le Devoir, A1

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Drug impaired driving fatalities on the rise in Washington State
The number of fatal car accidents involving drugged drivers is on the rise in Washington State. Shortly after pot was legalized in Washington, the percentage of potentially stoned drivers involved in fatal car accidents more than doubled, according to a study by the AAA Foundation for Traffic Safety. The most recent data suggests that in 2014, 17 per cent of drivers involved in fatal accidents had THC - the active ingredient in marijuana - in their blood. According to Shelly Baldwin, legislative and media relations manager for the Washington Traffic Safety Commission, the issue still looms large. CBC News (2016-12-21)

Marijuana shop raided. Owner charged, $20,000 of pot seized
A medical marijuana dispensary owner has been charged following a police raid of the business. Vice and drug officers - armed with a search warrant - arrived at the Royal Farmacy on Main Street East at Kenilworth Avenue around 1 p.m. Tuesday, where they seized $20,000 worth of marijuana and marijuana products, including edibles. Hamilton Spectator, A6

Perquisition dans une boutique de cannabis
La police de Gatineau a frappé mercredi après-midi en mettant la clef dans la porte de la première boutique de vente libre de marijuana à avoir pignon sur rue du côté québécois de la rivière des Outaouais. Au terme d'une courte enquête qui avait été entamée à peine 24 heures plus tôt à la suite d'informations reçues du public, des policiers munis d'un mandat de perquisition se sont rendus vers 14h30 au commerce Clinique Canna-Plus, situé au 341, boulevard Saint-Joseph, en face des Galeries de Hull. Sur place, trois femmes et un homme ont été arrêtés puis transportés au quartier général du Service de police de la Ville de Gatineau (SPVG), où ils devaient demeurer détenus toute la nuit en vue de comparaître devant le tribunal jeudi. Ces quatre individus pourraient faire face à des accusations de possession et de trafic de cannabis. Le Droit, 5

PUBLIC SERVICE / FONCTION PUBLIQUE

Ils se privent d'argent pour éviter Phénix
Les fonctionnaires fédéraux sont de plus en plus nombreux à se priver de revenus en refusant les promotions ou le temps supplémentaire, de peur que cela n'affecte leur salaire. «Depuis quelques semaines, on nous rapporte de plus en plus de cas d'employés qui refusent de prendre l'intérim de postes supérieurs ou de faire du temps supplémentaire. Ils sont trop craintifs à l'idée que Phénix «joue» dans leur paie régulière», affirme la porte-pa-role de l'Alliance de la Fonction publique du Canada (AFPC), Monique Déry. Le syndicat, qui regroupe 128 000 fonctionnaires, croit que le phénomène ne peut que prendre de l'ampleur dans les prochaines semaines si les problèmes du système de paie ne sont pas bientôt réglés. Journal de Québec, 7

*** CAPE says federal government isn't offering what it offered other unions**
A union representing thousands of federal government economists, translators and Library of Parliament workers says contract talks are at an impasse because the government isn't offering what it gave members of other large public service unions earlier this month. The Canadian Association of Professional Employees, or CAPE, has rejected the offer to some of its 12,000 members. The union's leadership says it's upset some of its employees aren't being offered the same raises as members of other unions, and that it isn't getting protection for members that give the government what it calls "evidence-based advice," according to a media release. CBC News

*** HP Canada complaint raises concerns over federal procurement process**
A spat between Hewlett-Packard Canada and Shared Services Canada (SSC) is bringing the accountability of the federal government department into sharp focus. The computer supplier filed a complaint with the Canadian International Trade Tribunal (CITT) in November, alleging that SSC wrongfully rejected its bid on a high-performance computing solution. The $430.4 million project in question is said to be for a weather forecasting supercomputer to be used by Environment Canada. HP Canada accuses the SSC of unfairly concluding that its bid didn't meet the conditions set out in its request for proposal (RFP). Reports said that HP has asked a federal court to determine whether SSC wrongly invoked a national security exception (NSE) during the procurement process and chose a solution from IBM. In 2012, SSC notified suppliers that it would invoke NSEs for procurements related to email, telecommunications and data centres. These exemptions are intended for use when there is a national security concern around a project. They enable government departments to avoid following procurement rules laid down by trade agreements when purchasing solutions such as IT equipment. An NSE means that they don't have to consider proposals from companies that may put other governments' interests first. IT World Canada (2016-12-21)

OTHER / AUTRE

Ses deux enfants sont nés en captivité
Les parents d'un Canadien retenu en otage en Afghanistan se désolent que la plus récente vidéo de sa famille et lui ait été leur première occasion de voir leurs petits-enfants, nés en captivité. Joshua Boyle et sa femme américaine, Caitlan Coleman, ont été enlevés en 2012 alors qu'ils voyageaient dans la région montagneuse du nord de l'Afghanistan. Dans une vidéo dévoilée plus tôt cette semaine, on peut apercevoir le couple et ses deux enfants implorer les «gouvernements des deux côtés» de parvenir à une entente pour leur libération. Les parents de Joshua Boyle affirment qu'ils ont entrevu leurs deux petits-enfants pour la première fois dans cette vidéo. Les enfants grimacent face à la caméra alors que les cliquetis des chaînes de Joshua se font entendre en trame de fond. Par communiqué, Patrick et Linda Boyle ont qualifié d'«incroyable» tout ce que Joshua et sa femme ont dû faire pour protéger les bambins. Selon une lettre de leur fils, sa femme et lui protègent leurs garçons en prétendant se livrer à un jeu avec les talibans. Voix de l'Est, 24; Canadian Press (The Guardian, Red Deer Advocate, The Telegram, Cape Breton Post, Times Colonist, Ottawa Sun, Waterloo Record, Calgary Sun, Edmonton Sun, Toronto Sun, Winnipeg Sun, Chronicle Herald)

*** Latvian envoy defends Canadian-led NATO mission**
Latvia's ambassador to Canada is defending a NATO decision to send a Canadian-led battle group to his Baltic country in 2017, after a Russian diplomat suggested this act of deterrence aimed at Moscow was a waste of resources that would be better spent fighting terrorism. Karlis Eihenbaums said it's Moscow's aggression that has made the deployment necessary, including a buildup of Russian military assets on Russian territory adjoining Eastern and Central European countries. Alexander Darchiev, Moscow's ambassador to Canada, told The Globe and Mail in an interview on Wednesday he felt the coming North Atlantic Treaty Organization deployment to Latvia was an unwise diversion of resources from fighting what he considered the biggest menace: terrorism. Mr. Darchiev acknowledged it was a "sovereign decision" made by Canada but said he felt it would be bad for European security. Mr. Eihenbaums said, however, that NATO's decision to shore up its eastern flank - including sending British fighter jets to Romania and U.S. tanks and soldiers to Poland - was triggered by Russia's annexation of Crimea in 2014

and the ongoing support Moscow is providing to pro-Russian militants in Eastern Ukraine still fighting a bloody war with Kiev. Globe and Mail

*** Trudeau pays back taxpayers about $38K for personal expenses**
Prime Minister Justin Trudeau reimbursed taxpayers at least $38,000 for personal and family expenses during his first year in office, with extra childcare for his three kids topping the list. CBC News has obtained financial records of more than two dozen reimbursements Trudeau made for food, internet service and caregivers since becoming prime minister on Nov. 4 last year, as well as his payments to National Defence and RCMP for personal and family use of government aircraft. Trudeau has paid National Defence more than $9,000 for personal and family travel on the military Challenger jets, nine such trips so far that included holiday destinations in St. Kitts Nevis and Tofino, B.C. The prime minister also reimbursed the RCMP for use of their aircraft to fly to Fogo Island, N.L., last March, at $556.20. CBC News

INTERNATIONAL

Berlin suspect had been under surveillance
The prime suspect for the Berlin massacre was under covert surveillance for months as a possible terrorist threat until police let him slip through their grasp earlier this month. Anis Amri, 24, a Tunisian asylum seeker who arrived in Germany last year, was investigated for "preparing a serious crime endangering national safety," involving funding the purchase of automatic weapons for use in a terrorist attack. Amri had been arrested earlier this year and was known to be a supporter of the terrorist group thought to be behind the Sousse terrorist attack in Tunisia, as well as being a suspected disciple of a notorious hate preacher. He had multiple identity documents with six different aliases under three nationalities, and a criminal record in Italy and Tunisia. He spent four years in an Italian prison before travelling to Germany after an expulsion order expired. The German authorities, who were facing serious questions Wednesday about how Amri was still at large, tried to deport him in June, but because he had no valid papers proving his nationality he was allowed to stay. In a further twist, Germany had asked Tunisia to issue a new passport for him so he could be deported, but the document only arrived Wednesday - two days after the Christmas market attack that claimed 12 lives. Postmedia Network (The Province, A18, Ottawa Citizen, National Post, Star Phoenix, Leader-Post, Edmonton Journal, Calgary Herald, London Free Press, Windsor Star); Associated Press (Times Colonist, Telegraph-Journal, Times & Transcript, Montreal Gazette, Vancouver Sun, National Post, Global News); Kingston Whig-Standard; Edmonton Sun (Ottawa Sun, Toronto Sun, Winnipeg Sun); * Le Devoir

*** Germany has 7,000 terror suspects at large and is finding it 'almost impossible' to monitor them, former UK intelligence chief says**
Germany is finding it 'almost impossible' to keep track of around 7,000 potential terror suspects in the country, a former British intelligence chief has warned. Richard Barrett, who was head of counter-terrorism at MI6, said the authorities were finding the number of 'live' cases unmanageable. The grim assessment came as German security services face difficult questions following the Berlin Christmas market massacre. Daily Mail

*** Attentat de Berlin: les autorités allemandes critiquées**
Les autorités allemandes faisaient face jeudi à une polémique croissante au sujet des dysfonctionnements qui ont permis au suspect tunisien de l'attentat au camion-bélier à Berlin d'échapper à la police alors qu'il était connu comme islamiste dangereux. «Ce n'est pas comme cela que nous allons garantir la sécurité de l'Allemagne», a dénoncé l'un des responsables du parti conservateur de la chancelière Angela Merkel (CDU), Armin Laschet, à propos des failles ayant empêché l'arrestation ou l'expulsion d'Anis Amri. Les informations que nous avons sur la manière dont les autorités ont travaillé sont choquantes», a-t-il ajouté sur la radio publique. Une chasse à l'homme à l'échelle européenne est en cours contre Anis Amri, un demandeur d'asile débouté de 24 ans, depuis que la justice allemande a lancé un mandat d'arrêt sur tout le continent, plus de deux jours après l'attentat qui a fait 12 morts sur un marché de Noël de Berlin. L'acte a été revendiqué par le groupe État islamique (EI). Six victimes sont

allemandes. Une septième a été identifiée comme étant une ressortissante israélienne, ont annoncé les autorités de son pays jeudi. Agence France-Presse (La Presse, TVA Nouvelles)

*** German market attack suspect's brother urges him to surrender**

Authorities across Europe scrambled Thursday to track down a Tunisian man suspected of driving a truck into a Christmas market in Berlin as one of his brothers urged him to surrender. Nearly three days after the deadly attack that killed 12 people and injured 48 others, the market in the centre of the capital was due to reopen. German authorities issued a wanted notice for Anis Amri on Wednesday and offered a reward of up to 100,000 euros ($104,000 US) for information leading to the 24-year-old's arrest, warning that he could be "violent and armed." One of Amri's brothers urged him to turn himself in. "I ask him to turn himself in to the police. If it is proved that he is involved, we dissociate ourselves from it," brother Abdelkader Amri told The Associated Press. He said Amri may have been radicalized in prison in Italy, where he went after leaving Tunisia in the wake of the Arab Spring uprisings. Associated Press (CBC News)

Jordan's king vows 'iron fist' response to security threats

Jordan will respond with an "iron fist" to those threatening its security, King Abdullah II said Wednesday after a series of attacks on police and tourists this week left 14 people dead. The extremist group Islamic State has claimed responsibility for some of the shootings, including a gun battle at a Crusader castle popular with foreign visitors. In all, 11 members of the security forces, two Jordanian civilians and a Canadian tourist have been killed in clashes this week. Five gunmen were also killed. The pro-Western kingdom is a key member of a U.S.-led military coalition against IS which controls parts of neighbouring Iraq and Syria. The state news agency Petra quoted the king as saying that "we will respond with an iron fist to any attempts to tamper with the kingdom's security." The Guardian, B6 (Cape Breton Post, Ottawa Sun, Waterloo Record)

Snow-capped end to Aleppo war

Hundreds of rebel fighters and civilians, including small children swaddled in thick blankets, were bused out of war-ravaged Aleppo in heavy snow on Wednesday as the evacuation of former rebel strongholds entered its final phase. Scenes of buses slowly driving out of Aleppo in a shroud of white offered an evocative finale to what has been one of the most brutal chapters in Syria's civil war. The departures from Aleppo pave the way for Syrian President Bashar Assad to assume full control, after more than four years of fighting over Syria's largest city. It marks the most significant victory for Assad since an uprising against his family's four-decade rule swept the country in 2011. The evacuations were set in motion last week after Syria's opposition agreed to surrender its last footholds in eastern Aleppo. Since then, about 25,000 fighters and civilians have been bused out, according to the United Nations. Associated Press (Toronto Star, A12)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
September 23, 2016 / le 23 septembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Immigration centres detain hundreds of children each year
An average of 242 children, including babies born in Canada, are held in immigration detention in Canada each year, according to a new report by the University of Toronto. "Conditions of detention are woefully unsuited for children. Immigration holding centres resemble medium-security prisons, with significant restrictions on privacy and liberty, inadequate access to education, insufficient recreational opportunities and poor nutrition," said the report, No Life for a Child, to be released on Parliament Hill Thursday. (…) **Public Safety Minister Ralph Goodale** has been under fire this year after three detainees died in custody of the Canada Border Services Agency. In August, Ottawa announced $138 million in funding to "enhance alternatives to detention" and invest in rebuilding immigration holding facilities. **A spokesperson for Goodale** said the minister welcomed the report as it underlines the government's commitment to create a better, fairer immigration detention system while upholding public safety.

***"Minister Goodale has been clear that he wants to try to avoid housing children in detention facilities, as much as humanly possible. He welcomes the report's suggestion that when decisions are made on the detention of parents, the best interests of their children should be given greater prominence,"* the spokesperson** said in an email. The report shows living in immigration detention causes serious psychological harm to children. Those who have lived in detention experience increased symptoms of depression, anxiety, post-traumatic stress and suicidal ideation, as well as developmental delays and behavioural issues. "These mental-health consequences often persist long after the children have been released, affecting their adjustment to life post-detention," the 77-page study said. Toronto Star, GT6

Blame Montreal's airport folly on a broken management model

Perhaps no three words in the French language generate more fear and loathing among air travellers these days than "Bienvenue à Montréal." To land in Canada's secondlargest city from an overseas or U.S. destination means experiencing customs wait times that stretch up to two hours (the worst in the country) and traffic bottlenecks exiting the airport that rival those of a developing country. Almost none of this is the fault of Aéroports de Montréal (ADM), the non-profit authority that runs Pierre Elliott Trudeau International Airport under a longterm lease from the federal government. ADM does the best it can, with limited financial resources and no control over customs or highways. But while the management model Ottawa adopted for Canada's airports more than two decades ago has been a good deal for the federal government, it's clearly not working for Montreal. (…) Montreal's business leaders have had enough. This month, a group led by ADM chief executive officer James Cherry and Montreal Board of Trade president Michel Leblanc wrote an open letter to **Public Security Minister Ralph Goodale** to complain about the CBSA's foot-dragging. "The higher traffic levels that Montreal-Trudeau has experienced this summer are not a surprise," they said, noting that the arrival of new carriers and expanded seasonal schedules of other airlines was known by CBSA well in advance. "The customs wait times ... are unacceptable and tarnish Montreal's image as a [global] metropolis." Globe and Mail, B4

TOP STORIES / MANCHETTES

Feds warn of potentially crippling 'insider' cyberthreat to key sectors

Federal officials have quietly warned operators of electrical grids, transportation hubs and other key infrastructure of the cyberthreat from insiders who could unleash devastating viruses and cripple systems, internal government notes reveal. Crucial networks that Canadians rely on for everyday needs face a "substantial threat" from rogue employees out to wreak digital havoc, warn the **Public Safety Canada** briefing notes. The insider threat is difficult to detect and can cause real damage." No special hacking skills are required, just a portable memory key loaded with a malicious code. As a result, it is important that organizations have the right security protocols and procedures, "for example by limiting access to systems only to those who genuinely need it." A federal briefing on the insider threat was delivered last December to leaders of the 10 most crucial infrastructure sectors, the notes say. They point out that over 90 per cent of critical infrastructure key to delivering everything from food and clean water to banking and health services is controlled by the private sector and all of it is dependent in one way or another on information technology to operate. Many critical infrastructure sectors are interdependent, meaning a problem in one could have a "cascading impact" in others. The notes, prepared earlier this year for Monik Beauregard, a senior assistant deputy minister at **Public Safety Canada**, were obtained by The Canadian Press under the Access to Information Act. Beauregard is chairing a panel today on the global implications of the challenges to cybersecurity at an intelligence conference in Ottawa. In addition, Greta Bossenmaier, the head of Canada's electronic spy agency, the Communications Security Establishment, plans to discuss the various cyberchallenges the country faces. The conference comes as the Liberal government undertakes a cybersecurity consultation that runs through mid-October. The overall aim is to identify gaps and opportunities, bring forward ideas to shape a renewed approach and capitalize on the advantages of new technology. Canadian Press (Guardian, Telegram, Cape Breton Post, CTV News, Global News)

Correctional service admits 'staff misconduct' in inmate's death

Correctional Service Canada has fired one staff member and disciplined three others after an inmate was beaten and repeatedly pepper-sprayed at a New Brunswick prison before his death. The top correctional official in Atlantic Canada admits there was "staff misconduct" and "excessive force" in the case of Matthew Hines, who died in hospital on May 27, 2015 - less than two hours after his struggle with guards at Dorchester Penitentiary began. "We take this case very seriously and we're trying to learn from it," Scott Harris, regional deputy commissioner for the Atlantic region, said in an interview. CBC News has also learned that RCMP have reopened the criminal investigation into Hines's death, after saying last month their investigation was finished and foul play had been ruled out. But "additional information" has since come to the RCMP's attention, prompting police to "re-examine" the case, according to Const. Hans Ouellette, a spokesman for the New Brunswick RCMP. He wouldn't say when the investigation was reopened or what kind of new information police received. The details of Hines's death were secret until last month, when CBC News revealed the quick escalation of force used against the 33-year-old Cape Breton man after he refused to return to his cell. Minutes after his struggle with guards began, Hines was hit and then pepper-sprayed five times - including four times in less than one minute. CBC News

'Very active investigation'
A small army of police officers is working to track the person or persons responsible for a bomb threat to Island schools now deemed not to have been a credible threat. RCMP Staff Sgt. Kevin Baillie says the police agency's entire provincial major crime unit has joined forces with members of the RCMP's federal investigation unit. Collaboration is also taking place with other jurisdictions that had similar threats made against schools in Winnipeg, Newfoundland and Nova Scotia on Wednesday and in Nunavut on Thursday. "We have a very active investigation that is continuing now, following up a couple of leads," says Baillie. When pressed on the leads, however, Baillie conceded police have not had any success in determining the origin or author of a fax threatening bombs in multiple P.E.I. schools would be detonated Wednesday. "We'd love to have a tip - someone to call in," he says. Between 50 and 60 RCMP officers were involved in the investigation Wednesday. (…) Baillie says the RCMP will review procedures in the next day or two to assess how police handled the bomb threat. He notes there is "nothing glaring" to him that was not done well on the RCMP's end. The Guardian, A1, 1, 2

Tackling potential danger
School officials in four Canadian provinces all received similar bomb threats this week, but each responded to the potential danger differently. Universities and schools across Prince Edward Island were evacuated Wednesday morning after **police** received a fax from someone threatening to detonate bombs at several schools. Three colleges in Nova Scotia were also evacuated after receiving threats. Hours later, a school board in Winnipeg received a similar bomb threat, but no schools were evacuated. And on Thursday, schools in three regions of Nunavut were closed due to a bomb threat, but reopened after lunch. "Assessing a bomb threat is very, very difficult," said Chris Mathers, a Toronto-based crime and risk consultant. "You can't examine a bomb threat in a vacuum." Mathers said a number of factors are considered when assessing the credibility of a bomb threat, including the frequency of the threats and whether similar threats have made. "If you're getting a bomb threat every day, eventually someone had to make a decision not to act out as the person making the threats wants them to," said Mathers. "And typically, serious bombers don't call it in." But he said with minimal information available, many officials would err on the side of caution, as was the case in P.E.I. P.E.I. RCMP StaffSgt. Kevin Baillie said when the threat was received Wednesday, police didn't have enough information to determine whether the threat was credible or not. Edmonton Sun, A67

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Déversement de pétrole : des excédents d'hydrocarbures demeurent dans la rivière Saskatchewan Nord**
Trois mois après un déversement de pétrole de la compagnie Husky Energy dans la rivière Saskatchewan Nord, l'Agence de la sécurité de l'eau de la province signale encore des excédents d'hydrocarbures dans la région de North Battleford et de Prince Albert. Dans une mise à jour publiée jeudi, elle note toutefois que ces niveaux ne sont pas nuisibles à la consommation d'eau courante ou pour les plantes. L'Agence affirme qu'elle se base sur l'analyse de 229 échantillons d'eau et de 4

échantillons de mousse. Vingt-deux échantillons démontrent la présence d'hydrocarbure dans des sédiments de 9 localités. Environ 200 000 litres de pétrole se sont retrouvés dans la rivière Saskatchewan Nord en juillet. L'Agence assure qu'elle continuera d'évaluer la qualité de l'eau et l'état des sédiments jusqu'au mois d'octobre. Elle indique qu'elle étudiera les effets du pétrole sur les sédiments dans plusieurs régions. Radio-Canada (2016-09-22)

*** North Battleford's incoming mayor faces no competition for tough job**
No one but Ryan Bater wants to be mayor of North Battleford, a city beset by an oil spill, racial tension and Canada's worst crime rate. On top of that, residents have been engaged in a heated debate over whether to amalgamate with the adjacent town of Battleford. "We definitely have issues to overcome," Bater said in an interview Thursday. When the nomination deadline passed this week, the former Liberal Party of Saskatchewan leader was the only one who had filed papers. It appeared current North Battleford Mayor Ian Hamilton was preparing for another campaign, but the incumbent pulled out a couple of weeks ago. In Saskatoon and Prince Albert, four candidates are vying for the mayor's chair. Regina and Moose Jaw each have five contenders. In all four cities, mayoral incumbents are seeking re-election. Bater, 38, said he planned to run for another term as a city councillor, but Hamilton's withdrawl "left a leadership void." City councillors and other others talked among themselves, several encouraged him to take on the job, and he agreed, he said... On July 20, the Husky oil spill forced North Battleford to shut off its main drinking water intake in the North Saskatchewan River and use alternate sources. An outpouring of hatred on social media and among some Battlefords-area residents followed the Aug. 9 killing of Red Pheasant Cree Nation man Colten Boushie on a nearby farm. Hundreds attended rallies outside the court appearances of the alleged murderer. North Battleford also currently ranks first on a national crime severity index. Bater said the oil spill was unfortunate, but Husky and the provincial government have treated North Battleford fairly. He said the new council will be watching closely to ensure more safeguards are put in place to prevent future spills. Leader-Post, A11

*** Rescuers pluck 15 from water in mock disaster**
Canadian and American coast guard personnel and their auxiliaries enjoyed a great Thursday morning on Passamaquoddy Bay. About 50 personnel, including volunteer 'survivors', took part in a joint search and rescue exercise, training together to respond to a real marine emergency in these international waters. The scenario: a vessel sinks following an on-board explosion. Mass casualties in the water and on life rafts, some injured, others deceased, conflicting accounts from the survivors. Vessels and crew taking part gathered for a briefing at the coast guard headquarters in Eastport, Maine. Phil Walker, Canadian Coast Guard rigid hull inflatable training (RHIOT) co-ordinator in Dartmouth, N.S., captained the media boat which left and eventually returned to the St. Andrews Biological Station wharf. His passengers included two volunteers who, when the time came, donned flotation suits and jumped overboard to play their roles as survivors awaiting rescue. Other survivors took their stations in orange life rafts. The crew on the rescue craft used the clues they got at the briefing in Eastport to find these orange dots in the water among the islands and rocks in the bay - hard enough on a calm day with a cloudless blue sky like this one, but next to impossible in more typically choppy water, in a storm, after dark and freezing cold. Survival suits, personal flotation devices, life rafts and other safety gear are bright orange for a reason, said Dave Griffiths, rescue specialist co-ordinator with the Canadian Coast Guard in Dartmouth. Telegraph-Journal, B5

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Li defends use of death penalty while pushing extradition pact
Chinese Premier Li Keqiang publicly defended the death penalty as he pressed Prime Minister Justin Trudeau to sign a formal extradition treaty while denying agents are covertly dispatched to Canada to

intimidate Chinese fugitives to return home. Mr. Li, the first Chinese leader to visit Canada in six years, is on a mission to forge closer ties. That included announcements to start exploratory talks on free trade, the settling of a canola dispute and pledges to double trade by 2025. (…) The Globe and Mail reported Wednesday that the Canadian Security Intelligence Service and RCMP are investigating the covert Chinese spy operation. CSIS has interviewed Chinese citizens living in Canada, all of whom have been threatened by agents from China. "I don't know where you got those reports," Mr. Li said when asked about The Globe report. "I can tell you firmly that China ... strictly follows international law and norms and we obey the laws of other countries." The Prime Minister said Canada would not deport anyone who would face execution but argued he was confident a formal extradition treaty could be worked out. Globe and Mail, A1; * Presse canadienne (Acadie-Nouvelle, Le Droit); * Le Devoir; * Agence QMI (Journal de Montréal, Journal de Québec)

* **Extradite to China**

A letter to the editor states, "Re Trudeau Defends Extradition Treaty Talks (Sept. 22): As Canadians watch a new relationship with China unfurl and our Prime Minister eagerly meets with Chinese leaders, it's worth glancing away from the big picture and focusing on smaller, often disturbing facts. CSIS has identified China as a country that spies on Canada in search of scientific, technological and economic information. China is doing irreparable environmental damage through widespread pollution. And human rights in China are - as Amnesty International, Human Rights Watch and others point out - literally brutal. Despite this, China is being encouraged to play a leading role in the development of the massive mineral-rich "Ring of Fire" region of Northern Ontario. We look the other way when it comes to questionable Chinese investment in real estate. And we thank leaders from the Middle Kingdom when they release a Canadian coffee shop owner and humanitarian imprisoned for two years on trumped-up charges (laid, it should be noted, in wake of the arrest of Su Bin in Vancouver on charges of stealing U.S. military secrets to sell to the Chinese). Justin Trudeau approaches China as a "friend" of Canada. Truth be told, any new Canada-China relationship will be complicated and based on economic convenience, not real friendship." Globe and Mail, A12

Monsef faces calls to step aside

Federal cabinet minister Maryam Monsef says she was shocked to find out she was born in Iran - not Afghanistan - but political opponents in her riding are challenging her claim and alleging her true birth country has "been known for quite awhile." Yet, one of Monsef 's first cousins said Thursday that he and his immediate family members weren't aware that she was born in Iran, and while a "shock" to them, it "is not a big deal." Monsef is also facing calls from a Conservative leadership contender to consider stepping aside from cabinet while an investigation can be completed. (…) Tony Clement said Thursday an investigation is required to confirm Monsef 's explanation of events, how the birthplace mix-up was missed by the federal security vetting and whether citizenship laws were violated. He also said Monsef "should consider seriously stepping aside if there is going to be an investigation." Incoming cabinet ministers go through a "rigorous vetting process," the Privy Council Office (PCO) said in a statement Thursday. It includes criminal background checks by the RCMP and by the Canada Revenue Agency for bankruptcies or financial insolvencies. The Canadian Security Intelligence Service (CSIS) does automated record checks of its databases for what's called "adverse intelligence traces" related to non-criminal matters from espionage to terrorism and subversion. The service will typically ask allied security intelligence agencies to check names against their databases, as well. But CSIS can only go so far, especially in such places as Afghanistan and Iran, where there are either no government records or reliable government agencies on which to rely and where the fog of war lingers. Postmedia Network (Leader-Post, N1, Windsor Star, National Post, Vancouver Sun, StarPhoenix, Montreal Gazette, Ottawa Citizen, Edmonton Journal, Calgary Herald, London Free Press); * Canadian Press (Times & Transcript); * Globe and Mail, A7

* **Edmonton notary public stripped of appointment**

An Edmonton notary public who was chastised for aiding the efforts of a selfproclaimed Freeman on the Land by a top Alberta judge is no longer a notary public, Alberta Justice confirmed Thursday. Edward J. Powell was named in Court of Queen's Bench Associate Chief Justice John Rooke's 2015 decision that restricts self-described Freeman on the Land Allen Boisjoli's ability to access Alberta courts. The scathing decision in which Rooke labelled Boisjoli, 45, a "vexatious litigant" was in reaction to Boisjoli's attempt to

subvert the legal process by filing a default judgment using his own forms to get out of paying a traffic ticket. Powell notarized those documents. On Wednesday, Edmonton police announced that Boisjoli is facing a criminal charge of intimidation of a justice system participant as a result of his alleged act of "paper terrorism" against the peace officer, which included a claim that the officer was liable to Boisjoli for $225,000. Notaries public perform a variety of functions, usually to do with the production and certification of official documents, as well as administering oaths and taking affidavits, affirmations or declarations. Postmedia Network (Edmonton Sun, A7, Edmonton Journal)

*** Hollywood gets it right on Snowden**

An opinion pieces states, "There is a moment in Oliver Stone's new biopic when Edward Snowden, the National Security Agency (NSA) leaker, distracted by a pre-dinner discussion with girlfriend Lindsay Mills, dashes to the stove where he has left the pasta. Testing the dangling fettuccine, he declares it as close to correctly cooked as he's managed. Whatever the film critics make of the Snowden docudrama, it, too, may come as close to correctly rendered as Hollywood can manage. If you want to understand the serious computer geek who dared defy the NSA and, indeed, the entire U.S. government, Stone gets it about right. (…) Though we might not express things in exactly the same way, many Canadians are also leery of some government activities. They're not being unpatriotic; it's an expression of the desire to see Canada flourish. Many, too, are concerned about the uncomfortably close relationship between the NSA and our own Communications Security Establishment (CSE), and about specific ways that the Anti-terrorism Act (Bill C-51) facilitates just such suspicionless surveillance (that is, placing under surveillance persons to whom are attached no already-existing suspicions) - based on "big data," as seen in the NSA. Films such as Snowden should be a spur to pressuring security agencies to more transparency and accountability. The current government's proposals for new oversight mechanisms are a solid start. This does not mean governments should abandon all surveillance, as the movie also makes clear. It means querying the idea that metadata - details such as the times, places and duration of communication between identifiable persons - is merely "like a phone book," or that oldfashioned labour-intensive sleuthing can be abandoned in favour of flashy new solutions involving big data. Equally, the Snowden biopic may inspire efforts to demystify the arcane algorithms that guide the security surveillance systems to their persons of interest. The film hints helpfully at ways these algorithms are far from the neutral instruments they may be sold as - when in fact they're shaped politically." Ottawa Citizen, A9

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Report urges Canada to end jailing of child migrants

A new report by human-rights researchers urges Canada to urgently find alternatives to locking up child migrants, saying the practice has a harmful and lasting effect on already vulnerable newcomers. Canada has held hundreds of children - including some from Syria and other war-torn regions - in immigration detention in recent years in violation of global legal obligations, says the report by the University of Toronto's international human-rights program. Researchers released the report, No Life for a Child, at a news conference Thursday. The Canada Border Services Agency holds newcomers who are considered a flight risk or a danger to the public and those whose identities cannot be confirmed. An average of 242 children were detained annually between 2010 and 2014, the report says. But it cautions the figure is actually higher, because it excludes those not subject to a detention order but who were held because their parents were in custody. Children are generally kept in federal immigration holding centres in Toronto and Laval, Que., facilities that are designed for long-term stays. Those facilities resemble medium-security prisons, with little privacy or freedom of movement, inadequate access to education and poor nutrition and recreation, the report says. Globe and Mail, A5; *Yahoo News; * RT

Province's sole super sniffer retires from service with her tail held high

Holly has hung up her collar after nine years of service with Canada Border Services Agency. "We're happy for her to be retiring but it's also just a bittersweet time because she was very well loved in the community and a great, excellent detector dog," said Luke Reimer, communications officer with CBSA. Aug. 12 was Holly's last day of work, based out of the North Portal crossing with her handler. "The detector dogs help by reducing labour intensive searches, by cutting down the time it takes to search through a large shipment by using noses. And that helps to improve the service for travellers for the time

needed to screen or examine passengers or luggage," Reimer said. During Holly's career she was involved in 216 seizure actions and was trained to sniff out guns and drugs all across Saskatchewan. Holly was a bright dog. She participated multiple times in the annual Canadian Police Canine Association Trials, placing first three years in a row and as runnerup twice. "It just goes to show that she was a great detector dog and it really shows the CBSA detector dog service program," Reimer said. Holly was the only detector dog based in Saskatchewan. She would travel back and forth along the American border and to nonland ports, wherever needed. Postmedia Network (Starphoenix, A9, Leader-Post)

* **Milk Throwing in Cornwall Ontario CCPS Police Blotter**
Stephen Kuno, age 55, of Potsdam, NY, was arrested on September 21, 2016. He was apprehended by Canada Border Service Agency this date for attempting to enter the country with a firearm in his vehicle. Cornwall Police were contacted and an investigation was conducted. He was subsequently charged with Unauthorized Importing of a Firearm, Possession of a Prohibited Firearm, and Careless Storage of a Firearm. He was released to appear in court on October 25, 2016. Cornwall Free Press

* **Sick woman who didn't know of citizenship issue faces deportation:advocacy group**
An advocacy group for female inmates says it is concerned about that the Canada Border Services Agency is attempting to deport a Halifax woman in serious medical distress. The Elizabeth Fry Society says a hearing will be held by the Immigration and Refugee Board of Canada today at the Dartmouth General Hospital for Fliss Cramman. The society says in a news release the Canada Border Services Agency is moving to deport the woman later this fall, three months after her hospitalization for a perforated colon. The group says that would run against her doctor's advice and despite ongoing critical health concerns. t says the woman was born in England, but was brought to Canada when she was eight years old and was unaware of her citizenship issues until she was jailed for drug offences two years ago. The society says Cramman doesn't pose a threat to public safety, has Canadian children, and has worked and paid taxes to the Canadian government. A spokeswoman for the Canada Border Services Agency was not immediately available for comment. Canadian Press (Metro)

* **Push on for bikes on tunnel buses**
Transit Windsor is taking steps to allow bikes to be transported for the first time on its tunnel buses heading into Detroit. Final approval by city council, likely to occur on Oct. 3, is the next step for Transit Windsor to proceed with an application to the Ontario Ministry of Transportation to carry bikes through the Detroit-Windsor tunnel, said Carolyn Brown, the city's corporate leader of transportation. All municipal buses are already equipped with bike racks, but the transportation ministry's permission is required to allow bikes to travel attached to the front of the bus through the border crossing, she said. "It's subject to council approval, then it will be a standard application to the ministry," Brown said. "They review it, we pay a small fee and we should be good to go." She could not provide exact timelines on when cyclists will officially be allowed to bring their bikes with them on the tunnel bus at the local border crossing. But customs authorities on both sides of the border are fine if tunnel bus passengers bring along their bikes, Brown said. (…) The move comes just months after a June 8 episode when Windsor resident Kyle Colasanti, 24, gambled he could successfully ride through the tunnel into Detroit on his own bike in order to see a downtown Steely Dan music concert. After extensive questioning by U.S. customs, Colasanti was allowed entry into Detroit, but he later conceded his decision was a bit foolish. Riding a bike through the tunnel or over the Ambassador Bridge is illegal. Windsor Star, A5

* **Canada-U.S. border crossing bridge in Rainy River, Ontario to be replaced**
A highway bridge connecting northwestern Ontario with northern Minnesota is slated to be replaced in the next few years, raising hopes that it will be easier to transport large cargo across the Canada-U.S. border.The bilateral project between Ontario's Ministry of Transportation and Minnesota's Department of Transportation is expected to replace the bridge between Rainy River, Ont., and Baudette, Minn., - a bridge that represents more than just an access point between the two communities."There's relationships, there's marriages, there's families living on both sides [of the border]," said Rainy River Coun. Gordon Prost."There's people who work on one side, live on the other side. There's even some education, schooling and stuff going on."Prost, who has also worked as a customs officer at the bridge, added that the old structure - built in 1959 - had some unique characteristics. "When you reach the halfway point, suddenly it was brighter, cleaner paint, and it was in nicer condition," he said. "So, you

knew when you were going from one country to the other."Prost added that "the Ontario side was the nicer side."The bridge is being replaced to conform with new maintenance standards in Minnesota and calls for the new structure to be built south of the existing bridge.The new bridge is expected to do away with the overhead structure present on the current one, meaning that larger and heavier loads will potentially be able to cross the expanse. Currently, it can be difficult to get large items into the area as there also restrictions on the bridges in Sioux Narrows and Fort Frances, Ontario. CBC News

Suited for the needs of the community
Deep in Manitoba's Bible Belt, the small cities of Winkler and Morden have drawn so many immigrants recently that newcomers are helping create new places of worship. There are now more than 25 churches in Winkler, up from 18 at the turn of the millennium. Immigrants are flocking to these cities in the Pembina Valley for two main reasons: quality of life and jobs. But driving through their quiet streets, a visitor wouldn't know the booming companies on the outskirts of both communities manufacture everything from down jackets to model homes. (…)Both cities and the surrounding region have grown by more than 3,000 people since, in great part to immigration programs. As their populations age and young adults move away, small cities and towns across Canada are increasingly looking to immigration to rejuvenate their workforce and expand their tax base. (…)More often than not, employers, immigration consultants or city officials from the region travel abroad to meet prospective immigrants, interview them on Skype or invite them for a visit to make sure they are a good fit. The criteria for selecting newcomers is often the opposite of those used by the federal immigration system. At times, the two cities have favoured community connections over Canada's points-based metrics or sought out people who didn't speak English. Notably, many of the people they pick probably wouldn't have made it into Canada without them.(…)Many immigrants who go to the Maritimes leave within a year of their arrival. In July, the Atlantic provinces and the federal government jointly announced a three-year pilot project to boost immigration as part of an economic growth strategy, taking in an additional 2,000 immigrants and their families in 2017. But those working to boost immigration to small cities and towns lament that the system is geared against them. Postmedia Network (Edmonton Journal, N2, Calgary Herald, London Free Press, Vancouver Sun, Starphoenix, Leader-Post, Windsor Star, Montreal Gazette, Ottawa Citizen)

* **Let's treat temporary foreign workers better**
An editorial states, “As successive federal governments wrestle with the controversial temporary foreign worker program, let’s not lose sight of one thing — the employees themselves. Employers in several sectors, such as agriculture and hospitality, depend on the program to keep their doors open. They need foreign workers to occupy positions that can’t be filled by Canadians — either because they don’t have the specialized knowledge or they don’t want to perform the menial work. Earlier this week, a parliamentary committee released a review of the program. The report invites attention to a year-long Calgary Herald investigation by Alia Dharssi, this year’s recipient of the Michelle Lang Fellowship in memory of the reporter killed while covering the conflict in Afghanistan. The final segment of Dharssi’s six-part series appears in today’s edition.The government, to the greatest extent possible, should stop the abuse of foreign workers by predatory recruiters who gouge applicants. Dharssi’s investigation found that many workers paid between $2,000 and $10,000 for access to a low-paid position and, even then, often faced mistreatment by their recruiters. Employers have also been involved in shady dealings.” Calgary Herald

Eurocracy not welcome here
An opinion piece states, “The European Union doesn't just want Canadian products and services in negotiating a Comprehensive Economic Trade Agreement (CETA) with us. It also wants our sovereignty and our soul. Canada should walk away from CETA, a deal scheduled to be signed at the Canada-EU summit in Brussels on Oct. 27. Otherwise, we may lose not just our Canadian character in pursuing this deal; we may also lose much of our economy. The EU's approach to trade has always been about more than lowering tariffs and ending quotas - it doesn't simply want an FTA (freetrade agreement), it wants a "comprehensive" trade agreement. The EU sees trade as a mechanism through which its political goals can be met. That's why it still insists that its trading partners agree to everything from welfare policies to open borders - it even demands this of the U.K. in any new trade deal that Britain strikes after it leaves the EU. For a while, it seemed that CETA would break the EU's mould in its deal with Canada, that the EU would not in the end insist on making Canada accept the type of political strings that it forced on

Switzerland and other European trading partners. But now, after a marathon, seven-year-long-and-running negotiation that seemingly resolved money matters - dairy quotas, intellectual property rights, investor protections - the EU's negotiating focus has turned to its social agenda." National Post, FP7; iPolitics

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Feds warn of potentially crippling 'insider' cyberthreat to key sectors
Federal officials have quietly warned operators of electrical grids, transportation hubs and other key infrastructure of the cyberthreat from insiders who could unleash devastating viruses and cripple systems, internal government notes reveal. Crucial networks that Canadians rely on for everyday needs face a "substantial threat" from rogue employees out to wreak digital havoc, warn the **Public Safety Canada** briefing notes. The insider threat is difficult to detect and can cause real damage." No special hacking skills are required, just a portable memory key loaded with a malicious code. As a result, it is important that organizations have the right security protocols and procedures, "for example by limiting access to systems only to those who genuinely need it." A federal briefing on the insider threat was delivered last December to leaders of the 10 most crucial infrastructure sectors, the notes say. They point out that over 90 per cent of critical infrastructure key to delivering everything from food and clean water to banking and health services is controlled by the private sector and all of it is dependent in one way or another on information technology to operate. Many critical infrastructure sectors are interdependent, meaning a problem in one could have a "cascading impact" in others. The notes, prepared earlier this year for Monik Beauregard, a senior assistant deputy minister at **Public Safety Canada**, were obtained by The Canadian Press under the Access to Information Act. Beauregard is chairing a panel today on the global implications of the challenges to cybersecurity at an intelligence conference in Ottawa. In addition, Greta Bossenmaier, the head of Canada's electronic spy agency, the Communications Security Establishment, plans to discuss the various cyberchallenges the country faces. The conference comes as the Liberal government undertakes a cybersecurity consultation that runs through mid-October. The overall aim is to identify gaps and opportunities, bring forward ideas to shape a renewed approach and capitalize on the advantages of new technology. Canadian Press (Guardian, Telegram, Cape Breton Post, CTV News, Global News)

* **Yahoo hack steals personal info from at least 500 million accounts**
Computer hackers swiped personal information from at least 500 million Yahoo accounts in what is believed to be the biggest digital break-in at an email provider. The massive security breakdown disclosed Thursday poses new headaches for beleaguered Yahoo CEO Marissa Mayer as she scrambles to close a $4.8 billion sale to Verizon. The breach dates back to late 2014, raising questions about the checks and balances within Yahoo -- a fallen internet star that has been laying off staff and trimming expenses to counter a steep drop in revenue during the past eight years. At the time of the break-in, Yahoo's security team was led by Alex Stamos, a respected industry executive who left last year to take a similar job at Facebook. Associated Press (Chronicle-Herald; Red Deer Advocate; St. John's Telegram; Toronto Sun); Le Soleil; Bloomberg (Ottawa Citizen); USA Today (Waterloo Region Record); National Post

LAW ENFORCEMENT / APPLICATION DE LA LOI

'Very active investigation'
A small army of police officers is working to track the person or persons responsible for a bomb threat to Island schools now deemed not to have been a credible threat. RCMP Staff Sgt. Kevin Baillie says the police agency's entire provincial major crime unit has joined forces with members of the RCMP's federal investigation unit. Collaboration is also taking place with other jurisdictions that had similar threats made against schools in Winnipeg, Newfoundland and Nova Scotia on Wednesday and in Nunavut on Thursday. "We have a very active investigation that is continuing now, following up a couple of leads," says Baillie. When pressed on the leads, however, Baillie conceded police have not had any success in determining the origin or author of a fax threatening bombs in multiple P.E.I. schools would be detonated

Wednesday. "We'd love to have a tip - someone to call in," he says. Between 50 and 60 RCMP officers were involved in the investigation Wednesday. (…) Baillie says the RCMP will review procedures in the next day or two to assess how police handled the bomb threat. He notes there is "nothing glaring" to him that was not done well on the RCMP's end. The Guardian, A1, 1; Cape Breton Post (The Guardian); * Globe and Mail

*** Nunavut minister praises police, schools for swift response to bomb scare**
While few people believed the Sept. 22 bomb threats against Nunavut's 43 schools held much weight, officials were more than happy to confirm the territory is safe from harm. Just before 9 a.m. that day, Education Minister Paul Quassa received a phone call and a copy of a fax sent to police, claiming bombs had been placed in schools in all three regions of the territory. "We've seen bomb threats here in Iqaluit [schools], but this is first time there's been a bomb threat made in all of our schools," Quassa said. By the time he made contact with senior education officials—many of whom were in Iqaluit for meetings—classes had already started for the day in schools through the Qikiqtani region. (…) The RCMP's response was equally fast; Quassa said police across Nunavut were able to sweep through schools that morning, determining by noon that the bomb threats were unfounded. "We take this kind of threat very seriously, even though we are very isolated from the rest of Canada," he said. "It was a relief to hear there was nothing serious." But as police cleared the territory's schools to re-open the afternoon of Sept. 22, the RCMP were responding to another scare, this time directed at southbound flights preparing to depart Iqaluit's airport. Police were seen sweeping at least one Ottawa-bound jet before the aircraft was cleared for take-off and the threat was also found to be non-credible. Now Nunavut RCMP said it's working with other agencies across the country to track who is responsible for the false threats faxed to Nunavut and other provinces this week. Nunatsiaq Online

Tackling potential danger
School officials in four Canadian provinces all received similar bomb threats this week, but each responded to the potential danger differently. Universities and schools across Prince Edward Island were evacuated Wednesday morning after **police** received a fax from someone threatening to detonate bombs at several schools. Three colleges in Nova Scotia were also evacuated after receiving threats. Hours later, a school board in Winnipeg received a similar bomb threat, but no schools were evacuated. And on Thursday, schools in three regions of Nunavut were closed due to a bomb threat, but reopened after lunch. "Assessing a bomb threat is very, very difficult," said Chris Mathers, a Toronto-based crime and risk consultant. "You can't examine a bomb threat in a vacuum." Mathers said a number of factors are considered when assessing the credibility of a bomb threat, including the frequency of the threats and whether similar threats have made. "If you're getting a bomb threat every day, eventually someone had to make a decision not to act out as the person making the threats wants them to," said Mathers. "And typically, serious bombers don't call it in." But he said with minimal information available, many officials would err on the side of caution, as was the case in P.E.I. P.E.I. RCMP StaffSgt. Kevin Baillie said when the threat was received Wednesday, police didn't have enough information to determine whether the threat was credible or not. Edmonton Sun, A67 (Chronicle Herald, Times & Transcript)

*** RCMP binocular purchase collapses amid allegations bid rigged in favour of one company**
What should have been a straightforward purchase of binoculars for the RCMP has gone off the rails after it emerged the deal was rigged to favour one particular company. A government watchdog has recommended the entire process be restarted, but this time in an open, fair and transparent manner - which amounts to yet another blow for the troubled federal government procurement system. The March 2016 purchase spiralled out of control, say industry representatives, after it became apparent that the requirements were geared toward one particular firm. One company refused to bid as a result. Another, MD Charlton Co., one of Canada's top police-equipment suppliers, raised objections that the purchase favoured a particular firm, which has not been named. The MD Charlton complaint was met with silence: federal officials refused to answer any questions about the purchase, according to an investigation by the Canadian International Trade Tribunal (CITT), the government watchdog. Then Public Services and Procurement Canada took the highly unusual step of trying to force MD Charlton to destroy a copy of the binocular specifications it had received - a key document the firm needed to prove the purchase was being rigged. (…) Industry representatives warned the government about the proposed purchase, shortly after the RCMP issued the call for equipment this year. The RCMP invoked a national security exemption

for the purchase of the night-vision binoculars, meaning that regular rules governing federal procurement didn't apply. It claimed the exemption was needed so criminals and terrorists wouldn't learn the technical specifications of the binoculars. The request was then sent to a pre-determined list of three potential bidders. Postmedia News (National Post)

Pictou revenge porn thread back online
The revenge-porn thread on a Russian-based pornography site that featured private photos of Pictou County women is back up again, just two days after being taken down. Girls of Pictou County was back online Thursday but no photos had been posted yet, said Kayde Stanley, the woman who waged a public campaign this week against the website's unauthorized use of intimate images. "It's disheartening, sad and unbelievable with everything going on," she said. "There is a post today requesting (photos of) specific girls." Stanley made the site public on social media earlier this week after someone told her there was a post about her. It was filled with photos of local women who did not consent to having their private photos shared. The thread had a note urging users to only post photos of people who consented, otherwise the RCMP would be involved. (...) Stanley said she was going to meet with the RCMP late Thursday to bring them information about the women she's spoken to this week. She said at least five of the women featured on the thread want law enforcement involved. "But there are at least seven women we were able to identify I haven't spoken to." Chronicle Herald, A1

* **U.S. alleges Vancouver firm laundered money on 'transnational' scale**
The U.S. government has named a little-known Vancouver financial company as a "significant transnational criminal organization" that it alleges has worked for 20 years with "direct mailer" scammers to launder hundreds of millions of dollars defrauded from millions of vulnerable victims. In a news conference on Thursday, U.S. Attorney General Loretta Lynch named PacNet, a company with offices in a building in downtown Vancouver, as a financial linchpin in global money laundering. PacNet was the payment processor - a sort of banking system middleman - that allowed global criminals to deposit cheques scammed from mostly elderly victims, Lynch alleged. "The schemes involve a complicated web of actors located across the world," she said. And in a stunning financial order that points to Vancouver's growing reputation as a hub for global money laundering, the U.S. government put PacNet on an international short list of about seven organizations that includes several of the world's most dangerous criminal cartels, including Las Zetas from Mexico and the Camorra from Italy. (...) Vancouver police spokesman Sgt. Brian Montague said Thursday in an email: "We do have good relationships with other law enforcement agencies in both Canada and the U.S., but unfortunately I am not able to share any information about investigations unless criminal charges are laid - so not able to confirm if there has been or there is any investigation by the VPD." B.C. RCMP spokesman Staff Sgt. Rob Vermeulen said Thursday afternoon that any comment on the matter would have to come from the force's national headquarters in Ottawa. Vancouver Sun

* **T.-N.-L.: L'association de la police provinciale veut que toutes les enquêtes sur la mort de Don Dunphy soient publiques**
Seules des bribes de l'enquête de la GRC sur la mort de Don Dunphy, abattu par un policier en 2015 ont été partagées, la semaine dernière. L'association qui représente les policiers de la Force constabulaire royale à Terre-Neuve et Labrador souhaite mettre fin aux hypothèses, en rendant toutes les enquêtes publiques. Don Dunphy a été abattu en 2015 dans sa résidence. L'association de la Force constabulaire royale soutient que le dévoilement incomplet des enquêtes alimente trop de spéculation au sein du public. Le policier qui a tiré les coups de feu mortels, l'agent Joe Smyth, faisait partie de l'équipe responsable de la protection du premier ministre, Paul Davis, à l'époque. La GRC a affirmé la semaine dernière qu'aucune accusation ne sera portée et que le policier n'a fait qu'employer la force nécessaire pour se défendre. Une enquête sur l'incident a également été menée par une unité d'enquêtes indépendantes de l'Alberta et par la police de Saskatoon. Le gouvernement provincial a lui aussi promis une enquête publique dès que possible. Radio-Canada; Times & Transcript, B4

Hillsborough man accused of ramming police car
A Hillsborough man is in custody on accusations he rammed a RCMP cruiser while officers were attempting to arrest him. Arthur Barry Russell appeared in provincial court Thursday and several charges were laid against him relating to an incident that occurred Wednesday afternoon in the Hillsborough area.

The Crown objected to his release and his bail hearing was set for Monday. Russell is charged with operating a motor vehicle on streets and trails in and around Hillsborough in a manner dangerous to the public, assaulting Cpl. Dan Poirier and Const. Matthew Beaulieu while threatening to use a vehicle as a weapon, failing to stop for police in an attempt to evade them and several breaches of probation. Times & Transcript, A3

Fake $100 bills passed in Sooke
Sooke RCMP are warning the public about counterfeit currency, after investigating five complaints from area businesses in the past month about phoney $100 bills. The circumstances of how the bills were passed are unknown because they weren't discovered until the businesses made their bank deposits, police said. The counterfeit bills have been created to look like ones in the new polymer series. Times Colonist, A4

*** Police cruiser set ablaze in B.C.**
A witness told Creston RCMP that they watched a man pour something on the police car and then threw a lit bottle on the car. The vehicle was parked in the RCMP detachment parking lot. After setting the vehicle on fire, the witness told officers that the man drove away. His vehicle description and the license plate was written down by the witness. The vehicle suffered damage to the rear area and trunk lid. Surrounding area police units were told about the incident and were provided with the vehicle description. An officer with the RCMP East Kootenay Traffic Services was in the Creston area and spotted the suspect vehicle just South of Moyie. Kelowna Now (2016-09-22)

Three arrested in bust at Medstead grow-op
RCMP say a grow-op bust last week in the RM of Medstead led to the largest seizure of marijuana in the province this year. Officers executed a search warrant at 11:20 a.m. on Sept. 16 in the Rural Municipality of Medstead, and found a "sophisticated" grow op, according to a news release issued Thursday. Officers seized about 700 marijuana plants, 2.3 kilograms of packaged pot and more than $6,000 cash, the release said. A 44-year-old man and a 34-year-old woman from the RM of Medstead were arrested alongside a 43-year-old man from Ontario. All three are charged with producing marijuana, possession of marijuana for trafficking and possession of property obtained by crime. Firearms charges will be laid as the investigation continues, the release said. Postmedia Network (StarPhoenix, A9, Leader-Post)

Tough break
A fleeing suspect suffered a broken clavicle when he was tackled by an RCMP officer in Portage la Prairie earlier this week. Manitoba's Independent Investigation Unit is looking into the case, as is customary when there are serious incidents involving police officers in this province. Officials with the IIU said the incident happened Tuesday morning, when an RCMP constable in Portage tried to pull over a vehicle they believed to be driving erratically. The vehicle turned offthe road and into a ditch, at which point three occupants got out and ran. The IIU said the officer caught one of the suspects "and, in the course of the arrest, both fell to the ground." The suspect complained he didn't feel well after being handcuffed and placed in the police vehicle. He was subsequently checked out at the detachment, then taken to hospital in Portage for X-rays, where the broken clavicle was confirmed. Winnipeg Sun, A6; * Winnipeg Free Press

No leads in Hannah's roadside assault case
It's been three weeks since Hannah was pushed out of the passenger side of a logging truck and left to lie injured and in pain on the side of Highway 101. RCMP told the Chronicle Herald on Thursday they still don't have a suspect. Released from a Nova Scotia hospital this week, Hannah told the Chronicle Herald that she feels she's not being taken seriously. "The RCMP were supposed to be in to see me at the hospital with a sketch artist but that hasn't happened." Hannah said she's afraid as more time goes on she'll remember fewer details of the night a truck driver tried to trade a ride for sex. Cpl. David Fairfax of the Annapolis District RCMP said he understands it can be frustrating waiting for the wheels of justice to turn. "We only have two sketch artists in the country, and the lead investigator on Hannah's case had to be seconded to a major criminal event in the area," he said in an interview. "Sometimes it just comes down to managing resources." Chronicle Herald, A5

*** Bonavista RCMP investigating dumping of needles, diabetic supplies**
The Bonavista RCMP detachment is investigating the dumping of diabetic supplies, including used needles, lancets, safety tabs and test strips in an area off Lance Cove Road in the town. Diabetic supplies, including used needles, lancets, safety tabs and test strips were found in an area off Lance Cove Road in Bonavista Thursday. -- RCMP photo The RCMP said in a news release, officers responded to a call around 5:30 p.m. Thursday regarding used needles dumped in an area frequented by pedestrians, ATV users and pet owners. The needles were dumped sometime Wednesday night or Thursday. The area was cleaned up with volunteer assistance. CBC News

*** Sask. producers look to set up patrol to protect rural properties**
Barry Kidd installed the first security cameras on his farm five years ago after his property was broken into. Now the Rosetown, Sask.-area man sleeps with two guns near his bed as the area continues to deal with crime. "I worked hard for this place to build up the way it is, and I don't want people coming in robbing me. This is my stuff, not theirs," Kidd said. Some producers in the area have shared photos with CBC News of guns they travel with while harvesting, saying it's a precaution due to crime in the area. On Monday, Rosetown RCMP responded to a report of an attempted armed robbery of a farmhand who was allegedly approached by three masked men carrying guns. CBC News

*** TIMBERLEA**
Police in Timberlea are asking the public to be on the lookout for a missing 15-year-old girl. An RCMP news release says Cali Elisabeth Singer was last seen leaving her home in Timberlea Tuesday morning. She never arrived at school that day. Police describe Singer as a biracial female, 5-foot-one and 96 pounds. Chronicle Herald, A4

*** Driving downtown could be royal pain**
Police are advising people planning to drive in downtown Vancouver during the upcoming royal visit to look for alternate routes and allow for longer travel times. William and Catherine, the Duke and Duchess of Cambridge, and their children, Prince George and Princess Charlotte, are set to visit Western Canada Sept. 24 to Oct. 1. They'll be based in Victoria, and will spend time in Vancouver, the Great Bear Rainforest, Bella Bella, Kelowna, Yukon and Haida Gwaii. (…) Neither the Vancouver Police Department, nor the RCMP - which is responsible for providing security for visiting members of the Royal Family - would provide additional information about tour stops, travel times, routes or specifics regarding traffic or street closures, also due to security reasons. The VPD suggested "those travelling near official locations listed as part of the royal visit look at alternate routes and give themselves extra time to get to where they are going, but any traffic disruptions should be minimal." Postmedia Network (The Province, A8, Vancouver Sun)

*** Rural crime a serious issue most don't get**
An editorial states, "This has been another tough week for rural Saskatchewan's image. Maybe a little of it can be blamed on an aging population that's both scared and reacting badly to growing social problems. But maybe the bigger problem is that we haven't bothered to take the time needed to recognize the real problems and their causes. Consider the now-popular Internet image of rifles in combines - all-too-easy confirmation of the East's wrong-headed view of rural western rednecks. One can almost hear the gun-registry advocates hollering: "See, I told you so." (…) After all, can we blame rural people - whether in their farmyards or alone in the field on their combines - for being damn scared after hearing RCMP reports of masked gunmen attempting to hold up people who are isolated from police or other help? Nearly lost in the image of rural Saskatchewan reverting to the Wild West is the less-spectacular story of how an economically challenged part of our country simply isn't getting the government support it needs. Large farms (the long-term result of Canada's cheap food policy) mean farmers are farther apart. In turn, that means huge policing challenges - especially in getting law enforcement to remote critical incidents in a timely manner. A news story by the Leader-Post's Craig Baird on Thursday thoroughly explores the reality of rural crime, and also the even more critical issue of rural RCMP detachment underfunding. (…)Municipalities of fewer than 5,000 people with RCMP detachments pay $77.06 per person, the Leader-Post story noted. Communities without a detachment pay $47.68 per person for policing. Communities can pay for an additional officer position at a detachment (an additional $130,000 per year). But with a rapidly declining rural population, can residents

afford to pay for extra police? Are other Canadians willing to subsidize rural people as much as they should? And then, there is the elephant in the room - why rural Saskatchewan might be more crime-ridden than it used to be." Postmedia Network (StarPhoenix, A12, Leader-Post)

*** Police contempt for public must be arrested**
An editorial states, "It's impossible to know whether the RCMP and RNC's obvious contempt for the public is a feeling returned in kind, but the actions of the Mounties and Constabulary are likely pushing more than a few people in that direction. The long-suffering citizens of Newfoundland may be accustomed to being treated with scorn and disregard by their politicians, but up until recently they surely expected more from their police forces. You have to wonder whether the police realize, or care, that they are destroying public trust and respect with their actions regarding the Donald Dunphy case. It verges on farcical, except that it is so serious. (…) What is extremely bothersome is the leadership of the RCMP and RNC apparently also subscribe to the notion that the public should shut up and doesn't deserve answers until the police decide they are good and ready to provide them. The situation is astounding. The leaders of the RNC and RCMP apparently regard the concepts of open, transparent, responsible, answerable power - in political governance and in policing - as mere textbook items that are fine in theory, but in practice can be ignored whenever necessary. (Albeit, in this, they are in the company of a good many politicians.)" The Telegram, B6

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Correctional service admits 'staff misconduct' in inmate's death
Correctional Service Canada has fired one staff member and disciplined three others after an inmate was beaten and repeatedly pepper-sprayed at a New Brunswick prison before his death. The top correctional official in Atlantic Canada admits there was "staff misconduct" and "excessive force" in the case of Matthew Hines, who died in hospital on May 27, 2015 - less than two hours after his struggle with guards at Dorchester Penitentiary began. "We take this case very seriously and we're trying to learn from it," Scott Harris, regional deputy commissioner for the Atlantic region, said in an interview. CBC News has also learned that RCMP have reopened the criminal investigation into Hines's death, after saying last month their investigation was finished and foul play had been ruled out. But "additional information" has since come to the RCMP's attention, prompting police to "re-examine" the case, according to Const. Hans Ouellette, a spokesman for the New Brunswick RCMP. He wouldn't say when the investigation was reopened or what kind of new information police received. The details of Hines's death were secret until last month, when CBC News revealed the quick escalation of force used against the 33-year-old Cape Breton man after he refused to return to his cell. Minutes after his struggle with guards began, Hines was hit and then pepper-sprayed five times - including four times in less than one minute. CBC News

*** Inmate dies after attack in jail**
An inmate who was assaulted earlier this month while in custody at the Calgary Remand Centre has died from his injuries, Calgary police have confirmed. Alvin Clifford Chiniquay, 40, had been in hospital on life support since he was allegedly attacked by his cellmate. He was found in life-threatening condition by emergency responders at about 9:30 a.m. on Sept. 9. The victim's cellmate was taken into custody. The homicide unit continues to investigate, but police say charges are expected to be laid against Chiniquay's cellmate. Chiniquay was taken offlife support on Thursday. An autopsy is expected to take place. Postmedia News (Calgary Herald, A10); * CBC News

*** Canada-wide warrant issued for man convicted of second-degree murder**
A man convicted of second-degree murder who is known to frequent the London and St. Thomas area is being sought by police. Lyle Ridgewell, 60, is wanted on a Canada-wide warrant for breach of parole. Ontario Provincial Police said Ridgewell is 5'6", 143 lbs. with hazel eyes and brown hair. London Free Press (CTV News)

*** Editorial: Justice system fails us all**
An editorial piece states, "Yet another report has come out about how slow, inefficient and expensive Canada's justice system is. How many more such reports will it take to spur governments and the

judiciary into making needed changes? Delays in the justice system are not merely inconvenient to those involved, they seriously threaten the rights of victims and the accused, and the well-being of society. The ponderous pace of justice is a problem all across Canada, but B.C. ranks near the bottom, according to a report released by the Macdonald-Laurier Institute. In B.C. Supreme Court last month, charges were stayed against a former Vancouver Island investment dealer because of what a judge called an unreasonably long wait for a trial. Charles Kamal Dass, who was a registered investment adviser in Port Alberni, was charged with 15 counts of theft, fraud and forgery, based on transactions with 13 persons and two corporations between 2000 and 2007, court was told. Criminal charges were laid in June 2013 and the trial was set to begin Aug. 2, but on the first day of trial, Dass's lawyer applied to have the charges stayed. The following week, Justice Robert Johnston advised Crown counsel he would direct a stay of proceedings because of the time the case has taken to come to trial." Times Colonist

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Thunder Bay police face allegations of 'systemic' racism
The Ontario police oversight body will hold a sweeping review of Thunder Bay Police's conduct in the investigations in the deaths of indigenous people. The Office of the Independent Police Review Director (OIPRD) will conduct their systemic review this fall. They will drill down on the deaths of Stacey DeBungee, 41, whose body was found in a Thunder Bay river on Oct. 19, 2015, and on "information and evidence" surrounding the deaths of seven students who attended a Thunder Bay high school from 2000 to 2011. DeBungee's body was found in the McIntyre River. Within three hours of the discovery, the Thunder Bay Police issued a statement that a body was found and that an "initial investigation does not indicate a suspicious death. A post mortem examination will be conducted to determine an exact cause of death." In a second press release on Oct. 20, 25 hours after the discovery, the police identified DeBungee and said DeBungee's "death has been deemed as non-criminal." "There is a systemic treatment of indigenous deaths that is not lost on any of my clients," said Julian Falconer, the DeBungee family lawyer who also acted for Nishnawbe Aski Nation at the inquest into the seven students' deaths. Police put both the releases out before a post mortem occurred, Falconer said. "They are less than worthy victims. This is simply a more acute example, a very clear example, of what is sadly being experienced in the murdered and missing indigenous women and girls' scenario. The quality of the investigations are in my decades of practice, well below the standard of anything I have ever seen," Falconer said. Toronto Star, A1

*** Forceful arrests decline, as police get busier**
Edmonton police officers are resorting to less forceful means to make arrests, a report to the city's police commission revealed Thursday. "We don't want to discourage our members from using force when it's necessary but it's imperative that the use of force is professional in its application, reasonable given the circumstances and defensible," Supt. Dave Christoffel said. Every time an officer uses force, be it through a physical disarming technique, using a weapon such as a gun or a baton, or even deploying a police dog, they have to fill out a report. In the first six months of 2016, the numbers of those incidents are down from the year previous. Police saw an increase in overall workload, dealing with 128,000 cases, up from slightly more than 124,000 last year. Despite that, use of force occurrences dropped from 1,175 in 2015 to 1,127 this year, something Christoffel called good news. (...)One area that saw a spike was the use of conducted energy weapons, or Tasers, which was up almost 89 per cent. (...) That said, out of the roughly 400 Tasers carried by police in the city, they were used just 17 times in the first six months of 2016. "I often thought that Tasers got a bit of a bad rap," said Coun. Scott McKeen, who serves on the commission. He said a lot of high-profile cases of Taser use leading to death in recent years put too much emphasis on the weapon itself and not the context. "It sounds ridiculous to say, but I'd rather have a Taser than a gun or even a baton, as far as causing physical harm to somebody who needs to be brought down in a humane way," McKeen said. Edmonton Journal, A4

Morphing crime rate: Halifax police chief says drop in numbers obscures rise in online wrongdoing

Statistics suggesting crime rates in Canada have been falling for decades may not tell the whole story when it comes to criminal wrongdoing, the chief of Halifax Regional Police says. Jean-Michel Blais says there are indications that the nature of crime is changing in a way that is not reflected in traditional crime data. "And this crime is not being committed by your neighbour, and probably not someone here in Nova Scotia or even in Canada," he said in an interview. "It's being committed by somebody in a different country." Blais, who plans to explore the issue today in a speech to the Halifax Chamber of Commerce, says traditional crimes appear to be "morphing" and migrating to criminal acts perpetrated online. As a result, he says, crime probably hasn't decreased as much as statistics might suggest. In 2014, a study in the United Kingdom found just over half of those surveyed in Britain had been the victim of an online crime, including identity theft, hacking and illegally accessing and stealing from bank accounts. The study found that much of this crime was never reported, which means it didn't show up in police statistics. The Get Safe Online survey, conducted by market research firm Vision Critical, also showed that 53 per cent of those surveyed said they considered online crimes as serious as physical crimes. "Crime really hasn't gone down as much as we think," Blais said in an interview. "It's ... migrated onto the Internet." Canadian Press (Guardian, B5, Time Colonist)

* **New cyberbullying law months away, justice minister says**
A landmark cyberbullying law that was ruled unconstitutional and struck down nearly 10 months ago won't be replaced until at least next spring, says Nova Scotia's justice minister. Diana Whalen said Thursday that provincial government officials are still consulting with experts and want to ensure the new law can withstand a court challenge. Whalen said it's important to take the time to do it right, noting the original law was passed in only three weeks with all-party support. "What we want to make sure is that we don't bring something in, in great haste that is going to be challenged again," said Whalen. "I'm not committing to a timeline, but we couldn't do it by this fall - it wouldn't be before the spring at the earliest." The Supreme Court of Nova Scotia struck down the CyberSafety Act last December, saying it infringed on charter rights involving freedom of expression. Canadian Press (Times & Transcript, B5, Guardian, Cape Breton Post, Chronicle Herald)

* **Nunavut: a fast, efficient justice system where victims fare poorly**
Nunavut's justice system deserves some of the highest marks in Canada for efficiency, fairness and access to justice, but failing marks for victims' services and costs, an Ottawa-based think-tank found in a national report card released Sept. 21. The report card, done for the Macdonald-Laurier Institute by law professor Benjamin Perrin and statistics expert Richard Audas, hands out grades ranging from F to A+ for each of Canada's 13 territorial and provincial justice systems. They graded each jurisdiction on five criteria: public safety, support for victims, costs and resources, fairness and access to justice, and efficiency. After that, each of the five grades is compiled to produce an overall mark. They gave Nunavut an A+ for fairness and access to justice, and an A for efficiency. Nunavut's A+ mark for "fairness and access to justice" is better than the marks they handed out to all other jurisdictions in that category. This likely means that Nunavut does exceptionally well in ensuring that the constitutional rights of accused persons are protected and that they get fair and impartial trials. On "efficiency," Nunavut's mark of A suggests that police are able to solve most crimes and that criminal cases proceed through the courts in a timely manner. Nunatsiaq News

* **'A misunderstanding': Northerners question failing grades on new justice report card: Nunavut, Yukon, N.W.T. receive Fs for victim support, costs and resources**
Some Northern officials are giving a new report evaluating the country's justice systems an A for effort, but say it inaccurately reflects the reality in Yukon, the N.W.T. and Nunavut due to "significant flaws" in methodology. The report, co-authored by associate professors Benjamin Perrin and Richard Audas of the Macdonald-Laurier Institute, is based mostly on data available from Statistics Canada. Each territory and province is given a letter grade for "five major objectives" of the justice system, according to the authors: public safety, support for victims, costs and resources, fairness and access to justice, and efficiency. Out of all 13 provinces and territories, Yukon placed 13th. Manitoba placed 12th, followed by the N.W.T. and then Nunavut. The three territories were the only regions in the country to get Fs — they got two each. One for the high cost of running the justice systems — everything from the cost per inmate to the number of RCMP officers per capita — and the other for a lack of support for the victims of crimes. CBC News

*** N.B. has great justice system, except for two crucial failings**
An opinion piece states, "This week the Macdonald-Laurier Institute public policy 'think tank' stated New Brunswick's criminal justice system ranks third among the 13 provinces and territories in Canada, behind only Prince Edward Island and Newfoundland. It gives us some bragging rights at a time when we have little to be bragging about as our economy continues to sink under its own decrepit state and continued political neglect. The study highlights some genuine positives about the criminal justice system in New Brunswick, including that it's less costly and more efficient than most of Canada, rendering justice more quickly. And we get great grades for public safety. We have fewer property crimes and only moderate rates for violent crimes compared to most of Canada. Many of us have known or intuited these things for years; it's partly what we refer to when we talk of the quality of life in the Maritimes despite the many challenges we face. It is also notable that, to quote the report, "the police in New Brunswick perform highly in public perceptions, particularly in enforcing the law, ensuring safety, satisfactions with public safety, supplying information, being approachable, being fair, and responding promptly." Take a bow, men and women of our police forces." Times & Transcript, A10

*** Rural crime a serious issue most don't get**
An opinion piece states, "This has been another tough week for rural Saskatchewan's image. Maybe a little of it can be blamed on an aging population that's both scared and reacting badly to growing social problems. But maybe the bigger problem is that we haven't bothered to take the time needed to recognize the real problems and their causes. Consider the now-popular Internet image of rifles in combines - all-too-easy confirmation of the East's wrong-headed view of rural western rednecks. One can almost hear the gunregistry advocates hollering: "See, I told you so." However, these images have emerged after Monday's incident near Fiske (between Kindersley and Rosetown in west-central Saskatchewan), in which three masked men carrying handguns tried to hold up a farmhand. Stories abound throughout rural Saskatchewan of vandalism, break-ins, vehicle, farm machinery and gas thefts, and even occasional home-invasion robberies with violence. This was the case even before the racially charged incident near Biggar that resulted in the shooting death of Red Pheasant First Nation resident Colten Boushie and a second-degree murder charge. Yes, the RCMP was right to issue a warning about proper use and storage of firearms before we see an unintentional tragedy. But it's far more complicated than rural people simply acting irrationally or misusing firearm privileges. After all, can we blame rural people - whether in their farmyards or alone in the field on their combines - for being damn scared after hearing RCMP reports of masked gunmen attempting to hold up people who are isolated from police or other help?" Leader-Post

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Stark lesson on need to act
The sudden guilty plea in a Regina court this week by Clayton Eichler to the murders of two young women, Kelly Goforth, 21, and Richele Bear, 23, puts in stark focus the grim reality and the heartbreak of the families whose loved ones are on Canada's long list of missing or murdered aboriginal women. While Eichler's 11th hour decision to plead guilty to two counts of second-degree murder and his expression of regret may have brought a measure of comfort to the family of Goforth, whose body was discovered in a hockey bag thrown away in a trash bin, there was no closure for the relatives of Bear, whose pleas to learn where her body could be found elicited no answer from the killer. A shouted response from the gallery to Eichler, "Burn in hell, you bastard," attests to the anguish and despair of the family. With the conviction that nets him at least 20 years in prison before parole eligibility, Eichler becomes Regina's first known serial killer. He joins the despicable ranks of the likes of Saskatoon's John Crawford, who brutally murdered three other indigenous women, Shelley Napope, 16, Eva Taysup, and Calinda Waterhen in the early 1990s. In sentencing Crawford, Queen's Bench Justice David Wright likened him to a "wild animal, a predator" and expressed deep regret that he couldn't extend the parole eligibility beyond 25 years. Starphoenix, A12

*** President of Native Women's Association of Canada stepping down**

The president of the Native Women's Association of Canada is stepping down to spend more time with her family, just weeks after the historic launch of a national inquiry into Canada's missing and murdered indigenous women. On Thursday morning, Dawn Lavell-Harvard, who was elected to a three-year term in July of 2015, issued a letter of resignation to NWAC's board of directors after more than 20 years of formal advocacy. (...) Looking back on her time at the helm, Dr. Lavell-Harvard is struck by the heightened awareness among Canadians about indigenous issues, as well as the dramatic shift in political tone. "I was at the head of the association during this amazing shift from a government that said the violence against indigenous women and girls was not even on their radar, to a government that has [launched] an inquiry," said Dr. Lavell-Harvard, a member of Wikwemikong First Nation, in northern Ontario. "This is something we have been pursuing for years." Former prime minister Stephen Harper dismissed calls for an inquiry, saying the tragedies were not part of a "sociological phenomenon" but rather criminal matters best handled by police. NWAC, as the leading voice for indigenous women in Canada, was in a constant state of agitation. Although the organization had been championing an inquiry for more than a decade, never had the matter been so prominent and hot-button. It was a major issue in last year's federal election, which saw the Liberals rise to power on the promise of a renewed nation-to-nation relationship with indigenous peoples. Globe and Mail (2016-09-22)

*** Trudeau needs to take action**

An opinion piece states, "The Liberal government of Justin Trudeau has, so far at least, talked a good game about rebuilding goodwill between Ottawa and Canada's First Peoples. He has said publicly on more than one occasion he wants to re-establish a "nation-to-nation" relationship with aboriginal communities. Trudeau has promised to end decades-old boil-water advisories on countless reserves in Canada within five years, earmarking roughly $1.8 billion to the task. Additionally, he has acknowledged the need to develop a mental health or suicide strategy for dealing with unconscionable rates of suicide among aboriginals. Most significantly, he has launched a wide-ranging inquiry into missing and murdered indigenous women and children. He also pledged to not move forward on major resource development projects in Canada that don't have sufficient social licence - especially from indigenous communities. The government has also indicated its intention to follow through on the 94 "calls to action" of the 2015 Truth and Reconciliation Commission Report. It has been silent recently on how that objective will be accomplished and how much money will be allocated for doing so. First Nations leaders, then, have reason to be skeptical at worst and cautiously optimistic at best." Winnipeg Free Press

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Marijuana - La DSP repousse le modèle de la SAQ

La Santé publique montréalaise rejette l'idée de confier la vente de marijuana, une fois légalisée, à la Société des alcools du Québec. Elle préconise plutôt la création d'une nouvelle agence provinciale qui ne subirait pas de pressions pour verser des profits au gouvernement. Si cette agence devait administrer les points de vente, " un tel monopole ne devrait pas être considéré comme une source majeure de revenus pour l'État ", juge la Direction régionale de la santé publique de Montréal dans un mémoire publié sur son site Web cette semaine. " La Société des alcools du Québec, à qui le gouvernement demande des profits, ne constitue pas un modèle ", ajoute-t-elle. Ce mémoire, qui met de l'avant 52 recommandations, a été préparé dans le cadre de la consultation amorcée par le fédéral en vue de la légalisation du cannabis. La période de consultation se terminait le 29 août. " On ne doit pas voir la marijuana comme source de revenus additionnelle ", explique le psychiatre Robert Perreault, qui est aussi médecin-conseil à la Direction de la santé publique de Montréal et l'un des auteurs de ce mémoire. " D'un point de vue de santé publique, la façon dont l'alcool est géré est problématique, car il y a une incitation à la consommation. On ne souhaite pas que la marijuana subisse le même traitement. " Le Devoir, A1

Homelessness, pot tax on UBCM agenda

Nearly 2,000 municipal politicians, civic staff and other community leaders are preparing for a five-day Union of B.C. Municipalities convention beginning Monday in Victoria. (...) Election of a new president and executive team is slated for Thursday, as Cariboo Regional District chairman Al Richmond ends his term leading the UBCM. He said the issue of marijuana regulation and tax sharing is expected to raise

strong interest among delegates, but housing affordability is also high on the agenda. Canadian Press (Times Colonist, B1)

Pot shop next to kids' classes angers parents
Some parents in Orléans are furious that an illegal pot shop has opened in the building where their children attend martial-arts classes and after-school tutoring. A marijuana dispensary called CannaGreen opened on Sept. 11 in the front of a small commercial building on St. Joseph Boulevard. (…) Municipalities and police forces are struggling to figure out what to do. Most dispensaries say they serve medical marijuana patients, and screen customers to make sure they have a medical condition. Medical marijuana is legal in Canada, but only if purchased from producers licensed by Health Canada, who send the products by mail. The federal government has promised to introduce legislation in the spring to legalize recreational marijuana. It's not known whether selling marijuana in stores will be allowed. The government has promised to "strictly regulate" sales to keep pot out of the hands of children and away from organized crime. In the meantime, it's become a free-for-all. Federal politicians warn that products sold at the illegal dispensaries are unregulated, and may be unsafe. Enforcement of the drug laws is up to police. In some cities, including Toronto, Quebec City, Barrie, Oshawa, Whitby and Peterborough and parts of B.C., police have raided the dispensaries. Employees and owners have been charged with drug trafficking and other offences. In Vancouver, police have chosen not to raid the shops unless there is evidence the operators are selling to minors or connected to organized crime. Ottawa Citizen, A1

Test de crédibilité, test d'identité
Bono avait d'abord lancé ces mots dans un discours au Centre Air Canada, à Toronto, fin 2003 lors de l'élection officielle de Paul Martin à la tête du pays. Le rockeur irlandais ne tarissait pas d'éloges à l'endroit de Paul Martin, qui s'était engagé à accroître significativement les budgets canadiens d'aide aux pays en développement et dans les programmes de lutte contre les épidémies. Il les a répétés samedi à la Conférence de reconstitution des ressources du Fonds mondial de lutte contre le sida, la tuberculose et le paludisme tenue à Montréal sous l'égide du gouvernement Trudeau. (…)Difficile à dire parce que pour le moment, le succès de M. Trudeau repose beaucoup plus sur ce qu'il a promis de faire que sur ce qu'il a accompli après bientôt un an au pouvoir. (…)La légalisation de la marijuana, autre promesse de Justin Trudeau, occupera aussi les esprits. Normalement, les nouveaux gouvernements préfèrent enclencher leurs réformes dans les deux premières années de leur mandat, question de libérer la voie vers les prochaines élections. On sent toutefois plus de prudence que d'empressement sur cette question. Autres dossiers chauds : la réforme de la loi C-51 (antiterroriste), les projets de pipeline, l'aide financière à Bombardier, le financement de la santé pour les provinces, la négociation des traités de libre-échange et d'une nouvelle entente sur le bois d'oeuvre avec les États-Unis. La Presse

Vintage Vinyl celebrates 25 years as pot attitudes change
Vintage Vinyl and Hemp Emporium is known for a lot of things, notably its history with marijuana. Dylan and Janelle Baumet's father Pat opened Vintage Vinyl and Hemp Emporium 25 years ago in downtown Regina. The store has remained a family business over the years and sells everything from records to marijuana smoking accessories. (…)The Liberal government is on the path to legalizing marijuana, which Dylan believes is for the best and is long overdue. Vintage Vinyl is the longest-running hemp store in Canada so Dylan believes that legalization will just help the store to grow. Leader-Post, A3

Not high on pot shop
Parents in Orleans are furious that an illegal pot shop has opened where their children attend martialarts classes and after-school tutoring. A marijuana dispensary called CannaGreen opened on Sept. 11 in a building on St. Joseph Boulevard that also houses The Edge Taekwon-Do Academy and Kumon Math and Reading Centre. All the businesses share a parking lot in the back. (…)At least 15 mari juana dispensaries have opened in town. (…)None of the dispensaries has a business licence. City bylaws don't include provisions for illegal pot shops. Mayor Jim Watson has repeatedly declined to comment on the issue. "The federal government regulates marijuana laws, and Ottawa Police has the jurisdiction to enforce them if a complaint arises," a statement from his office said. The federal government says these dispensaries are all illegal, and municipalities and police forces are struggling to figure out what to do. Most dispensaries say they serve medical marijuana patients, and screen customers to make sure they have a medical condition. Medical marijuana is legal in Canada, but only if purchased from producers

licensed by Health Canada, who send the products by mail. The federal government has promised to introduce legislation to legalize recreational marijuana in the spring and "strictly regulate" sales to keep pot out of the hands of children. Ottawa Sun, A11

PUBLIC SERVICE / FONCTION PUBLIQUE

Phoenix payroll chaos: Prison guards struggling to make ends meet
The prison guards who watch over some of Canada's most dangerous criminals are the latest to see their pay lost to glitches in the federal government's new automated national payroll system. Kent Institution corrections officer Doug Holloway was left scrambling to meet a car payment and buy groceries this week, after he didn't get paid at all. His previous two cheques also fell short, forcing Holloway, his wife and three of his four children — his eldest has left home — to go without as they waited for emergency salary advances that took several days to come. "I have my car payments scheduled with my paydays," said Holloway, whose family is still living in Grande Cache, Alta., where he worked at a federal prison before transferring to Kent three months ago. "I was catching myself thinking, do I have enough on my MasterCard so I can buy milk to have on my cereal?" Province

OTHER / AUTRE

* **Pour un gouvernement qui « se bat pour protéger ses ressortissants »**
Q Quand vous êtes sorti de prison, vous avez dit que l'ancien premier ministre canadien Stephen Harper vous avait « trahi » et « laissé tomber » et vous avez dénoncé le manque de soutien aux Canadiens qui sont détenus à l'étranger. Pensez-vous que la situation s'est améliorée depuis ? R Oui, c'est le jour et la nuit. Alors que j'étais en prison, Stephen Harper, plutôt que d'user de toute son influence pour intervenir auprès du président égyptien, a délégué ses responsabilités à ses subalternes. Les diplomates canadiens ont fait du super travail, mais ils me disaient qu'ils étaient menottés par Ottawa. On ne peut pas comparer cela à ce que le gouvernement Trudeau fait aujourd'hui. Les faits sont éloquents. Les libéraux ont récemment réussi à faire libérer le Canadien Kevin Garratt en Chine et à ramener au pays Khaled al-Qazzaz, l'ancien bras droit de l'ex-président Mohamed Morsi, avec qui j'ai été emprisonné en Égypte. Ce sont deux grands succès. C'est plus important que jamais d'avoir des gouvernements qui se battent pour protéger leurs ressortissants. À travers le monde, pas juste en Égypte, les pays créent des lois antiterroristes très vagues qui font que tous les Canadiens à l'étranger _ et pas seulement les journalistes et les travailleurs humanitaires sur la ligne de front _ peuvent être mis en prison et être accusés de terrorisme ou d'espionnage. C'est sans précédent. On le voit avec Homa Hoodfar [la professeure de Concordia détenue en Iran]. Et il n'y a pas de communiqué de presse ou de rhétorique vide qui puisse vous aider à ce moment-là. Vous avez besoin d'une intervention robuste de votre gouvernement et de votre famille. Q Dans le même ordre d'idées, vous défendez un projet de charte qui renforcerait la protection des ressortissants canadiens à l'étranger. Avez-vous une oreille attentive à Ottawa ? R J'aimerais que cette charte, que je défends conjointement avec Amnistie internationale, devienne une loi qui obligerait le gouvernement canadien à agir quand un Canadien est détenu à l'étranger. En ce moment, c'est à la discrétion des politiciens, alors qu'en Allemagne, aux États-Unis, au Brésil, c'est la loi. Nous projetons d'en faire un projet de loi bientôt avec le soutien de politiciens néo-démocrates qui ont manifesté leur intérêt. Et jusqu'à maintenant, nous avons reçu une excellente réponse de Justin Trudeau et du ministre des Affaires étrangères, Stéphane Dion. La Presse, 17; Montreal Gazette

* **Sailors and pilots hitting St. John's as anti-submarine warfare training wraps up - About 3,000 people took part in multi-nation anti-submarine training**
Warships are descending upon St. John's this morning for the end of the Cutlass Fury training exercise. The exercise saw groups from Canada, the United States, Spain, the United Kingdom and France work together on anti-submarine warfare simulations off Nova Scotia and Newfoundland, the biggest such exercise on the coast in more than 20 years, said Capt. Craig Skjerpen. "We're pretending that there's a conflict and we made it all better through our training," said Skjerpen from HMCS Fredericton. He said anti-submarine training is crucial for the armed forces. "Because of their ability to hide, their stealth, to be

able to move into an area, they can pose a significant threat to maintaining the sea lanes. Keeping those lanes open is crucial to a nation's economy, said Skjerpen. "This kind of threat, if it's imposed on a nation with submarines, we have to be able to defend ourselves and be able to maintain those sea lanes of communication open to global commerce." CBC News

INTERNATIONAL

*** Government signs peace deal with warlord**
Afghanistan's government signed a draft peace deal on Thursday with a designated "global terrorist" after lengthy negotiations that could pave the way for a similar accord with the Taliban, who have been waging war on Kabul for 15 years. The deal with warlord Gulbuddin Hekmatyar is the country's first peace agreement since the Taliban launched their insurgency in 2001, after being driven from power in the wake of the 9/11 attacks on the United States. It grants full political rights to his Hezb-i-Islami Gulbuddin party and obliges the Afghan authorities to work to have it removed from the United Nations' list of foreign terrorist organizations. Hekmatyar himself was designated by the U.S. as a "global terrorist" in 2003. The agreement ends years of talks between Kabul and Hekmatyar. It enables him to return to Afghanistan after 20 years in exile - he is believed to live in Pakistan. Associated Press (Vancouver Sun, Whitehorse Daily Star, London Free Press, Montreal Gazette, Edmonton Journal, Leader-Post, Ottawa Citizen, Windsor Star, Calgary Herald, National Post)

*** Man pleads guilty in blogger beheading plot**
A Rhode Island man charged with plotting to help the Islamic State group has pleaded guilty to conspiracy charges, including a plot to behead conservative blogger Pamela Geller. Nicholas Rovinski pleaded guilty Thursday in U.S. District Court in Boston to two federal charges including conspiracy to commit acts of terrorism transcending national boundaries. Prosecutors say Rovinski, of Warwick, plotted with two Massachusetts men to kill Geller. The plot was never carried out. Rovinski's lawyer says his client renounces allegiance to the Islamic State group. Prosecutors alleged the 25-year-old, while in jail, tried to recruit people to carry out violent attacks in the United States. A plea agreement Rovinski reached with prosecutors called for a sentence of between 15 and 22 years in prison. Sentencing is scheduled for March 23. Associated Press (Guardian, B6, Cape Breton Post)

*** Prosecutors charge white Oklahoma police officer, who fatally shot unarmed black man, with manslaughter**
Prosecutors in Tulsa, Oklahoma, charged a white police officer who fatally shot an unarmed black man on a city street with first-degree manslaughter Thursday. Tulsa County District Attorney Steve Kunzweiler filed the charge less than a week after officer Betty Shelby shot and killed 40-year-old Terence Crutcher on Sept. 16. Kunzweiler said arrangements were being made for Shelby's surrender. "I do not know why things happen in this world the way they do," Kunzweiler said, adding that he determined first-degree manslaughter the appropriate charge. "We need to pray for wisdom and guidance." Dashcam and aerial footage of the shooting and its aftermath showed Crutcher walking away from Shelby with his arms in the air. The footage does not offer a clear view of when Shelby fired the single shot that killed Crutcher. Her attorney has said Crutcher was not following police commands and that Shelby opened fire when the man began to reach into his SUV window. But Crutcher's family immediately discounted that claim, saying the father of four posed no threat to the officers. They also pointed to an enlarged photo from police footage that appears to show Crutcher's window was rolled up. And police said Crutcher did not have gun on him or in his vehicle. Associated Press (National Post)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
September 26, 2016 / le 26 septembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

McGuinty to earn extra $42,000 as head of Joint National Security Committee
The bill at the centre of debate in the House of Commons for most of this week-Bill C-22, the government's proposed legislation to create a National Security and Intelligence Committee of Parliamentarians-comes with sizeable pay bumps for those selected to be on it. The bill, currently at second reading, was introduced just ahead of MPs fleeing Parliament for the summer, and is being sponsored by Government House Leader Bardish Chagger (Waterloo, Ont.). The government has dedicated three days of debate to it in the House this week-Tuesday, Wednesday, and Friday-in hopes of passing it at second reading and getting it off to the Public Safety and National Security Committee by the end of the week. (…) Mr. McGuinty said it will be Mr. Trudeau's purview on what the committee studies and noted that **Public Safety Minister Ralph Goodale** (Regina- Wascana, Sask.) has been conducting parallel consultations on potential Bill C-51 reforms. Further, the work of the committee's secretariat

would be exempt from the Access to Information Act, as the bill states that it "shall refuse to disclose any record requested under this Act that contains information obtained or created by it or on its behalf in the course of assisting the National Security and Intelligence Committee of Parliamentarians in fulfilling its mandate." The bill follows through on a Liberal campaign promise to create an all-party committee to oversee the government's national security agencies in an effort to align with the other countries in the so-called "Five Eyes" alliance, which includes Canada, the United States, the United Kingdom, Australia, and New Zealand. Hill Times

Canada says new border accord with China will speed deportations
An agreement signed between Canada's border agency and China will result in the faster deportation of Chinese citizens deemed inadmissible by Canadian authorities, a Liberal government spokesman said on Sunday. The deal will allow Chinese officials to travel to Canada to interview Chinese citizens considered inadmissible, with the aim of verifying their identities and documents, said **Scott Bardsley, press secretary to Public Safety Minister Ralph Goodale**. **Bardsley** said the verification process could otherwise take a long time and had often delayed deportations. (…) The border agency agreement, which will not be in place immediately, is similar to one China has with the European Union, and officials from both countries will revisit the matter in November, said **Bardsley**. (…) The countries on Thursday settled a trade dispute and said they would start exploratory talks on a free trade pact. The countries also signed a memorandum of understanding under which the Royal Canadian Mounted Police and the Ministry of Public Security of China will cooperate to combat a broad range of crimes. **Bardsley** said the memorandum was a renewal of a similar one signed in 2010 that called for broad cooperation. Reuters (2016-09-25)

It's time for a commission of inquiry on Afghan detainees
An opinion piece by NDP MP Hélène Laverdière states, "Over the past months, we have seen renewed calls on the Canadian government to launch a Commission of Inquiry into Canada's practices and policies relating to the transfer of hundreds of detainees to Afghan authorities, during Canada's mission in Afghanistan. In June, more than 40 civil society groups, lawyers, academics and prominent Canadians signed a letter calling for a Commission of Inquiry. Signatories included former prime minister Joe Clark, the inaugural chair of the Security Intelligence Review Committee Ron Atkey, Ed Broadbent, Stephen Lewis, Canadian diplomats posted to Afghanistan during the war, the secretary general of Amnesty International Canada, and leading scholars and representatives of human rights, foreign policy, and lawyers' organizations. New Democrats were among the signatories. (…) Stéphane Dion and **Ralph Goodale** strongly supported the NDP's call for a public inquiry while in opposition. Now, as ministers responsible for Global Affairs and Public Security-two of the three ministries with responsibility for this case-they are abdicating their responsibilities and refusing to pursue the matter. The third minister involved is the minister of National Defence and it is alarming that the government has assigned to him the role of responding to these allegations. Sajjan was a senior officer in Kandahar during the period in question and it is likely that he would be a key witness at an inquiry. The potential conflict of interest should disqualify him from oversight of this case. This is not solely a Defence issue, and in no way should be handled by this minister alone. It is time for the prime minister to take the lead." Hill Times

TOP STORIES / MANCHETTES

Spy chief issues encryption warning
The head of Canada's electronic spy agency warned Friday the advent of super-fast quantum computers will cripple current encryption methods for securing sensitive government and personal information within a decade. In a rare public speech, Greta Bossenmaier, chief of the Communications Security Establishment, said cryptologists at the CSE and around the world are racing to find new cryptographic standards before Y2Q - years to quantum - predicted for 2026. She was the third senior CSE official in less than a week to warn publicly of the threat quantum computing poses to widely used public key cryptography (PKC), protecting sensitive data transmissions from hackers, hacktivists, foreign state spies and other malicious actors. The CSE is best known as a spy agency - it collects, decrypts and analyzes phone calls, faxes, emails, tweets, satellite and other electronic signals emanating from adversarial foreign nations and overseas threat actors. But it's also mandated to protect government computer

systems and networks, and the information they carry. Already, federal computer systems are "probed" more than 100 million time a day by suspected malicious actors searching for vulnerabilities. Now, "the challenge of protecting systems is about to get a lot harder thanks to quantum computing," Bossenmaier told an Ottawa conference of the Canadian Association for Security and Intelligence Studies. Postmedia Network (Kingston Whig-Standard, B1, Ottawa Citizen)

An extradition treaty with China sends a message about corruption

A lawyer at Duhaime Law, with a specialized practice in anti-money laundering, counterterrorist financing and asset recovery. The topic of an extradition treaty between Canada and China is at the forefront among the news media, government officials and the public these days. Indeed, it should be, because it's a topic that's important to both countries. There are a lot of experts telling us what's wrong with an extradition treaty with China. We are told that Canada can't sign an extradition treaty with China because China has capital punishment. But that's never been a bar to entering into an extradition treaty. Canada has extradition treaties with the United States, Japan, Zimbabwe, Singapore and the Maldives, all of which have capital punishment. (...) The Globe and Mail recently published a story about a foreign national who bought houses in Vancouver using third parties to obtain mortgages. That practice, if not disclosed to the banks in advance, would cause the banks, realtors and insurers conducting legally required due diligence to unwittingly file reports to the Financial Transactions and Reports Analysis Centre of Canada with the wrong persons identified as conducting financial transactions. The resulting (unwitting) systematic filing of reports with the wrong persons identified would stand in the way of FinTRAC's efforts to process information accurately, jeopardizing our security against money laundering and terrorist financing. The rule of law would not prevail if there were an absence of legal transparency - the public would be defrauded of the delivery of a vital public service by a few foreign homeowners and we would all be placed at risk. Globe and Mail, B4

Canada deports family to Ukraine as appeals fail

Canada deported a mentally ill 15-yearold boy to Ukraine Sunday night, despite medical evidence it is likely to trigger a second suicide attempt. Two border guards approached Vladyslav Zadorozhnyi the minute he arrived in the departures hall, and asked, as a formality, whether he is ready to go. "I don't know what to say," he said. "I feel very bad. Anxiety." Wearing a sporty zipup and a backpack, his hair carefully gelled, he was taken into the border security office with his mother Maryna Zadorozhna, 34, and his brother Andriy, 7. They arrived with the tearful parents of Vladyslav's new best friend, Alex, a classmate in his west Toronto school. (...) A key factor appears to have been Canada's late discovery of a fraud charge in Ukraine against Andriy. It was first mentioned by Canada on September 14 - more than a year after the family arrived, and a few days after the first scheduled deportation was cancelled at the 11th hour - in a letter from a senior immigration officer with the Backlog Reduction Office of Citizenship and Immigration Canada. Andriy denies being charged with fraud, and his refugee application includes clean police records checks. His counsel suggests the unspecified charge has been fabricated, and fits with the family's story about persecution by gangsters allied with crooked police, which a refugee tribunal did not believe. In an emergency hearing Saturday, the family's lawyer Hart Kaminker argued the process has been procedurally unfair and below the legal standard of how Canada treats children. Canadian Border Services Agency is "acutely aware of the fragility of Vladyslav's health," and putting the family on this "roller coaster," with two deportations scheduled in as many weeks, is not being "alert, alive and sensitive" to the boy's best interests. Those three words were used by the Supreme Court of Canada, in the 1999 case of Mavis Baker, a Jamaican woman whose four children were born in Canada. The case made a child's interests a mandatory factor in any deportation decisions that affect the child. But it did not make them a "primary" consideration. That is the higher standard set by the United Nations Convention on the Rights of the Child, which Canada has signed. Vladyslav's file was reviewed by a doctor on behalf of CBSA, who disagreed with a psychiatrist and judged him fit to fly, with no communicable disease. CBSA also confirmed medical staff will be on hand in Kyiv. Postmedia Network (National Post, A3, Vancouver Sun)

Waterloo Regional Police take extra precautions to avoid drug exposure during investigations: Inspector

Local police officers are taking more precautions during drug seizures and when helping those who have overdosed because of the dangers involved in even inadvertently touching certain drugs, the head of

Waterloo Regional Police's strategic and tactical services division says. "We've had to do some significant changes even just within our own service here in regards to the handling of those drugs once they're seized just because of the relative danger of them," Insp. Dave Bishop told CBC News. (…)The RCMP released a video earlier this month warning about the dangers first responders face when it comes to fentanyl. "The danger this drug presents to all Canadians cannot be overstated," RCMP Commissioner Bob Paulson said in a release. "It's spreading across the country, leaving a trail of misery and death, and first responders and the public need to know that even being near it can make you sick, or worse." The video tells the story of Const. Rob Dupuis in Kamloops, B.C., who found a man slumped over the steering wheel of his vehicle. The man was arrested, Dupuis put him in the cruiser and then went back to search the vehicle. "I noticed there was a bit of a chemical smell," Dupuis said. He started to feel lightheaded and nauseous, so he asked the man what he had in the car and the man said it was fentanyl. Dupuis had a urine test and it found he had trace opioids in his system. "The traffic stop is one of the most dangerous things that we'll ever do in our career because of the unknown. Now adding fentanyl to the mixture, you're stopping a vehicle and you think it's drugs and you're looking at it and you go, 'Oh wow, that looks like cocaine or heroin,' you just don't know anymore," he said. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NIL

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** An extradition treaty with China sends a message about corruption**
A lawyer at Duhaime Law, with a specialized practice in anti-money laundering, counterterrorist financing and asset recovery. The topic of an extradition treaty between Canada and China is at the forefront among the news media, government officials and the public these days. Indeed, it should be, because it's a topic that's important to both countries. There are a lot of experts telling us what's wrong with an extradition treaty with China. We are told that Canada can't sign an extradition treaty with China because China has capital punishment. But that's never been a bar to entering into an extradition treaty. Canada has extradition treaties with the United States, Japan, Zimbabwe, Singapore and the Maldives, all of which have capital punishment. (…) The Globe and Mail recently published a story about a foreign national who bought houses in Vancouver using third parties to obtain mortgages. That practice, if not disclosed to the banks in advance, would cause the banks, realtors and insurers conducting legally required due diligence to unwittingly file reports to the Financial Transactions and Reports Analysis Centre of Canada with the wrong persons identified as conducting financial transactions. The resulting (unwitting) systematic filing of reports with the wrong persons identified would stand in the way of FinTRAC's efforts to process information accurately, jeopardizing our security against money laundering and terrorist financing. The rule of law would not prevail if there were an absence of legal transparency - the public would be defrauded of the delivery of a vital public service by a few foreign homeowners and we would all be placed at risk. Globe and Mail, B4

*** Tackling compliance challenges**
Move over fintech: Start ups using technology to solve compliance challenges for heavily-regulated financial services firms are on the rise. And one area generating interest among entrepreneurs is automation of the time-consuming process of verifying clients for banks and payment companies. Banks invest a lot of time and effort to prove their clients really are who they say, and that they are not tied to

criminal or terrorist organizations. The "know your client," or KYC, process is a crucial part of the anti-money laundering, or AML, practices all banks must follow. But it's a process that can drive up costs and create compliance risks, and the penalties can be heavy when the banks get it wrong. In April, authorities fined an unnamed Canadian bank $1.1 million for not reporting a suspicious transaction. HSBC, which had already paid $1.9 billion to resolve a drug cartel money laundering investigation in 2012, was sued again this past February by families of the cartel's victims. (...) So-called regtech firms work in a constantly shifting regulatory landscape with many regional variations. Canada's Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) regime is supported by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. "Canada's AML/ATF Regime is continually reviewed to ensure that it remains effective and addresses the changing financial landscape, including the development of financial technology," Paul Duchesne, deputy spokesperson at Canada's Department of Finance, said. Jacqueline Shinfield, partner at legal firm Blake, Cassels Graydon LLP, who specializes in financial compliance agrees the regulations keep evolving. For example, "There are changes coming in June next year that deal with the requirement to determine whether or not the account holder is a politically exposed domestic person, as opposed to a politically exposed foreign person," she noted. As well, the Financial Transactions Reports Analysis Centre of Canada (FINTRAC), which enforces compliance with the AML/ATF, is looking into the growing number of financial technology startups to figure out which qualify as money services businesses. Financial Post, FP4

*** The CSIS spy who co-founded Heritage Front neo-Nazi group . . . and shares the story behind the stories**

Find the fence. Follow the fence. Find the spy. That's not terribly sexy work in the world of investigative journalism, but it is, in this stranger-than-fiction episode, the truth of how, in 1995, I tracked down Grant Bristow, a government agent who had infiltrated the Canadian neo-Nazi group, the Heritage Front. Bristow was now in hiding after allegations surfaced that the CSIS mole had instigated and funded many of the criminal acts he was supposed to be monitoring. He co-founded the hate-mongering Heritage Front and allegedly drew up lists of targets for the group, encouraging its members to spy on and harass prominent Jewish leaders, all while on the government payroll. After he was outed, the government took its spy in from the cold and hid him, allegedly for his protection. Finding Bristow had become an obsession among the ultracompetitive Toronto media. Now, courtesy of a source, I had a photograph of the disgraced spy, sitting in the backyard of his new house somewhere in Canada. Beside him, by a pinkish-white stucco post, a pair of crutches to one side. If I could find that fence, I could find Bristow. I had worked on the Bristow case for months, chasing multiple, fruitless sightings. I had compiled quite a bit of information on Bristow's time inside the Heritage Front, even his visit to Libya as a guest of Moammar Gadhafi, but I had drawn a complete blank as to his current whereabouts. Then came the lucky break. A man walked into the Star newsroom carrying photographs of Bristow, his wife and son, which he claimed had been taken at their new hideout, somewhere out west, possibly Calgary or Edmonton. CSIS had given Bristow a new identity, a new home and two brand-new cars, he said. Toronto Star, GT3

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Canada deports family to Ukraine as appeals fail

Canada deported a mentally ill 15-yearold boy to Ukraine Sunday night, despite medical evidence it is likely to trigger a second suicide attempt. Two border guards approached Vladyslav Zadorozhnyi the minute he arrived in the departures hall, and asked, as a formality, whether he is ready to go. "I don't know what to say," he said. "I feel very bad. Anxiety." Wearing a sporty zipup and a backpack, his hair carefully gelled, he was taken into the border security office with his mother Maryna Zadorozhna, 34, and his brother Andriy, 7. They arrived with the tearful parents of Vladyslav's new best friend, Alex, a classmate in his west Toronto school. (...) A key factor appears to have been Canada's late discovery of a fraud charge in Ukraine against Andriy. It was first mentioned by Canada on September 14 - more than a year after the family arrived, and a few days after the first scheduled deportation was cancelled at the 11th hour - in a letter from a senior immigration officer with the Backlog Reduction Office of Citizenship and Immigration Canada. Andriy denies being charged with fraud, and his refugee application includes clean police records checks. His counsel suggests the unspecified charge has been fabricated, and fits with the family's story about persecution by gangsters allied with crooked police, which a refugee tribunal

did not believe. In an emergency hearing Saturday, the family's lawyer Hart Kaminker argued the process has been procedurally unfair and below the legal standard of how Canada treats children. Canadian Border Services Agency is "acutely aware of the fragility of Vladyslav's health," and putting the family on this "roller coaster," with two deportations scheduled in as many weeks, is not being "alert, alive and sensitive" to the boy's best interests. Those three words were used by the Supreme Court of Canada, in the 1999 case of Mavis Baker, a Jamaican woman whose four children were born in Canada. The case made a child's interests a mandatory factor in any deportation decisions that affect the child. But it did not make them a "primary" consideration. That is the higher standard set by the United Nations Convention on the Rights of the Child, which Canada has signed. Vladyslav's file was reviewed by a doctor on behalf of CBSA, who disagreed with a psychiatrist and judged him fit to fly, with no communicable disease. CBSA also confirmed medical staff will be on hand in Kyiv. Postmedia Network (National Post, A3, Vancouver Sun)

*** Calgary mother and daughter who fled domestic abuse forced to leave Canada**

Two years after they came to the country to escape an abusive relationship, a mother and her daughter are being forced to leave Calgary and return to their home country on Monday. Ariunaa Demberel and her daughter Enky Ankhbayar came to Canada back in 2014 to escape from an abusive ex-husband. Demberel says he kidnapped and assaulted them before they made the decision to flee Mongolia, their home country. The pair applied for refugee status in hopes of staying here, but a judge ruled over the weekend that they would have to leave. In the ruling, the judge said there would be no 'irreparable harm' associated with the act of deportation and there no psychological harm posed to either of them. Demberel says she attempted to appeal to a federal court to put their deportation on hold, so Enky could finish her final year of high school in Canada, but that was not to be. "I don't want to break the law, so they told me to come to the airport tomorrow at 7:00, so I will be there and I have no plans. I don't know, I don't have any plans, I guess," she said. CTV News

Representatives for Chinese economic fugitives critical of extradition treaty talks

Alex Ning remembers the feeling of despair when a man he had helped represent returned to China to face embezzlement charges. Mr. Ning, a Vancouver-area immigration consultant, said Gao Shan "couldn't stand the pressure" after his father, brother and brother-in-law were detained by Chinese authorities for aiding and abetting. It was Mr. Ning's first case in which China sought the return of an economic fugitive. Today, Mr. Ning says he is helping about 30 others who are in the same situation as Mr. Gao. Mr. Ning said about half have been visited by Chinese authorities on Canadian soil. The other half, he said, have been pressed to return to China over the phone or online. The Globe and Mail reported last week that China's security services have been sending undercover agents into Canada on tourist visas to strong-arm expatriates to return home, including some suspected of corruption and other criminal activities. And with the Canadian government recently agreeing to negotiate an extradition treaty with China, representatives for some who have returned to the country in recent years to face criminal charges are criticizing the move – and noting there can be unpleasant surprises for those who go back.(…) He was ordered deported by this country's Federal Court after China provided several assurances, including that Mr. Lai would not face the death penalty. Mr. Lai was convicted on charges of smuggling and bribery in 2012 and sentenced to life in prison. "I don't think he anticipated that he wouldn't get proper medical care," Mr. Matas said in an interview. Mr. Matas said one of the assurances Mr. Lai received was that Canadian officials would be able to visit him in custody. However, Mr. Matas said he was later told by the Canadian embassy in China that the assurances did not apply post-conviction. Globe and Mail, A3 (2016-09-25)

*** Border officials kept busy in August**

Americans continue to run afoul of Canadian law when they try to enter Alberta. But dozens of would-be visitors – some of them convicted criminals – were refused entry during a busy August at southern Alberta's border crossings And two of them were teenagers who may have arrived at the Coutts crossing by accident. Officials with the Canada Border Services Agency say it was the undeclared guns – a pistol, a rifle and a shotgun – that first raised the alarm. Then the officers learned the two had been reported as missing children, who may not have realized they were about to leave the U.S. They were arrested and turned over to American authorities to be returned to their parents. Lethbridge Herald

Guns, throwing stars among weapons seized at border
Border officials are reminding travellers to leave their weapons at home after guns and bladed throwing cards were seized at local crossings last month. An Ontario man is facing charges after he was caught transporting throwing stars, knives and knifed throwing cards at the Windsor-Detroit Tunnel. The Canada Border Services Agency said the man was crossing through the tunnel on Aug. 16. Officers located and seized the throwing stars, knife throwing cards and knives in a plastic bag in the vehicle's trunk under several layers of personal goods. The vehicle was seized as penalty and the man was arrested and charged. (…)On Aug. 10, an Ontario resident and NEXUS member was referred to secondary inspection regarding importing a classic car with a declared value of US$20,000. Research revealed the purchase price of the vintage car was actually US$85,250. The man was arrested and released. He will appear in court next month. On Aug. 4, a man from Michigan was referred to secondary inspection at the tunnel where officers discovered a firearm under the passenger seat, .5 grams of marijuana and four amphetamine pills. The gun and drugs were seized and the man was arrested. He was scheduled to appear in court on Sept. 12 but did not attend. A warrant has been issued for his arrest. On Aug. 10, a man arrived at the tunnel to inquire about his admissibility for future trips to Canada. During the course of the exam, the man admitted to not declaring a firearm and ammunition which were located in the vehicle. Officers also located pepper spray and a switch blade. He was arrested and the weapons were seized. Windsor Star, A3

*** Windsor man at centre of 1999 human trafficking case denied bail**
A Windsor man who fled to Canada rather than face time behind bars for 'alien trafficking' in the United States has been denied bail. American court documents reveal that in 1999 Sang Thanh Nguyen was stopped by the Coast Guard while travelling by boat between Amherstburg and Michigan. Eleven "Chinese aliens" were found aboard the boat and Nguyen was arrested and charged with human smuggling. At the time he pleaded guilty and agreed to spend 15 months in prison, but he did not appear at his sentencing hearing and instead absconded to Windsor where he lived and worked for 17 years. (…) During those years American authorities did make some efforts to find Nguyen, but according to information read in court by Superior Court Justice T.J. Carey, they were under the incorrect impression that Canada wouldn't sign an extradition order for human smuggling. "One is a little astounded when the U.S. is visible outside this courtroom window and authorities are in offices a few kilometres from here, that nobody picked up the phone," said Carey. In 2015 Canadian authorities alerted their American counterparts that Nguyen was in the country, because of suspicions that he may have been active in human trafficking again, although there was no evidence disclosed that he was. An extradition order was signed and Nguyen was arrested on August 11. Windsor Star, A6

Migrant workers caravan hits Toronto en route to Parliament Hill
As symbols go, the schedule of the "Harvesting Freedom Caravan" that hit Toronto on Sunday could hardly have been better designed. Activists campaigning for an end to exploitation of migrant workers in Canada set out on Labour Day weekend from the Ontario town of Leamington, home to the largest concentration of agricultural greenhouses in North America. They aim to conclude in Ottawa - where they say the problem must be addressed - just before Thanksgiving weekend, when Canadians across the country will be preparing to chow down on what the caravaners describe as the fruits and produce of injustice. On Sunday morning, the caravan protested outside the Ontario Food Terminal. And in the afternoon, at Ryerson University, leaders attended a screening of director Min Sook Lee's jarring documentary Migrant Dreams. It was all part of a campaign asking Canadians to consider where, how and by whom the food they enjoy is picked and packed. (…) At the rally, farm workers - including Gabriel Allahdua, a 45-year-old father of two from St. Lucia who works in Leamington - spoke about the conditions they endure under the temporary foreign workers program. Allahdua, carrying protest signs shaped like pumpkins and apples, told the Star later that the problem is rooted in government laws and policies. "In Canada, if you have no status you have no rights. And if you have no rights it means that you are vulnerable. And because we are vulnerable, we have been exploited." Critics say the federal Seasonal Agricultural Worker Program is 50 years old this year and long past due for wholesale reform or replacement. For half a century, producers have been profiting and Canadians have been dining out on the sweat and misery of migrant workers treated as disposable labour, caravan organizers said. Toronto Star

B.C. urges Ottawa to fix tech talent gap

B.C. Premier Christy Clark is pressing Ottawa to open the floodgates for high-skilled foreign tech workers to immigrate to Canada, saying her province's burgeoning tech sector faces an acute shortage of talent to fill thousands of jobs. (...)The Premier's call adds to those from technology companies across Canada who have put pressure on the Liberal government to speed up and streamline the immigration process so they can more readily recruit top foreign talent. They say that unless the government dramatically shortens visa-processing times for foreign programmers, researchers and tech executives, they will lose out to other countries for talent needed to help grow their business and create jobs here. (...)Streamlining the [immigration process] and increasing total immigration "makes a world of sense" for his and other companies. Mr. Booth and other Canadian tech executives have made their case in recent weeks directly to Immigration Minister John McCallum to streamline the immigration process in round tables in Ottawa, Toronto and Vancouver organized by the Council of Canadian Innovators, a lobby group representing emerging Canadian tech firms. Globe and Mail, B1

* **Dion's stance confusing: critics**

Foreign Affairs Minister Stéphane Dion sowed confusion and showcased cracks in Liberal ranks when he angrily denied recently that negotiations are under way on an extradition treaty with China, critics say. One federal official said that Mr. Dion was simply flustered about semantics when he denied the launch of talks: "Preliminary discussions are a precursor to negotiations and those discussions have only just begun. "Still, another senior Liberal added, "I'm not clear what [Mr. Dion] was trying to say. "In a telephone interview with The Globe and Mail on Friday, Mr. Dion insisted there are no negotiations in the works that could see Canada return Chinese fugitives accused of economic crimes. "Your paper should check the facts. There is no negotiation. To write like pretending it is, it is wrong. Stop that please," Mr. Dion said. When asked what kinds of specific guarantees the Canadian government would demand with a formal Chinese extradition treaty, Mr. Dion again became testy. "We never extradite people to countries who have the death penalty. Your question is unfair because never the government of Canada would do such a thing. And why you are implying that is beyond me. That's my answer to your question." However, Canada has returned more than 1,400 Chinese nationals since 2009, most of whom were involved in illegal immigration. In addition, Canada has an extradition treaty with the United States, although Ottawa insists on receiving assurances that people will not face the death penalty if they are sent back to face the American justice system. Globe and Mail, A6

Don't wait to improve borders

Fewer than two months remain before elections in the United States, and public interest in Canada is riveted on the campaign for president. It's important, however, not to lose sight of the opportunities our governments still have to make progress on issues vital to the future of our economic relationship - progress that can and should be made before the end of the presidency of Barack Obama. Now, more than ever, Canada should be making a concerted effort to ensure initiatives undertaken during the past several years to improve the security and efficiency of our borders and eliminate costly and unnecessary regulatory impediments to business between our two countries can be shown to have benefits that will sustain them during the next administration.(...)Strengthening border security, eliminating costly and needless regulatory impediments to trade and focusing on outcomes such as improved health, safety, environmental and consumer protection while making government more efficient are worthy objectives regardless of the political stripe of the next president. Bilateral priorities don't change when governments on either side of the border change. If Canada waits until a new administration is in place in Washington, a great deal of momentum, goodwill and opportunity will be lost. This is the time to demonstrate agreements that have mutual economic benefits are possible to achieve. Now is a good time for both governments to reaffirm publicly their commitment to work together to improve border and regulatory management. Winnipeg Free Press, A7

* **The driver who fled as a girl lay dying**

An opinion piece states, "Kara Parman lay dying in the road. The 7-year-old Toronto girl was crossing the street to buy some candy when she was struck by a car. The driver sped off. It was Nov. 22, 1993. Kara, a Grade 3 student, died after lingering in a coma for five days. Police set up a special squad and launched a massive dragnet to catch the driver. I was searching for him, too. I worked day and night, following a tip that he might have been a Portuguese immigrant. I knocked on doors across Toronto's

Portuguese community: body shops, cafés, neighbourhood parties. Like the police, I was coming up with nothing. The trail went cold for more than a year. (...) I went back to Portugal and accompanied Jose Fernandes Castro to Canada. When we arrived at Pearson airport on March 2, 1995, two RCMP officers came aboard and arrested him. He was carrying a letter from his priest and another from his mother to Kara's mom. Castro, sentenced to a year in jail, was released after eight months and immediately deported to Portugal. The story garnered international headlines and praise from my employer, colleagues, the police and Kara's mother, Karen, who went on radio and television to thank me for bringing closure to her nightmare." Toronto Star, GT3

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Spy chief issues encryption warning**

The head of Canada's electronic spy agency warned Friday the advent of super-fast quantum computers will cripple current encryption methods for securing sensitive government and personal information within a decade. In a rare public speech, Greta Bossenmaier, chief of the Communications Security Establishment, said cryptologists at the CSE and around the world are racing to find new cryptographic standards before Y2Q - years to quantum - predicted for 2026. She was the third senior CSE official in less than a week to warn publicly of the threat quantum computing poses to widely used public key cryptography (PKC), protecting sensitive data transmissions from hackers, hacktivists, foreign state spies and other malicious actors. The CSE is best known as a spy agency - it collects, decrypts and analyzes phone calls, faxes, emails, tweets, satellite and other electronic signals emanating from adversarial foreign nations and overseas threat actors. But it's also mandated to protect government computer systems and networks, and the information they carry. Already, federal computer systems are "probed" more than 100 million time a day by suspected malicious actors searching for vulnerabilities. Now, "the challenge of protecting systems is about to get a lot harder thanks to quantum computing," Bossenmaier told an Ottawa conference of the Canadian Association for Security and Intelligence Studies. Postmedia Network (Kingston Whig-Standard, B1, Ottawa Citizen)

Spy agency exec calls for debate on encryption

Canadians are being encouraged to ask more questions about the security of their electronic devices from an unlikely source - an executive at the country's electronic intelligence agency. Scott Jones, the deputy director of IT security at the Communications Security Establishment (CSE), said Canadians need to start taking a greater interest in how their electronic devices protect personal information. "We should be asking when we go and buy the stuff we have at home, OK, tell me how it's being protected," Jones said in an interview. "If it's my cellphone, does it have encryption if I lose it? Can somebody just read the data off of it or not? We need to start asking questions like that ... We need to start helping each other, and helping citizens, helping businesses, helping the government. When we're buying these products, they need to be secure by default." It may come as a bit of a surprise to hear an employee at CSE counselling Canadians to protect private information. The agency was thrust into the spotlight after U.S. whistleblower Edward Snowden's disclosures. CSE is part of the Five Eyes security alliance, which includes spy agencies in the U.S., the United Kingdom, Australia and New Zealand. Snowden's disclosures revealed the mass surveillance programs used by those countries, including programs that scooped up their own citizens' data. Jones's comments also come as law enforcement agencies in the U.S. and Canada are forcefully arguing for the need to limit encryption - calling for so-called "back doors" that would let authorities decode citizens' data. The argument is that encryption helps bad guys - terrorists, organized crime, child pornographers - hide their tracks. The everyday uses for encryption, such as protecting credit card transactions, safeguarding personal messages, or protecting sensitive government documents, are brought up less often. Toronto Star, A4

*** Les grands enjeux**

(...) En juin 2015, environ 1400 passagers du transporteur polonais LOT ont été coincés à l'aéroport Chopin de Varsovie en raison d'une cyberattaque touchant 10 avions. De tels incidents demeurent rares même si chaque mois, les systèmes informatiques aériens du monde subissent en moyenne 1000 cyberattaques, selon l'Agence européenne de la sécurité aérienne. Des experts vont jusqu'à prédire que le prochain gros attentat terroriste sera le fait de pirates informatiques. Après l'adoption d'un plan d'action

en 2014, l'OACI demandera à ses pays membres d'avaliser une résolution leur enjoignant de redoubler d'efforts en la matière. La Presse

*** American spies get wireless devices**
U.S. spies are catching up to the masses in their gradual embrace of 21st-century technology, from installing wireless connections in secure facilities to wielding iPhones and tablets, according to an official with the U.S. National Geospatial-Intelligence Agency. "We'd be cutting off our noses to spite our faces by denying us those kinds of tools," Matt Conner, deputy chief information security officer of the agency, said. The NGA provides intelligence to other parts of the government from battlefield maps to satellite imagery of national disasters. It's among agencies that are working with the Director of National Intelligence to study how to maximize the use of secure wireless networks and devices, while still maintaining the cover that spies need. Bloomberg News (National Post)

*** Yahoo email hack: Are biometrics the answer to a safer online world? Not yet, says expert**
Yahoo admits that 500 million of its email accounts were compromised in 2014. Ransomware attacks lock or cripple hospitals' computer networks unless they hand over a massive payout. Actors and celebrities' websites are hacked, or nude photos are stolen and spread online. Oh, and your antivirus programs aren't solving the problem.. The flood of headlines suggests the frequency and severity of cyberattacks is getting worse, instead of better. Are the tools we're using to keep our personal information secure keeping up? Technological advances in security measures are slowly gaining traction. Biometrics, especially, have grown in popularity. By scanning your fingerprint, retina, or even listening to your heartbeat, devices can identify you with data that's unique only to you - and without the hassle of remembering and managing multiple passwords over dozens of services. It sounds like a promising, password-free future. But Eldon Sprickerhoff, chief security strategist of Cambridge, Ont-based cybersecurity firm eSentire, warns that it will be a long time before any single method can supplant traditional passwords as the preferred method of locking down your online accounts. CBC.ca

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Waterloo Regional Police take extra precautions to avoid drug exposure during investigations: Inspector**
Local police officers are taking more precautions during drug seizures and when helping those who have overdosed because of the dangers involved in even inadvertently touching certain drugs, the head of Waterloo Regional Police's strategic and tactical services division says. "We've had to do some significant changes even just within our own service here in regards to the handling of those drugs once they're seized just because of the relative danger of them," Insp. Dave Bishop told CBC News. (...)The RCMP released a video earlier this month warning about the dangers first responders face when it comes to fentanyl. "The danger this drug presents to all Canadians cannot be overstated," RCMP Commissioner Bob Paulson said in a release. "It's spreading across the country, leaving a trail of misery and death, and first responders and the public need to know that even being near it can make you sick, or worse." The video tells the story of Const. Rob Dupuis in Kamloops, B.C., who found a man slumped over the steering wheel of his vehicle. The man was arrested, Dupuis put him in the cruiser and then went back to search the vehicle. "I noticed there was a bit of a chemical smell," Dupuis said. He started to feel lightheaded and nauseous, so he asked the man what he had in the car and the man said it was fentanyl. Dupuis had a urine test and it found he had trace opioids in his system. "The traffic stop is one of the most dangerous things that we'll ever do in our career because of the unknown. Now adding fentanyl to the mixture, you're stopping a vehicle and you think it's drugs and you're looking at it and you go, 'Oh wow, that looks like cocaine or heroin,' you just don't know anymore," he said. CBC News

100 fallen officers honoured at annual memorial
No names were added to the roll of 100 fallen officers remembered Sunday at the Alberta legislature during the Police and Peace Officers' Memorial Day ceremony. But for those whose loved ones fell in the line of duty, the occasion was still a bittersweet one. (...) We're always very fortunate when we don't have to add another name to the memorial," said Alberta Justice Minister and Solicitor General Kathleen Ganley. "We're really grateful for that but there are many families here to mourn those that they have lost

so it's still a very sad day but an important day to remember the service provided to all Albertans," she said. Deputy Commissioner Marianne Ryan, commanding officer of RCMP in Alberta, said the day is an emotional reminder that officers put themselves in harm's way every day. She pointed to massive wildfires earlier this year that forced the evacuation of communities in northeastern Alberta including Fort McMurray. "When the wildfires first struck, I was immediately advised that our officers were running towards subdivisions banging on doors trying to get people evacuated," she continued. "While the firemen did an outstanding job of fighting the fires, our folks did an outstanding job of keeping people safe ... at great personal risk both for themselves and knowing that their homes were likely in the path of the fire and not knowing where their own families and children were. Postmedia Network (Edmonton Journal, A1, Edmonton Sun, Calgary Herald); The Telegram; Postmedia Network (Leader-Post, StarPhoenix); Winnipeg Sun

Fallen Island Mountie added to honour roll

As he concluded the ceremony Sunday in Vancouver's Stanley Park, Chaplain Jim Turner told those attending the British Columbia Law Enforcement Memorial that, by this time next year, he hopes for one thing. "It is my prayer that, by this time next year, we will have no more names to add to the honour roll," Turner told the crowd. The annual ceremony is well attended by representatives of B.C's law enforcement and public safety community and their counterparts in the United States. The new name Turner was talking about was the Const. Sarah Beckett of the RCMP's West Shore detachment on Vancouver Island, who was killed April 5 when her police cruiser was hit by a pickup truck in a Langford intersection. (...) Beckett's name also was added to an honour roll, cenotaph and memorial wall at the RCMP's national memorial service for fallen members Sunday. The memorial ceremony is held annually at RCMP Depot Division in Regina, where the force's academy is located. The addition of Beckett's name to the memorial brings the total number of fallen members to 237 since the creation of the North-West Mounted Police in 1873. During the Vancouver ceremony, RCMP Deputy Commissioner Craig Callens said a death among the ranks is a burden on everyone in the force. "We are here to honour those police office who have made the ultimate sacrifice," said Callens. "Fresh in our minds is Const. Beckett," he said. "I can tell you Sarah exemplified the very best." Postmedia Network (Vancouver Sun, A9, The Province); CBC News; Agence QMI (Journal de Montréal); * Radio-Canada

Too much talking, cellphone use, during federal 'lockdown' exercise, report says

A "lockdown" exercise designed to test whether federal workers know what to do if a gunman ever stormed their Ottawa office building was marred by too much talking, too many ringing cellphones and too many hiding spots that were too visible. "Employees at all levels were heard talking while they were hiding," says an internal report on the March 30, 2016, exercise. "Remind employees to stay quiet to prevent the aggressor from knowing where they are hiding." The fake "lockdown" was conducted this spring just a few blocks from Parliament Hill, where a real gunman had stormed the Centre Block and started shooting on Oct. 22, 2014. The gunman died in a shootout, after killing a soldier at the National War Memorial and injuring a House of Commons guard. (...) Local police, RCMP and the office workers themselves were given plenty of notice for the 2 p.m. ET exercise, and were told how to behave over the eight minutes that a faux gunman was supposedly roaming the halls looking for victims. But the concept seemed to be poorly understood, or not taken seriously, by significant numbers of participants. "Cellular telephones could be heard ringing in hiding areas," says the report. "Remind employees to participate fully in the exercise by turning off their electronic devices." Observers also noted that the glow from cellphones could tip an "active shooter" to the presence of a hiding worker. "RCMP Protective Policing recommends that cellular telephones be turned off during an incident and this approach will be evaluated." CBC News

*** Bomb threats force Mohawk College students out of their dorms**

A series of bomb threats forced students to evacuate their dorms at Mohawk College on Sunday night. The phone calls came at about 9 p.m., Hamilton police said. McMaster University and Joseph Brant Hospital in Burlington were also targeted. However, all locations were checked and nothing was found. Students have since been allowed back into their dorms. The bomb threats come days after similar incidents in P.E.I., Nova Scotia, Manitoba and Nunavut. Last week, every single school in Prince Edward Island was evacuated due to a bomb scare, sending parents scrambling. RCMP spokesman Sgt. Kevin

Baillie said a fax was sent to Ottawa RCMP Wednesday morning from someone threatening to detonate bombs at several schools. City News

Police investigate five more bomb threats
The woman running for mayor of Halifax wants "big consequences" for those making fake bomb threats after five more hoax calls this weekend. Mayoral candidate Lil MacPherson said Sunday these calls are wasting emergency resources. "This is unacceptable in this city," said MacPherson. "These people are taking away special services that will be going to people who really need them." (…) On Sunday, five separate bomb threats were reported to police during the early morning hours. The RCMP say they received an anonymous call at 1:30 a.m. from a male who claimed he was in the parking lot of Cole Harbour Place with bombs and a hunting rifle. Police immediately cordoned off the area but found nothing. Shortly after 2 a.m., the RCMP office received an anonymous, automated phone message saying there was a bomb at Halifax Stanfield International Airport. Halifax Regional Police and the RCMP Police Dog Service conducted a search and also found nothing. Around the same time, Dalhousie University received a threatening automated phone message. Chronicle Herald, A5; Canadian Press (Winnipeg Sun, London Free Press, Edmonton Journal, National Post, StarPhoenix, Windsor Star, Montreal Gazette, Vancouver Sun, Calgary Herald, Leader-Post, Ottawa Citizen)

Targeted Surrey shooting sends two to hospital
Two people are in hospital after an apparent targeted shooting in Surrey on Sunday. Surrey RCMP were called to a home in the 4200-block 152nd Street after learning of the incident. When police arrived, they found the adult male and female residents of the house suffering from non-life-threatening injuries. The victims were taken to a local hospital via ambulance. Vancouver Sun

Royal Visit
Vancouver came together Sunday to give the Duke and Duchess of Cambridge a welcome so warm that it felt like a truly Canadian embrace - respectful, enthusiastic and multinational. Vancouver showed up bearing flowers, wearing cocktail dresses and dress shirts, tiaras and Union Jacks, and replicas of Diana's exquisite sapphire ring. We also came carrying hand-written signs that pleaded our causes: reconciliation, climate change, fisheries and the environment, pipelines and PTSD - and if the royal engagements of the day are any indication, that's exactly the way the duke and duchess want it to be. At every stop, with Prime Minister Justin Trudeau and his wife, Sophie Gregoire Trudeau, serving as escorts, the duke and duchess walked a fine line between the glamour and drama, the glitter and grit. (…) RCMP officers conduct a sweep as hundreds of people wait to greet the Duke and Duchess of Cambridge before their arrival at the B.C. Legislature in Victoria, B.C., Saturday, Sept 24, 2016. Vancouver Sun

*** Crossfield not moving forward with security cameras**
Town-operated security cameras will not be going up in Crossfield. Discussions about the feasibility of security cameras has been a recurring topic in council since Chief Administrative Officer Ken Bosman spoke of the Town's "future technological vision" at a meeting May 17. During its Sept. 20 regular meeting, council agreed it was clear both residents and RCMP were not in favour of the matter following a Sept. 15 open house surrounding a proposed Video Surveillance Cameras in Public Areas policy. "I think we've heard from the people that security is important to them, but this is not the right solution," Bosman said. According to Councillor Hadi Feltham, much of RCMP's concern regarding the use of surveillance video is that most incidents occur between midnight and 4 a.m. when recording conditions are poor. Mayor Nathan Anderson said if RCMP didn't have faith the security cameras could be utilized effectively, there was no point in continuing to pursue the effort. "People said they didn't want it (and) RCMP said it wasn't useful, so my thought is that we're not moving ahead with it," he said. Feltham said the RCMP recommended Crossfield invest in a second peace officer or more enhanced policing shifts rather than security cameras. Rocky View Weekly

*** Vancouver fintech named criminal organisation by US**
US authorities have named a Vancouver fintech called PacNet Group a "significant transnational criminal organisation" and is seizing its U.S. assets. The US Treasury Department's Office of Foreign Assets Control (OFAC) alleges the PacNet Group has been involved for years in criminal activity, including money laundering and facilitating mail fraud. "PacNet has knowingly facilitated the fraudulent activities of

its customers for many years, and today's designations are aimed at shielding Americans and the nation's financial system from the large-scale, illicit money flow that are generated by these scams against vulnerable individuals," OFAC acting director John Smith said in a press release. It's not known yet if the RCMP have been involved with the investigation that led the OFAC to list PacNet and its affiliates as a transnational criminal organisation, or if the network is even on the RCMP's radar. The allegations have not been proven in a Canadian court or confirmed by Canadian police. South China Morning Post

Will Ft. Simpson situation lead to reflection?
An editorial states, "Where small communities are concerned, bad news almost always travels faster than good. That was certainly the case when Const. Akira Currier arrested Wrigley's Daryl Sibbeston on Fort Simpson's main drag at lunch time on a busy Friday afternoon. It's been just over a year since Currier moved to Fort Simpson. In that time, he's become a familiar face at the schools, helping out with the end-of-school bike rodeo that took place in June, coming out to check stops and even participating in last year's barbecue for Family Violence Awareness Week. Now, on the eve of that same week this year, his Sept. 9 arrest of Sibbeston has left the Wrigley man with a black eye and a bloody face. It was a metaphorical black eye for RCMP, as well - witnesses say Sibbeston was intoxicated at the time of his arrest but they also say he was alone and not causing trouble when the RCMP pulled up. People are entitled - obligated, even - to ask questions and criticize the RCMP officer's methods when they hear such accounts, even after the RCMP charged (…) It is unfortunate that the RCMP's good deeds in the community are now tainted in the eyes of many. Initiatives to combat impaired driving, drug busts, safety training and anti-bullying initiatives for the community's children and youth should not be overshadowed by Sibbeston's arrest." NWT News

Bomb hoax at P.E.I., N.S. schools reminds us of valuable lesson
An editorial states, "Last Wednesday, briefly, there was an international news story out of the Maritimes, featured prominently on the 'front' home pages of CNN and BBC news websites. Many citizens may have rapidly forgotten about it since the whole thing quietly slipped out of view, being one more apparent hoax in a jittery western world. (…) The RCMP wasted no time responding and evacuating schools, getting students to safe pickup points. The school system's plans for such emergencies worked well too. That nothing was exploding, or had exploded, helped, but the organization was clearly there and impressive. That's good, because as the international media attention indicated, **terror** can strike anywhere, anytime, and when least expected. That's what makes it terrifying." Times & Transcript, A8

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Sex offender sent back to prison
A 54-year-old sex offender who was living at the Henry Traill Community Correctional Centre, on Bath Road across from the Frontenac Mall, has been returned to prison for failing to disclose what he claims was a simple friendship with a Kingston woman. John R. McCauley pleaded guilty in Kingston's Ontario Court of Justice to violating a condition of a 10-year, long-term supervision order imposed on him in January 2002, which requires that he report all relationships, platonic or otherwise, to his parole officer. He was given enhanced credit on 163 days of pretrial custody and sentenced to a further 957 days in lock-up, a little more than two years and seven months. Justice Larry O'Brien was told that McCauley served a five-year federal sentence for sexual assault before being released initially on his long-term supervision order. However, according to Crown attorney Ross Drummond, the supervision order was suspended in August 2013 after McCauley was convicted of criminal harassment and sent back to prison for another 27 months. In January 2015, he was released again from Warkworth Institution and sent to Henry Traill - a federal halfway house operated by Correctional Service Canada - to resume long-term supervision. It was impressed on him that a key condition of his supervision was reporting all friendships and relationships so his pertinent offence history could be disclosed. Kingston Whig-Standard, A1

Breaking bad: These eight broke parole, now the cops need your help finding them
They did the crime, and they did some time ... then decided they'd been punished enough. Many of this month's Crime Stoppers Most Wanted were granted early release then are believed to have violated their parole conditions and left their court-appointed residences. If you know where they're hiding out, contact

Crime Stoppers - they pay cash for tips that lead to an arrest. Kayla Allen, 29, was to serve two years after being convicted of break and enter and drug possession. Instead she was released early on June 10, 2016. (…) Jesse Thompsett, 25, was charged and convicted on several offences including aggravated assault, and received a three-year jail sentence. He was given early parole on Aug. 22,2016, but only two days later he breached his conditions of release and has disappeared. There is a Canada-wide warrant in effect. Jason Moar was handed 31 months upon conviction of manslaughter. He was however deemed a good candidate for early release and started parole on Aug. 4, 2016. Moar, 24, made it till Aug. 30 before breaching his conditions. His current whereabouts is unknown and a Canada-wide warrant has been issued. Winnipeg Sun

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Sextortion of children on the rise**
Canadian cases of online sex-related extortion — "sextortion" — against children are increasing, following trends in the United States. U.S. federal officials and advocates are urging educators and parents to help raise awareness at school events. In sextortion cases, preying adults typically pose on social media as someone younger to coerce victims into sending inappropriate photos or video clips. Once initial images are delivered, the adult threatens to expose them publicly unless the victim sends more explicit pictures. The Canadian Centre for Child Protection reported that in 2012, the organization received three cases of sextortion cases a month through its Cybertip.ca line. Now, it receives upwards of 15 a month. Last September, the centre said it saw a spike of 40% in teen sextortion tips in a six-month period. Toronto Sun

*** Awareness week against cyberbullying, online exploitation kicks off in Quebec**
Sunday marks the beginning of an awareness week to teach kids and their parents how to handle intimidation and violence, and Sûreté du Québec wants them to be aware of the resources available to combat cyberbullying and sexual exploitation. The SQ says these issues have grown in recent years thanks to new technology. And as much as these things happen in a virtual world, the criminals acts have real victims. (…) Youth and their parents can find out how to manage risk and what actions to take when they have been the victim of cyberbullying. Anyone can signal a concern about the sexual exploitation of a minor to Canada's tipline to report the online sexual exploitation of children at cyberaide.ca. Montreal Gazette

*** Sex Slavery Thriving On Facebook And WhatsApp. Mark Zuckerberg, Are You Listening?**
An opinion piece states, "Sex slavery is very real today, even though International Law says it's illegal in every country of the world. In fact it is so real, that according to the Global Slavery Index, "45.8 million people are in some form of modern slavery in 167 countries", as of 2016. Just let that truth sink in. According to findings made by the report, 58% of those enslaved live in India, China, Pakistan, Bangladesh and Uzbekistan. This doesn't mean that the slate for other countries is clean. Luxembourg, Ireland, Norway, Denmark, Switzerland, Austria, Sweden and Belgium, the United States and Canada, and Australia and New Zealand fall into the category of lower estimated prevalence. Yes, the international law prohibits slavery. And yet, slavery is very, very existential. We're in the 21st century—the digital age. And slavery is as prevalent as it was in the dark ages. It's just the medium that has changed now. Technology—the boon of our lives; that's what organisations like the ISIS and Boko Haram are using to facilitate the trade, no holds barred. In fact, the Islamic State has openly advocated the revival of sex slavery, without any fear whatsoever. We could debate over why they have no fear. But, there isn't much of a debate, really." MensXP

2 free passes show flaws in system
An opinion piece states, "A teen from a village near Fredericton was granted a conditional discharge some time ago for a break-in at an area school, which meant he would have no criminal record for the crime. While this might irk some, it was a just outcome, as the offender had no prior record, and the philosophy that young offenders ought to be given chances and that the system should focus on rehabilitation for them, is a sound one, entrenched in our Youth Criminal Justice Act. However, it's not a

perfect piece of legislation, as a recent development for the same offender demonstrated. The same young man, now an adult, was in court in Fredericton recently to be sentenced for another break-in committed when he was a minor, this one at a church. The glitch in the case arises from the fact the church burglary occurred before the one at the school, meaning the young man, whose identity is protected by the Youth Criminal Justice Act, appeared as a first-time offender for the second time. As a result, he was once again given a conditional discharge. Two break-ins. Two investigations. Two guilty pleas. And technically, zero convictions. (…) The fault lies with the Youth Criminal Justice Act. Its focus on rehabilitation of youths is an honourable one, just as it was for its predecessor, the Young Offenders Act. (…) Ottawa needs to revisit this legislation and ensure it's serving all of society, not just kids who have gone astray." Daily Gleaner

Un sédatif pour éléphants, la nouvelle «drogue du jour»
Les autorités craignent qu'un sédatif pour éléphants, 10 000 fois plus puissant que la morphine et ayant déjà fait des victimes aux États-unis, ne fasse son apparition dans nos rues. «C'est très inquiétant, parce qu'on voit déjà une vague de surdoses avec de nouvelles drogues, comme le fentanyl. Donc, le fait que le carfentanil puisse s'ajouter à ça... On risque d'avoir davantage de surdoses», a averti Jessica Martel, du Groupe de recherche et d'intervention psychosociale (GRIP) de Montréal. Le carfentanil, un tranquillisant utilisé depuis longtemps pour endormir certains gros animaux comme les éléphants, semble depuis peu être devenu l'ingrédient secret des chimistes clandestins. Ce sont surtout les consommateurs d'héroïne qui sont à risque, puisque du carfentanil y est mélangé pour «couper la drogue». La plupart en consomment à leur insu. «C'est dangereux, parce qu'il suffit d'une erreur de dosage pour que ça entraîne une mort par surdose», craint Jean-François Mary, directeur général de l'Association québécoise pour la promotion de la santé des personnes utilisatrices de drogues (AQPSUD). En effet, selon la GRC, 20 microgrammes de carfentanil (un poids moindre que celui de quelques grains de sel), peuvent être mortels. Selon Santé Canada, le carfentanil n'aurait fait son entrée au pays sur le marché clandestin que cette année. Les autorités ont effectué en juin dernier une première saisie à Vancouver. Journal de Montréal, 3 (Journal de Québec)

Victim was a suspect in 2014 killing
The man shot dead in a hail of gunfire outside a troubled westend eatery Sunday morning in the city's second weekend homicide was once under investigation for his suspected role in the 2014 unsolved killing of Jabeir Jemmie. Abdi Jama, 26, also known by the street name "Ajax," was shot multiple times around 6 a.m. in a Shillington Avenue parking lot where a large group had congregated. Jama had previously been inside eatery The Suya Spot, long heralded by nearby residents and police as a problem area. The restaurant is well-known to anti-gang and drug officers for its clientele. Police believe Jama's death is gang-related. (…) Ottawa police said they are very concerned about the escalating gun violence in the city. "We are obviously seeing an increase in gun violence," Duty Insp. Sean McDade said. "We're very concerned for public safety." Coun. Rick Chiarelli, in whose College ward Thompson was killed, said he wants to know if the issue is one of police resources and thinks it's time to revisit talks about police budgets and officer allocation. "It's kind of a wake-up call to everybody in the city," Chiarelli said. "And we have to help police get control of the situation in all parts of the city. You get fear being struck in the hearts of people across the city." Ottawa Citizen, A1

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Native leader to support families in new role
Francyne Joe remembers her eighth birthday, not for the McDonald's restaurant in Kamloops, B.C., where it was spent with friends, but rather for what she saw en route from her home on Lower Nicola reserve. She spotted her 12-year-old cousin, Monica Jack, riding her bike along the highway. It was May 6, 1978 - the last day Monica would be seen alive. In the years since, Ms. Joe has travelled that stretch of road, one of several B.C. highways notorious for the alarming number of indigenous women who have disappeared or died violently along them. On Saturday, Ms. Joe was appointed interim president of the Native Women's Association of Canada (NWAC), taking on the role just weeks after the historic launch of

a national inquiry into Canada's missing and murdered indigenous women and girls. (…) NWAC was at the fore in pressing for the long-sought national inquiry, and it will undoubtedly play a key role as the commission carries out its work over the next two years. Ms. Joe said her priority will be ensuring that victims' loved ones are heard and supported. "We need to ensure that the inquiry is going in the direction that the families want," she said. "The children of these victims need as much support as they can get." She also said she intends to continue pressing for an independent civilian body that would review cases where the quality of the investigation has come into question. She plans to raise the issue with federal ministers, as well as with the RCMP and the Canadian Association of Chiefs of Police. Nearly one month into the inquiry, Ms. Joe said she had expected more to have been done. There is no website or phone line for victims' families to call with questions or concerns. Globe and Mail, A13

*** First class lawyers: Lakehead's new graduates embody its small-town, northern, Indigenous focus**

Canada's newest law school opened in northern Ontario in 2013 with a unique commitment to teach about small-town practice, natural resources and environmental issues and, not least, Indigenous law. This week, the first graduates of Lakehead University's Bora Laskin Faculty of Law are among those being called to the bar at a Law Society of Upper Canada ceremony in Toronto. (…) In the first cohort, four students self-identified as Indigenous while another four have Indigenous roots-a modest start on Laskin's ambitions to recruit future First Nations, Metis and Inuit lawyers. "This is a marathon, not a sprint," says dean Angelique EagleWoman, the first Indigenous woman to head a law faculty in Canada. Her faculty is expanding its outreach efforts this fall. Already, some Laskin graduates see themselves as agents of change following last year's recommendations of the Truth and Reconciliation Commission and a newly established federal inquiry into missing and murdered Indigenous women. Macleans

*** Trek in memory of missing/murdered women**

Joseph Alfred Beaver is walking from Athabasca all the way to Terrace, B.C., in memory of murdered and missing aboriginal women. The 71-year-old from Calling Lake had breakfast Friday morning at the Grande Prairie Friendship Centre before setting out again, followed by about 25 women who were seeing him off. Beaver said he'd originally planned to go to Fort St. John, but he decided to extend his trek to Terrace B.C. so that he could walk the Highway of Tears, the name given to the stretch of Highway 16 where nine women – all but one of them aboriginal – were murdered between 1989 and 2006. "The idea for this memorial walk didn't happen overnight; I've had several relatives that went missing over the years," Beaver said. (…) Beaver said he supports the newly established inquiry on missing and murdered Indigenous women, which started Sept. 1 and goes until Dec. 31, 2018. "I have to say thank you to the Prime Minister for creating the inquiry. Now, I hope something does come out of it, not just spending millions of dollars." Beaver would like to a see a memorial on B.C.'s Highway 16. Daily Herald Tribune (2016-09-25)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Are we ready for neighbourhood sales of pot? Hell no, say worried parents**

Pretty soon, marijuana will officially be wonderful. God help us. There was a revealing story in Friday's Citizen by reporter Jacquie Miller about a marijuana dispensary in Orléans that opened in a building that also houses a couple of services that cater mostly to children. (…) It suggests - as parents, as suburban communities that cherish safety, as a people spooked by a national fentanyl crisis, as guardians who worry what our teenagers are up to at night - we are not wholly ready for this. Here, evidently, are the groups jittery about marijuana becoming legally available at an outlet near you: parents, young kids, senior citizens who never touch the stuff, cranky middle-aged newspaper hacks, small businessmen who don't want pot shops nearby, the police, educators and plenty, plenty more. So, who are we really legalizing marijuana for? I was noodling through statistics from the Canadian Centre on Substance Abuse. What an eye-opener. According to a respected national survey done in 2013, eight per cent of adults 25 and older reported cannabis use in the previous year. Yes, eight. The rate in 2012 was 8.4, while the figure from 2011 was 6.7 per cent. If the entire over-15 population is considered, the rate in 2013 was 10.6 per cent. The rate among the 15-to-24 year-olds was, of course, higher, but not shockingly so: 24.4 per cent for past-year use, with males twice as likely to have used. To recap, as a

country we're about to twist ourselves into knots because eight per cent, or one in 12 Canadians, has used pot - and maybe only once - in the last year. And of those eight per cent, it appears a good chunk are young people, males especially, going through a skater-boy phase. Ottawa Citizen, A2

*** What's next for marijuana legalization?**
With Canada inching towards marijuana legalization, the federal government announced on April 20, 2016, that a new law is expected to be introduced in the spring of 2017. A nine-membered task force, chaired by Anne McLellan (a former deputy prime minister under the prime minister Paul Martin), will be talking to provincial, territorial, and municipal governments, indigenous people, youth, and addiction and health experts on the subject. Of the eight other members on the government task force, five are doctors. While the constitution of the task force symbolizes the focus on health, many of us may pause to deliberate over the context of this debate within a larger narrative. Kiran Siddiqui, a fourth-year student pursuing a comparative physiology specialist, has a similar view. "I'm sure this debate has many more layers than just legalizing or prohibiting, but I think it is good that we are paying attention to it, especially its effects on health and contribution to chronic disease," says Siddiqui. If you find yourself doing some preliminary research on the development of the legalization policy in Canada, as I did for this piece, you may find the subject being largely divided into either support for prohibition, driven by results shown by scientific research, or a call for legalization, motivated by the need to remove the social stigma around active users. However, the U of T faculty is taking a more holistic approach towards understanding the complexities of the debate. In order to discuss the complexities, we'll start with the basics. "The first thing is of course [...] that cannabis is not a deadly drug," says Harold Kalant, an emeritus professor with both an M.D. and Ph.D., who previously taught at U of T's Department of Pharmacology and Toxicology. "But it has shown to lead to problems with certain maturation processes required for the development of our executive functions, such as working memory, reasoning, [and] problem solving." The Medium

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

Canadian one of three people taken hostage in Libya
Ottawa has confirmed that a Canadian is among three people taken hostage in Libya last week. In a statement Sunday, Global Affairs spokesman Michael O'Shaughnessy says the Canadian government is "diligently pursuing all appropriate channels to obtain more information about this troubling incident." He says the government will not comment further or release any information that may compromise efforts to secure the hostages' release or endanger the safety of Canadian citizens. Earlier in the week, a Libyan official said authorities were investigating the abduction of three foreigners working for a maintenance company near the border with Algeria. Canadian Press (Guardian, B4, National Post, Province); * Journal de Montréal, 26

*** Mohamed Fahmy comes to Concordia: Award-winning journalist talks about his experience in prison and calls for the university to support Homa Hoodfar**
Concordia University welcomed Egyptian-born Canadian journalist Mohamed Fahmy as a lecturer for the first in a series of homecoming lectures at the Sir George Williams campus on Sept. 22. Just over one year ago, Fahmy was released from prison in Cairo, Egypt. He, along with two of his colleagues, were accused of being terrorists, he said. They were arrested in December 2013, and found guilty in June 2014, staying incarcerated for over 400 days. Fahmy also spent six weeks in solitary confinement. To a full house at the D.B. Clarke theatre, Fahmy spoke about his experience in prison and his campaign to free other journalists in similar situations. Fahmy detailed his experience working at various news stations prior to his arrest—namely CNN, the BBC, and Al-Jazeera, where he worked as an English bureau chief in Cairo. "I knew it was going to be a challenge when I took the [Al-Jazeera] job," he said. "My last story, before going to prison, was on the branding of the Muslim Brotherhood as a terrorist organization." Concordian

*** Putin on a roll , but has big issues at home**

Vladimir Putin' s cold heart will have been gladdened by Stephane Dion ' s eagerness for Ottawa to re-engage with the Russian dictator - a rapprochement that began with little fanfare when Canada ' s foreign minister met for half an hour two months ago in the Far East with the Kremlin ' s top diplomat, Sergei Lavrov. Almost everything still appears to be going the Russian president ' s way - on the surface. Although voter turnout was feeble last week, Putin ' s United Russia Party was returned to parliament with three-quarters of the seats. Russian warplanes have resumed their relentless bombing of the besieged Syrian city of Aleppo on behalf of Bashar Assad ' s ghastly regime. A rickety aircraft carrier is going to wave the Russian tricolour off Syria ' s Mediterranean coast. There has also been another uptick in violence by Russian proxies in eastern Ukraine to keep the Balts and Poles wondering whether they might be next on Putin ' s hit list. (...) As ISIL, Al-Nusra and al-Qaida lose their grasp in western Iraq and Syria, some of their jihadi zealots have shifted their attention to Western Europe, the Maghreb and sub-Saharan Africa. Others are returning home to the former Soviet republics of Turkmenistan, Uzbekistan, Kazakhstan and Kyrgyzstan, which like Ukraine the Kremlin has never stopped considering to be part of its informal empire, and to secessionist-minded Chechnya, Dagestan and Ingushetia, which are part of Russia. Crimean Tatars have also begun to create problems on the Black Sea peninsula that Russian forces annexed from Ukraine in 2014. It is not well known in the West that Russia has 20 million Muslims - one in seven citizens. Nor is it generally known that as many as 7,000 jihadists are from what Russia considers its sphere of influence, including as many as 2,400 Russians, which Aron notes is far more than any western European country. Most Russian Muslims are strongly secular. They have little interest in their religion and even less in radical Islam. But as Belgium, France and Britain have discovered, it only takes a few inspired radicals to cause hideous violence and tie up many police and soldiers. Putin is gravely concerned by the prospect of homegrown Islamic terror spilling north from the Caucasus. Postmedia Network (London Free Press, N5, National Post, Edmonton Journal, StarPhoenix Windsor Star, Montral Gazette, Vancouver Sun, Calgary Herald, Leader-Post, Ottawa Citizen)

*** Decision on House vote peacekeeping mission into Africa 'putting the cart before the horse': Defence minister**

The House of Commons should debate Canada's upcoming peacekeeping mission into Africa, where Canada could use force if needed to protect civilians, but it's still too early to say if it should vote on it, says Defence Minister Harjit Sajjan. "First we need to decide on what we're going to do; to decide on the parliamentary process that it needs to take, and that is very important, to be able to decide the process before we decide on how; it literally is putting the cart before the horse," said Mr. Sajjan (Vancouver South, B.C.) in a sit-down interview with The Hill Times last Wednesday afternoon. Mr. Sajjan told The Canadian Press earlier this month that Canada was still determining where to send an estimated 600 Canadian soldiers, although it's believed that it could be Mali, and he said that Canada could use force if needed. "When Canada goes in, yes, we will be fulfilling that mandate of protection of civilians and proactively acting in that manner. And we expect other nations to do the same thing. That's one concern I do have and I will be looking at that all the way through," he told CP, after it was reported in July that foreign aid workers in the Democratic Republic of Congo and Mali were raped and attacked by local soldiers and local peacekeepers failed to respond for hours. Hill Times

INTERNATIONAL

Jordanian writer killed before trial for cartoon mocking Islam

A prominent Jordanian writer was shot dead by a suspected Islamist gunman Sunday outside the courtroom where he was due to stand trial for offending Islam by sharing a cartoon on Facebook. Nahed Hattar, a 56-year-old intellectual from Jordan's Christian minority, was gunned down on the steps of a courthouse in Amman in what appeared to be a religiously motivated attack. The gunman was arrested at the scene and a security source identified him as Riyad Ismail Abdullah, a 49-yearold imam. The killing is a fresh blow to Jordan's image as a bastion of stability amid the sectarian violence wracking much of the Middle East. It is also the latest in a string of killings linked to cartoons about Islam. Hattar was arrested last month for sharing a cartoon on his Facebook page that showed a jihadist smoking in bed with two women while Allah waits attentively at the window for him. The jihadist orders Allah to fetch him some

wine and take away the dirty plates while demanding the archangel Gabriel get him some cashew nuts. Telegraph (Province, A18); Le Devoir

*** État de Washington - L'auteur présumé de la fusillade dans un centre commercial arrêté**
Au terme d'une chasse à l'homme de 24 heures dans le nord-ouest des États-Unis, la police a annoncé samedi avoir capturé le tireur présumé, un jeune homme de 20 ans né en Turquie, accusé d'avoir tué cinq personnes dans un centre commercial. Selon le porte-parole de la police de l'État de Washington, Mark Francis, le suspect se nomme Arcan Cetin, est âgé de 20 ans, et réside à Oak Harbor, une ville voisine de Burlington, commune de quelques milliers d'habitants à 110 km au nord de Seattle où a eu lieu la fusillade vendredi soir. Aucun autre suspect n'est recherché, a précisé le porte-parole, au lendemain de la fusillade qui a tué quatre femmes et un homme dans le centre commercial Cascade Mall de Burlington. Le tireur, qui avait été présenté dans un premier temps par la police comme un jeune d'origine hispanique, a ouvert le feu au rayon maquillage d'un grand magasin de l'enseigne Macy's. Une page Facebook, présentée comme étant celle du suspect, indique qu'Arcan Cetin est né à Adana, quatrième ville de Turquie située sur les bords de la Méditerranée. Il a fait ses études à Oak Harbor et travaillé dans une épicerie de Widbey Island, une autre localité de l'État de Washington. Agence France-Presse (LE Devoir, B3)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 1, 2016 / le 1 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

D'autres reporters surveillés?
Le chef de la police de Montréal n'a pas exclu lundi que d'autres journalistes soient sous surveillance, à la fin d'une journée au cours de laquelle le monde politique a unanimement exprimé sa vive préoccupation par rapport à l'espionnage du téléphone cellulaire de Patrick Lagacé. Au cours d'un point de presse tendu, Philippe Pichet a défendu l'obtention par ses hommes de 24 mandats judiciaires concernant l'iPhone du journaliste entre janvier et juin dernier. La Presse a révélé lundi que la police avait fait main basse - avec la bénédiction de la justice - sur la liste complète des interlocuteurs du journaliste pendant plusieurs mois, ainsi que sur ses données de localisation transmises par le GPS intégré au téléphone. (…) À Ottawa aussi, on était inquiets. «Je suis troublée par les révélations d'aujourd'hui», a écrit la ministre Mélanie Joly sur les médias sociaux. Le **ministre fédéral de la Sécurité publique Ralph Goodale** se dit ***«certainement prêt à avoir une discussion de politique sérieuse» et «à entendre les***

représentations» des médias sur la façon dont les forces policières devraient concilier leurs enquêtes avec la protection des sources journalistiques et la liberté de la presse. Le **ministre Goodale**, qui n'a pas voulu commenter le cas de Patrick Lagacé, mais qui se dit «***profondément préoccupé par ce genre de dossier»***, s'assurera prochainement auprès du commissaire de la Gendarmerie royale du Canada Bob Paulson que les directives fédérales en vigueur sont respectées dans les faits. En dehors du monde politique, la Fédération professionnelle des journalistes du Québec (FPJQ) et Reporters sans frontières ont tous deux exprimé leur indignation face aux actions du Service de police de la Ville de Montréal (SPVM). Le Nouvelliste, 6 (La Presse)

«Troublant», «inacceptable», «extrêmement grave»
Quelques réactions aux révélations d'espionnage de policiers à l'endroit du journaliste Patrick Lagacé. «Lorsque j'ai lu le journal ce matin [hier] et que j'ai vu le cas de Patrick Lagacé, on est passé par toutes sortes d'émotions. On trouve cela préoccupant, on trouve cela inacceptable.» - Denis Coderre, maire de Montréal. ***«Nous devons traiter de cet enjeu sérieusement, et je suis certainement prêt à entendre les représentations [des médias et d'associations de journalistes comme la FPJQ] sur ce qui pourrait être un meilleur ensemble de règles.»*** **- Ralph Goodale, ministre fédéral de la Sécurité publique.** «C'est extrêmement grave, ce qui a été permis. [...] Il faut se tenir debout face à une telle invasion de nos droits et libertés. [...] Je trouve ça ahurissant, je suis abasourdi qu'on soit en train de vivre ça au Canada au XXIe siècle. [...] Ça renvoie à une question fondamentale : dans quelle sorte de société nous voulons vivre?» - Thomas Mulcair, chef du Nouveau Parti démocratique. La Tribune, 11 (La Presse)

Une enquête publique demandée par les médias
Après la saisie de l'ordinateur d'un journaliste du Journal de Montréal et la mise sous surveillance d'un chroniqueur de La Presse, un exbâtonnier du québec et plusieurs médias réclament une commission d'enquête sur les pratiques policières à l'égard des sources journalistiques. Le cellulaire du journaliste Patrick Lagacé a été placé sous surveillance en début d'année, dans le cadre d'une enquête interne du spvm, a révélé hier la presse. les enquêteurs auraient obtenu les numéros de téléphone entrant sur l'appareil. ses allées et venues auraient aussi été surveillées grâce au système gps du téléphone. (…) ce qu'ils ont dit... «la première chose qui s'impose, c'est de vérifier que les processus en place et les politiques qu'utilisent les corps policiers lorsqu'ils demandent de tels mandats soient dument respectés. (…) la capacité de la presse de faire son travail, c'est très important. » -martin coiteux, ministre de la sécurité publique «je trouve ça très inquiétant. il n'y a rien de plus important pour les journalistes que les sources journalistiques .» -Nathalie Roy, députée caquiste et ancienne journaliste «le spvm devra s'expliquer. la liberté de la presse et la protection des sources journalistiques sont des choses fondamentales dans une démocratie.» -Agnès maltais, députée du parti québécois «il faut une sépa - ration claire des pouvoirs entre l'administration et le service de police. il est inconcevable que le chef de police n'ait pas été mis au courant. et s'il n'a pas été mis au courant, c'est qu'il a perdu le contrôle de son organisation.» -luc ferrandez, chef intérimaire de projet Montréal «je lui ai dit (au directeur pichet) que j'étais préoccupé par ce que je voyais et je lui ai réitéré que la question de la liberté de la presse est importante.» -Denis Coderre, maire de Montréal ***«la liberté de la presse est un principe fondamental qui est en fait protégé dans la charte canadienne des droits et des libertés. le plus grand soin doit être pris par les forces de l'ordre quand des enquêtes criminelles et le journalisme se croisent.» -*** **Ralph Goodale, ministre fédéral de la sécurité publique** «vous êtes journaliste? la police vous espionne pour identifier vos sources, ce n'est pas hypothétique. c'est maintenant.» -Edward Snowden, lanceur d'alerte bien connu. Agence QMI (Journal de Québec, 4, Journal de Montréal)

Grits rapped for unspent funds
Like the Harper government before it, the Trudeau government left billions of dollars unspent on everything from national parks to veterans services to economic development grants during the 2015-16 fiscal year. The so-called "lapsed" funding for fiscal 2016 is $9.7 billion, according to the Public Accounts of Canada. All of those unspent funds were used to pay down the federal debt. This year's three-volume public accounts also close the books on fiscal 2016, a year in which the Harper Conservatives controlled the purse strings for the first seven months and the Trudeau Liberals for the final five months. (…) **Public Safety Canada**, which includes the RCMP, the Correctional Service of Canada, and Canada Border Services Agency, was authorized to spend $9.2 billion in fiscal 2016 but left unspent 11.6 per cent of that

- about $1 billion. **Scott Bardsley, press secretary to Public Safety Minister Ralph Goodale**, said the lion's share of the lapse - about $700 million - was related to disaster relief for the provinces that, while booked by the federal government in 2016, was not paid out. Infrastructure Canada left $858 million unspent, nearly 20 per cent of the $4.4 billion it was authorized to use in 2016. Postmedia Network Kingston Whig-Standard, B1/Front, London Free Press, Leader-Post, Vancouver Sun, Ottawa Citizen, StarPhoenix, National Post, Montreal Gazette)

Ahmadiyya Caliph to meet with city's growing faith community
The head of the world's Ahmadiyya Muslims will visit Saskatchewan for the first time, spending a day in Saskatoon before inaugurating Regina's first purpose-built mosque. The Caliph, Hazrat Mirza Masroor Ahmad, arrived Monday evening in Saskatoon, where he was greeted by Ahmadi Muslims and public officials. Among Ahmadiyya Muslims, the Caliph is the highestranking member of the sect, after the Prophet Muhammad. "Whenever his Holiness comes to Canada, his primary objective is to meet with members of his community. Saskatchewan ... particularly Saskatoon, has become, believe it or not, a hub for the community, even though we're headquartered in Toronto," spokesman Safwan Choudhry said. In his one-day Saskatoon visit, he is expected to meet with members of the community, local administration of the Ahmadiyya Muslim Jama' at, Syrian refugees and local politicians. Choudry said the Caliph spends time meeting with young women, as he is a strong advocate for women's rights and equal freedoms for women. The visit is a part of his Canadian tour, which included a meeting with Prime Minister Justin Trudeau earlier this month. He also gave a rare interview to CBC National anchor Peter Mansbridge. Premier Brad Wall and **federal Minister of Public Safety Ralph Goodale** are expected to attend a reception alongside him in Regina. The Caliph's visit coincides with the inauguration of Regina's mosque, which will be broadcast worldwide. The province's largest mosque is scheduled for inauguration in Saskatoon in about a month. "If that kind of tells you why Saskatchewan's become so important ... with a growing community here, members of our community have found Saskatchewan, particularly as a province, Saskatoon, especially, to be good to them," Choudhry said. StarPhoenix, A7

TOP STORIES / MANCHETTES

Prison watchdog alarmed by pepper-spray use
Canada's prison watchdog is calling for tighter controls on the use of pepper spray in federal penitentiaries amid concerns correctional officers have taken to dousing inmates with the noxious repellent on a "routine" basis. Pepper spray was used in 60 per cent of the incidents in which Correctional Service Canada officers used force last year, correctional investigator Howard Sapers said in his annual report on the state of Canada's prisons and prisoners, released Monday. That works out to more than 1,000 times - three times as often as five years ago. The increase was not the result of an increase in dangerous security incidents, said Sapers, who instead blamed the simple fact that pepper spray became standard equipment for correctional officers in September 2010. As a result, officers are abandoning other interventions, such as simply talking to inmates, in favour of their spray cans. Correctional Services Canada said it is reviewing its policies around the use and oversight of pepper spray and other chemicals and will report back in April. Canadian Press (Times & Transcript, B3, National Post, Red Deer Advocate, Daily Gleaner); Le Devoir; Le Journal de Montréal (Le Journal de Québec)

Killer wants out: Bernardo's day-parole hearing set for March
School girl killer Paul Bernardo has a day parole hearing tentatively set for March, the Toronto Sun has learned. Bernardo was sentenced in 1995 to life in prison with no parole for 25 years for the horrific sex slayings of teens Leslie Mahaffy and Kristen French. Lawyer Tim Danson, who represents the Mahaffy and French families, said he believes the system will work. "I don't believe that Paul Bernardo will ever be paroled, now or in the future," Danson said Monday night. "Having said that, remember, I represent the victims of Paul Bernardo, and so we will take nothing for granted, we will be very vigilant." Prominent Toronto criminal lawyer Edward Prutschi, who has no connection to the case, said he's also confident Bernardo will not taste freedom anytime soon. "He's the poster child for incarceration in Canada," Prutschi said. "If there's one person who personifies the desire to actually see somebody serve the rest of

their life behind bars, it's Paul Bernardo." Toronto Sun, A16 (Edmonton Sun, Winnipeg Sun, Ottawa Sun, Winnipeg Sun); Toronto Star

Ottawa plans to reduce use of mandatory prison sentences
The Trudeau government intends to cut widespread use of mandatory minimum sentences by giving judges back their discretion over punishment, Justice Minister Jody Wilson-Raybould says. The changes will undo a major element of the Harper government's tough-on-crime agenda. Judges will be given the "appropriate discretion to be able to impose sentences, engage and understand - as they do better than anybody else - the individual that is before them," the Justice Minister told The Globe and Mail in an interview as the Liberals near the end of their first year in power. "To base their decisions on the actual circumstances of the case before them and render judgment." She said new legislation on mandatory minimums is coming soon, "certainly in the early part of next year." Last month, the government gave judges back the discretion they had lost in 2013 over the victim surcharge - a financial penalty from which judges once routinely exempted impoverished offenders, until it became mandatory. A new federal law rolling back mandatory minimum terms could cut the number of Canadians incarcerated, which is high despite falling crime rates. It could also reduce the rates of indigenous people behind bars. Globe and Mail, A1

Complaints about elderly B.C. couple's arrest prompt federal investigation
Days after troubling footage emerged of Mounties arresting an elderly couple in Coquitlam, B.C., a federal agency is launching an investigation into the officers' conduct. The Civilian Review and Complaints Commission for the RCMP said it has received more than a dozen complaints from people expressing concerns about the YouTube video, which at one point shows an officer dragging a senior down a stairwell. "We've received approximately 15 complaints from concerned citizens," said Richard Evans, senior director for the independent agency. "Some were present at the scene and some were not." The incident, which took place after a heated strata meeting at a Best Western hotel, is already being investigated by the New Westminster Police Department, which will decide whether to recommend charges against the officers involved. But the Civilian Review and Complaints Commission's probe could potentially lead to changes in RCMP policy moving forward, Evans said. "Our investigation is designed to make findings and recommendations about [officers'] conduct to inform better policing practices," he told CTV News. "Issues like: Did they have the authority to arrest? Was the appropriate use of force used? Were the RMCP members there properly trained? Were they properly supervised? Was there a language issue?" CTV News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** MLAs honour wildfire heroes**
Darby Allen still thinks about the wildfire that swept through Fort McMurray. The Wood Buffalo fire chief has good days and bad; the evacuation of 80,000 people from the city still plays on his mind. He wonders: "Could we have done more?" Monday was one of the good days, as he and his fellow first responders were recognized at the Alberta legislature for their work during the disaster. I's been six months since the blaze - nicknamed The Beast - ripped through the region, destroying homes and livelihoods. While 85 per cent of structures were saved, the situation was touch and go as temperatures rose and winds fanned the flames, playing havoc with firefighting efforts. Postmedia News (Edmonton Journal, A3; Calgary Herald, Calgary Sun, Edmonton Sun); CBC News; Canadian Press (Red Deer Advocate)

*** Maximum fine for causing wildfire jumping to $1M under new bill**
Proposed amendments to legislation would substantially hike fines for people or companies that cause forest fires by ignoring fire bans or improperly extinguishing campfires. The changes are contained in Bill 24, the proposed Forest and Prairie Protection Amendment Act. Maximum fines under the amendments would jump from $5,000 to $1 million for corporations and up to $100,000 for individuals. Companies could be fined up to $10,000 for not having a proper wildfire plan and inadequate firefighting equipment on site. CBC News (2016-10-31)

*** B.C. gets a failing grade for flood preparedness in new report**
British Columbia is one of the least prepared provinces to deal with a major flood, according to a recently released national report called Climate Change and the Preparedness of Canadian Provinces and Yukon to Limit Potential Flood Damage. B.C. and Prince Edward Island have the lowest overall grade of D, while Ontario scored the highest with a B-minus on preparedness to limit climate change-related flood damage. No province was a standout. The overall average for all 10 provinces and Yukon was C. B.C. received aD grade in 11 of the 12 assessment categories that examined issues such as whether the province or territory has a flood plan map, how well the transportation system would function during flooding, and whether drinking water sources would be protected. Postmedia News (Vancouver Sun, A2; Vancouver Province)

*** Don't blame Mother Nature for flooding's devastating impact**
An opinion piece states "Reports of human loss and suffering from flooding are far too frequent. And while the reports heighten our perception of the problem, they still don't fully illustrate the growing impacts of floods on people and their homes. Or accurately reflect the cause. According to the World Bank report Cities and Flooding, A Guide to Integrated Urban Flood Risk Management for the 21st Century, the 10-year moving median number of reported flood events is rising steadily and was a full 16 times higher in 2010 than 50 years earlier. Floods are nothing new. They are natural events that have been happening for millennia, shaping the earth we live on and creating much of the natural bounty that supports us. Still, we like to villainize nature when it brings us harm. Floods, like wildfires, have gotten a very bad name because of the harm to people we associate with these events. But Mother Nature is not the problem. Dr. Gilbert White, the late founder of the internationally-recognized Natural Hazards Center in Boulder, Colo., put it well: "Floods are acts of nature; but flood losses are largely acts of man." We must take heed of this wisdom as we plan for resilience -- especially in light of climate change." Torstar (Daily Gleaner, A7; Waterloo Region Record)

*** Warning as Canada faces rising costs of climate change**
Canada is ill-prepared for the increased flooding and extreme weather that climate change will bring, and needs to act now, a new report expected to be released today has claimed. The report – which comes as the insurance industry is increasingly concerned over the cost of weather-related events and natural disasters post-Fort McMurray – warns that the country must take action or face much higher costs to fix damaged buildings and infrastructure in the future. The University of Waterloo's Intact Centre on Climate Adaptation evaluated provincial efforts to mitigate disasters from the flooding that will be caused by extreme weather and rising sea levels. Insurance Business (2016-10-31)

*** Canada safety watchdog says action needed on train crew fatigue**
Too many Canadian train crews are not getting sufficient rest and railroads need to do more to apply fatigue science to scheduling, the country's transport safety watchdog said on Monday. The Transportation Safety Board of Canada, an independent government agency, singled out rail fatigue in its 2016 watch list, which identifies key safety issues in Canadian transportation. TSB Chair Kathy Fox said by phone the board would meet with industry and government representatives as soon as Tuesday to push for concrete action, including the creation of more predictable schedules for employees who often work on two hours' notice. Reuters (2016-10-31)

*** Heiltsuk diesel-spill site too tough to clean up: Booms torn apart in rough weather**
An opinion piece states "I am a Raincoast Conservation Foundation biologist lucky enough to study black and grizzly bear populations in Heiltsuk Territory and to call Bella Bella home. I'm often astounded by the richness of this area. Unfortunately, my time recently has been spent in awe, not of ecological and cultural treasures, but of the aftermath of a petroleum tug-barge tanker crashing into one of them. Almost two weeks ago, the Nathan E. Stewart drove straight into a reef in Heiltsuk waters in the middle of the night. Fortunately, the barge was empty, but the tug sank and began leaking marine diesel. In the aftermath of the accident, it took more than a week to remove the remaining leaking oil from the tug, and, two weeks in, the tug is still in the water, diesel slicks are still being observed and area beaches remain contaminated. That this happened is beyond disappointing, but where it happened is devastating." Times Colonist, A11

*** The real mess is our woeful oil-spill response system**
An opinion piece states "Every time there's a minor oil spill on the B.C. coast, it's treated as yet another warning that a bigger spill is possible and it's time to do something about it. It's been going on for years. From the 2007 Kinder Morgan pipeline breach that dumped 70,000 litres of crude into Burrard Inlet and sprayed a dozen homes with smelly oil to the 2015 spill of toxic bunker fuel into English Bay from the leaky MV Marathassa cargo ship. The latest wake-up call is the release of an estimated 105,000 litres of diesel fuel into the waters off Bella Bella from the Nathan E. Stewart tugboat that struck a reef and sank Oct. 13. As with the Marathassa spill, the emergency response to the tugboat spill has been criticized for being slow and ineffective. Sadly, this doesn't come as a surprise to experts who have taken a close, hard look at B.C.'s oil-spill prevention and response system, and found it sorely lacking." Vancouver Province, A7

*** Crew member hoisted from boat off Cape Scott for medical help**
A crew member on a fishing boat about 60 nautical miles northwest of Cape Scott was hoisted onto a Royal Canadian Air Force helicopter Monday after having unspecified medical issues. Victoria's Joint Rescue Co-ordination Centre was informed of the situation about 1 p.m. by Prince Rupert Coast Guard Radio and sent the helicopter, a fixed-wing aircraft and two coast guard vessels to the scene. The helicopter took the man to Port Hardy, where he was put on the fixed-wing aircraft and flown to Victoria for treatment. Times Colonist

*** Search on for missing senior in C.B.S**
A search is underway for missing 82-year-old man in the Kelligrews area of Conception Bay South. The Royal Newfoundland Constabulary said William Snelgrove was last seen at 1 p.m. on Monday when he left his personal care home to go berry picking off Middle Bight Road. He is five feet nine inches tall, 130 pounds and is believed to be wearing a white jacket, black pants, red hat and green boots. Police said Snelgrove has medical issues and they are concerned about his safety. The Rovers ground search and rescue team and a Cormorant helicopter from the search and rescue squadron in Gander were active Monday night. CBC News

Search for missing hunters underway near Quesnel
A search for a pair of hunters is underway northeast of Quesnel. 55 year old Glen Brooker and his 10 year old step son were reported overdue Sunday. They left their home Saturday to hunt the Stoney Lake or Narrow Lake area. Brooker was driving a 2005 Dodge Pickup and was pulling a grey and green Kingfisher riverboat. The pair also had their chocolate coloured Lab dog with them. RCMP are working with Search and Rescue officials. CKPG News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Une grappe sans racines**
Une chaire de recherche mondiale en prévention de la radicalisation rayonnera à l'Université de Sherbrooke même si l'institution n'a jamais perçu le moindre signe que de ses étudiants buvaient à la fontaine de l'intolérance et de la violence. Convenons qu'il était pour le moins incongru que deux représentants du gouvernement québécois, dont le ministre responsable de l'Estrie, Luc Fortin, vantent lundi matin la contribution de l'Université de Sherbrooke à la création d'un comité scientifique au lendemain de révélations associant un autre de ses anciens étudiants aux djihadistes. «Je salue le dynamisme de l'Université de Sherbrooke, qui est à l'origine de cette initiative inspirante que le gouvernement québécois appuie fièrement», a pourtant mis en valeur la ministre des Relations internationales et de la Francophonie, Christine St-Pierre, en annonçant la nouvelle en présence de représentants de l'UNESCO. «La région de Sherbrooke continue de se démarquer sur la scène

internationale grâce à son expertise et à son savoir-faire», a renchéri son collègue Fortin, si l'on se fie au communiqué de presse émis par le gouvernement et diffusé sur le Portail Québec. La Tribune, 4; Montreal Gazette

*** Les visages de la radicalisation**

«Je suis là pour m'excuser.» Devant nous, un grand baraqué. Rempli de remords. La Fédération des Québécois de souche, c'est lui. Ou plutôt, c'était lui, quand il cultivait le nationalisme blanc, vraiment blanc. «Je suis le fondateur, le seul et unique. C'est parti de ma tête.» Et elle était rasée, cette tête, à l'époque skinhead. Lui, c'est Maxime Fiset, de Québec, aujourd'hui étudiant universitaire... qui a déjà pensé faire sauter une bombe comme celle du marathon de Boston. Il a aussi été modérateur pour un site Web très raciste. Lundi, il est sorti de l'ombre pour dire qu'il a tout balancé. La radicalisation violente, «c'est plus proche de nous qu'on pense», prévient-il. Il était rendu à un tel point que les policiers l'ont arrêté pour propagande haineuse. (...) C'était avant l'État islamique. C'était les talibans, Al-Qaida. Mubin Shaikh étudiait la religion. Il avait 19 ans. Il est parti du Canada en voyage initiatique au Pakistan. Pas dans des camps. Juste un voyage de jeune croyant, raconte-t-il. Et il a rencontré ses nouveaux voisins, des talibans de la ville de Quetta. «Ils sont encore là.» Il a appris quoi? «Que pour être un vrai musulman, il faut combattre. Au retour, il a rejoint d'autres extrémistes ici. Il a recruté dans des mosquées, des conférences islamistes. Puis il y a eu le 11 septembre 2001, les tours de New York qui tombent. Ça, c'était trop pour lui. Il est parti pour la Syrie (bien avant la guerre). «J'ai appris le vrai islam.» Revenu au Canada, il a vu un de ses amis se faire arrêter. Il a alors appelé les services secrets : «Ils m'ont recruté pour être agent infiltrateur. Pendant deux ans, j'ai été infiltré.» Il a aussi travaillé pour la GRC. L'arrestation du groupe des 18 de Toronto, inspiré par Al-Qaida, c'est un peu lui. Il jure que cet épisode policier est derrière, qu'il se concentre sur son doctorat en psychologie en Angleterre. Son sujet : comment contrer et prévenir l'extrémisme. La Presse (Le Soleil)

*** Pas de filière djihadiste à l'UdeS**

Malgré les dernières révélations sur un ex-étudiant de l'Université de Sherbrooke qui serait un présumé djihadiste, «on ne peut pas encore parler de filière de radicalisation islamiste» à l'UdeS, estime le professeur David Morin de l'UdeS, codirecteur de l'Observatoire sur la radicalisation et l'extrémisme violent (OSR). M. Morin deviendra le cotitulaire d'une nouvelle Chaire de recherche en prévention de la radicalisation et de l'extrémisme violent, dont la création a été annoncée lundi à la Conférence Québec-Unesco intitulée «Internet et la radicalisation des jeunes : prévenir et agir ensemble». Le Toronto Star révélait qu'un autre ancien étudiant de l'UdeS, Assane Kamara, fait face à une série de chefs d'accusation de terrorisme au Sénégal parce qu'il aurait tenté de joindre les rangs de l'État islamique (EI). Son nom s'ajoute à celui de trois Sherbrookois qui ont fait les manchettes, Zakria Habibi, Samir Halilovic et Youssef Sakhir, qui auraient fui le Canada pour joindre la Syrie. En 2015, Chiheb Esseghaier, un ex-étudiant de l'UdeS qui a été membre de l'Association musulmane de l'UdeS (AMUS), a reçu une peine de prison à vie après avoir comploté dans le but de faire dérailler un train de passagers de VIA Rail entre Toronto et New York. La Tribune, 5 (La Presse)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Mystery man spent two years in prison being grilled by CBSA

For more than two years, a man who calls himself Paul Rooney sat in a Maple Ridge prison while border agents tried to figure out exactly who he was and where he came from. They interviewed his friends and co-workers, examined his health records and ran his fingerprints through international databases. Officially speaking, Paul Rooney's origins were a complete mystery. The Canada Border Services Agency came up short, and earlier this year, the Immigration and Refugee Board ordered Rooney released from detention at the Fraser Regional Correctional Centre, a decision that has now been upheld twice by the Federal Court. "He may or may not have been born in Toronto. He may or may not have been born in St. Vincent and the Grenadines. He may or may not have been born in England ... In other words, he may or may not be Canadian," Federal Court Justice Sean Harrington wrote in a decision back in March. (...) Vancouver police opened an investigation, though no charges were laid, and officers with the Canada Border Services Agency dropped by his workplace to interview him. When they learned he may have been born in England, they detained him and got an order to deport him on

Oct. 28, 2013. The only question was where to send him. Neither the U.K. nor St. Vincent and the Grenadines recognized Rooney as a citizen. Interpol was alerted and his photo was distributed internationally, but there were no hits. (...) There are no guidelines for how long someone can be kept in immigration detention, but the onus is on the federal government to prove each month that imprisonment is justified. In a case like Rooney's, that means CBSA officers need to show progress in determining someone's real name and citizenship status. Postmedia Network (Vancouver Sun, A1, The Province)

Woolly mammoth tusk, $100K in jewelry seized at Windsor border
A woolly mammoth tusk and nearly $100,000 worth of jewelry were among the more unusual items Windsor border officers seized in September. Officers with the Canada Border Services Agency seized the jewelry on Sept. 9 from an American woman who was sent to secondary inspection at the Ambassador Bridge. A search of her vehicle revealed several empty jewelry boxes. Officers then searched her handbag and found a large amount of gold jewelry, which the woman said was from Dubai. (...) Officers came across the mammoth tusk on Sept. 20. Two Canadian residents told a customs officer at the bridge they had $760 worth of antiquities, including the tusk. Officers discovered the tusk was actually worth $6,100. The CBSA said there are no restrictions on importing the items, but travellers must still declare the proper value. They were slapped with a $3,317 penalty. Border officers also seized several guns at southern Ontario border crossings in September. Windsor Star, A5

Defence no refuge
An immigration fraudster who tried to use deception and bribes to sponsor 528 refugees into Canada has undermined the public's confidence in the country's refugee process, an Ottawa judge said Monday before sentencing the man to three years and nine months in prison. Ontario Superior Court Justice Robert Beaudoin also expressed surprise that Mohamed Farah Abdulle was able to carry out his scheme for as long as he did without being detected by officials at Citizenship and Immigration Canada. "He just learned how to exploit the apparent lack of oversight in the system," said the judge. Over a five-year period, the 54-year-old former janitor participated in 170 sponsorship applications that attempted to bring 528 refugees to Canada. Thirty-seven refugees were successfully sponsored. (...) Abdulle's trial heard that Canada Border Services Agency investigators found a stack of citizenship and permanent residence cards that were an inch thick after executing search warrants. Postmedia Network (Ottawa Sun, A3, Toronto Sun, Calgary Sun, Edmonton Sun, Winnipeg Sun)

*** New terminal opens at Calgary International Airport**
After five years of construction, the first passengers passed through the gates of Calgary's new $2 billion airport terminal on Monday. The completed project doubles the space at the airport, at 185, 000 square metres. Officials say the new building has all the amenities that travellers are looking for including; automated check-ins, 50 shopping and dining locations and a 300 room hotel. Security lines are expected to move faster and four passengers will now be able to check through at the same time. Canada Border Services Agency says the new space will be the agency's primary location in the Prairie Region. The CBSA says 5,200 travellers can now be accommodated, which is more than double the amount of the old terminal. The agency has also installed 54 automated kiosks, 44 automated border clearance kiosks and 10 NEXUS kiosks. Passengers who are looking to make connecting flights can take advantage of a new and secure connection corridor. "We are grateful to the airport authority for all of their hard work on this project. The new CBSA space demonstrates the strong relationship that CBSA has with YYC," said Kim R. Scoville, Regional Director General, Prairie Region, CBSA. Last year, the CBSA processed over 2.2 million travellers and over 111,000 NEXUS passages at the Calgary airport. CTV News (2016-10-31)

*** Canada's naive about immigrants, refugees**
An opinion piece states, "During a panel discussion on CTV News last week I was lectured by the two other panelists - one Liberal, one NDP - over my assertion we need to be careful about who we let in as immigrants and refugees. They both insisted there is no problem with arrivals from other countries, nor will there be. When I asked about the Shafia family, there was no response, other than to continue to assert that immigrants and refugees pose no danger to our safety or "Canadian values," a term which, sadly, too many people mock. (...) In 2008, then federa l auditor general Sheila Fraser reported Canada's border agency had lost track of 41,000 illegal immigrants, noting this was, "jeopardizing the integrity of Canada's immigration program". All of those people were under deportation orders, but we

didn't know then, and may still not know, where they went. Why were they deemed ineligible? Was it safe to let them go free? Several of the terrorists that attacked Paris came in to Europe through Greece, posing as Syrian refugees. Could the same thing happen here? Obviously, if we are so naive and careless as to assume that it never could happen." Postmedia Network (Ottawa Sun, A15, Toronto Sun)

Masse makes Halloween-themed member statement on new bridge
Windsor West NDP MP Brian Masse used his member statement in the House of Commons Monday to draw attention to what he believes is government dawdling on the construction of the Gordie Howe International Bridge. "Mr. Speaker, Halloween is the perfect time of year to talk about the Windsor-Detroit border, because under the current government it keeps getting scarier and scarier," Masse told the House. "After stirring up old Liberal ghosts to lead Canada's most important infrastructure priority, the project seems to have slipped into the Twilight Zone. "Whether it is spooky backroom conversations with the ghouls at the Ambassador Bridge or a zombie-like approach to property acquisition, the government appears to be lost in a haunted corn maze rather than on track to build a new crossing." Windsor Star

* **Auerbach, Schafenacker heading for Canadian border**
The two UNBC graduate students jailed and released in North Dakota are heading for the border today. Katriona Auerbach and Nicole Schafenacker drove from Prince George to North Dakota to protest the Dakota Access pipeline. Their UNBC research supervisor Dr. Sarah de Leeuw confirmed the girls were caught up in a mass arrest on Thursday. (…) Auerbach and Schafenacker were told there shouldn't be any issues crossing the border, despite the pending charges. The two are testing that advice at a border crossing; de Leeuw was uncertain which one the two are heading for. My Prince George Now

300 000 nouveaux arrivants pour 2017
Le Canada n'augmentera pas le nombre d'immigrants qu'il accueillera l'an prochain, mais il jette les bases pour une éventuelle hausse des seuils dans les années à venir. Les chiffres annoncés lundi à la Chambre des communes indiquent que le Canada prévoit recevoir 300 000 nouveaux arrivants l'an prochain, soit la même proportion d'immigrants qui doivent arriver durant l'année en cours. Ce seuil avait été revu, l'an dernier, à la hausse dans le but d'accueillir plus de réfugiés syriens. Le Nouvelliste, 20 (Le Soleil, Le Droit); Canadian Press (Red Deer Advocate, London Free Press, Leader-Post, Vancouver Sun, Montreal Gazette, Ottawa Citizen, StarPhoenix, National Post, The Telegram, Cape Breton Post, Edmonton Journal, Times Colonist, Times & Transcript); Agence QMI (Journal de Montréal); Globe and Mail; * Le Devoir; * Postmedia Network (Vancouver Sun, The Province)

* **Over 7,000 Irish workers expected to go to Canada this year**
With the Irish economy improving, the impetus to travel overseas in search of employment has dwindled for many. However, experts at VisaFirst.com say that while some people no longer feel "forced" to move away, Ireland's love affair with travel has certainly not gone away and an estimated 6,500 Irish workers are expected to sign up for the 2016/2017 Canadian Working Holiday programme, which has just opened its doors to applicants. The migration experts say that every year there are disappointed applicants to the 3 stage application process, but that, in the main, this is largely down to poorly completed and tardy application forms. (…) VisaFirst.com say that over the last 10 years the numbers of Irish travelling to Canada on temporary work visas had risen significantly, but that as a result of the upturn in the economy the last couple of years have seen the numbers fall somewhat. However, VisaFirst.com says that while temporary visa figures appear to be falling, Ireland was still ranked the 11th highest country to be issued work permits in 2014. Business World

Jury hears details of Tamil migrants' ocean journey
A Tamil man whose uncle died during their voyage to Canada on a migrant vessel six years ago has told a human-smuggling trial his relative was extremely ill in the days leading up to his death. The MV Sun Sea docked in British Columbia in August, 2010, carrying 492 Sri Lankan Tamils - 380 men, 63 women and 49 children. The ship was the second Tamil migrant vessel to arrive in this province in less than a year and made international headlines. Kunarobinson Christhurajah, Lesly Emmanuel, Nadarajah Mahendran and Thampeernayagam Rajaratnam have each been charged under the Immigration and Refugee Protection Act with organizing the trip. Their jury trial began two weeks ago in Vancouver. Globe and Mail, S1

Not all removals are extraditions
A letter to the editor states, "Re: Dozens already extradited to China, Oct. 24. This story confuses two separate processes for removing individuals from Canada and sending them to another country: extradition and deportation (through removal orders). These are distinct situations based in different legislation. Extradition involves a crime committed in one country and a person located in another country who has either been charged and is wanted for trial, or has been convicted of that crime. It is triggered by a request from the country where the crime was committed to return the person to face trial or sentence. Deportation involves the removal from a country of a person who has either entered the country illegally or has otherwise lost the right to remain legally. Both of these areas of Canadian law are complex, and each involves the fundamental question of what conditions in other countries should prevent return under any circumstances. However, it does not help the discussion of either subject to conflate the two and it is misleading in a discussion of a potential extradition treaty to present total removal statistics as extradition totals." Ottawa Citizen, A6

* **Harper was right: Private refugee sponsorship works better**
An opinion piece states, "It was the image that first turned the tide of the 2015 election: a photograph of a little boy, washed up on a Greek beach, his face in the sand, his tiny trainers still on his feet. Overnight, the haunting picture of Alan Kurdi, a four-year-old Turkish refugee who perished trying to cross the Mediterranean Sea, ostensibly after his family was refused refugee status in Canada, made Syrian migrants the top issue of the campaign. The story disrupted the Conservative narrative of Justin Trudeau being "not ready" and focused public attention on the government's refugee policy, including its failure to meet its modest resettlement targets of 3,500 migrants in 2015. (…) But a year later, it turns out that the Harper government's refugee policy, which emphasized private sponsorship over mass government assistance, may have had more going for it than it got credit for. According to a report released this week by Immigration, Refugees and Citizenship Canada, cited by the *Toronto Star*, government-assisted refugees have a tougher time adapting to Canadian life than their privately-sponsored counterparts - and cost the taxpayer more in the process." iPolitics

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

* **Complaints about elderly B.C. couple's arrest prompt federal investigation**
Days after troubling footage emerged of Mounties arresting an elderly couple in Coquitlam, B.C., a federal agency is launching an investigation into the officers' conduct. The Civilian Review and Complaints Commission for the RCMP said it has received more than a dozen complaints from people expressing concerns about the YouTube video, which at one point shows an officer dragging a senior down a stairwell. "We've received approximately 15 complaints from concerned citizens," said Richard Evans, senior director for the independent agency. "Some were present at the scene and some were not." The incident, which took place after a heated strata meeting at a Best Western hotel, is already being investigated by the New Westminster Police Department, which will decide whether to recommend charges against the officers involved. But the Civilian Review and Complaints Commission's probe could potentially lead to changes in RCMP policy moving forward, Evans said. "Our investigation is designed to make findings and recommendations about [officers'] conduct to inform better policing practices," he told CTV News. "Issues like: Did they have the authority to arrest? Was the appropriate use of force used? Were the RMCP members there properly trained? Were they properly supervised? Was there a language issue?" CTV News

Elderly couple speak out about Coquitlam RCMP altercation caught on video
An elderly Korean couple are speaking out about how they were treated by Coquitlam RCMP after a video of the incident went viral. Seventy-eight year old Myung Ju Lee was shown being dragged down the

stairs by an officer after police were called to the local Best Western hotel on Oct. 26. “Then the police come in and grab my arm, and twist it, then.. push the stairs.” Police were originally called after reports that a fight had broken out at a regular strata meeting. RCMP said in a statement following the incident that the couple had refused to leave the site at the time. “Then the police come in and grab my arm, and twist it, then.. push the stairs.” Police were originally called after reports that a fight had broken out at a regular strata meeting. RCMP said in a statement following the incident that the couple had refused to leave the site at the time. Myung Ju’s wife, Kap Su Lee, was also restrained by officers and says she was left with bruises. Their five-year-old granddaughter was with them the entire time, she can be seen screaming and crying throughout the video footage. The young girl is living with her grandparents full time so that she can attend school in Vancouver while her parents live in Edmonton. AM 730

*** La SQ met sur pied un grand centre de «cybersurveillance»**
Le directeur général de la SQ, Martin Prud'homme, a confirmé la création de cette équipe spéciale à La Presse, hier, lors de la conférence parrainée conjointement par l'UNESCO et le gouvernement québécois, à Québec, et ayant pour thème «Internet et la radicalisation des jeunes». Une vingtaine de policiers travailleront sous peu dans cette unité centralisée sous les ordres du capitaine Jean Lafrenière. Et les budgets seront au rendez-vous, promet le patron du corps policier. Même si les logiciels, les équipements et la formation coûtent cher dans ce domaine. «C'est un des sujets de discussion à la conférence aujourd'hui: on se doit d'être au bon niveau dans l'ensemble des domaines. On veut regrouper nos équipes et augmenter leurs ressources humaines et matérielles. C'est vraiment une priorité», a affirmé M. Prud'homme. Ces patrouilleurs du Net devront être à l'affût d'un ensemble de crimes, pas seulement de ce qu'on appelait autrefois la cybercriminalité. «Aujourd'hui, on peut avoir de l'extorsion sur internet, des agressions sexuelles, de la pornographie juvénile ou de la radicalisation», dit M. Prud'homme. Des policiers du Service de police de la Ville de Montréal et de la Gendarmerie royale du Canada participent déjà à l'initiative, dont le succès reposera aussi beaucoup sur la collaboration de la population, selon le directeur général, qui encourage les citoyens à dénoncer les gestes potentiellement criminels sur le web, même s'ils peuvent parfois avoir l'impression que leur signalement reste sans effet pendant longtemps. La Presse

*** Faire notre travail**
Tout a commencé par un texto de l'éditeur adjoint de La Presse, Éric Trottier. « Faut que je te parle, jeune homme. » C'était jeudi en fin d'après-midi, je venais de finir une répétition pour l'enregistrement de Deux hommes en or, l'émission que je coanime à Télé-Québec. Je rappelle donc Éric. Sur le bruit de fond caractéristique des conférences téléphoniques, il m'annonce qu'il est avec Patrick Bourbeau, l'avocat de La Presse. Me Bourbeau m'explique les détails de l'affaire. Les quatre policiers arrêtés en juillet_ Mon nom qui apparaît sur le radar des enquêteurs_ Une demande faite à un juge_ Un de nos procureurs qui parle à celui de la Couronne. Et mon téléphone, espionné pour ses métadonnées pendant six mois. Pendant six mois, la police de Montréal a pu avoir accès à tous les numéros qui entraient dans mon téléphone, à tous ceux que je composais. Pour des appels ou pour des textos. Si vous m'avez appelé entre le 13 janvier et le 7 juillet, si je vous ai appelé, si nous avons échangé des textos : la police de Montréal le sait. Ce fut plus fort que moi : dans le hall du Monument-National, j'ai lâché un gros juron du terroir québécois qui commence avec un T et qui finit avec un K. En majuscules. J'étais sous le choc. Sans être expert du droit des médias, j'ai tout de suite anticipé ce qui s'est confirmé par la suite : la police qui obtient le droit d'espionner un journaliste de la sorte, c'est du jamais-vu au Canada. Ça ne s'est pas vu pour trouver les sources d'articles traitant de sécurité nationale, de l'armée canadienne, de terrorisme. Mais le SPVM, lui, a obtenu le droit inusité de m'espionner pour des affaires de crimes de droit commun qui sont, dans le grand ordre des choses, stupéfiantes de banalité. La Presse, 4

*** Montreal journalist ' spied on ' by police**
A Montreal journalist whose iPhone was monitored by police for months says he was outraged to discover he had been '' spied on '' as part of what he calls an effort to identify his sources. '' I was living in the fiction that police officers wouldn ' t dare do that, and in the fiction that judges were protecting journalists - and this type of police intrusion ,'' Patrick Lagace, a columnist for La Presse, said in an interview Monday '' Clearly, I was naive .'' The French-language newspaper said it learned at least 24 surveillance warrants were issued for Lagace ' s phone this year at the request of the Montreal Police ' s special investigations unit. That section is responsible for looking into crime in the police force. Three of

those warrants reportedly authorized police to get the phone numbers for all Lagace ' s incoming and outgoing texts and calls, while another allowed them to track the phone ' s location via its GPS chip. The surveillance was ordered as part of an internal probe into allegations police anti-gang investigators fabricated evidence. Five police officers were arrested this summer and two were charged as a result. Lagace said police told him they obtained the courtauthorized warrants because they believed the target of one of their investigations was feeding him information. Canadian Press (London Free Press, N3, Leader-Post, Vancouver Sun, Edmonton Journal, Ottawa Citizen, Windsor Star, StarPhoenix, Waterloo Region Record, Calgary Herald, National Post); Montreal Gazette; Le Devoir; Globe and Mail; Toronto Star; La Voix de l'Est

*** Liberté de presse et protection des sources journalistiques - Les élus doivent passer aux actes**
Un article d'opinion rapporte, « Nous, dirigeants des principales salles de rédaction de Montréal, tenons à exprimer notre indignation et notre inquiétude face à l'espionnage électronique du journaliste Patrick Lagacé par la police de Montréal. Il est inacceptable que des enquêteurs aient pu obtenir accès aux données téléphoniques et à la géolocalisation d'un journaliste sans autre motif que d'identifier des sources journalistiques à l'intérieur du corps de police. Ce n'est pas le seul cas d'intrusion injustifiée des autorités policières dans le travail des journalistes. En juin, le premier ministre Justin Trudeau avait qualifié d"' inacceptable " la filature par la GRC des journalistes Joël-Denis Bellavance et Gilles Toupin, de La Presse. Puis en septembre, l'Assemblée nationale a adopté à l'unanimité une motion pour " rappeler l'importance du principe de protection des sources journalistiques " après que la Sûreté du Québec eut perquisitionné l'ordinateur du journaliste Michaël Nguyen, du Journal de Montréal. Dans les trois cas, les élus ont soit dénoncé l'intervention policière, soit s'en sont dits fortement préoccupés. Des actions concrètes sont nécessaires pour protéger les sources journalistiques formellement. C'est essentiel pour la liberté de la presse, un droit fondamental consacré par la Charte canadienne des droits et libertés et reconnu par la Cour suprême du Canada. La procédure pour obtenir un mandat de surveillance contre un journaliste doit être plus contraignante pour les corps policiers. » Le Devoir, A9

*** A bad precedent**
An editorial states, ""'Are you a journalist?" tweeted American whistleblower Edward Snowden on Monday. "The police spying on you specifically to ID your sources isn't a hypothetical," he warned. "This is today." Snowden was referring to the case of Patrick Lagacé, a columnist at Montreal's La Presse newspaper, who revealed that police have been spying on him for months, tracking his whereabouts using his cellphone and monitoring his calls and texts. Montreal police suspected that a target of one of their internal investigations was leaking information to Lagacé and so applied for - and, bizarrely, received - a series of warrants to monitor the columnist. The state spying on a journalist suspected of no wrongdoing, in an apparent attempt to identify his sources, is unprecedented in Canadian history and poses a troubling threat to freedom of the press." Toronto Star, A10

Woman killed by son had informed police she was afraid of him
Statement heard at sentencing of Michael McCormick, who pleaded guilty to manslaughter. Ten days before she was killed, Pamella Dyer told police she was afraid of her adult son, Michael McCormick, because crystal meth made him delusional. "He thinks I'm not his mother, that I'm out to get him," Dyer told RCMP in a video recorded statement on July 10, 2014. "He's using meth," she said on the recording, played in Victoria Supreme Court Monday. "And when he is in that state, he is as strong as an ox and he has no mind." On July 20, 2014, Dyer, 64, was found lying dead in her Sooke home, at 2227 French Rd. McCormick was arrested and charged with second-degree murder on Sept. 17, 2014. McCormick, 38, was in B.C. Supreme Court for a sentencing hearing on Monday after pleading guilty to manslaughter in his mother's death. He entered the guilty plea on Oct. 11. Prosecutor Ruth Picha told Justice Brian Mackenzie that the Crown is seeking a prison sentence of 12 to 15 years. Picha said McCormick's addiction to crystal meth and personality disorders led to bizarre behaviour. But psychiatric examinations determined McCormick is not mentally ill. Times Colonist, A1/Front

Vader reversal cold comfort for McCann clan
"This has gone on a long time, to say the least," Justice Denny Thomas said with a grimace. That's an understatement. On Monday, Thomas vacated Travis Vader's two second-degree murder convictions, which he had handed down Sept. 15. In effect, he reversed himself and found Vader was not guilty of

murder. But Thomas wasn't done. He then found the Alberta man guilty of two counts of manslaughter in the deaths of Lyle and Marie McCann, the St. Albert seniors who disappeared west of Edmonton while on a camping holiday in June 2010. (…) A more likely sentence, suggested Sankoff, could be around 15 years. Crown prosecutor Ashley Finlayson seemed sanguine Monday. "We felt justice would be done," he said calmly outside the courthouse. It may not look like justice to everyone. After 6-1/2years of blunders by the RCMP, the Crown prosecutors office and the trial judge, this case has taxed public patience and diminished public confidence in the administration of justice in Alberta. Edmonton Journal, A1/Front; * Globe and Mail

Jury watches video recording of Morningstar's police interview
Devin Morningstar told police investigators during a jailhouse interview, a video recording of which was shown to jurors Monday, that Marissa Shephard sent her young son away hours before Baylee Wylie was killed, telling people at her house she was worried for his safety. (…) In the video, played in Court of Queen's Bench, Morningstar was crying and unintelligible at times at the start of the video as he spoke to two police officers from the RCMP Major Crime Unit who visited him in jail two days after his arrest for murder. In the Dec. 20 video, Morningstar said he participated in the attack on Wylie but didn't kill him. "I know I deserve a punishment, but I did not murder that guy," he told Codiac RCMP Sgt. Jim MacPherson when the video was played for the jury Monday morning. "Who did?" asked the investigator. "Tyler," said the murder suspect. Times & Transcript, A1, Front

* **Former military members who were discharged over sexuality launch class-action suits**
People discharged from service because of their sexuality say they suffered extreme psychological trauma from the experience by inaction from Ottawa, former members of the Canadian military who were discharged because of their sexuality are launching class-action lawsuits against the federal government. The plaintiffs seek redress for members of the Canadian Forces and the federal public service "who were investigated, targeted, sanctioned and/or who were discharged or terminated by the Government of Canada because of their sexual orientation, gender identity or gender expression," according to a statement of claim deposited Monday in Quebec Superior Court. (…)Beginning in the 1950s, security agencies sought to identify suspected homosexuals serving in the military and public service, including government agencies such as the CBC and the National Film Board. The investigations continued until the 1990s, when the Mulroney government ordered an end to the practice. At one point, the RCMP had the names of 9,000 people on file. Those targeted were subject to dismissal, demotion or other punishment. Many simply left the military or the public service rather than face investigation. Ms. Roy was dismissed from the military in 1984, after being labelled a sexual deviant because she is a lesbian. Globe and Mail

Inquest into police shooting death of Felix Taqqaugaq begins in Igloolik: Man was shot in his own home after officers say he threatened them with a weapon
More than four years after Felix Taqqaugaq was shot and killed by RCMP officers in his own home, his family and the community of Igloolik, Nunavut, will get some answers starting today. Taqqaugaq died March 20, 2012. A coroner's inquest into the death begins Tuesday morning in Igloolik and is scheduled to run until Nov. 11. It's a mandatory inquest since the death was police-related. Nunavut Chief Coroner Padma Suramala will preside over the inquest, which will detail the events surrounding Taqqaugaq's death, and the findings from the subsequent investigation by the Ottawa Police Service. The details of the investigation, which was completed last year, have not yet been made public. In March 2012, Taqqaugaq phoned in to the community radio station in Igloolik and started ranting. Family members said he suffered from mental health issues. After the rant, someone in the community called the RCMP and police went to his house to check on him. CBC News

Fort McMurray first responders recognized for battling 'The Beast'
Darby Allen still thinks about the wildfire that swept through Fort McMurray. The Wood Buffalo fire chief has good days and bad; the evacuation of 80,000 people from the city still plays on his mind, the thought of, "Could we have done more?" Monday was one of the good days, as he and his fellow first responders were recognized at the Alberta legislature for their work during the disaster. (…) In addition, companies without a firefighting plan or a lack of firefighting equipment on-site could also face a fine of $10,000 per offence. There will also be an increased focus on handing out tickets for careless use of campfires. Peace

officers, forestry, fish and wildlife and conservation officers and RCMP officers will be able to hand out tickets from $150 to $1,000. Roughly 70 per cent of wildfires in the last five years were caused by people and RCMP have said they believe the Fort McMurray fire was caused by human activity. Edmonton Sun

*** Ex-tax auditor acquitted in corruption case**
One of the eight Canada Revenue Agency auditors charged in connection with an RCMP investigation into alleged corruption at the taxman's offices was acquitted at the Montreal courthouse Monday. Quebec Court Judge Christian Tremblay found Luigi Falcone not guilty on all four counts he has faced since 2012, when charges were laid against him in Project Cloche. The charges involved allegations that Falcone, 54, of Laval, Que., solicited a $50,000 bribe from a man who owned a restaurant in Notre-Dame-de-Grâce at the time. The owner, Mario Agostini, alleged that Falcone falsely claimed he had looked at his file at the Canada Revenue Agency, found out it was going to pursue him for $250,000 in undeclared revenue and warned he might go to jail. Agostini testified that he turned down Falcone's offer after consulting a lawyer and an accountant. Six witnesses testified for the Crown during the trial in February. Falcone gave evidence in his own defence. "Mr. Agostini is not credible and (was) unreliable concerning some of his testimony," Tremblay said before acquitting Falcone, who worked for CRA in 1990-2009. The judge even raised the possibility that Agostini misunderstood Falcone after asking his advice on what to do about the actual audit his restaurant was about to be subject to. Leader-Post, N6 (Windsor Star, National Post, Gazette)

*** Man arrested after costume gun scare at Camosun**
What's thought to be a poorly-thought out Halloween costume caused a scare at Camosun College's Lansdowne campus Monday afternoon when a man was spotted in army fatigues and what looked to be a pistol strapped to his leg. A 28-year-old man has been arrested and Saanich police are recommending one charge of possession of a weapon for a dangerous purpose. Police responded to several reports of a man with a handgun on the Lansdowne campus around 3 p.m. Officers were on scene within four minutes and quickly arrested a man, said Saanich police spokesman acting Sgt. Jereme Leslie. A replica hand gun was seized. "We would like to remind people that carrying an imitation firearm is extremely dangerous, even at Halloween," Leslie said. "Responding to this incident put many people at possible risk." It's unclear if the man is a Camosun student. The man will appear in court in mid-December. (…) Victoria police took 12 people into cells for public intoxication between noon on Friday and noon on Monday, according to department spokesman Bowen Osoko. West Shore RCMP arrested two people for public intoxication Saturday night. Times Colonist, A3

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Prison watchdog alarmed by pepper-spray use
Canada's prison watchdog is calling for tighter controls on the use of pepper spray in federal penitentiaries amid concerns correctional officers have taken to dousing inmates with the noxious repellent on a "routine" basis. Pepper spray was used in 60 per cent of the incidents in which Correctional Service Canada officers used force last year, correctional investigator Howard Sapers said in his annual report on the state of Canada's prisons and prisoners, released Monday. That works out to more than 1,000 times - three times as often as five years ago. The increase was not the result of an increase in dangerous security incidents, said Sapers, who instead blamed the simple fact that pepper spray became standard equipment for correctional officers in September 2010. As a result, officers are abandoning other interventions, such as simply talking to inmates, in favour of their spray cans. Correctional Services Canada said it is reviewing its policies around the use and oversight of pepper spray and other chemicals and will report back in April. Canadian Press (Times & Transcript, B3, National Post, Red Deer Advocate, Daily Gleaner); Le Devoir; Le Journal de Montréal (Le Journal de Québec)

*** Former inmates get fresh start by launching their own businesses**
Learning about the principles of entrepreneurship, from writing a business plan to managing cash flow and developing marketing strategies, is important to anyone looking to start a small business. When the lessons are delivered in a federal penitentiary, they are all the more critical, educators and volunteers

who offer such courses say. The audience is captive, to say the least, and the message is particularly poignant given the sort of past business experience many prisoners have, as well as their challenging job prospects for the future. "You can't just hang out a shingle and say you're open for business," says Sue Tait, a business consultant and teacher in Bracebridge, Ont., who has developed an entrepreneurial training program for inmates. "Being self-employed eliminates a huge barrier that many inmates face upon release." Ms. Tait, who owns a small business selling jewellery along with her husband, Stan, and has a background teaching entrepreneurship to at-risk populations, was contracted last year by St. Lawrence College to deliver the course to two groups of inmates at Beaver Creek Institution, a minimum– and medium-security federal prison operated by the Correctional Service of Canada (CSC) in nearby Gravenhurst, Ont. CSC provides a broad range of correctional programs and interventions to meet offenders' needs and address their risk of reoffending, says Brittanie Sullivan, a spokeswoman for the service. Corcan, a special operating agency within CSC, provides employment, vocational training and employability skills to offenders. Globe and Mail

*** Ottawa plans to reduce use of mandatory prison sentences**

The Trudeau government intends to cut widespread use of mandatory minimum sentences by giving judges back their discretion over punishment, Justice Minister Jody Wilson-Raybould says. The changes will undo a major element of the Harper government's tough-on-crime agenda. Judges will be given the "appropriate discretion to be able to impose sentences, engage and understand - as they do better than anybody else - the individual that is before them," the Justice Minister told The Globe and Mail in an interview as the Liberals near the end of their first year in power. "To base their decisions on the actual circumstances of the case before them and render judgment." She said new legislation on mandatory minimums is coming soon, "certainly in the early part of next year." Last month, the government gave judges back the discretion they had lost in 2013 over the victim surcharge - a financial penalty from which judges once routinely exempted impoverished offenders, until it became mandatory. A new federal law rolling back mandatory minimum terms could cut the number of Canadians incarcerated, which is high despite falling crime rates. It could also reduce the rates of indigenous people behind bars. Globe and Mail, A1

*** Killer wants out: Bernardo's day-parole hearing set for March**

School girl killer Paul Bernardo has a day parole hearing tentatively set for March, the Toronto Sun has learned. Bernardo was sentenced in 1995 to life in prison with no parole for 25 years for the horrific sex slayings of teens Leslie Mahaffy and Kristen French. Lawyer Tim Danson, who represents the Mahaffy and French families, said he believes the system will work. "I don't believe that Paul Bernardo will ever be paroled, now or in the future," Danson said Monday night. "Having said that, remember, I represent the victims of Paul Bernardo, and so we will take nothing for granted, we will be very vigilant." Prominent Toronto criminal lawyer Edward Prutschi, who has no connection to the case, said he's also confident Bernardo will not taste freedom anytime soon. "He's the poster child for incarceration in Canada," Prutschi said. "If there's one person who personifies the desire to actually see somebody serve the rest of their life behind bars, it's Paul Bernardo." Toronto Sun, A16 (Edmonton Sun, Winnipeg Sun, Ottawa Sun, Winnipeg Sun); Toronto Star

Years in solitary 'disturbing,' Wynne admits

The treatment of an inmate held in segregation for four years is "extremely disturbing," Ontario Premier Kathleen Wynne said Monday, but she declined to call it torture. Adam Capay has been in isolation for 52 months at a Thunder Bay, Ont., jail. Until recently he had been held in a Plexiglas cell with the lights on 24 hours a day, but after his case gained public attention, Capay was moved to a standard cell, with access to a day room, telephone and television, though is still being kept apart from the general population. Correctional Services Minister David Orazietti said Monday he has asked ministry officials to confirm that no one else is being held in the conditions Capay faced for four years. Federal correctional investigator Howard Sapers called Capay's case "troubling," and said he had never before heard of someone being kept in such conditions. There have been cases, however, in the federal system in which offenders are kept in segregation for years, he said. "Until we have a legislated cap, I'm very concerned that long-term segregation and segregation that could go on almost indefinitely is still possible," Sapers said in Ottawa. Critics have called the 23-year-old First Nations man's treatment torture, but Wynne would not, when asked Monday. Canadian Press (National Post, A5, Waterloo Region Record, Hamilton

Spectator, * Kingston Whig Standard); Globe and Mail; * Toronto Sun (Ottawa Sun, Edmonton Sun); * Le Droit

Canada's record in human rights 'on the upswing'
Canada's human-rights record has improved in the year since the Liberals took office, but major issues regarding prisons and First Nations remain, says the secretary general of Amnesty International Canada's English division. Excessive solitary confinement and stepping on indigenous Canadians' cultural concerns are troubling, despite steps forward, Alex Neve told the Times Colonist. Amnesty was founded in 1961 as a source of support for the unjustly imprisoned, and Neve draws attention to "the outrageously excessive use of solitary confinement in the Canadian prison system." Any more than 15 days in a row is torture, and Canada is guilty of that, he said, adding that Canada's rates of solitary confinement are far greater than in other democracies. "We use it more frequently and for longer periods of time. Solitary confinement isn't just a prison management tool; it very often constitutes torture," he said. "Its impact is severe and often irreversible, and even UN human rights experts have made it clear that solitary confinement should never be used for more than 15 days at a time." Canadian prison watchdog Howard Sapers issued a report last March saying that on any given day, 500 federal prisoners are in solitary. More than one-quarter of inmates are in solitary during their sentences. Times Colonist, A4

* **Adam Capay's lawyer plans 'habeas corpus' application to review solitary confinement**
The lawyer for a 24-year-old First Nations man who had been in solitary confinement in Ontario for more than four years says he will ask the court to formally review his client's detention. Anthony Bryant is representing Adam Capay on the charge of first degree murder. Capay was charged in 2012 with the death of another inmate at the Thunder Bay Correctional Centre. Since then he has been held in segregation, most recently at the Thunder Bay District Jail, where his situation came to the attention of the Chief Commissioner of the Ontario Human Rights Commission during a tour last month. Bryant said he is planning to file a habeas corpus application "to have the nature of [Capay's] pre-trial detention reviewed and to see if that can be properly ameliorated." Habeas corpus is a legal concept - a test of the validity of a prisoner's detention - dating back to the Common Law of England. CBC News

* **Capay case**
Re Long Stay In Segregation Could Mitigate Prosecution Of Capay (Oct. 31)
A letter to the editor states, "Like many others, I was horrified to read of the plight of Adam Capay who has spent four years in solitary without facing trial, only to be taken out of one solitary cell and placed in another. The inhumanity of that is mind-boggling." Globe and Mail, A10

* **Capay case**
Re Solitary Confinement Is Pure Torture. I Know, I Was There (Oct. 31
A letter to the editor states, "As I read Donald Best's piece, all I kept thinking was, "In my country?" How can this be? My Canada does not include such human rights violations. Apparently I am very wrong." Globe and Mail, A10

* **Capay case**
A letter to the editor states, "What is happening in Canada? I am appalled by the story about the young man held in solitary in an Ontario jail for four years, without a trial." Globe and Mail, A10

* **Dennis Oland's lawyer asks top court to rule in its favour**
Dennis Oland's lawyer says the country's top court must find that the New Brunswick Court of Appeal made a mistake in originally denying his client bail "so it can't come back to haunt us" if a pending second murder trial takes an "unfortunate turn." Less than a week after he walked free from a Fredericton courthouse, still charged with the murder of his father but his conviction now overturned, Oland was in Ottawa as the Supreme Court of Canada heard arguments on a potentially groundbreaking legal question. Despite successfully securing a re-trial and then his release from custody, the country's top court - on the ask of Oland's lawyer and several interveners, including other provinces - decided to use the Oland case to delve into when convicted killers can be granted bail. Dennis Oland made the trip to Ottawa to watch. Daily Gleaner, A1; Canadian Press (Cape Breton Post, Chronicle-Herald, Red Deer Advocate)

*** Fry society wants mandatory jail death inquests reinstated**
The province isn't backing away from removing a level of accountability in the death of inmates. Right now, a coroner's inquest takes place if someone being held in a Saskatchewan correctional facility or in police custody dies. The only time an inquest is not held is if the person clearly died from natural causes. Now, the province is removing the part of the law that makes those inquests mandatory. Coroner's inquests aim to determine how, when, where and by what means someone in custody died, while also informing the public about the circumstances of the death. They also alert the public to dangerous practices within provincial correctional facilities and make recommendations to avoid preventable deaths. Sue Delaney, executive director of the Elizabeth Fry Society, says the decision by the government is short-sighted and does a disservice to the justice system. StarPhoenix, A2 (Leader-Post)

*** Inmates awaiting trial put pressure on jail system**
Manitoba's provincial adult jail population is rising quickly, largely due to a burgeoning group awaiting trial. Julie Frederickson, the province's deputy minister of justice, told a legislative committee Monday the current count "under roof" stands at 2,555. That's an increase of 100 since June. Frederickson said the increase is mainly due to a rising number of inmates on remand. She said the number of those serving out sentences is relatively stable. The department has said 70 per cent of inmates in provincial jails are on remand. Winnipeg Free Press, B2

*** Overdose kills inmate**
Justin Thompson was supposed to get out of jail this week, after beating his main charges and finishing up a minor sentence. Instead, he died Monday in his London provincial jail cell of a drug overdose, just days before completing a three-week term for failing to get fingerprinted. His cellmate, a man accused in a Sarnia murder case, was clinging to life in hospital. Both men, sources say, fell victim to illegal drugs - likely heroin - at Elgin-Middlesex Detention Centre (EMDC), a frequent flashpoint for troubles in Ontario ' s correctional system. The overdoses also come amid mounting debate over why the jail still isn't equipped with a body scanner that can detect weapons and drugs. London Free Press, A1

Dangerous offender status sought for man
It's been a long time coming, but the office of Kingston's Crown attorney is applying to seek a dangerous offender designation for a 39-year-old sexual predator initially sent to prison in 2004 for drugging and raping three women in North Bay between 1999 and 2002. The decision follows Rene R. Bourdon's convictions in Kingston's Superior Court on two new counts of sexual assault in the Kingston area; eight violations of the long-term supervision order imposed on him 12 years ago at his original sentencing; and fraudulent personation in the service of a sex scheme of Rube Goldberg complexity. In the first nine months following his release in November 2005, however, his release was suspended four times for violating conditions of the LTSO and he was shunted between all three (at that time) Ontario federal halfway houses directly operated by Correctional Service Canada. Known as community correctional centres, they're the the only halfway houses in the system that can't refuse to accept high-risk offenders. The Parole Board of Canada banned his computer access and prohibited him from having a cellphone capable of taking photos. After his release, he was sent back to Hamilton, where he was back in hot water with the Parole Board by April 2009, again over a computer. Kingston Whig-Standard, A1

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Opioid overdose treatment kit requires training before use, but available soon**
Government-funded kits announced this summer that will contain the antidote for the deadly drug Fentanyl and other opioid overdoses aren't on the streets yet. While there's no specific timeline, provincial officials are still promising a fall launch. The province announced funding for the Naloxone take-home kits in late August. According to the Department of Health, within days of that announcement, it struck a working group - addictions experts, representatives of regional health authorities, government and the Aids Committee of Newfoundland and Labrador - that has been meeting regularly. People who

take the kit home have to be trained on its use and just last week, a train-the-trainer program got started. The Telegram, A3

*** Authority awaits OK on safe-injection sites**
Vancouver's health authority has applied for two new supervised injection sites to combat the drug overdose crisis. Vancouver Coastal Health says the proposed sites would be embedded into existing community health-care centres that serve addicts in the Downtown Eastside. British Columbia declared a public health emergency earlier this year over a spike in overdoses, many of them linked to the dangerous opioid fentanyl. Vancouver Sun, A8

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Indigenous and Northern Affairs Minister speaks at Trinity College: Bennett talks Nation-to-Nation, endangered languages, re-Indigenizing urban spaces**
Federal Indigenous and Northern Affairs Minister Carolyn Bennett spoke at Trinity College on October 28. The event was part of a series called *Conversations with the Chancellor Bill Graham*; it consisted of a brief introduction made by Trinity Provost Mayo Moran, a discussion period, and a question and answer period. A reception was held when the formal event finished. (…) The preservation of Indigenous languages was also discussed; Bennett reiterated that the endangered languages and the extreme importance of Indigenous education are the responsibility of the government. Throughout the conversation, specific examples of Indigenous concerns and issues arose. There was discussion on pipelines, the United Nations Declaration on the Rights of Indigenous Peoples, missing and murdered Indigenous women and girls, as well as the Trans-Pacific Partnership deal. (…) In terms of resolution, Bennett said that the government must change their "urban-Aboriginal strategy." Bennett explained how this relies on a "commitment to reconciliation." Varsity (U of T)

*** Alberta trucking company says racist slur sticker 'a joke'**
A photo taken of a truck with a sticker above the front grill has gone viral on social media as a result of its derogatory language towards indigenous women. The sticker, which read "One Squaw Too Many," was spotted in the area of Grande Cache, Alta. and has some wondering if charges should be laid for hate speech. Grande Cache RCMP confirmed they received a complaint about the truck and have dealt with the matter, declining to go into anymore detail. No charges have been laid against the company. Sandra Jansen, MLA for Calgary-North West who shared the post on social media, said when she saw the post it made her blood boil. "There's absolutely nothing funny about this when across the country we're defining the parameters of the Missing and Murdered Indigenous Women Inquiry and talking about some serious endemic problems." she said. Metro News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

Hope for 'Liberal mandate' sways PSAC to reopen talks with Treasury Board
The largest federal union says it has decided to return to the bargaining table this week with the federal government's promise of a "revised mandate" that could revive stalled contract talks. Robyn Benson, president of the Public Service Alliance of Canada, said Treasury Board negotiators signalled the government may be willing to move on key issues, including the contentious issue of replacing the existing sick leave regime. (…) The Liberals picked up bargaining a year ago and have so far stuck with the same short-term disability proposal the Conservatives made - with some improvements. Benson said

PSAC had no further dates booked for bargaining until Treasury Board negotiators recently suggested the government was ready to make changes to its previous position. With that, the bargaining team for the border guards at the Canada Border Services Agency meet with federal negotiators Tuesday. The rest of the bargaining teams have booked talks for Thursday and Friday and into the weekend. Benson said she expects an up dated position on the proposal to replace sick leave with a shortterm disability plan. Unions have signed a solidarity pact against making concessions on the issue. PSAC previously asked the government to take sick leave offthe table to get negotiations going again. Postmedia Network (Ottawa Citizen, A3, Ottawa Sun)

*** Passer «de la parole aux actes»**

Plusieurs centaines de fonctionnaires fédéraux sont descendus dans la rue lundi midi pour montrer leur mécontentement devant le bureau du premier ministre Justin Trudeau, réclamant qu'il passe «de la parole aux actes». En ce 31 octobre, jour de l'Halloween et à la veille de la reprise des négociations en vue du renouvellement de la convention collective, plusieurs syndiqués de l'Alliance de la fonction publique du Canada (AFPC) étaient costumés pour cette bruyante manifestation, appuyés par des collègues représentant d'autres organisations syndicales. Ensemble, ils voulaient rappeler au gouvernement Trudeau qu'ils sont toujours en quête d'un nouveau contrat de travail alors que les discussions ont été amorcées il y a déjà plus de deux ans. Les manifestants en avaient aussi gros sur le coeur en raison des problèmes avec le système de paie Phénix qui ne sont toujours pas réglés, malgré l'engagement de résoudre les 82000 dossiers problématiques en ce jour du 31 octobre. «Lors des dernières élections, la population a dit non aux coupes du gouvernement conservateur dans les services publics. Mais nos membres n'ont vu aucun changement depuis l'arrivée des libéraux. M. Trudeau est déguisé en Stephen Harper. Il est temps qu'il change son costume», a lancé la présidente de l'AFPC, Robyn Benson, qui a reproché au gouvernement libéral d'avoir recyclé le programme des conservateurs à la table de négociation. L'AFPC a décidé de retourner négocier mardi après avoir appris qu'un nouveau mandat a été donné aux négociateurs du Conseil du Trésor. «S'il n'y a pas d'entente cette semaine, nous allons devoir constater que c'est l'impasse dans les négociations», a indiqué la présidente Benson. Le Droit, 9 (La Presse)

*** «Le respect, pas sorcier!»**

C'était jour d'Halloween et de manifestation lundi au Centre fiscal de Shawinigan, d'où le thème «Le respect, c'est pas sorcier!». Et parmi les doléances des membres de l'Alliance de la fonction publique du Canada, il y a ce fameux système de paie Phénix qui fait encore défaut pour 30 000 employés. «Le gouvernement fédéral a confirmé qu'il ne pourra pas régler tous les problèmes liés au système Phénix d'ici le 31 octobre. La sous-ministre de Services publics et Approvisionnement Canada, Marie Lemay, a indiqué qu'il restait plus de 30 000 dossiers à régler. En juin, le gouvernement avait reconnu que plus de 80 000 fonctionnaires avaient été victimes d'erreurs de paye», a fait savoir le conseiller syndical de l'AFPC, Normand Pelletier. La seule retombée positive de ces ratés, c'est qu'un total de 20 employés ont été rappelés au service de la rémunération de Santé Canada à Shawinigan afin de venir à la rescousse du système de paie Phénix. «Bon nombre de travailleurs attendent toujours que la situation se règle. C'est très décevant. Nous avions émis des réserves concernant l'échéance et demandé au gouvernement d'être plus réaliste. Plusieurs questions demeurent sans réponse», avait déjà déploré le vice-président exécutif national de l'AFPC, Chris Aylward. Or, aux 80 000 dossiers qui étaient à régler s'ajoutent les autres cas rapportés depuis juin. «Pourquoi le gouvernement n'en parle-t-il pas?», se demande le syndicat. Le Nouvelliste, 5 (La Presse)

She'll speak in senate for 'the women who have died'

Ashley Smith. Terry Baker. Camille Strickland-Murphy. Veronica Park. Kinew James. They're women who've died behind bars in Canada - and if you know their names, it's likely due to the advocacy of Ottawan Kim Pate, a champion for incarcerated women named Monday as one of a new breed of independent senator. Reporter Megan Gillis spoke with Pate about her optimism that she can make a difference in the Senate. Ottawa Citizen, A8; CBC News; Canadian Press (Chronicle-Herald, Prince George Citizen, Times & Transcript, Times Colonist); Kingston Whig-Standard; Journal de Montréal; Le Droit

OTHER / AUTRE

NIL

INTERNATIONAL

NIL

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 2, 2016 / le 2 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Quebec acts to protect press freedom after police tracking of journalists
The Quebec government has moved quickly with a series of measures to try to restore confidence in the judicial system and protect press freedom amid a widening controversy over the surveillance of journalists by police. Premier Philippe Couillard announced his government would immediately send directives to the province's three largest police forces aimed at making it harder to obtain a search warrant against a journalist. "People have died for the freedom of the press," Mr. Couillard said. (…) The Ministry of Public Security will also begin an "inspection" of procedures at the province's largest forces - Montreal, Quebec City and the provincial Sûreté du Québec. The precise mandate was not clear. And rules to obtain the kind of warrant that put La Presse columnist Mr. Lagacé in the police's sights - a process that has come under heavy criticism - will be tightened. Officers will have to get clearance from the Quebec public prosecutor's office before seeking a warrant before the courts. (…) In Ottawa, **Public Safety Minister**

Ralph Goodale told reporters his government is open to toughening the rules that govern how and when the federal government can investigate members of the media. "***We'll look at the ministerial directive at the federal level to ensure that is appropriate and sufficient in the circumstances. If we think some additional adjustment needs to be taken, we'll make it,"*** he said. RCMP Commissioner Bob Paulson added he was not aware of "any **ongoing investigations or surveillance activities against any journalists."** Globe and Mail, A1

Enquête publique et projet de loi réclamés à Ottawa
La pression s'accentue sur le gouvernement Trudeau à la suite de l'affaire Patrick Lagacé. Le NPD veut une enquête publique. Le sénateur indépendant André Pratte et le Bloc québécois entendent tous deux déposer un projet de loi sur la protection des sources journalistiques si le gouvernement n'en propose pas un, a appris La Presse. Et le commissaire à la protection de la vie privée du Canada souhaite aussi des lois plus claires en matière de protection des sources journalistiques. Le gouvernement Trudeau estime « prématurée » la question d'une intervention législative, mais le ministre fédéral de la Sécurité publique Ralph Goodale a annoncé hier qu'il « examinera » la directive ministérielle de 2003 demandant aux forces policières de porter une « attention spéciale » au statut des médias dans le cadre d'enquêtes sur la sécurité nationale. Le cabinet du **ministre Goodale** n'était pas en mesure d'indiquer hier si cet « examen » comprendrait des consultations publiques. ***« Le ministre examine la directive ministérielle [_] afin de s'assurer que les plus grands soins sont pris lorsque des enquêtes criminelles et du journalisme se recoupent et que la valeur canadienne fondamentale de la liberté de presse est protégée »,*** a indiqué **Scott Bardsley, attaché de presse du ministre Goodale**, qui se dit ***« toujours ouvert à recevoir des représentations »*** sur le sujet. Plusieurs parlementaires auront des suggestions pour le gouvernement Trudeau. Au Sénat, le sénateur indépendant André Pratte, qui a été journaliste pendant 37 ans (la grande majorité du temps à La Presse) avant d'être nommé au Sénat au printemps dernier, se dit « prêt à déposer un projet de loi privé » si le gouvernement n'a pas l'intention de revoir les lois en vigueur. La Presse + (Le Nouvelliste, Le Soleil, La Voix de l'Est)

Le commissaire à la protection de la vie privée s'inquiète Des lois plus claires sont nécessaires
Le commissaire à la protection de la vie privée du Canada, Daniel Therrien, croit que l'affaire entourant la surveillance policière dont le journaliste Patrick Lagacé a fait l'objet démontre que des lois plus claires en la matière sont nécessaires. Daniel Therrien estime que le Parlement a son rôle à jouer pour mieux orienter les tribunaux quant aux circonstances permettant d'accorder des mandats pour obtenir des informations sensibles. C'est ce qu'il a indiqué au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, mardi. Ce dernier travaille actuellement sur une réforme de la Loi sur la protection des renseignements personnels. (…) Le ***ministre fédéral de la Sécurité publique, Ralph Goodale***, a toutefois fait valoir que la Cour suprême avait déjà énoncé selon quels critères il est justifié que des corps policiers interfèrent avec la liberté de la presse. **M. Goodale** a nié que des directives supplémentaires soient nécessaires. ***«C'est assez clair dans la Charte des droits et libertés. Je ne vois pas comment (nous) pourrions le rendre plus clair que d'enchâsser (le principe) dans la Constitution canadienne»***, a-t-il dit à la sortie d'une réunion du Cabinet. Le ministre a néanmoins invité les associations journalistiques et tous ceux qui veulent livrer des recommandations à le faire. Le chef du Nouveau parti démocratique (NPD), Thomas Mulcair, a pour sa part profité de la période de questions pour exhorter le ministre à indiquer si d'autres journalistes sont actuellement surveillés, demande à laquelle **M. Goodale** a refusé de répondre. Presse canadienne (Le Droit, 16); Canadian Press (Times & Transcript, Chronicle-Herald, Ottawa Sun, Edmonton Sun)

Dompter la police ?
On ne pourra pas accuser, cette fois, le gouvernement Couillard d'avoir trop tardé à réagir ou de l'avoir fait trop mollement. À quelque chose malheur est bon, dit-on, et à peine plus de 24 heures après que l'« affaire Lagacé » eut éclaté au grand jour, Philippe Couillard a annoncé trois mesures importantes, dont une devrait ralentir passablement la « machine distributrice » de mandats de surveillance. Dorénavant, a annoncé M. Couillard, hier, les journalistes jouiront d'un niveau accru de protection, comme les députés, les juges et les avocats, et c'est le Directeur des poursuites criminelles et pénales (et non plus un juge de paix) qui étudiera la demande de mandat faite par un corps de police. La multiplication, pendant des mois, des mandats de surveillance à l'endroit de Patrick Lagacé démontre que c'était presque aussi facile pour les enquêteurs du SPVM que de retirer de l'argent au guichet automatique de la banque du coin.

(…) Au fédéral, le gouvernement Trudeau a d'ailleurs baissé les bras devant la GRC, qui s'est pourtant rendue coupable de filature illégale de deux autres collègues, Joël-Denis Bellavance et Gilles Toupin. Le **ministre de la Sécurité publique, Ralph Goodale**, a affirmé lundi que ***« la liberté de la presse est une valeur canadienne fondamentale »***, mais son gouvernement a décidé le printemps dernier de fermer les yeux sur cette grave violation de la liberté de la presse par la police fédérale. La Presse +; Canadian Press (Red Deer Advocate)

A dark age in our prisons
An opinion piece states, "Canada's prison system has outdone itself again, only not in a good way. The Ontario human rights commissioner recently revealed that Adam Capay had been held in solitary confinement for more than 1,500 days in a Plexiglas room that was constantly bathed in artificial light. This surpassed already horrifying precedents, including those set by Richard Wolfe, who spent 640 days in solitary, Edward Snowshoe, who spent 162 days, and Ashley Smith, who spent close to a year. While these are some of the worst-known cases, the practice is evidently widespread. As the Office of the Correctional Investigator (OCI) noted in its annual report, released in March, there were 8,300 placements in administrative segregation and 200 placements in disciplinary segregation in 2014-15 alone. Most troublingly, the OCI found that Correctional Services Canada was favouring administrative segregation in order to "circumvent the more onerous due process requirements of the disciplinary segregation system." Whereas disciplinary segregation cannot exceed 30 days, administrative segregation can be of indeterminate length. Fortunately, there's reason to believe change is on the way. Prime Minister Justin Trudeau instructed the justice minister last fall to eliminate long-term segregation. Advocacy groups may force the government's hand if its resolve weakens: they are challenging solitary confinement as unconstitutional in court. And in the wake of the Capay controversy, **Public Safety Minister Ralph Goodale** has said a package of prison reforms is forthcoming." National Post, A9

*** OpenMedia meeting with Public Safety emphasized the importance of a genuine consultation on C-51**
A blog post states, "Yesterday, we met with top officials at **Public Safety Canada** to discuss ongoing privacy concerns shared by Canadians across the country. Right now, the ministry is running a public consultation about Bill C-51, privacy, and national security, asking for feedback from Canadians on some of the most pressing civil liberties issues of our time. Meanwhile, we've been hearing from you for well over a year that Canadians expect a full repeal of the "Canadian Patriot Act" -- Bill C-51. Brought into force by Stephen Harper's Conservative government in 2015, Bill C-51 puts our freedom of expression rights on the chopping block, throws the door open to widespread information sharing among a huge range of government agencies, gives CSIS spies powers that would normally be reserved for police, and puts our privacy at risk in a number of different ways. You already know all this -- and that's why you've been calling on the government to take immediate action and completely repeal this legislation and start from scratch. And yesterday, we made sure that **Minister Ralph Goodale's** top advisers were reminded of that fact, and that they promised Canadians they would address our privacy deficit in the last election." Rabble

TOP STORIES / MANCHETTES

Quebec acts to protect press freedom after police tracking of journalists
The Quebec government has moved quickly with a series of measures to try to restore confidence in the judicial system and protect press freedom amid a widening controversy over the surveillance of journalists by police. Premier Philippe Couillard announced his government would immediately send directives to the province's three largest police forces aimed at making it harder to obtain a search warrant against a journalist. "People have died for the freedom of the press," Mr. Couillard said. (…) The Ministry of Public Security will also begin an "inspection" of procedures at the province's largest forces - Montreal, Quebec City and the provincial Sûreté du Québec. The precise mandate was not clear. And rules to obtain the kind of warrant that put La Presse columnist Mr. Lagacé in the police's sights - a process that has come under heavy criticism - will be tightened. Officers will have to get clearance from the Quebec public prosecutor's office before seeking a warrant before the courts. (…) In Ottawa, **Public Safety Minister Ralph Goodale** told reporters his government is open to toughening the rules that govern how and when

the federal government can investigate members of the media. "***We'll look at the ministerial directive at the federal level to ensure that is appropriate and sufficient in the circumstances. If we think some additional adjustment needs to be taken, we'll make it,"*** he said. RCMP Commissioner Bob Paulson added he was not aware of "any **ongoing investigations or surveillance activities against any journalists."** Globe and Mail, A1

Watchdog downplays marijuana revenue potential
The parliamentary budget watchdog is being a bit of a buzz kill when it comes to forecasting government revenue windfalls from legalized marijuana. "We're talking millions and millions - not billions and billions - of dollars of revenues," Jean-Denis Frechette, the parliamentary budget officer, said Tuesday after releasing a study entitled, Legalized Cannabis: Fiscal Considerations. The 77-page report finds that the federal government may have little fiscal space to heavily tax cannabis the way it does tobacco without pushing the legal price well beyond that of currently illicit pot. What's more, the Liberal government's stated aims of decreasing marijuana use and accessibility for young Canadians while choking off pot revenues from organized crime will require a delicate balancing act, the study found. Price legal pot too high and the black market will continue to flourish. Too low and governments could be seen to be encouraging its use. The report projects sales tax revenue in 2018 could be as low as $356 million and as high as $959 million, with a likely take of about $618 million based on legalized retail cannabis selling for $9 per gram - in line with current street prices. Canadian Press (Chronicle-Herald, A1, Toronto Star, Kingston Whig-Standard, Ottawa Sun, Times Colonist, Daily Gleaner, Telegraph-Journal, Times & Transcript, Red Deer Advocate)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Quake readiness : Group sends $65-billion seismic upgrade proposal to Ottawa**
A group that includes Green party Leader Elizabeth May, structural engineers and earthquake-safety advocates are pitching a bold $65-billion program to the federal government to promote seismic upgrades of buildings across Canada. The idea is that Ottawa would reimburse building owners 50 cents on the dollar after seismic upgrades are complete. The program would stretch over 25 years and build resiliency into homes and commercial and municipal buildings, particularly in British Columbia, to counter the risk from a massive earthquake, similar in extent to the quake and ensuing tsunami that hit Japan in 2011, killing more than 16,000 people, or from a shallow earthquake nearer the surface such as the 2011 earthquake in Christchurch, New Zealand, that killed 185 people. The program would also focus on the Ottawa and St. Lawrence river valleys, where a significant earthquake risk has been identified. Scientists have estimated the probability of a major earthquake causing damage in a populated area of British Columbia in the next 50 years at 30 per cent. Postmedia (Vancouver Sun, A6; Vancouver Province)

*** Why I want this veteran-led disaster response team to grow in Canada: When I first heard about Team Rubicon, I was inspired. Little did I know that Canada would need it so soon thereafter**
An opinion piece by Veterans Affairs Minister Kent Hehr states " (…) When I first heard about Team Rubicon, I was inspired-not only by what they were doing, but by the opportunity it presented to the men and women who had served, who would yet again be able to put their incredible skills to work. I felt compelled to do whatever I could to bring them to Canada. Little did I know that Canada would need Team Rubicon so soon thereafter. In May of this year, disaster hit northern Alberta and Saskatchewan with wildfires displacing thousands of people. It was the largest fire evacuation in Albertan history and has been deemed the costliest disaster in Canadian history. I was tasked with heading a cabinet committee charged with leading the federal response. To that end, we expedited more than $400-million to the response and continue to provide any and all assistance that we can. I can tell you that the federal government will continue to stand shoulder to shoulder with the people of Alberta and Saskatchewan for as long as it takes to move past this tragedy. For its part, Team Rubicon deployed more than 80 members from the United States, the United Kingdom, Australia, and from Canada, to help with the relief efforts (…) As minister of veterans affairs and associate minister of national defence, I can tell you that those who have served possess the skills and training to help those coping with disaster. It is why I love Team Rubicon; it allows those volunteering to continue with their mission and to help those most in need

in doing so. I am very proud to help facilitate the establishment of Team Rubicon Canada; it is only fitting that a country with our values has a Team Rubicon to call its own." Hill Times

*** Avalanche educators weigh pros, cons of social media on safety**
As social media continues to grow in popularity, Canadian avalanche educators say it can have both pitfalls and benefits for skiers and snowboarders heading into the backcountry. In October, avalanche experts from around the world met in Colorado for the International Snow Science Workshop. It included discussions on how social media can influence decision making because it can lead to a culture of competitiveness on Instagram feeds and in YouTube videos. Officials in Alberta and British Columbia, however, said there have always been outside factors on how skiers and snowboarders make decisions in the backcountry (...) They also started a new approach last year by having a team of Avalanche Ambassadors, mostly high-profile athletes who have a big social media networks, to promote training and safe backcountry behaviour. Calgary Herald, A9

*** Barely passable grade on flood preparedness demands immediate action: report**
All 10 Canadian provinces and Yukon are not making the grade when it comes to flood preparedness, signalling the need for change, including not allowing municipalities to override provincial or territorial direction on development in flood-prone areas, argues a new report from the Intact Centre on Climate Adaptation at the University of Waterloo. Canadian Underwriter (2016-10-31)

*** Flooding study gives C- grade**
New Brunswick received a 'C-minus' in flood preparedness in a new nationwide report released by the University of Waterloo. The report's authors said the province did well when it comes to responding to emergencies but not as well in preventing them. The report collected data from a survey sent out to provincial ministries and departments involved in flood prevention, mitigation and emergency response management. The survey, conducted between December and April, asked officials to answer questions in 12 categories that included items such as the province's role in mapping flood prone areas, in land-use planning, emergency preparedness and response, and mitigating flood risk to drinking water systems. Daily Gleaner, B4 (Times & Transcript)

*** Thanksgiving storm one for the record books: 'There's no city that could have withstood that kind of a downpour'**
The Thanksgiving Day storm that caused widespread flooding in the Cape Breton Regional Municipality will go down in the history books as the wettest day ever recorded on the island. Reviewing weather data that dates back to 1870, Environment Canada senior climatologist David Phillips said the rain that fell Oct. 10 in Sydney established a new benchmark for precipitation in Cape Breton. A total of 219 mm of rain was recorded that day at one official recording station in Sydney, and at the Sydney Airport 136 mm of rain was reported. "(Previously) the wettest ever day in Sydney was 129 mm back on Aug. 17, 1981," he said. "So this one totally swamped the previous wettest day ever, and that's in any month. I looked at the wettest days in the entire period of records." Provincially, the Oct. 10 storm in Cape Breton will also register among the wettest days ever, with only a rainfall of 239 mm in Halifax on Sept. 21, 1942, eclipsing what happened in Sydney. "It was absolutely unprecedented. It was incredibly damaging," said Phillips. "I do a thing at the end of the year called the top 10 weather stories of the year (in Canada) - this is clearly going to be one of the stories." Cape Breton Post, A4

*** Keeping firefighters safe: Seventeen Cape Breton fire departments receive funding**
A total of 77 provincial emergency service providers have received a safety boost from the government. The province recently announced approximately $1 million, under the provincial Emergency Services Provider Fund, will go to assist fire departments across the province, 17 of which are in Cape Breton (...)The Emergency Services Provider Fund is used to help groups buy equipment such as personal protective equipment, self-contained breathing apparatus and rescue tools. Eligible groups receive up to 50 per cent of eligible costs to a maximum of $20,000. First responders include fire departments, Hazmat organizations and ground search and rescue teams. Cape Breton Post, A2/ FRONT

*** CN Rail to continue oil spill clean-up near Gogama, Ont.**
After months of lobbying and protesting by people in the small northern Ontario town, CN Rail has agreed

to do further clean-up of an oil spill near Gogama. "I was ecstatic for sure," says Gogama fire chief Mike Benson, who was recently elected as the chair of the local services board, the government in the unincorporated township. Benson says he was surprised to find out Monday that CN Rail wants to do further dredging on the Makami River and remove more soil from the river bottom contaminated with oil from the fiery train derailment in March 2015. CBC News (2016-11-01)

*** Le maire de Lac-Mégantic ému**

Le maire de Lac-Mégantic, Jean-Guy Cloutier, s'est dit ému «comme jamais auparavant», au terme de l'inauguration officielle de l'ouverture des rues de son centre-ville, confinées depuis plus de trois ans, inauguration qu'il a effectuée symboliquement sur une bicyclette électrique GeeBee. Ce qui allait très bien avec l'adoption, par les élus municipaux, d'une philosophie écologique pour la reconstruction de leur centre-ville, traduite par plusieurs certifications obligatoires pour la conception des nouveaux édifices, comme Leeds et Novoclimat, pour ne nommer que ces deux-là. «C'est pas croyable, émotionnellement, j'aurais de la difficulté à parler davantage et j'aurai une autre émotion quand je verrai les premières automobiles déambuler sur la rue Frontenac. Les citoyens attendaient ça depuis longtemps. Ils ne viendront pas tous aujourd'hui, avec leurs automobiles. Il y en a qui ne pourront pas. Mais je respecte ça. Que chacun le fasse à son rythme!» a-t-il déclaré. La Presse (La Tribune, 6); CBC News

*** Family claims police bungled search**

The family of a Regina woman whose body was found near Swift Current on Oct. 2 after she had been missing nearly two weeks, have outlined in scathing terms their concerns about the work of the Regina Police Service (RPS), RCMP and Search and Rescue officials in the search for her. The vehicle belonging to 65-yearold semi-retired teacher Judy Campbell was found on Sept. 27. But her body was not found until Oct. 2, when volunteer searchers discovered it in long grass just 225 feet from her Subaru Cross Trek, in an area apparently previously combed over by the combined authorities' search team. Though questions are raised about the search itself, the main concern outlined in a letter to Postmedia News from Campbell's brother, David Howlett, and sister, Karin Mitchell, is that despite Campbell telling her family she was going to Swift Current to visit her mother, police traced a final text from her phone to a cell tower in the North Battleford area. As a result, the search was directed to that region in error, the family claims. Postmedia (StarPhoenix, A3; Leader-Post)

*** Missing Quesnel hunters found 'safe and sound,' police say**

Quesnel RCMP say a pair of hunters are "safe and sound" after not returning from a hunting trip on Saturday. In a release, police say Glen Booker, 55, and his stepson, 10, were found just before noon PT on Tuesday by a helicopter operated by Dunkley Lumber. "The hunters' vehicle experienced mechanical issues on a very remote road forcing them to stay out longer than expected," Sgt. Chris Riddle wrote. "Both individuals are in good spirits and are on their way back to Quesnel to connect with their family." CBC News

*** RCAF SAR Techs come to aid of ailing sailor**

Late Monday afternoon 442 Transport and Rescue Squadron was involved in a mission to medevac a crew member of a commercial fishing vessel to hospital for immediate care, the Canadian Forces said in a news release Tuesday. More details from the news release: The vessel was 60 nautical miles (110 km) northwest of Cape Scott at the time of the call for assistance, A CH-149 Cormorant helicopter and a CC-115 Buffalo were tasked to respond, The Buffalo arrived on scene first and after making contact with the crew by radio provided them instructions to prepare for the arrival of the Cormorant with SAR Techs on board. Ottawa Citizen

*** Family overjoyed missing senior found alive**

The Royal Newfoundland Constabulary says searchers have found William Snelgrove, 82, missing since Monday in the Conception Bay South area after he left to go berry picking. Police were alerted Monday shortly after 7 p.m. that Snelgrove was overdue from his berrypicking trip. He'd last been seen on foot in the area of the Power Substation on Middle Bight Road in Foxtrap just after 1 p.m. Monday. At approximately 3 p.m. Tuesday, a C.B.S. resident located Snelgrove in a wooded area in Conception Bay South near Red Bridge Road. He was treated by the C.B.S. Fire Department and was conveyed to hospital for additional medical assessment. St. John's Telegram, A4

*** Police warn outdoors enthusiasts to prepare for winter months**
With the days shrinking and the weather getting colder, Wood Buffalo RCMP are warning people heading into the wilderness to be mindful of their surroundings and outdoor plans. On Oct. 27, search and rescue teams with Wood Buffalo RCMP spent the day looking for two individuals near the Richardson Sand Dunes and Six Lakes area, located north of Fort McMurray. One individual had gotten lost. The second individual had maintenance issues with the off-road vehicle they were using and needed help. Fort McMurray Today

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** How Montreal police were able to use legal means to track a journalist**
The Quebec government says it wants to make it more difficult to obtain a search warrant that would target a journalist, raising the bar to a higher level – on par with lawyers and judges. The move, announced by Premier Philippe Couillard, comes after it came to light that La Presse journalist Patrick Lagacé was being spied on by Montreal police. Through 24 issued surveillance warrants, the SPVM was able to obtain the identities of the people he spoke and texted with as well as to track his whereabouts via his iPhone's GPS. (...) Though some have pointed to the contentious anti-terrorism legislation, Bill C-51, as a catalyst for more invasive police tactics in Canada, Christopher Parsons, managing director of the Telecom Transparency Project at Citizen Lab, says a bill originally passed to curb cyberbullying may be to blame. Bill C-13 amended the Criminal Code to allow police to, among other things, track an object, person, or transmission of data if the authorities have the suspicion or belief that doing so could assist an investigation. Parsons said that Bill C-13 was "sold to the Canadian public as necessary to stop cyberbullying," but applies to the general public. (...) Even CSIS, he said, "tends to place the monitoring of journalists alongside monitoring of academics or monitoring certain government officials, so they're fairly protected." "The very fact that they were using these very, very invasive tools to monitor where the journalist was going and whom they were speaking with struck me as fairly extraordinary." CBC News

Police union wants chief's resignation
The head of the Montreal police union said police Chief Philippe Pichet should be fired for allowing his officers to spy on journalists, calling the decision to track the cellphones of La Presse columnist Patrick Lagacé and at least three other reporters "unforgivable." "It was a serious error in judgment and it is unforgivable," Yves Francoeur, head of La Fraternité des policiers et policières de Montréal told the Montreal Gazette Tuesday. "The SPVM is the second largest police service in Quebec and the fifth largest municipal force in North America, so we need a strong leader." La Presse reported Monday that police requested 24 search warrants to track Lagacé's iPhone since January, which allowed police to access the numbers Lagacé had called or received calls from and track him by activating a GPS mechanism on his phone. At least three other journalists have since learned they were under similar surveillance by police - Félix Séguin of TVA, Monic Néron from 98.5 FM, and freelance journalist Fabrice de Pierrebourg. Montreal Gazette, A1

*** Journalistes surveillés - La protection des sources passe-t-elle par une loi?**
Ce qu'il faut désormais appeler l"' affaire Lagacé " montre qu'il y a visiblement un problème. Reste à trouver la solution. Vaut-il mieux appliquer les principes établis par la Cour suprême du Canada en matière de protection des sources journalistiques ? Faut-il plutôt enchâsser cette protection dans une nouvelle loi ? Québec réagit au lendemain des révélations d'espionnage par la police de Montréal du journaliste de La Presse Patrick Lagacé, à la suite d'un mandat délivré par une juge de paix magistrate. Le ministère de la Sécurité publique accordera dès cette semaine aux journalistes le même niveau de difficulté pour l'obtention d'une surveillance légale qu'aux députés, juges et avocats. Québec annonce aussi la formation d'un groupe d'experts formé par le gouvernement pour formuler des recommandations

sur le délicat sujet. Le groupe des sages, dirigé par " un juge de prestige ", pourra aller jusqu'à recommander l'adoption d'une loi pour mieux protéger les sources journalistiques. C'était le souhait de Claude Robillard pendant tout le temps qu'il a agi comme secrétaire général de la Fédération professionnelle des journalistes du Québec (FPJQ), de 1989 à 2014. Il n'a pas changé d'idée. Le Devoir, A2I; La Presse (Le Quotidien, Le Nouvelliste, Le Droit, Le Soleil); Montreal Gazette, 1, 2; La Presse +; La Tribune; La Voix de l'Est

* **Des cas controversés ici et ailleurs**
Les pratiques de surveillance des États préoccupent depuis des années les organisations de défense des droits de l'homme. Bien que les révélations d'Edward Snowden sur la National Security Agency (NSA) américaine aient attiré l'attention du public sur les risques inhérents aux nouvelles technologies de communication, nombre d'États continuent à faire la sourde oreille aux appels en faveur d'une plus grande transparence et d'un encadrement accru. Alors que le Service de police de la Ville de Montréal se retrouve sur la sellette pour avoir espionné un journaliste, un nouveau rapport diffusé par l'International Network of Civil Liberties Organizations (INCLO) dresse un préoccupant état des lieux en matière de surveillance en évoquant des cas survenus dans une dizaine de pays, dont le Canada. (…) En 2009, le Service canadien du renseignement de sécurité (SCRS) a demandé l'autorisation à un juge de la cour fédérale de travailler avec le Centre de sécurité des télécommunications (CSTC) pour surveiller deux Canadiens jugés suspects lors de leurs déplacements à l'étranger. Le CSTC n'est normalement pas autorisé à cibler ainsi des Canadiens, mais l'autorisation a été accordée. Le magistrat a appris quelques années plus tard que des services de renseignements étrangers avaient aussi été mis à profit par le CSTC pour espionner les deux hommes, ce qui contrevenait aux engagements pris pour protéger les informations recueillies. Il a fait annuler le mandat en 2013. Le rapport de l'INCLO relève que l'on ne sait toujours pas qui étaient les deux individus ciblés ni quelle était la nature de leurs activités. La Presse +

* **Curbing online extremism 'like trying to block wind'**
Pulling hate material from the Internet will never be enough to curb the phenomenon of violent extremism, the head of free expression and international relations at Google told a conference on radicalization Tuesday. "What we've seen over the past couple of years is a realization that simply taking the content down doesn't work because one website goes down, two or three more are up the very next day," Ross LaJeunesse said. "Simply taking down the content doesn't address the feeling and the hatred which caused the speech in the first place. You need to engage the speakers who are promoting radicalization and hate online." He acknowledged that Google, the U.S.-based company that runs a search engine and the video-sharing service YouTube, has a role to play and argued the company is taking that responsibility very seriously. "We have started doing various programs, where, much like a regular advertising campaign, when someone searches for a key word that we think indicates they're looking for radical content, we then show them an advertising campaign about content that counters that speech," LaJeunesse said. Montreal Gazette, A6

* **De jeunes internautes montent au front**
Pour contrer les extrémistes violents sur le Web, il faut faire en sorte que des jeunes leur répliquent sur le Web, estiment de nombreux participants à la Conférence de l'UNESCO sur Internet et la radicalisation. Charlotte De Mesmaeke, 24 ans, et Amal Hamich, 30 ans, font partie de la délégation belge de « Non à la haine ». « Non à la haine » est une campagne européenne lancée en 2013 pour lutter contre tous les discours haineux en ligne et hors ligne. Après avoir dressé un portrait de la radicalisation lundi, la Conférence de l'UNESCO tournait mardi les projecteurs vers les solutions, ou du moins des pistes de solutions, pour endiguer le phénomène. (…) Amal porte le voile ; Charlotte pas. Elles s'insurgent contre la haine de l'Occident, l'islamophobie et toutes les formes d'intolérance. Dans leurs temps libres, ces deux « activistes » donnent des formations dans les écoles. « On ne met pas de barrière avec les jeunes. On crée un espace sans jugement, précise Amal. Même s'il y a un discours raciste, ce n'est pas grave dans le cadre de la discussion parce que l'objectif, c'est de savoir d'où vient ce discours et ce qui pousse la personne à penser de cette manière. » Au Québec, elles ont collaboré à la création d'un organisme du genre. Le gouvernement Couillard a annoncé mardi une aide de 10 000 $ pour en élargir l'impact. Le Devoir

* **La Commission des droits de la personne juge le projet de loi 62 discriminatoire**

La Commission des droits de la personne et des droits de la jeunesse (CDPDJ) a réduit en pièces, mardi, le projet de loi 62 sur la neutralité de l'État tandis que la Ligue des droits et libertés (LDL) a accusé le gouvernement libéral de vouloir faire du *« profilage religieux »*. C'est l'article 9 qui représente le principal écueil du projet de loi 62, selon la CDPDJ et la LDL, c'est-à-dire l'obligation faite à un employé de l'État de fournir les services, et à toute personne d'obtenir ce service, à visage découvert. (…)La charte des valeurs québécoises du PQ a constitué l'une des sources de la radicalisation de jeunes, suggère l'auteur d'une bande dessinée dévoilée par le premier ministre Philippe Couillard en marge de la conférence Québec-UNESCO sur l'« Internet et la radicalisation des jeunes » mardi. Le bédéiste El Diablo écrit qu'*«* on n'avait pas besoin d'être comme les autres pour faire partie intégrante de la société [québécoise] ». « Ça a changé ? » demande un personnage. « Ouais ! Quasiment du jour au lendemain. Quand ils ont sorti leur fameuse " Loi pour la neutralité des valeurs " », répond un autre. « Il n'y a aucune exagération. C'est la parole des jeunes », a soutenu le directeur général du Centre de prévention de la radicalisation menant à la violence, Herman Deparice-Okomba, qui a commandé la bédé. La charte *« nourrissait le phénomène* [de la radicalisation] *par les mesures d'exclusion »*, a fait valoir M. Couillard. Le Devoir

*** La censure est inefficace contre la radicalisation, dit Google**

Les gouvernements engagés dans la lutte contre la propagande des groupes jihadistes sur internet ont compris que la censure était inefficace et menaçait la libre expression sur la toile, a relevé mardi un dirigeant de Google. «Nous avons assisté à un énorme changement d'attitude des gouvernements», a confié à l'AFP Ross LaJeunesse, responsable des relations internationales du géant d'internet, interrogé sur les lois anti-terroristes adoptées par des pays comme la France ou le Canada dans la foulée d'attaques jihadistes. «À chaque fois qu'une crise éclate, il peut arriver que les gouvernements en fassent trop. Mais nous trouvons, avec les discussions que nous menons actuellement avec eux, que les gouvernements réalisent que la (censure) n'est pas la bonne approche», a-t-il déclaré en marge de la conférence «Internet et la radicalisation des jeunes », organisée lundi et mardi par l'UNESCO à Québec. « Au début, les États ne voulaient pas parler de contre discours et nous disaient seulement: ce contenu est mauvais, retirez-le! », a indiqué M. LaJeunesse, notant que Google se permettait d'interpeler « les législateurs lorsqu'ils sont trop zélés». Agence France-Presse (TVA Nouvelles); Agence France-Presse (Huffington Post) (2016-11-01)

*** Les dessous de la radicalisation**

Mardi, c'était le deuxième et dernier jour de la conférence de l'UNESCO sur la radicalisation violente des jeunes, à Québec. Les organisateurs ont dit que c'est un succès; le premier ministre a dit qu'il va agir. Et l'«Appel de Québec» - florilège de voeux rédigés avant même la tenue des débats - a été signé par les élites... Mais en parlant avec les spécialistes, on a aussi ouvert des portes moins convenues. Jour 2 des morceaux choisis! Le titre est un peu fort! Mais à l'extrême gauche comme à l'extrême droite, chez les djihadistes comme les farouches pro-vie, il existe bel et bien un modus operandi similaire afin d'attirer et retenir des recrues pour gonfler les rangs. La titulaire de la Chaire de recherche du Canada sur les conflits et le terrorisme de l'Université Laval, Aurélie Campana, étudie la question depuis nombre d'années. Sur le terrain. Pour embarquer plus de membres, on remarque que les factions extrémistes, qui avaient l'habitude de se cacher, tendent à sortir au grand jour, observe-t-elle. Ils soignent leur aura : «il y a une euphorisation du discours haineux». Tout pour attirer. Et pas besoin d'enrôler des convaincus. «La radicalisation n'est pas nécessairement préalable au recrutement.» En fait, souvent, les nouveaux ne maîtrisent pas du tout l'idéologie! La Presse (2016-11-01)

Education of women key to curbing radicals, Caliph says

The spiritual leader of up to 20 million Ahmadi Muslims is emphasizing the importance of educating women to prevent the radicalization of youth. "The literacy rate of our women is more than men," said the Caliph, Hazrat Mirza Masroor Ahmad, who was in Saskatoon on Tuesday as part of a Canada-wide tour. "And we say if the woman is not well educated, she cannot train her children well. "If the children are not trained properly, they cannot be good citizens. They cannot be law-abiding citizens. (…) In a morning news conference, he praised Canada as a peaceful country. Canadians are tolerant due to the nation's multiculturalism, and Ahmadis don't face many challenges here - save for the "economic crisis" faced by everyone, he said. Throughout his tour of Canada, the Caliph has addressed the issue of peace - including when he spoke to Parliament in Ottawa earlier this month. When asked about the importance of his message of peace to Muslims, he said "It is quite obvious. This is the message that you need today."

Spreading the "true message of Islam" - peace and harmony - is also the way to address misconceptions about Muslims, he said. StarPhoenix, A1

*** Ottawa falls short of real oversight for C-51 powers**
An editorial states, "Last year, former prime minister Stephen Harper's Bill C-51 brought in controversial new security powers, despite the opposition of hundreds of thousands of Canadians and the advice of legal scholars and civil liberties organizations. Resisting calls from the NDP and others to repeal the law, the Liberal government has kept C-51 on the books. Under the legislation, the sharing of personal information between government agencies was expanded, the Canadian Security Intelligence Service was given unprecedented powers to disrupt terrorist plots and a range of perceived security threats, the right of police to preventively arrest people was expanded, and urging others to commit terrorism became a criminal offence. Now, Parliament is debating a proposal to plug a long-standing gap in our security architecture: Canada today stands alone among our closest allies in lacking independent, elected oversight of security and intelligence agencies. Unfortunately, the government's plan falls short of giving Canadians a real watchdog for their rights and safety. Bill C-22 would create a committee without the powers, the independence and the public trust needed to get the job done. The prime minister and cabinet would appoint its members, hand-pick its head, control the information it receives, block investigations into certain areas, and revise its reports without notifying Parliament and the public." Province, A13

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Canadian couple faces U.S. charges for allegedly importing, exporting fentanyl
A Canadian couple is accused of importing fentanyl products from China into the United States and then mailing the powerful opioid drugs to Canada. Karl and Sorina Morrison, both 59, were arrested at a border crossing near Niagara Falls, N.Y., last month after an investigation by U.S. authorities. The Kitchener, Ont., couple has been charged with conspiracy to import and export controlled substances and analogues, and attempt to export controlled substances and analogues. Each charge carries a maximum penalty of 20 years in prison and a $1-million fine. The couple has pleaded not guilty. In a criminal complaint filed with a New York court, a Homeland Security agent says a package mailed from China to Karl Morrison at a mailbox in a UPS store in Niagara Falls, N.Y., contained four packets, two of which were found to contain types of fentanyl. (…) The complaint notes that the Morrisons have a son and that since 2009, five packages mailed to him were seized by the Canada Border Services Agency after they were found to contain controlled substances. Canadian Press (The Telegram, The Guardian, Times Colonist, 570 News, Thunder Bay Chronicle-Journal, Cape Breton Post, Global News, Guelph Mercury); * Presse canadienne (L'Actualité)

*** The CBSA (As Administrator Of Laws) Must Follow CITT Decisions (Subject To Limited Exceptions)**
This case is a must-read for all customs and trade lawyers. This case is a must-read by other administrative lawyers who appear before quasi-judicial tribunals. The general administrative law rules for law enforcers and tribunals have been clarified in simple, understandable terms. May there be greater certainty, greater predictability and finality as a result of this important case. On October 21, 2016, Justice David Stratas of Canada's Federal Court released a game-changing customs decision/administrative law, which is *Canada (Attorney General) v. Bri-Chem Supply Ltd.*, 2016 FCA 257 (the "Bri-Chem Decision – FCA"). The Federal Court of Appeal has spoken. The Canada Border Services Agency ("CBSA") is an "administrator" of Canada's border laws. The Canadian International Trade Tribunal ("CITT") is a a quasi-judicial tribunal that has been granted the powers of a superior court of record. The CBSA must follow the decisions of the CITT and can no longer ignore decisions it does not agree with (subject to general rules set out below). I will put money on an appeal of the Bri-Chem Decision-FCA to the Supreme Court of Canada. As a result, I expect more significant developments in Canada's customs and trade laws regimes to be forthcoming. But, until then, the Bri-Chem Decision-FCA is a significant decision that will be quoted often by counsel for importers who are the subject of CBSA enforcement actions. It will also be quoted by lawyers who regularly appear before other tribunals. Mondaq

Ottawa unveils strategy to court foreign tech talent
The federal government is rolling out measures to lure more foreign cash and talent to Canada as it tries to dig the country out of a slow-growth trap. The strategy, unveiled Tuesday by Finance Minister Bill Morneau, includes measures that will make it easier for fast-growing Canadian tech firms and multinational corporations operating here to quickly bring in skilled foreign workers for jobs they are struggling to fill in Canada. For qualifying companies, Ottawa said it will establish a twoweek "standard" for approving visas and work permits early next year - down from several months - and create a 30-days-ayear work permit allowing companies to bring in workers for short stints. The permit is intended for intercompany work exchanges, study exchanges and to fill temporary needs, according to the finance department. Globe and Mail, B1

* **Crimes contre nature**
La contrebande d'animaux exotiques est devenue presque banale en Amazonie péruvienne. Singes, tortues, perroquets sont capturés sans égard aux espèces menacées et exportés grâce à la complaisance des autorités. (…) Impossible de savoir si le ministère canadien de l'Environnement est au courant de ce stratagème de permis truqués. Ce ministère, qui est responsable de l'application de la Convention sur le commerce international des espèces de faune et de flore sauvages menacées d'extinction, se montre peu bavard. «Le permis atteste que l'animal, l'espèce végétale ou le produit est issu d'une source durable», s'est contentée de préciser sa porte-parole par courriel, ajoutant que 85 agents de la faune travaillent en collaboration avec les agents frontaliers pour inspecter les cargaisons à destination du Canada. L'éleveur québécois Dominic Lapointe assure que la combine employée par les trafiquants péruviens n'est pas un cas isolé. (…)Il déplore que les douaniers canadiens manquent de formation sur ce commerce. L'Actualité

My NEXUS plan went nowhere
A letter to the editor states, "Re: "Screening at Canadian airports should be faster, smarter, safer" (Opinion, Oct. 19) My partner and I tried to apply for the NEXUS program. In October 2013, we duly completed our forms and each sent our $50 fee. We waited for a call for the interview step of the enrolment procedure but never heard a word back until a letter arrived five months later saying, "Applicant did not finalize program enrolment within required time frame." After a series of phone calls that yielded no clear means of following up, we abandoned the process. Needless to say, were $100 out-of-pocket for our efforts!" Montreal Gazette, A8

Don't forget today's needs
An editorial states, "Governments usually get criticized for thinking short-term. Since they have to go back to the voters every four years, they're naturally fixated on what can get done by the next election. So it seems a bit churlish to fault Finance Minister Bill Morneau for thinking too long term. In his fall fiscal update, Morneau is looking way down the road - announcing measures he hopes will make sure Canada's economy is more productive "one, two and three decades from now." (…) He also plans to make it easier for companies to bring in highly qualified workers by speeding up applications for work permits and visas. That's fine as long as they truly bring in special skills needed to help businesses staff up quickly, and just don't displace Canadians who could do the same jobs. It must not be a repeat of the Conservatives' ill-fated temporary foreign-workers program." Toronto Star, A14

* **Gordie Howe Bridge may never be built**
A letter to the editor states, "Re: Behind the bridge, by Anne Jarvis, Oct. 28. Congratulations to Anne Jarvis for an excellent piece of investigative journalism. It seems clear that this bridge may never be built for any number of reasons: the attitude of the current owner of the Ambassador Bridge, the lack of initiative from the government in Ottawa, the change in direction from the state of Michigan, and the continuing decline in bridge traffic. What will be the result if the current situation does not change? Windsor residents will still be left with the noise, fumes and truck traffic. The Ontario government will have constructed a very expensive highway to nowhere. The federal government will build a bridge in Montreal because there are a lot more Liberal votes in Montreal than there are in Windsor." Windsor Star

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Cybersecurity talent shortage on the radar of government, business**
An international shortage of cybersecurity talent is expected to grow over the next few years, according to the Information and Communications Technology Council. The council's vice-president of talent innovation, Sandra Saric, said there's an expected need for more than 1.5 million people to work in cybersecurity globally by 2020. Solving the talent shortage was one of the challenges emphasized by government and private industry executives at a cybersecurity forum at the GTEC conference in Ottawa on Tuesday. It's an annual technology event that brings together business and government. "Getting more people to take science, technology, engineering and mathematics courses and degree programs, and also training them to be cybersecurity savvy is probably the first challenge," said Scott Jones, assistant deputy minister responsible for the information technology security program with Communications Security Establishment Canada (CSEC). Saric said there's a need for computer scientists, analysts, investigators and psychologists, as well as communications and marketing professionals. "We connect with the Ottawa police who have a cybercrime unit, they're having difficulty finding people. I've spoken to the RCMP who are also struggling ... it's across the board," she said. Saric said the Information and Communications Technology Council, a Canadian non-profit, is working on developing talented students before they have even graduated high school. CBC News

*** Britain updates cyber security strategy**
Britain has launched a new national cyber security strategy, promising to spend $3.1 billion over the next five years to strengthen the defences of government, critical national infrastructure sectors and the wider economy. That includes the ability to mount offensive cyber action to retaliate against state or criminal actors. The announcement from chancellor of the exchequer (finance minister) Philip Hammond on Tuesday comes as Ottawa enters the last month of its public consultation on updating Canada's national security policy framework, which includes cyber issues. Questions raised in the Canadian consultation paper include under what conditions telecom and Internet providers should have to give police and intelligence agents access to basic subscriber information, whether providers should have to buy equipment to give police access to communications, how much subscriber data should providers have to keep and for how long and whether makers of encryption products should have to have a back door for law enforcement and intelligence agencies. IT World Canada (2016-11-01)

*** Microsoft Says Russian Hackers Exploited Flaw in Windows**
The hackers believed responsible for breaking into computers at the Democratic National Committee have exploited previously undisclosed flaws in Microsoft Corp.'s Windows operating system and Adobe Systems Inc.'s Flash software, Microsoft said Tuesday. It is unclear if those hackers, reportedly tied to Russia, used the newly disclosed vulnerabilities to hack into the DNC. Microsoft Tuesday criticized Alphabet Inc's Google for publicly identifying the Windows flaw on Monday, before Microsoft had had a chance to issue a patch. Wall Street Journal

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Python made 'growling noises' after killing New Brunswick boys, Mountie testifies**
Jean-Claude Savoie pleaded not guilty to criminal negligence causing death after two sleeping boys were suffocated in his apartment. A 45-kilogram python lunged, snapped its jaws, and made "growling noises" when it was forced back into its pen after killing two sleeping boys, an RCMP officer told a New Brunswick jury Tuesday. Const. Stephane Dugas described the scene on the morning of Aug. 5, 2013, shortly after Jean-Claude Savoie, who is facing trial for criminal negligence in the boys' deaths, called 911. Dugas testified that he found Savoie wearing a bloody shirt, two boys who were beyond medical help, and a 4.7-metre snake in the laundry room. Savoie followed Dugas' instructions to return the snake to its enclosure, where it made noises, rose up almost 1.8 metres and lunged at the glass, Dugas said. The two boys — four-year-old Noah Barthe and his six-year-old brother, Connor — were covered in bruises, and one had a lot of wounds. "I knew at the time not much could be done," said Dugas. "There was lots of blood." Toronto Star; Regina Leader-Post; Sputnik News; La Presse

*** 'I did do it. I wasn't myself': Man told police he was using crystal meth when he killed his mother, court hears**

Michael McCormick told police he was in the grip of a crystal meth psychosis when he killed his mother, Pamella Dyer, at her home in Sooke in July 2014. "She came downstairs and we got in a big fight right away," McCormick told Det. Mike Darling in an interview videotaped at West Shore RCMP detachment on Sept. 17, 2014. "I don't even know what happened. It was a big red blur for me. It wasn't me. Well, it was me, obviously. But it wasn't the right Mike. It was stupid, f--ing drugged out, f--ing idiot Mike." McCormick, 38, was originally charged with the second-degree murder of his mother. Last month, he pleaded guilty to the lesser offence of manslaughter. At his sentencing hearing Monday, Justice Brian MacKenzie heard that Dyer probably died on July 19. She was found dead the next day. Crown prosecutor Ruth Picha, seeking a prison sentence of 12 to 15 years, told the court the cause of Dyer's death was likely asphyxia caused by 25 fractures to the ribs, a blood clot to the lungs and a person lying on Dyer's body. At the sentencing hearing Tuesday, the Crown played the videotape of McCormick's confession. In the small interview room with photos of the crime scene taped to the wall, Darling tells McCormick his DNA has been found in blood on a milk carton found at the scene. McCormick denies killing his mother. Times Colonist, A3

Nanaimo man sprays family with bear spray during Halloween

A Nanaimo family had their Halloween ruined when an angry driver sprayed them and several bystanders with bear spray, RCMP said Tuesday. All were treated at the scene by paramedics. Police said the incident happened at about 8 p.m. Monday when a vehicle in the area of Cilaire and Montrose was reportedly driving too fast and revving its engine. Several parents were concerned as sidewalks were full with children going door to door. At one point the vehicle drove past and several parents yelled at the driver to slow down. During the exchange, an adult male allegedly struck the passing vehicle with a flashlight causing some damage. The driver got out, demanding to know who hit his vehicle. The suspect driver then grabbed a can of bear spray and sprayed not only the male who hit his vehicle but also his wife and seven-year-old son. Other parents came to help and were also contaminated by the affects of the spray. Witnesses obtained the licence plate number of the vehicle. The driver, who appeared to be in his early '20s, was later identified and has provided a statement to investigators. The investigation is continuing. Province

Former RCMP officer assault trial on P.E.I. delayed

Judge issues warrants for witnesses in Jeffrey Rae Gillis assault trial. A trial for a former RCMP officer charged with assault and uttering threats was adjourned Tuesday after two key witnesses didn't show up to court. Chief Judge Nancy Orr issued warrants for the two witnesses who were scheduled to testify in Jeffrey Rae Gillis's trial in provincial court in Charlottetown. Gillis was charged with uttering threats and two counts of assault. The trial was scheduled for two days, but Crown attorney David O'Brien told the court the two main witnesses in his case weren't there. O'Brien said he received a text message from one of the witnesses who said they didn't want to pursue the matter further. Guardian

*** Wiltz: Bull on both sides of the border**

An opinion piece states, "It is my opinion that we really have no choice when it comes to presidential candidates in next Tuesday's election. It comes down to Supreme Court nominations, our Constitution and our national defense. President Obama has run roughshod over our Constitution, and Hillary Clinton will continue to do the same. Yes, Donald Trump can be offensive and obnoxious, but he will not sell out the United States. (…) In June of 2013, flash floods struck Southern Alberta. In High River, one of the hardest hit communities, the citizens were forced to evacuate immediately. They had no time to load up their most valued possessions. Access to the largely submerged town was controlled by the Royal Canadian Mounted Police to prevent looting. What followed was unthinkable. The RCMP made forcible entries into private residences by breaking down doors and picking locks. They claimed they did this to search for flood victims and stranded pets despite the fact that no people or pets were reported missing. The RCMP also searched for firearms and confiscated all they found." Daily Republic

*** Cohen: There's a Canadian parallel to the FBI vs. Clinton, and the RCMP hasn't explained it**

An opinion piece states, "Kennedy learned that Dr. Martin Luther King, Jr., had been arrested on a technicality – a traffic charge – and was in jail. On Oct. 26, Kennedy called King's wife, Coretta, to show

his sympathy and offer his help. His brother, Robert F. Kennedy, made a call of concern to the judge. Surprisingly, King was released. African-Americans voted for Kennedy overwhelmingly. They may have been the difference in a race that Kennedy won by some 118,000 votes. (…) Did the RCMP sway the election? Two years later, a report from Paul Kennedy, the RCMP's public complaints commissioner, said the decision "had an adverse impact" on the vote and called it "a pre-meditated and calculated course of conduct." He said he had not "the slightest idea what was going through the commissioner's mind." Yet this all passed with little notice – and without consequences. In Canada, there was no outrage, no broader inquiry, no accountability. (…) In Canada, Zaccardelli, who threw the election to the Conservatives, has said nothing. He still owes us an explanation. Wasylycia-Leis, who said it was "credible" to think Goodale was involved in the allegations, and who expressed righteous indignation at other injustices as an MP, says she has no regrets. She still owes Goodale, whose reputation was smeared, an apology. (She ran for mayor of Winnipeg in 2010 and was trounced, poetically). More than a decade later, no one explains. No one apologizes. This is Canada's politics of passivity. No chance of that happening down here." Ottawa Citizen

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Paul Bernardo seeks day parole
The families of two school girls brutally raped and killed by Paul Bernardo say the notorious killer's application for day parole is "gut-wrenching." Bernardo is scheduled for a day parole hearing next March. Tim Danson, the lawyer for the families of Bernardo's murder victims, 14-year-old Leslie Mahaffy and 15-year-old Kristen French, is confident Bernardo will never be granted parole. "I believe he will die in prison," Danson said. "But we take nothing for granted and will be vigilant responding to Bernardo every step of the way." Canadian Press (Times Colonist, A7, Times & Transcript, Red Deer Advocate, Hamilton Spectator, Daily Gleaner, Waterloo Region Record, National Post, Kingston Whig-Standard); La Presse Canadienne (L'Acadie Nouvelle)

Bernardo playing odds: Parole bid not hurt by dangerous offender label
School girl killer and serial rapist Paul Bernardo is the only known Canadian offender to consent to being declared a dangerous offender, says a well-known Toronto defence lawyer. Dan Brodsky, who often represents dangerous offender candidates, said Bernardo agreed to the designation because it "has the tactical advantage of not airing the facts (of the crimes) and no psychiatric assessment. "He was taken to Royal Ottawa Hospital for an assessment, but no report was prepared," Brodsky said. When Bernardo consented to the declaration and its indeterminate sentence in November 1995, Bernardo pleaded guilty to a slate of rapes in Scarborough and St. Catharines, and the manslaughter of Tammy Homolka. Bernardo was already serving his life sentence for the first-degree murders of Leslie Mahaffy, 14, and Kristen French, 15. As a result, the dangerous offender declaration didn't change his parole eligibility. Dangerous offenders can seek release on parole seven years after the date of their offences, but Bernardo was prohibited from doing so because of his murder sentence. Bernardo, now 52, who'll tentatively be applying for day parole in March, has been eligible to make such an application since Feb. 17, 2015. Toronto Sun, A6

*** A man called monster: After watching mom brutally murdered, son fears dad's return**
Daniel Benoit remembers everything from that summer night when he was four years old, from the layout of his home to the way his mother screamed as the monster - called dad - brutally killed her. In July 1997, Dale Ogden killed Benoit's mother, Judy Ogden. Ogden was convicted of the second-degree murder of his wife, sentenced to life and sent to prison in February 2000. He had faced theft, extortion and assault charges long before his murder trial. At sentencing, Judge Gail Welsh could have given him more time, but she chose to set parole at 14 years. He could have been sentenced to as little as 10. Dale Ogden has been out on day parole since September, after being released from William Head Institution. He is currently living in a halfway house on Vancouver Island. Last year, Benoit filed an application as a victim under Correctional Services Canada so he could receive information on Ogden's whereabouts. He even wrote a victim impact statement that was read aloud at Ogden's parole hearing. But reliving the nightmare to produce the statement did nothing to keep Ogden behind bars. His parole was granted. Benoit went so far as to request a current picture of the man, so he could be on lookout. His

request went unanswered. He also filed a geographic separation request with Corrections Services Canada to keep Ogden out of Newfoundland and Labrador. Benoit's fear is that, despite that order, Ogden could still show up on his doorstep - and after one scare, he wants Correctional Services Canada to do more. On Sept. 30, Benoit received a call from officials saying a warrant had been issued for his father's arrest because police could not confirm his location. Ogden was quickly detained, but Benoit wasn't notified until 24 hours later. Benoit believes he wouldn't be as fearful if Correctional Services Canada were more transparent. Benoit said he will continue to contact the parole board and Correctional Services Canada, requesting a recent picture of Ogden - a picture that will show how much or how little they look alike. CBC News

*** Ex-Spitfire Johnson to be released pending appeal**

The Ontario Court of Appeal has ruled former Windsor Spitfire Ben Johnson can be released on bail while he challenges his sexual assault conviction. But Johnson remained in custody Tuesday, the ruling from the appellate judge coming down too late for Johnson to be released the same day. Superior Court Justice Kirk Munroe sentenced Johnson last week to three years in prison for having sex with a 16-year-old girl who was too drunk to consent. Johnson was taken from the courthouse to Windsor's South West Detention Centre to begin serving his sentence. Eventually, he was to be transferred to a federal penitentiary. Johnson filed his appeal two days into his sentence. He is being represented by the Toronto firm Lockyer Campbell Posner, which specializes in appellate law and whose partner, James Lockyer, is a founding director of the Association in Defence of the Wrongly Convicted. Lockyer was involved in overturning the murder convictions of Guy Paul Morin and Steven Truscott, among others. Windsor Star, A5

*** Fixing solitary crisis starts at the top**

An editorial states, "In the two weeks since the world woke up to the plight of Adam Capay, two things have become clear. One, federal and provincial politicians have no intention of accepting responsibility for the multiple factors that conspired to place a young indigenous man in solitary confinement for more than 1,500 days while awaiting trial. And two, only those same politicians have the power to end this kind of human-rights abuse. The culture of indifference reflected in the treatment of Mr. Capay starts at the top." Globe and Mail, A16

*** Every Manitoba jail over capacity: Inmates 'will be living in tents' warns advocate**

Every provincially-run jail in Manitoba has more inmates than what each facility is rated to hold. There are 2,555 inmates in seven facilities - the capacity for all Manitoba jails is 2,010 inmates. "People will be living in tents at some point. There is just too many people going into the system and not enough people going out and the solution isn't to build more jails," said John Hutton, executive director of the John Howard Society. Overcrowding is most severe at the Headingley Correctional Centre. The capacity is 549, but there are 842 inmates inside. Six other Manitoba jails are also overcrowded. The Manitoba government has made attempts in the past two years to lessen the backlog but despite those efforts, there's been a seven per cent increase in the inmate population since 2013. CBC News

Grits take fire over London jail woes

Troubles at London's provincial jail have spilled into the Ontario legislature again. A frequent flashpoint for problems in the province's correctional system, from overcrowding to violence, the Elgin-Middlesex-Detention Centre was thrust under the political spotlight Tuesday over drug overdoses a day earlier that left one inmate dead and his cellmate in hospital. London New Democrat Teresa Armstrong blasted the Liberal government for the problems at the jail during the daily question period at Queen's Park. London Free Press, A1

*** It's straight sadness: Lawyer for dead inmate questions prisoner classification at EMDC**

Justin Thompson told a judge he was done with drugs. standing before Ontario Court Justice George Brophy in a Goderich courtroom last month, when he was sentenced to 21 days in jail for failing to provide his fingerprints to police, the 27-year-old said he wanted to push his brushes with the law behind him. But Monday, 10 days after that Oct. 21 hearing, Thompson died of a drug overdose - it was either heroin or fentanyl powder, sources suggested - at the embattled Elgin-Middlesex Detention Centre (EMDC), the provincial jail in London often in the headlines for overcrowding, violence and other

troubles. Thompson's cellmate, Warren Williams, 45, of Sarnia, in custody awaiting trial for first-degree murder in the death of a Sarnia man in March, also overdosed but survived. London Free Press, A3

OD TREATMENT: Jails need 'immediate' access
The arrival of the highly potent opioid fentanyl in Nova Scotia is prompting the province's jails to move more quickly on a plan to provide frontline staff with a potentially life-saving overdose reversal drug, says the director of correctional services. Sean Kelly said a final decision on whether to allow guards or other staff to provide naloxone in jail overdose cases hasn't been taken, but it is necessary to make the drug quickly available in the province's prisons. However, in two cases over the past two-and-a-half years, inmates have died in prison cells from opioid overdoses and the existing response system wasn't able to revive them. Chronicle-Herald, A3 * (Cape Breton Post, Times & Transcript)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

* **Alberta Child and Youth Advocate calls for tighter policies to prevent online child sexual exploitation**
The provincial government must take steps to improve protection for young Albertans vulnerable to online sexual exploitation, the province's child and youth advocate said Tuesday. The new recommendation from Del Graff stemmed from an investigation into the tragic case of a teenage girl who died by suicide at age 17. Among the issues she faced in her last few years was a lack of supportive relationships that helped put her at risk of attracting Internet predators, he said in his report on the case. Calgary Herald, A1 (Edmonton Journal)

* **Coroners Service to hold first-of-a-kind inquest into fentanyl death**
The B.C. Coroners Service has announced a coroner's inquest into the fentanyl-related death of a Coquitlam man and will establish a team to provide more timely and in-depth probes into illicit drug overdoses. It is the first time an inquest has been called to investigate a death relating to the fentanyl epidemic, part of the B.C. government's efforts to prevent further overdoses. Brandon Juhani Jansen, 20, died while staying at a substance-abuse treatment centre in Powell River in March 2016. Chief coroner Lisa Lapointe said the B.C. Coroners Service is deeply concerned about the rising number of illicit drug deaths in B.C. Times Colonist; The Province

* **Naloxone nasal spray will be available to combat overdoses**
A new tool to save lives after an overdose will soon be available in Waterloo Region. Nasal spray naloxone, which reverses the effects of an opioid overdose, will be available to those at risk, likely in the new year. Opioid overdoses are regularly reported in the region in recent months, often linked with powerful bootleg fentanyl. Waterloo Region Record

* **'It's very scary right now': Bear Clan Patrol looking to carry fentanyl antidote**
The Bear Clan Patrol spends their days and nights walking the streets of Winnipeg and now they want to carry a drug which could save lives. Bear Clan spokesperson James Favel says fentanyl and carfentanil, a synthetic opioid that is 100 times stronger than the highly addictive fentanyl, "scares the life out" of him. "We are seeing a stark rise in the amount of syringes that we are finding around the community," he said. "The places that we are finding them is not typical either." Syringes used to be found mostly under bridges, in the industrial areas and places where people could "hide away," Favel said. However, now the patrol is finding them at the bell tower gathering area and along busy streets. Favel said the Bear Clan has been in talks with paramedics about how they can get the training that is needed to carry naloxone, which can block or reverse the effects of opiod medications such as fentanyl. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Canada's Feminist Prime Minister, One Year In**
An opinion piece states, "One year ago, Justin Trudeau took office as Canada's 23rd prime minister and promptly fulfilled a major campaign promise by appointing a diverse and gender balanced cabinet that "looks like Canada." When a reporter asked why appointing women was a priority, Trudeau shrugged and responded with his now-famous quip, "because it's 2015." (…) Human Rights Watch's investigations in northern British Colombia have documented police officers' abusive treatment of indigenous women and girls, including excessive use of force, physical assault, rape, and other forms of sexual violence. In Saskatchewan, indigenous women, including victims of violence, have also reported a deep distrust of police, recounting incidents of misconduct, abuse, and neglect. First Nations women are significantly overrepresented among homicide victims, and this violence – coupled with mistreatment by the very officers charged with protecting them – leaves many indigenous women in a near constant state of insecurity. For years, this problem was ignored by the Canadian government and one of Trudeau's most significant early policy decisions was his decisive action to launch a national public inquiry into missing and murdered indigenous women and girls. While the inquiry is an essential step forward, its terms do not explicitly mention policing. For this process to be successful, the inquiry must include rigorous investigations into police misconduct and take an unflinching look at critics' allegations of widespread misogyny and racism in the ranks of Canada's police forces." Human Rights Watch

*** Le CEDAW tient le Canada responsable de ses résultats décevants en matière de droits des femmes**
Un article d'opinion rapporte « Les résultats du Canada en matière d'égalité des femmes ont été la cible de toutes les critiques aux Nations Unies, à Genève, cette semaine. La 65e session du Comité pour l'élimination de la discrimination à l'égard des femmes (CEDAW) a lieu à un moment opportun pour les Canadiennes. Le Canada a un nouveau gouvernement fédéral, ainsi qu'un premier ministre qui se dit féministe, préconise une relation de nation à nation et reconnaît que « la pauvreté est sexiste ». Nous savons que les mots comptent, mais il nous faut maintenant de l'action. (…) Les organisations de femmes autochtones, de droits des femmes et de droits de la personne accueillent favorablement la création de l'enquête nationale sur les femmes et les filles disparues et assassinées. Cependant, nous demeurons préoccupées par l'insuffisance du cadre de référence et par le fait que 37 autres recommandations de l'enquête sur la crise des meurtres et disparitions menée par le comité CEDAW n'ont pas encore été mises en œuvre. » CDEACF (2016-11-01)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Watchdog downplays marijuana revenue potential
The parliamentary budget watchdog is being a bit of a buzz kill when it comes to forecasting government revenue windfalls from legalized marijuana. "We're talking millions and millions - not billions and billions - of dollars of revenues," Jean-Denis Frechette, the parliamentary budget officer, said Tuesday after releasing a study entitled, Legalized Cannabis: Fiscal Considerations. The 77-page report finds that the federal government may have little fiscal space to heavily tax cannabis the way it does tobacco without pushing the legal price well beyond that of currently illicit pot. What's more, the Liberal government's stated aims of decreasing marijuana use and accessibility for young Canadians while choking off pot revenues from organized crime will require a delicate balancing act, the study found. Price legal pot too high and the black market will continue to flourish. Too low and governments could be seen to be encouraging its use. The report projects sales tax revenue in 2018 could be as low as $356 million and as high as $959 million, with a likely take of about $618 million based on legalized retail cannabis selling for $9 per gram - in line with current street prices. Canadian Press (Chronicle-Herald, A1, Toronto Star, Kingston Whig-Standard, Ottawa Sun, Times Colonist, Daily Gleaner, Telegraph-Journal, Times & Transcript, Red Deer Advocate)

*** So much for that marijuana tax bonanza**

In about 30 or 40 years, today's millennials may well be wistfully telling their grandchildren about the good old days, when smoking pot was fun. The signs are already out there: Legalizing marijuana is going to be a sobering experience - a buzz-kill, in fact - for pot users and governments too. The latest party crasher is none other than the Parliamentary Budget Officer. In a report issued Tuesday, Jean-Denis Fréchette warned that tax revenues from pot legalization, at least at the outset, would be in the hundreds of millions of dollars - not the billions that governments may have envisioned. The reason for this modest outlook is simple: The government can't afford to price marijuana above what the illegal market will bear, not if it wants pot smokers to switch to official, legal suppliers. Or, as the report puts it: "When legalization occurs, the government may have little fiscal space to apply tax without pushing the price of legal cannabis significantly above the illegal market price." The report echoes similar warnings issued a couple of months ago by the head of the federal government's own task force on marijuana legalization and regulation. Former deputy prime minister Anne McLellan said in an interview with CBC in September that governments would need to find the "sweet spot" on pricing marijuana, to stay competitive with the illegal market. iPolitics

*** All you need to know about marijuana legalization in Canada**

Picture this: you're driving back from a weekend at the cottage with your friends. It's Sunday at noon, and the countryside is beautiful. Suddenly you see blue and red flashing lights ahead; it's a roadside spot check. You kill the music. You tell yourself you've got nothing to worry about. You're sober as a gopher. In fact, you're kind of wired on that large Timmies coffee you stopped for an hour ago. You're fine. You pull over and the officer comes up to the window. He asks you a few questions, and looks around the inside of the car. Suddenly he seems to get a whiff of something. The next thing you know, he's asking you to take a breathalyzer test. No biggie, you think. You certainly imbibed last night by the campfire, but you got a good night's sleep, and woke up feeling refreshed—the booze should be long-gone from your system by now. (…) But critics say decriminalization doesn't solve the problem of the $7-billion weed black market in Canada. Sure, stoners will be off the hook, but the organized crime that produces and sells weed will continue to operate. Only legalization will destroy the black market, they say. That's how Prime Minister Justin Trudeau sees it; he's ruled out decriminalization between now and the spring of 2017, when the Liberals plan to introduce the new law. So what will be in that law? If we scan the government's discussion paper for clues, there are some likely factors. The paper suggests the following elements are "largely self-evident": legalized possession of a certain amount of weed; regulations surrounding its production, distribution, quality, safety, potency and access; new criminal laws to punish those who try to keep selling illegally; support for prevention, addiction and other services; an education and awareness campaign; and data-gathering. Hill Times

PUBLIC SERVICE / FONCTION PUBLIQUE

Feds continue to struggle with Phoenix pay system: Employees still waiting for money as government misses Oct. 31 deadline to fix problems

Samuel Bourget has been waiting for a $700 paycheque since June. He's an Operational Records Management System (ORMS) officer with the RCMP, and one of 22,000 federal employees who are missing money because of problems with the Phoenix pay system. The federal Department of Public Services and Procurement failed to reach its Oct. 31 deadline to clear the backlog of 82,000 employees who were waiting for money. In July, deputy minister of Public Services and Procurement Canada Marie Lemay estimated about 720 public servants were missing paycheques, while another 1,100 were missing payments for parental leave, long-term disability and severance. The other 80,000 hadn't been paid for supplementary or extra duties, overtime, or, like Bourget - pay adjustments. The money he's missing should have been a raise he received in June. "As it goes longer, it adds up," he said. He was one of about a dozen people who braved the cold to protest in front of the Greenstone Government of Canada Building on Monday. The Public Service Alliance of Canada North organized the Day of Action. Bourget has two children at home, and says even though the amount owed to him isn't astronomical, it's affecting his life. "With my wife at home with the kids, money's tight to begin with. Every little bit helps, and if you don't (get) it then that's another decision you have to make on what you're going to purchase or go without," he said. Yellowknifer; Telegraph-Journal

*** Christie Blatchford: New Senate appointments just more of the same**
An opinion piece states, "With slavish regard to the late, great Dorothy Parker, the new Canadian senators - 14 of them, thus far, the most recent six announced this week - run the gamut from A to B. In other words, while they may turn out to be grand appointments and may be brimming with noble intentions, on the surface they are just like all the others who went before them, utterly conventional good Canadians chosen from the most conventional quarters of this curious country... The others either mostly worked for government (former Ontario government deputy minister and secretary of cabinet Tony Dean) or for organizations supported mostly by government (the ferocious justice advocate Kim Pate, former Federal Court Judge Howard Wetston, and the aforementioned Boniface). Where are the ordinary Joes? The steelworkers, teachers, the guys on the line at Ford, the out-of-work oilpatch folks, the cashiers at Metro? Where is there anywhere someone who isn't from the conventionally approved swaths of Canadian society?" National Post

OTHER / AUTRE

*** $17.5-million spent on security during Obama visit: fiscal update to Parliament**
The federal government spent $17.5-million on security when U.S. President Barack Obama visited Ottawa for a summit of North America's three national leaders last June, show spending details revealed Tuesday in the government's annual fall fiscal update to Parliament. The cost of heavy security and protection for President Obama, Prime Minister Justin Trudeau, and Mexico President Enrique Peña Nieto at the June 29 summit is contained in a list of $2.8-billion-worth of costs and forecast spending due to "policy actions" the government has taken since the first Liberal budget last March... As well, the government spent $104.5-million on assistance to residents of Fort McMurray, Alta., after the oil sands city was ravaged by wildfires, through matching funds with private donations from across the country. The mini-budget also disclosed the government has significantly increased the budget for a national commission of inquiry into missing and murdered indigenous women and girls. The government initially earmarked $40-million for the inquiry in the 2016 Budget last March, and then amped that up to $53.8-million when it revealed more details in August. Hill Times (2016-11-01)

*** Canada marches into mission with 'eyes wide open,' Sajjan says**
Defence Minister Harjit Sajjan is headed to Mali and Senegal on a fact-finding mission next week as the federal government makes plans to deploy a military mission to Africa. Sajjan's five-day visit comes after an August trip to the Democratic Republic of Congo, Ethiopia, Kenya, Tanzania and Uganda, all against the backdrop of the Liberal pledge to commit troops to an African mission. "We need to go into this eyes wide open, making sure that ... we look at the complexities of how (peace) operations have been done in the past and what we need to do," Sajjan told reporters in Ottawa. Sajjan offered no timeline of when a decision on the deployment could be made. (...) The Liberal government is weighing options to deploy as many as 600 soldiers and 160 police officers somewhere in Africa on a peace mission. Lang praised Sajjan for taking time to carefully consider the deployment, given the risks. Toronto Star, A1

INTERNATIONAL

'True Liberation' of Mosul begins
Waving white flags and looking equally relieved and bewildered, crowds of civilians were headed for safety Tuesday, riding in battered cars and trucks that rumbled down the road east of Bazwaya. Iraqi troops had arrived in Bazwaya and were using the strategic village on the eastern outskirts of Mosul as the launch pad for their first assault on the city limits. By the end of the day, troops from the Golden Division, part of Iraq's Counter Terrorism Service (CTS), had seized a foothold inside the city at Gogjali, an industrial district of Mosul less than five kilometres away. "Now is the beginning of the true liberation of the city of Mosul," Gen. Taleb Sheghati al-Kenani, head of the CTS, said from Gogjali. Iraq's Joint Operations Command said troops had "entered the Judaidat Al-Mufti area, within the left bank of the city." The assaults mark the beginning of the endgame in a massive offensive launched two weeks ago and involving tens of thousands of Iraqi and Kurdish troops backed by U.S.-led airstrikes. Residents inside the

city reported airstrikes and artillery pounding the city. "We can see Daesh (also known as the Islamic State of Iraq and the Levant, or ISIL) fighters firing toward the Iraqi forces and moving in cars between the alleys of the neighbourhood. It's street fighting," one resident said. National Post, A1

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 3, 2016 / le 3 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Surveillance de journalistes : mutisme à la GRC et au SCRS
Le commissaire de la GRC Bob Paulson a dit mercredi «ne pas être au courant que nous avons des enquêtes actives ou de la surveillance à l'égard de journalistes», mais la GRC n'a pas voulu confirmer si des journalistes ont été surveillés dans le cadre de ses enquêtes. Un cas de filature avait été rendu public il y a un an, celui du journaliste de La Presse Joël-Denis Bellavance qui a été pris en filature en 2007. Tout en précisant «reconnaître» et «respecter [...] l'importance de la liberté et de l'indépendance de la presse», la Gendarmerie royale du Canada (GRC) a indiqué ne pas pouvoir commenter «l'existence d'enquêtes en cours» ou «discuter des détails opérationnels» d'enquêtes passées. (...) Le Service canadien de renseignement de sécurité (SCRS) n'a pas répondu aux questions de La Presse à savoir si l'organisme fédéral responsable des enquêtes de sécurité nationale (...) Le **ministre Goodale** examine la Directive ministérielle sur les enquêtes dans les secteurs sensibles existante afin de s'assurer que les

plus grands soins sont pris lorsque des enquêtes criminelles et du journalisme se recoupent et que la valeur canadienne fondamentale de la liberté de presse est protégée. Il est toujours ouvert à recevoir des représentations sur ce qu'il y a d'autre à faire pour protéger les libertés fondamentales de la presse», indique **Scott Bardsley, attaché de presse du ministre fédéral de la Sécurité publique Ralph Goodale**. (...) Le **ministre Goodale** doit demander des comptes aux services policiers sous sa juridiction et rendre des comptes en Chambre aussi. Tout ça va peut-être nous permettre de découvrir qui est surveillé, mais ça ne règle pas le problème, ce qui rend encore plus pertinent et urgent que jamais notre projet de loi [sur la protection des sources journalistiques].» Le Parti conservateur du Canada aimerait que le **ministre Goodale** fasse un examen de la situation et vienne en faire rapport en comité parlementaire. La Presse (2016-11-02)

*** Une enquête fédérale demandée par le npd**
Alors que Justin Trudeau promet de faire le «nécessaire» pour défendre la liberté de presse, Thomas Mulcair demande la tenue d'une enquête fédérale. «Ce gouvernement est à la défense de liberté de la presse et on va faire ce qui est nécessaire pour l'encadrer s'il y a d'autres étapes nécessaires», a soutenu le premier ministre, hier ma-tin, à l'entrée de la réunion hebdomadaire de son caucus. Le chef sortant du NPD, Thomas Mulcair, n'est pour sa part pas rassuré par la situation et exige la tenue d'une enquête fédérale pour s'assurer que les journalistes ne fassent pas l'objet d'une surveillance similaire de la part de la GRC. «Au Canada, en ce moment, il y a combien de journalistes qui sont surveillés soit par la GRC, soit par le SCRS? [...]. Alors moi, je m'attends à ce que Justin Trudeau tire ça au clair», a-t-il dit. Le **ministre fédéral de la Sécurité publique, Ralph Goodale**, a indiqué que le commissaire de la GRC, Bob Paulson, avait dit ne pas être au courant de cas de journalistes qui feraient actuellement l'objet d'une telle surveillance. Le Bloc québécois entend déposer un projet de loi privé sur la protection des sources journalistiques. Journal de Montréal, 26

Better protection for reporters sought in wake of Montreal surveillance
Independent senator and former journalist André Pratte wants the federal government to look at beefing up protection for reporters and their sources. Pratte said that if the government shows no interest, he'll pursue the idea himself. It is "quite worrisome" that Montreal police obtained warrants to monitor one of his former colleagues, La Presse columnist Patrick Lagacé, Pratte said Wednesday in an interview. "I think it is time to look at this again." The newspaper said this week it had learned at least 24 surveillance warrants were issued for Lagacé's iPhone this year in connection with an internal probe into allegations police anti-gang investigators fabricated evidence. **Public Safety Minister Ralph Goodale** said the Supreme Court of Canada has already explicitly laid out the test that must be satisfied when police investigations intersect with media freedoms. In two key 2010 rulings, the high court did not create blanket constitutional protection for journalists, saying they are a "heterogeneous and ill-defined group of writers and speakers." Instead, the court spelled out a four-point test that allows judges to weigh competing public interests on a case-by-case basis. The Lagacé case shows more is needed, said Pratte, a former editorial writer at La Presse. "I don't think we can simply say: 'The Supreme Court has issued those criteria, and they're good enough.' Well, obviously, they were not good enough to protect Mr. Lagacé and his sources for a period of five months." Despite his apparent reluctance to revisit the existing regime, **Goodale** left the door open a crack. Canadian Press (Times Colonist, D3, Chronicle-Herald)

Six more journalists confirmed as targets of police surveillance
A controversy over police surveillance of the press in Quebec deepened Wednesday with revelations that six journalists, including some of the province's top investigative reporters, had their cellphones surreptitiously monitored by provincial law enforcement as far back as 2013. The disclosures made by several media outlets and confirmed by the provincial Sûreté du Québec suggest that covert police surveillance of Quebec journalists dates further back and is more widespread than previously known. La Presse revealed this week that one of its journalists, columnist Patrick Lagacé, had his iPhone data tracked by Montreal police for months this year after they obtained search warrants. On Wednesday, Quebec provincial police said it had also obtained court warrants to monitor the log of incoming and outgoing cellphone calls of six journalists. (...) On Tuesday, the Premier attempted to get ahead of the controversy, announcing measures to tighten rules for obtaining search warrants against journalists and striking a panel of experts to look into the situation. In Ottawa that day, **Public Safety Minister Ralph**

Goodale told reporters his government is open to toughening the rules that govern how and when the federal government can investigate members of the media. Globe and Mail, A1

Ils ont dit

« Je couvre la politique depuis près de 40 ans, souvent sur des dossiers délicats. On se dit toujours que c'est possible d'être épié par les policiers, mais on est convaincu qu'ils n'oseraient pas aller jusque-là. Bien, il semble qu'on se soit trompé. » Denis Lessard, chef du bureau parlementaire de La Presse à Québec. « Je suis assez surpris de voir qu'un juge de paix ait pu autoriser un mandat à mon sujet alors que je n'avais pas écrit sur Michel Arsenault. [_] Le seul motif que je vois pour faire l'objet d'un mandat, c'est que ma conjointe [Marie-Maude Denis] avait déjà fait des reportages sur Michel Arsenault. ». Éric Thibault, Journal de Montréal. (...) « La réponse de la SQ de dévoiler [ces informations] démontre que le public a besoin d'être rassuré. Ce sont des questions auxquelles [la GRC et le SCRS] doivent répondre. On continue de demander une enquête publique qui nous permettrait de constater les faits : est-ce une pratique répandue ou arbitraire ? » Matthew Dubé, porte-parole du NPD en matière de sécurité publique. « Comme n'importe qui, je vois que si la SQ et le SVPM le font, je ne tomberais pas en bas de ma chaise [si les corps policiers fédéraux le font aussi]. Le **ministre Goodale** doit demander des comptes aux services policiers sous sa juridiction et rendre des comptes en Chambre aussi. » Rhéal Fortin, chef par intérim du Bloc québécois. La Presse +

Bridge cameras not for police

An editorial states, "There is general unease when police or government officials pry deeper into the private affairs of citizens. We are constantly monitored and watched - and most times, not even aware of it. When citizens stop caring about this intrusion or welcome surveillance - it's even more disturbing. The issue of surveillance cameras is back in the news with a request from the Charlottetown police department to gain quicker access to special cameras that record every vehicle travelling on and off P.E.I. In 2009, a security-obsessed former government provided funds to install licence plate reader cameras on the Confederation Bridge. We were assured the applications would be for traveller information, emergency response management and vehicle safety. (...) New police powers to track Canadians are basically limitless. There is little oversight and the Quebec reporter is an example of how abuses can happen. It's being blamed on a cultural shift that began with the passing of Bill C-51under the previous Conservative government. The Liberals pledged to amend parts of the Bill, but have done nothing. **Public Safety Minister Ralph Goodale** expressed horror at the Quebec warrants. Fine, then do something about it. » Guardian, A6

TOP STORIES / MANCHETTES

Mutisme à la GRC et au SCRS

La GRC et le Service canadien du renseignement de sécurité (SCRS), les deux corps policiers fédéraux, ne veulent pas confirmer s'ils ont déjà mis des journalistes sous surveillance, contrairement à la SQ, qui a dévoilé ces informations hier à la suite de vérifications internes. Si le premier ministre du Canada Justin Trudeau a promis hier de « faire ce qui est nécessaire » pour défendre la liberté de la presse, son gouvernement ne demandera toutefois pas aux corps policiers fédéraux de dévoiler publiquement ce type d'informations, comme le réclament le Bloc québécois et le Nouveau Parti démocratique. La GRC précise seulement que « les cas où des enquêtes de la GRC concernant des journalistes ont eu lieu sont extrêmement rares ». La Presse +

Les Canadiens mal protégés contre la surveillance abusive, selon Snowden

Les Canadiens sont très mal protégés contre les pratiques de surveillance abusives, estime Edward Snowden, qui s'alarme des possibilités ouvertes aux services de renseignements d'ici et d'ailleurs par les nouvelles technologies de communication. L'ex-sous-traitant de la National Security Agency (NSA), qui participait hier à une vidéoconférence organisée par l'Université McGill, a souligné que le système de régulation des services de renseignement canadiens était probablement le plus « déficient en Occident ». Il a déploré à ce titre que le gouvernement libéral de Justin Trudeau tarde à réviser la Loi antiterroriste, dite loi C-51, qui confère des pouvoirs accrus à ces mêmes services. Nombre d'analystes, a-t-il relevé, pensent que la loi en question est trop mal formulée pour être modifiée et devrait tout bonnement être

retirée. M. Snowden estime qu'il n'est tout simplement pas possible, ici ou ailleurs, de faire confiance aux autorités pour utiliser de manière responsable les technologies de surveillance existantes. La Presse +, 1; Agence QMI (Journal de Montréal, Journal de Québec) (2016-11-03); Montreal Gazette (2016-11-02)

Six journalistes ciblés par la SQ
Après le SPVM, au tour de la Sûreté du Québec. Le corps policier national québécois admet avoir obtenu secrètement les registres téléphoniques de six journalistes, dans le cadre d'une enquête sur les fuites d'informations aux médias amorcée en 2013. C'est ce qu'a confirmé le corps policier hier après-midi, dans la foulée des vérifications demandées par le directeur général Martin Prud'homme. Celui-ci dit avoir tout ignoré de cette affaire jusqu'ici puisqu'elle s'était déroulée sous la direction de son prédécesseur, Mario Laprise. «M. Prud'homme est très irrité», a affirmé le capitaine Guy Lapointe, porte-parole de la SQ. Joint par La Presse, Mario Laprise a refusé de discuter de l'affaire. «Je n'ai pas de commentaires à faire par rapport à ça. Il y a des vérifications qui sont faites, on va laisser les gens faire leur travail», a-t-il laissé tomber. La liste des gens visés. Parmi les reporters ciblés par la SQ, on retrouve le chef du bureau parlementaire de La Presse à Québec, Denis Lessard. «Je couvre la politique depuis près de 40 ans, souvent sur des dossiers délicats. On se dit toujours que c'est possible d'être épié par les policiers, mais on est convaincu qu'ils n'oseraient pas aller jusque-là. Eh bien, il semble qu'on se soit trompé», a-t-il réagi. Les journalistes de Radio-Canada Alain Gravel, Marie-Maude Denis et Isabelle Richer sont aussi du nombre, tout comme Éric Thibault, journaliste au Journal de Montréal et conjoint de Marie-Maude Denis. Le sixième journaliste est André Cédilot, journaliste chevronné de La Presse qui a ensuite travaillé pour Radio-Canada. La Presse (Le Quotidien, 21, Le Nouvelliste, La Voix de l'Est, La Tribune); Le Soleil; Le Droit; Agence QMI (Journal de Montréal, Journal de Québec)

Shafia murder convictions to stand
A father, mother and son found guilty in the drowning deaths of three teenaged sisters and another woman who had apparently shamed the family lost their bid Wednesday to overturn their first-degree murder convictions. In unanimously rejecting an appeal by the Shafia family members, Ontario's top court ruled, among other things, that expert evidence on so-called honour killings had been properly admitted at their trial and the son was properly tried as an adult. Canadian Press (Kingston Whig-Standard, A1, The Guardian, Waterloo Region Record, Red Deer Advocate, The Telegram, Ottawa Citizen, Times & Transcript, Whitehorse Daily Star, Hamilton Spectator, Times Colonist, Chronicle-Herald, National Post, Cape Breton Post); La Presse Canadienne (Le Devoir, Le Quotidien, La Tribune, La Presse); Le Journal de Québec (Journal de Montréal); Edmonton Sun (Calgary Sun, Ottawa Sun, Toronto Sun)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

* **Is the Beast still burning? Fort McMurray wildfire may smoulder through winter**
The Beast could still be burning. The fire which devastated much of Fort McMurray in May may still be smouldering, deep underground. At its peak, the fire was moving 30 to 40 metres per minute, creating its own weather pattern of wind and lighting. It crowned high in the trees, raining down ash and cinders as it raced north, jumping the Athabasca River, and wrapping itself around the northern Alberta city like a noose. Even then, smouldering ash underground grew into powerful infernos, making the fire an unpredictable foe for firefighters. In the end the Beast covered 589,552 hectares and devoured 2,400 structures. Extinguished on the surface, the fire may continue burning undetected throughout the winter, feeding on peat and dead vegetation. CBC News

* **Six months after the fire, families still reach out for help**
At a hotel in downtown Fort McMurray, workers in coveralls walk through the faded carpeted hallways, coming and going from their shifts at some of the many construction sites in the city. But behind one of the doors, there is other work underway. Colouring books and brightly coloured paper line a table, as the five Goetz children are immersed in a crafting session. The two adjoining hotel rooms, each with queen beds, became the temporary home for the family of seven on Tuesday (…) His family has now been put up in the hotel temporarily by the Red Cross, assistance Goetz originally didn't realize was available to his family. Officials with the Red Cross say are seeing up to 125 people in Fort McMurray each day and many

of them are people who are asking for help for the first time because they thought they would be able to get by on their own. "We are Albertans. There is a can-do attitude in this province," said Jennifer McManus, the vice-president for Alberta and the Northwest Territories with the Canadian Red Cross. CBC News

*** Slowdown in oilsands rebuild cuts revenue for camp firm**
A Calgary company that operates work camps for the oilsands industry in northern Alberta says demand for its services has been weaker than expected over the summer following the Fort Mc-Murray wildfire. Horizon North Logistics Inc. said Wednesday that rebuilding efforts in the oilsands region of northern Alberta have proceeded at a much slower pace than expected and demand for its camp, catering and modular building services fell off "significantly" in September. Horizon North's 665-unit Blacksand Executive Lodge near Fort McMurray was destroyed by the wildfire in May. It says it expects to settle its insurance claim by year-end, without giving any dollar target. On a conference call, CEO Rod Graham blamed lower activity for a 27 per cent drop in Horizon's revenue to about $60 million in the quarter ended Sept. 30 versus the same period last year. Postmedia (Calgary Herald, B2; Edmonton Journal, Edmonton Sun, Red Deer Advocate)

*** Drones useful in fight against wildfires, but how to deploy them up for debate**
The use of drones in battling wildfires in Alberta could save millions of dollars and reduce the risk to front line pilots flying dangerous sorties over blazes like the one that devastated Fort McMurray in May. But just how unmanned aerial vehicles (UAV) can be best utilized in the heat of a raging inferno is still up for debate. Their role in wildfire management was one of the topics at a three-day conference and trade show in Edmonton dedicated to the burgeoning technology (…) On Tuesday, the NDP government brought in new rules in Alberta that ban drones that may interfere with firefighting. This year, Alberta spent millions of dollars as firefighters battled 1,329 wildfires. The province's five-year average for aircraft costs in wildfire management is roughly $128 million, so it is important to fire officials to look at all types of technologies that could save money and lives, McIlwaine said. "We spend a lot of money on aircraft," McIlwaine said. "And we are responsible to the taxpayers." Drones equipped with infrared imaging could be used in tracking fire fronts and large-incident fire mapping, as well as post-blaze fire investigation. And they could also be used to complement the province's fire detection program, which currently relies on 126 lookouts around the province. B.C. has tested the use of drones over the past two fire seasons and announced in August it is adding them to the province's firefighting arsenal. Postmedia (Edmonton Journal, A3; Edmonton Sun)

*** IBC commends federal government's focus on infrastructure and flood mitigation in 2016 fall economic statement**
In the statement, released on Tuesday, the federal government proposed $21.9 billion over 11 years for green infrastructure, including targeted investments that "support greenhouse gas emission reductions; enable greater climate change adaptation and resilience; and ensure that more communities can provide clean air and safe drinking water for their citizens." The Government of Canada said in the economic statement that it will "work with its provincial, territorial, municipal and Indigenous partners to evaluate, select and fund the green infrastructure projects that will deliver the best outcomes for Canadians." Projects that may receive additional investments include, among others: the construction of infrastructure to help manage the risk associated with floods and wildfires (…) IBC said that the "frequency and severity of flooding events and wildfires are having a significant impact on Canadians across the country. Canada must build a culture of disaster risk reduction that resonates with consumers and engages all levels of government, businesses, and institutions." Canadian Underwriter (2016-11-02)

*** Flood warnings likely on tap as November forecast includes more rain**
After a record rainy October, the start of November doesn't look much better. Heavy rainfall forecast for the next few days has forced officials to warn of potential evacuations in parts of B.C. due to flooding. A high wind warning is also in place for the coast of Haida Gwaii, with winds expected to hit 90 km/h overnight Wednesday. As the storm system moves through, the area will get more than 100 millimetres of precipitation. According to Environment Canada meteorologist Ross Macdonald, the rainy start to November may be a sign of more to come. Vancouver Province, A6

*** Alberta's flood plain mapping gets failing grade**
Alberta's lack of progress in mapping future flooding hazards dragged down the province's grade in a university study's rating of provinces' disaster readiness. The province scored a C-plus in a University of Waterloo study on climate change adaptation, slightly above the C-minus average nationwide. But that mark would have been higher if Alberta's flood plain mapping was updated to better reflect future extreme weather events that are increasingly likely given climate change, said Dr. Blair Feltmate of the Intact Centre on Climate Adaptation at the U of W. "I do find it somewhat shocking ... if it was seven months after the 2013 event I could see it," said Feltmate. "But three years later, the flood plain maps haven't been brought up to date." Postmedia (Calgary Herald, A5; Calgary Sun)

*** $108M insured damage in local flooding**
Swamped homes, stalled vehicles and soaked industrial properties affected by September's flooding in Windsor and Tecumseh resulted in almost $108 million worth of damage, according to the Insurance Bureau of Canada. The IBC confirmed Wednesday more than 6,000 claims - for home, auto and business - were filed with insurers after record levels of rain ruined hundreds of basements in Windsor and Tecumseh. Peter Karageorgos, a spokesman for the IBC, said the organization considers any event where there's more than $25 million in damages a catastrophe. "The dollar amount from the flood is large," he said. "But the more interesting point is the number of claims. That shows how widespread the damage was." Windsor Star, A7; CBC News

*** Urgent repairs needed at Bay d'Espoir**
Newfoundland and Labrador Hydro is moving fast to complete repairs, welding work, on a key piece of infrastructure at the island's largest power plant - the hydroelectric power plant at Bay d'Espoir. The push is on to complete the required maintenance, estimated at $12.9 million, to avoid heading into the winter season with significantly reduced island power reserves. The utility is also trying to repair access roads in the area, after damage from more than 200 millimetres of rain dumped on Oct. 10 by the remnants of hurricane Matthew. There were at least 24 washouts on roughly 400 kilometres of utility roads around the Bay d'Espoir power system, including an access road to the neighbouring Upper Salmon power plant. The road repair is estimated at an additional $4.6 million, according to information filed with the Public Utilities Board. Telegram, A3

*** Search for missing Codroy Valley hunting guide into 2nd day**
A ground search will continue Thursday for a 49-year-old man who became separated from his hunting group Tuesday afternoon on Newfoundland's west coast. The RCMP said a helicopter search continued until midnight Wednesday and it will be back in the air Thursday as well, weather permitting. Barachois Ground Search and Rescue, a Joint Rescue Coordination Centre helicopter and RCMP assisted in the search which began shortly after the man was reported missing at 1 p.m. Wednesday. CBC News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Join the #YourNatlSec twitter chat and tell Public Safety Minister Ralph Goodale Canadians want privacy reforms
If you're one of the millions of Canadians who oppose Bill C-51, you probably have a lot to say to decision-makers about your reasons why. And this Thursday, November 3 at 8:00 pm EST/5:00 pm PST, Public Safety Minister Ralph Goodale will be on Twitter holding an "online discussion focusing on national security accountability" using the hashtag #YourNatlSec. It's a huge chance for us to join our voices together and flood the conversation with pro-privacy messages -- will you join us? Rabble (2016-11-02)

*** National security green paper is a whitewash**
An opinion piece state, "To guide the much-lauded and keenly anticipated public consultation on national security - billed as an unprecedented opportunity for Canadians to shape national security law and policy - the government has published a national security green paper entitled "Our Security, Our Rights." The configuration of the title reflects the general orientation of the document: security first, rights second. While the green paper's self-proclaimed purpose is "to prompt discussion and debate about Canada's

national security framework," it seems far more concerned with manufacturing consent for Bill C-51's dramatic - and likely unconstitutional - expansion of security powers, than with enabling a well-informed public consultation. The federal privacy commissioner has observed that the "tone of the Government's discussion ... focuses heavily on challenges for law enforcement and national security agencies," as opposed to "democratic rights and privacy." According to the BC Civil Liberties Association (BCCLA), the green paper "reads like it was drafted by a public relations firm tasked with selling the current state of extraordinary, unaccountable powers." (And in response, the BCCLA has produced a "Different Shade of Green Paper," elucidating several problematic aspects of the Canadian national security framework that the government "forgot to mention.") The government's green paper and associated "background document" are a montage of tendentious elements. There are the Pablum reassurances ("National security institutions in Canada are professional, responsible, and effective ... They work within a well-defined set of legal authorities and respect Canadian law")." Toronto Star, A21

* **National security review must acknowledge Canadian government's shortcomings**
An opinion piece state, "The Liberal Party is conducting a national security review process to figure out how to fulfil its election-time promise of amending the "problematic" parts of Bill C-51, now the Anti-Terrorism Act. The government has published a 21-page "Green Paper," along with a 73-page backgrounder, to pose questions to the Canadian public on the parameters of what reforms should take place. But the Green Paper's rhetoric and the national consultation itself go beyond just the topic of Bill C-51. It goes on to pose more general and philosophical questions of what kind of society Canadians want to live in and how the citizens of this country want to prioritize what are apparently the competing rights of security and freedom. Unfortunately, though the Green Paper admirably addresses the important issues of Canada's national review structure (or lack thereof), as well as the secretive relationship between intelligence-gathering and the due process of law, its overarching outlook doesn't include a strong civil liberties perspective. (...) In other words, the consultation process and the Green Paper seem to have more or less ignored the robust criticisms regarding Canada's national security apparatus by civil society organizations, preferring instead to source (or "consult") public opinion as if Canadians haven't been voicing their concerns all this time. For instance, numerous civil society organizations, such as Canadian Journalists for Free Expression (CJFE) and the Canadian Civil Liberties Association (CCLA) have sounded the alarm on how Canadian agencies have collected metadata over the years. Individuals within government such as Daniel Therrien, the Harper-appointed Privacy Commissioner, along with Jean-Marie Plouffe, the former Commissioner of the Communications Security Establishment (CSE), have voiced similar concerns as to how current collection of "signals intelligence," which includes metadata, continues to jeopardize the privacy of Canadian citizens. And yet, despite these voices, the Green Paper doesn't include any mention of the CSE, Canada's main agency for the collection of signals intel." CBC News (2016-11-02)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

* **Mutisme à la GRC et au SCRS**
La GRC et le Service canadien du renseignement de sécurité (SCRS), les deux corps policiers fédéraux, ne veulent pas confirmer s'ils ont déjà mis des journalistes sous surveillance, contrairement à la SQ, qui a dévoilé ces informations hier à la suite de vérifications internes. Si le premier ministre du Canada Justin Trudeau a promis hier de « faire ce qui est nécessaire » pour défendre la liberté de la presse, son gouvernement ne demandera toutefois pas aux corps policiers fédéraux de dévoiler publiquement ce type d'informations, comme le réclament le Bloc québécois et le Nouveau Parti démocratique. La GRC précise seulement que « les cas où des enquêtes de la GRC concernant des journalistes ont eu lieu sont extrêmement rares ». La Presse +

Les Canadiens mal protégés contre la surveillance abusive, selon Snowden
Les Canadiens sont très mal protégés contre les pratiques de surveillance abusives, estime Edward Snowden, qui s'alarme des possibilités ouvertes aux services de renseignements d'ici et d'ailleurs par les nouvelles technologies de communication. L'ex-sous-traitant de la National Security Agency (NSA), qui participait hier à une vidéoconférence organisée par l'Université McGill, a souligné que le système de régulation des services de renseignement canadiens était probablement le plus « déficient en Occident ».

Il a déploré à ce titre que le gouvernement libéral de Justin Trudeau tarde à réviser la Loi antiterroriste, dite loi C-51, qui confère des pouvoirs accrus à ces mêmes services. Nombre d'analystes, a-t-il relevé, pensent que la loi en question est trop mal formulée pour être modifiée et devrait tout bonnement être retirée. M. Snowden estime qu'il n'est tout simplement pas possible, ici ou ailleurs, de faire confiance aux autorités pour utiliser de manière responsable les technologies de surveillance existantes. La Presse +, 1; Agence QMI (Journal de Montréal, Journal de Québec) (2016-11-03); Montreal Gazette (2016-11-02)

* **Six journalistes ciblés par la SQ**
Après le SPVM, au tour de la Sûreté du Québec. Le corps policier national québécois admet avoir obtenu secrètement les registres téléphoniques de six journalistes, dans le cadre d'une enquête sur les fuites d'informations aux médias amorcée en 2013. C'est ce qu'a confirmé le corps policier hier après-midi, dans la foulée des vérifications demandées par le directeur général Martin Prud'homme. Celui-ci dit avoir tout ignoré de cette affaire jusqu'ici puisqu'elle s'était déroulée sous la direction de son prédécesseur, Mario Laprise. «M. Prud'homme est très irrité», a affirmé le capitaine Guy Lapointe, porte-parole de la SQ. Joint par La Presse, Mario Laprise a refusé de discuter de l'affaire. «Je n'ai pas de commentaires à faire par rapport à ça. Il y a des vérifications qui sont faites, on va laisser les gens faire leur travail», a-t-il laissé tomber. La liste des gens visés. Parmi les reporters ciblés par la SQ, on retrouve le chef du bureau parlementaire de La Presse à Québec, Denis Lessard. «Je couvre la politique depuis près de 40 ans, souvent sur des dossiers délicats. On se dit toujours que c'est possible d'être épié par les policiers, mais on est convaincu qu'ils n'oseraient pas aller jusque-là. Eh bien, il semble qu'on se soit trompé», a-t-il réagi. Les journalistes de Radio-Canada Alain Gravel, Marie-Maude Denis et Isabelle Richer sont aussi du nombre, tout comme Éric Thibault, journaliste au Journal de Montréal et conjoint de Marie-Maude Denis. Le sixième journaliste est André Cédilot, journaliste chevronné de La Presse qui a ensuite travaillé pour Radio-Canada. La Presse (Le Quotidien, 21, Le Nouvelliste, La Voix de l'Est, La Tribune); Le Soleil; Le Droit; Agence QMI (Journal de Montréal, Journal de Québec)

* **Liberté de presse - La SQ a espionné six journalistes**
En lieu et place de l'" affaire Lagacé ", il faudra désormais traiter du scandale de la surveillance des journalistes : la Sûreté du Québec a confirmé mercredi qu'elle avait, tout comme la police de Montréal, traqué des reporters au cours des dernières années dans le cadre d'une enquête, suscitant une nouvelle vague d'inquiétudes et de dénonciations dans l'univers des médias. Le SPVM n'était donc pas seul à épier les faits et gestes des journalistes du Québec. En 2013, la SQ a mis sous surveillance les téléphones cellulaires de Marie-Maude Denis, Alain Gravel et Isabelle Richer de Radio-Canada, du chef du bureau de La Presse à l'Assemblée nationale, Denis Lessard, du reporter spécialiste du crime organisé André Cédilot et d'Éric Thibault du Journal de Montréal. Le corps de police tentait alors de faire la lumière sur une fuite d'information concernant l'enquête policière qui visait le président de la Fédération des travailleurs du Québec, Michel Arsenault. La SQ en a elle-même fait la révélation mercredi. (…) À Ottawa, le premier ministre Justin Trudeau s'est montré ouvert à la possibilité de revoir les lois pour protéger la liberté de presse. " On va regarder attentivement les conversations qui vont avoir lieu entre l'Hôtel de Ville de Montréal et [le SPVM], mais [...] comme on a dit plusieurs fois, ce gouvernement [se porte] à la défense de la liberté de la presse et on va faire ce qui est nécessaire pour l'encadrer, s'il y a d'autres étapes nécessaires. " Fait inquiétant, ni la Gendarmerie royale du Canada ni le Service canadien du renseignement de sécurité (SCRS) n'ont voulu préciser si des journalistes avaient déjà été, ou se trouvent actuellement sous écoute électronique. La Presse, A1, A8

* **Bienvenue dans le Club**
Alain (Gravel) ! Éric (Thibault) ! Denis (Lessard) ! Marie-Maude (Denis) ! Isabelle (Richer) ! Enchanté, moi, c'est Affaire. Comme dans Affaire Lagacé. Je me suis trouvé un nouveau prénom, cette semaine. Bienvenue, donc. Oui, bienvenue dans le Club des Journalistes espionnés ! Le local ne paie pas de mine, comme vous le voyez, mais c'est chaleureux ! Il y a de la bière dans le frigo (achetez-en de temps en temps), le mot de passe du WiFi est sur le routeur et le divan est un peu miteux, mais au moins on a le câble : RDI, LCN, TVA Sports, RDS, Canal Vie. Pour le téléphone, avant de faire un interurbain, faites le 9 et… C'est une blague, je n'ai pas fait installer le téléphone. On ne sait jamais, hein ? Blague à part, je suis content de vous recevoir. Je me sentais un peu seul, ici… Je l'ai dit toute la semaine : je suis sûr que je ne suis pas le seul à avoir été espionné par la police. Je pensais surtout au Service de police de la Ville de Montréal (SPVM), dont les réponses au sujet de l'espionnage d'autres journalistes ont été on ne

peut plus évasives. Et là, hier, paf, on a su le résultat des vérifications internes faites par la Sûreté du Québec (SQ) dans la foulée des révélations de La Presse : en 2013, six journalistes ont fait l'objet de mesures que Nixon à son plus parano n'aurait pas reniées. La Presse +

* **How to protect yourself (and your phone) from surveillance**
Cyber security and online privacy experts aren't surprised by revelations that Quebec and Montreal have been spying on several journalists. In fact they say journalists — and the public at large — are far too careless. When the news came out this week that police had been spying on LaPresse journalist Patrick Lagacé, it was no surprise to Geneviève Lajeunesse with Crypto Québec. "I was shocked by their shock." Here are five key tips to sum up Lajeunesse's advice on protection from online surveillance, whether you're a journalist, an anonymous source, or a citizen who happens to protect your privacy. CBC News

* **Protection des sources - Assez les abus!**
Un éditorial note, « La liberté de presse est menacée au Québec. Il est grand temps d'adopter une loi sur la protection des sources pour mettre fin aux abus de la police.\r\nIl ne s'agit plus d'un cas isolé ou d'un abus de pouvoir anecdotique par une grosse police en mal de contrôle. L'espionnage des journalistes d'enquête est un mal si répandu au Québec qu'il faut maintenant des actions fermes pour casser cette désagréable impression de vivre dans un État policier. Ces tares ne sont pas uniques au SPVM puisque la Sûreté du Québec (SQ) fouine aussi dans les téléphones intelligents des journalistes. Radio-Canada a révélé mercredi que la police provinciale avait obtenu les registres d'appels des téléphones intelligents de trois de ses reporters, Isabelle Richer, Marie-Maude Denis et Alain Gravel. Au total, les communications d'une bonne dizaine de journalistes ont été épiées par le Service de police de la Ville de Montréal (SPVM) ou la SQ depuis 2013. La dérive des policiers n'a d'égale que celle des juges de paix qui ont autorisé ces chasses aux sources. Deux institutions fondamentales en démocratie, la police et la justice, ont traité la liberté de presse, le journalisme d'enquête et la protection des sources avec une grossière indélicatesse. Le resserrement des règles dans l'octroi des mandats de surveillance des journalistes, annoncé mardi par le premier ministre Philippe Couillard, est un pas dans la bonne direction. » Le Devoir, A6; Montreal Gazette

* **Challenging jihadist propaganda online eggs on extremists: experts**
Challenging online jihadist propaganda with counterarguments or shutting down extremist websites and social media accounts have little impact, and distract from the real threat, according to experts. As the Islamic State group (IS) spread across parts of Iraq and Syria, it ramped up its outreach to youths. Videos shared online depicting executions and others touting the creation of a caliphate became powerful recruiting tools, drawing hundreds of Western youths to the Middle East to join IS. Experts who met this week in Quebec City to find ways to combat this threat agreed that IS has used online propaganda to extend the conflict zone like no other. (...) The American, British and Canadian governments have taken similar measures, and with the help of major Internet firms such as Twitter took down some 235,000 extremist accounts in the first six months. Digital Journal

* **La radicalisation, une «crise de l'engagement»**
Un article d'opinion rapporte, « Alors que se tient actuellement à Québec une grande conférence sur la radicalisation, il semble utile de se faire attentif à une voix venue du passé, mais pourtant bien présente, celle de Hannah Arendt. Dans un très beau texte de 1953, intitulé Compréhension et politique, la philosophe d'origine allemande écrivait que « dans la mesure où les totalitarismes sont apparus dans un monde non totalitaire (ils ne sont pas tombés du ciel, mais ont cristallisé des éléments présents dans ce monde), le processus de leur compréhension implique clairement, et peut-être essentiellement, que nous nous comprenions nous-mêmes ». Si ces quelques lignes concernent au premier chef le phénomène totalitaire — le nazisme et le stalinisme analysés par Arendt —, il est possible d'en tirer une leçon utile dans le cadre de la lutte contre toutes les formes de radicalisation menant à la violence. En effet, on y retrouve l'idée chère à Arendt de la « cristallisation » d'éléments présents dans la société qui, combinés les uns aux autres, peuvent déboucher sur des évènements catastrophiques. Ainsi en est-il de la radicalisation religieuse menant à la violence dont il a été largement question ces derniers mois. Cette dernière « n'est pas tombée du ciel » pour reprendre les mots de la philosophe. » Le Devoir

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Ministry promises to help children of immigrants get health coverage
A representative for migrants struggling to get health coverage for their B.C.-born children is "in a bit of shock" after the Ministry of Health called her organization this week with a pledge to fix the problem. Following months of campaigning by Sanctuary Health and the B.C. Health Coalition, three ministry staffphoned both organizations Tuesday to assure them it will help the affected families acquire coverage. Parents with precarious immigration status, represented by both groups, had complained the application process for B.C.'s Medical Services Plan (MSP) prevented them from enrolling their B.C.-born children. The ministry's call came a day after Postmedia published a frontpage article about the struggle of two parents from Mexico who have five times attempted to enrol their 18-month-old, B.C.-born son for MSP coverage. Both parents said their applications were hampered by requirements they provide documentation they don't possess and concern their identities would be shared with the Canada Border Services Agency. (...) Cruz said concern about the ministry contacting the CBSA was a major factor for these families and said the ministry assured them it doesn't contact border officials. Postmedia Network (Vancouver Sun, A5, The Province)

Couple charged with importing fentanyl
A couple from Kitchener is accused of importing fentanyl products from China into the United States and then mailing the powerful opioid drugs to Canada. Karl and Sorina Morrison, both 59, were arrested at a border crossing near Niagara Falls, N.Y., last month after an investigation by U.S. authorities. The couple has been charged with conspiracy to import and export controlled substances and analogues, and attempt to export controlled substances and analogues. Each charge carries a maximum penalty of 20 years in prison and a $1-million fine. (...) In a criminal complaint filed with a New York court, a Homeland Security agent says a package mailed from China to Karl Morrison at a mailbox in a UPS store in Niagara Falls, N.Y., contained four packets, two of which were found to contain types of fentanyl. (...) The complaint notes that the Morrisons have a son and that since 2009, five packages mailed to him were seized by the Canada Border Services Agency after they were found to contain controlled substances. Canadian Press (Kitchener-Waterloo Record, A1, Telegraph-Journal, Hamilton Spectator, Toronto Star); Calgary Sun (Ottawa Sun, Toronto Sun, Edmonton Sun)

Feds' fast-track of skilled, foreign workers lauded
The "critical" problem B.C. companies face in trying to lure skilled foreign workers to sectors such as technology and film may have been resolved with a new federal policy on hiring short-term overseas help. That was the preliminary conclusion Wednesday of B.C. Jobs Minister Shirley Bond, Vancouver Mayor Gregor Robertson, industry associations and one immigration policy expert in response to Finance Minister Bill Morneau's plan to fast-track foreign talent, announced Tuesday as part of his federal economic update. Bond went so far as to say the initiative could help convince Lululemon - which recently warned it could move its Vancouver head office overseas if the Temporary Foreign Worker Program doesn't become more flexible - to stay. (...) The plan includes setting what the government acknowledges is an "ambitious" two-week standard to process visas and work permits for "low-risk, high-skill talent" for "high-growth Canadian companies that need to access global talent in order to facilitate and accelerate investments that create jobs and growth." As part of the plan, Ottawa will create a "short-duration work permit" that applies to employees in Canada for fewer than 30 days a year, or those here on "brief academic stays." Vancouver Sun, A1

Crown seeks prison for LaSalle mother in gun smuggling case
A Crown prosecutor requested during a court sentence hearing Wednesday that a LaSalle mother found guilty of smuggling three loaded, nine-millimetre handguns into Canada receive three to four years in a federal penitentiary. (...) Michelle Downey, 38, on Aug. 10 was found guilty of 22 criminal and Customs Act charges by Superior Court Justice Scott Campbell. The woman testified during her trial she didn't know acquaintances in Detroit had hidden the guns behind the glove box in her car before she drove over the Ambassador Bridge on April 21, 2013. But Campbell determined based on evidence that Downey's explanation wasn't believable - that she knew about the guns in her vehicle, what she was doing was a crime and was paid $1,000 in cash each time to smuggle handguns into Canada. Windsor Star, A7

*** Six months of Peace Bridge lane closures begins on Nov. 15**
With the busy summer tourism season out of the way, the Peace Bridge Authority announced this week it would soon be bringing in long-term lane closures related to construction work. Starting on Nov. 15, one lane will be closed – bringing the bridge down to just two lanes – and will remain closed until May 15, 2017. The closure is necessary to accommodate the $100-million rehabilitation project on the bridge. As it preps to bring in the closures, the PBA also urged, yet again, to have inspection booths staffed to appropriate levels needed to keep traffic flowing smoothly. Border wait times over the summer skyrocketed, however, the PBA said much of the delays were due to the high number of vacancies at the inspection booths. Through the summer, it was not uncommon to see only a handful of inspection booths open, while the rest sat empty. "So long as customs appropriately staffs and keeps inspection lanes open this winter, then we anticipate little to no traffic disruption," said PBA Board Chair Sam Hoyt. (…) "While we are pleased that a respected, third-party traffic consultant has determined that our closure plan will not impact the continued flow of cars and trucks across the span, it is important to note that this positive traffic flow scenario is contingent on proper Customs staffing and inspection lane availability," said Hoyt. "We've gotten strong indications from U.S. Customs and Border Protection that they can meet the staffing demand and we need Canada Border Services Agency to follow suit." Niagara This Week (2016-11-02)

Politics This Morning: Lisa Raitt to hold press conference to kickoff leadership bid
Today is Thursday, Nov. 3. (…) Representatives from Immigration, Refugees and Citizenship Canada (IRCC) and the Canada Border Services Agency (CBSA) will be holding a teleconference to provide details on the Electronic Travel Authorization (eTA) program, and other updates to travel document requirements. This is set to the place at 1 p.m. and is for background only-not for attribution. Hill Times

*** PVT Canada 2017 : les inscriptions sont ouvertes**
Depuis ce lundi 17 octobre les inscriptions au PVT Canada 2017 sont ouvertes, ce sont les autorités canadiennes qui en ont fait l'annonce. Les jeunes Français et Belges souhaitant s'envoler vers le Canada peuvent soumettre leur candidature en ligne afin de pouvoir participer aux rondes d'invitations prévues pour dans quelques semaines. (…) Les places d'obtention du PVT Canada sont limitées en raison d'un quota établi. En 2016 il était de 6 500 places pour les citoyens français et 750 pour les citoyens belges. Le nombre de demandes étant supérieur aux places disponibles, la sélection des candidats se fait par tirage au sort depuis 2016, alors qu'auparavant elle se basait sur la règle du premier arrivé, premier servi. Le Parisien Étudiant

*** Desserte aéroportuaire : l'Office du tourisme de Québec interpelé**
L'ancien président du Réseau de transport de la capitale (RTC), Gilles Marcotte, croit que c'est à l'Office du tourisme de Québec d'assumer le leadership pour l'implantation d'une éventuelle navette aéroportuaire. L'Office avait pourtant rejeté un tel projet en 2013. « Tous les organismes qui travaillent au développement du tourisme devraient contribuer », suggère M. Marcotte, qui a été à la tête du RTC en 2006. Déjà, à l'époque, l'idée d'une desserte vers l'aéroport Jean-Lesage était discutée, mais plus ou moins structurée », se rappelle-t-il. Dix ans plus tard, il estime qu'il est temps que le dossier se concrétise. « On investit beaucoup d'argent dans les infrastructures dans l'aéroport avec le centre de prédédouanement. Donc, on a besoin d'une navette. C'est officiel. » Radio-Canada (2016-11-02)

Stay home
A letter to the editor states, "Note to American celebrities threatening to "come to Canada" if Trump gets elected: Our Canada Border Services may have something to say about your decision. This ain't Hollywood, folks. It's The Great White North and we do the choosing!" Toronto Sun, A16

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Teen charged for prank bomb threat in Vernon**

A youth has been criminally charged in relation to a prank bomb threat at the Landing Plaza last summer. The Vernon RCMP confirms a 17-year-old is facing a charge under the 'false messages' section of the criminal code after he allegedly made a prank call about a bomb. The incident prompted a full scale emergency response from police, the fire department, B.C. Ambulance, and bylaw services on July 12. Numerous businesses in the Landing Plaza on 25 Avenue were evacuated and forced to close down while police investigated the threat. While no one was hurt and the incident turned out to be a hoax, it was serious enough for police to recommend charges to Crown counsel. Shortly after the prank, Sgt. Mike Moyer of the Vernon RCMP said they wanted to send a strong message that such acts will not be tolerated. The false messages charge is laid against people who send information they know to be false, either by letter, telegram, phone, cable or radio, with the intent to injure or alarm others. The offence carries a maximum sentence of two years in jail. The incident in Vernon is not the first time police in the Interior have been deceived with false information — an act known as 'swatting'. Last year in Kamloops, several schools were locked down due to swatting pranks involving fake bomb threats. Because he is a minor, the teen's identity is protected under the Youth Act. Infotel

*** In Canadian first, liquid fentanyl seized on the street, Hamilton police say**

In what Hamilton, Ont., police believed is a first in Canada, fentanyl in a liquid form has been seized from suspected street-level drug dealers. The dark brown glass vial of liquid, containing about 20 mL of liquid, was confiscated by Hamilton police's vice and drug unit in May, but was originally believed to be GHB. It was sent to Health Canada for routine laboratory testing along with other drugs seized prior to a criminal prosecution. The test results showed it was liquid fentanyl. Even then the significance didn't register. Det. Const. Adam Brown, of the city's drug unit, said it was not until he attended a fentanyl-themed police conference in Alberta this month that he learned how unique a find it was. Experts at the conference told him that liquid fentanyl had not previously been seized on the streets in Canada. "Fentanyl hasn't been widely seen in Hamilton. It was at the conference, in discussions with people who had the specialized knowledge, that we realized the seizure was such a big deal. "This is something very new to us," he said. "It is extremely dangerous, even in small amounts." Fentanyl is a powerful opioid painkiller. When Brown handles the vial he wears a full chemical protection suit, a respirator and double rubber gloves because fentanyl can easily be absorbed through the skin. Health Canada estimates a lethal dose of pure fentanyl for a typical adult is as little as two milligrams. National Post; Hamilton Spectator

*** Surrey Mountie accused of child luring to appear in court Nov. 30**

Surrey RCMP Constable Dario Devic is expected to appear in Surrey provincial court on Nov. 30 on a charge of child luring. Devic was arrested on Sept. 9 after Creep Catcher Surrey, a citizen group that aims to weed out "potential predators" and "blast" them in social media, did a sting outside a local mall. A woman working with Creep Catcher Surrey posed as a 15-year-old girl and allegedly communicated with the officer online after posting an ad on Craigslist. A meeting was set up outside the Boston Pizza at Surrey Central Shopping Mall in Whalley and Creep Catcher Surrey president Ryan LaForge and his crew live-streamed the sting on the Internet. Devic's last court appearance, set for Oct. 19, was adjourned to Wednesday, Nov. 2. He didn't appear in court on either date. Supporters of Creep Catchers, wearing black hoodies and masking their faces with scarves, rallied outside the courthouse on Oct. 19. A handful of them were also at court Wednesday, when the arraignment hearing date was set. LaForge told the Now another rally will be staged on Nov. 30 and he expects it will be bigger than the first. Now News

*** RCMP part of international raids on Darknet users**

Law enforcement agencies around the world are stepping up their efforts to check the growth of cyber crime, most recently last week when nine police and intelligence agencies, including the RCMP, launched co-ordinated action against buyers and sellers of illicit drugs and other illegal activities on Darknet global marketplaces. "In Canada, the collaboration between the Royal Canadian Mounted Police, Canada Post, and the Canada Border Services Agency led to the identification and targeting of an international distributor of narcotics based in Quebec that was operating on the Darknet," the force said in the statement. "This resulted in numerous seizures and the detention of an individual involved in the international distribution of the narcotics. The investigation is ongoing." Internationally the action, dubbed by all participants as Operation Hyperion, resulted in numerous international seizures, arrests and leads on cases related to the buying and selling of illicit drugs and other goods on the Darknet, the part of the

Internet only accessible through browsers that ensure Websites selling illegal material can only be reached anonymously. The RCMP said the operation will also help law enforcement agencies continue to combat the trafficking of illegal goods and services by identifying new smuggling networks and trends. IT World Canada (2016-11-02)

*** Kamloops RCMP predict Fortis B.C. phone scam will be back as temperatures drop**
A scam that has surfaced on and off over the years in a variety of forms could be back in Kamloops this winter. Kamloops RCMP spokesperson Cpl. Jodi Shelkie says a phony Fortis B.C. phone call scam has the potential to rob residents of their hard earned money. "Some people call and say 'I'm from Fortis and you're way behind on your gas bill. If you don't pay it we're going to cut off your gas immediately'," Shelkie says. This can cause homeowners to panic, she says, with residents believing they will have their gas shut off and have their house become cold in the winter. "They'll ask for a prepaid debit card or something," Shelkie says, "It's better (for them) if they have a prepaid credit card." Shelkie says there are steps people can take to protect themselves from scammers. "Even if they do call, just say 'I'm going to call back and ask for accounting and speak to them," Shelkie says. Last summer, Fortis B.C. sent out a news release about the scam. Infotel (2016-11-02)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Shafia murder convictions to stand
A father, mother and son found guilty in the drowning deaths of three teenaged sisters and another woman who had apparently shamed the family lost their bid Wednesday to overturn their first-degree murder convictions. In unanimously rejecting an appeal by the Shafia family members, Ontario's top court ruled, among other things, that expert evidence on so-called honour killings had been properly admitted at their trial and the son was properly tried as an adult. Canadian Press (Kingston Whig-Standard, A1, The Guardian, Waterloo Region Record, Red Deer Advocate, The Telegram, Ottawa Citizen, Times & Transcript, Whitehorse Daily Star, Hamilton Spectator, Times Colonist, Chronicle-Herald, National Post, Cape Breton Post); La Presse Canadienne (Le Devoir, Le Quotidien, La Tribune, La Presse); Le Journal de Québec (Journal de Montréal); Edmonton Sun (Calgary Sun, Ottawa Sun, Toronto Sun)

Kingston Penitentiary's next life
An opinion piece states, "Although a credible sifting of ideas from the community for reworking the site, one worries about the joint city/correctional service visioning project missing Kingston Penitentiary's overriding historical and social/economic importance to the Kingston region, how it has been a cultural anchor for decades. This must not fade to black but be commemorated in the redevelopment of the site. It is totemic: seven generations of breadwinners - builders, architects, prison guards, healthcare trained staff, warden's staff - have driven the Kingston economy and minimized evil and danger lurking among the law-abiding for 177 years... For Canada, "KP is a monument to correctional history," reports architectural historian Jennifer McKendry, the same as is Eastern Penitentiary at Philadelphia for the U.S. You can shortcut through KP's labyrinthine history via **Correctional Service Canada's** "Historical Overview." Kingston Whig-Standard, A5

*** Judy Ogden's murder, Dale Ogden's release 'a fail in the justice system': St. John's lawyer**
St. John's lawyer Lynn Moore remembers the 1997 murder of Judy Ogden. Moore was a Crown attorney at the time. She especially remembers thinking the crime could have been prevented. "Specifically, I recall that he [Dale Ogden] was on bail when he committed this murder and that struck me as a failing of the justice system. That he was allowed or given the opportunity to commit this heinous crime," she said. Dale Ogden, who had a court order to stay away from his estranged wife Judy, forced his way into her home and beat her to death while their four-year-old son Daniel watched. Ogden served 16 years behind bars for second degree murder. He was released in September of this year. Daniel Benoit is now 22 and suffers from post traumatic stress . He's fighting with Correctional Services Canada and the National Parole Board for more information on the whereabouts of his father, who is out on day parole near Victoria, B.C. Benoit is registered as a victim, but does not feel Correctional Services Canada is transparent enough on Ogden's whereabouts and who he is in contact with. He requested recent pictures

of his father, but his request went unanswered. The Privacy Act protects Ogden's personal information. CBC News

*** Keep killers in jail longer, says convict's son**
A Newfoundland man who was four years old when he saw his father brutally beat his mother to death says he's living in fear knowing Dale Ogden is out on day parole and believes he should have received a more punitive sentence. Daniel Benoit, 22, said he wants to start a national conversation about murder sentences and Canada's justice system in general, which he says lets convicted murderers off too easily. Ogden was sentenced to life in prison for the second-degree murder of his wife Judy Ogden in early 2000, and the judge set his parole eligibility at 14 years. He has been out on day parole since September after being released from William Head Institution in Victoria, B.C. Canadian Press (Chronicle-Herald, A10, The Guardian)

*** Indigenous jail population: Prison reforms must go beyond justice**
An opinion piece states, "Last week, Australian Attorney-General George Brandis launched yet another inquiry into what he called a "national tragedy" - the country's exploding aboriginal prison population - and directed the Australian Law Reform Commission to come up with solutions to the crisis... You could easily substitute Canada for Australia in the above sentence. Despite long ago recognizing the travesty of disproportionate indigenous incarceration, the aboriginal prison population has risen unabated in both countries. While they make up 4.3 per cent of Canada's population, First Nations, Métis and Inuit account for a quarter of inmates in federal prisons. In the past decade, the overall federal prison population rose by 10 per cent; aboriginal incarceration spiked by 50 per cent... About half of Canada's 1.5 million aboriginals are under the age of 25 and the indigenous population is projected to grow at as much as twice the rate of the overall population over the next two decades. Without major changes, Canada will soon be facing an ever bigger aboriginal incarceration crisis." Globe and Mail

*** Woman tried to smuggle morphine into prison**
A Winnipeg woman has been convicted of attempting to smuggle morphine into Stony Mountain Institution after a judge rejected her claim she feared she might be "done in" if she didn't comply. Sandra Dignard, 36, was arrested Dec. 21, 2012, after corrections officers caught her trying to enter the prison with 100 morphine tablets hidden on her body. Dignard will return to court for sentencing early next year following the completion of a court ordered pre-sentence report. Winnipeg Sun, A3

*** Sentence Turfed: Court of Appeal overturns adult conviction for woman in U of C student's murder**
Alberta's top court has overturned the adult sentence handed to a woman who took part in the slaying of U of C student Brett Wiese, reducing her punishment to the maximum youth term. In a 2-1 split decision the Alberta Court of Appeal said the appropriate sentence for the now 21-year-old is four years of custody followed by three years of community supervision. In a dissenting opinion, Justice Bryan O'Ferrall said he would have upheld the life sentence without parole for a minimum seven years, handed the woman in May, 2015. But in overturning the adult sentence handed the convicted killer, Justice Patricia Rowbotham said Court of Queen's Bench Justice Charlene Anderson erred in finding the woman's blameworthiness wasn't diminished by her immaturity. Since the offender is now serving a youth sentence she can no longer be identified. Calgary Sun, A16 (Calgary Herald); CBC News

*** Johnson released pending appeal**
Former Windsor Spitfire Ben Johnson, sentenced last week to three years in prison for a 2013 rape, was released from jail on $45,000 bail Wednesday and ordered to live in Windsor, according to documents signed by a local justice of the peace. The Ontario Court of Appeal Tuesday granted Johnson bail pending appeal. Johnson was able to fulfil the bail requirements Wednesday. Windsor Star, A5; London Free Press

*** Prisons shouldn't allow conjugal visits**
Re: "Prison conjugal visits defended," Nov. 1.
A letter to the editor states, "The rationalization in support of conjugal visits in our federal prisons program is not convincing. Whether you believe the purpose of incarceration is to impose retribution or enable

rehabilitation, neither justifies the facilitation of sexual privileges for prison inmates. Unintended consequences inevitably occur. A case in point is that of the noted eight-month pregnancy of prisoner Kelly Ellard, impregnated on a conjugal visit by a boyfriend who was a prisoner on day parole from a different prison. It is past time to emulate prison policy from such jurisdictions as Britain and the U.S. (federally), where conjugal visits are not allowed." Times Colonist, A11

*** Torture behind bars**
An editorial states, "Ontario Premier Kathleen Wynne isn't taking lightly reports that a prisoner facing trial in her province was subjected to treatment defined as torture. Far from it. When asked, she volunteered that it was "extremely disturbing." And she assumed it was being looked into. Oh. Good. Recent revelations about Adam Capay's horrific treatment in an Ontario correctional facility are, indeed, extremely disturbing. But not, unfortunately, a surprise. The province has a major problem with its jails and court system. Yet based on its plodding, lackadaisical response to this incident and many others, the government seems unable to grasp the fact." National Post, A8

*** Different takes on Adam Capay case**
Justice delayed, once again, Editorial Oct. 30
A letter to the editor states, "Adam Capay spent four years in solitary while awaiting trial. Since by UN standards his ordeal was worse than the most severe sentence he would be likely to get if he was tried and found guilty, he should be released, with compensation, immediately. There's also the question of the jail superintendent and anyone else responsible for keeping him in solitary. Perhaps they should spend a few months in solitary so they can understand what they have done." Toronto Star, A20

*** Time to address systemic inequality**
An opinion piece states, "Manitoba has a prison problem. It isn't just that Manitoba imprisons its citizens at nearly three times the Canadian average. And it isn't just that 60 per cent of those prisoners are legally innocent, in prison awaiting trial. Nor is it simply that 70 per cent of people in Manitoba prisons are indigenous, a number more indicative of serious systemic racism in Manitoba than anything else. Although each of those numbers is concerning on their own, confronting the prison problem became unavoidable when we learned that in 2016, seven people have died while in custody in Manitoba. Five of those were inmates at the Winnipeg Remand Centre. The deaths in state custody of Hollie Hall, Errol Greene, Robert McAdam, Russell Spence and three others whose names we do not yet know, are all tragedies. Each of these people relied on the government and were under the complete control of the government. Their medicine was dispensed (or not) according to government policies. They were given emergency medical treatment (or not) according to government policies. They were allowed to leave their cell (or not) according to government policies. The government must be held accountable for their deaths." Winnipeg Free Press

*** Showered In Complaints: Ottawa jail among tops for gripes, despite size**
The Ottawa-Carleton Detention Centre remained among the three most complained-about jails in Ontario, despite being the only jail in the top five that housed fewer than 1,000 inmates. There were 394 complaints about the Ottawa jail to provincial ombudsman Paul Dube during the 2015-16 fiscal year, the ombudsman said in his annual report released Wednesday. The good news was that the number of complaints has been trending slightly downward since 2013-14, when there were 416 complaints. It was also down slightly from the previous year's 410 complaints. The Ottawa-Carleton Detention Centre "has consistently been one of the most complained-about in the province," said the ombudsman. The OCDC made the top three even though it has a capacity of 505 inmates, less than half that of the Central East Correctional Centre in Lindsay, Ont., which had 647 complaints, and the Toronto South Detention Centre, which had 455 complaints. The bulk of complaints from OCDC were about health care issues, but there were also 27 about segregation and 26 about living conditions, the ombudsman said. That included one from an inmate who was housed in a shower in March 2016. Ottawa Sun, A10 (Ottawa Citizen)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Lack of funding forces women's addiction centre to halt services**
Despite the overwhelming need for addiction services in New Brunswick, a women's treatment facility in Tracy will suspend services as of Dec. 1. Bridges of Canada, a non-profit organization, has been operating the Sarah Tracy Centre for Women in Tracy, which is located about 40 minutes from Fredericton, since the spring of 2014. Misty McLaughlin, a spokeswoman for the centre, said Wednesday that the centre will be temporarily suspending services to its clients as of the first of next month because it lacks the $800,000 required to run the live-in centre and addictions treatment programs offered there. Times & Transcript, A6

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Genesis House Looks To Reach More Demographics With New And Established Initiatives**
The women's shelter will host its annual Family Dance this Friday, November 4th at the Morden Friendship Centre, the usual P.J. parties are planned at the branches of the South Central Regional Library, and Peace Begins at Home hockey games with the Winkler Flyers, Garden Valley Collegiate Zodiacs, and Pembina Valley Hawks. (...)In addition to their established events during the month of November, Braun said the women's shelter is launching some news things. "Last year I was able to attend the World Conference for Shelters, and the United Nations has a couple of things they do, so we are picking up on one of those things." She said they have engaged with the art galleries in Winkler, Morden, and Altona to light up in purple." This will take place during the 16 days of activism for gender based violence, November 25th to December 10th. During the 16 days of activism, Braun noted the art gallery in Morden will exhibit the faceless dolls, representing missing and murdered Aboriginal woman. Pembina Valley Online

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Edmonton city councillors consider zoning restrictions on marijuana dispensaries**
City councillors are asking if new marijuana dispensaries should be kept away from schools and restricted like liquor stores. Worried about a proliferation of dispensaries and grow-ops when Ottawa legalizes recreational marijuana, Coun. Mike Nickel introduced a lengthy zoning inquiry at council's planning committee Wednesday. "We can't bury our heads in the sand anymore on this. ... We need to be proactive," Nickel said, pointing to the way marijuana dispensaries spread in Vancouver, rivalling the number of Starbucks. Vancouver has since restricted how close each pot shop can be to the others, similar to how Edmonton limits liquor stores to being 500 metres from a competitor. Liquor stores here must also be 100 metres from a school. But drinking liquor near a store doesn't affect bystanders the same way a cloud of pot smoke would, Nickel said: "As an intoxicant, how are you going to deal with that?" The federal Liberals committed to legalizing and restricting access to marijuana in their 2015 throne speech. They've launched a task force with cross-country meetings on how to effectively do that. Edmonton Sun

*** Cannabis in your blood stream doesn't mean you're stoned**
Before raising the alarm on cannabis-impaired motor vehicle accidents, the stats presented in this article require additional clarification and contextualization. Unlike alcohol, for which there is a close correlation between blood-alcohol content and impairment, there is no defined standard of impairment for cannabis. Determining whether or not these drivers were impaired by cannabis is further complicated by the fact that tetrahydrocannabinol (THC) — the primary psychoactive component in cannabis — can be detected in the blood several days and even weeks after consuming cannabis. This means that the observed increases in the proportion of fatally injured drivers testing positive for cannabis in these states might not

indicate increases in cannabis-impaired driving, but rather general increases in cannabis use following legalization. This is particularly plausible when we take into consideration the overall rate of motor vehicle accidents over time. Surveillance for cannabis among drivers in Colorado and Washington likely increased with legalization. Province

*** Beer Companies Don't Know How to Handle Marijuana Legalization Yet**
One of the bigger unknowns in the marijuana legalization movement is how the end of prohibition will affect the alcohol and tobacco industries. While current generations may not let legal weed curb their booze and cigarette cravings drastically, future generations may not see the benefit of straying from cannabis for a more dangerous alternative. Understandably, beer companies are nervous about that precise possibility. On a recent conference call to discuss quarterly earnings, Molson Coors International CEO Stewart Glendinning gave some insight as to how his company was handling looming cannabis legalization. Asked by an analyst how the imminent legal marijuana market in Canada may affect beer sales, Glendinning answered, "Cannabis is something we are thinking very carefully about, not only as a business but also as an industry." Canada is set to introduce recreational marijuana legislation in the Spring that will legalize the plant nationwide. Marijuana

*** Canada legal cannabis no tax windfall: report**
Canada will have little wiggle room to tax recreational marijuana sales when it moves to legalize the psychoactive drug, a report to parliament said Tuesday. One of the principal rationales cited by supporters for ending the prohibition on pot has been the bounty of tax revenues legalization would bring. But parliamentary budget officer Jean-Denis Frechette, tasked with providing independent analysis to lawmakers, warned it would not be a bonanza. Retail sales taxes are expected to be relatively modest at the start -- about Can$300 million to Can$600 million (US$224 million to US$448 million) and not billions, he said. That is far below the annual future cannabis tax revenue of up to Can$5 billion estimated by CIBC World Markets in January. Also, tax policy decisions will require trade-offs between the government's two main objectives: discouraging consumption among Canadian youths and reducing the profits in the illicit cannabis market. China Post

PUBLIC SERVICE / FONCTION PUBLIQUE

*** After Phoenix and Shared Services problems, government seeks feedback on digital future**
The federal government continues to receive advice on how it should improve its digital future as it works to fix problem-plagued projects including the Phoenix payroll system and Shared Services Canada. In a so-called, "intimate, armchair discussion" at the annual GTEC conference in Ottawa on Wednesday, parliamentary secretary for Public Services and Procurement Canada, Leona Alleslev opened up about the pitfalls experienced in the development of Shared Services Canada, or SSC. The department that's drawn criticism from other departments, including the RCMP, Statistics Canada and the Auditor General. Alleslev acknowledged the project has been ambitious with aggressive timelines and its attempt to save money. (…) Shared Services was created to streamline information technology across the government by combining more than 100 different email systems into one, reducing the number of data centres from 600 to about 20 and make the systems more secure and reliable. It was also supposed to save money. But to date, savings have not been realized, only 80 data centres have been closed, and the centralized email system is currently on hold with no scheduled date for completion. CBC News

*** Bonuses at Shared Services Canada despite criticisms**
Shared Services Canada approved more than $1.5 million in bonuses and merit pay for its executives, despite a year of widespread criticism of the agency's botched technology projects. More than 100 senior managers were awarded the extra pay in the summer, including 19 who received bonuses of about $4,300 each, CBC News has learned. The executives also received so-called "performance pay" for succeeding or surpassing expectations, sharing a pot of $1.5 million among them, or an estimated $15,000 each on average. CBC News

OTHER / AUTRE

NIL

INTERNATIONAL

*** German interior minister lauds detention of terror suspect**
Germany's top security official is praising the detention of a suspected extremist in Berlin, saying it shows authorities are being vigilant and doing "everything to avoid terrorist attacks in Germany." The man, who claims to be 27 and from Syria, was taken into custody late Wednesday on suspicion of being a member of the Islamic State militant group. Interior Minister Thomas de Maiziere said Thursday "it is very good this person has been taken out of circulation." He said the suspect had been under surveillance for a while, but didn't give further details. Associated Press (Metro News) (2016-11-03); Deutsche Welle (2016-11-02)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 4, 2016 / le 4 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

*** Feds hold Twitter consultation on national security**
Public Safety Canada held a Twitter chat Thursday night to hear what Canadians think about national security and its responsibility to Canadians. The department in charge of the RCMP, the Canadian Security Intelligence Service and its oversight body, and the Canada Border Services Agency asked people to tweet them using the hashtag #YourNatlSec starting at 8 p.m. ET to discuss accountability in national security. (...) **Public Safety Minister Ralph Goodale** didn't participate in the Twitter chat. New Democrat justice critic Murray Rankin says he wanted as many people as possible to participate. "Any effort to get Canadians engaged is great," he said. The department is holding national security townhalls across the country until Dec. 15. It's also is accepting input on its website too. Rankin, who once served as a lawyer to the Security Intelligence Review Committee, says he'd like to see changes to C-22. The bill would set up a parliamentary committee to review spy agency activity after the fact, but no oversight

during operations. **Goodale** has promised more changes to C-51 are still to come, but Rankin says he wants to know when. "It's been more than a year. I haven't seen a single comma change in C-51, which is an odious bill that deserves to be, we say, repealed," he said. CTV News (2016-11-03)

*** CSIS collected data on citizens for past 10 years**
Canada's spies for almost a decade illegally kept and analyzed data on people who posed no threat to national security, a federal court judge has ruled. In a scathing ruling, Justice Simon Noël said the Canadian Security Intelligence Service had illegally retained an unknown amount of data on "third party" and "non-threat" individuals since 2006. CSIS fed that data into a powerful database that allowed the agency to draw out "specific, intimate insights into the lifestyle and personal choices of individuals," read the heavily censored court ruling, circulated to journalists on Thursday. (...) The revelations prompted an unprecedented snap press conference by CSIS director Michel Coulombe. Coulombe told journalists the agency believed its actions were legal, from 2006 until October's ruling, but accepts Noël's findings. Coulombe could not, however, explain why CSIS believed it needed to inform the court of ODAC's existence in 2006, but failed to do so for almost 10 years. "I'll be honest, we went through our records and we really can't find a good explanation of why the court was not informed," Coulombe told reporters Thursday evening. Coulombe was clear that CSIS believed the program was useful and effective, and said he would like to keep it in operation. "That is something I will discuss with officials, (**Public Safety Minister Ralph Goodale**) and it is a public policy decision that the government and parliamentarians will have to make," the director said. In a statement, **Goodale** said the government will not appeal Noël's decision. But the minister did leave open the possibility of changing the CSIS Act to allow for such techniques in the future. **Goodale** noted the court ruling found the legislation governing CSIS was beginning to ***"show its age"*** after 30 years, and threats and investigative techniques have changed over that time. **Goodale** said he would be discussing CSIS's failure to tell the court the full truth, however, with the agency's senior management. ***"In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the (government) are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms,"*** **Goodale** wrote. Toronto Star, A1

*** Le SCRS a conservé illégalement des données personnelles**
L'agence d'espionnage du Canada a agi dans l'illégalité en conservant des données personnelles pendant 10 ans, a tranché la Cour fédérale. Dans un jugement rendu public hier, le magistrat Simon Noël a statué que le Service canadien du renseignement de sécurité (SCRS) avait manqué à son devoir d'informer le tribunal de son programme de collecte de données, qui opérait en vertu d'ordonnances judiciaires. Le juge Noël estime que le SCRS aurait dû communiquer ses activités à la Cour puisqu'elles ne concernaient pas directement la sécurité nationale. Colliger les données permet à l'agence d'identifier des habitudes de déplacements, de communication, de comportements et de liens qui lui seraient sinon inaccessibles, a indiqué hier le directeur du SCRS Michel Coulombe, qui dit « regretter que le SCRS a manqué à son obligation de franchise envers la Cour ». Rappelant « l'efficacité de l'analytique de données », le SCRS a l'intention de poursuivre ce programme dans le respect de la loi. Le **ministre de la Sécurité publique, Ralph Goodale**, a indiqué **« accueillir positivement »** la décision rendue dans cette affaire, et a souligné que le gouvernement n'interjetterait pas appel. Le **ministre Goodale** a dit prendre **« très au sérieux »** les conclusions du juge et a assuré qu'il ferait le suivi avec le SCRS. ***« Lorsqu'il est question de la sécurité et du renseignement, les Canadiens doivent avoir la certitude que tous les ministères et organismes du gouvernement du Canada réussissent efficacement à assurer la sécurité des Canadiens, et ce, en accordant autant d'importance au respect de nos droits et libertés »,*** a indiqué le **ministre Goodale** dans un communiqué. La Presse, 10; Journal de Montréal

CSIS data program illegal, court rules
The Federal Court of Canada has faulted Canada's domestic spy agency for unlawfully retaining data and for not being truthful with judges who authorize its intelligence programs. Separately, the court also revealed that the spy agency no longer needs warrants to collect Canadians' tax records. All this has been exposed in a rare ruling about the growing scope of Canadian intelligence collection disclosed by the court on Thursday. At issue is how the federal domestic spy service has been pushing past its legal boundaries in the name of collecting data, in hopes of rounding out the holdings of a little-known Canadian intelligence facility dubbed the "operational data analysis centre." Many corporations and

government agencies are now gravitating toward so-called big data computer analytics that can predict patterns of future behaviour based upon records about what has happened in the past. Spy agencies are no different, and the centre in question appears to be the Canadian Security Intelligence Service's equivalent of a crystal ball - a place where intelligence analysts attempt to deduce future threats by examining, and re-examining, volumes of data. (...) Following the ruling, **Public Safety Minister Ralph Goodale** released a statement that was equal parts stern and upbeat. ***"I will be pursuing this criticism with the executive management of the service,"*** he said. But **Mr. Goodale** added that the judges mentioned that CSIS's data-analytics program "***has yielded some useful intelligence results."*** He suggested the program could be bolstered with a few legislative changes. ***"The CSIS Act is now more than 30 years old and showing its age as global affairs, threat profiles, technology and public expectations have rapidly evolved,"*** **Mr. Goodale** wrote. Globe and Mail, A15

CSIS broke law by keeping sensitive metadata

A Federal Court judge says Canada's spy agency illegally kept potentially revealing electronic data about people who posed no security threat over a 10-year period. In a hard-hitting ruling made public Thursday, Justice Simon Noel said the Canadian Security Intelligence Service breached its duty to inform the court of its data-collection program, since the information was gathered using judicial warrants. CSIS should not have held on to the information since it was not directly related to threats to the security of Canada, the ruling said. "Ultimately, the rule of law must prevail," Noel wrote, adding, "without it, the actions of people and institutions cannot be trusted to accurately reflect the purpose they were entrusted to fulfil." **Public Safety Minister Ralph Goodale** welcomed the decision and said the government would not appeal. CSIS crunched the data beginning in 2006 using a powerful program known as the Operational Data Analysis Centre to produce intelligence that can reveal specific, intimate details about people the spy service monitors, the judge said. The improperly retained material was metadata - information associated with a communication, such as a telephone number or email address, but not the message itself. Canadian Press (Hamilton Spectator, A8, Calgary Sun, Edmonton Sun, Kingston Whig-Standard, Ottawa Sun, London Free Press, Toronto Sun, Winnipeg Sun, Waterloo Region Record, Fort McMurray Today); Presse canadienne (Le Droit)

Secret CSIS unit illegally kept data, court rules

A previously unknown unit of Canada's intelligence service has been illegally keeping data unrelated to national security threats, the Federal Court disclosed Thursday. In a hard-hitting ruling that was partly blacked out, Justice Simon Noel rebuked the Canadian Security Intelligence Service for not telling the court about a secret metadata program launched in 2006. The Operational Data Analysis Centre was unknown even to the judges who had been issuing the warrants to collect the information it mined, according to Noel's ruling. (...) **Public Safety Minister Ralph Goodale** said the government would not appeal the decision and would ask the Security Intelligence Review Committee to ***"monitor the situation carefully to ensure compliance."*** **Goodale** said he intended to speak to the CSIS executive about Noel's findings and had taken note of the court's observation that the CSIS Act was ***"now more than 30 years old and showing its age."*** The ruling touched on an issue many governments are struggling to address: amid fears over terrorism, how far can they can intrude into the lives of citizens in the name of national security? Postmedia Network (National Post, A1/Front (Edmonton Journal, Calgary Herald, StarPhoenix, Windsor Star, Leader-Post, Ottawa Citizen, Montreal Gazette, London Free Press)

* **Canadian spy agency put on notice**

A Canadian federal court has dealt the country's spy agency a major blow by declaring it illegally kept data collected during investigations over the past decade. It has also threatened sanctions if it happens again. Although judges have previously criticised the Canadian Security Intelligence Service (CSIS) for a lack of openness, the ruling is being seen as particularly uncompromising. Federal Court Judge Simon Noel said CSIS secretly set up a special data analysis centre in 2006 to help track potential terrorism suspects. However, he said it stored and retained electronic information from people not linked to particular threats, which it was not permitted to do."CSIS has a limited mandate which does not permit the retention of associated data ... as it has done so since 2006. Therefore this retention of associated data is illegal," Judge Noel said in the ruling. (...) "The fact that CSIS could go 10 years retaining large quantities of our sensitive private information, yet we're only finding out about this now, and only as a result of a court judgement, is deeply concerning," said David Christopher of OpenMedia, an advocacy group. (...)

Federal Public Safety Minister Ralph Goodale, who has overall responsibility for law enforcement agencies, welcomed the ruling and said the government would not appeal it. ***"I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service," Goodale*** said in a statement. Radio on New Zealand

*** Canadian Court Rules Spy Agency Illegally Kept Data Unrelated to Threats**
A Canadian court issued a strong rebuke to the country's intelligence agency in a ruling released Thursday, saying the Canadian Security Intelligence Service broke the law by holding on to data that wasn't directly related to security threats. Federal Court Justice Simon Noel said CSIS overstepped its mandate when it began retaining and analyzing metadata that wasn't relevant to investigations or prosecution, or to national defense or international affairs. Metadata can include information such as a telephone number or email address but doesn't include the content of a communication. The data was sent to a CSIS program called the Operational Data Analysis Centre for processing, which the court judgment said has the ability to produce "specific, intimate details" on the life and environment of individuals under investigation. The program was launched in 2006, according to the judgment. The issue of data collection has come under greater scrutiny since former U.S. National Security Agency contractor Edward Snowden revealed that agency was conducting surveillance of U.S. citizens. (...) **Canada Public Safety Minister Ralph Goodale** said in a statement that the government doesn't intend to appeal the court's decision. Wall Street Journal (2016-11-03)

*** Judge raps Canada spy agency for data collection abuse**
The head of the Canadian Security Intelligence Service said he agreed with a court ruling that the spy agency had held onto sensitive data beyond the time frame allowed by court warrants. CSIS director Michel Coulombe ordered all access to information dating back as far as 2006 to be denied while the agency assesses the legal impact of the decision and determines how best to move forward. "I regret that we did not meet our duty of candor to the court and I commit to continuing my efforts with the deputy minister of justice to address this concern," CSIS director Coulombe told a press conference. "All associated data collected under warrant was done so legally. The court's key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected," Coulombe said. (...) **Public Safety Minister Ralph Goodale**, meanwhile, welcomed the ruling, saying in a statement that ***"the court's insight and guidance are timely, coming in the midst of the public consultations we now have underway about Canada's national security framework."***
AFP (Yahoo! News) (2016-11-03)

Online national security quiz is not exactly neutral
An opinion piece state, "Making sense of the federal government's online national security quiz is not easy. The Liberal government, which during last year's election campaign had promised to scrap significant portions of the anti-terror law known as Bill C-51, now says it wants to see what Canadians have to say before acting. To that end, according to a spokesperson for **Public Safety Minister Ralph Goodale**, the government has held 27 face-to-face consultation sessions. More are in the offing. But the jewel in the crown for Justin Trudeau's very modern government is an online questionnaire. Here, the Liberal government has received 9,500 individual responses and 9,300 bulk submissions. I'm surprised it got that many. Canada's anti-terror legislation is both complicated and technical. What, for instance, is a lay person supposed to make of this question in the online quiz: "Do the current Section 38 procedures of the Canada Evidence Act properly balance fairness with security in legal proceedings?" Mind you, the online consultation does include a so-called green paper written in passably clear English that purports to describe how the current system works. But like **Goodale** himself, this green paper exudes a soothing, untroubled tone suggesting that - in the end - the law as written is pretty sensible and, at most, needs only a few tweaks." Toronto Star, A13

Aucun journaliste n'est épié par la GRC ou le SCRS, affirme Trudeau
Le premier ministre Justin Trudeau a indiqué jeudi qu'aucun journaliste ne faisait actuellement l'objet d'une surveillance de la part des services policiers ou de renseignement fédéraux. Disant suivre avec « préoccupation » les cas des reporters du Québec qui ont été espionnés par deux corps policiers de la province, il a affirmé avoir effectué des vérifications auprès de la Gendarmerie royale du Canada (GRC)

et du Service canadien du renseignement de sécurité (SCRS). « Dès qu'on a commencé à avoir ces nouvelles, j'ai commencé à communiquer avec le commissaire de la GRC et le SCRS pour m'assurer qu'effectivement, il n'y a aucune activité de ce type qui se passe au niveau fédéral », a-t-il dit en conférence de presse à Ottawa. « On a des balises, des règles et des paramètres très stricts en place, et j'ai été rassuré qu'ils sont tous en train d'être suivis, et on peut être rassurés qu'au niveau fédéral, on n'a pas cette préoccupation », a poursuivi Justin Trudeau. (…) Le chef néodémocrate Thomas Mulcair n'achète pas les réponses de Justin Trudeau, pas plus que celles fournies en Chambre par le **ministre de la Sécurité publique, Ralph Goodale**. Selon lui, les deux hommes ne disent pas explicitement qu'aucun journaliste n'est espionné. « Je vous invite à faire comme j'ai fait : d'aller lire et relire les réponses. [_] J'ai la transcription, et M. Trudeau n'a à aucun moment affirmé qu'il n'y avait aucune cause de surveillance policière en ce moment au Canada », a-t-il insisté en point de presse. Presse canadienne (Le Devoir, Le Soleil)

Advocates urge Grits to reduce number of women in prison
Sometimes when she goes to the grocery store, all Alia Pierini can do is sit in the parking lot, unable to bear the idea of going inside. She tries a different store, but Pierini, 31, often ends up coming home without the food she had planned to buy for lunch. "I feel like a big loser, to be honest, but I can't help it," the former prisoner told a news conference Thursday as she described the lingering anxiety, panic and fear she still feels as a result of months spent alone in solitary confinement. Pierini, from Chilliwack, B.C., was behind bars for 44 months after she was convicted on drug and assault charges. The last stretch of time she spent in solitary lasted a full eight months. Now a regional advocate for female prisoners in federal custody, Pierini joined the Canadian Association of Elizabeth Fry Societies, which provides support for women and girls in the justice system, in calling on the Liberal government to reduce the number of women behind bars. The association's longtime executive director, Kim Pate - newly recommended for the Senate by Prime Minister Justin Trudeau - urged the government to give judges the discretion to overturn or alter the mandatory minimum sentences brought in by the previous Conservative government. Pate also recommended making more use of sections of the Corrections and Conditional Release Act that allow federal inmates to be transferred to a provincial facility - or a hospital, such as in cases of mental illness - and for aboriginal communities to provide their own correctional services. **Public Safety Minister Ralph Goodale**, who is working with Wilson-Raybould on reviewing the inquest recommendations, has said that when it comes to administrative segregation, the government is looking at reforms that touch on everything from policy and programs to physical infrastructure and hopes to have specific proposals sometime this winter. "***We need to dramatically change the scenario, and we're working at that***," **Goodale said** last week. Canadian Press (Times & Transcript, B3, Daily Gleaner, Red Deer Advocate)

TOP STORIES / MANCHETTES

Feds hold Twitter consultation on national security
Public Safety Canada held a Twitter chat Thursday night to hear what Canadians think about national security and its responsibility to Canadians. The department in charge of the RCMP, the Canadian Security Intelligence Service and its oversight body, and the Canada Border Services Agency asked people to tweet them using the hashtag #YourNatlSec starting at 8 p.m. ET to discuss accountability in national security. (…) **Public Safety Minister Ralph Goodale** didn't participate in the Twitter chat. New Democrat justice critic Murray Rankin says he wanted as many people as possible to participate. "Any effort to get Canadians engaged is great," he said. The department is holding national security townhalls across the country until Dec. 15. It's also is accepting input on its website too. Rankin, who once served as a lawyer to the Security Intelligence Review Committee, says he'd like to see changes to C-22. The bill would set up a parliamentary committee to review spy agency activity after the fact, but no oversight during operations. **Goodale** has promised more changes to C-51 are still to come, but Rankin says he wants to know when. "It's been more than a year. I haven't seen a single comma change in C-51, which is an odious bill that deserves to be, we say, repealed," he said. CTV News (2016-11-03)

CSIS collected data on citizens for past 10 years

Canada's spies for almost a decade illegally kept and analyzed data on people who posed no threat to national security, a federal court judge has ruled. In a scathing ruling, Justice Simon Noël said the Canadian Security Intelligence Service had illegally retained an unknown amount of data on "third party" and "non-threat" individuals since 2006. CSIS fed that data into a powerful database that allowed the agency to draw out "specific, intimate insights into the lifestyle and personal choices of individuals," read the heavily censored court ruling, circulated to journalists on Thursday. (…) The revelations prompted an unprecedented snap press conference by CSIS director Michel Coulombe. Coulombe told journalists the agency believed its actions were legal, from 2006 until October's ruling, but accepts Noël's findings. Coulombe could not, however, explain why CSIS believed it needed to inform the court of ODAC's existence in 2006, but failed to do so for almost 10 years. "I'll be honest, we went through our records and we really can't find a good explanation of why the court was not informed," Coulombe told reporters Thursday evening. Coulombe was clear that CSIS believed the program was useful and effective, and said he would like to keep it in operation. "That is something I will discuss with officials, (**Public Safety Minister Ralph Goodale**) and it is a public policy decision that the government and parliamentarians will have to make," the director said. In a statement, **Goodale** said the government will not appeal Noël's decision. But the minister did leave open the possibility of changing the CSIS Act to allow for such techniques in the future. **Goodale** noted the court ruling found the legislation governing CSIS was beginning to ***"show its age"*** after 30 years, and threats and investigative techniques have changed over that time. **Goodale** said he would be discussing CSIS's failure to tell the court the full truth, however, with the agency's senior management. ***"In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the (government) are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms,"*** **Goodale** wrote. Toronto Star, A1

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Ottawa exigera l'installation d'enregistreurs dans les locomotives**

Ottawa exigera dorénavant l'installation d'enregistreurs audio-vidéo dans les locomotives, comme le recommandait le Bureau de la sécurité des transports, a annoncé jeudi le ministre fédéral des Transports. Marc Garneau a indiqué que ces appareils serviront aux enquêtes sur les accidents comme celui de Lac-Mégantic, qui a fait 47 morts à l'été de 2013. Le ministre a aussi promis que l'examen de la Loi sur la sécurité ferroviaire sera terminé en 2017 plutôt qu'en 2018, afin de renforcer plus rapidement la sécurité du réseau de chemins de fer. M. Garneau était à Montréal, jeudi matin, pour présenter sa stratégie «Transports 2030» - fruit de consultations que le nouveau ministre a menées depuis six mois. «Des accidents surviendront toujours, mais nous devons tirer des leçons de notre expérience pour tenter de les éviter à l'avenir», a-t-il lancé. Le président-directeur général de la Compagnie des chemins de fer nationaux du Canada (CN) a accueilli favorablement l'annonce concernant l'installation d'enregistreurs. Par voie de communiqué, Luc Jobin a souligné qu'il s'agit d'un «outil puissant et important» afin de comprendre les facteurs provoquant des accidents. Le Soleil, 14; Canadian Press (Times and Transcript; Whig-Standard)

*** Recording captures countdown to oil disaster**

The officer of the watch aboard the tugboat Nathan E. Stewart checked in with the Coast Guard's marine traffic centre in Prince Rupert late on the evening of Oct. 12, making a routine report of his vessel's progress through the inside passage of B.C.'s north coast as it passed Freeman Point, pushing a 100metre-long empty fuel barge. After confirming there was no other marine traffic in the area, the official with the Coast Guard's Marine Communications and Traffic Services (MCTS) concluded the radio exchange, wishing the bridge crew a "safe watch" as the articulated tug and barge headed south toward Milbanke Sound on a route through the heart of the Great Bear Rainforest. But the night ended in disaster, with the tugboat running aground and a large oil spill lapping at the shores of the rain forest. The accident occurred as the federal Liberal government was preparing to respond to British Columbia's calls for a "worldleading marine oil spill response" plan as early as Monday - and weeks ahead of a decision on the fate of Kinder Morgan's proposed oil pipeline expansion to the west coast. Audio recordings obtained by The Globe and Mail reveal how first responders struggled to get a clear picture of the unfolding

disaster, while the crew of the U.S.-based tugboat sought to manage the accident in hostile waters. Globe and Mail, S1

*** Feds to unveil coastal protection plan, face B.C. vs. Alberta choice in pipeline politics**
The Trudeau government, put on notice by its own advisory panel that it must choose between B.C.'s interests and those of Alberta when deciding whether to approve the Kinder Morgan pipeline expansion, is expected to announce a new coastal protection strategy within days. B.C. Premier Christy Clark has insisted for years that her government won't allow an oilsands pipeline project to proceed unless Ottawa meets her conditions, which include the need for a "world-leading" marine and land-spill response regime. Federal Transport Minister Marc Garneau, scheduled to be in Bella Bella Sunday to observe the impact of a recent diesel oil spill, told a Montreal audience that Ottawa is serious about protecting Canada's coasts. He said Thursday that will announce details "in coming days" of a plan to improve tanker safety and spill response regimes on Canada's coastlines. "We must and we will offer more robust environmental protections for our coastal areas and oceans," Garneau said. "Canada needs a national world-class plan to increase maritime safety and improve emergency response and strengthen partnerships with indigenous peoples and coastal communities." Postmedia News (Vancouver Sun; Vancouver Province)

*** Soil dumping to resume at Shawnigan Lake, B.C., following court ruling - Appeal court overrules previous decision by B.C. Supreme Court**
A B.C. Court of Appeal ruling has cleared the way for dumping to continue at a Vancouver Island contaminated soil facility. The decision overturns a B.C. Supreme Court ruling that previously gave the Cowichan Valley Regional District the authority to prohibit soil dumping under its local bylaws. The Shawnigan Lake soil facility is categorized as a mining activity because the operation involves filling an old quarry. The site has drawn controversy for years. Many residents say they're concerned that contaminated dirt could taint the water of Shawnigan Lake, which thousands of people in the area north of Victoria rely on for drinking water. The soil dump has received several warnings from the Ministry of Environment over water escaping the property. But the ministry has been satisfied with fixes made, allowing it to continue operating under a provincial permit. Canadian Press (CBC News) (2016-11-03)

*** Earthquake felt in Trout Brook area**
Residents in the Trout Brook area may be a bit shaken following a small earthquake Tuesday night. The 3.1-magnitude quake, while small, led to at least 30 felt reports to Earthquakes Canada. "This is about the size where you'd expect that people would have felt it close to where it originated from, so maybe 20 kilometres to 50 kilometres [away from the initial site] ... people would have felt it," said seismologist Michal Kolaj in a phone interview from Ottawa... The strength of the earthquake, a magnitude of 3.1, is not uncommon for the area, said Kolaj. In terms of historical seismicity in New Brunswick, in 1982, there was a series of earthquakes near the Miramichi area. "New Brunswick has had 5.0 magnitude to six ... historically, but these are rare events," he said. "There was the McAdam swarm [in February 2016 in the village of McAdam area], which was a series of earthquakes that occurred in [southwestern] New Brunswick. We tend to lump New Brunswick into what we call the northern Appalachian seismic zone, so it's an area where we do expect earthquakes, but of course, we're not talking about [a place] like west coast B.C., which is on the play boundary type of thing. We don't have those types of things in Eastern Canada, but we do get earthquakes." Times and Transcript, B5

*** Missing hunting guide still not found - Search to resume at daybreak today**
A search Thursday didn't yield any results for missing 49-year-old male hunting guide Randy Hilliard from Codroy Valley. The RCMP said the man was reported missing around 1:04 p.m. Monday with his last known location near Little Mica Pond, located inland on the opposite side of the highway from the Jeffrey's area in Bay St. George South. Brian Joy, co-ordinator of the Barachois Ground Search and Rescue team, said members have been on the ground since Wednesday afternoon; however, he said little searching was done due to the weather conditions in the area. He said a Royal Canadian Air Force Cormorant helicopter made its way to the area on Thursday afternoon and he and another search and rescue member went up to help out as spotters for about two hours; however low cloud cover hampered the search. "The cloud cover was so low we could only fly about 70 feet from the ground; whereas in good conditions we were told the helicopter flies at about 500 feet for visibility at a further distance," Joy said. He said in the conditions they were working in, the missing man would have to be straight belwo

them to be spotted. Joy said 16 search and rescue members were on hand, joined by members of the Stephenville-Kippens-Port au Port Search and Rescue team. Plans are to resume the search at daylight Friday and hopefully get a window for an air search. St. John's Telegram, A8

*** Waiting for the Big One**
An opinion piece states "On a recent trip to Fort McMurray, I met a woman who shared a sad but familiar story. Rewaida's family lost their home in the wildfires last May. Still shaking her head in disbelief, Rewaida told me that before the disaster, her family often donated to the Canadian Red Cross when others needed help somewhere in the world. She never expected to need that help herself. Like more than 80,000 others from the Wood Buffalo region, Rewaida and her family fled with almost nothing as flames engulfed the forests. Struck by this tragedy, Canadians from coast to coast responded like never before, so the Red Cross could help Rewaida and all those needing support. But Rewaida's story illustrates another important fact. No one wants to think disasters can happen to them or those they love. At the Red Cross, we know how often things go wrong. Every three hours, the Red Cross responds to emergencies large and small - from fires in Canadian neighbourhoods to earthquakes overseas. Too often, people tell us they weren't ready and just didn't know what to do. Now, six months since people were caught off-guard by the Alberta wildfires, the Red Cross is calling upon our nation and every Canadian to get better prepared for disaster. Although none of us wants to imagine worst-case scenarios, our experience and our mission compel us to do exactly that. And what keeps us up at night are thoughts about the 'Big One' - a catastrophic emergency hitting this country. We've already seen what earthquakes can do to industrialized nations like Japan. Our message is clear: It's time for Canadians to prepare robust, comprehensive and collaborative pre-disaster plans. It is time to invest in emergency preparedness, so that our cities, towns and small communities can protect their residents, forests, coasts and infrastructure from fires, storms, earthquakes, floods and other natural disasters." iPolitics

*** Put a price on pollution to improve people's health**
An opinion piece states "Climate change is the biggest health threat of the 21st century, according to the World Health Organization. What does it mean for Canada and how can we respond? Canada has already seen smoke-related health impacts and stressful evacuations as the result of increased wildfires; the spread of Lyme disease in New Brunswick; and food security and mental health challenges related to rapid changes in the Far North, which is two to three degrees Celsius warmer than it was in the 1950s. Climate change is no longer just a suspected diagnosis. It's a health emergency, causing systemic damage to the well-being of many around the world, including Canada. The consequences are far-reaching: climate-related drought and subsequent crop failure are exacerbating factors in the conflict in Syria, for example.. The Lancet, one of the world's most respected medical journals, reports that based on current emissions trajectories, temperature increases over the next 85 years may bring dire consequences. It says resultant sea-level rise, malnutrition, conflict and other destabilizing factors would be 'incompatible with an organized global community.'" Canadian Press (Daily Gleaner, A8)

*** Shift to renewables easy on the pocketbook - Nuclear power infrastructure is expensive to maintain - it's time for Ontario to change**
An opinion piece states "We just weathered one of the hottest summers on record in Ontario. We're not alone: Around the world, temperature records are being set and broken like it was an Olympic event. Storms get more severe, people wade through streets flooded chest-deep in water, and wildfires consume huge areas left bone-dry by 100-year droughts that now seem to be annual events. We know we can't simply ignore what climate change is doing to our planet. But we have left the problem unchecked for so long that we now need ambitious solutions that can sometimes feel out of reach. But despite the perception that change will be difficult, solutions like shifting to 100-per-cent clean renewable energy are actually well within our grasp. In fact, more than 1,000 jurisdictions around the world have already committed to going 100-per-cent renewable by 2050, including the City of Vancouver. In 2016, wind power alone provided enough energy to meet 97 per cent of Scottish household electricity needs. In Canada, the power supplied by renewable sources such as wind, solar and biomass, grew sixfold in the last decade. Progress is happening faster than we think." Hamilton Spectator, A15

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Hillary Clinton was warned in 2010 that U.S.-Canada intelligence sharing 'may be controversial for Canadians'
Huma Abedin warned Hillary Clinton in 2010 that cables from the U.S. Embassy in Ottawa could cause problems for Stephen Harper's government, emails released Thursday show. "Two cables set for release contain especially sensitive information on counterterrorism and intelligence sharing. The depth of bilateral cooperation detailed in the cables may be controversial for Canadians," said longtime Clinton-advisor Abedin. The email between Abedin and the then-U.S. Secretary of State is one of 357 released Thursday by the State Department in response to a lawsuit. More emails are scheduled for release Friday. Abedin's email was sent on Nov. 27 2010. On Nov. 29 the New York Times published a story detailing a 2008 conversation between the former head of the Canadian Security Intelligence Service Jim Judd and senior State Department counsellor Eliot Cohen. (...) One of the most significant revelations was the Canadian government's concern in 2004 that they were being locked out of the Five Eyes network as punishment for not joining the U.S.-led war in Iraq. One leaked document said the Canadian government had: "expressed concern at multiple levels that their exclusion from a traditional 'four-eyes' construct is 'punishment' for Canada's nonparticipation in Iraq and they fear that the Iraq-related channel may evolve into a more permanent 'three-eyes' only structure." The Five Eyes network is an alliance between the signals intelligence agencies of Canada, the United States, Australia, the United Kingdom and New Zealand. Signals intelligence agencies focus on monitoring people via telephone and computer instead of by relying on human agents to monitor them in person. The five countries divided the world during the Cold War with each spying on certain regions and all sharing the information they intercepted. The United States temporarily restricted Canada and New Zealand's access within the Five Eyes network following both countries reluctance to join the 2003 war in Iraq. National Post

* **Federal court ruling deems CSIS data mining actions unacceptable**
The Federal Court of Canada has handed down a ruling stating that CSIS (Canadian Security Intelligence Service) illegally stored data for over 10 years. Justice Simon Noel reportedly ruled Thursday that, since the information was collected using judicial warrants, the federal agency breached its duty to inform the court of its mechanisms. The *CBC* reports that since the information was not collected to national security threats against Canada, the data should not have been retained by CSIS. CSIS published an statement which conveys that the agency accepts the decision of the court and will take steps to respond. “The Federal Court has recently ruled on the retention of associated data linked to third party information. CSIS fully accepts the Court’s decision, and has taken immediate actions to respond. Given the Court’s decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward,” read the letter. When asked about whether Canadians would be able to rebuild their trust in the agency, chief general counsel for Justice Canada Robert Frater told the CBC that CSIS now understands its limits. Mobile Syrup (2016-11-03)

* **« Aucune activité » de surveillance par la GRC ou le SCRS, assure Trudeau**
Le directeur du SCRS ne peut confirmer que des journalistes n'ont pas été visés par des mandats de surveillance par le passé. Après le SPVM et la SQ, les journalistes ont-ils aussi été surveillés par les corps policiers fédéraux ? Après avoir vérifié auprès de la GRC et du SCRS, le premier ministre du Canada Justin Trudeau se dit « rassuré » qu'il « n'y a effectivement aucune activité » de surveillance de journalistes par les corps policiers fédéraux. Le directeur du SCRS, Michel Coulombe, n'est toutefois pas aussi affirmatif. S'il dit que « ce qui s'est passé au Québec ne se produit pas au niveau fédéral », M. Coulombe a refusé de confirmer de façon claire que des journalistes n'ont pas été visés par des mandats de surveillance du SCRS au cours des cinq dernières années. Questionné hier en conférence de presse à savoir si le Service canadien de renseignement de sécurité (SCRS) a obtenu des mandats de

surveillance sur des journalistes au cours des cinq dernières années, le directeur du SCRS Michel Coulombe a répondu « ne pas commenter sur des questions opérationnelles ». Il a servi la même réponse quand il lui a été demandé s'il avait entamé des vérifications internes cette semaine pour savoir si son organisme avait déjà surveillé des journalistes, comme l'a fait la Sûreté du Québec qui a dévoilé avoir mis six journalistes sous surveillance _ parfois durant des années. La Presse +; Times Colonist

*** Quebec to probe surveillance of media**

Quebec has announced a public inquiry into press freedom and police surveillance amid fresh disclosures that the monitoring of some journalists' cellphones lasted as long as five years and targeted an ever-growing list of reporters. On Thursday, new evidence added to growing concerns about the scope of the police spying. Three of Quebec's most respected investigative journalists said they were told by the provincial Sûreté du Québec that their phone data had been tracked from 2008 to 2013 - the very years police were unearthing and exposing corruption in Quebec's construction industry. The disclosures suggest police would have been able to access logs of calls that included those from whistle-blowers dealing with highly sensitive matters. "During this whole period - I feel sick about it - the police had their noses in our phones," Alain Gravel, an award-winning Radio-Canada journalist, said on the public broadcaster on Thursday. Two other Radio-Canada television journalists, Marie-Maude Denis and Isabelle Richer, say they too were told they were under scrutiny for five years. All three had been identified on Wednesday as part of a group of six journalists targeted for surveillance by the provincial police. Globe and Mail, A3; Montreal Gazette; Postmedia Network (Toronto Sun, Winnipeg Sun, Ottawa Sun, Edmonton Sun)

Public inquiry into spying on journalists

The normally tension filled relationship between the media and government took a strange twist this week in the National Assembly. Politicians - from the premier down - were standing up for freedom of the press and the protection of journalistic sources. Thursday's decision by the Couillard regime to go whole hog into a commission of inquiry over police spying on reporters - the same professionals who have made the Liberal government's life miserable for years by exposing corruption and ethical dalliances - will go down in history. For one thing, it's a first in Quebec, launched post-haste by a government known for notorious dithering on issues of ethics and integrity. (…) The panel is to include a representative of the media and the police and will be presided over by a judge. It will have similar powers to the Charbonneau Commission, meaning it can solicit opinions from experts, convene witnesses and hold public hearings. It was a stony-faced Premier Philippe Couillard who rose in the legislature to confirm the decision. He said the government's decision to act swiftly "illustrates the gravity of the issue." Fundamental democratic principles - freedom of the press and the independence of political, judiciary and journalistic institutions - were on the line, he said. "Public confidence is shaken," Public Security Minister Martin Coiteux told reporters earlier at the Vallée news conference. Parti Québécois Leader Jean-François Lisée, who Thursday morning had asked again that the Bureau des enquêtes indépendantes be handed the issue, welcomed the government's decision. Montreal Gazette, A1/Front; Le Devoir; National Post; Le Droit (Le Soleil)

*** Grands maux, grands remèdes**

Un éditorial rapporte, « L'« affaire Lagacé » a pris de l'ampleur. Il est normal que les mesures correctrices en prennent aussi. Plus tôt cette semaine, les Québécois ont appris que le journaliste Patrick Lagacé avait fait l'objet d'une filature électronique où tous ses appels, textos et données de géolocalisation ont été épiées pendant plusieurs mois. Seule la police de Montréal, qui avait obtenu l'approbation d'une juge de paix, était concernée. La population croyait que cette histoire inquiétante était, somme toute, assez circonscrite. Puis, comme un fil qui se détricote d'un chandail de laine, trois autres journalistes ont été ciblés : Fabrice de Pierrebourg, autrefois de La Presse, Monic Néron, du 98,5 FM, et Félix Séguin, du Journal de Montréal. Mercredi, l'histoire a pris une ampleur insoupçonnée : la Sûreté du Québec est aussi impliquée. Six autres journalistes -- Isabelle Richer, Denis Lessard, André Cédilot et Éric Thibault -- ont parfois fait l'objet de filatures bien plus larges, et sur une bien plus longue période. Dans les cas d'Alain Gravel et Marie-Mau-de Denis, qui pilotaient l'émission Enquête, sur les ondes de RadioCanada, l'espionnage téléphonique a duré cinq ans. A peu près les mêmes années au cours desquelles elle et lui déshabillaient l'industrie de la construction au Québec et fournissaient au gouvernement les raisons de créer ce qui a été la commission d'enquête Charbonneau. Qu'est-ce que ce sera demain ? La

Gendarmerie royale du Canada ? Notre corps d'espionnage, le Service canadien du renseignement de sécurité ? Le Centre de la sécurité des télécommunications ? En voilà d'autres qui n'ont peu à faire des contraintes sur les métadonnées de nos appels ! Le Droit (La Presse); Le Nouvelliste

*** Fragile est la démocratie**

Un article d'opinion note, « L'onde de choc se fait sentir à travers le Québec. La police de Montréal et la sûreté du Québec espionnent les journalistes. des collègues dont le champ d'activité est l'enquête. Que des policiers enquêteurs les perçoivent comme des compétiteurs ne devrait surprendre que les naïfs et plus largement tous ceux qui croient que la démocratie est inscrite dans les fondements mêmes de la société. (...) En ce sens, la démocratie est un idéal. La réalité démocratique est une autre affaire. La police, par définition, protège les citoyens, mais elle est aussi une institution répressive. Son éthique, sa morale ne lui appartiennent pas en pro-pre. La police doit être indépendante de la politique, mais ses pouvoirs lui sont conférés par les parlements et les Assemblées nationales. L'espionnage policier rendu public cette semaine en dit long sur le déra - page de notre démocratie. Que les policiers se soient présentés devant un juge pour obtenir les autorisations pour mettre la main sur les registres téléphoniques des journalistes ne peut leur servir d'excuse. Faute de trouver eux-mêmes les sources, ils instrumentalisent mes confrères. Et les juges qui ont accordé leur demande sans se questionner ont fait preuve d'une légèreté de jugement, ce qui pour un juge, fût-il juge de paix, est une faute professionnelle. Agence QMI (Journal de Montréal, Journal de Québec)

*** Spying an attack on freedom**

An editorial states, "you thought we are living in a country with freedom of the press you need to think again after revelations this week. A well known journalist, Patrick Lagace with La Presse, discovered Montreal police had been spying on his whereabouts using GPS on his phone, monitoring his calls and texts for an extended period this year. It is important to know Montreal police did not consider Lagace a threat to national security nor was he a threat to public safety, which may have been a reasonable argument in favour of the surveillance. Montreal police simply wanted to know which police officer had been leaking information to the press. The revelation has made international news. This sort of surveillance may be common in developing countries but not many people would have believed it would happen in Canada. The vice president of information at La Presse, Eric Trottier, told media this week "this is the kind of thing you see in Russia, or North Korea." He called the practice extremely dangerous." Medicine Hat News

*** Liberals look at more changes to foreign investment rules**

The federal government's decision to more quickly loosen rules on foreign investment in Canadian companies is a signal that the country is more open to international money and more changes are on the way, Finance Minister Bill Morneau said Thursday. He didn't detail what further changes could be coming, or what protected industries - telecommunications and cultural companies, for example - the government may open to foreign investors. Morneau said that whatever rules the government lays down on foreign investment will protect Canadians and national interests, while giving investors clarity so they can consider making investments here. "If we're able to do things that create excellent jobs for Canadians, those are things we should be doing," Morneau said in an interview with The Canadian Press. Prime Minister Justin Trudeau and other cabinet ministers have been trying to sell investors on the idea of Canada as a great investment destination and this week they loosened rules about foreign takeovers of domestic companies and foreign investment levels in airlines. The federal foreign investment law gives the government enormous powers to review takeovers or mergers involving domestic and foreign companies and block those that don't provide a net benefit to the country. Cabinet can also block deals that may raise national security issues, but the act doesn't clearly define national security. The Liberals loosened the rules for reviews of foreign investment in their fall economic update, raising the threshold for review to $1 billion from $600 million and doing so more than two years sooner than previously planned. The government also promised to publish guidelines by the end of the year to explain which investments would be subject to national security reviews. Canadian Press (Chronicle-Herald, B4)

*** Poll suggests only 9% of Canadians remember infrastructure spending as budget initiative**

When Finance Minister Bill Morneau stood up in the House of Commons Tuesday to announce he would be adding tens of billions in additional money into an already hefty infrastructure plan, he had more than

just conviction driving him. The Liberal government also had polling that suggested infrastructure spending was the most memorable part of a largely forgettable economic plan. The poll was conducted in June and the questions suggest that even then the government wanted to explore just how enthusiastic Canadians were about infrastructure spending. (…) The majority of Canadians gave a passing grade when asked whether the government was on the right track. The exception was Alberta, where there were more negative responses than positive. Under the title "management of issues," Trudeau's Liberals got the highest marks for the way they have dealt with the question of national security. CBC News

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Un transporteur reçoit sa sentence
Le jugement est tombé au dossier d'un homme de Saint-Césaire reconnu coupable d'avoir voulu importer illégalement 14,3 tonnes de tabac en vrac. Une amende de 10 000 $ et un an de prison à domicile ont récemment été imposés à Jean-François Beaulieu, 42 ans, qui possède une entreprise de transport portant son nom. M. Beaulieu avait été arrêté alors qu'il tentait de rentrer au pays par le poste frontalier de Saint-Armand/Philipsburg, un peu avant minuit le 21 novembre 2013. Son camion-remorque contenait 132 boîtes. Les agents ont remarqué qu'une forte odeur de tabac s'en dégageait. Selon l'Agence des services frontaliers du Canada (ASFC), la somme des droits et taxes éludés s'élevait à plus de 1,6 M$. «La Loi sur les douanes stipule que toutes les marchandises qui entrent au Canada doivent être déclarées», avait indiqué le directeur général régional de l'ASFC, Benoît Chiquette. «La contrebande de marchandises, les fausses déclarations et les autres infractions liées aux douanes peuvent mener à des sanctions administratives et à des poursuites judiciaires.» Voix de l'Est (La Presse)

Deportation order stayed for prisoner
A Nigerian man who was facing deportation amid a court fight to secure a $60,000 award by an Ontario judge over mistreatment during jail lockdowns has been granted a last-minute reprieve. Jamil Ogiamien, 46, was awarded the compensation in a decision in May by Superior Court Justice Douglas Gray. But the ruling is under appeal by both the federal and Ontario governments and not scheduled to be heard until February. (…)He was scheduled to be deported on Friday to Nigeria, a country he left as a child and has no memory of. Ogiamien was arrested and charged by Peel Regional Police in April 2013 for impaired driving and possession of cannabis. Although he was acquitted of the charges a year later, he continued to be held by Canada Border Services Agency for alleged immigration violations, until June 1, when the court ordered the compensation and his immediate release from detention. However, border enforcement officials arrested him again in October when he showed up in their office for his regular reporting. Toronto Star, GT6

Smugglers win new deportation hearing
Two men caught trying to bring people from the United States into Canada across the St. Lawrence River on an inflatable raft have had their deportation orders put on hold in the wake of last year's landmark Supreme Court of Canada ruling on human smuggling. (…) They found Tamazi Gechuashvili, then 59, and a citizen of Georgia, the former Soviet republic. He said he was lost, the Immigration and Refugee Board (IRB) heard. The officers searched his vehicle and discovered a patch kit for an inflatable rubber raft and a backpack containing a letter to Robert Comeau. Gechuashvili, who had applied for permanent resident status in Canada, was arrested. The crew on the other side fared no better. U.S. Border Patrol found Michael Robertson, a Canadian, with two foreign nationals, also Georgians. Robertson admitted he was trying to smuggle the two into Canada. (…) Gechuashvili and Vashakidze were deemed inadmissible to Canada on the grounds of organized criminality for international people smuggling. Both were ordered deported, but have not yet been removed. Since then, the Immigration and Refugee Protection Act changed after a court challenge. The Supreme Court reversed the interpretation of the organized criminality section last November, ruling only smugglers obtaining financial or material benefit could be considered transnational organized crime participants. Gechuashvili and Vashakidze appealed to the Federal Court for their cases to be reassessed by the IRB. Postmedia Network, N3 (Montreal Gazette, Edmonton Journal, Calgary Herald, Star Phoenix, Windsor Star, London Free Press, Leader-Post, The Province, Ottawa Citizen, National Post)

Refugee pleads guilty to theft, avoids possible deportation
A refugee from Iran who stole $3,500 in goods from a Home Depot in Waterloo could have faced deportation but caught a break in Kitchener court on Thursday. Ali Mahmoudian, 37, put several items in a garbage can at the King Street North store, closed the lid and went through self-checkout, paying for only the can. (...) He pleaded guilty on Thursday to theft under $5,000. Justice Colin Westman struck the conviction when the prosecution and defence jointly recommended a conditional discharge. A conviction may have led to deportation. Kitchener-Waterloo Record, B4

*** Monsef's critics are spreading 'misinformation,' Trudeau says**
Prime Minister Justin Trudeau says political detractors are conflating Democratic Institutions Minister Maryam Monsef's complex refugee story with that of deliberate dishonesty as questions about her birthplace linger. (...) The revelation has prompted questions about whether Ms. Monsef misrepresented her birthplace. Sun Media has reported that a file has been opened to investigate Ms. Monsef for possible citizenship fraud, although sources tell The Globe this is not the case. Mr. Trudeau was asked Thursday following a town-hall event with high-school students to mark his first year in government whether the information that Ms. Monsef was born in Iran could cause her Canadian citizenship to be revoked. The current law allows for citizenship to be revoked without a hearing if a Canadian is found to have misrepresented him or herself in their application. "This is a situation in which people are conflating, for political reasons, the very real situation that so many refugees face - of fleeing from conflict situations where there is not always perfect clarity on which side of a border one is born on, or the conditions in which one is raised, and mixing that with very deliberate acts of omission or else dishonesty in trying to gain Canadian citizenship through fraudulent declarations or attestations," Mr. Trudeau said. Globe and Mail, A6, Presse canadienne (Le Droit, Le Devoir), Canadian Press (Calgary Sun, Edmonton Sun, Toronto Sun, Winnipeg Sun, Ottawa Sun, Kingston Whig-Standard, London Free Press)

*** Mentally ill Edmonton man in deportation limbo could be sent to Montreal**
A mentally ill deportee stuck in an Edmonton jail may be sent to Quebec to get health services not available in Alberta. (...) Gelle, who fled-war-torn Somalia with his family as a child, has spent half his life and nearly his entire Canadian existence in and out of jail. Now 31, he has suffered from severe mental illness since he was 13, according to his mother, who also lives in Edmonton. He has been convicted of dozens of crimes but has remained in the remand centre after serving sentences because he is considered too dangerous to be released. Authorities hope to deport him but the Somali government has said it won't accept mentally ill people being returned to that country. At Monday's review, Sebastian Thibodeau, the hearings officer lawyer representing the government, said the goal is to stabilize Gelle so he can still be deported. (...)But Gelle's lawyer, Ruth Williams, told officials she has found no local alternative to address the severity of Gelle's condition, which requires long-term treatment so he can be stabilized. As a result, Canadian Border Services Agency officials say Gelle might have to be sent to Louis-Philippe Pinel Institute, a psychiatric facility in Montreal. CBC News

*** Bientôt plus de compagnies aériennes à bas prix**
Ottawa a ouvert la porte jeudi aux investisseurs étrangers dans le secteur aérien afin de créer des lignes à bas prix. «On veut créer plus de compétition pour augmenter le nombre de destinations et faire baisser les prix des billets d'avion pour les consommateurs», a lancé le ministre fédéral des Transports, Marc Garneau. (...)Le ministre Garneau souhaite une réorganisation. Conscient du temps d'attente «inacceptable» à l'aéroport Pierre-Elliott-Trudeau, le ministre fédéral Marc Garneau croit qu'il faut réorganiser le passage aux douanes. «Pour améliorer le contrôle de sûreté, il y a la technologie, pour les douanes, il y a la question de l'utilisation des ressources pour les heures de pointe et la possibilité d'avoir plus de guichets automatisés, tous ces facteurs seront examinés», a indiqué Marc Garneau, ministre fédéral des Transports. Rappelons que cet été, d'importantes files d'attente s'étaient créées en amont des douanes, certains passagers devant patienter jusqu'à trois heures avant d'atteindre un guichet. À l'époque, le Syndicat des Douanes et de l'Immigration avait alors déploré le manque criant d'effectifs. Bien qu'aucune décision ne soit encore prise, le ministre Garneau a confirmé se pencher présentement sur la question avec la Sécurité publique du Canada. Agence QMI (TVA Nouvelles) (2016-11-03)

*** Talent is global today. Canada needs to adapt**
An opinion piece states, "President and CEO of the Canadian Employee Relocation Council in Toronto T here is strong consensus today that the key to future economic prosperity is through knowledge-based economies. (…)Immigration is but one of several policy options available to the government to cushion the impact of a growing skills shortage and an aging population. For that reason, Immigration Minister John McCallum is on the right track in announcing increased immigration targets of 300,000 for 2017, one of the most ambitious targets in more than a century. (…) Canada must adapt to this reality and implement more flexible rules to facilitate the movement of highly skilled talent into our country, even if they're not always interested in permanent residency. Earlier this year, we conducted an employer survey on the impact of changes to the temporary foreign worker program introduced by the former Conservative government. Fifty-nine per cent reported the changes have had a negative impact on their ability to recruit skilled workers, and 16 per cent had moved work outside of Canada." Globe and Mail, B4

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

*** Microsoft to block Windows flaw used by Russian hackers**
Microsoft says it will release a patch next week to address vulnerabilities in its Windows operating system exploited by a group reportedly tied to the Russian government and linked to the theft of emails from the Democratic National Committee. The group, called Strontium by Microsoft but Fancy Bear or APT 28 by other security researchers, has been tied to Russian state-sponsored hacking. U.S. government intelligence agencies have said Russian groups were behind attempts to interfere with this year's U.S. presidential election. Strontium has targeted government agencies, diplomatic institutions, military organizations, plus defence contractors and public policy research institutes, Microsoft's executive vice-president of Windows and devices group, Terry Myerson, said in a blog post. The patch doesn't mean that Strontium or other hackers will no longer be able to launch attacks, merely that they will need to find new vulnerabilities. Fancy Bear/Strontium has a history of using security holes in software that are unknown. USA Today (Hamilton Spectator, A13; Waterloo Region Record; Toronto Star)

*** Why light bulbs may be the next hacker target**
The so-called Internet of Things, its proponents argue, offers many benefits: energy efficiency, technology so convenient it can anticipate what you want, even reduced congestion on the roads. Now here's the bad news: Putting a bunch of wirelessly connected devices in one area could prove irresistible to hackers. And it could allow them to spread malicious code through the air, like a flu virus on an airplane. Researchers reported in a paper made public on Thursday that they have uncovered a flaw in a wireless technology that is often included in smart home devices like lights, switches, locks, thermostats and many of the components of the much-ballyhooed "smart home" of the future. The researchers focused on the Philips Hue smart light bulb and found that the wireless flaw could allow hackers to take control of the light bulbs, according to researchers at the Weizmann Institute of Science near Tel Aviv and Dalhousie University in Halifax. That may not sound like a big deal. But imagine thousands or even hundreds of thousands of Internet-connected devices in proximity. Malware created by hackers could be spread like a pathogen among the devices by compromising just one of them. And they wouldn't have to have direct access to the devices to infect them: The researchers were able to spread infection in a network inside a building by driving a car 75 metres away. New York Times (Waterloo Region-Record, C10; Toronto Star)

*** How to protect yourself (and your phone) from surveillance**
Cyber security and online privacy experts aren't surprised by revelations that Quebec and Montreal police have been spying on several journalists. In fact they say journalists - and the public at large - are far too careless. When the news came out this week that police had been spying on LaPresse journalist Patrick Lagacé, it was no surprise to Geneviève Lajeunesse with Crypto Québec. "I was shocked by their shock," she said. Here are five key tips to sum up Lajeunesse's advice on protection from online surveillance, whether you're a journalist, an anonymous source, or a citizen who wants to protect your privacy. CBC News (2016-11-03)

LAW ENFORCEMENT / APPLICATION DE LA LOI

New Brunswick RCMP's first e-joints seizure earns man 2 years in prison
An Ottawa man was sent to prison on Thursday after being caught trafficking marijuana and e-joints in southeastern New Brunswick. Stephane J. André Fournier, 40, pleaded guilty in Moncton provincial court in late January to possessing marijuana, hydromorphone and cannabis resin. The prosecutor withdrew three counts of trafficking those substances. Judge Alfred Brien followed a joint recommendation on Thursday for two years in prison. Prosecutor Patrice Deschenes told the court that a Mountie pulled over a vehicle on the Trans-Canada Highway in River Glade on Oct. 7, 2015. Upon approaching the vehicle, the officer smelled fresh cannabis and further investigation resulted in the seizure of three briefcases containing 12 kilograms of marijuana, several e-joints or electronic marijuana vapour cigarettes that contained cannabis resin, along with some hydromorphone pills. He admitted to police he was transporting the illegal substances from Ottawa to Nova Scotia for re-sale. The defence told the court the offender committed the crimes out of economic necessity. "Clearly this was a bad decision on your part," said Brien. New Brunswick RCMP said after the arrest that it was their first seizure of e-joints in this province. Times & TranscriptTimes & Transcript

* **Des francophones de la GRC intentent une action collective**
Des francophones de la Gendarmerie royale du Canada veulent intenter une action collective contre leur employeur en raison de la discrimination et du harcèlement qu'ils disent subir à cause de leur langue. «Les opportunités d'avancement sont de beaucoup diminuées pour des policiers francophones, alors que dans l'autre sens, un unilingue anglophone peut accéder à un haut grade», s'insurge Paul Dupuis, un retraité de la police fédérale, à l'origine de ce recours. Cet ancien sergent d'état-major, qui a aussi été président de l'Association des membres de la police montée du Québec (AMPMQ), n'est pas tendre envers son ex-employeur. Dans la demande déposée au palais de justice de Montréal, il affirme avoir été victime «d'une campagne de harcèlement systématique» à cause de son militantisme pour ses droits linguistiques et de ses revendications pour créer un syndicat au sein de la police fédérale. «Après une campagne de harcèlement prolongée [...] M. Dupuis s'est senti de prendre sa retraite en 2016», peut-on lire dans le document de cour. Journal De Montreal; La Presse

Police seek details on suspect: RCMP-led homicide unit releases photo of 21-year-old man in hopes of gaining information from public
Homicide investigators are still trying to piece together the past of a young man who they believe drifted between Alberta and British Columbia before allegedly stabbing an Abbotsford high-school student to death in a random attack that has shocked the conservative suburb. On Thursday morning, the Lower Mainland's RCMP-led homicide unit released a photo of the 21-year-old suspect, which was captured by the security camera of a local Abbotsford business and shows the suspect just hours before he is alleged to have entered Abbotsford Senior Secondary School barefoot on Tuesday afternoon and stabbed two female students. In the photo, the slim young man wears running shoes, blue jeans, a camouflage hoodie and a backpack. Police are hoping the photo prompts more information from the public about the suspect, about whom they say they know very little. Spokeswoman StaffSergeant Jennifer Pound said the young man, who is in jail facing second-degree murder and aggravated assault charges, had no apparent connection to the community, the school or the two girls he is accused of stabbing. Globe and Mail

$100M radio network for first responders goes live
With the flip of a lever on a silver control box, a $100-million, state-of-the-art digital radio network for New Brunswick's first-responders went live on Thursday. It's called the New Brunswick trunk mobile radio project and it will allow 3,400 police, firefighters, paramedics, forest rangers, school bus drivers, and snowplow operators now - and up to 8,000 in the future - to communicate clearly, quickly, and easily. It replaces a 30-year-old system that lacked coverage in some parts of the province and didn't allow different agencies to talk to each other. (...)Larry Tremblay, RCMP assistant commissioner for J Division, said the new radio system will make communications between agencies smoother, more reliable and give wider coverage. "I can say this new system will enhance the safety of our police officers when they are out on call, as well as the safety of other first-responders assisting them," he said. "Every call we answer carries risks for all involved and this new system will help reduce that risk by ensuring better

communication." New Brunswick Fire Chiefs Association president Dan McCoy said information is one of the most important requirements when responding to a call. Daily Gleaner

Nanaimo sheriff rushed to hospital after exposure to fentanyl
The potentially lethal drug has become so rampant and led to so many fatal overdoses that the province has declared a health emergency and this incident reminds front line workers of the risk they run everyday. In the war on Fentanyl, Const. Justin Ickringill has gotten closer than any officer wants to be to the potentially lethal drug. "I was immediately light headed and dizzy," says the Nanaimo RCMP officer. "I had a racing heart and it caught me by surprise. (…)Monday a Nanaimo deputy sheriff became the latest front line worker to experience an accidental exposure to it. When conducting a gloved search of a prisoner at the RCMP detachment before transport to court she was exposed to the crystal-like substance in the pocket of a jacket being searched, and quickly became ill. "She was taken to the hospital in Nanaimo and the doctor determined that it was in fact Fentanyl that she was exposed to," says Dean Purdy of BCGEU's Corrections & Sheriff's Unit. "So from our standpoint it's a big concern for us because we would like to see some interim measures put into place so that we can try and prevent this." RCMP say fentanyl has now made its way into everything from marijuana, to cocaine and heroin. Chek News

Surveillance of reporters in Quebec to be probed: PM
As Quebec announced plans Thursday to hold an inquiry into freedom of the press and police surveillance of journalists, Prime Minister Justin Trudeau said spying on reporters is not happening at the federal level. The Quebec government said a public inquiry will be held against the backdrop of revelations that various forces monitored reporters' phones for years. A panel of experts that was announced this week will have all the powers typically granted to a commission of inquiry, including being able to compel witnesses to testify, said Justice Minister Stéphanie Vallée. "We consider it's important for the population of Quebec to trust their public institutions," she said. On Thursday, some of the reporters targeted by provincial police learned that authorities obtained years worth of phone logs. Meanwhile, the controversy reverberated in Ottawa, where Trudeau said monitoring of journalists does not take place. Trudeau told reporters he immediately contacted RCMP and CSIS leadership after news broke about the Quebec surveillance. "There is nothing of this sort happening at the federal level," he said. "We have actually very strong safeguards and protections in place to protect freedom of the press in the course of the business conducted by CSIS and the RCMP." Times Colonist; * Canoe

*** Former Mountie on trial in Moncton for impaired driving**
Arresting officer says Ronald Cleveland suggested he 'pretend that you never found me'. Former RCMP sergeant Ronald Cleveland is on trial in Moncton on a charge of impaired driving dating back to an incident in the early hours of March 21, 2014. Cleveland was released from the RCMP on a medical discharge earlier this year. Testifying Thursday, Const. Joel Arsenault described how uncomfortable he was arresting a superior officer. "Up until June 4, that was the worst day of my career," Arsenault said, referring to the day a few months later when three Codiac RCMP officers would be shot and killed by a lone gunman. Arsenault testified the RCMP had received a call about a possible drunk driver. The caller gave a license plate number that was traced back to Cleveland. Arsenault said he recognized his fellow RCMP member's name. CBC News

*** Halloween snatch and grab in Kelowna**
A cashier in Kelowna was the victim of a snatch and grab on Halloween night. Shortly before 10 p.m., Monday, Oct. 31 a man entered the Esso in the 2300 block of Highway 97 North and asked for a pack of cigarettes, according to a Central Okanagan Crime Stoppers media release. "When the clerk turned to get them, the man reached under the lottery ticket glass and grabbed a tray of $3 lottery tickets," it says. Roughly 55 tickets including Crossword, Bingo, Lucky Lines, Holiday Homes and Solitaire were stolen. The suspect is between 30 and 35 years of age with a short beard and wearing beige pants. He also had on a grey hoodie with orange writing on the front. Infotel

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

The Sun steps up again for victim: Murdered woman's brother turns to us for help in parole issue

For Chris Gill, the email was brief but exceedingly welcome. "Just a quick message to advise you that the offender in question did not go out on the scheduled ETA (escorted temporary absence) today," wrote Maurice Hebert, regional victim services manager for Corrections Canada. "I will be forwarding you a letter in the next few days to provide details in relation to our previous conversations." Score that a victory for a brother determined to ensure his sister's killer remains safely behind bars. The offender in question was Greg Ashford, who, at 23, strangled Gill's sister Faith "Faye" Russell, a University of Toronto dental school supervisor, and then went on to murder Brenda Garside, a pregnant Moncton prostitute, while he was on the run across the country in 1985. Ashford eventually surrendered and pleaded guilty to two counts of second-degree murder. Sentenced to life with no chance of parole for 20 years, he's at Dorchester Penitentiary in New Brunswick. Eligible for full release since 2005, he's always abandoned his application when Gill and his family went public with their opposition. Last year, Ashford reconsidered his request to attend four-hour Narcotics Anonymous meetings outside the prison after a Toronto Sun story questioned why the heroin addict was being allowed in the company of vulnerable women who wouldn't know of his past. Now he was angling for release again. Gill was shocked to learn a warden had the authority to overrule the security concerns of the parole board - a panel that had carefully examined Ashford's case last year and found he still posed "an above-average risk" to the community. He was consumed with rage towards women when he killed in the past and at his hearing, there were no signs that he'd changed. For now, at least, Ashford won't be out after all. "Your story had a huge impact on the warden changing her mind. It also led to Corrections Canada getting bombarded with emails. To be honest, they did not want the negative attention." Toronto Sun, A8

Un meurtrier pourra sortir de prison plus tôt
Un meurtrier emprisonné depuis 17 ans peut demander une libération conditionnelle dès maintenant s'il le désire, a tranché un jury à Longueuil. Danny Bouchard-Asselin a de quoi être heureux. Les huit femmes et quatre hommes auxquels il a raconté sa vie ces deux dernières semaines ont jugé hier qu'il pourrait s'adresser à la Commission des libérations conditionnelles plus tôt que prévu, comme il le souhaitait. Le 9 mars 2001, un premier jury avait reconnu Bouchard-Asselin coupable du meurtre prémédité de Sylvain Bélanger. Il avait alors été condamné à la prison à vie, sans possibilité de libération avant 25 ans. Puisqu'il est incarcéré depuis le 17 septembre 1999, cette échéance était prévue pour 2024. Il serait alors admissible à une libération conditionnelle totale, c'est-à-dire qu'il pourrait vivre à l'extérieur des murs du pénitencier. Ce n'est toutefois pas un automatisme, car la Commission des libérations conditionnelles du Canada (CLCC) doit évaluer le dossier. De plus, le délinquant demeurerait sous le joug des services correctionnels jusqu'à sa mort. Le meurtrier aujourd'hui âgé de 38 ans s'est prévalu de la clause de la dernière chance pour faire réduire ce délai. Un jury de Longueuil devait prendre la décision, en se basant sur le caractère du détenu, sa conduite en prison et la nature de son crime, entre autres. Après une journée de délibérations, les jurés ont décidé hier de fixer la date de son admissibilité à une libération conditionnelle totale à 20 ans, soit en 2019. Le Journal de Montréal, 18; * Journal de Chambly

*** Victim rights not protected, says Stephenville women's group about Ogden case**
The Bay St. George Status of Women Council says the death of Judy Ogden and the release of the man convicted of her murder illustrates the need to improve victim rights. Council co-chair Bernice Hancock is speaking out after Ogden's son, Daniel Benoit, talked to CBC about his fears. Benoit is concerned that his father, Dale Ogden, who served 14 years in prison before his release in September, will try to contact him. Dale Ogden's parole documents state that he had a previous conviction of assault against his first wife, in 1992. He was convicted of killing his second wife, Judy, after beating her to death in front of their son, then four-years-old, in July 1997. Hancock said she sees a theme with women in violent intimate relationships; the victim's rights are not protected. Parole Board of Canada documents state Ogden is required to disclose any relationships with women directly to the parole board. The board said he is still at a high risk of violent abusive behavior to women. CBC News

*** Rafferty judge made no mistake**
London's Superior Court Justice Thomas Heeney did an "exemplary" job handling the difficult first-degree murder trial of Michael Rafferty, Ontario ' s highest court concludes. "The trial judge made none of the errors that (Rafferty) has raised," the Ontario court of appeal states in the written reasons dismissing his appeal, released Thursday. "On the contrary, his handling of a difficult trial, was, in our view, exemplary."

The three-member court panel rejected on Oct. 24 Rafferty's appeal of his first-degree murder conviction of Victoria (Tori) Stafford, stating that written reasons would follow. Rafferty was convicted in 2012 of the kidnapping, rape and murder of eight-year-old Tori on April 8, 2009. London Free Press, A5; Toronto Sun; Canadian Press (Chronicle-Herald, National Post)

*** Pedophile loses bid to have sentence reduced**
The Nova Scotia Court of Appeal has turned down Jason Troy Pitts' appeal of his child pornography and other sex-related charges. Pitts, who pleaded guilty in October 2014 to charges of accessing and making child pornography and eight charges of conspiracy to commit sexual assault on a child, received a global sentence of seven years, but appealed his five-year sentence on the sex assault charges as "harsh and excessive." Chronicle-Herald; Cape Breton Post

*** Two-year sentence reduction for man who sexually assaulted mentally disabled daughter**
A Vernon man who was convicted of sexually assaulting his mentally disabled daughter has had his sentenced reduced by two years on appeal. The man, who can only be identified by the initials R.J.B. due to a publication ban, had attacked his daughter, identified as A.B., an average of two times a week, from November 1998 to September 2002, when A.B. was between 10 and 14 years old. B.C. Supreme Court Justice Alison Beames, who was not the trial judge, sentenced R.J.B., who had a previous conviction for sexually offending against another daughter from his first marriage, to six years in prison. On appeal, the Crown and defence agreed that Beames had erred by sentencing R. J. B on the basis that the sexual assaults involved sexual intercourse. The main issue on appeal was whether the sentence was "demonstrably unfit" and should be reduced. In a ruling released Thursday, a three-judge panel of the B.C. Court of Appeal concluded that the sentence was unfit and should be reduced to four years in prison. In his reasons for judgment, Justice John Savage said that Beames had included in her consideration an aggravating factor that was not present, in the context of an uncertain "factual matrix" in the case. Vancouver Sun

Report calls for improved inmate reintegration plans
David was in his late 50s when he first set foot inside Ottawa's detention centre, Day 1 of what would be nearly a year inside the province's jails. He quickly learned that toothpaste makes a good glue, that working in the jail kitchen has its perks like french fries and pizza, and that you never tell anyone you are sick because you'll end up in medical segregation. But his real education began the day he walked out of jail on early work release with little more than his canteen money. In a new report released Thursday, the John Howard Society said there isn't enough being done in Ontario to help reintegrate inmates back into society after they serve their sentences. According to Keast, Ontario inmates are often leaving jails or prisons without appropriate discharge plans. Every jail in Ontario has a discharge planner, but frequently inmates are receiving little to no assistance in planning for life after release, she said. The ministry of community safety and correctional services said they work with inmates to connect them with outside agencies, but participation isn't mandatory and some inmates choose not to take part. According to the report, inmates who are released often don't receive reintegration support, and they struggle to find stable housing, employment or educational opportunities. Ottawa Citizen, A1 * (Ottawa Sun); Ottawa Sun (Ottawa Citizen)

*** Increased number of inmates costing Sask. $10M more per year**
An increase in the number of inmates in Saskatchewan's jails is hitting the province in the pocket. At the end of August, the average daily count for all facilities was 1,871 - up from the 1,710 count for the year before. That means there are about 160 more inmates behind bars every day in the province compared to one year ago. With the average cost per inmate at approximately $62,000 per year, the province is having to pony up $10 million more annually. Justice Minister Gord Wyant said the number is significant enough to impact the upcoming budget. Inmates on remand make up about 60 per cent of the population in provincial jails. CBC News

*** Indiscernible: The eight-part series, ending Saturday, chronicles the demise and jailhouse death of area realtor Jamie High**
In life, Jamie High had trouble getting the attention he needed from Ontario's health care and justice systems. In death, at least, he's received a measure of official recognition in the provincial body charged

with overseeing those systems. London West New Democrat MPP Peggy Sattler rose in the Ontario legislature Thursday to make a statement about High, who died at age 40 after being found lifeless on the floor of a jail cell. High's death is the subject of an eight-part London Free Press series, called Indiscernible, online in its entirety and finishing in print on Saturday. London Free Press

*** Correctional officer at Ottawa jail sent to hospital after sucker punch by inmate**
A correctional officer at the Ottawa jail was sent to hospital Wednesday after he was sucker-punched in the face by an inmate, according to the union representing correctional officers. The union alleges the assault is a consequence of recent changes the ministry made regarding the use of disciplinary segregation. The ministry limited disciplinary segregation to 15 consecutive days and no longer allows institutions to take away privileges of offenders who are in disciplinary segregation. The union representing correctional officers is opposed to those changes, arguing it puts correctional officers at risk because inmates no longer have anything to lose. The changes were abruptly announced one day before the Ontario Human Rights Commission released a scathing report on statistics that it alleged showed the ministry's systemic overuse of segregation. The union has argued the ministry shouldn't have made the changes to disciplinary segregation without first coming up with an alternative. They also allege the real problem with segregation involves inmates who are being held in what is known as administrative segregation. The commission's report showed more than two-thirds of all segregated inmates were in segregation for administrative reasons, including because they suffered from mental health problems, asked to be there, or were deemed a threat to the safety and security of the institution. Ottawa Citizen (Ottawa Sun)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Police knew in summer about liquid fentanyl**
Police knew as far back as July that there was liquid fentanyl in Hamilton - months before they alerted the public of the presence of the deadly drug. The small vial of the potent milky liquid was seized during a raid of a central mountain home back on May 26. Police said Wednesday that it was only last week that they received results that the drug was indeed liquid fentanyl and not GHB as they had originally suspected. But Health Canada says it sent them those lab test results on July 12. Det. Const. Adam Brown in the Vice and Drug unit clarified Thursday that while the police service did indeed receive the "certificate of analysis" at that time, he wasn't made personally aware of it until last week. They're not physical documents that land on officers' desks, he says. But having recently attended a conference on fentanyl in Calgary, he made an inquiry about seizures of the drug in Hamilton - and learned of the liquid fentanyl findings. Hamilton Spectator, A1; Calgary Sun (Edmonton Sun, Winnipeg Sun); Canadian Press (Times Colonist, Red Deer Advocate)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Thunder Bay cops face probe for all missing persons cases**
Review broadened to focus on interaction with indigenous community. All indigenous missing persons and death investigations will be under the microscope of the Ontario police watchdog as it expands its "systemic review" of the Thunder Bay Police Services, looking for discriminatory conduct. The sweeping review, to be conducted by the Office of the Independent Police Review Director, was formally unveiled on Wednesday and begins immediately. The issue of police racism toward indigenous people has galvanized the country in wake of greater exposure to the issue of murdered and missing indigenous women and girls. Many indigenous families have not been satisfied with how police authorities handled their initial complaints about their loved ones, and how they followed up on them. Those concerns spill over into all aspects of the justice system and in cases of other indigenous death investigations. The incarceration of Adam Capay in segregation in a Thunder Bay cell for four years, without a trial, is a stark

reminder of human rights inequalities. The systemic review will focus on the interaction between the police and indigenous people in Thunder Bay; if indigenous people have been "over-policed" or "under-policed," and if investigations have been carried out in a discriminatory manner, said Gerry McNeilly, the Independent Police Review director. Toronto Star; CBC News

* **Missing, murdered Indigenous women cases face systemic review in Thunder Bay, Ont.**
Ontario's police watchdog says he'll share the results of his systemic review into how Thunder Bay police investigate the disappearances and deaths of Indigenous peoples with the national public inquiry into missing and murdered Indigenous women. The Ontario Independent Police Review Director, Gerry McNeilly, set the terms for his review this week after "alarming questions" were raised about how officers interact with Indigenous peoples. Rainy River First Nations Chief Jim Leonard is one of the people asking those questions. He filed the complaint that prompted the review after Thunder Bay police said the death of one of his community members was accidental. CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

* **Nepean pot shop case highlights hazy enforcement rules for police**
A knife point robbery didn't do it. Neither did a truck crashing through the store's front window. Nothing seemed to be able to shut down CannaGreen, a marijuana dispensary in a Nepean strip mall this summer, until the owner of the building slapped an eviction notice on the front of the store. But even then the bailiff hired to enforce the order said the owner of the pot shop got back into the store and kept selling. And that's when Ottawa police came on Wednesday to help the bailiff enforce the eviction and arrested a man for trespassing. Ottawa police have said they are hesitant to enforce trafficking charges against dispensaries, given the fact that they could be thrown out of court once federal legislation comes into effect. But the CannaGreen situation may provide the blueprint for how neighbourhoods and police deal with the proliferation of unregulated pot dispensaries that have popped up in the capital after the federal government signaled its intent to legalize marijuana: where the criminal laws are murky, municipal bylaws and provincial regulations can be used to shut stores down. CBC News

* **Calgary to ask Ottawa for a slice of pot pie**
When marijuana legalization hits Canada in spring 2017, Calgary hopes it gets a cut of the new tax revenue that's sure to follow. On Thursday, a council committee approved official positions that the city will present to Ottawa as the federal government begins making decisions about how pot legislation should be crafted. Those policy positions include making sure the city has control over licensing, that people are allowed to grow a limited amount of cannabis at home, and that Calgary get a slice not just of any marijuana tax, but of all sin taxes. CBC News (2016-11-03)

PUBLIC SERVICE / FONCTION PUBLIQUE

* **Federal pay system a worker's nightmare**
A letter to the editor state, "Over 30,000 workers are waiting to have their paycheques fixed, many haven't been paid in months, due to the federal government's new pay system, Phoenix. Phoenix was rolled out in February of 2015, despite being warned by the Public Service Alliance of Canada (its largest union), that the system was flawed. How many of us could miss a paycheque and still pay our bills? Imagine not being paid for months. People have lost their homes or quit to find other jobs and the stress and anxiety this has caused is unimaginable. If this was any other employer, they would have been fined and action taken against them right away. But, because it's the federal government they've been able to get away with this. We've heard from workers who are coming into work sick and cancelling their vacations because they are afraid they will be the next victims of these pay issues." Windsor Star

OTHER / AUTRE

* **Canada has more to offer in Africa than military muscle, Trudeau says**

Canada's soon-to-be-announced peace mission to Africa will attempt to tackle "root causes of conflict" because going to fight is not justification enough for deployment, says Prime Minister Justin Trudeau. "Canada has an awful lot to offer other than just stopping people from shooting at each other," Trudeau said Thursday, though he added that is "an important and one of the first things that we want to do" in any engagement. However, Trudeau said Canadians expect a "layered approach" to any United Nations mission that will "create the conditions for longer-term stability and security." Trudeau's Liberal government is weighing where to dispatch up to 600 Canadian troops and 150 police officers on an African peace mission. Trudeau told reporters that a decision is expected "in the coming weeks." Defence Minister Harjit Sajjan suggested the "peace operation" will include the goal of countering the radicalization of youth in impoverished countries. At a news conference and at an earlier town hall session with 300 high school students to mark a year since the Liberal government took power, Trudeau and Sajjan articulated some considerations in the government's looming decision. "It's not just about going out and fighting and trying to solve conflict," said Sajjan. "We need to start looking at the root cause and preventing it in the first place." That means looking at a problem "not just from a national defence perspective, it's going to be looking at a whole-of-government perspective, of having an impact for the youth that are out there," Sajjan told the students. Sajjan referred to the strikingly youthful population of most African countries, where 50-60 per cent of people are aged 24 or younger. "Instead of them being radicalized and going into other groups" Canada will aim to empower them, he said. Toronto Star, A1

*** Exclusive: Canada Paid More Than $855,000 for Will and Kate to Visit**
The Duke and Duchess of Cambridge balled out on Canada's dime when they visited their former British colony in late September, spending an estimated grand total of $855,600 on their week-long trip to BC and the Yukon, according to numbers obtained by VICE News through an access to information request. VICE News (2016-11-03)

INTERNATIONAL

NIL

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
November 10, 2016 / le 10 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

*** Latest U.S. marijuana votes could bolster Canada's legalization effort: law prof - See more at:**
Canada's effort to craft a legalized marijuana regime could be boosted by the move of four more U.S. states to approve recreational use of the drug, says a Halifax law professor. As it designs a new system, the Liberal government must address the fact Canada is a signatory to three international conventions that require criminalization of the production and possession of cannabis. (…) Currently someone convicted of simple possession of up to 30 grams of marijuana is eligible to apply for a pardon, now known as a record suspension, five years after their sentence is completed. An internal **Public Safety Canada** briefing note, released under the Access to Information Act, says the issue of record suspensions will be "important to consider during the marijuana legalization discussions." The federal task force's report ***"may include recommendations on past convictions,"*** said **Scott Bardsley, a spokesman for Public Safety Minister Ralph Goodale**. Until new legislation comes into effect, current

laws and rules remain in place, **Bardsley** added. Canadian Press (Times Colonist, CTV News, Brandon Sun)

TOP STORIES / MANCHETTES

Support grows for prison farms
Public consultations carried out by the federal government suggest there is "strong support" for reopening prison farms that were shut down across the country six years ago. The Liberal government is currently carrying out a feasibility study on penitentiary farms and is looking in particular at the possibility of reopening two in the Kingston, Ont., area. As part of that study, the Correctional Service of Canada conducted an online survey between June 2 and Aug. 4, inviting Canadians to weigh in on re-establishing the farms. The results of that consultation - which drew responses from 5,890 respondents - were released publicly on Wednesday. "There seems to be large recognition of the value of institutional agribusiness and thus, a strong support for re-establishing penitentiary farms," the consultation report released by CSC said. The CSC's consultation on the farms found that the main factors supporting reopening the farms included the need to help the rehabilitation of inmates and the positive impact the farms could have in communities. Canadian Press (Ottawa Sun; Times Colonist, Kingston Whig-Standard)

New rules for dual citizens, foreign visitors
Americans looking to move north following Donald Trump's surprise presidential victory presumably crashed the Canadian immigration website Tuesday, but agency officials could see another surge in traffic this week. Starting today, the federal government will enforce new rules intended to bring Canada's entry requirements in line with those of the U.S. Foreign nationals who don't normally need a visa to come to Canada will now have to comply with a new entry requirement, known as an electronic travel authorization (eTA). Exceptions include U.S. citizens and travellers with a valid Canadian visa. Canadian citizens, dual citizens and permanent residents don't need to apply for an eTA. But dual Canadian citizens who are in the habit of flying with their foreign passport will no longer be able to do so, starting Thursday - though the government will make some exceptions for a brief time for those whose travel plans are "imminent." Postmedia Network (Ottawa Citizen, Ottawa Sun)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

***Eleven families evacuated as flooding hits near Port Alberni, B.C.**
Wet weather is forcing evacuations on Vancouver Island and evacuation alerts in the Lower Mainland as rising waters threaten to flood homes. Eleven families have been moved from the Tseshaht First Nation on Vancouver Island as the Somass River surges over its banks in low-lying areas west of Port Alberni, B.C. An evacuation alert has also been issued for homes in Pemberton, B.C., and on the Lil'Wat First Nation, near Lillooet River. Drivers have also been warned to watch for high water levels, as creeks and rivers spill onto the road ways. Tseshaht emergency preparedness co-ordinator Hugh Braker said the state of emergency has not been lifted and the river continued to rise Wednesday. Canadian Press (CFJC Today)

***'Dismal news' for flooded First Nation**
Flood waters that have closed a section of Highway 4, which connects Port Alberni with Ucluelet and Tofino, are expected to rise and should remain for some time. After water from the Somass River threatened the highway for several days as heavy rain fell, it was fully blocked Tuesday night about three kilometres west of Port Alberni where the Tseshaht reserve is located. "The news is extremely dismal," said Hugh Braker, emergency-preparedness co-ordinator for the Tseshaht First Nation, on Wednesday. He expects the record flood levels of 2014 to be surpassed on the weekend as more storms arrive... The Ministry of Transportation has opened a detour around the closure via McCloy Lake Road, Stirling Arm Drive and Faber Road. The route will add about 10 minutes driving time to the west coast, said Janelle Erwin, the ministry's deputy regional director. Rain around Port Alberni let up Wednesday but another

storm is expected to begin tonight and extend into Friday, said Environment Canada meteorologist Matt MacDonald. Times Colonist, A6

***Une crue provoque une alerte d'évacuation à Pemberton**
En Colombie-Britannique, une alerte d'évacuation a été lancée aux résidents du village de Pemberton qui habitent dans le secteur de la route Airport en raison d'un risque de débordement d'une rivière. Le Centre de prévision des régimes fluviaux a lancé des avis de risque d'inondation pour la rivière Lillooet près de Pemberton et la rivière Squamish près de Brackendale. La Première Nation Lil'Wat a aussi alerté ses membres, selon la province. Les résidents doivent être en mesure de vite quitter le secteur, car un ordre d'évacuation peut être déclenché à tout moment. Radio Canada; AM 640; CBC News

***Flood of trouble spots**
Edmonton made history Wednesday by being the first Canadian municipality to give residents access to home-specific flood history and predictions for overland flooding. Americans are able to access a detailed home insurance claim history for any property they own through LexisNexis. But Canada has no similar program and insurance companies guard their histories for competitive advantage. On Wednesday, Edmonton was forced by Postmedia's Freedom of Information request to disclose its maps, which are not related to flooding caused by the river. Officials also added a complete set of flood reports for each upland home dating back to 1946, and outlined the sewers they expect to reach capacity in a 1-in-100-year flash flood, causing backups into basements. Those maps - with red zones in many neighbourhoods spanning several city blocks - are now publicly available at edmonton.ca/floodmitigation. Postmedia Network (Edmonton Sun, A10; Edmonton Journal); Metro News; CBC News

***Flare exercise Nov. 11 as part of survival course for sailors**
In the early afternoon of Nov. 11, an emergency flare exercise will take place on the grounds of the PEI Ground Search and Rescue Base and surrounding grounds around the Charlottetown Airport. WaveSkills Sailing School is hosting an Offshore Personal Survival at Sea course involving two types of flares and fire extinguishing exercises, as well as various water exercises offsite. The afternoon of Saturday, Nov. 12 is an alternative date for the flare exercise pending weather or an increase in airport traffic. The flare exercise is part of a two-day course offered by Wave Skills Sailing School and is aimed at preparing sailors for potential scenarios which may arise while offshore. Guardian, C8

***Spill cleanup rules hard on small firms**
New federal regulations designed to ensure that pipelines have "readily accessible" funds on hand to deal with oil or gas spills will have little impact on major pipeline projects, but could spell trouble for smaller companies, lawyers say. The rules come as several major Canadian pipeline projects are in various stages of development, including Enbridge Inc.'s Northern Gateway, Kinder Morgan's Trans Mountain Expansion and Trans-Canada Corp.'s Energy East. "I would absolutely not expect the regulations to be a deterrent to major pipeline developments, neither chilling nor boosting the risk profile significantly," says Allison Sears of Stikeman Elliott LLP in Calgary. "It is the smaller pipeline producers with lower capacity infrastructure who may struggle to meet some of these requirements." The regulations, which apply to all federally regulated interprovincial pipelines, follow the Pipeline Safety Act, which came into force in June. They are designed to ensure that pipeline companies are adequately prepared to cover response, remediation costs and liability claims if there is an unintended or uncontrolled release from their pipelines. Postmedia Network (Edmonton Journal, B10; Windsor Star)

***Hydroelectric dams spike methylmercury risk for indigenous people**
The Muskrat Falls project will cause a spike in toxic methylmercury in wild food sources that are crucial to Labrador communities, says a new Harvard University study of hydro dam effects on indigenous people. "Methylmercury concentrations in locally caught fish, birds and seals - which nearby Inuit populations use as a source of food - likely will increase up to 10-fold" in the dammed lower Churchill River, it says of Muskrat Falls. "After flooding, expected mean methylmercury concentrations in lake trout, seal, tern eggs, brook trout and char liver are all projected to be at or above the Canadian retail limit for methylmercury." Average exposure to the neurotoxin for local Inuit "is forecasted to double following flooding, and over half of the women of childbearing age and young children in the most northern community (Rigolet) are projected to exceed the U.S. Environmental Protection Agency's" guidelines, says the study. The peer-

reviewed paper was published today in the journal "Environmental Science & Technology." Canadian Press (Whitehorse Star; Telegram; Gazette; Whig Standard; Calgary Herald)

***Clark and Trudeau begin a dance**
An opinion piece states, "Here's the unofficial checklist on the call-and-response dance the federal and provincial governments are doing about marineresponse capabilities on the West Coast. The minuet will likely end with Prime Minister Justin Trudeau and Premier Christy Clark standing together with arms linked on the proposition that Canada will soon have a "world class" safety regime to deal with marine oil spills. Then two new dances will begin on the other conditions Clark has set before B.C. will sign off as full backers of the Trans Mountain pipeline expansion project. They include First Nations buy-in and a fair share of the pipeline revenue to B.C. for risks incurred..." Times-Colonist, A12

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

New rules for dual citizens, foreign visitors
Americans looking to move north following Donald Trump's surprise presidential victory presumably crashed the Canadian immigration website Tuesday, but agency officials could see another surge in traffic this week. Starting today, the federal government will enforce new rules intended to bring Canada's entry requirements in line with those of the U.S. Foreign nationals who don't normally need a visa to come to Canada will now have to comply with a new entry requirement, known as an electronic travel authorization (eTA). Exceptions include U.S. citizens and travellers with a valid Canadian visa. Canadian citizens, dual citizens and permanent residents don't need to apply for an eTA. But dual Canadian citizens who are in the habit of flying with their foreign passport will no longer be able to do so, starting Thursday - though the government will make some exceptions for a brief time for those whose travel plans are "imminent." Postmedia Network (Ottawa Citizen, Ottawa Sun)

Five ways Donald Trump could have an impact on Canada
Canada's close relationship with America has been rattled by the election of Donald Trump. Canadians are worried about how Trump's campaign promises - if fulfilled - could reverberate north of the border. Here are the key issues to watch and what Trump has said about each. Trade: Donald Trump made radically overhauling U.S. trade arrangements a key issue in his campaign, and this issue could have the greatest effect on Canada after he takes power. The president-elect campaigned on a pledge to force Canada and Mexico to renegotiate the North American Free Trade Agreement, to provide greater benefits to U.S. businesses. (...) Border: Trump vows to build a wall on the U.S.-Mexico border but rejected a wall on the border with Canada as too long, too expensive, and unnecessary. Yet it's far from clear if a Trump administration will honour deals to ensure a thinner, smoother border to the north. Canada and the U.S. have a "perimeter" approach to economic and border security that saw countless travel and security screening procedures harmonized. Bills to enable more information-sharing on entries and exits, and more pre-clearance of cross-border travellers are now before Parliament and the U.S. Congress. Canadian Ambassador David McNaughton is "quite optimistic" a lame-duck Congress will pass the necessary legislation because of bipartisan support before a new administration takes over. But the business community worries if NAFTA collapses, the flow of goods and people across the border could be choked by tariff and non-tariff regulations and/or stiffer immigration controls in the guise of security

concerns. McNaughton says he's nevertheless "open" to discussions about reopening NAFTA. Toronto Star (2016-11-09)

*** Nova Scotia woman awaits deportation to country she hasn't seen since childhood**
After finishing a two-year prison sentence for being an accessory after the fact in a 2014 homicide, Debra Spencer finds herself living in a halfway house in Sydney, N.S., because she has nowhere else to go. Except for one place: She may be deported to a country she hasn't visited since she was a child. Born in the nation of St. Vincent and the Grenadines, the 32-year-old, who has lived in Canada for two decades, was ordered deported back to the Carribean country in the fall of 2015, following her conviction. She's heard no word on when she might be sent, but fears what will happen if she is. CBC News

Feds launch bid phase for Howe bridge build
The federal government on Thursday is launching the final phase of bidding to construct the Gordie Howe International Bridge, signalling it is still committed to the project. (...) The release of a request for proposals to determine who will build the border crossing between Windsor and Detroit comes 11 months later than anticipated, and Sohi admits that will prevent it from being completed by the original target year of 2020. (...)He said an analysis was done of the risks related to expropriating properties for the project in Detroit, including a handful owned by Ambassador Bridge owner Matty Moroun, who has fought in court to stop the project. (...)When asked whether the Canadian government was interested in buying the 87-year old Ambassador Bridge from Moroun, Sohi said the government is focused on building the Howe crossing. "We are not having any (further) conversations with Mr. Moroun on this," the minister said. "We understand the importance of building this new crossing between Michigan and Windsor and we are moving forward on that." The Ambassador Bridge company declined to comment Wednesday. Postmedia Network (Windsor Star, A1)

*** Bid request issued for Gordie Howe bridge**
In a big step forward for the Gordie Howe International Bridge project, the Windsor-Detroit Bridge Authority on Thursday announced that it has issued the formal request for proposals to three teams of finalists vying to build the massive span. (...)The bridge authority, the Canadian entity charged with getting the project done, will then choose a winning team about a year from now. (...) Amarjeet Sohi, Canada's minister of infrastructure and communities, echoed that. “The Gordie Howe International Bridge is one of the most significant infrastructure projects in North America because of its vital role in maintaining and growing Canada’s most important trade relationship and closest partnership with the United States," he said. The Gordie Howe International Bridge is planned as a six-lane span that will cross the Detroit River about two miles downstream from the Ambassador Bridge. When built, it will link directly into I-75 on the Detroit side and connect via the new Herb Gray Parkway with Canadian highways. Detroit Free Press; CBC; CTV

*** Celebrating city's 'wonderful asset'**
Windsorites have been using the Herb Gray Parkway Trail for months - but now they can do it officially, with the 17-kilometre bicycling and walking route having had its formal opening ceremony. "The Parkway Trail is a continuous pathway with bridges and tunnels, allowing both pedestrians and cyclists to travel end-to-end along the parkway without ever encountering a vehicle," Ontario Minister of Transportation Steven Del Duca in Windsor on Wednesday. (...) Asked about lack of certainty surrounding construction of the Gordie Howe Bridge - the yet-to-be-built border crossing that the Herb Gray Parkway is meant to service - Del Duca said he knows the federal government has been working hard to bring the project to reality. "I'm looking forward to hearing an update, which I anticipate will be coming over the next number of days or weeks," Del Duca said. "I also know the province has worked very hard to produce the infrastructure outcome that we're standing alongside today... We'll continue to work with all of our partners." Del Duca described the Gordie Howe Bridge as the transportation option that "makes sense economically, for Ontario and for Canada, but also makes sense in terms of quality of life." Postmedia Network (Windsor Star, A3)

*** Detroit area in shellshock after Trump win**
"Right now it's still a matter of processing what happened in the United States," said Saeed Khan, who teaches history and global studies at Wayne State University. (...) Khan worries a Trump presidency will

affect the border. "There are a lot of statements president-elect Trump has made regarding immigration," Khan said. "It's more focused on the Mexican border than the Canadian border. But there's going to be a perception, particularly with Arabs and Muslims, and maybe even Hispanic people crossing the border. "There's going to be a sense of foreboding." Aaron Kall, the director of the University of Michigan debate program, wonders what Trump will do for the proposed Gordie Howe International Bridge, though he did note that the Republican president-elect has talked a lot about investing in infrastructure. But he said trade programs that affect Canada - such as NAFTA and the Trans-Pacific Partnership - could end up being scrapped, potentially affecting cross-border business. Postmedia Network (Windsor Star)

*** What's in store for Canada now?**
An opinion piece states, "A campaign marked by sexism, racism and xenophobia, by anger, resentment and fear. A country divided by gender, colour and class, by education and geography. People who voted against candidates, not for them. And a staggering win by the most unlikely and volatile candidate with seemingly few real plans. What now for our neighbour and ally? What now for Canada, living in its shadow? (...) What about the Gordie Howe International Bridge? The two countries are building it together to carry that trade across the border. Construction hasn't started. It was the Republicans who refused money for the new U.S. customs plaza. It was Republicans in Michigan who refused to spend any money on the project. Now, there's a Republican president. The party also controls Congress. Can the presidential permit be revoked? Matty Moroun, owner of the competing Ambassador Bridge, has the money, lawyers and government connections to ask that question. Postmedia Network (Windsor Star)

New Opportunities - More cargo headed to Port of Halifax
A huge consortium of shipping lines is going to be sending more container vessels to the Ceres Group's Fairview Cove Container Terminal at the Port of Halifax. (...)The exact impact of the recently-inked Canada-European Comprehensive Economic and Trade Agreement on shipping volumes to and from Europe is also still up in the air. When it is ratified, likely in mid-2017, CETA will immediately wipe out tariffs on 98 per cent of non-agricultural goods and another one per cent of those tariffs will be phased out over the next seven years. Tariffs on seafood and agricultural products will be phased out over three to seven years. Karen Oldfield, president and chief executive officer of the Halifax Port Authority, has lauded the federal government for CETA and said it will create growth opportunities for Nova Scotia and Atlantic Canadian exports to Europe. Halifax Chronicle Herald, B1

*** Canadian spy agency concealed mass data intelligence-bank from courts**
An opinion piece states, "In a damning ruling issued last Thursday, Federal Court Judge Simon Noel sharply criticized the Canadian Security Intelligence Service (CSIS), the country's premier spy agency, for concealing the existence of a mass data collection program for over a decade. (...)Coulombe added that all access to the illegally collected data has been halted. Significantly, however, the store of metadata has not been destroyed, but continues to be expanded because CSIS has other means of increasing its volume. Provisions in Bill C-51, passed by the Harper Conservatives with the support of the Liberals in 2015, mean that CSIS can collect data from 17 government departments without a warrant, including the Canada Revenue Agency, the border service and CSE. As Noel noted, this meant CSIS now has free access to such information as Canadians' tax returns." World Socialist Website

*** Les producteurs gardés en otage par le gouvernement fédéral**
Selon le député néo-démocrate, le secteur agricole, qui constitue 12 % de l'économie du Bas-Saint-Laurent, a raison d'être déçu du gouvernement Trudeau, car les producteurs laitiers et fromagers sont toujours dans l'incertitude quant aux compensations promises en lien avec l'accord commercial avec l'Europe. « Les Libéraux ont suggéré la semaine dernière qu'il y aurait compensation, mais rien n'a été annoncé officiellement. Les Conservateurs avaient, quant à eux, promis 4,3 milliards de $ pour le secteur », se souvient Guy Caron. La question du lait diafiltré n'est toujours pas réglée et le député fédéral estime que la solution pour régler le problème est pourtant simple : « En uniformisant la définition du lait diafiltré utilisée par l'Agence des services frontaliers du Canada et celle utilisée par l'Agence canadienne d'inspection des aliments, le problème serait réglé demain matin. » L'Agence des services frontaliers du Canada considère ce lait transformé comme une protéine, et non du lait, lui permettant d'entrer au pays en contournant les quotas de la gestion de l'offre, explique le député. Et l'Agence canadienne

d'inspection des aliments considère quant à elle qu'il s'agit bien de lait et qu'il peut donc être utilisé dans la production de fromage et de yogourt. L'Avantage (201-11-09)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

***City organization reeling from malicious cyber attack**
U.S. presidential candidate Hillary Clinton isn't the only one upset about Russian cyber attacks these days. A Sarnia-based cultural organization was victimized this summer by hackers who seized its computer system and demanded a ransom to unlock the files and data. A director with the non-profit agency, which The Journal has agreed not to name, opened a computer file in July and discovered names and numbers had been replaced with bizarre-looking digits. She opened an older version of the same document from a year earlier and found the same thing. An on-screen pop-up announced: "This file has been converted to a Zepto file." She called an IT professional and learned the organization was in trouble. "The bottom line was that we were totally encrypted," the director said. The computer was infected with a type of malicious software called ransomware, which encrypts sensitive data until it can only be unlocked with a keycode. The hackers demanded $2,000 in bitcoins, an online currency that's nearly impossible to trace. When the director contacted law enforcement she was in for another surprise. Sarnia Police, the OPP and the RCMP all said they couldn't help. Sarnia Journal

***Major cloud is infested with malware, researchers say**
Cloud repositories are actively supplying malware, according to computer experts. And problematically, it's insidious and hard to find. Hundreds of buckets have been undermined, says Xiaojing Liao, a graduate student at Georgia Tech who's the lead author on a study that's looking into the problem. Buckets are chunks of storage used in cloud operations… The recent "study of cloud hosting services has found that as many as 10 percent of the repositories hosted by them have been compromised," the article continues. The "bad repositories," called "Bars," were found on "leading cloud platforms like Amazon and Google" the paper says (PDF). Those major cloud services are often thought of as being highly secure because of their use of encryption and large numbers of staff dedicated to security. Network World

***Android banking malware attacks more than 300,000 devices in two months**
A newly-discovered Android banking malware has been found exploiting a flaw in Google's Chrome browser, allowing hackers to infect more than 300,000 devices in just two months. The Trojan, known as Svpeng, had been infecting as many as 37,000 victims per day until it was uncovered by Kaspersky Labs and patched out by Google. The malware campaign originally began by implanting a malicious piece of adware code into Google AdSense. The malware also disguised itself as an important browser update or a popular app, too, to ensure that victims download it. Once downloaded, the malware resorts to social engineering to make sure that it gets installed, telling victims to enable third-party installations due to the "urgency" of the update it is purporting to be. The creators are only targeting Russian-speaking users at this time, though Kaspersky warns that they may shift focus. IBS Intelligence

***Google Slaps Malware Sites With Punishments Similar To Giving Kids Time-Out**
Google is upping the ante when it comes to dealing with websites that have malicious content by branding them with a "Repeat Offender" label. This is the search engine company's way of telling users that these websites have been known to infect computers with malware or phish for personal information in the past. It's also a way for Google to do something about malware without completely removing the sites from its indexing list. Google has been warning users against potentially harmful sites through their Google Chrome browser for years, Tech Crunch reports. When a user visits a site that Google believes carries some harmful code, Chrome will take the user to a warning page before allowing them to proceed. If the user's computer gets infected because they chose to ignore the warning, at least Google did its part. Eventually, however, these sites figured out a way to get around the filter by playing nice for a little while until Google forgave them. Once the websites are back in the search engine company's good graces, the warning page would be removed. At that time, they'll resume their illicit activities as before. Well, it seems Google has had enough and has announced that any website caught infecting users with malware repeatedly will be cut off once again. The sites won't be able to request for re-verification for 30 days, which is good news for users. Unfortunately, once the 30 days are up, these websites can do what

they did before and play the innocent online entities that learned their lesson card. The month-long delay might be inconvenient, but there still ways around it that enterprising ne'er do wells can take advantage of. Econo Times

LAW ENFORCEMENT / APPLICATION DE LA LOI

*** Jury finds python owner not guilty in deaths of New Brunswick boys**

A jury has found a New Brunswick man not guilty of criminal negligence causing death after his African rock python escaped its enclosure and killed two young boys three years ago. Four-year-old Noah Barthe and Connor Barthe, 6, died during a sleepover in Jean-Claude Savoie's apartment in August 2013. (…) Matchim said an investigation by the RCMP and two subsequent reviews concluded that charges were not appropriate. He said he received that assurance in writing. The lawyer said a new lead investigator was then appointed and suddenly is client found himself facing a charge. (…)He responded to the earlier testimony of RCMP officers about the python's aggressive behaviour after it was captured - hissing and lunging at the glass of the enclosure. "A snake that responds like that is a very aggressive snake," he said. "It was an extreme response to human presence. This animal was dangerous." Truro Daily

Nanaimo city council calls for RCMP to investigate Mayor

If there was still any hope of Nanaimo council healing from their very public fractures, this new scandal will end that. "Well this is a really strange situation obviously and a situation that is really complex," says Coun. Bill McKay. As city council openly calls for RCMP to investigate Nanaimo Mayor Bill McKay for alleged corruption. "When you hide something everyone assumes its corruption and that's the allegation," says Coun. Jerry Hong. "Until he comes forward and presents it and shows it otherwise that's what the allegations are." It's the latest in a saga of dysfunctional chapters in this council's story that was seen publicly for the first time last March, when 7 city councillors signed a letter calling for McKay's resignation "You know the public asked why we did it. These are some of the things why," says Hong. Chek

Four cattle dead after chased by four-by-four

Okotoks RCMP are looking for help to catch individuals responsible for the death of four cattle after they were chased by a vehicle on a rural property in the DeWinton area. Sometime on Oct. 7 someone opened the gate to a property west of Macleod Trail where the animals were grazing. The suspects drove a four-by-four vehicle onto the ranch land and used it to chase cattle for an unknown length of time."It looked like someone had come in and chased them," said Heather Mills, who owned the animals with her family. "From what we could see it looked like they had brought them up the fence line where we had a catch pen. I don't know if they were trying to steal them or if it was a cruel joke." She said they want people to be aware and watchful for anything suspicious. Mills said the loss of four animals will impact their farm. The cattle were insured, but they are working to see how much they will receive. "This is livelihood and it affects everyone in the long run if people are injuring animals," she said. "There isn't a large margin at the end of the day for what farmers get off their cattle." Mills said she and her husband received a phone call from someone living on a neighbouring property that there was a dead cow. They were in Calgary at the time and received a second call soon after about a second animal. Upon arriving, Mills she said they counted their herd and realized another was missing. After euthanizing another, in total four animals were dead. Western Wheel

Court told of cop's data hunt

Repeated bids to access police data that was allegedly sold by a city cop were described in court Wednesday by another officer. Staff Sgt. Jasbir Kainth told court he zeroed in on five days between March 10 and July 5, 2010 in which Det. Gerard Brand allegedly dug up information on people sought by a lending company trying to track down deadbeat debtors. He was paid $2,300 by the lending firm, contends Edmonton-based Crown lawyer Leah Boyd. "Were there any entries queried by Mr. Brand on that date?" asked Boyd, referring to June 16, 2010. (…) Kainth said he also sought out Brand's access record to the RCMP computer database shared with city police. "I asked for an audit of Brand's CPIC queries," he said, referring to the system known as the Canadian Police Information Centre. Two computers were seized from Brand's home along with other records to be analyzed. He's also accused of

providing information on four people obtained through his employment for a friend. Calgary Sun, A18 (Calgary Herald)

Surrey mayor wants three tiers for RCMP auxiliary policing program
Surrey Mayor Linda Hepner said the city favours the third of three options governing the future of the RCMP's Auxiliary Constable Program. This option, which Hepner said is also the favoured choice of the Union of B.C. Municipalities, presents a three-tiered system which she says "allows us the broadest range of services." "I think it's a better option for both the city and the volunteers," Hepner told the Now. "It may very well take them into a career of law enforcement." The three options the RCMP is considering include settling with the status quo, setting up a community corps programs, or adopting a three-tiered program that would incorporate both options one and two. In January Surrey's roughly 80 volunteer cops – the largest contingent of roughly 1,500 auxiliaries across Canada – learned from RCMP headquarters in Ottawa that they would no longer be able to ride with Mounties, receive firearms familiarization training, and that their uniforms will be changed to better distinguish them from regular officers. Now Newspaper

* **Nipawin RCMP issue Amber Alert for 7-year-old Sask. girl believed to be taken by father**
Nipawin RCMP have activated an Amber Alert for seven-year-old Nia Eastman believed to have been taken by her father Adam Jay Eastman, 45, Wednesday night. RCMP said Nia was to be returned home to her mother by 7:00 p.m. A vehicle believed to be operated by her father was located on a rural property east of Smeaton, Sask., near Snowden around 10:00 p.m. Neither Nia nor Adam were found with the vehicle. Officers are searching the vicinity. Police have described Nia as 3'9" with shoulder-length blonde hair. She was last seen wearing pink eyeglasses, purple long-sleeved shirt with butterflies, pink skirt and purple leggings with silver trim at the bottom. 650 CKOM; Global News; Toronto Star; CBC News

Pot dispensary owner charged with trafficking after two raids in Whitewood
A marijuana dispensary owner has been charged with a range of offences after Broadview RCMP conducted two raids in Whitewood, about 175 km east of Regina, on Tuesday. An RCMP brief said that marijuana and property, including cellphones, computers, cash and three vehicles, were all seized during raids on a business - not named by RCMP but known to be Martin Medical Services on the 600 block of 3rd Ave. in Whitewood - and a private residence. Jerry Matthew Martin, 45, is charged with offences relating to the "operation of an unlawful marijuana dispensary," RCMP said. These include the trafficking and possession of marijuana and cannabis resin, possession of the proceeds of crime, trafficking in the proceeds of crime and laundering the proceeds of crime. After an appearance at provincial court in Broadview on Wednesday, Martin was released to reappear on Nov. 23. Martin and his lawyer, the Vancouver-based medical marijuana advocate Kirk Tousaw, could not be reached for comment. Star Phoenix, A7 (Leader-Post)

* **First Nations police service recommends its own disbanding at suicide inquest**
The suicide of a First Nations woman in the back of a police truck is causing Canada's largest Indigenous police service to do some soul searching. The Nishnawbe Aski Police Service, which covers 34 First Nations in northern Ontario, told an inquest into Lena Anderson's death that it has neither the resources nor the legal foundation to do its job properly. So it took the drastic step on Wednesday of asking the jury at the inquest to recommend the police force be disbanded if Ontario does not bring it under the province's Police Services Act by March 31, 2017. "Enough is enough," said Nishnawbe Aski Police Service (NAPS) board chair Mike Metatawabin. "We can't do this all the time where you promise something and then turn around and say you can't do it." Ontario's Ministry of Community Safety and Correctional Services says it plans to introduce legislation in the spring that will "modernize" the Police Services Act and that it is consulting with First Nations on "exploring a legislative framework for First Nations policing." CBC News

* **Two men facing charges in kidnapping in mountain resort town of Jasper, Alta.**
RCMP say two men have been charged after an armed kidnapping in Jasper Alta., on Saturday. Mounties say the complainant has taken into a vehicle by two males armed with firearms, but managed to jump out of the moving vehicle and ran into a nearby business for help. He was taken to hospital and treated for non-life threatening injuries. A few hours later, RCMP in nearby Hinton conducted a high-risk traffic stop and took one male into custody while another man turned himself in at the local detachment two days

later. Otto Richard Latimer, 21, and Nathan Rodney Shevalier, 29, are charged with forcible confinement, uttering threats to cause death, possession of a weapon for a dangerous purpose and theft under $5000, along with additional charges for Shevalier. Lethbridge Herald

Zero tolerance for job horrors
An opinion piece states, "'To all the women who have been impacted by the force's failure to have protected your experience at work, and on behalf of every leader, supervisor or manager, every commissioner: I stand humbly before you today and solemnly offer our sincere apology." Those words, uttered by RCMP Commissioner Bob Paulson on Oct. 6, put on the public record what far too many female Mounties already knew for decades to be true: They were victims of workplace sexual harassment and abuse, some to such a degree careers were cut short and personal lives were ruined. The apology and accompanying multi-million-dollar financial settlement was preceded by separate class action lawsuits filed by two former RCMP officers, representing hundreds of women. Linda Davidson said she was sexually harassed by a male supervisor, when she was a young officer. Her legal claim stated she continued to face such attitudes as she rose through the ranks to become an inspector. Janet Merlo said she had to deal with sexist attitudes while on the force, even to the point of a manager asking why she didn't "keep her f---legs closed" when he learned she was pregnant. Both reported having to put up with sexual innuendos, comments and pranks. But both also said they blamed a minority of former colleagues for fostering such a toxic work environment. As the national police force took its first steps toward closure, a similar issue would come to light in Calgary." Winnipeg Sun

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Support grows for prison farms
Public consultations carried out by the federal government suggest there is "strong support" for reopening prison farms that were shut down across the country six years ago. The Liberal government is currently carrying out a feasibility study on penitentiary farms and is looking in particular at the possibility of reopening two in the Kingston, Ont., area. As part of that study, the Correctional Service of Canada conducted an online survey between June 2 and Aug. 4, inviting Canadians to weigh in on re-establishing the farms. The results of that consultation - which drew responses from 5,890 respondents - were released publicly on Wednesday. "There seems to be large recognition of the value of institutional agribusiness and thus, a strong support for re-establishing penitentiary farms," the consultation report released by CSC said. The CSC's consultation on the farms found that the main factors supporting reopening the farms included the need to help the rehabilitation of inmates and the positive impact the farms could have in communities. Canadian Press (Ottawa Sun; Times Colonist, Kingston Whig-Standard)

* **Prisoner segregation puts us all at risk: advocate**
A prisoner advocate is speaking out against prolonged segregation, after three prisoners filed a lawsuit claiming they were isolated for more than six weeks at Edmonton Institution, a maximum security facility. "Human contact is natural and it's an absolute must for human beings," said Chris Hay, executive director of the John Howard Society of Alberta. He noted isolation can lead to despair, health problems, suicidal thoughts and sometimes irreversible mental issues. In a statement of claim for their $5.6-million lawsuit against the Attorney General of Canada, Matthew Christopher Hamm, 37, Taylor Tobin, 19, and Shawn Keepness, 31, say they were forced to stay in segregation for 43 consecutive days under suspicion that they were conspiring to assault correctional officers. The Corrections and Conditional Release Act states an inmate can be kept in segregation for a maximum of 30 days for breaking an institution's rules, while UN guidelines say no one should be segregated for more than 15 days. Hay has also spoken out against increased charges for prisoners to make phone calls, which he said plays into the same issue – further removing prisoners from the outside world makes them less able to reintegrate. That, he said, means more danger for guards on the inside and society on the outside. He applauded apprenticeship programs that kept prisoners working from the inside, though those have been disappearing. According to Correctional Services Canada, 26 prisoners at Edmonton Institution were actively in segregation on Oct. 9. "All institutions adhere to legislation and policy surrounding

administrative segregation, and ensure that all viable alternatives to placement in administrative segregation are explored," spokesperson Lori Halfper said in an e-mail. Metro News (2016-11-08)

*** No way to prevent inmate suicides, inquest judge says**
Nothing can be done to stop prison inmates "bent on taking their own life," a Manitoba provincial court judge says in an inquest decision released Wednesday. Gilbert Moise, 21, committed suicide on April 7, 2013, about midway through a five-year sentence at Stony Mountain Institution. "Sadly, events such as this are not uncommon, and many inquests into similar situations have been held," Judge Dale Harvey wrote in the 10-page decision. Harvey did not make any recommendations for changes in prison policies or procedures to prevent similar deaths in the future. The inquest, mandatory when an inmate dies in custody, was called by the province's chief medical examiner in December 2013 and conducted in May of this year. The inquest was told Moise was seen by a psychiatrist two days before his death and said he wasn't thinking of causing harm to himself or committing suicide. Moise was last seen by a guard about an hour before his death sitting on his bed in his cell with the television off. Winnipeg Free Press, 11

Court rejects killer's 'suicide pact' argument
When Thomas Elton and Brenda Turcan married in 2005, both were convicted killers. Then Elton strangled and stabbed his chronically ill wife in June 2009. He was later convicted of second-degree murder, despite explaining that the couple had a suicide pact and that he only killed Turcan because he thought she had overdosed in an attempt to die that day. In 2012, a trial judge accepted that Elton believed he was committing a mercy killing, but ruled that he was still guilty of murder because the evidence showed his wife died by his hand and had not overdosed. In 2014, Elton was sentenced to life in prison with no parole eligibility for 25 years. He appealed the verdict, arguing that the trial judge erred by not fully considering whether "he aided the victim's suicide or committed her murder." On Wednesday, the B.C. Court of Appeal dismissed Elton's appeal and upheld his murder conviction. Elton's appeal was heard last March, four months after the two-time killer was found dead in his jail cell at Matsqui Institution in Abbotsford. The B.C. Coroners Service is still investigating his death, the coroner said Wednesday. The Province, A12 (Vancouver Sun)

Man convicted of murdering future brother-in-law deserves re-trial, lawyer tells appeals court
Questionable evidence from a "Mr. Big" sting operation should garner a convicted killer a new trial, an appeal panel heard Wednesday. Some of the claims Neil Lee Yakimchuk made to an undercover police officer following the Dec. 15, 2008, murder of Juan Carlos Dequina are dubious and should be subject to further court examination, lawyer Alias Sanders told the Alberta Court of Appeal. Yakimchuk was convicted in April 2014 of first-degree murder in the shooting death of his brother-in-law-to-be Dequina, who was lured to a remote road on the Tsuut'ina First Nation and shot in the back of the head. When Yakimchuk was convicted and sentenced to life in prison without parole eligibility, Justice Earl Wilson slammed him for his deceitful testimony, saying "this is a stone-cold killing." The appeal panel will render its decision at a later date and Yakimchuk remains in custody. Calgary Herald

*** Kidnapper handed 12-year term**
An Edmonton criminal convicted of the thumb-chopping abduction of a man who drove into a restaurant patio and killed a young boy was handed a 12-year prison term Wednesday. Steven (Diamond) Vollrath, 33, was earlier convicted of kidnapping, aggravated assault, impersonating police and possession of a dangerous weapon in connection with the Jan. 22, 2015, abduction of Richard Suter, 65, from his Riverbend home. Provincial court Judge Elizabeth Johnson noted the violent offence was "planned and deliberate" and motivated by a "heinous" reason, that being "to extract vengeance by inflicting serious harm." Suter was sentenced to four months in jail on Dec. 17, 2015, after earlier pleading guilty to refusing to provide a breath sample where a death ensued. However, the Court of Appeal of Alberta later called the sentence "unfit" and increased it to 26 months. He was also banned from driving for 30 months. Edmonton Journal, A7 (Calgary Sun, Toronto Sun, Edmonton Sun, StarPhoenix)

*** Low on staff, jail couldn't help High, inquest told**
No one could help Jamie High in the final moments he lay dying on the floor of a segregation cell at London's provincial jail because there weren't enough correctional officers in the unit, an inquest into his death heard. A shortage of nurses also prevented a mental-health specialist from doing what he wanted

to help the St. Thomas realtor, the inquest heard Wednesday. Understaffing – along with overcrowding - have often been cited in recent years as contributors to problems at the Elgin-Middlesex Detention Centre (EMDC), a frequent flashpoint for troubles in Ontario ' s correctional system. London Free Press, A1

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** 20% of Ontario drug-benefit recipients on prescription opioids**
More than 20 per cent of adults on Ontario's publicly-funded drug benefit plan are taking doctor-prescribed opioids, swelling to nearly 30 per cent in some parts of the province, says a new study to be released on Thursday. The study tracks the use of such painkillers as oxycodone and fentanyl in Ontario. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

*** Calls for justice, communication, and cultural display at Amnesty Forum**
While it wasn't a full house, the audience was engaged at Amnesty International's public forum in Fort St. John on Friday, Nov. 4. The forum acted as a venue to discuss the findings of Amnesty's report Out of Sight, Out Of Mind: Gender, Indigenous Rights, and Energy Development in Northeast B.C., and had five panelists on stage as voices for various aspects of the report. (…) Calls for justice for missing and murdered indigenous people were also raised. Inspector Mike Kurvers, detachment commander for the Fort St. John RCMP, spoke about the role of police in the community, particularly in dealing with the shadow population of transient workers who come through the area to work in the oil patch. "We are aware of it, we understand it, but from a police perspective it hasn't impacted the detachment to date. We still get the same number of calls and … treat each call on its own merits," Kurvers said. Alaska Highway News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

*** Tuesday's vote saw more U.S. states legalize pot: Why Canada could benefit**
There could be an upside for Canada now that several U.S. states have decided to legalize marijuana, according to one of the architects of Canada's pot policy. On Tuesday night while Americans were electing Donald J. Trump as their next president, several states also had ballot questions about whether to legalize pot for recreational use. California, Nevada and Massachusetts all said yes. All three states plan to have possession of small quantities of marijuana legalized by Jan. 1, 2017. That means by early next year, more than one in five Americans will live in a state where marijuana is legal for adult use. So what does it mean for Canada? Bill Blair, parliamentary secretary to the minister of justice and former Toronto police chief, told CBC News he sees a couple of benefits. "I think we will have an opportunity to learn from them and I think there's also some encouraging signs that they'll be more investment in research and more information about how this can be safely and healthfully regulated," said Blair. Canadian officials have already taken a look at how legalization has worked in Colorado and Washington state as the Trudeau government prepares to table its own legislation in spring of 2017. Oregon, Alaska and Washington, D.C., have also already legalized the drug. With 97 per cent of the vote in, Maine voters were separated by less than a percentage point, leaning towards legalization. California's move is significant because it's the most populous U.S. state, clocking in at around 39 million people. CBC News

*** No sale for medical marijuana business in St. John's**
The owner of Health Cannabis on Water Street in St. John's says he has been put on notice by the Royal Newfoundland Constabulary: sell marijuana and risk criminal charges. The warning comes despite the federal government's promise of new legislation to come in spring 2017 - expected to legalize the

business of marijuana and possession for more than just medical use. "They called my landlord a couple of days ago," said David Ferkul, who spoke with The Telegram Wednesday afternoon. "Then he gave us a number. I phoned them back. They waited a couple of days and I finally got the call today." He said the caution was also delivered in writing. A business for patients: Ferkul said Health Cannabis is a "members only" spot, with membership being limited to medical marijuana licence holders. The location is only open on weekends and potentially some other, unusual hours. "The new federal law states that you have to receive your (prescription) marijuana through mail order from one of the 36 licenced producers," he said, referring to a list of producers licenced by Health Canada (the list is available on the regulator's website). Telegram, A5

*** B.C. pot grower seeing green as more states legalize marijuana**
As California, Nevada, Maine and Massachusetts appear set to join the growing list of states that have legalized recreational pot, one of B.C.'s biggest medical marijuana producers is seeing big opportunities in the American market. After several successful ballot initiatives south of the border this week, B.C. will soon be the only West Coast jurisdiction between the Bering Sea and Tijuana where toking up is still restricted to medical use. But the people behind Tilray, the federally licensed cannabis production facility on Vancouver Island, aren't concerned about losing their edge to rivals south of the border when Canada eventually legalizes pot. "I think Canadian companies have a huge advantage based on the very tight regulatory framework that exists in the medical cannabis program in Canada," Tilray president Brendan Kennedy said Wednesday. That tight framework may have squeezed out many entrepreneurs interested in jumping into the legal medical marijuana business, but the lack of competition has allowed licensed producers like Tilray to grow quite large. Vancouver Sun, A5

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

*** Plenty of questions on peacekeeping**
An opinion piece state, "Last week the Star ran a series of articles on Canada's peacemaking options in Africa and quoted both Justin Trudeau and Romeo Dallaire as saying that these missions must offer more than military might. Yet there were no specifics about non-military options. Similarly, the government's recent cross-country public consultations on defence policy and cyber security only focused on militarized options. What can be made of Canadian peacekeeping when Canada increases its direct military involvement in Iraq and in the NATO exercises up to the Russian border, as Canada is now No. 6 in worldwide arms sales ($15 billion sales to Saudi Arabia), with the Trudeau government further watering down of weapons export regulations? How can the public evaluate peacekeeping when they are not informed that Canada just voted against the UN Open Ended Working Group resolution to eliminate nuclear weapons?" Toronto Star

INTERNATIONAL

*** One injured after grenade attack outside French embassy in Athens**
A hand grenade attack outside the French Embassy in central Athens slightly wounded a policeman early Thursday, police said, days before outgoing U.S. President Barack Obama is due to visit the Greek capital. Authorities said the policeman, who had been on guard outside the embassy, was wounded when unknown assailants threw a hand grenade outside the embassy building, located opposite Parliament on a major avenue. Police shut down the area to vehicles and pedestrians for several hours while anti-terrorism forensics experts combed the scene for evidence. The government condemned the attack and described it as an act of terrorism, adding that the police would track down the culprits. "The relations of friendship and solidarity between Greece and France can't be affected in the slightest by such terrorist

acts," government spokesman Dimitris Tzanakopoulos said in a statement released by his office. Associated Press (CTV News); Agence France-Presse (Digital Journal)

*** Pakistan wants to work on counter-terrorism with Trump**
Pakistani foreign affairs adviser Sartaj Aziz says his country would like to work with U.S. President-elect Donald Trump on the common interest of combatting terrorism. In an interview with Pakistan's Geo News channel Thursday, he says that helping negotiate a political settlement in Afghanistan is another area where the two countries could work together. The U.S. president-elect has publicly criticized Pakistan in the past for battling some Islamic militant groups while tolerating others. Associated Press (Metro News)

*** Chinese official named head of Interpol, drawing criticism**
A top Chinese police official was elected president of Interpol on Thursday, setting off alarm bells among rights advocates over abuses and a lack of transparency within China's legal system, as well as the potential misuse of the police organization to attack Beijing's political opponents.Vice Public Security Minister Meng Hongwei was named as the first Chinese to hold the post at the organization's general assembly on the Indonesian island of Bali, Interpol announced in a press release.The Lyon, France-based International Criminal Police Organization has 190 member nations and has the power to issue "red notices." It's the closest instrument to an international arrest warrant in use today. Interpol circulates those notices to member countries listing people who are wanted for extradition.While Interpol's charter officially bars it from undertaking "any intervention or activities of a political, military, religious or racial character," critics say some governments, primarily Russia and Iran, have abused the system to harass and detain opponents of their regimes. Interpol says it has a special vetting process to prevent that from happening. Associated Press (Times Colonist)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
February 20, 2016 / le 20 février 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

***'Unacceptable toxicity' at the RCMP needs to be cleaned up, says Ralph Goodale**
Canada's public safety minister says the latest allegations of harassment and bullying have made the RCMP ***"an embarrassment." "This is the national police force, this is an icon of the nation and it's got to be remedied very quickly to Canadian satisfaction. Canadians will not tolerate any half measures in the response here,"*** **Ralph Goodale** said in an interview with host Chris Hall on CBC Radio's The House. The strong condemnation comes after CBC News reported allegations of unwanted sexual touching, bullying and rampant nudity in the workplace at the explosives training unit of the Canadian Police College in Ottawa. ***"It's an embarrassment, and I think [RCMP Commissioner Bob Paulson] is fully aware of that. That this kind of conduct and behaviour is simply unacceptable in the most absolute of terms and it's got to stop. It's got to be properly disciplined,"*** **Goodale** said in an interview that is set to air Saturday morning (...)**The public safety minister** said he spoke to Paulson Friday morning after the alleged misconduct was revealed. ***"I expressed to the commissioner very clearly my outrage at this situation. He knows very clearly what I expect. I expect a complete transparent and comprehensive investigation. I expect strong discipline that suits the misbehaviour that has taken place,"*** **Goodale** said. ***"How could this have***

happened in a facility that is designed to train police officers?" he said. ***"I expect a clean-up of what appears to be unacceptable toxicity in the workplace at the RCMP, where people should expect exemplary behaviour, not this kind of bizarre and degrading kind of conduct."*** RCMP Deputy Commissioner Peter Henschel told CBC News Thursday that he immediately ordered another review of the conduct. CBC News

Goodale outraged by mounties' 'Toxic Workplace'
The public safety minister says he has expressed his outrage to the country's top Mountie over the latest allegations of sexual harassment in the force. **Ralph Goodale** says he told RCMP Commissioner Bob Paulson he expects a comprehensive, transparent investigation, strong discipline, support for victims and a plan to end what he calls ***"this toxic workplace behaviour."*** The strong words come after CBC News reported allegations of unwanted sexual touching, bullying and rampant nudity in the workplace at the explosives training unit of the Canadian Police College in Ottawa. In a statement, **Goodale** said Prime Minister Justin Trudeau has given him a clear mandate to ensure the RCMP is a healthy workplace free from harassment and sexual violence. **Goodale's parliamentary secretary, Michel Picard**, confirmed two RCMP members had been suspended in relation to the allegations. Const. Annie Delisle, an RCMP spokeswoman, had no additional comment. The RCMP has been beset by numerous cases of sexual harassment and bullying. Canadian Press (National Post, A7; Waterloo Region Record, Cape Breton Post)

Electronic spies lack government oversight
Canada's electronic spies can assist CSIS with the agency's new mandate to disrupt security threats with little oversight from politicians or the courts, documents obtained by the Star show. The Communications Security Establishment (CSE) told Defence Minister Harjit Sajjan last November they can aid CSIS with new "threat reduction" efforts - a power granted to the agency under Bill C-51. It's not unusual for CSE to lend a hand to police or intelligence agencies; in addition to electronic espionage and cyber defence, assistance to law enforcement is one of the agency's core mandates. But that assistance often requires a warrant. But under C-51, CSIS can take action to reduce threats to national security without a warrant - so long as the agency's efforts don't violate Canadian law or charter rights. CSE confirmed that they do not necessarily need a court's approval to assist CSIS in threat reduction. The new power has opened the door for CSE to act as a "virtuous hacker" for CSIS, according to national security researcher Craig Forcese. "This was the sleeper in C-51, because CSE is barely mentioned in C-51," said Forcese, a vocal critic of the new terrorism law. "CSE has been a watcher ... It has not been able to do things kinetically to people. But under the umbrella of CSIS assistance, it can now go kinetic (...)"**A spokesperson for Public Safety Minister Ralph Goodale** noted that the Liberals have promised to revisit some of the more controversial aspects of the bill, but did not address the specific question of CSIS-CSE co-operation. ***"(The government) will launch broad, public consultations on our national security framework to ensure that our police and security agencies are being effective at keeping us safe, and that our values, rights and freedoms are being respected,"*** **Scott Bardsley** wrote in a statement. ***"We want to hear from parliamentarians, from subject-matter experts, from the general public and from foreign partners ... We'll listen to Canadians and we'll produce a truly Canadian model that will work well for us."*** Toronto Star, A12

Les conservateurs déçus de l'abandon de l'appel
Pour les conservateurs, le gouvernement trudeau a pris une mauvaise décision en ne s'opposant plus à la décision de la Cour d'appel d'alberta d'accorder à Omar Khadr sa liberté sous caution. Jeudi, **le ministre de la Sécurité publique Ralph Goodale** avait annoncé que son gouvernement abandonnait son appel, ce qui permettra à M. Khadr de jouir de sa liberté sous caution. Ainsi, ce dernier pourra attendre la décision en appel de ses déclarations de culpabilité aux États-Unis sans craindre de devoir retourner en prison au Canada. «Nous sommes déçus par cette décision, a fait savoir le porte-parole de l'opposition officielle en matière de sécurité publique, Erin O'toole, hier. La sécurité publique demeure une priorité importante pour le Parti conservateur, et l'expérience de la famille Khadr montre que la radicalisation au Canada peut entraîner des risques, ici au pays et à l'étranger.» Agence QMI (Journal de Montréal, 38; Journal de Québec)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Cyberthreats could pose danger to oilpatch infrastructure
Alberta's energy department will hold meetings in the coming weeks to discuss the threat of cyberattacks on oil-and-gas infrastructure - an issue that was flagged in a recent report by the province's auditor general. The report noted the Alberta government does not require provincially regulated oil-and-gas operators to meet minimum IT security standards for the systems that control pumps, valves and other key oil-and-gas equipment. There are standards for utilities, but electrical operators aren't required to comply with those until October of next year. Although the threat of an attack on the oil-and-gas industry was found to be low, the auditor general's report says there's been no government assessment of what the impact would be if a cyberattack were to occur. Alberta Energy Minister Marg McCuaig-Boyd says her department accepts the auditor general's recommendations. Canadian Press (St. John's Telegram, A22; Red Deer Advocate, Calgary Herald, Calgary Sun, Waterloo Region Record, Times Colonist, *Whitehorse Daily Star)

New bill targets PTSD
A bill introduced to the Ontario legislature would give first responders who are battling posttraumatic stress disorder (PTSD) extra support. The Supporting Ontario's First Responders Act was introduced by Labour Minister Kevin Flynn and Community Safety and Correctional Services Minister Yasir Naqvi on Thursday. If passed, which is likely, due to the Liberal majority, the act would amend the Workplace Safety and Insurance Act and the Ministry of Labour Act. The act would expedite the claims process for those diagnosed with PTSD, require employers to implement PTSD prevention plans and remove the need to prove a link between PTSD and a workplace event. "Given all that we ask of our first responders, it is only fair that we support them when they need us most," Flynn said in a news release. "This legislation will give first responders and those who work in corrections the peace of mind they deserve, and our prevention, resiliency and research initiatives will round out a comprehensive PTSD approach we can all be proud of and that will protect the brave men and women who we entrust with keeping us safe and secure." The act will apply to police officers, dispatchers of police, firefighters, First nations emergency response teams, paramedics, ambulance services, and workers in youth justice facilities and correctional institutions. Kingston Whig-Standard, A1

Two rescuers to get Red Cross bravery award
Bravery may not be their middle names, but it's something Earl LeBlanc and Naveed Majid have embraced. The two men will be honoured next month with the Red Cross Rescuer Award. The accolade acknowledges the efforts of non-professional rescuers and off-duty first responders who go out of their way to save a life, prevent further injury and/or provide comfort to the injured. Daily Gleaner, A2

1st confirmed case of Zika virus in Ontario, province says
Ontario's first case of the Zika virus has been confirmed by the province's Ministry of Health and Long-Term Care. In a statement, the province's chief medical officer of health said Friday that Public Health Ontario received positive test results for the virus in an individual who had travelled to Colombia. The ministry did not confirm whether the person affected is a man or a woman, but did say that the patient is not pregnant. CBC News

Canadian family on board helicopter that crashed into Pearl Harbor
A Canadian family was on board a helicopter that crashed into Pearl Harbor Thursday. The family of four visiting from Canada and the pilot on board made it out, but one passenger – a 15-year-old boy who was trapped underwater and had to be cut free from his seat – remained hospitalized in critical condition Friday. Global News

***Making mountains safe for skiers**
Avalanche experts in Canada are working on a new project in hopes of helping recreational backcountry enthusiasts answer a question that could help save their lives: What would the pros do? The $1.02-million research spree comes as organizations such as Avalanche Canada continue to expand their outreach efforts, trying to broaden the range of folks who take their traditional and standardized safety courses. The research slice depends on academics; the expansion plans lean on professional skiers such as Leah

Evans offering a cool factor to education (…) Avalanche information available to the public today provides technical information about snow layers, as well potential hazards relative to terrain. Mr. Haegeli wants to add another aspect by providing mountain fans - even experienced ones - with more refined guidelines on what type of terrain would be most appropriate under certain conditions. Globe and Mail, S1

***Avalanche warning issued for southeastern B.C**
Avalanche Canada has issued an immediate warning as potentially deadly snow conditions develop on slopes across parts of eastern and southeastern British Columbia. The warning is in effect through to Monday, Feb. 22, and covers the North and South Columbia regions, the Purcell Mountains and the Kootenay Boundary. Glacier National Park has issued a similar warning for backcountry users in that region east of Revelstoke. Canadian Press (Red Deer Advocate, A4, Times Colonist, Calgary Sun)

***Ice-cutters launching on Red River due March 2**
If the mild weather wasn't enough to convince you spring is around the corner, maybe this will: the province's ice-cutting machines will be out on the Red River north of Selkirk this weekend. Ice-cutting is set to begin Sunday as part of the province's flood-fighting effort. The next day, icebreakers are scheduled to be on the river between Netley Creek and Netley Lake, cutting and scoring the ice to help enable ice movement and reduce jamming. The province has yet to release a spring flood outlook. However, a spring flood forecast released Thursday by the U.S. Weather Service said the threat is slightly lower than average in North Dakota. Postmedia Network (Winnipeg Sun, A7)

*** Flood restoration open house in Rocky on March 1**
An open house in Rocky Mountain House on March 1 will provide updated information of efforts to restore backcountry trails damaged in the 2013 floods. The Alberta government will host information sessions in three communities along the Eastern Slopes to share progress on repairs to the damaged trails and set rehabilitation priorities for the 2016 season. Red Deer Advocate, C1

***New technology helps increase safety for the deaf and hard of hearing**
Hearing smoke alarms blaring and escaping a fire is a terrifying experience for anyone. Now, imagine if you are deaf or hard of hearing. A smoke alarm with an integrated LED strobe light has been introduced by Kidde Canada to help the deaf and their family members have greater peace of mind in fire emergencies. Designed to be hardwired into a home's electrical system, the new device also features a 10-year sealed backup battery to keep the alarm functioning during a power outage. Postmedia Network (Edmonton Sun, H14)

*** Lac-Mégantic, une ville en sursis**
Un article d'opinion dit "La catastrophe ferroviaire du 6 juillet 2013 de Lac-Mégantic avait été pressentie huit mois avant son triste avènement. Cette tragédie qui a coûté la vie à 47 personnes en plus de détruire près de la moitié du centre-ville de Lac-Mégantic avait pourtant fait l'objet de plusieurs avertissements préalables. Le 12 novembre 2012, les élus de la municipalité de Lac-Mégantic et ceux de la MRC avaient effectivement adressé une mise en garde écrite à la Montreal Maine & Atlantic ainsi qu'à deux ministres du gouvernement Harper, Denis Lebel, ministre des Transports, et Christian Paradis, lieutenant de Stephen Harper au Québec. Cette lettre accompagnée d'une résolution officielle de la municipalité déplorait le piètre état du tronçon de chemin de fer à l'entrée de la municipalité. La résolution précisait que le chemin de fer avait été endommagé par des pluies abondantes survenues en 2008, et que les travaux correctifs s'imposaient rapidement. " La Tribune, 13

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Why don't we charge more people with terrorism?
An opinion piece by Senator Daniel Lang states "I have just returned from a NATO meeting in Brussels where our delegation heard that Europe's security concerns mirror many of ours: an unpredictable and belligerent Russia continues to challenge the transatlantic alliance; mass migration is destabilizing Europe; and Islamic radicalization is on the rise. During the past three years that I have chaired the Standing Senate Committee on National Security and Defence, we have studied and reported on the

threats to national security. Our report, Countering the Terrorist Threat in Canada, was clear about the terrorist threat we face. After nine months of hearings and testimony from over 100 witnesses, we learned that: n By late 2014, authorities identified 318 radical Canadian jihadists, 93 of them seeking to travel abroad, 145 overseas and 80 returnees. These numbers have since increased. There were 683 identified cases of terrorist financing in the last five years, to our knowledge, there have not been any specific charges or prosecutions were initiated. Foreign funds had entered Canada for religious-oriented programming despite their donors and recipients being linked to radicalization. Eight Canadian charities had their charitable status revoked because of indirect or direct connections to terrorism - yet none of their executive or staff faced criminal prosecution. Terrorist promotion and radicalization remain a concern in many areas of society, including at schools, colleges, and in religious facilities." Postmedia Network (Calgary Sun, N15; Toronto Sun, Edmonton Sun, Winnipeg Sun, Ottawa Sun)

Wrong to fund radical agency
An opinion piece states "Bravo to the Trudeau Liberals for supporting Tony Clement and Michelle Rempel's opposition motion to condemn the 'Boycott, Divestment and Sanctions' (BDS) movement against Israel. BDS is popular on university campuses, but most people see it for what it is, a hateful movement trying to delegitimize the world's only Jewish state and the Middle East's only democracy. While it was refreshing to see Prime Minister Justin Trudeau stand up for peace and freedom in Israel, this symbolic gesture came only days after a troubling media report." Postmedia Network (Calgary Sun, N15; Ottawa Sun, Edmonton Sun, Toronto Sun)

Grits soft on terror
A letter to the editor states "It is not surprising in the least that the Liberals have dropped a bail appeal against Canada's most infamous terrorist, Omar Khadr. The Grits' soft stance on terrorism began when they announced their withdrawing of our bombing mission against ISIS. Expect the feds to cave to his lawsuit demands and put the taxpayer on the hook for millions of dollars. It would also not surprise me if Omar became a special adviser with regards to our Middle East policy." Ottawa Sun, A20

***Snowden to make SFU presentation**
A man considered everything from a heroic whistleblower to a traitor is making a cyber visit to British Columbia. Edward Snowden will make the keynote presentation, via web link, as part of a Simon Fraser University program examining the opportunities and dangers of online data gathering. The presentation, at Vancouver's Queen Elizabeth Theatre on April 5, will be followed by a moderated discussion with expert panellists from SFU and the B.C. Civil Liberties Association. Times Colonist, A7

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

***Couillard, champion du libre-échange**
Pour sa première visite à Washington, vendredi, le premier ministre Philippe Couillard s'est positionné comme un champion du libre-échange devant des gens d'affaires ainsi qu'avec Michael Froman, le représentant américain au Commerce. " C'est de la musique à nos oreilles de vous entendre parler de l'importance du libre-échange et du libre marché ", lui a répondu Jodi Hanson Bond, vice-présidente de la Chambre de commerce des États-Unis. Concernant sa rencontre avec Michael Froman, qui dirige l'organisme en charge de négocier et d'administrer les accords commerciaux aux États-Unis, le premier ministre a dit avoir fait des progrès sur le projet d'installer des centres de prédédouanement à l'aéroport de Québec et à la gare centrale de Montréal. " Le signal est positif, a précisé M. Couillard. La question à l'aéroport de Québec semble très bien aller. A la gare [de Montréal], c'est un peu plus compliqué, mais cela va bien aussi. On peut être optimiste qu'on va être capable de régler ces questions, ce qui va être un gros avantage non seulement pour nos voyageurs, mais également pour les transports de marchandises. " Ces centres permettraient que des douanes soient installées à même l'aéroport de Québec et la gare de Montréal, comme c'est déjà le cas à l'aéroport Pierre-Elliott Trudeau. Le Devoir, C1; La Presse Canadienne (Le Quotidien, La Voix de l'Est); Agence QMI (Journal de Québec, Journal de Montréal)

***Border agents expand scope of investigation**

Agents of the Canada Border Services Agency were at the Cavendish Farms plant in New Annan Wednesday, the same day they moved in on a Charlottetown motel. But nobody is saying why or whether the two incidents are connected. Allan Donovan, a communications officer with the agency, confirmed agents were at Cavendish Farms during an interview with The Guardian on Friday. "I can't provide any further details because the investigation is ongoing," he said. In an email, Mary Keith, a spokeswoman for Cavendish Farms, said the company itself was not part of the agency's investigation and Cavendish Farms had no information regarding the matter. A witness at the plant said border agents left with one of the plant's workers. On the same day, border agents spent hours at the Sherwood Inn and Motel removing boxes of documents from the main building and two units from the adjacent motel. The agency would not provide The Guardian with any details about its activities at the motel saying it is part of an ongoing investigation. Charlottetown Guardian, A3/FRONT

***Activist urges Russian rights sanctions**

Anglo-American financier and anti-Putin campaigner Bill Browder arrives in Canada Monday seeking all-party support to adopt a Canadian version of the U.S. Magnitsky Act, which freezes assets and bans visas of Russian human-rights violators. Mr. Browder, who campaigned to get the U.S. Congress to pass the law in 2013, is meeting cabinet ministers, officials from the Prime Minister's Office and members of Parliament from all parties, and will appear before the Commons Foreign Affairs committee. "I am coming back to Canada to basically uphold the Liberals to their promise and to make this law," he said in a telephone interview from London, where he has been living since he was deported from Russia in 2005. "It should apply to all the perpetrators of human-rights abuses in Russia. Not just the people who tortured and killed Sergei Magnitsky." Parliament unanimously adopted a motion put forward by then Liberal MP Irwin Cotler last year, calling for U.S.-style sanctions against individual human-rights violators in Russia, including those involved in the 2009 detention, torture and murder of Russian whistle-blower Sergei Magnitsky. Globe and Mail, A3

***FAA banned Canadian private planes from U.S. airspace for 1 month**

U.S. security decision that banned private Canadian aircraft from flying through American airspace when travelling between cities in Canada affected dozens of flights and cost thousands of dollars in extra fuel before the decision was reversed, industry officials say. The U.S. Federal Aviation Administration [FAA] issued a notice Dec.14 last year warning private pilots that all foreign private planes now had to obtain diplomatic clearance from the secretary of state before entering U.S. airspace (...)The issue began when the FAA issued a notice to airmen (NOTAM) Dec.14, 2015 warning non commercial pilots about increased security measures. "The FAA administrator hereby orders that all U.S. territorial airspace is national defence airspace," read the notice. "Pilots of such aircraft that do not adhere to procedures in the special security requirements contained in the NOTAM may be intercepted, detained and interviewed by law enforcement, U.S. Secret Service, or other security personnel. "Any person who knowingly or willfully violates the special security requirements ... may be subject to penalties," the notice said.
Both aviation groups contacted Transport Canada to discover officials in the department had no idea the notice had been issued by the U.S. authorities. "How come nobody knows about this," Toering asked. "How come Transport wasn't advised? How come our embassies weren't advised? CBC News

Officers find nearly five kilos of suspected heroin at Halifax airport

The Canada Border Services Agency says nearly five kilograms of suspected heroin has been seized at Halifax Stanfield International Airport. The agency says CBSA officers discovered inconsistencies in a traveller's suitcase during a routine secondary examination on Sunday. The officers dismantled the suitcase and found a large package hidden in the suitcase liner. The agency says tests identified a substance in the package as suspected heroin. Canadian Press (Cape Breton Post, A10; Red Deer Advocate)

Holy Mackerel! Heroin in frozen fish

Canada Border Services Agency says there was something fishy about a shipment inspected at Toronto's airport - and it wasn't just the frozen fish. CBSA says officers at Pearson International Airport were conducting a routine examination of cargo arriving off a flight from Lahore, Pakistan, on Tuesday when they discovered suspected heroin. Officials say officers found two small packages deep within a large

shipment of frozen fish that were similarly wrapped and loosely placed inside the contents. The packages were cut open and the contents tested positive for heroin. Canadian Press (Toronto Sun, A4)

***Ex-fugitive convicted of Seattle rape**
A former Edmonton man and highrisk sex offender who escaped Canada in 2013 has been found guilty of raping a 69-year-old woman in Seattle. Michael Stanley, 49, triggered a manhunt across Saskatchewan and Alberta when he cut off his ankle bracelet in Lloydminster on the boundary of the two provinces and made a run for the U.S. border, which he managed to cross unchallenged. At the time, Canadian authorities alerted their U.S. counterparts about Stanley. But U.S. officials determined he was a U.S. citizen and they had no reason to arrest him, so let him enter the country. Canadian officials did not ask for his extradition. Times Colonist, A10; Canadian Press (Kingston Whig-Standard, Calgary Sun, Winnipeg Sun, Edmonton Sun, Toronto Sun)

*** Séduire les touristes américains**
La MRC Brome-Missisquoi profitera de la faiblesse du dollar canadien pour faire de l'oeil aux touristes américains. Une campagne marketing est en chantier pour les attirer dans la région cet été. C'est à la demande de quelques maires que l'équipe du CLD Brome-Missisquoi se penche sur le dossier, explique son directeur du développement économique, Denis Beauchamp. « Y a-t-il moyen de tirer avantage de ce contexte pour encourager nos voisins à venir nous voir ? On travaille là-dessus », dit-il (…) La région a déjà été plus fréquentée par les Américains, a fait remarquer M. Beauchamp, citant la fin des années 90 et le début des années 2000. Le contexte international a changé depuis, note-t-il. Les attentats du 11 septembre 2001, suivi du resserrement des contrôles douaniers et de la crise du SCRAS (syndrome respiratoire aigu sévère) ont découragé les Américains de voyager au Canada, a indiqué M. Beauchamp. Par ailleurs, le refus du Canada de participer à la guerre en Irak en 2003 a également eu un impact négatif. La Voix de l'Est, 11

***BCSC fines woman $37 million for cross-border Ponzi scheme**
The B.C. Securities Commission has found that former Mission resident Doris Elizabeth Nelson committed fraud with her Little Loan Shoppe payday loan business that was a front for a cross-border Ponzi scheme that had raised as much as $135 million US. In a decision released Friday, the commission levied $37 million in fines against Nelson and banned her permanently from B.C. financial markets after finding that her business "was the front for a widespread Ponzi scheme that resulted in at least 121 British Columbia investors making investments," and suffering losses. Of the $19 million that B.C. investors put into the scheme, $18.5 million remains unaccounted for (…) Nelson is currently in a U.S. jail serving a nine-year sentence on wire fraud charges after pleading guilty in 2014 to 110 counts in the U.S. District Court of Eastern Washington. Her lawyer said she has filed an appeal seeking to withdraw her initial plea and seek a full trial. Vancouver Sun

***Myrtle Beach has a deal for Canadians**
The limping loonie has meant trouble for u.S. destinations that rely on Canadian visitors. The Canadian Press recently reported that tourismto the States was down 9% in 2015 compared to the same period in 2014. Myrtle beach is one of those destinations that relies on Canadian tourism dollars to inject millions into the local economy. So many of us visit the South Carolina destination each year, it hosts an annual Canadian-american days Festival with special events just for visitors from north of the border. In light of the weak loonie, the Myrtle beach Convention and Visitors bureau has launched a new promotion to attract Canadian travellers and help them save. Postmedia News (London Free Press, F2)

CYBER SECURITY / CYBERSÉCURITÉ

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Psychologists fighting national-security ban

Canada's police forces are increasingly calling on psychologists to help them get into the minds of criminals - seeking advice on how to talk to suspects or deciding whether they are being truthful. But this growing relationship has invited scrutiny, especially after a damning report last year uncovered severe ethics violations by prominent U.S. psychologists who had helped Washington develop torture and other coercive techniques to question terrorism suspects. The American Psychological Association (APA) subsequently prohibited all its members, including about 800 Canadians, from participating in any national security-related interrogations. Now a leading Canadian forensic psychologist has entered the fray. Stephen Porter penned a column this month in the journal Canadian Psychology, calling the blanket ban a "kneejerk" overreaction and making the case for expanding psychologists' roles in criminal investigations. The University of British Columbia professor says while the actions of the American psychologists were reprehensible, the ban could create the wrong impression that psychologists have nothing to contribute to law enforcement or national security. "It suggests we don' t have knowledge that is meaningful ... and that we can't be expected to act ethically," said Porter, who is regularly called on by police to help in cases. "Psychological science has really led to a lot of great knowledge that is relevant to interviewing suspects, including terror suspects - interviewing them in humane but also effective ways." The controversy erupted last July, after an independent report found senior APA members had worked with the Pentagon and the Central Intelligence Agency in developing "enhanced interrogation" methods and manipulating ethical guidelines. Postmedia News (National Post, A6)

***Shootings show dangers facing police in remote communities**

It's hard to think of anything that Steve Déry or his partner could have done differently to avert tragedy that night in Kuujjuaq. Responding to a routine call, they pulled up to a bungalow on the Inuit territory to break up a fist fight inside the home. It was during the short walk between their squad car and the front door that the first shot rang out. The bullet clipped Déry's partner in the shoulder, crumpling him on impact. Before they could assess the damage, both men sought shelter behind the police cruiser. Then, more shots from inside the house. In that second burst of gunfire, a .300 calibre bullet pierced Déry's left cheekbone and exited through his jaw, causing a massive hemorrhage. He fell and sustained two more gunshot wounds to his ankle and foot before his partner picked up Déry's sidearm, fired two rounds at the house and dragged him behind another vehicle. But despite the efforts of his partner - who was severely injured when he pulled Déry to safety - the initial gunshot wound proved fatal, according to the Quebec coroner's report obtained by the Montreal Gazette. While paramedics tried, in vain, to revive the 27-year-old Déry, the shooter barricaded himself in the house. After a 16-hour standoff with police, the shooter committed suicide on the morning of March 3, 2013. Fast-forward three years and a remarkably similar situation unfolded in the Lac Simon First Nation, near Val-d'Or. Though details are still hazy, 26-year-old Thierry Leroux and his partner were responding to a routine call on the Algonquin reserve last week when the officer was fatally gunned down. The suspect then turned his weapon on himself and ended his life. Next week - as information from a police and coroner's investigation into Leroux's death begins to surface - teachers at Quebec's police academy will get together hoping to determine whether these situations are avoidable or simply an enduring risk of the job. Montreal Gazette, A3

***Changes to auxiliary RCMP role risky to officers: retired Mountie**

The safety of Mounties is at greater risk after sweeping changes to the duties of volunteer RCMP members, a retired RCMP officer says. “Auxiliaries are the extra eyes, ears and muscle if you need it and you certainly need it at times,” says Ret. Const. Paul Christoffersen, who rode with auxiliary constables for 25 years as he worked highway patrol in Banff and Strathcona County before retiring to Fort Saskatchewan in 2002. Once riding shotgun with regular force RCMP officers, the results of a year-long safety review in January saw the national police force halt all ride-alongs and firearms training for auxiliary constables, volunteer police who dedicate more than 160 hours annually to assisting regular RCMP members with community engagement and crime prevention work. Edmonton Journal, A3; Edmonton Sun

Three plead guilty in RCMP drug sting

Suitcases stuffed with millions handed over at a Vancouver hotel. Cryptic text messages about massive cocaine deliveries. Secret meetings from Vancouver to Panama City. Details of a major 2012 undercover investigation into some Hells Angels and associates were revealed at sentencing hearings of suspects who've pleaded guilty in the case. The RCMP "arranged a reverse sting sale of 500 kilograms of cocaine

for $14.8 million," according to an agreed statement of facts at one of the sentencing hearings. "Over a series of meetings with the principal conspirators, the RCMP undercover officers obtained approximately $4 million cash in exchange for 200 kilograms of cocaine." Police announced in August 2012 that two full-patch Kelowna Hells Angels and six others had been arrested on drug charges, plus two counts of working for a criminal organization. Three of the associates - Murray Trekofski, Orhan Saydam and Kevin Van Kalkeren - have since quietly pleaded guilty, but those proceedings were covered by publication bans until Friday. Vancouver Sun, A5

One Woodstock Mountie disciplined, transferred
One of four Woodstock Mounties suspended late last year has been 'severely' disciplined and transferred, while the three other officers remain under criminal investigation. Assistant Commissioner Roger Brown, commanding officer of the RCMP in New Brunswick, said the officer has gone through a conduct hearing and has been moved out of the community. The unnamed officer has received "a pretty severe sanction," Brown said. "I can't get into the sanction because it's an internal process," the assistant commissioner said in an interview. "He took full responsibility, has moved on and is doing a good job." The RCMP announced Dec. 8 that four members of the Woodstock detachment were being suspended for "discreditable conduct" and were also the subject of a criminal investigation, but that no charges had yet been laid. Telegraph-Journal (Daily Gleaner, A1)

***RCMP making strides in battling mental illness**
Battling mental illness continues to be a top priority for the RCMP in New Brunswick. Assistant Commissioner Roger Brown said Friday that significant progress is being made. Brown said over the last year-plus, the force has worked to increase awareness surrounding post-traumatic stress disorder and other mental-health issues while zeroing in on the stigma attached to it. "I see a huge difference in the dialogue," Brown said. "I have seen our numbers drop 50-60 per cent in the last year of people who were off (work)." He said members are talking openly about it and the negative stigma attached to it doesn't seem to be as prevalent. Daily Gleaner, A7

***Missing snowmobiler**
When Will Lapensee's four-year old daughter Mia woke up Friday morning, she told her mom it would be the day Daddy came home. The story of the dream was shared publicly on a Facebook post by Will Lapensee's aunt minutes after the family had received the news. Friday morning RCMP divers found the body of the 26-year old New Ross man, who fell through the ice riding a snowmobile the night of Feb. 13. The snowmobile he was on was a gift for his birthday. Lapensee turned 26 on Feb. 10. RCMP say members of the Underwater Recovery Team located a body in Black River Lake at about 11:20 a.m. Friday, close to where Lapensee's snowmobile was seen to have gone through the ice. Chronicle-Herald, A4; TC Media (Cape Breton Post, A10)

***Red Deer Mounties investigate shooting**
Red Deer RCMP are appealing to the public for help in identifying a man who fired a shot at a passing vehicle last week. Police say shortly before 11:30 p.m. on Feb. 11, the victim was turning to head east onto 19th Street from 50th Avenue when a newer looking green Chrysler 200 or 300 pulled up beside his vehicle. A man in the front passenger seat then leaned out of the window and fired what appeared to be a handgun across the hood of the victim's vehicle. Calgary Herald, A9

***Okotoks RCMP confirm missing man has been found**
An Okotoks man reported missing this week has been found alive, say RCMP. Zachary Lavin, 19, left his residence in Okotoks around 4 p.m. Wednesday bound for work in Blackfalds, north of Red Deer. He never showed up for work and was reported missing by his family. RCMP said Lavin was located in the Kananaskis area on Friday and was receiving medical treatment for exposure and sustained injuries. No further information was provided on the nature of Lavin's disappearance. Calgary Herald

***Rimbey RCMP Recover 70-Year-Old Letters In Stolen Vehicle**
RCMP are trying to find relatives of a woman and a man who wrote letters to each other as far back as the 1940s. Mounties found a bundle of the handwritten letters in a stolen vehicle in central Alberta. The names on the envelopes are Margaret Clark and Mungo Clark, including one that shows he was a gunner

who served in the 40th Battery, 11th Field Regiment, Canadian Army overseas. RCMP Cpl. Laurel Scott said the letters are likely to be of sentimental value to someone. Canadian Press (Huffington Post, National Post)

***RCMP warning public about phone scam**
The RCMP in Newfoundland and Labrador is warning the public about a phone scam where fraudsters are claiming to be from the RCMP and are demanding money. The RCMP said in a news release, the callers are aggressive, saying that the victims have been fined or are in trouble with a federal government agency. They sometimes claim that the victim will be arrested if the money is not paid. "Some of these fraudsters are making themselves seem legitimate by running a program that shows an RCMP phone number on the victim's call display," the release states. "This is a scam. RCMP is advising anyone who receives one of these calls to hang up and to not send money or provide personal information." St. John's Telegram

***Festival and event organizers struggle with rising police fees**
Festival and event organizers are struggling to find ways to cut costs and scrape together enough money to cover ballooning police fees. And the organizer of one of the city's biggest, the Servus Heritage Festival, says they may have to consider an admission fee to make up the shortfall. Jim Gibbon, executive director of the Edmonton Heritage Festival Association, said this July's threeday event at Hawrelak Park is expected to cost a total of $226,000, up $63,000 from the previous year. Seventy-five per cent of that bill is for policing. "We don't charge admission. So my current statement to police is, 'How do I pay you? Where does this money come from to pay you?"' he asked. Police officers provide security oversight and traffic management for hundreds of concerts, sports games, parades, road races and other public gatherings each year. In 2014, police worked 1,314 events. Because such events often take place on weekends and evenings when officers are offduty, those on festival shifts typically earn double time. Edmonton Journal, A2; Edmonton Sun

***Last of the rioters hauled off to jail**
The last two Stanley Cup rioters still standing have fallen. Five years after they dared thumb their noses at Vancouver residents and the rule of law, William Fisher and Jeffrey Milne were taken to the Big House on Friday. They earned the ignominious distinction of being the final two of the riotous 300 dealt with by the legal system. Fisher, who arrived late for sentencing, was given a total of 36 months imprisonment and Milne got 32 months for rioting, masking their faces, inciting others, multiple cowardly assaults and other charges. Vancouver Sun, A4

***City's officers take the de-escalator**
A man has barricaded himself inside a home and is threatening to commit suicide.
He has physically assaulted his ex-girlfriend. She escaped, called 911 and told the dispatcher that her ex-boyfriend was planning to swallow a bottle of pills to end it all. For police arriving on-scene, it's an emotionally charged and volatile situation - and officers are now learning it's one where listening and empathy may go further than force. Every Toronto police officer has to take annual training that specifically tests their negotiation skills, requiring them to demonstrate listening and response strategies to de-escalate tense situations, such as the scenario of the suicidal man barricaded in his home. "Through empathetic listening, we hope to build a rapport with the view to ultimately influencing behaviour in a positive way," Toronto Police College training Const. Stephen Jones told reporters Friday. "This really improves our chances of a peaceful outcome for us and for our folks in the community." Toronto Star, GT1

***How to transform the police force and its budget**
When David Soknacki was first contacted by the mayor's office near the end of last year about sitting on a task force to tackle police reform and rein in the Toronto force's ballooning $1-billion budget, he said no thanks. When Mayor John Tory called again last week, his answer was more or less the same. "I said I would think about it, which was a polite way of saying no," said Mr. Soknacki, the businessman and former Scarborough city councillor who dropped out of the race for mayor in 2014. Mr. Soknacki, who despite his fiscal conservatism served as budget chief in the first term of left-leaning mayor David Miller, said he simply did not feel that Mr. Tory or Toronto Police Services Board chairman Andy Pringle were

serious about their commitment to radical change at the police force. However, after subsequent conversations, he decided to take the pair's assurances at "face value." Chief Mark Saunders has joined Mr. Tory and Mr. Pringle in saying he is ready to reform policing in Toronto. Globe and Mail, M1

***Time to stop clownish attire of police**
An editorial states "Never-ending, purposeless protest gestures are beginning to erode public confidence in Montreal's police force. This casual-looking approach to policing could have unintended consequences as a handful of protesters are blurring the lines between protest and nuisance. As tension mounts between taxi and Uber drivers, the potential for serious violence is obvious. In plain view of reporters, officers "stood by but didn't intervene" as cabbies pelted eggs at their competitors' vehicles. A group of Montreal taxi drivers has also promised to continue deploying roving squads to summon and sequester Uber drivers. Some cabbies, wearing cowboy hats and brandishing fake pistols and badges, have also taken it upon themselves to steal phones being used by unlicensed drivers - in plain view of cameras. "We have seized the device you use as your weapon to transport people illegally." Montreal Gazette, A10

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Christopher Watts' short-lived freedom
Christopher Watts, the convicted sex offender jailed in the 2001 death of a Kitchener teen, was released from prison last November with a sober warning he was at a high risk to reoffend. He lasted only a few weeks before he was back behind bars. Watts was set free last fall after serving a 12-year sentence for manslaughter, sexual interference and sexual assault in the death of 13-year-old Amanda Raymond. The teen died of an overdose after a party at Watts' Somme Island house on Puslinch Lake. A recently released Parole Board of Canada report paints a revealing portrait of Watts - describing him as an unremorseful, sex-obsessed career criminal who consistently sees himself as a victim, a "totally defiant" man without any sense of guilt or remorse. In the Jan. 26 report, the parole board expressed concern that as a free man, Watts is simply too great a threat to the public. "The Board is satisfied there is no appropriate program of supervision that can be established which would adequately protect society from your risk to reoffend," the parole board wrote (...) The parole board wants Watts to be charged with breaching the conditions of his parole, a move that could keep him in prison for up to 10 more years if he's convicted. For now, Watts is back in a federal prison, waiting for the new charge to be processed by the courts. Waterloo Region Record, A1

Transfer of killers like Gregory Despres to less secure facilities postponed
A transfer to a less-secure facility of high-risk offenders deemed not criminally responsible for their actions has been postponed, but that's small comfort to some victims. Gregory Allan Despres, 33, brutally murdered Fred (Papa) Fulton, 74, and Veronica (Verna) Decarie, 70, in their Slope Road home in Minto in April 2005. He was eventually deemed not criminally responsible for his actions after two trials, and he's since been held at the Shepody Healing Centre, a federal health-care facility on the grounds of Dorchester Penitentiary with a secure psychiatric unit. Offenders deemed not responsible for their actions due to mental disorders are the responsibility of the provincial government, and most are held at the Restigouche Hospital Centre, a psychiatric hospital in Campbellton. However, a handful of such offenders are held at Shepody, a federal facility, due to various factors, including higher security risks. The province pays the federal government to house such offenders at Shepody. The arrangement is about to end, as was revealed last year. Shepody was set to transfer those provincial detainees out in the spring, but Correctional Service Canada (CSC) now says the plan has changed. "CSC has been working with the Province of New Brunswick to return patients deemed not criminally responsible (NCR) back under provincial care and responsibility. It was anticipated that this could be completed by April 1, 2016," Correctional Service of Canada spokeswoman Sabrina Nash wrote in an email to The Daily Gleaner. Daily Gleaner, A4

Day parole granted to convicted sex offender
A former high school youth worker who went to prison after committing several sex offences has been granted day parole. Arthur Francis McGuigan was sentenced in October 2014 to five years, four months and four days in prison on charges that included two counts of sexual exploitation, luring and drug

possession for the purpose of trafficking. A recent Parole Board of Canada decision granted McGuigan day parole for six months, during which time he will live in a halfway house. In its report, the board said it was satisfied McGuigan's release plan contains the right level of structure and resources needed to mitigate his risk of reoffending. Charlottetown Guardian, A1/A2

Les détenues paient le prix de l'austérité
Sans qu'on en fasse de cas, les détenues de la prison Tanguay doivent être transférées dans les prochains jours à l'institut Leclerc, qui deviendra ainsi un établissement mixte. Ces femmes privées de leur liberté font ici les frais des mesures d'austérité, pensent plusieurs spécialistes, qui dénoncent d'importants reculs. Construite en 1964, la prison Tanguay a été déclarée désuète par Québec en septembre dernier. Ce n'est pas le cas de la prison Leclerc, pourtant édifiée quatre ans plus tôt, et fermée en 2012 par le gouvernement fédéral pour cause de... désuétude, rappelle la criminologue Sylvie Frigon, de l'Université d'Ottawa. " S'il existe une prison désuète, c'est bien Leclerc (...)" Québec, qui ne cache pas que sa décision est motivée en partie par des " raisons économiques ", fait valoir que les prisonnières de Tanguay seront placées dans une aile séparée, dans une prison ancienne. Prison dont l'aspect austère n'invite guère à la réhabilitation, rétorque Sylvie Frigon. " Je suis perplexe à propos de ce qu'on veut faire ici. On recule, d'une certaine façon. " La criminologue rappelle en effet que, dans l'histoire, les expériences des prisons mixtes n'ont pas fonctionné, un fait qui est non seulement connu, mais bien documenté. " Les femmes ont déjà été dans les mêmes établissements que les hommes. Ça ne marchait pas, parce qu'elles ont besoin de soins particuliers. Mais on revient malgré tout à ça!" Le Devoir, A1

***Inmate gets more jail time for destructive one-man riot**
A Saint John man will spend more time in jail for creating havoc during a drunken rampage at Dorchester Penitentiary in 2014. Terrance Joseph Keleher, 29, was sentenced Friday to 19 months in jail and ordered to pay $5,961.98 in damages to Correctional Service Canada after pleading guilty to a mischief charge related to the Aug. 23, 2014, incident at the medium-security prison. Court heard several inmates had made a brew at the prison that evening and a guard was called to Keleher's cell because he had a shank - a homemade knife - and a needle. When the guard went back to his station to await the arrival of an emergency response team to handle the situation, Keleher managed to get out of his cell and went on a rampage with a lead pipe. Times & Transcript, A8

***De retour en prison pour une histoire de contact sexuel et de leurre d'enfant**
Libéré puisqu'il contestait en Cour d'appel le jugement rendu contre lui dans une histoire de contact sexuel et de leurre d'enfant, un homme de l'île d'Orléans a désormais trois jours pour se constituer prisonnier puisque le banc formé de trois juges a maintenu sa culpabilité. En octobre 2013, Francis Drouin a été trouvé coupable de s'être offert des «soirées de gars» avec un ado de 13 ans où masturbation, fellation, pénétration digitale et pénétration pénienne étaient à l'honneur. En mai 2014, la juge Johanne Roy l'avait condamné à purger une peine de quatre ans de détention en rappelant que, «pendant une longue période et à de nombreuses reprises, vous avez profité de la vulnérabilité de la victime sans vous soucier des conséquences que vos gestes pourraient avoir sur elle». Agence QMI (Journal de Québec, 54; Journal de Montréal)

***Parole given to robber**
A P.E.I. man who was involved in a violent robbery of a drug dealer was recently granted full parole. Chase James Roper, 25, is serving a four-year sentence for several offences, including armed robbery, assault with a weapon and drug trafficking. In a recent report, the Parole Board of Canada said it was satisfied releasing Roper wouldn't result in an undue risk to the community and would help with his reintegration as a law-abiding citizen. Roper has been on day parole since last summer and the board's report said he successfully completed a substance abuse program. He has been participating in a methadone program and all of his urine samples have been clean, the report said. Charlottetown Guardian, A3

***Bring Back the death penalty**
Paul Bernado has applied for day parole. Things have not changed because this man was sent to jail. Crimes of the nature that put him behind bars are still being committed. Victims who lost their lives had no choice given to them after coming into contact with those who ended their lives. We imprison killers,

they get to wake up each day and sleep at night, put in their time and apply for parole. Kristen French, Leslie Mahaffy, Tammy Homolka, Tori Stafford, Noelle Paquette, and Tim Bosma have no such luxuries. London Free Press, E3

***Death of inmate at Collins Bay**
A 29-year-old inmate died at Collins Bay Institution's medium-security unit on Friday. A Correctional Service of Canada release states that Ryan James Henke was found unresponsive in his cell at around 1 p.m. Staff members responded immediately and emergency services were called, but the inmate could not be resuscitated. Kingston Whig-Standard

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

***Les armes longues plus utilisées pour les crimes**
Au moment où le débat fait rage sur la création d'un registre québécois des armes à feu, des données obtenues par Le Journal montrent que près de 80 % des armes saisies par la police après un crime ou un suicide sont des armes d'épaule. Ces statistiques inédites de la Sûreté du Québec révèlent également que pas moins de 20 555 armes à feu liées à un drame ont été confisquées par des corps policiers de la province sur une période de 20 ans, entre 1991 et 2011. Du lot, on compte 16 300 armes longues. Deux mois après le dépôt du projet de loi 64 du gouvernement Couillard visant à implanter un registre québécois des armes à feu, ces données ont de quoi contredire ceux qui s'y opposent. «Ça me surprend, mais il ne faut pas tirer de conclusions hâtives avec ces chiffres», insiste François Picard, président de «Tous contre un registre québécois des armes à feu». Agence QMI (Journal de Québec, Journal de Montréal)

Drug losses rise at small B.C. hospitals
The number of prescription drug thefts and losses has been rising at smaller B.C. hospitals over the years, with opioids most often disappearing, Health Canada data show. Across British Columbia, the units of narcotics lost have more than tripled, from 778 in 2012 to 2,416 in 2014. For the first half of 2015, the most recent statistics available, 1,710 units were lost. The problem, highlighted by the overdose death of Vancouver hospital care aide Kerri O'Keefe last August, has prompted B.C. Health Minister Terry Lake to write to all the province's health authorities and ask them to raise their narcotics security level. Globe and Mail, S1

Student confesses to creating shaming poll
A female student from Marystown Central High School has confessed to creating an online poll discovered last week by students from the school. Sgt. Larry Turner, with the Burin Peninsula RCMP, told The Southern Gazette Friday the student, who cannot be named under the Youth Criminal Justice Act, will not face charges in relation to the matter. The Southern Gazette broke the story about the poll this week. A release issued by the RCMP said the girl was apologetic and embarrassed by her actions. Police say they are satisfied the student understands the impact of what she has done, as well as the potential actions this could have caused. TC Media (St. John's Telegram, A9)

***Unseen but still there**
It was a weekday morning four days before Valentine's Day. Not the time most of us expect to see the street sex trade awake and at work. I was driving along Sargent Avenue, on my way to a news conference announcing the Joy Smith Foundation's launch of a public service campaign to educate us on what human trafficking looks like in Canada. Which, ironically, is when I noticed the first one standing alone on the sidewalk, skimpily dressed at -18 C. Then a second was further along. The first looked young and may not have been a sexually exploited girl. Police will tell you that, these days, it's harder to know for sure at first glance. The second was older, and it wasn't so hard to tell. She gave me a look - an out-of-it, drugged-up look. And a wave. The time was 10:45 a.m. McDonald's drive-thru was still serving breakfast. What police statistics officially categorize as "sex-trade workers" are out even earlier - during and even just before the morning rush hour - servicing men who are on their way to work. The scene on Sargent caused a flashback to a teenage girl I saw working Selkirk Avenue in November 2014. The body

of sexually exploited and slain 15-year-old Tina Fontaine had been found in the Red River just three months earlier. Now another potential Tina. "Where are the police?" I remember asking myself. Winnipeg Free Press

***Reserves need help**
An editorial states "three teenagers take their own lives in an eight-week period. A young police officer is shot dead responding to a domestic call, then the shooter turns the gun on himself. A report by Quebec's ombudsman describes horrific prison conditions, sometimes with seven or more detainees in cells intended for two, limited access to water, and no beds. The news coming out of indigenous communities in Quebec in recent days has been devastating. Immediate action is required. Of course, there is no quick fix. Any effort to bring about meaningful change in remote communities plagued by violence, suicide and substance abuse requires a deep examination of underlying causes, like rampant poverty, housing shortages and the legacy of residential schools. Public Security Minister Martin Coiteux is right to say the province must work with its indigenous peoples to find long-term solutions." Montreal Gazette, A10

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

***Work for reconciliation**
An editorial states "In this critical year of the Truth and Reconciliation Commission 94 Calls to Action for reconciliation among all the nations of peoples who live in Canada, Wilfrid Laurier University sided with, and amplified, the voices of survivors of Indian residential schools and families of murdered and missing indigenous women. The school did so after thoughtful discourse across the university community and wider publics. The real gift of patriots Jim Rodger and Dave Caputo is the resultant learning we've all been exposed to. This real gift of community engagement and learning is in perfect continuity with their legacy as educators who have empowered students, teachers and systems to lean toward informed dialogue with curious, open, hearts and minds. Because they brought the statue project forward there have already been responses to the Calls to Action, unlike the situation after the work of the much-ignored Royal Commission on Aboriginal People of 1996 which first told us these stories that we still are not ready to hear." Waterloo Region Record

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

Syrian family anxious for housing
Two rooms with two double beds and suitcases carefully tucked away around a desk in the corner of one room. It looks like an ordinary set of hotel rooms, but this is where a family of six Syrian refugees has lived for almost a month. "We're comfortable here," Aumaima Al Zrikat said through a translator. Her husband, Khaldoun Al Masalmeh, smiled in agreement. She said people in other countries are living in tents, so her family is grateful to be safe in Canada, even if they have been living in hotel rooms since Jan. 24. "It's kind of like a ray of light for our kids," she explained. Waterloo Region Record, A1

***Phone scammers swindle Syrian refugees**
A family of Syrian refugees in New Brunswick has lost about $400 after falling prey to a phone scam offering lessons to teach the English language. Saint John Police Sgt. Lori Magee says the family was contacted Monday by someone seeking money and banking information in exchange for the lessons. She says once the family's interpreter learned of the scam, he called the bank and police, but the money had already been taken from an account. Canadian Press (Chronicle-Herald, A9; Charlottetown Guardian, Ottawa Sun, Winnipeg Free Press, StarPhoenix, Montreal Gazette, Calgary Herald, Ottawa Citizen, Windsor Star, Times and Transcript, Edmonton Journal)

PUBLIC SERVICE / FONCTION PUBLIQUE

PS death benefits are in surplus
Canada's public servants are living so long their death-benefits account has a $2.6-billion surplus. That has some worried that the federal government could use the overage to offset its mounting deficit. The latest actuarial report by the Office of the Chief Actuary into the 60-year-old plan showed it had a $2.6-billion surplus after setting aside $642 million in death benefits obligations for 2014. The plan has been running surpluses for years and the report estimates it will hit $4.3 billion by 2039. The premiums and interest are not set aside, but instead go into the consolidated revenue account, from which the government also pays all benefits. That's one reason why the Professional Institute of the Public Service of Canada, which represents professionals from federal engineers to scientists, has long argued the fund should be transferred from the consolidated revenue account into a segregated fund. PIPSC Vice-President Shannon Bittman said, in a report, that federal unions should "keep close tabs" on the fund to ensure the "government doesn't amend the legislation" to allow them to claim the surplus. Postmedia News (Ottawa Citizen, A1; National Post)

Shared Services' other big problem: Data centres
After the pummeling it received this month from Auditor General Michael Ferguson, Shared Services Canada will be happy to focus on its next big project. Unfortunately, any respite is likely to be brief. The project itself looks pretty straightforward. Sometime in the next few weeks the government's computer services agency is expected to award a $450 million, 25-year contract to expand and maintain a flagship data centre at Base Borden, Ont. It's the context surrounding this procurement that's problematic for Shared Services. Ottawa Citizen, A4

OTHER / AUTRE

Coupes fédérales - Les libéraux publient des données retenues par les conservateurs
Le gouvernement libéral continue de révoquer les décisions qu'il reprochait à ses prédécesseurs. Le fédéral a remis vendredi au directeur parlementaire du budget une ventilation partielle des compressions imposées à l'appareil fédéral par les troupes de Stephen Harper depuis 2012 -- et tenues secrètes jusqu'ici. " C'est une priorité pour nous de rétablir une culture de transparence comme gouvernement, et donc c'était important de rendre publique cette information ", a fait valoir le président du Conseil du Trésor, Scott Brison, vendred (...)Bien que le tableau du ministre Brison distingue les sommes coupées parmi les diverses agences ou divisions des ministères fédéraux, les sous-catégories demeurent vagues. Ainsi, les données montrent que le ministère de laSécurité publique a perdu 687,9 millions par année -- dont 24,4 millions ont été retranchés au Service canadien du renseignement de sécurité, 295 millions à Service correctionnel Canada, 195 millions à la Gendarmerie royale du Canada et 143 millions à l'Agence des services frontaliers. Mais le document se contente d'indiquer que l'Agence a " rationalisé les services internes " pour économiser 63,9 millions, " transformé les services internes " pour économiser 22,6 millions, et " transformé les programmes " pour épargner 31,6 millions. Le Devoir, A2

***Defence chief on defensive**
The country's top military commander was dragged Friday into the long-standing political debate of what constitutes combat in Iraq, even as the Trudeau government comes to grips with the imploding situation in Libya, where U.S. warplanes have struck extremist training camps. The bombings are seen, potentially, as the opening round in a new front against the Islamic State of Iraq and the Levant, which has for months been building up its presence in the civil war-torn North African nation. A year ago, Gen. Jonathan Vance's predecessor struggled to explain to a House of Commons committee how firefights involving special forces troops and guiding airstrikes for Kurdish forces was not considered combat. It was Vance's turn on Friday, as he rejected categorically the suggestion that his definition of combat was made to measure for the Trudeau government's political needs. "I reject that totally," Vance said. "I am the expert in what is and what is not combat." Canadian Press (Chronicle-Herald, A7; Cape Breton Post, Red Deer Advocate, Times Colonist, Telegraph-Journal); Postmedia News (Ottawa Citizen, London Free Press); Globe and Mail

***Middle East's choppy waters**

An opinion piece states "(…) The situation facing the Canadian government today is not necessarily more dangerous, but it is far more complicated than it used to be. Among the factors that make the contemporary Middle East so complex are: (a) the rise of Islamist extremism and terrorism; (b) raging civil wars in Syria and Yemen; (c) the virtual collapse of the Iraqi state; (d) the intensification of the hostile competition between Shia Iran and Sunni Saudi Arabia; (e) the adversarial relationship between the Turkish government and its Kurdish population; and (g) the collapse in the price of oil. All of this makes policy formulation powers to contribute to the peacekeeping forces in the Middle East." Until the early 1970s, the Arab-Israeli conflict remained Canada's main focus in the region. It was why Canada established embassies in Tel Aviv, Cairo and Beirut to monitor the situation. At that time, however, Canada began to broaden its perspectives and interests in the region." Kingston Whig-Standard

INTERNATIONAL

Cyclone Winston: Category five system hits Fiji; curfew declared amid fears for those outside cities

Tropical Cyclone Winston has made landfall on Fiji's main island, bringing damaging winds and huge ocean swells towards the capital Suva. "For the next several hours, most of the population around the northern coast of Viti Levu will experience destructive winds," chief meteorologist Ravind Kumar said. He said the rest of the country would also experience "very destructive" winds and "torrential rainfall" as the cyclone continued to move. The Fijian Government issued a curfew for the whole of Fiji, taking effect after 6:00pm local time. ABC

Spy agencies share intelligence

European intelligence agencies plan to boost their fight against Islamic militants by creating a virtual network to share information among up to 30 countries, officials said Friday. The Counter Terrorism Group -a discreet and informal grouping of domestic spy agencies from the 28 European Union countries, Norway and Switzerland-aims to create the new platform by July 1, according to a joint statement by German and Dutch intelligence agencies. The Nov. 13 attacks in Paris by extremists linked to the Islamic State group, which left 130 people dead, prompted renewed calls for greater cross-border intelligence co-operation in Europe. Associated Press (London Free Press, B4; Chronicle-Herald)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Sent to: PS.F DL_DMS F.SP + !DMS External +CBSA Today's News + CSC & PBC Today's News + RCMP Today's News + RCMP Today's News 2

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
February 21, 2016 / le 21 février 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

BC avalanche claims another life
An avalanche in BC's mountains has killed yet another snowmobiler. The avalanche near Golden on Saturday swept away four snowmobilers. A 30-year-old Calgary man was killed, and a fellow rider from Winnipeg had to be hospitalized. The two others, also from Calgary, did not need treatment. Avalanche Canada had issued an avalanche warning as potentially deadly snow conditions develop on slopes across parts of eastern and southeastern British Columbia. News 1130; Canadian Press (Edmonton Sun, A25; Calgary Sun, Ottawa Sun, Winnipeg Sun, Toronto Sun, London Free Press, Times Colonist, Vancouver Sun, Charlottetown Guardian, St. John's Telegram); Calgary Herald; Vancouver Province

Emergency crews practice rescues at Silver Star
The sun is shining and snow conditions are ideal for Emergency Services Day at Silver Star Mountain Resort, benefiting the Vernon Jubilee Hospital Foundation. Free live showcases will be taking place in the village throughout the day including simulated ski patrol lift evacuations, fire rescue crew rope rescues and jaws of life extrications, search and rescue helicopter winch rescue demos, an RCMP police dog demo and more. Twenty dollars from every lift ticket sold on Saturday will also be donated to the Vernon Jubilee Hospital. Global News

Toronto company using big data to predict the spread of Zika
Wayne Gretzky may be an unlikely inspiration for an infectious disease researcher. Yet here Dr. Kamran Khan is, on a demonically busy Monday evening, referencing the Great One. "Skating to where the puck is going, not where it's been" - this is Khan's goal for himself and his colleagues at BlueDot, the company he launched to help decision-makers prepare for and respond to infectious disease outbreaks. Since January, when the Zika virus sent public health officials in Brazil scrambling, Khan has been deluged with requests - everyone from the BBC to the CDC (the U.S. Centers for Disease Control). Conceived in the wake of Toronto's 2003 SARS outbreak and launched in 2013, BlueDot, housed at St. Michael's Hospital's Li Ka Shing Knowledge Institute, draws on big data to create predictive models of where, when and how an outbreak will spread - not where the puck is, but where it will be. Sports teams, stock markets, climate science and election campaigns have all been transformed by mathematical modelling. Likewise, infectious disease modelling has become a critical piece in the public-health tool kit, especially during epidemics and emergencies. But disease modellers grapple with unique disadvantages. "One of our big challenges is really related to data availability," says Amy Greer, Canada Research Chair in population disease modelling at the University of Guelph. Toronto Star, IN1

Home-made hope
A Winnipeg-based lab is set to begin production on the first Zika vaccine. Scientists at the National Microbiology Laboratory (NML) gained international prominence last year for their Ebola vaccine, which quickly proved a "game-changer" that protected everyone who received it. Now, only days after most people learned the word "Zika," the Winnipeg-based researchers may have done it again. The lab's head of special pathogens said last month they could have a vaccine to combat the mosquito-born illness ready by year's end. "This vaccine is easy to produce. It could be cranked to very high levels in a really short time," Dr. Gary Kobinger told Reuters. Canadian Press (Winnipeg Sun, A6)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Snowden to make cyber visit to Simon Fraser University
A man considered everything from a heroic whistleblower to a traitor is making a cyber visit to British Columbia. Edward Snowden will make the keynote presentation, via web link, as part of a Simon Fraser university program examining the opportunities and dangers of online data gathering. The presentation, at Vancouver's Queen Elizabeth Theatre on April 5, will be followed by a moderated discussion with expert panellists from SFU and the B.C. Civil Liberties association. Snowden is a former employee of the national Security agency in the United States. Canadian Press (Edmonton Sun, A30

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Can caper crushed
An Alberta recycling company is fighting one of the largest administrative penalties ever levied after Alberta Environment slapped it with an $844,778 fine for collecting refunds on out-of-province beverage containers. The massive penalty against Alberta Reclaim and Recycling and owners Johnny Ha and Shawn Diep includes a $769,778 "economic benefits assessment" that is being challenged before the Environmental Appeals Board (EAB) this spring, according to board spokesman Gilbert Van Nes (...) The elaborate plan was uncovered when Canada immigration officials were directed to a warehouse in northwest Edmonton after receiving a tip that illegal immigrants were working there. Immigration officers found several illegal immigrants pulling apart bales of crushed cans and beverage containers and placing

them into plastic garbage bags (…) The penalty against Reclaim and Recycling was levied by Alberta Environment on Feb. 20, 2015, after a two-year investigation that involved Canada Border Services Agency, environmental protection officers, Edmonton police, private investigators and CN Police. Edmonton Sun, A4

Parole-jumping sex offender found guilty in Seattle rape
A former Edmonton man and high-risk sex offender who escaped Canada in 2013 has been found guilty of raping a 69-year-old woman in Seattle. Michael Stanley, 49, triggered a manhunt across Saskatchewan and Alberta when he cut offhis ankle bracelet in Lloydminster on the boundary of the two provinces and made a run for the U.S. border, where he managed to cross unchallenged. At the time, Canadian authorities alerted their U.S. counterparts about Stanley, but they determined he was a U.S. citizen and they had no reason to arrest him, so let him enter the country, while Canadian officials decided not to ask for his extradition. Stanley has a long history of crime, including sexually assaulting disabled children and an 82-year-old woman in Lethbridge, Alta. Canadian Press (Edmonton Sun, A5; Calgary Sun)

An American export Canadians don't want
An opinion piece states "The United States is to Canada what Mexico is to the United States: the reason for border trouble. The U.S. gets illegal immigrants smuggled from Mexico; Canada gets illegal guns smuggled from the U.S. But who, pray tell, gets the worst of it? Much is made about the impact of illegal immigration on states along the southern U.S. border. But what about the impact of illegal weapons making their way into the country to our north? Smuggled firearms from the United States are fuelling bloodshed in Canada. A couple of sentences from a story in The Washington Post this week by William Marsden said it all: "Homicides in Toronto spiked to 80 in 2005, from 64 in 2004, and the majority were shooting-related. About 70 per cent of the guns used were handguns and automatic weapons smuggled from the United States, police say." While the number of shootings has decreased, gun seizures by the Canadian Border Services Agency reportedly are up: 226 illegal weapons were seized in 2012, most of them handguns; there were 316 by 2015. To be sure, gun-violence numbers in the U.S. swamp Canada's: There were 156 gun-related homicides in Canada in 2014, Marsden reported, compared with 10,945 the same year here." Waterloo Region Record

Stop detaining migrants without cause
An opinion piece states "When 16-year-old Mohammed's parents helped their son flee to Canada, they surely could not have imagined that their child would be held in immigration detention and much less that he would be put in isolation for three weeks. But indeed, this is how the Canada Border Services Agency (CBSA) treated the arrival of this unaccompanied and vulnerable youth. Mohammed's family had fled Syria for Egypt and when Mohammed's permit expired, rather than risk deportation to Syria, his parents did what any parent would do: try to protect their child. Mohammed flew to the U.S. and then presented to the Canadian border to make a claim for refugee protection. Unaccompanied minors may claim asylum in Canada, even if they have travelled through the United States, but due to a technicality, the CBSA officer who greeted Mohammed deemed him "ineligible" to claim refugee status and promptly sent him to immigration detention. If only Mohammed (to protect his privacy, we're not using his real name) were an exceptional case. In truth, hundreds of innocent migrant and refugee children find themselves in immigration detention centres each year in Canada, as do thousands of adults. Babies, children and adolescents are held in Montreal and Toronto in what are essentially medium security prisons, surrounded by high razor-wire fences, staffed by guards, where children are denied regular schooling, held to rigid schedules, pervasively understimulated and live with a sense of uncertainty and fear." Toronto Star, A11

CYBER SECURITY / CYBERSÉCURITÉ

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Richmond asking residents whether they want a non-RCMP police force
For Richmond residents, twenty cents of every tax dollar they pay the city goes towards paying the RCMP. Now, city council is asking for public input over whether or not to replace the Mounties and adopt an independent municipal police force. The city's mayor admits it's a conversation that's been going on for years. "What I want to know is what people think of making a change and if they're prepared to make a change, are they willing to pay the cost of making that change," said Malcolm Brodie. The city pays $41.5 million every year for the RCMP's services. Making the switch to an independent municipal force would cost about two to four million dollars more, along with a one-time transition cost of $19.6 million. Global News

Hells Angels plead guilty in trafficking conspiracy
Three of eight men charged after police targeted the Hells Angels in an elaborate international sting operation have quietly entered guilty pleas. The pleas of Kevin Van Kalkaren, Murray Elmer Trekofski and Orhan Saydam in connection with a major cocaine conspiracy were initially subject to publication bans imposed by the trial judge, B.C. Supreme Court Justice Carol Ross. But details of the pleas can now be reported. The judge lifted the publication bans after the five remaining accused - David Giles, vice-president of the Hells Angels' Kelowna chapter; Bryan Oldham, sergeant at arms of the Kelowna chapter; and Hells Angels associates James Howard, Michael Read and Shawn Womacks - re-elected to be tried by judge alone on Friday. The most recent plea was entered earlier this year by Van Kalkaren, who played a bigger role in the conspiracy than Trekofski and Saydam, who have both already been sentenced after entering their pleas in 2014. Vancouver Province, A14

Four charged after Chilliwack dial-a-dope sting
Four people have been charged in connection with a Chilliwack diala-dope operation dismantled last year during an undercover police investigation. In the fall of 2014, B.C. Mounties received reports of heroin allegedly being sold by a dial-a-dope organization on a property in the 8100-block Young Street.
Later that year, the RCMP's crime reduction unit launched an investigation that sent undercover officers to buy heroin from a suspect. "As police pursued their investigation, the quantity of drugs sold in each covert sale increased, along with officers also being offered brass knuckles equipped with built in conducted energy weapons for purchase," read a media release announcing the charges. From January to March of 2015, undercover cops conducted six more drug purchases from the suspect, with each transaction captured on surveillance by investigators. As a result, investigators identified two Chilliwack addresses as being connected to the dial-a-dope operation, one in the 10000-block Woods Avenue, the other in the 9300-block Nowell Street. In March and April of 2015, RCMP executed a search warrant on each of the two properties. At the first home, police seized six grams of methamphetamine, more than 490 g of phenacetin, 570 pills containing MDMA and TFMPP, approximately 360 g of TFMPP, four firearms, a conducted-energy weapon, cash and evidence of drug trafficking. Vancouver Province, A13

Fort McMurray RCMP determine abduction report unfounded
Police in Fort McMurray have called off the search for a teenage girl after determining she was not abducted. On Thursday at 8:30 a.m., a witness saw an older man grab and drag a kicking girl into a white SUV outside Fort McMurray's Holy Trinity High School, RCMP Cpl. Wanita Patey said.
No one of the girl's age or description was been reported missing to police or the school, but RCMP began an investigation. Officers began knocking on doors of more than 80 people in the area who own a white Chevrolet Equinox. Edmonton Journal

Threat brings police to school Monday
A threat against an employee scrawled on a bathroom cubicle wall at St. Albert's Paul Kane High School has prompted RCMP to send officers to the school on Monday, police say. A student visiting the school for a sports match Wednesday discovered the threat in the bathroom and told a coach, who alerted school staff, Paula Power, a St. Albert Public Schools spokeswoman, said on Saturday. RCMP spokeswoman Cpl. Laurel Scott said the threat was not signed, and police have not yet identified any suspects. A letter from the school sent to parents Friday said RCMP are coming to the school Monday as a necessary precaution. Edmonton Sun, A6

RCMP to wear pink
Two Penticton RCMP officers will be wearing pink shirts to promote anti-bullying awareness on Feb. 24. Cpl. Jas Johal and Cpl. Don Wrigglesworth will visit local schools and speak to students about the power of speaking out against bullying. In support of National Pink Shirt Day – raising awareness against bullying – RCMP across the province are wearing pink to show their support. "Raising awareness on the issues and standing together in pink with our communities, allows us to take a collective stance and show there is no tolerance for this behaviour," said Deputy Commissioner Craig Callens, commanding officer of the B.C. RCMP. Castanet

Legalizing marijuana: let's get this right
An opinion piece states "the legalization of marijuana in Canada now appears to be a question of when and how, not if. The new federal government has committed to this initiative and is now looking at how to implement it. A large part of our society believes marijuana is a relatively harmless substance, but that isn't entirely true. The impact of marijuana on an adolescent's brain can be severe. In fact, study after study has shown that frequent marijuana use by young people can have a number of negative effects and leave lasting impairments on a brain that is still growing and developing. In a recent report, for example, the Canadian Centre on Substance Abuse states that "early and frequent [marijuana] use can seriously limit a young person's educational, occupational and social development, and some of these adverse effects may be irreversible." Toronto Star

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Halfway house worker attacked by gunmen before fatal shooting, jury hears
The jury in a Vancouver murder trial heard Friday from a halfway house worker who was pistol-whipped just prior to the fatal shooting of a resident at the home. In a videotaped statement, Roger Woelke described how two armed men burst into the halfway house near Cambie Street in Vancouver, both of the men smelling of booze. Woelke, who has since died of natural causes, said the two suspects were dressed head to toe in black and had bandanas or masks covering their faces. The two men screamed, "Where's Randy? Where's Randy?" Woelke told then-Vancouver police homicide Sgt. Laurence Rankin in an interview four days after the September 2009 slaying of Raj Soomel. Woelke said he mistakenly told the men that a resident of the home named Randy Naicker, who had recently been released from prison on parole, had gone to a nearby store. Vancouver Province, A18

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

The invisible dead
Brad Chapman collapsed in the doorway of a Walton St. nail salon in downtown Toronto just before dawn last Aug. 18. Cocaine, opioids and amphetamines coursed through his body; they were the long-time drug user's preferred substances. Homeless, the streets were Chapman's haven for 20 years when he wasn't in jail. Those dire circumstances for the father of three were a world apart from the middle-class comfort of Etobicoke, where Chapman was raised by a loving family, competed in rep hockey, learned French and played piano by ear. A security guard making his rounds shortly before 5 a.m. at the Chelsea Hotel, just steps from the nail salon, noticed a man slumped over in an alcove. To the man's left lay a syringe, spoon and a cigarette lighter; to his right, an empty Crown Royal bottle, a police report would later note. The concerned guard, George Plaier, called 911. The man, later identified as Chapman, was dying. He would soon become part of Ontario's growing ghost population: The uncounted homeless dead. Toronto Star, A1

Country singer helps the PTSD fight with benefit concert series
Music is said to be a healer. But a Canadian singersonger is taking that one step further by using a series of concerts to raise money to fight Post-Traumatic Stress Disorder. Winnipeg-born country singer Jessie Williams, who brings her House Concert Series to Edmonton on March 5, hopes to raise $500,000 for PTSD-related charities during her tour of more than 60 towns and cities across Canada over the year.

"First responders and the military cover a wide range of our nation," said Williams. "So it's imperative that we do something to help them be able to access more programs and provide the resources to them for different therapeutic processes. "Because not one process works for everybody." Edmonton Sun, A7

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Indigenous law could play role in inquiry
Indigenous Affairs Minister Carolyn Bennett says she is considering ways to incorporate indigenous law into the national inquiry on missing and murdered aboriginal women. The Native Women's Association of Canada and the Feminist Alliance for International Action published a list of recommendations for the upcoming national inquiry that argued mainstream Canadian law had failed to adequately address the problem of violence against indigenous women. "Missing and murdered indigenous women are a consequence of state lawlessness created by Canadian law's inability to deal with the ongoing aftermath of colonialism and its attendant violence," says the report, published last week, based on discussions at a symposium on the inquiry that took place at the University of Ottawa last month. "These spaces of lawlessness are also the result of the denial of indigenous laws and legal orders since the arrival of settlers. The inquiry must not perpetuate the undermining and erasure of indigenous laws and legal orders." Toronto Star, A4

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

GOP senator 'a little concerned' about refugees in Canada
Sen. Ron Johnson (R-Wisc.) on Sunday said he is "a little concerned" about radical Islamic terrorists posing as refugees entering Canada. The Wisconsin lawmaker said Canadian Prime Minister Justin Trudeau expedited the process of approving asylum seekers in the wake of the Syrian refugee crisis. "Of course, with Prime Minister Trudeau's announced plan of basically tripling the number of refugees to bring in – we held a hearing about this, actually," Johnson told radio show host John Catsimatidis on AM 970 New York. "And on average, prior to this program, it would take about 62 months for Canada to properly vet a refugee," he added. "Now they're going to triple the number they're going to let in, and they're going to do it in less than 12 months." The Hill

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

NIL

INTERNATIONAL

Michigan shootings: At least seven killed in US city
US police have publicly identified a man suspected of driving around the Michigan city of Kalamazoo and randomly shooting people. Kalamazoo department of public safety chief Jeff Hadley named the suspect as Jason Dalton, 45, of Kalamazoo county, the AP news agency reported. Dalton reportedly has no known criminal history. Michigan police earlier launched a manhunt after six people were killed and several others were injured in seemingly-random shootings near a Kalamazoo car dealership and

restaurant late on Saturday night. Al Jazeera English; Associated Press (Toronto Star, CBC News, CTV News)

Fiji super cyclone kills five, raises fears of health crisis
Downed power lines and flooding are hampering relief efforts in Fiji after one of the most powerful storms recorded in the southern hemisphere tore through the Pacific island nation, flattening remote villages and killing at least five people. Harsh winds and torrential rains tore up homes and cut power, water and communications links across the nation of about 900,000 people, although Suva, the capital, escaped the brunt after the storm changed direction at the last minute. Prime Minister Frank Bainimarama confirmed the death toll and declared a 30-day state of emergency, with schools ordered to shut and a nationwide curfew extended until Monday morning. "When we are able we will provide timelines for the return of water and power," he said, adding that electricity supply to some areas had been deliberately cut to avert further damage. Reuters

Syria's Homs hit by deadly twin car bombings
Homs city is largely under government control and has regularly been targeted in bomb attacks, including a deadly double bombing last month that killed at least 22 people and was claimed by the Islamic State of Iraq and the Levant (ISIL). The bombings came as Syrian government forces continued to tighten their grip around Aleppo province, as they push for the Islamic State of Iraq and the Levant's (ISIL) stronghold in Raqqa. The Observatory said on Sunday that government forces backed by Russian air strikes have captured 18 villages in Aleppo's eastern suburbs - giving them access to 40km of the highway between Aleppo and Raqqa. Al Jazeera English

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Sent to: PS.F DL_DMS F.SP + !DMS External +CBSA Today's News + CSC & PBC Today's News + RCMP Today's News + RCMP Today's News 2

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
July 31, 2015 / le 31 juillet 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via Infomédia

MINISTER / MINISTRE

*** Border crossings getting upgrades**
Border crossings at Carway and Del Bonita will soon be part of a federal $113-million modernization project. MP Jim Hillyer, on behalf of **Steven Blaney**, **Canada's minister of Public Safety and Emergency Preparedness**, announced Thursday that the Harper government will invest the estimated amount to improve infrastructure at ports of entry in the Prairie region. "***By investing in border infrastructure at the Carway and Del Bonita ports of entry, the Harper Government is helping support the economy in Alberta,"*** Hillyer said. The infrastructure investment includes design finalization, site services, geotechnical and environmental assessments, as well as modular building construction, including structural, mechanical, electrical, internal fit-up, commissioning, project management and signage. Construction work is planned to begin in 2017. The $440-million border infrastructure investment, combined with previous Beyond the Border infrastructure commitments, is anticipated to provide a major upgrade to ports of entry. Lethbridge Herald

*** Twenty-eight years since infamous Black Friday tornado**
Friday marks the 28-year anniversary of Black Friday, when a large tornado ripped through southeast Edmonton and Strathcona County on July 31, 1987. The F4 tornado, which was a mile wide at its widest point and brought winds clocked at between 300 and 400 km/h, is known as the second deadliest tornado in Canadian history, behind only the Regina cyclone of 1912, which killed 28. The tornado left 27 people dead and injured 600 others. A further 1,700 people were forced to evacuate their homes. Rivers rose up to eight metres in some areas due to heavy rains. On top of the loss of human life, Black Friday resulted in hundreds on millions of dollars in damage. The most costly damage in dollar terms was caused by the

hail that accompanied it. Estimated total cost to government was $32,748,959. Total damage costs, according to **Public Safety Canada**, was $662.3 million. Edmonton Sun, 4

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

***Drought effects linger, study shows**
New research suggests that Canada's drought-stricken forests will take years longer to recover from dry weather than previously thought. In a study published in Science magazine, William Anderegg of Princeton University said trees feel the lingering effects of a drought for up to four years. "Drought is always (thought of) as a light switch: when it's dry, trees grow slowly, but the moment the rains come back and the soil gets wetter, it's like the trees recover perfectly and almost immediately," he said. "It turns out it doesn't work like that." The study could lead to changes in forest management, Anderegg suggested. Because wildfires are routinely suppressed, many forests are denser than they would naturally be. "That leaves them vulnerable to drought, large forest fires and insect outbreaks. Things like thinning out the density of trees would certainly increase resilience." Canadian Press (Edmonton Journal, A7; Edmonton Sun, Times and Transcript)

***Reservists were ready to help**
I wish to thank the people of Saskatchewan for their support in allowing my soldiers from 38 Canadian Brigade Group the time away from their families and work in support of the forest firefighting north of Prince Albert. 38 Canadian Brigade Group, the army reserves of Saskatchewan, Manitoba and Northwest Ontario, have a proud history of serving in domestic operations, specifically during the floods in Manitoba. Our "citizen" soldiers, train together throughout the year, learning how to work as a team in austere conditions. We come together, prepared because of training that demands sacrifice from the families and employers of reservists. On July 4, the province of Saskatchewan made the request for help to the Canadian Armed Forces. It was not long after that I started receiving requests for the reserve units of Saskatchewan to help supply the much-needed manpower. Within hours, my soldiers - from Prince Albert, Yorkton, Moose Jaw, Regina and Saskatoon - responded to this call for assistance. Col. Geoff Abthorpe, Thunder Bay Abthorpe is commander of 38 Canadian Brigade Group. Leader-Post, A6

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Cairo court delays releasing verdict in Fahmy's trial
Mohamed Fahmy's legal saga was drawn out further on Thursday as an Egyptian court abruptly postponed a much-anticipated verdict in his widely denounced terror trial. The Canadian journalist - who was first arrested 19 months ago - expressed frustration at the delay, which will now see him return to a Cairo court on Aug. 2. "It's just mind-boggling the way they continue to play with our emotions here," Fahmy told The Canadian Press. "It's very hard on everyone." Fahmy said his lawyers have confirmed that the case is expected to be back in court on Sunday, but there was speculation that date could be pushed back as two judicial officials speaking on condition of anonymity said the judge was seriously ill. "I took a bag to court today with towels, a toothbrush, slippers ... just in case I was sentenced," Fahmy said. "This is how our life is so controlled by this ordeal ... it's just really, really stressful." Fahmy added that he and his fiancee, Marwa Omara, had married each other. "We couldn't celebrate because we were very anxious," he said. "I wanted to complete the marriage before the verdict because if we were married, Marwa could easily visit me in prison."... Canadian Press (Windsor Star, D1/Front, Toronto Star, A11, Red Deer Advocate, Ottawa Sun, Leader-Post, Gazette, Ottawa Citizen, C2, National Post, A6, Edmonton Journal, Calgary Herald, Ottawa Sun); Presse Canadienne (Le Droit, 19, Le Devoir, A2); Globe and Mail, A3

*** WikiLeaks says U.S. spied on Japanese government officials**
The WikiLeaks website published documents Friday that it says shows the U.S. government spied on Japanese officials and companies. The documents include what appear to be five U.S. National Security Agency reports, four of which are marked top-secret, that provide intelligence on Japanese positions on

international trade and climate change. They date from 2007 to 2009. A notation on one of the top-secret reports on climate change before the 2008 G8 summit is marked for sharing with Australia, Canada, Great Britain and New Zealand, according to WikiLeaks. It's not clear if it was actually shared. The organization also posted what it says is an NSA list of 35 Japanese targets for telephone intercepts including the Japanese Cabinet office, Bank of Japan officials, Finance and Trade Ministry numbers, the natural gas division at Mitsubishi and the petroleum division at Mitsui. The Japanese government and the two companies had no immediate response to the postings, which went up on the WikiLeaks website late afternoon Japan time. The validity of the documents could not be independently verified, though WikiLeaks has released U.S. government documents many times in the past. Three of the apparent NSA reports deal with climate change, and the other two with agricultural trade issues, including U.S. cherry exports to Japan. WikiLeaks has released similar documents in recent weeks that it said show NSA spying on Germany, France and Brazil. U.S. spying on its allies became an issue in 2013, when WikiLeaks released documents leaked by former NSA contractor Edward Snowden that showed the NSA had been eavesdropping on the cellphone of German Chancellor Angela Merkel. CBC News; BBC News

*** How the UK is countering Islamism**

An editorial states "I recently returned from the UK, where I had the chance to observe Muslim communities and learn about government policies that affect them. These policies may have a bearing on how we handle Islamist extremism and counter- radicalization efforts in Canada. British Prime Minister David Cameron recently outlined a sweeping, five-year deradicalization plan after the terrorist slaughter of British vacationers on a Tunisian beach in June. He explained the major components of the UK's Counter- Terrorism and Security Act to an audience in Birmingham. The overall strategy primarily addresses the disturbing phenomenon of hundreds of British Muslims joining ISIL. The act includes measures to counter the tenets of Islamism, identify people who promote radical ideas, enable "moderate" Muslims and encourage Muslim integration. The five-year plan also seeks to address Muslim grievances with the West. As Cameron put it, when apologists for terrorism, "say that these are wronged Muslims getting revenge on their Western wrongdoers, let's remind them: from Kosovo to Somalia, countries like Britain have stepped in to save Muslim people from massacres. It's groups like ISIL, al-Qaida and Boko Haram that are the ones murdering Muslims." ... Postmedia News (Ottawa Sun, 23, Edmonton Sun, 15, Calgary Sun, 15, Toronto Sun)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Hammer attacker faces deportation

The man who tried to kill a 13-year-old in a hammer attack will likely be sent back to Iraq, the same place he left as a refugee more than a decade ago. Rafid Jihad was convicted of attempted murder in May in the savage attack that left teenager Jacob Mitchell with a fractured skull. Jihad is very likely to lose his permanent residency and subsequently be deported, his defence lawyer Frank Retar said in Superior Court Thursday afternoon. The law says permanent residents lose their status if sentenced to longer than six months, or if convicted of a serious crime that comes with a maximum sentence of 10 years or more. Both the Crown and defence submissions for a sentence are longer than six months. Retar asked the judge for a 44-month jail sentence, less about 21 months of time already served. Assistant Crown Eric Costaris argued for six to eight years in jail. The maximum sentence for attempted murder is imprisonment for life. "I believe he will be deported and return to Iraq," Retar said after the hearing. "Rafid Jihad is looking forward to putting this behind him. He's actually looking forward to - and has said more than once - his intention is to return to Iraq." Retar said Jihad came to Canada in 2002 as a refugee. The Christian Iraqi's mother and two sisters live here. His father died two years ago. Retar said it appears Jihad has no concerns about returning to Iraq. "He has uncles there. He came from there. Since coming to Canada he has returned to visit twice to visit for lengthy periods of time," he said. Mitchell's mother Rosa said she just wants to see a resolution soon, to give closure to her family and the rest of the community. Windsor Star, A3

Le mandat d'arrestation levé

L'ambiance confinée est beaucoup moins oppressante et une aura d'allégresse s'échappe même des lieux. Un poids immense vient de tomber des épaules de la famille kurde réfugiée depuis janvier dans le sous-sol de l'église Saint-Michel, à Rougemont. Ils peuvent enfin sortir marcher, travailler et vivre dans une maison qui sera la leur. Depuis le 23 juillet, le mandat d'arrestation qui pesait contre eux pour les renvoyer dans leur pays d'origine, la Turquie, a été levé par les agents des services frontaliers. Pour ce faire, ils ont eu à se rendre à Sherbrooke pour faire une nouvelle demande d'Examen des risques avant renvoi (ERAR), malgré la crainte d'être arrêté en chemin ou encore sur place. « On avait une crainte, mais au retour, on était très contents », lance Kamber Turk, père de trois filles. Selon lui, l'accueil était plus favorable à Sherbrooke qu'à Montréal. « Les gens de Sherbrooke étaient très gentils et ils se sont bien occupés de nous, renchérit sa femme Ceylan. Je pense qu'on avait peur pour rien. » La première chose que le couple et le frère de Kamber, Orhan, ont faite ? « On a appelé nos proches pour leur dire qu'on était libres. » Dès le lendemain, Ceylan prenait sa première marche avec les enfants. « La journée qu'on est allés à Sherbrooke, j'ai eu mal à la tête. C'était la première fois que je sortais et on était stressés. Le vendredi, j'ai amené les enfants pour prendre une marche. C'était un peu bizarre », dit-elle en riant. Orhan compare la situation à une douche bouillante et difficilement supportable, qui vient de s'arrêter. « On respire mieux. » La Voix de l'Est, 2; La Presse

'Inhumane' to deport bank robber, lawyer says

The lawyer for a Yemenborn convicted bank robber who has been behind bars for more than 20 months plans to take her client's case to Federal Court of Canada for the third time after the Immigration and Refugee Board ruled Thursday he can now be deported to Yemen. Arghavan Gerami, the lawyer representing 26-yearold Ahmed Ali Ahmed, said she plans to ask the Federal Court to order her client's release because there's no way he can be deported given the current security situation in Yemen. Ahmed has been in immigration custody since he finished a two-year robbery sentence and has been deprived of the reconstructive surgery he needs for a torn ligament in his knee, Gerami said. "Even if you're going to try to remove him, it's inhumane in his medical condition to send him to a war zone where he will have no access to medical care," Gerami said. "His continued detention, based on the new medical evidence that we have, constitutes cruel and unusual treatment." Gerami argued that the Canada Border Services Agency's fourth attempt, planned for August, to deport Ahmed to Yemen will likely fail, which would result in his continued detention. Previous attempts to deport him have been thwarted because the airport in Yemen has been closed. It has since reopened, but only for aid to be delivered by military planes, she said. At Ahmed's last detention review on Thursday - he is afforded one every 30 days - the board found he was still a flight risk and a danger to the public. Ahmed's criminal record includes sexual assault, robbery and forgery convictions. Ottawa Citizen, A10

Man jailed in child porn smuggling

A French citizen caught bringing child pornography into the country has been sentenced to 90 days in jail. Nicolas Michel Clement Roux, 25, was arrested July 16 at Halifax Stanfield International Airport after he arrived on a Condor Airlines flight from Frankfurt, Germany. During a secondary customs examination, a Canada Border Services Agency officer found 244 animated images of child pornography on a memory card in Roux's tablet computer. Roux pleaded guilty Thursday in Dartmouth provincial court to a Customs Act charge of smuggling child pornography and a Criminal Code charge of possession. Crown attorney Perry Borden told the court the anime on the memory card featured characters as young as nine being sexually abused. Roux will be deported after he gets out of jail, Borden said. Defence lawyer Ron Pizzo said his client is studying for his master's degree in France and the convictions will affect his career choice and his ability to travel in the future. The incident has been "a wakeup call" for Roux, Pizzo said. "He understands he may need help." Chronicle Herald, A8

Deportation of man found with gun cache in Peterborough stalled

High-level talks are taking place between Canada and Pakistan over the fate of a Pakistani terrorist group member who has been detained at the Central East Correctional Centre in Lindsay for the past nine months after being found with a gun cache in Peterborough in 2012, a federal official says. Mohammed Aqeeq Ansari was to be deported back to Pakistan on July 14 but his removal was called off at the request of Pakistani authorities, the Canada Border Services Agency official disclosed at a hearing in Toronto. Although Ansari holds a valid Pakistani passport, officials have asked to interview him at their

consulate in Toronto. The CBSA said Pakistan was conducting "verifications." Otherwise, it was unclear why they had halted his return. "Honestly speaking I have no idea at all," said Asghar Ali Golo, the Consul General of Pakistan in Toronto. He said he had just returned from Pakistan and was unfamiliar with the case but would be able to answer questions on Monday. The Department of Foreign Affairs and the Pakistani High Commission in Ottawa are now involved, the CBSA said. The head of Canada's mission in Islamabad was to discuss the issue with Pakistan's Ministry of Interior on July 27. "We're trying to move this along locally, national and internationally. The agency is doing everything it can to get approval to remove Mr. Ansari," Jessica Lourenco, a CBSA official, told the Immigration and Refugee Board at a hearing to decide whether he should remain in detention. A landed immigrant, Ansari has lived in Canada since 2007. He was arrested in Toronto on Oct. 27 on the grounds he was a member of the Pakistani terrorist group Sipah-e-Sahaba Pakistan and a danger to Canada's security. Peterborough Examiner

Investigation into security breach at Vancouver Airport has wrapped

The investigation into a major security breach at YVR last month has wrapped up, but the Canada Border Services Agency is refusing to say what action was taken against the airline involved. It was Sunday, June 7, when an Air Canada flight arrived at YVR from Beijing. Almost 350 passengers were misdirected into the domestic area and failed to clear customs. They were quickly rounded up, and processed correctly, but at the time, Canada Border Services said the airline could face fines and possible prosecution. Today, CBSA spokesperson Robin Barcham says the investigation has concluded, and actions were taken to ensure security measures are strictly followed. But she refused to say what that action was. CKNW AM 980

Loonie keeping shoppers here - - Cross-border trip plans down: poll - Trend boosting local economy

A new survey shows the weak Canadian dollar is causing more Canadian residents to decide against cross-border shopping trips and spend their money at home. The data released this week from the RetailMeNot.ca survey showed 58 per cent of the Canadians surveyed said the weak Canadian dollar would stop them from visiting the U.S. while 66 per cent said cross-border shopping wasn't worth it anymore due to how much money they are losing on the exchange rate. Marina James, the CEO of Economic Development Winnipeg, wasn't surprised by the survey's findings. "It stands to reason that kind of burden on a U.S. exchange is just too much for people, adding in gas and hotels, to realize any retail saving in the U.S., so they'll be spending their dollars at home and their entertainment dollars at home," she said. [...] "We've opened up this at-par deal for any room, any day. You can pay with Canadian cash at par, or if you want to pay with a card or American cash, we'll just discount the room as to whatever the exchange rate is that day," Kuntz said. Statistics provided by Canadian Border Services Agency showed fewer travellers in 2015 than last year from Canada to the U.S. at the Emerson border crossing in both April (down by about 19,000) and May (down by about 11,000). However, in June, there was an increase in travellers from Canada to the U.S. (of about 9,000). Winnipeg Free Press, B5

Falling loonie helps drive retail sales

Retailers on both sides of the border are feeling the effects of the falling Canadian dollar, with fewer people crossing into Washington state and an increase in the number of Americans vacationing in B.C. More than 400,000 fewer privately-owned vehicles travelled south through the four land border crossings between the Lower Mainland and Blaine, Lynden and Sumas in the first six months of 2015 compared with the first six months of 2014, according to statistics collected by Western Washington University's Border Policy Research Institute. From January to June of last year, the Canadian dollar was worth between 90 and 92 cents US. During the first six months of 2015 it was worth between 77 and 87 cents. A recent border policy brief published by the institute states that the primary purpose for crossing the border for Canadians is shopping - including buying gas and picking up purchases sent to U.S. mailboxes - while Americans cross primarily for a vacation and recreation. Ken Peacock, chief economist and vicepresident at the Business Council of B.C., said retail sales in B.C. are currently very strong, with the total value of retail sales increasing by 8.3 per cent this May compared with the same month last year. Peacock said a number of factors are contributing to the growth, but a decline in crossborder shopping is "definitely a factor in helping boost retail sales." The Province, A3

Beat the Civic holiday border rush: CBSA
You'll want to plan ahead if you're heading state-side for the Civic Holiday weekend. The CBSA says peak traffic volume times at the Cornwall port of entry will be between 1 p.m. and 5 p.m. on Monday where the wait time could be more than 20 minutes. The agency says you can speed up the process by making sure you have all your documentation ready, including your passport. You're only allowed to bring back $200 after 24 hours in the United States duty-free and $800 after 48 hours. Also a reminder about purchases. Raw poultry, poultry products and by-products not fully cooked, including eggs and raw pet foods from several states are not allowed because of an outbreak of avian flu. Cornwall Newswatch

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

***U of T lab the bane of Italian spyware firm**
A Toronto research lab has caused a lot of grief to an Italian spyware firm allegedly linked to oppressive regimes, leaked files suggest. In emails, the firm Hacking Team was forced to suspend a client after a damning report from University of Toronto's Citizen Lab (CL), a monitor of "political power in cyberspace." After another report by Citizen Lab, the firm's executives were so agitated they wanted to "hit CL hard" through litigation, though they ultimately aborted that plan. The emails' release was the result of an ironic turn of events, in which Hacking Team, a peddler of software that grants unauthorized access to people's computers, was itself hacked. The data corroborated what Citizen Lab - based at U of T's Munk School of Global Affairs - has been reporting for years, embroiling Hacking Team in a storm of controversy. Citizen Lab director Ron Deibert said it is "interesting" to find out his lab's work - seven reports since 2012 - had had an impact on Hacking Team, but the contents of the leaked files were still "very discouraging." In March, Deibert sent an open letter to Hacking Team. The letter accompanied a fresh report on Hacking Team allegedly selling its technology to Ethiopia, which was said to have used it to spy on journalists. According to leaked files, CEO David Vincenzetti forwarded it to senior members, writing, "It's from our dearest friends at the U of Toronto." Later correspondence confirmed that Ethiopia was dropped as a client due to Citizen Lab's report... But according to leaked emails, the firm offered to reinstate Ethiopia about two months later, with strict conditions and a bigger bill. Hacking Team spokesman Eric Rabe told the Star the firm will not speak to the validity of the leaked files, though he said the emails were "part of the discussion." Toronto Star, GT4

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP widow says husband was made a 'scapegoat' in Dziekanski death
The wife of an RCMP officer who killed himself two years ago claims that her husband was used by the Mounties a scapegoat in the death of Robert Dziekanski at Vancouver's airport in October 2007. In a statement of claim filed in B.C. Supreme Court, Sheila Lemaitre says her husband, Pierre, was told he would lose his job if he tried to correct misinformation given to the media about the night Dziekanski died. The sergeant was the media relations officer who released information about the incident where the Polish immigrant was jolted with a police Taser and died on the floor of the arrivals area. The lawsuit claims Lemaitre wanted to correct the information, but was ordered not to and as a result was accused by the public as being the "RCMP liar" and the "RCMP spin doctor." The statement says the RCMP knew Lemaitre was under extreme psychological distress caused by the negligence of the force and that it could result in his becoming suicidal. None of the allegations have been proven in court, and no specific dollar figure is mentioned in the lawsuit. Canadian Press (The Guardian, Cape Breton Post, Times Colonist, Vancouver Sun, Edmonton Sun, Calgary Sun, Toronto Sun, Ottawa Sun, Winnipeg Sun, Kingston Whig Standard, London Free Press); Globe and Mail; Postmedia News (The Province)

Calgary homicide victim was coming to Saskatoon to reconnect with family
The day before he was killed at a Calgary house party, Levi Marance was making plans to move to Saskatoon. Marance's biological mother, Marie-Eve Smith, said she was texting with him about plans to set up a new life in the city the day before his murder. He was supposed to get on a bus, and she and her other sons were going to pick him up in Saskatoon, she said. "He wanted more than anything to come here. He wanted to be with us. He would always say 'I'm coming home soon.' " Smith said, recalling one

of her last conversations with him. Marance was raised in a large adopted family in Red Deer, but was couch surfing with friends in Calgary at the time of his death. Smith said she gave him up for adoption to her aunt shortly after his birth, and because Marance was adopted into her extended family, she had regular contact with him. She described him as a fierce protector of his other siblings. "For the last week and half I talked to him every day. He didn't sound messed up. He wasn't drinking. He was just really excited to come here to be with us," she said. The 18-year-old was stabbed at a house party in an apartment complex in northwest Calgary on July 19. He died in hospital from his injuries, police said. In interviews earlier this week, Lynda Marance, Levi's adopted mother, said the teen was addicted to crystal meth at the time of his death. Smith said her son was couch surfing because he was kicked out of the house in Red Deer nearly two years ago. She disputes the claim that he was addicted to drugs, saying she knew him well enough to know he was not an addict. "I really believe he was not addicted to crystal meth. I know he tried it. We were close enough that he told me he tried it." Smith said her son did have runins with the law in Alberta and he had told the family a Calgary-based street gang was trying to "jump him in" against his will when he was killed. She does not know whether the gang has any connection to his death, she said. Postmedia News (StarPhoenix, A1, Leader Post)

Shooting victim had mental illness

One month before he was shot dead by a Peel Regional Police officer, Jermaine Carby was apprehended under Ontario's Mental Health Act after attempting to disarm a Toronto police officer, the Star has learned. After he was taken to hospital following apprehension by police, Carby threatened to commit suicide by hanging or injecting air into his veins through a syringe. Information detailing Carby's mental-health apprehension was provided to his relatives during a meeting with the Special Investigations Unit last week, after the police watchdog ruled the unnamed officer who killed Carby during a traffic stop last September would not face criminal charges. Carby's family recorded the meeting with SIU officials, including director Tony Loparco, and provided the Star with audio from the meeting. The family has also provided the coroner's and toxicology reports. The information sheds new light on Carby's mental health - including suicidal tendencies - and raises fresh questions about how much the Peel officers knew about Carby's background in the moments before he was killed. Carby's family was told at the meeting that the in-car computer Carby's name was run through would have reported that he had "suicidal tendencies," "mental instability" and had previously tried to disarm an officer... Moments after being pulled over, the officer ran Carby's name through the Canadian Police Information Centre (CPIC), a national database that includes criminal files, and discovered Carby had a lengthy criminal record and outstanding warrants from British Columbia. According to the SIU investigation, when the officer questioned Carby about the warrants, he pulled out a knife and moved toward officers, prompting one of two officers who arrived as backup to shoot. But when the officer who made the initial traffic stop ran Carby's name through his in-car computer, CPIC also cautioned the officer, via a warning note, that Carby had previously attempted to disarm a police officer, the family was told in the meeting. Toronto Star, GT1

Privacy and information

An editorial states, “Two recent news stories in New Brunswick create an interesting juxtaposition for the general public, in our view, on where we are headed on the matter of privacy laws as opposed to the right to information. Recently, the RCMP cited federal privacy laws to announce that it will no longer release the names of crime and accident victims to the general public. Subsequently the federal Privacy Commissioner stated "It is up to the RCMP to determine whether the public interest outweighs privacy concerns." In our opinion that gives the RCMP too much latitude in making an arbitrary and potentially dangerous interpretation of privacy laws. The RCMP and all police officers are admirable for the difficult job they have, but aside from fighting crime, part of their job is to protect the rights of citizens, including 'the right to know.' Perhaps that stance can be interpreted as self-serving, coming as it does from an organization that depends on information to stay in business. That might be fair comment, but what is really at stake here is the public's right to information. There may be rare cases where the RCMP should withhold information temporarily if the identity of a crime victim could compromise an ongoing investigation, but a blanket policy to potentially withhold information in all cases and for no reason related to police work is neither necessary nor advisable. Call it an exaggeration, but we see it as the thin edge of the wedge toward a 'blanket policy' of secrecy in police work....” Times & Transcript, A10

Ontario to consult the public on carding
With the Black Lives Matter protest that blocked traffic on the Allen Expressway this week still fresh in the minds of many, the provincial government has announced plans to begin public consultations on street checks, or carding. The consultations - which will be held with community organizations, policing partners, academics, civil liberty organizations as well as asking the general public for online participation - are to begin in August. Toronto Mayor John Tory had pledged in June to reform carding in the city, but then decided to delay any action until the province reviewed the controversial police practice and set up province wide regulations. Community Safety Minister Yasir Naqvi announced in June that the provincial government planned to review the practice often called street checks outside Toronto. "Our government takes the protection of human rights very seriously and has been clear that we have zero tolerance for racism or marginalization, including any form of discrimination based on skin colour, background, religion or gender," said Naqvi in a news release. "We stand opposed to any practice where police stop individuals without reason, cause or for clear policing purposes." The consultations will develop new rules so the practice of street checks is "right-based and properly carried out, protecting individual charter and human rights, strengthening public accountability and allowing for a consistent and clearly defined approach for police," the Ontario government's release said. Toronto Star, GT2

Grande Prairie gets new top cop
RCMP in Grande Prairie have a new boss. Grande Prairie Chief Supt. Brenda Lucki, district commander for the RCMP's Western Alberta District, announced Thursday that the detatchment in Grande Prairie-Beaverlodge will be led by Supt. John Ferguson. "We are pleased to have Supt. Ferguson join our team," says Horacio Galanti, Grande Prairie community safety director. "Grande Prairie is a growing, diverse community and a hub for the region. His extensive background is a great fit, particularly in priority areas such as drug activity." Ferguson, a graduate of Queen's University in Ontario and father of three, has most recently filled roles at "H" Division in Nova Scotia including Federal Policing Officer and District Officer for Northeast Nova District. Edmonton Sun, 8

Mounties charge man with human trafficking
Mounties have charged a 25-year-old man in southern Alberta with human trafficking and prostitution offences. Police say the charges came while investigating a youth reported missing. They say the investigation found evidence that the youth was an alleged victim of human trafficking. A man from Airdrie is facing several charges, including assault, human trafficking and living off the avails of prostitution. Postmedia News (Edmonton Journal, A7); Calgary Herald

Ex-B.C. gangster under arrest after moving to Ontario
A former B.C. gangster has been arrested in Ottawa on drug and weapons charges. Damion Ryan, who is now a prospect for the Ontario Nomads' chapter of the Hells Angels biker gang, was picked up on July 17. Det. Staff Sgt. Len Isnor, of the Ontario Provincial Police, confirmed Ryan's arrest to The Vancouver Sun. Isnor said the investigation by the OPP's Biker Enforcement Unit is continuing. Ryan was associated with the so-called Wolf Pack alliance while he was in Metro Vancouver. It consisted of some Independent Soldiers' gangsters, some members of the Red Scorpion gang and some Hells Angels. The alliance was locked in a bloody gang war that resulted in the slayings of several high profile gangsters like Red Scorpion Jonathan Bacon, Sandip Duhre and brothers Gurmit and Sukh Dhak. Ryan's name surfaced earlier this year in a B.C. Supreme Court ruling in a gun case involving his associate Dean Wiwchar, who is a suspect in the 2012 Duhre murder. Postmedia News (Vancouver)

* **Top cop in Kelowna probing Mountie's confrontational traffic stop, reports say**
A video that shows a Mountie's confrontational encounter with a driver and her passenger is reportedly under investigation by the officer in charge of Kelowna's RCMP detachment. Supt. Nick Romanchuk has told multiple media outlets that he has asked for a review of the video, which was posted on Facebook by a man with the user name Shawn Michaelz and had been shared more than 1,800 times by Thursday evening. Michaelz wrote that the encounter began when he saw the officer make a left turn without signalling. "I throw my hands up in the air in the passenger seat of the vehicle and the cop gets mad and pulls a U-turn in the intersection to pull us over," the post reads. The video shows the Mountie asking, "So, what would you like to say to me, as a police officer?" The female driver responds by asking why she was pulled over. "Any time someone is going to go like that to a police officer, then they're obviously

upset about something," the officer replies. He goes on to say that he was looking for a licence plate, looked down at his computer screen, and lost track of his position on the road. When the car's passenger suggests that could be considered distracted driving, the officer says, "Distracted driving? OK, well, we'll have a look at your paint job, your rims, make sure they're high enough from the ground," before walking away to call for a member of the traffic section. The video is edited, so it's unclear how long the encounter lasted, but it shows the officer checking the driver's licence and insurance and telling her he needs to make sure the vehicle is road-worthy. Postmedia News (Vancouver Sun)

*** Under the influence**
An editorial states, "So, are we winning the war on drunk driving? Some days, you have to wonder. And Wednesday was one of those days, at least as far as the Bay St. George detachment of the RCMP is concerned. During a 24-hour period spanning parts of July 29 and July 30, the Bay St. George RCMP responded to 14 calls for service. Of those, somewhere between one-fourth and one-fifth were drunk-driving complaints. Here's how the first one looked in a Thursday morning news release: "At 10: 27 a.m. police received a report from a Stephenville business indicating that a customer had just driven to their location and appeared to be intoxicated. Police attended and located the 61-year-old male resident of Stephenville and arrested him for impaired driving. The man subsequently provided a breath sample that (was) 2 1/2 times the legal limit. The male will appear in court on Oct. 5th to enter a plea to impaired driving charges." ... Are we winning the war? Some days, you can hope that we are. Other days, like Wednesday, it's pretty clear we're still losing battles." The Telegram, A6

***B.C. groups protest against Kinder Morgan pipeline review**
The National Energy Board (NEB) is facing a fresh round of resistance to its embattled review of the proposed Kinder Morgan Trans Mountain pipeline expansion. Three separate parties - British Columbia's Opposition New Democrats, the city of Burnaby and the Sierra Club - all issued renewed challenges to the process on Thursday. Kinder Morgan hopes to triple the bitumen-carrying capacity of the Trans Mountain line by laying almost 1,000 kilometres of new pipe between Edmonton and Metro Vancouver, increasing the number of tankers in Burrard Inlet to 34 from the current five per month. The strongly-worded letter from B.C.'s opposition party details four major concerns with the NEB process, including that it lacks the public's confidence, doesn't consider climate change, hasn't required Kinder Morgan to disclose its emergency response plans and failed to ensure First Nations were on board. Meantime, the city of Burnaby sent a letter to the NEB refusing to provide extra policing services for the upcoming Trans Mountain hearings in September. The board had asked for seven officers and one supervisor. Burnaby Mayor Derek Corrigan said the city has limited police resources to serve its own needs, and has asked the NEB to make other arrangements with the RCMP's head office in B.C. "We are also extremely concerned that the NEB has come into Burnaby and is doing things that we know are going to be provocative," he said. Canadian Press (Toronto Star, A8; Red Deer Advocate)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

*** Officials mum on CSC headquarters break-in**
Correctional Service Canada officials are tight-lipped as to why a break-in at one of their regional headquarters buildings in April wasn't made public. In the early morning hours of April 22, a burglar broke into the regional staff college at 443 Union St. The suspect gained entry to the building by smashing a window pane at the front entrance. There was no security at the regional headquarters at the time of the break-in. In an email to the Whig-Standard on Thursday, **CSC** confirmed that a break-in took place on April 22, commissionaires and Kingston Police responded to the scene and a letter was sent out to employees the following morning. But **CSC** didn't comment on whether security was increased at the facility since the break-in. "As there is an ongoing investigation, **CSC** cannot comment further," Shannon Mills, a communications officer with CSC, wrote in an email. Mills added that "ensuring the safety and security of institutions, staff, inmates and the public is **CSC**'s priority." According to the website Cancrime, sources said that the facility stores confidential files, a variety of pistols, rifles, shotguns and tear gas guns as well as a large amount of ammunition. The firearms and ammunition were stored in high security vaults, which the burglar didn't have access to. According to an internal memo, also obtained by

Cancrime, all the thief took were keys to a **CSC** staff vehicle but the vehicle wasn't stolen. After the break-in, alarms sounded and the patrol commissionaire and Kingston Police responded. Therese Lalonde, the director of the staff college, wrote in the memo that a walkthrough of the facility took place later that morning to see if anything else was stolen. "No other items were found to be missing and no area was found vandalized," she wrote. Kingston Whig-Standard, A1

*** Collins Bay inmate murdered**

The inmate who died on Monday at Kingston General Hospital after needing medical attention in the medium security exercise yard of Collins Bay Institution on Sunday was murdered, said the Joint Forces Penitentiary Squad in a release. John MacDonald, 55, had been serving a sentence of five years, 10 months and 16 days, since June 8, 2010 for two counts of robbery. A post mortem examination was performed at Ottawa General Hospital this week and the death was deemed to be a homicide. As in all death cases in institutions the Joint Forces Penitentiary Squad was called into investigate MacDonald's death along with investigators from Corrections Canada. The homicide is being investigated under the direction of Det. Insp. Jim Gorry of the Ontario Provincial Police Criminal Investigation Branch. Officials are not releasing anymore information on the death while the investigation is ongoing. Kingston Whig-Standard, A3

*** A way out needed for the held down**

The news Wednesday that 22-yearold inmate Camille Strickland-Murphy was found unresponsive in her cell in Nova Institution for women in Truro could be seen as inevitable. She had been in court many times - once when she held a knife to someone's throat; another when she had written a threatening note to a pharmacy in an attempt to rob it. She suffered from attention deficit hyperactivity disorder, obsessive/compulsive disorder, social anxiety disorder, and panic disorder. That cocktail of mental health issues was garnished with a history of alcohol and drug abuse. It was reported earlier this year that she attempted suicide by stuffing paper in her pant leg and catching herself on fire. Mark Gruchy, a lawyer and president of the local chapter of the Canadian Mental Health Association, says such cases are avoidable tragedies. "When you see an individual who is having problems with addiction and underlying mental-health problems you are seeing the tip of the iceberg of the culmination of usually innumerable personal disasters that have now culminated into this massive social problem," he says. People who find themselves in a position like hers come from a complex place and the remedy to their problems has its complexities, too. It involves engagement in the housing, employment, socializing, addiction and mental - health issues they face, Gruchy argues. "You have people who are already in a weakened state who are having more and more piled on top of them that even an otherwise well-situated person would have difficulty overcoming." That erosion of normalcy and deposition of problems on them makes finding a way out impossible. The result is desperation which, as the saying goes, calls for desperate measures. A big part of the solution, Gruchy says, would be a drug court, such as those that exist in larger Canadian cities. The Telegram, A5

*** Inmate had history of health issues**

A 22-year-old inmate found dead in her cell at the Nova Institution for Women had a history of mental health and substance abuse issues, prior to being sentenced on an armed robbery conviction last November. Camille Strickland-Murphy, who had been serving a sentence of two years, eight months and two days, stemming from last Nov. 10, in St. Johns, NL, was found unresponsive in her cell Tuesday evening at the women's prison in Truro. During her sentencing, according to information published last November in the St. John's Telegram, Newfoundland provincial court judge Pamela Goulding noted that Strickland-Murphy had suffered from attention deficit hyperactivity disorder, obsessive/compulsive disorder, social anxiety disorder and panic disorder, as well as a history of alcohol and drug abuse. '"During her (previous) incarceration (in 2012), the offender was assaulted severely, which resulted in a brain injury. She now has hydrocephalus and experiences headaches, fainting and seizures,"' the Telegram reported last fall, from Goulding's written report. It has also been reported that during the 2012 sentencing, Strickland-Murphy had asked to be housed in a federal institution to get help for her mental health issues. When asked Wednesday by the Truro Daily News whether Strickland-Murphy had been enrolled in any programs to deal with her issues, prison warden Laurie Bernard said she could not provide that information for confidentiality reasons. "I'm not able to comment on that at this time," Bernard said. "What I can confirm, is that as with all deaths in custody, the coroner and medical examiner were

called in to investigate. And as with all such cases, she said, **CSC** will conduct its own investigation as well. Cape Breton Post, A9

*** Camille Strickland-Murphy's death prompts calls for overhaul of N.L. justice system**
Following the death of Camille Strickland-Murphy in a Nova Scotia prison, a local lawyer says there needs to be a major overhaul of how the Newfoundland and Labrador justice system deals with mental health issues and addictions. "Whenever someone ends up in prison, that's the culmination of a disaster," said St. John's defence lawyer Mark Gruchy. Camille Strickland-Murphy died Tuesday night, while serving a three-year sentence at the Nova Scotia Institute for Women. (CBC) "Prison is a disaster. It is not a solution, it's the end of the road. And we can only hope that it doesn't get worse." Strickland-Murphy was a St. John's resident, who was serving a three-year sentence for the armed robbery of a Shoppers Drug Mart in Newfoundland in 2014. She had drug and alcohol addictions as well as mental illness. The provincial correctional system does not offer any treatment options, so Strickland-Murphy chose to go to federal prison on the mainland so she could get help. CBC News

*** More than six years after her child was slain, Tara McDonald is helping bring new life to others**
First, she was Canada's most horrible mother, vilified across the nation. "I was made to be such a wicked, wicked witch," Tara McDonald remembered. "So heartless, evil, cold." Then, the body of her daughter Tori Stafford was found and two strangers charged with her kidnapping, rape and murder. McDonald became Canada's grieving mother, her home filled with stuffed teddy bears and other mementoes sent from sorrowful people across the country. "I still have bad days. There are some days it takes me longer to put on my happy face and get out there to be with people," she said. But now, McDonald is finally starting her new life as the ultimate mother, a doula helping other women bring children into the world. "When I see a newborn baby, I think of life," McDonald said Thursday, setting up a booth for her service, Your Body, Your Birth, at London Ribfest. "Don't get me wrong; if I see a little girl who's eight years old with blond hair and blue eyes, of course I think to myself, that is a beautiful child that looks like Tori, and that tugs at my heart. But Victoria loved life and she would want me to be doing what I love." Rather than make her shy away from children and parents, her daughter's horrific death has brought her closer to them, McDonald said. "I think it has allowed me to be a more compassionate person and a more understanding person. I didn't have any second thoughts at all. It made me stronger to do it." Eight-year-old Tori was kidnapped April 8, 2009, while walking home from her school in Woodstock and killed that same evening in a wooded area of a farm north of Guelph. Two Woodstock residents, Michael Rafferty and Terri-Lynne McClintic, were convicted of first-degree murder, kidnapping and sexual assault causing bodily harm and sentenced to life in prison. London Free Press, A1 (Calgary Herald, Montreal Gazette, National Post, Edmonton Journal, StarPhoenix, Windsor Star, Leader-Post, The Province)

*** Conditions imposed on violent offender's release to halfway house**
A P.E.I. man who has a history of killing animals and said he would feel no distress killing a person was recently granted a statutory release from prison. Bradley Orville Perry was serving a two-year, four-month and twenty-seven day sentence for several offences, including using a firearm to commit theft and possessing an unregistered restricted weapon. Perry was also convicted of careless use of a firearm, possession of property obtained by crime and failing to comply with a condition of an undertaking. It was his second sentence of more than two years. In a recent report, the parole board imposed several conditions on Perry's release, including that he live in a halfway house. The report outlines some of Perry's criminal history and file information collected during a prior sentence. Some of Perry's offences involved the use of weapons, such as knives and a loaded shotgun, which he used during a domestic dispute. Perry's file showed he killed domestic animals, such as pet birds and a former girlfriend's cat. He also admitted to strangling pigeons from his cell window while serving his most recent sentence. Perry said he didn't feel any distress over killing small animals and wouldn't if he killed a person, although the potential of going to prison was a deterrent to killing someone. In imposing the conditions on Perry's release, the board said past issues with his ability to control his emotions led to impulsive and violent behaviour. During an incident involving a family member, Perry hit their head off a coffee table and during another he used a loaded shotgun to threaten a girlfriend. Charlottetown Guardian, A1

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Fund contributes to community projects**

The Yukon government has awarded more than $103,000 to eight Yukon community organizations for projects that support healthy communities. Among the recipients is the Yukon Council on Aging, which has been given $5,796. That group will use its funding to modernize its website to enhance its accessibility and to incorporate a more user-friendly design. "Working with seniors' organizations, the Yukon Council on Aging spearheads the sharing of information of interest to seniors in Yukon," council president Connie Dublenko said in a recent news release. "This project will help us achieve our goal of encouraging respect for the contributions senior citizens have made, and of understanding the aspirations and issues of concern in the lives of Yukon seniors." The Association of Yukon Fire Chiefs will access $15,000 from the Community Development Fund (CDF) to provide training and education tools to firefighters that will focus on community safety and property conservation. "The Association of Yukon Fire Chiefs is grateful and excited to receive CDF support," said president Jim Regimbal, who is also Dawson City's fire chief. "The funding will help us achieve our primary goals of life safety and preservation of property by providing Yukon fire chiefs and senior fire officers with the additional training and educational tools needed to protect their communities." The Copper Ridge Neighbourhood Association was awarded $20,000 to build a playground, install accessible benches and improve landscaping at Lazulite Park. Whitehorse Daily Star, 5

*** Young citizens on patrol**

For the fifth summer, Kingston Police have a few more feet on the ground helping them patrol the city. William Arsenault, 17, and Trevor Kirby, 15, are the newest summer recruits for the Youth in Policing Initiative (YIPI) program. Supervised by Const. Josh Conner, the Kingston Police Youth Officer, the teenagers perform a variety of crime prevention measures, public relations duties and community outreach programs. Duties include foot patrol, bike patrol, check vehicles for valuables inside and give out Lock It Or Lose It forms, attend community barbecues and other community events. Their duties don't include any police business that will put them in harm's way. During Wednesday's searing heat, the the pair were downtown checking on unlocked cars as part of the Lock It Or Lose It program. "It's a crime prevention program to make sure people don't have valuables in their car and make sure their cars are locked," said Kirby, who is going into Grade 10 at Regiopolis-Notre Dame in the fall. As part of the program, both Arsenault and Kirby look in vehicles in city parking lots and along city streets to visually ascertain if the car is locked and if it has any valuables inside. After their inspection, they place a ticket on the car that isn't a fine but advises the car's owner to keep their valuables secure. Last week, they found a laptop, cellphone and keys to the car in an unlocked vehicle. So far this summer they haven't found any dogs or babies left in hot cars. Kingston Whig-Standard, A2

*** $1M will help abuse victims**

A London-based centre that helps survivors of domestic violence and child abuse has received a $1-million infusion to become a national hub for supporting victims. The Centre for Research and Education on Violence Against Women and Children will get slightly more than $1 million from the Public Health Agency of Canada to become a national hub that looks at the health and well-being of trauma survivors. The money means programs and research being done in all parts of Canada will be connected to help agencies and health professionals do the best possible job, said Linda Baker, the centre's learning director. "This is an opportunity to bring together community organizations that are working with survivors with leading researchers and health professionals," Baker said. "Usually, projects are done but they stay in silos, in isolated clumps. For the first time in terms of trauma-informed health promotion, we can maximize the impact. An innovative practice in Nunavut or the Maritimes can be shared." The money will be used to connect the work of community-based projects in Canada for five years. The projects support victims of violence from a health perspective. The knowledge hub will consolidate the data from various projects to better help families affected by violence. London Free Press, A5

PUBLIC SERVICE / FONCTION PUBLIQUE

***Up and down journey for PS**
As of last month, nearly 317,000 people worked for the federal government, its various agencies and the armed forces - just one per cent more than when the Conservatives were sworn in early in 2006. On the eve of a federal election, Prime Minister Stephen Harper now finds himself in the crosshairs of public sector unions concentrating on the last half of the Conservative decade. "This government is cutting public service budgets across the country, without regard for the safety and welfare of millions of Canadians," read the newspaper ads published this week by the Public Service Alliance of Canada, the largest federal government union. PSAC may not have long to make its points: its spending on ads will be limited under the rules that kick in once the election campaign begins. But overall, government workers haven't done badly, certainly in comparison with workers in other industries. The federal government's total payroll last year was $45 billion including benefits, up from $29 billion in 2006 when Stephen Harper was sworn in as prime minister. The rise was not gradual. Pay and benefits across the federal government jumped nine per cent annually from 2006 to 2010, then weakened considerably to two per cent per year during the following four years - reflecting the big drop in the number of employees. Ottawa Citizen, A1

OTHER / AUTRE

État islamique
Peu d'informations ont filtré de la rencontre tenue à Québec jeudi pour faire le point sur la riposte internationale au groupe armé État islamique (ÉI) et planifier les prochaines étapes. Les échanges, sous haute sécurité, se sont déroulés derrière des portes closes dans la salle de bal du Château Frontenac, entre quelque 150 dignitaires, politiciens et militaires provenant d'une vingtaine de pays. Plusieurs enjeux, politiques et militaires, étaient à l'ordre du jour des discussions qui se sont étirées durant environ sept heures, en vue de s'assurer que tous étaient bien sur la même longueur d'ondes au sein de la coalition internationale déterminée à faire cesser les exactions commises par le groupe extrémiste, qui sévit en Irak et en Syrie. La coalition prévoyait notamment s'interroger sur l'efficacité des frappes aériennes dirigées jusqu'à maintenant contre le groupe. Dans un communiqué, le ministre canadien des Affaires Étrangères, Rob Nicholson, qui était l'hôte de la rencontre, a dit que le Canada était prêt à accroître son effort en injectant 8,3 millions $ supplémentaires en vue de soutenir les Irakiens dans différentes actions destinées à contrer le groupe armé, notamment en augmentant les mesures de sécurité aux frontières et en apportant davantage d'aide humanitaire à la population dans le besoin.
Le ministre irakien des Affaires étrangères, Ibrahim al-Jafaari, accompagné de nombreux gardes du corps, était présent à Québec, tout comme le général américain à la retraite John Allen, envoyé spécial du président des États-Unis Barack Obama. Le Canada a profité de l'occasion pour réitérer sa détermination à assumer le leadership de la lutte contre le terrorisme en s'attaquant aux pratiques «barbares» de l'ÉI, une bataille entreprise il y a un an à l'échelle internationale... La Presse Canadienne (Acadie Nouvelle, 18); Agence QMI (Journal de Montréal, 24, Journal de Québec, 7)

INTERNATIONAL / INTERNATIONAL

Debris offer clue to fate of Flight 370
A seacrusted wing part washed up on an island in the western Indian Ocean may be the first trace of Malaysia Airlines Flight 370 since it vanished nearly a year and a half ago, and a tragic but finally solid clue to one of aviation's most perplexing and expensive mysteries. Malaysia's prime minister said Thursday the debris found on the French island of Reunion will be sent for investigation to the French city of Toulouse, hub of the European aviation industry. "We have had many false alarms before, but for the sake of the families who have lost loved ones, and suffered such heartbreaking uncertainty, I pray that we will find out the truth so that they may have closure and peace," Najib Razak said on his personal blog. Najib promised to make any new information public quickly. Air safety investigators - one of them a Boeing investigator - have identified the component as a "flaperon" from the trailing edge of a Boeing 777

wing, a U.S. official said. Flight 370, which disappeared March 8, 2014, with 239 people on board, is the only 777 known to be missing. The piece could help investigators figure out how the plane crashed, but whether it will help search crews pinpoint the rest of the wreckage is unclear, given the complexity of the currents in the southern Indian Ocean and the time that has elapsed since the plane disappeared.
"It's the first real evidence that there is a possibility that a part of the aircraft may have been found," said Australian Transport Minister Warren Truss, whose country is leading the search for the plane in a remote patch of ocean far off Australia's west coast. "It's too early to make that judgment, but clearly we are treating this as a major lead." Flight 370 had been travelling from Kuala Lumpur to Beijing, but investigators believe based on satellite data that the plane turned south into the Indian Ocean after vanishing from radar. If the wing part is from the Malaysian plane, it would bolster that theory and put to rest others that it travelled north, or landed somewhere after being hijacked... Associated Press (Red Deer Advocate, A7, Daily Gleaner, Kingston Whig Standard, London Free Press, Chronicle Herald, A15, Windsor Star, StarPhoenix, Gazette, National Post, A3); CBC News; * Associated Press (Edmonton Journal, A17, Vancouver Sun, B4, Calgary Herald)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Today's News / Actualités
May 6, 2016 / le 6 mai 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Alberta offering emergency stipends to Ft. Mac evacuees
The 88,000-plus evacuees who fled the catastrophic Fort McMurray wildfire will be getting financial aid from the Alberta government, Premier Rachel Notley said Friday. "One of the key issues facing people displaced by this disaster is immediate challenges: food and shelter," Notley told reporters during a briefing in Edmonton. "As we did after the Slave Lake fire and the southern Alberta flood, cabinet today authorized the government to provide emergency financial assistance to people who have been displaced." Every adult evacuee will receive $1,250 in emergency stipends, Notley said, while dependents will get $500 each. The fire, officials said Friday, has grown exponentially to cover more than 101,000 hectares. Critical infrastructure — including the hospital and the downtown core — remain intact. Responders say they expect the challenging firefighting situation, spurred by a lack of rain and tinder-box conditions, will continue. "***They're dealing with an absolute beast of a fire, one of the worst we've ever seen***," **Public Safety Minister Ralph Goodale** told reporters, Friday. The cause of the fire remains

under investigation, Alberta officials said, adding winds are expected to redirect the fire towards a forested area in the northeast. Mandatory evacuation orders remain in place and it's not safe yet for residents to return, Notley said. iPolitics

Alberta Wildfires Roar on as Evacuee Convoy Drives to Safety
Wildfires ravaging the center of Canada's oil production region in northern Alberta continued to grow, covering more than 1,000 square kilometers (390 square miles) as police shepherd convoys of families to safety through the now-devastated town of Fort McMurray. The fire is spreading north and south, covering an area almost the size of Hong Kong, forcing evacuations from oil camps where Fort McMurray residents had fled earlier this week, police said. The ferocity of the fire was unprecedented, said Chad Morrison, a senior wildfire manager for the Alberta government. "This is an extreme, rare fire event, that is something that is historic for us," Morrison said at a press conference in Edmonton, flanked by Alberta Premier Rachel Notley and a brigadier general from Canada's military. "There is no amount of resources we are going to be able to put on this fire that can hold it." As many as 25,000 of Fort McMurray's 80,000 evacuated residents had gone north to oil-sands work camps before the fires overtook the town, cutting them off from the rest of the country. That area is no longer guaranteed safe, **federal Public Safety Minister Ralph Goodale said**. Police began escorting convoys of 50 vehicles at a time through the fire zone Friday morning, working to get the 10,000 people to safety in towns south of the city. Bloomberg News

Canadians donate millions to Red Cross for Fort McMurray relief effort
People from across the country have banded together in what the president of the Canadian Red Cross says is an unprecedented ``Canadian moment," donating $30 million by Friday morning to help the victims of the massive wild fire in Fort McMurray, Alta. ``Canadians are collectively coming together to show their care and compassion," Conrad Sauve said Friday. ``We have over 100,000 Canadians that have come to us with texts to donate. We're getting offers from every part of the country, including corporate Canada in terms of workplace (fundraising) campaigns." About 14,000 families in need from the Fort McMurray area have registered with the Red Cross and that number is expected to grow. Both the federal and Alberta governments have promised to match all donations to the Red Cross for the relief efforts in Fort McMurray. The money is used to mobilize and provide support Red Cross volunteers who are helping evacuees. The cash is also used to provide basic goods to people fleeing the fire. **Public Safety Minister Ralph Goodale** said the Fort McMurray blaze is ``***an absolute beast of a fire***'' that is one of the worst ever seen. ``***The situation is still evolving. It's still very dangerous***." Canadian Press (Chronicle-Herald); La Presse Canadienne (L'actualité); News Talk 1010; CHQR News Talk 770 AM

Broadcast Media / Médias télédiffusés:

CTV News - Power Play interviewed Jim Reiter, Saskatchewan Government Relations Minister regarding the federal, provincial, and territorial ministers responsible for emergency management meeting which took place today with **federal Public Safety Minister Ralph Goodale**. Rough Transcript

CTV News - Power Play interviewed B.C. Premier Christie Clark discussed wildfires. During the conversation, Premier Clark commented that financial assistance to the provinces from the federal government for disasters has typically been slow and says that funds needs to be distributed quicker. Following this, Power Play reported on comments made by **Public Safety Minister Ralph Goodale** earlier today in regards to disaster financial assistance. Rough Transcript

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray fire evacuees get first view of burned city
Displaced Fort McMurray residents got a sobering drive-by view of their burned city Friday in a convoy that was moving evacuees south to reunite with families and friends. Officials said shifting winds were

giving the embattled northern Alberta city a break, but they added the fire that forced 80,000 people from their homes remained out of control and was likely to burn for weeks. In Edmonton, Premier Rachel Notley announced the government will provide debit cards to help evacuees with immediate needs. Adults will receive $1,250 each and dependents $500. The cost to the province is estimated at $100 million. The first convoy of 50 vehicles drove through the oilsands city from the north at about 6 a.m. It was escorted by the RCMP and a police helicopter was monitoring the area in case winds shifted to create a renewed fire danger along the route. Premier Rachel Notley said the plan was to get 500 vehicles out by ground and 5,500 people by air. Another 7,000 were flown out Thursday. More than 20,000 displaced residents had been living in oilsands work camps since Tuesday after the blaze cut the main road through Fort McMurray and sent residents fleeing either north or south. The fire itself stood at just over 1,000 square kilometres. There was no renewed update on number of structures burned, which stood at 1,600 Wednesday, mainly in city neighbourhoods to the south and southwest. Chad Morrison, Alberta's senior wildfire manager, said critical infrastructure - the downtown, the water treatment plant, the hospital and the airport - remained intact. The blaze also hit the evacuated village of Anzac to the south of the city where it destroyed 12 structures. Morrison said winds were moving the blaze away from Fort McMurray toward unoccupied areas to the north and east. Canadian Press (Winnipeg Free Press); National Post; Toronto Star; Edmonton Sun; Daily Mail; Reuters (Huffington Post); The Guardian; NY Times; AFP (TVA Nouvelles); Journal de Montréal; Radio-Canada

Fort McMurray wildfire: P.E.I. man in convoy 'could reach out and touch' fire
A P.E.I. man says fires were so close to his car as he headed out of Fort McMurray on Friday he could reach out and touch them. Vernon Gillespie was relieved to be in the convoy leaving an oil camp in northern Alberta, going through Fort McMurray, and out of the fire zone. But it was more frightening than he expected. Gillespie said there were hundreds of vehicles in front of him, and it was very slow moving. CBC News; Global News

Smoke hits Saskatchewan as Fort McMurray wildfires burn
Saskatchewan is still breathing smoke coming from the wildfires near Fort McMurray, Alta. According to Environment Canada, northwest winds are spreading the smoke from the wildfires in northeast Alberta to western Saskatchewan. As a result, some areas will experience poor air quality and reduced visibility. The weather station has issued a special air quality statements for north-western Saskatchewan, including Saskatoon, Buffalo Narrows, Beauval, Île à la Crosse, La Loche, Clearwater River Provincial Park, Cluff Lake, Martensville, Warman, Rostern, Delisle and Wakaw. The statement is also extended to the communities of Meadow Lake, Big River, Green Lake, Pierceland, Prince Albert, Shellbrook, Spiritwood, Duck Lake, the Battlefords, Unity, Maidstone and St. Walburg. CBC News

Firebreak around Fort McMurray wouldn't have saved city, official says
Building a firebreak around Fort McMurray wouldn't have helped prevent a wildfire from devastating the city this week, says Alberta's top wildfire official. "I want to be clear," Chad Morrison said at a news conference. "With the nature of this fire and the dangerous conditions we have, no size of firebreak would hold this fire from doing anything. This fire jumped the Athabasca River, which is over a kilometre wide." After a wildfire destroyed about one-third of the town of Slave Lake in May 2011, the province commissioned a study that looked for ways to prevent similar disasters. The committee made 21 recommendations, but in its final report concluded there was little that could have been done to save the town, which suffered what was at time the second-costliest disaster in Canadian history, with an estimated $742 million in insurance claims. CBC News

Fort McMurray wildfire: First clear satellite images show deserted streets, burned homes
Early Friday morning, Google released the first clear images of fire-ravaged Fort McMurray taken from space. They show deserted streets and whole neighbourhoods devastated. The space image was taken Wednesday by Terra Bella, a subsidiary of Google that operates satellites. A larger original version can be seen here. (Go to that link to look for a specific home.) Global News

Fort McMurray fire has economists cutting growth forecasts for Canada
Economists trying to gauge the impact of the Fort McMurray wildfire and its disruption of oilsands production are already cutting their outlooks for the Canadian economy. Current estimates are that

anywhere from 900,000 to one million barrels of oilsands production have been suspended due to the fire. "The situation remains fluid, and uncertainty remains about how long production disruptions will persist," economists at Royal Bank of Canada said in an economic comment released Friday. "However, if we assume those shutdowns last for two weeks, they would subtract 0.5 per cent from May GDP." RBC said it expects much of the decline in oilsands production will be reversed in the months to come. "Although the loss of oil production is likely to be the largest factor impacting monthly GDP data, the absence of evacuated residents will also limit retail sales and hours worked outside of the oil and gas production sector," the bank said. CBC News; Globe and Mail

Ottawa et Gatineau se serrent les coudes pour Fort McMurray
Alors que les flammes continuent de faire des ravages à Fort McMurray, des collectes de dons sont organisées à Ottawa et à Gatineau pour venir en aide aux évacués. Vendredi soir, le Centre national des arts d'Ottawa recueillera des dons lors du spectacle de Royal Wood. Les dirigeants des mosquées d'Ottawa et Gatineau ont aussi lancé un appel à la générosité aux membres de leur communauté. Tous sont invités à faire des dons en argent à la Croix-Rouge canadienne. Radio-Canada

Fort McMurray : des travailleurs étrangers pourraient devoir quitter le pays
Des groupes militants affirment que les travailleurs étrangers temporaires forcés de se déplacer en raison de l'incendie qui ravage Fort McMurray courent un risque plus grand encore que les autres résidants qui ont dû fuir la ville du nord de l'Alberta. Ils affirment que plusieurs d'entre eux pourraient se retrouver en véritable situation de crise en ce qui a trait au logement, puisqu'ils n'ont souvent pas de famille ou d'amis pouvant les accueillir dans la région. La Presse Canadienne (La Presse); Radio-Canada

What gives Fort McMurray an edge in overcoming 'beast' of a wildfire
If you're stuck in an epic traffic jam, inching through billows of smoke as a wall of flame devours trees alongside you and you've no idea if your home or anything in it will be there when you get back, you'd be forgiven for freaking out. That didn't happen on Highway 63 this week. If an inferno's going to upend your community and force almost 90,000 people from their homes, Fort McMurray is pretty disaster-resilient — well positioned to cope, and bounce back. As a "nasty, dirty," "beast" of a wildfire tore through Alberta forest like kindling this week, tens of thousands of people and animals made it to safety and almost no one got hurt. That's not to minimize the damage: Two teenage girls died in a fiery car crash on Highway 881 Wednesday afternoon as their family made the trek south. And those 88,000 evacuees are stuck in limbo, not knowing when they'll be able to go home or what will be left of their homes when they do. Many, Wildrose leader Brian Jean among them, already know not much remains. Global News

Fort McMurray wildfire continues to take toll on Alberta oilsands
The wildfire ripping through the Fort McMurray, Alta., area continued to set back Alberta's crude industry Friday as concerns arose that the disaster may have taken out as much as half of Canada's oilsands output. It is difficult to say with certainty how much oilsands bitumen is offline because production levels have fluctuated throughout the week and companies have not disclosed precise figures. But Nick Lupick, an oilsands analyst for AltaCorp Capital, said his latest estimate is that between 1.1 million and 1.25 million barrels of oil per day have been knocked from oilsands production. Global News

Fort McMurray pets rescued by 'rogue' volunteer rescue team
The catastrophic wildfire has made a ghost town out of Fort McMurray. But Wyatt Colquhoun-Rivard and a small group of volunteers broke the smoke-heavy silence temporarily with the sound of breaking glass, as they smashed their way into homes looking for stranded pets. They ignored an evacuation order earlier this week to rescue as many stranded pets as they could, animals left behind by evacuees when they were ordered out of the city. CBC News; Canoë

Fort McMurray man watches his home burn on security cam
As James O'Reilly joined the exodus out of Fort McMurray on jammed Highway 63 on Tuesday, he watched the view from his home's security camera on his iPhone as flames broke through a window and devoured his living room. The video shows flames swirling outside O'Reilly's windows in the Abasand neighbourhood, just minutes after thousands of residents were ordered out of the city. CBC News

New homes spring up for Fort McMurray evacuees
Lac La Biche's newest neighbourhood is rising out of the ground in a matter of hours. Its residents are expected to move in almost immediately. Under the hot, springtime sun, crews are working to place dozens of mobile homes in the soil of the Alberta town, which lies 289 kilometres south of fire-ravaged Fort McMurray. CBC News

Firebreak around Fort McMurray wouldn't have saved city, official says
Building a firebreak around Fort McMurray wouldn't have helped prevent a wildfire from devastating the city this week, says Alberta's top wildfire official. "I want to be clear," Chad Morrison said at a news conference. "With the nature of this fire and the dangerous conditions we have, no size of firebreak would hold this fire from doing anything. This fire jumped the Athabasca River, which is over a kilometre wide." - Convoy of evacuees get 1st glimpse of fire-ravaged city After a wildfire destroyed about one-third of the town of Slave Lake in May 2011, the province commissioned a study that looked for ways to prevent similar disasters. The committee made 21 recommendations, but in its final report concluded there was little that could have been done to save the town, which suffered what was at time the second-costliest disaster in Canadian history, with an estimated $742 million in insurance claims. CBC.ca

Air assets play critical role fighting Alberta wildfire from the sky: experts
The image of a helicopter ferrying a small bucket of water through towering plumes of smoke made clear the daunting, seemingly futile, task of fighting the Fort McMurray wildfire from the sky. To observers, it was like flicking water on a raging grass fire. But experts in fire suppression and management say the aircraft play a critical role in a multipronged strategy in containing expansive fires. "It has a target and a usefulness, for sure," said Roger Collet, a wildfire prevention officer with Natural Resources in New Brunswick. Cape Breton Post

Broadcast Media / Médias télédiffusés :

CBC News provided live coverage of a news conference by the premier of Alberta, Rachel Notley, Brig.-Gen. Wayne Eyre, commander of Canadian Forces in Western Canada and other officials on the situation with wildfires and evacuations in Fort McMurray. The city of Fort McMurray is not safe to return to and this will be true for a significant period of time. The town site is going to be secured and protected by the RCMP. Rough Transcript

CTV News interviewed Sgt. Jack Poitras of the Alberta RCMP regarding searching for Fort McMurray residents who may have chosen to stay behind. Rough Transcript

CBC News - Power & Politics interviewed Alberta Premier Rachel Notley regarding the Fort McMurray wildfires. Rough Transcript

CBC News interviewed the Leader of the Opposition, Rona Ambrose, on meeting evacuees from Fort McMurray. Rough Transcript

CBC News interviewed Norm Sutton, Platoon Chief, Strathcona fire service, east of Edmonton. Rough Transcript

CTV News - Power Play interviewed Brig-Gen. Wayne Eyre, Military Commander for Western Canada regarding the federal assistance being offered to Fort McMurray. Rough Transcript

CBC News reported live from Alberta where Premier Rachel Notley and Edmonton Mayor Don Iveson provided an update. Rough Transcript

False alarm: Tsunami alert sent out in error for B.C. coast, Vancouver Island
Emergency officials in B.C. say an automated tsunami alert for most of B.C.'s coast and Vancouver Island was triggered in error. There is no tsunami threat to B.C. at this time, authorities are assuring residents. Emergency Management BC sent out an email alert Friday just before 2 p.m. incorrectly warning of a large earthquake in the Pacific Basin, including tsunami alerts for Haida Gwaii, Vancouver

Island and B.C.'s north and south coasts. The false alarm was set off during maintenance work on the BC Emergency Response Management System. CTV News

Most MPs endorse Comox coast guard station shutdown
A House of Commons committee gave its conditional nod of approval Friday to the federal government's planned closure next week of a communications station in Comox. Liberal and Conservative MPs on the committee, overriding the objections of the New Democratic Party, accepted the Canadian Coast Guard's argument that mariner and public safety won't be threatened by the move. "The committee has been sufficiently reassured that the capacity of the Canadian Coast Guard to respond to emergency situations has not diminished," stated a news release issued following the tabling of the report in Parliament. However, the committee issued a number of recommendations calling on the government to closely monitor the situation to ensure problems don't develop. Vancouver Sun

NATIONAL SECURITY / SÉCURITÉ NATIONALE

La GRC a saisi des calepins djihadistes troublants
En mai 2015, la GRC arrêtait in extremis huit jeunes soupçonnés de vouloir rejoindre les djihadistes en Syrie, à l'aéroport Pierre-Elliott-Trudeau de Montréal. L'une d'entre eux transportait deux calepins de notes troublants dans ses bagages. Ils détaillaient la marche à suivre pour les jeunes, et les raisons qui les ont poussés à partir en zone de guerre. L'un d'eux contient une lettre d'adieu. La jeune femme y explique qu'elle devait quitter le Québec, une terre des «mécréants», pour aller faire la «hijra», l'émigration dans un pays musulman, souligne une déclaration de la GRC qu'a obtenu notre Bureau d'enquête. Parmi tous les pays où l'islam est majoritaire, elle choisit la partie de la Syrie sous le contrôle de l'État islamique, «puisque c'est là que la charia est appliquée», selon le document, déposé à la Cour du Québec. Elle ajoute que «si un morceau des terres musulmanes est touché, il est obligatoire de faire le djihad pour repousser l'ennemi». «L'auteure dit que si elle tombe en martyre, Allah lui demandera qui sont les personnes qu'elle aime pour qu'ils puissent entrer au paradis», rapportent aussi les enquêteurs de l'Équipe intégrée de sécurité nationale (EISN), l'escouade antiterroriste que dirige la police fédérale. Journal de Montréal

Une ado montréalaise voulait quitter la « terre des mécréants »
C'est ce que révèlent de nouveaux documents judiciaires sur l'interception d'un groupe de jeunes soupçonnés d'avoir voulu rejoindre des djihadistes en mai 2015. Les documents ont été rendus publics aujourd'hui à la demande de plusieurs médias, dont La Presse. Dans la lettre saisie par les policiers, la jeune femme écrit avoir le choix de vivre à « Dar el kufr » (terre des mécréants) ou à « Dar el Islam » (terre de l'islam). Elle dit avoir l'obligation de faire la Hijra (immigration) parce qu'elle vit dans un pays de mécréants. Elle raconte partir vers le « Shaam » (la Syrie) « puisque c'est là que la Sharia, la charte des lois islamiques, est appliquée »... Elle évoque aussi ce que sera sa vie en Syrie. Elle dit que « personne ne lui a promis qu'elle vivra dans le luxe puisque c'est Dar el harb (terre de la guerre) ». Elle raconte qu'elle voulait se marier avec un « frère avec qui elle a fait des plans », mais que sa famille aurait refusé. Les documents ne précisent pas si le « frère » en question devait lui aussi faire partie du voyage. Il est important de préciser que le contenu de ces documents, préparés par la GRC, n'a pas été prouvé devant le tribunal. La Presse

Expert witness based report on accused Mountie's version of events, trial hears
A psychologist testifying at the trial of an Ottawa Mountie accused of severely abusing his son said he accepted the father's version of events as fact, and that those facts formed the basis of the report the clinician wrote for the court. The 44-year-old member of the Royal Mounted Police and his wife, the boy's stepmother, have both pleaded not guilty to aggravated assault, failing to provide the necessaries of life and forcible confinement. The father also faces charges of sexual assault causing bodily harm and assault with a weapon. His 37-year-old wife and step mother of the boy was also charged with assault with a weapon. A publication ban prevents naming anyone in the trial in order to protect the identity of the boy, who is now 14 years-old. The psychologist has treated the Mountie in more than 50 one-hour therapy sessions. CBC News

Eid's counsel mulls strategy for sentencing on fraud convictions
Former construction boss and CSIS informant Roland Eid appeared in court Friday for the first of what could be several sessions before Justice Timothy Ray in connection with the sentencing phase of his criminal fraud proceeding. Eid was convicted on Monday of 10 counts of fraud and other offences related to the 2008 bankruptcy of his firm ICI Construction. Ray ruled that Eid had perpetrated a fraud by shifting $1.7 million in company funds to a personal account in his native Lebanon - funds, the judge said, should have been held in trust to pay for wages and materials at ICI's ongoing projects. Ottawa Citizen

New allies in the war against extremism
Géraldine, in Belgium, learned of her son's death through a text message: "Congratulations," it said. "Be proud of him. He is now a martyr." Karolina Dam, in Denmark, got the same cold news delivered to her by a stranger with links to ISIS on her doorstep. Christianne Boudreau, at home in Calgary, got a call from a Canadian journalist who had seen a Tweet about her son's death in Syria and wanted a photo of him. For the mothers of jihadist recruits, without even a grave to visit, there is no Hallmark card or bouquet of flowers that will make this Mother's Day any easier. But what sets these mothers apart from the thousands of others living a private hell as they mourn their sons and daughters is their determination to spare other parents the same grief. A growing body of research suggests that mothers in Canada and elsewhere, given the knowledge and training, are uniquely well placed to prevent their children from becoming radicalized. In the global fight against extremism, they can be key allies, Boudreau said.(…) In senate hearings this week, RCMP commissioner Bob Paulson revealed that 63 jihadists have returned to Canada. Though alarming, the updated figures might still be low, since they may only include the people governments know about, or who have been reported missing by families and friends. Given the stigma and fear of prosecution for returning fighters, many families don't report them. That means potentially 62,000 parents in distress or mourning (...)Herman Okomba-Déparice, the head of Montreal's Centre for the Prevention of Radicalization Leading to Violence(https://info-radical.org/en/), has come to the same conclusion. "Among those who left for Syria, mothers are at the centre of their identity. If there's one person they will call from Syria, it's their mother - without fail," Okomba-Déparice said. "Radicalization doesn't erase their love for their mother. We have to capitalize on that." Gazette

Mayors are coming together to ignite change
When Mayor Matt Brown headed out to Edmonton in the first week of April with his just concluded Poverty Panel report in hand, he was only one of many politicians marking a change in the landscape of Canadian politics. Indeed, the official moniker of the conference said it all: "Cities Reducing Poverty: When Mayors Lead." It's far too early to tell whether this city's chief elected official will effectively implement the report of the panel (on which I served), but in Edmonton he found himself in dynamic company. Highlighting the conference were Naheed Nenshi (Calgary), Don Iveson (Edmonton), and Brock Carlton, the CEO of the Federation of Canadian Municipalities. Nenshi summed it up when he proclaimed, "It's time to push our conversation further: into our communities, the minds of our decision-makers, our business leaders, and others, and start creating partnerships together." … "Climate Change. Terrorism. Refugees. Inequality. Pandemic disease. In our interdependent 21st century world, nation states and international organizations are finding it ever more difficult to respond to the global challenges facing humanity. At the same time, cities are demonstrating a remarkable capacity to govern themselves democratically and efficiently, both locally and, in networks, globally." Postmedia Network (London Free Press)

Winnipeg man charged with child porn, bestiality offences
A police investigation that began in Switzerland has resulted in sex charges being laid against a Winnipeg man. Winnipeg police said Friday that Swiss investigators in Zurich and Aargau began an undercover investigation relating to child pornography in January. At some point, investigators determined a person utilizing an IP address in Winnipeg was not only in possession of child pornography, but also making it available to other users. Winnipeg's Internet Child Exploitation unit were told of the findings and, on March 22, raided a Renfrew Street house, seizing several electronic devices. Those devices contained numerous child pornography videos and photos, with police saying the kids being between the ages of two and 12. Andrew Harrison, 36, was arrested Thursday morning. He's been charged with possessing child pornography, accessing child pornography, and importing, distributing, selling, or possessing for the purpose of distributing or selling child pornography. Toronto Sun

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Trudeau looking into U.S. war-dodger issue but gives no commitments

The Liberal government is reviewing Canada's stance on American war dodgers that have sought refuge in this country rather than fight in Iraq, Prime Minister Trudeau said Friday. Trudeau, however, gave no commitments that Ottawa might smooth the path to permanent residency for the conscientious objectors, some of whom have been forced to return to the U.S. to face prison terms, but said the issue was a live one. "It's one that we are looking into actively as a government," Trudeau said after a transit-funding announcement in Toronto. He did not elaborate. Outside the transit yard where Trudeau was speaking, a handful of protesters from the War Resisters Support Campaign quietly held up a banner and signs calling on the government to let them stay. Last summer, a campaigning Trudeau criticized the Conservative government under prime minister Stephen Harper for acting in a way he called "lacking compassion and lacking understanding" when it came to U.S. soldiers. "I am supportive of the principle of allowing conscientious objectors to stay," Trudeau said at the time. He called it "problematic" and "disappointing" and unworthy of Canada that Conservative MPs had cheered in the Commons in 2012 amid word that one of the Americans, a mother of four, had been arrested after deportation to the U.S., where she was later court-martialled and gave birth in prison. "I am committed ... to restoring our sense of compassion and openness and a place that is a safe haven for people to come here." However, little appears to have happened since the Liberals took office last fall. In an email to The Canadian Press last month, a spokesperson for Immigration Minister John McCallum said he had "no indication that a decision was made or is about to be made" on the issue. Starting a decade ago, scores of U.S. military personnel who objected to the war in Iraq sought refuge in Canada. They argued the military effort had not been sanctioned by the United Nations and was illegal. Some have been fighting for years to obtain regular status while the government has sought to deport them. Hamilton Spectator

Western premiers call for more health care dollars, immigration, free trade

Canada's western premiers on Friday called on the federal government to increase its share of health care funding, to reduce barriers to immigration, to put more money into roads, rails and ports and to improve international trade access to natural resources. Wrapping up a two-day conference in Vancouver, the premiers struck a somewhat defiant tone as they laid many of the issues on their agenda at the feet of the federal Liberal government. Without changes from Ottawa, Canada's trade in resources and its workforce employment and health care will all suffer, they said. And to underscore their view that much of the country's economic power comes from Western Canada's natural resources, they pointed to the effect the Fort McMurray wildfire is having on the economy. On Friday, some economic analysts downgraded Canada's second quarter GDP growth forecast from 1.5 per cent to zero as a result of the wildfire's effect on Alberta's oil production. "If any Canadian listening today doubts how important Western Canada's natural resources are to this country, they should pay attention to that fact," said B.C. Premier Christy Clark. "As Fort McMurray burns, and as the economic infrastructure that has so long has supported Canadians is threatened, international observers are suggesting our economic growth is going to suffer disastrously." Vancouver Sun

A TPP deal falling victim to U.S. election may be good news for Canada

An opinion piece states "The road to ratification of the massive Trans-Pacific Partnership trade deal was always going to be long and arduous. The fact that trade-bashing Donald Trump is now the presumptive standard bearer of the U.S. Republican Party makes that journey all the more difficult in the months ahead. Oddly enough, the demise or postponement of the TPP just might be a good thing for Canada. Really? Canada is a small, export-oriented economy. Surely, this country should seize every opportunity to advance rules-based trade and break into new markets. Of course. But joining the 12-country TPP was always more of a defensive gambit for Canada, rather than about making substantive and transformative trade gains. New research bears this out. A recent C.D. Howe Institute study was the first publicly available economic modelling of what's in the deal for Canada. The study found that the country stands to make "relatively modest" gains from the TPP, including a 0.08-per-cent boost to GDP by 2035. The benefits are limited because tariffs are already generally low in the region, countries kept their most protected sectors off the table, and some companies won't bother going through the red tape to get the preferential access the deal offers, the study concluded. And besides, Canada already enjoys preferential access to the United States and Mexico through the North American free-trade agreement.TPP was a

rear-guard action for Canada, which came late to the table. The United States was bent on getting the deal done to create a counterweight to China in the region - with or without Canada." Globe and Mail

Taking down the walls to innovation
An opinion piece states "Canada faces an economic "wall" whether protectionists such as Donald Trump and Bernie Sanders win or whether Hillary Clinton does. The wall is a virtual one erected by Canadian governments that have not made emerging technologies a priority as well as the nature of the physical border and free trade agreement itself. Emerging technologies transform exponentially so a trade and taxation refresh is urgent. Historically, this has always been essential. In the 1960s Canada was about to be shut out of auto manufacturing and relegated to importing U.S. cars. That is when Ottawa policymakers invented the Auto Pact, which is a cornerstone of the country's living standards.Now the border has "thickened" again - to autos and oil - so Canadians face tough choices and must reinvent. Related The great fintech debate: Will regulating financial upstarts 'level the playing field,' or stifle innovation? If the Toronto-Waterloo region is to stay competitive it needs a better transportation link. In autos, Canadian taxpayers have been spending a fortune to build a second bridge to link Detroit and Windsor to stay in the auto game. In oil, the Keystone Pipeline XL has been nixed so other strategies are needed. And now Canada must join the new economy of robotics, nanotechnology, biotech, artificial intelligence, computation and energy." National Post

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Nearly three-quarters of firms globally hit by cyber attacks
Information security remains one of the most important concerns for data managers, and for very good reason. A new international study reveals that nearly three-quarters of organizations were the victims of a security incident in the past year alone. The International Trends in Cybersecurity report from CompTIA, the not-for-profit association for the technology industry, finds that nearly three out of four organizations globally have been plagued by at least one security breach or incident in the past year, with about 60 percent of breaches categorized as serious. The report also reveals that organizations are altering security practices and policies because of greater reliance on cloud computing and mobile technology solutions. More than 1,500 business and technology executives in 12 countries were surveyed. The report includes data from Australia, Brazil, Canada, Germany, India, Japan, Malaysia, Mexico, South Africa, Thailand, the United Arab Emirates and the United Kingdom. Health Data Management

LAW ENFORCEMENT / APPLICATION DE LA LOI

REAL SCOOP: Police face tech obstacles in criminal cases
RCMP Commissioner Bob Paulson was in B.C. in late March speaking to the Vancouver Board of Trade, as well as the Vancouver Sun's editorial board. One of the things he stressed was that police face real obstacles in trying to collect evidence from telecommunications companies, even when they have the court orders authorizing them to get the information. He said it's particularly an issue in child exploitation cases where online predators take great care to cover their tracks. I thought this was an interesting story to pursue, especially with the recent U.S. case where the FBI was battling in court with Apple over getting access to data stored on the iPhone of one of the San Bernardino shooters. Vancouver Sun

Coroner's jury finds man died by suicide after escaping RCMP custody
A coroner's jury is recommending more training and oversight of guards at RCMP detachments following an inquest into the death of a Hall Beach man who escaped from police custody. Tommy Anguilianuk died Jan. 21, 2013. Anguilianuk had asked a guard at the local detachment to let him get some fresh air at around 12:45 a.m. That's when he escaped. Bylaw officers found Anguilianuk's body about two hours later under the steps of a house. He had shot himself. Following this week's inquest, the coroner's jury ruled Anguilianuk's death a suicide and issued 13 recommendations, mostly to RCMP and the Government of Nunavut. CBC News

Okanagan men try to run but are arrested on North Thompson logging road
Three Central Okanagan men on parole are facing at least a half dozen charges each after speeding past an officer on Highway 5 south of Little Fort this week. A Clearwater RCMP officer saw two vehicles approaching him rapidly from behind around 1:30 p.m., May 4, Cpl. Dan Moskaluk says in a release. "The officer pulled over to the side of the road and in an attempt to simply slow the vehicles down and carry on with his other duties, he activated his rear emergency lights to get the drivers attention," Moskaluk says. "The two vehicles then increased their speed and sped past him." An RCMP Air Services helicopter, a dog team from Kamloops and back-up from 100 Mile House and Barriere Detachments were called. InfoNews.ca; Global News

RCMP seek suspect in huge 2015 Bobtail Lake, B.C. wildfire
As several major wildfires rage in northeastern British Columbia, Prince George RCMP are still searching for the person, or people, suspected of sparking a forest fire one year ago. The Bobtail Lake blaze was first spotted on May 8, 2015. It charred 240 square kilometres of woodland 50 kilometres southwest of Prince George and forced evacuation of properties at Norman Lake and Naltesby Lake, also known as Bobtail Lake. The fire took weeks to control, and RCMP and Wildfire Management Branch officials confirm it was human-caused. CTV News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Godin named national union president
A former federal correctional service officer with Kingston ties has been acclaimed president of the national union that represents officers working in institutions across Canada. Napanee native Jason Godin, who is also a founding member of the Union of Canadian Correctional Officers, was officially given the position for a three-year term at the union's national general assembly in Quebec City this week. "I'm completely honoured to lead our members over the next few years," said Godin on Friday morning while making his way back to Kingston, where he lives and from where he works. The union represents more than 7,200 correctional officers nationally, with approximately 1,600 working in the Ontario region and 1,000 of those in Kingston-area institutions... Looking forward over the next three years, Godin has a few items he'd like to see dealt with. "Priority No. 1 for us is to settle the collective agreement with the current government that clearly recognizes our distinct working conditions," he said. Godin said he and his executive enjoy a good working relationship with CSC commissioner Don Head. Godin said they meet at least eight times a year. Kingston Whig-Standard

Mark Steven Vandendool, who robbed a bank to get into McGill University, now charged with a dozen holdups
In February 2006, Mark Steven Vandendool desperately wanted to get into McGill University's Schulich School of Music. The Kitchener, Ont. resident was 24 and showed promise as a guitar player. By his own admission his life at that point was heading nowhere (something that would later be attributed to an undiagnosed case of attention deficit disorder) and he figured his passion for classical guitar would provide him with a goal he cared about pursuing. He hoped to audition for the school, but his car wasn't working and he didn't want to ask his parents for help. So on Feb. 20, 2006, he walked into a bank in Plattsville, Ont. — a small town about 20 kilometres southwest of Kitchener — armed with a fake gun. He used it to threaten two bank tellers inside and demanded they give him $50,000... He passed the audition and was accepted to the prestigious McGill school, but that posed another problem for Vandendool. As he would later tell the Parole Board of Canada, he also needed money for tuition. This, according to Vandendool, explains why, on March 2, 2006, he tried to rob a TD branch in New Dundee, Ont., about 10 kilometres southwest of Kitchener, but failed miserably... Vandendool received an overall five-year sentence (which was later reduced to three years through an appeal), but held on to his music dream while serving the prison term at a federal penitentiary in Ontario. He spent his spare time in the penitentiary's chapel, practising classical guitar and providing lessons to other inmates. He worked full-time cleaning the penitentiary and Correctional Service Canada staff later created a position for him as a music coordinator for chapel functions. Montreal Gazette

Hearing for Maurice (Mom) Boucher switched to Montreal for security reasons
A judge has ordered that murder-related proceedings involving former Hells Angels kingpin Maurice (Mom) Boucher be switched to a Montreal courthouse. Boucher is to have a preliminary hearing next week on charges of conspiracy to murder crime figure Raynald Desjardins in prison. The hearing was to be held in Longueuil, but a judge agreed Friday to a Crown request it be moved to the Gouin courthouse. That Montreal facility is linked by a tunnel to a detention centre where Boucher will stay during the hearing. Gazette; La Presse

Seizure of contraband at Dorchester Penitentiary
On April 24, 2016, at 9 p.m., three packages containing drugs and tobacco was seized outside the perimeter of Dorchester Penitentiary, a medium security federal penitentiary. The contraband seized included tobacco, hashish, nicotine patches and fentanyl patches. The total estimated institutional value of this seizure is over $63,000. The Correctional Service of Canada (CSC) has set up a telephone tip line for all federal institutions to receive additional information about activities relating to security at CSC institutions. These activities may be related to drug use or trafficking that may threaten the safety and security of visitors, inmates and staff members working at CSC institutions. Sackville Tribune Post; Global News

'You are at a crossroads,' Judge tells Matthew King as he heads to jail for assault
In sentencing Matthew King to four years for aggravated assault, a judge in St. John's said King has shown no remorse for the vicious attack on his former girlfriend that left her with fractures to her face, two missing teeth, and other injuries. The assault happened in the home King, 26, shared with his girlfriend Julie Summers in the Goulds area of St. John's in April of 2015. CBC News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Provinces 'in the weeds' on how to handle pot shops, Wynne says
Ontario Premier Kathleen Wynne says storefront shops selling marijuana will continue to blur the lines of the law around pot until the federal government clarifies the rules around the use of recreational weed. The federal government plans to unveil new legislation next spring that would legalize cannabis. In the meantime, cities have seen a growing number of marijuana dispensaries open up. Wynne says cities and provinces remain confused over what to do with those pot shops because Ottawa has yet to clarify rules between recreational and medicinal marijuana. CTV News

Pharmacies should be allowed to sell medical marijuana, Loblaw president Galen G. Weston says
Galen G. Weston wants in on the medical marijuana business. Weston, the head of the country's largest drugstore and grocery chain, said Thursday that pharmacists are well-positioned to dispense the drug in a safe manner. "We're an industry that is extremely effective at managing controlled substances," said Weston, Loblaw's president and executive chairman, following the company's annual general meeting Thursday. Canadian Press (National Post)

Medical marijuana dispensaries 'verging on being out of control,' Mayor John Tory says
The proliferation of medical marijuana dispensaries across Toronto neighourhoods is "verging on being out of control," Mayor John Tory said Friday, hinting that city officials may have to find a way to curb the growing number of pot shops. "I don't think it's sustainable for neighbourhoods, and for life in neighbourhoods that we want to be peaceful, quiet and law-abiding, to have 20, 21, 31 medical marijuana dispensaries," said Tory Friday. "You have to do these things in an orderly way that respects public safety and health and access to minors." Tory said he spoke about the issue 10 days ago with Bill Blair, Toronto's former police chief and now parliamentary secretary to the justice minister. Blair is also the Liberal government's point man on pot legalization. CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

Top bureaucrat identifies workplace mental health and PS renewal as top priorities
In his annual report, the clerk of the Privy Council has put renewed emphasis on improving mental health in the public service and increasing and accelerating the effort to renew the bureaucracy with new blood.The federal public service is Canada's largest employer with about 257,000 employees. Michael Wernick's report to the prime minister was tabled Friday morning. The document trumpeted successes including: The effort to resettle thousands of Syrian refugees in Canada; Moving goods across the Canada-U.S. border, at a rate of over $1 million a minute; and, Processing 82 per cent of all tax returns electronically. Wernick is the 23rd clerk of the Privy Council. He was appointed to the top job in the federal bureaucracy on Jan. 22. Ottawa Citizen

OTHER / AUTRES

NIL

INTERNATIONAL

Le mystérieux lanceur d'alerte des Panama Papers s'explique dans un manifeste
Il écrit dans un anglais soigné et possède un sens critique acéré : le lanceur d'alerte à l'origine de la fuite monumentale des Panama Papers ne dévoile guère d'informations sur lui-même dans le manifeste qu'il vient de publier. Mais pour que le scandale serve à quelque chose, et pour que cessent les violations d'une myriade de lois en matière de fiscalité, il se dit prêt à collaborer avec les autorités, à la condition qu'on lui assure l'immunité. Car il ne veut pas subir le sort des Edward Snowden, Bradley Birkenfeld et Antoine Deltour. Ces lanceurs d'alerte « ont vu leur vie détruite par les circonstances dans lesquelles ils se sont trouvés après avoir révélé d'incontournables malversations », dénonce-t-il dans le manifeste qu'il a confié au Süddeutsche Zeitung et qu'il a intitulé « La révolution sera numérique ». Radio-Canada

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Fire

CanadianPM
The government's match of individual donations to @redcrosscanada will backdate to May 3rd and continue to May 31, without a cap. #ymmfire

RMWoodBuffalo
1200-1400 vehicles have already passed through Fort McMurray on their way south - will continue as conditions permit #ymm #ymmfire

RachelNotley
Here's my latest update on the wildfire situation in Northern Alberta: http://bit.ly/1YdrBtY #ymmfire #fortmacfire

CBCNews
Firebreak around Fort McMurray wouldn't have saved city, official says http://ift.tt/1SSFbTv

Other

CTV_PowerPlay
ICYMI: BC Premier @christyclarkbc says the Feds need to be faster with monetary support after disasters http://goo.gl/VIF4y2 #cdnpoli

Safety_Canada
We're working w/ provinces & territories to restore funding for heavy urban search & rescue programs. #EMFPT2016 #EmergencyManagement

Securite_Canada
Travail avec prov./terr. pour rétablir financement progr. recherche/sauvetage en milieu urbain équipement lourd. #GUFPT2016 #GestionUrgence

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Sent to: !INTERNAL; CBSA Today's News; CSC & PBC Today's News; PS Today's News; RCMP Today's News; RCMP Today's News 2

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
May 1, 2015 / le 1 mai 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

Lawyer suspended from security committee
A Hamilton lawyer and former chair of the defunct and scandal-plagued SISO has been suspended by the federal government from his longtime position as a member of the Cross-Cultural Roundtable on National Security. A spokesperson for federal **Public Safety Minister Steven Blaney** said Hussein Hamdani has been suspended from his advisory position pending an investigation into allegations of whether or not he has links to "***radical ideology***." A news report by French-language network TVA of Quebec published Wednesday raised questions about written statements made by Hamdani nearly 20 years ago. The news report also made allegations suggesting Hamdani has been involved in the past with organizations that have provided funding, directly or indirectly, to groups associated with terror. Jeremy Laurin, press secretary for **Blaney**, said in a statement the allegations against Hamdani are "***very concerning***." "***While questions surrounding this individual's links to radical ideology have circulated for some time, it was hoped that he could be a positive influence to promote Canadian values in the Muslim community***," Laurin stated. "***It is now becoming clear this may not have been the case***." Hamdani said in an email that he has no comment at present on either the suspension or possible investigation. "I have not been formally informed that I have been suspended or that there is a review ongoing," Hamdani's statement said. "It would be premature for me to give a comment until I get all the facts from the officials directly." In a subsequent telephone interview, he categorically denied the allegations made in the TVA news report. "I have long denied them and I continue to deny them," said Hamdani. "This is just an attempt to silence a prominent voice in the Muslim community." Hamdani was one of the original 15 people who was appointed to the roundtable when it was created by the federal government in 2005. Hamilton Spectator. A1

Ex-NHL goaltender fears for his family's lives
It was the call former NHLer Don Edwards had been fighting to avoid for 24 years. George Harding Lovie had brutally murdered his parents, stalked and raped his sister, and had a standing threat to murder any other member of the Edwards family he could find, including Don's children. And then, with almost no warning, this month Corrections Canada informed the Edwards family that they had decided to start letting Lovie out on unsupervised work releases. "We have no idea what he's doing or where he is, all we know is that he's in the Gravenhurst area," said Edwards, who is now campaigning hard to get Lovie back behind bars. He's contacting local media, sending out appeals to **Public Safety Minister Steven Blaney** and Prime Minister Stephen Harper and, at the very least, warning residents of Gravenhurst that there's now a killer in their midst. "We're fighting like hell to keep this guy incarcerated," he said. "We honestly feel that our family's lives are in danger; we also feel that other Canadian citizens' lives are in danger." In 1990, Edwards' sister Michele broke offa six-month relationship with Lovie after she found him becoming overly possessive. But Lovie continued to stalk Michele for months, and on Feb. 18, 1991, he broke into her home with a borrowed knife and gun and forcibly confined her for six hours, alternately raping her and threatening to kill her and her family if she told authorities. She reported the crime to Hamilton Wentworth Regional Police, who arrested Lovie but released him after two days. Four weeks after that, he followed through on his threat. Armed with a newly purchased rifle, he surprised Michele near her parents home, and shot at her as she ran inside for protection. He shot Michele's mother, Donna, as she attempted to barricade the doors. Arnold, Michele's father, rushed forward to confront the intruder, and was stabbed multiple times. Ottawa Citizen, C1 (National Post, Calgary Herald, Leader-Post, StarPhoenix, Windsor Star)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Middle River : inondation et évacuation**
Les quelques résidants évacués sur la rue Mathilda, à Middle River, près de Bathurst, attendaient toujours, jeudi, que le niveau de l'eau baisse pour rentrer chez eux. Dans cette localité, située à une douzaine de kilomètres de Bathurst, les familles affectées sont parties d'elles-mêmes, mardi vers 18 h, en raison d'embâcles qui se sont formés sur la rivière Middle. L'Acadie Nouvelle, A2

*** Canada, U.S. to announce rail safety standards**
Canadian and U.S. transportation officials will announce new standards for tank cars carrying crude oil and other flammable liquids during a meeting in Washington on Friday morning. The long-awaited deal is expected to outline time frames for phasing out older, less durable tank cars and transitioning to a "next generation" standard with thicker steel and thermal protection. The changes are meant to help the cars better withstand a derailment and collision while limiting the amount of crude that can spill and ignite. Canada has already proposed a 10-year phase-in period for the new tank cars, but regulators in the United States have not yet announced their plans. The Canadian proposal has been criticized by safety experts, who say it will leave weaker tank cars on the rails for too long. Globe and Mail, A4

*** Forest fire season begins today on island, May 15 in Labrador**
Newfoundland residents preparing to burn brush as part of spring clean-up activities around their properties should note that the 2015 forest fire season is now underway. This year's season opened Friday and will run until Oct. 15. For the island, this year's season has been extended by two weeks in the fall, due to above-average temperatures and increased forest fire activity in recent years. In Labrador, the season begins on May 15 and ends on Sept. 30. CBC.ca

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Should Canadian military personnel and the country's spies be protected by a whistleblower law?
The Ottawa-based Democracy Watch has raised the issue of ensuring that whistle-blower protection is extended to members of the Canadian Forces and the country's spy agencies. The organization repeated its recommendation in the wake of a report released Thursday outlining numerous cases of sexual

harassment and assault in the Canadian military. Democracy Watch noted that the Canadian Forces are exempt from the federal whistleblower protection law. That means a whistleblower in the military cannot complain to the federal Integrity Commissioner "and instead is forced to file a complaint to people who are in the military and who are not fully independent from the chain of command," the organization pointed out. Democracy Watch recently sent a letter to Prime Minister Stephen Harper and the federal Cabinet calling for key changes to ensure people who work within Canada's spy agencies and military are protected if they blow the whistle on wrongdoing. The federal whistleblower protection law exempts the Canadian Security Intelligence Service (CSIS), Canadian Security Establishment (CSE) and the Canadian Forces from the requirement to have an employee code of conduct, and does not protect people who work at these institutions if they blow the whistle on wrongdoing, Democracy Watch points out. In contrast, Security Intelligence Review Committee (SIRC) - which helps oversee CSIS is required to have a code of conduct and people who work there are covered by the whistleblower protection law, it added. "Conduct codes and independent, effective whistleblower protection are essential to prevent abuses of power and it is extremely dangerous that Canada's spy agencies and military are not required to have these key accountability measures," Duff Conacher, co-founder of Democracy Watch and Visiting Professor at the University of Ottawa said in a statement. Ottawa Citizen.com

* **Privacy? There is tweet irony in that - Even without surveillance cams, our lives are for all to see**
Digital witnesses, what's the point of even sleeping? / If I can't show it, if you can't see me / What's the point of doing anything? Those lyrics come from the St. Vincent song Digital Witness, a comment on our times if there ever was one. Last spring, I had the pleasure of interviewing the singer/songwriter, who also goes by Annie Clark, for this paper. When I asked her about that song, Clark said she was interested in exploring the overlap between surveillance and our increasing tendency toward Internet over-share. She was astonished at how much of ourselves we give away for the consumption of others and how freely we give it. When is TMI actually TMI? "We had a hunch that we were being watched, and thanks to Mr. (Edward) Snowden (the NSA whistleblower), we had our hunch very much confirmed," she said in our interview. "We have the knowledge that the government is looking in on us, and then we have the other side of that, which is this platform on which we can create an idealized version of ourselves that can be as aspirational as we want - but it's two-dimensional. We equate day-to-day minutiae with news. We're all the star of our own show." I was reminded of that interview when reading about downtown surveillance cameras. Footage from one camera proved instrumental in finding John Paul Ostamas who, in a matter of days, was charged with the homicides of three vulnerable men.[...] If you are on the Internet, you're already living under surveillance - by digital companies, certainly, and potentially the so-called "incidental" surveillance by governmental agencies such as the NSA or the Canadian electronic spy agency, the Communications Security Establishment (CSE). But we also surveil each other. We, too, are digital witnesses. The average social-media user isn't doing this in a malicious way - though how "Facebook creeping" became regarded as the cutesy, innocuous cousin of stalking I'll never know. Winnipeg Free Press, A4

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Governor General touts border security during Detroit visit
Canada's Governor General completed his Midwest tour of the U.S. with a stop in Detroit Thursday morning after taking a personal tour of the cross-border law enforcement team known as Shiprider. David Johnston addressed members of the U.S. Coast Guard and the RCMP praising them for their work in securing the shared North American border and for sending a strong message to smugglers who have long gone undetected in some of the shared international waters. "The Shiprider program is but one example in a long history of such co-operation on border security between our two countries," he said in his speech during a visit at U.S. Coast Guard Sector Detroit. "This program is so important, because so much of our border runs through waterways." Shiprider, with the official title of Integrated Cross Border Maritime Law Enforcement Operations, is a team of specially trained officers with status to work together in shared international waters along the Detroit River. "Both Canadians and Americans are dedicated to border security," Johnston said. "What could be a better image of this than RCMP, U.S. Coast Guard and other law enforcement officers working together on the same boat?" The governor general then took a tour of the Detroit River on a patrol boat to get a closer look at Shiprider operations. "What struck with me

the most was this enormous willingness to make such a strong relationship between the two countries and see our border as secure as possible," he said later in an interview. The border security program has been touted as a huge success by governments on both sides of the border. What began as a pilot project in 2007, with teams operating in Ontario and B.C., eventually led to temporary Shiprider teams working during special events like the 2010 Vancouver Olympics. Windsor Star, A3

Quebec deplores changes to foreign worker rules

Quebec cabinet ministers warned the province could lose jobs unless Ottawa backs down on recent changes to the temporary foreign worker program. Quebec had asked the federal government to delay the reform until they could reach a compromise, but new restrictions on hiring temporary foreign workers came into effect Thursday. The program allows employers who can't find qualified workers locally to recruit them abroad. Last June, after media reported that some employers abused the program, the federal government tightened the rules. In some job sectors, including retail, businesses can no longer hire a temporary foreign worker in a region where the unemployment rate is above six per cent. Montreal, Laval, Sherbrooke and many other regions' jobless rate was higher than that last year. Many Quebec businesses have complained that the new restrictions will make it harder for them to find the workers they need, Immigration, Diversity and Inclusiveness Minister Kathleen Weil said. They have also told her the new rules could lead them to move some of their activities south of the border. To make matters worse, while the western provinces and Ontario benefit from a growing workforce, Quebec's is in decline, she told the Montreal Gazette. "Our situation is that the shortage is going to get worse," she said. "Immigration, whether it's temporary or permanent, is how we can solve that problem." Quebec is still pressing the federal government to relax some of the new rules. "This is not the end of this exchange (with Ottawa). It can't be," she said. "It's just so irrational that we would somehow hamper the development of our businesses, certain sectors, our regions and our economy." The office of federal Employment Minister Pierre Poilievre said the point of the reform is to ensure that Quebecers are hired before foreign workers. Montreal Gazette, A6

A duty-free duty to travellers - Emerson shop at border the first one in Canada outside an airport

Trivia question: Where was the first duty-free shop in Canada outside of an airport? The place name above gives it away so here's an added question: What year did it open? Mike Resch opened the first "land" duty-free shop in the country in Emerson on Dec. 15, 1982. He still has his original licence with the "No. 1" to prove it. "It was part of a pilot project. There were only six licences issued: in B.C., Alberta, Saskatchewan, Manitoba, Quebec and New Brunswick," explained Resch, 69. "The reason Ontario wasn't given one was because the federal government couldn't come to an agreement with the bridge owners, who wanted their own shops." Resch is originally from Germany, where he was a ski enthusiast, regularly crossing the border into Austria and making purchases at duty-free stores. When he moved to Emerson, he wondered why there were no duty-free shops beyond those in airports. The first duty-free shop in the world opened in Shannon Airport in Ireland in 1947. Resch joined a lobbying effort by the tourism industry in the late 1970s to increase traveller money spent on the Canadian side through duty-free stores, says son Simon, who manages the Emerson Duty Free Shop. But it was a rough start for the duty-free shops in the early 1980s. Canadian travel to the United States quickly fell off when the Canadian dollar plunged to the low 70-cent US level. Winnipeg Free Press, A7

Anger, questions remain over Moroun's deal with Detroit mayor

Some community leaders who have spent over a decade fighting against Ambassador Bridge owner Matty Moroun expressed anger Thursday over a closed-door deal with Detroit Mayor Mike Duggan that moves the billionaire a huge step closer to building a new six-lane span next to his current bridge. What is the proposed agreement? The deal would see glass, grass and $3 million in cash handed over by the Morouns in exchange for the rights to a section of city-owned Riverside Park - the last property required by the bridge owner in Detroit to pave the way for construction of a twin span. Three acres of municipal land - Riverside Park - will go to the Ambassador Bridge. In exchange, the bridge company will provide the city with five acres of other riverfront property it owns, plus $3 million for park improvements. Another $2 million will come after the state of Michigan approves the land transfer. Permits for his twin span on the U.S. side have stalled because Moroun for years had been unable to acquire portions of the park he needs. About five years ago, he fenced off a large section of the park, called it his own and even installed armed security. A community backlash put Riverside Park back in the city's hands. The proposed deal

also calls for 1,050 windows to be installed by Moroun at the Michigan Central Depot - the abandoned train station west of the bridge he has owned for nearly 20 years. Who's upset? "I'm extremely disappointed the mayor would sit down with Moroun before he even talked to residents about this," said former state representative and community activist Rashida Tlaib. "He opened the door to (the Morouns) after we have worked on this for so long." Windsor Star, A2

Vancouver developer says he's innocent of corruption charges he faces in China
A wealthy Vancouver businessman is heading to the Federal Court of Canada in June as part of his lengthy bid to avoid being sent to China to face corruption charges. Mo Yeung (Michael) Ching, also known as Cheng Muyang, was named last week by Chinese state media as being among the country's top 100 fugitives, a list that includes 25 others in Canada. But Ching has alleged that the evidence against him was a product of torture, and he has also suggested the charges were influenced by domestic Chinese politics. He has not been tried or convicted of any crime. Ching has a lot at stake, as he faces a maximum penalty of life in jail on the charge of "misappropriation of public funds, embezzlement [and] transfer and concealment of illegally acquired goods," according to the 2001 arrest warrant obtained by the Vancouver Sun. Times Colonist, B4

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP boss praises Moncton for resilience in tragedy
RCMP Assistant Commissioner Roger Brown says plans are progressing for a permanent memorial in Moncton for three officers killed in the line of duty last June, but details of what form it will take and where it will be located have not yet been decided. Brown was in Moncton on Thursday to speak to members of the Greater Moncton Chamber of Commerce on the subject of leadership. He praised the citizens of Moncton for their support of the RCMP in the aftermath of last year's shootings and said we all have the capacity within ourselves to become good leaders and make a difference in the lives of others. Brown said the process of planning the monument is underway with input from the federal, provincial and municipal governments, led by the mayor's office. He said federal funding has already been set aside, and artists from across the country have been asked for proposals for a design. "We want a memorial that reflects the lives of these three individuals, not just as police officers but as dads, as community members, and something for the community to reflect on the impact, the input and the like," Brown said. The process is well underway." He said the committee will invite community input on the monument on what it will look like and where it will be located. "We want to come up with a monument that is appropriate to reflect what we all went through together," Brown said. In his speech to members of the Greater Moncton Chamber of Commerce, Brown said the shooting deaths of three RCMP officers last June 4 was a traumatic time for him and all members of the force, but it was also a time when "the community was there for us when we really needed them." Times & Transcript, A1; L'Acadie Nouvelle

Informant pays off in crystal meth probe
So determined to crack down on a drug booming in popularity and wreaking havoc on the streets, London's drug squad used a rare tactic, a police "agent." The agent -- someone already immersed in the city's drug subculture -- was paid as an informant to work with dozens of undercover officers during a three-month probe focused on getting crystal methamphetamine off the streets. It marked the first time investigators have singled out the drug that propelled the Breaking Bad TV series. Outreach workers blame the synthetic drug for ravaging addicts in the city. "It's the one that's making people sick. It's the one that's putting people in the hospital. It's creating addicts. It's weakening our society," said Det. Sgt. Chris McCoy, head of London's guns and drugs unit that headed the joint investigation with the RCMP. "It's a bad drug. There are overdoses all the time," McCoy said. "We were looking to dealers of crystal meth. We wanted to find out how it is coming into our city. We knew primarily who our dealers were but we wanted to learn more about chains of supply." London police rarely use agents in drug probes. In the

last 20 years, agents were used in four joint investigations with RCMP, McCoy said. After the three-month probe that included dozens of undercover officers, police searched 10 residences -- nine in London and one in Waterloo -- arrested 12 people and seized drugs, cash, seven cars and a gun. Though they got some of what they were after -- about 1.7 kilograms of crystal meth valued at $171,100 -- police got a larger quantity of crack cocaine and also seized about 1.4 kilograms of cocaine. London Free Press, A1

Harper security files kept sealed

A judge has ruled that the unusually strict sealing order on a case involving allegations of leaks from the prime minister's RCMP protective detail shall stay in place. Ontario Superior Court Justice Mary Vallee rejected the arguments of media lawyer Brian McLeod Rogers, who applied two weeks ago for her to unseal documents in an affidavit filed in December by a lawyer acting for Sgt. Peter Merrifield, who is suing the RCMP for harassment and bullying, alleging systematic abuse and coverups by senior Mounties. The documents, which are believed to contain information about Prime Minister Stephen Harper's family, were sealed by Vallee in December at the request of lawyers for the federal Justice Department, who have been fighting Merrifield's suit on behalf of the RCMP. Rogers argued in court that Vallee should unseal portions of the documents, which are believed to have been sealed because they contain information that could identify a confidential informant. But Vallee ruled Thursday that none of the information can be made public and she can't say why. "All of the information in those materials and the order relates to a subject matter which must be protected from disclosure," she wrote... Sources say the sealed affidavit in this case is accompanied by four letters sent by private investigator Derrick Snowdy to assistant RCMP commissioner Stephen White. The letters contain allegations about RCMP wrongdoing, including repeated information leaks that threaten the safety of confidential informants, and the leak of private information about Harper's family by officers from the prime minister's protection detail. Postmedia news (National Post, Windsor Star, D1, StarPhoenix, Vancouver Sun, Montreal Gazette, Calgary Herald, Edmonton Journal, Ottawa Citizen); Canadian Press (Times Colonist)

New police chief stands by carding comments

Facing blowback after revealing he has no plans to abolish "carding," new Toronto police Chief Mark Saunders is standing by his statement that crime would increase if the controversial practice halts, saying he can't please everyone. "If I don't get criticism, I don't think I'm doing the job right. I don't expect the entire world to think that what I say is right, and that we're all going to be happy about it," he told reporters Thursday, after a brief appearance at the Young Men's Stand Up conference at George Brown College. Not a week into the job - he took over from outgoing chief Bill Blair on Sunday - Saunders is on the receiving end of criticism for saying on Wednesday that abolishing carding was "not the way in which we are going to say 'everything is going to be better.'" Saunders made the remarks to reporters after his first public appearance as chief at the Second African Canadian Summit, where he assured attendees he was committed to bias-free policing and improving officer training to eliminate "random" street stops. "We are not going to be random at what we record," Saunders said Thursday. But Saunders maintains that ending carding would compromise public safety. Toronto Star

OPP to investigate Vaughan deputy mayor Michael Di Biase

An OPP investigation has been launched into Vaughan Deputy Mayor Michael Di Biase's role in development deals, according to the man who filed the complaint. Richard Lorello alleges Di Biase's cottage is being built with the help of one of the companies that Di Biase may have helped get work from the city. "Today (Thursday) around 2 pm, an OPP officer said the OPP was taking over the investigation," Lorello told the Star. Shortly after, he says, he was also contacted by an OPP detective inspector with the criminal investigations branch. "In the last 48 hours, between the York Regional Police and the OPP, they decided that the OPP would take over the investigation," Lorello told the Star. Lorello has a history of challenging Vaughan council members on issues of transparency and accountability and has unsuccessfully run for council. Earlier Thursday, the Vaughan Citizen reported that, according to its sources, York Region Police had launched an investigation into city contracts signed during Di Biase's 24 years in office, including his time in the mayor's chair from 2002 to 2006 and, more recently, while a local and regional councillor. Officers are also looking into any role he might have played in the city's tendering process to secure municipal contracts for companies, including Maystar General Contractors, the firm that built Vaughan city hall, a source told the Citizen. The Star could not confirm with either the OPP or York police that a formal investigation has been launched. Lorello stated he had been clearly told by the OPP

that an "investigation" is underway. Toronto Star

London costs in line with similar forces

As Brad Duncan moves through his final week as London police chief, he hands the badge to successor John Pare with encouraging news attached. Though the new top cop will face the same financial pressures -- annual raises for officers that drive up the force's ballooning budget -- an audit presented to politicians this week indicates London police spending is in line with other municipal forces. "I think this is a good news story in terms of our performance relative to other communities," Paul Paolatto, a member of the board that oversees London police, told city hall's audit committee. Paolatto was among the police brass uncomfortable when the previous council, led by then-councillor Matt Brown, called on police to follow other city-funded agencies and open their books to an external audit. Last year, London police did so, and a review by PriceWaterhouseCoopers suggests the pressures driving up the London police budget -- it checks in at more than $93 million this year -- are faced by other cities, too. In fact, by some measurements London police are performing better than comparable cities. In a recent interview, Brown, now mayor, applauded police brass for agreeing to the audit. Police have already started reducing costs by cutting jobs and closing their headquarters overnight. "They've worked hard to find savings and efficiencies and we've been able to change the conversation, when we compare what we were seeing a few years ago to the progress we're seeing today," Brown said. For context, today's $93-million police budget was only $59.8 million a little more than a decade ago. London Free Press, A4

Man arrested after two-day armed standoff with police

A two-day armed standoff with police ended without any injuries after a man was taken into custody Thursday morning, RCMP said. Mounties first responded Tuesday afternoon to reports of a "distraught" man, and later said shots were fired from within the home. This prompted police in Iqaluit's Happy Valley neighbourhood to block off the area and shut down a nearby school. "(It's a) volatile situation," RCMP Const. Malcolm McNeil said by phone from Nunavut's capital Wednesday night. The city of Iqaluit and the Red Cross had set up an emergency shelter at Iqaluit's Arctic Winter Games complex on Tuesday for people who didn't have anyone to stay with outside their neighbourhood. Police had closed the nearby Joamie elementary school Tuesday because it was "in view" of the barricaded house, McNeil said, noting that children are often "sledding on the hill and playing" outside the school. RCMP said the blockades would remain for an undetermined length of time Thursday while they investigate. Postmedia Network (Kingston Whig Standard, Edmonton Sun)

Deux conducteurs d'autobus scolaire accuses

Des policiers de la Sûreté du Québec et de la GRC ont procédé à l'arrestation de 11 individus dans le cadre d'une opération visant le démantèlement d'un réseau de vente de méthamphétamine dans la région de Drummondville. Les deux présumées têtes dirigeantes étaient conducteurs d'autobus scolaires. Rocky Robitaille, 48 ans, et France Brochu, 53 ans, travaillaient depuis près d'une dizaine d'années pour Bourgeault et fils, l'un des transporteurs affiliés à la Commission scolaire des Chênes. Leur rôle consistait bien évidemment à amener des élèves vers leur milieu scolaire. Également employé chez Bourgeault et fils, Daniel Côté connaît les accusés depuis quelques années. Rien, selon lui, ne laissait présager tel événement. «Je suis très, très surpris. Ça démontre que parfois les gens ont une vie cachée. Il y a bien eu quelques anicroches au fil des ans, mais ça allait très bien, ils étaient de bons travailleurs», estime-t-il. Lors de son embauche, M. Robitaille n'avait pas d'antécédent judiciaire. Il a bien eu quelques démêlées avec la justice qui ont été source de discussions avec les propriétaires de l'entreprise. Les gestionnaires ont finalement jugé que l'écart de conduite ne justifiait pas un congédiement. Selon la porte-parole de la SQ, Éloïse Cossette, Robitaille, Brochu et au moins une dizaine de complices auraient été impliqués dans le trafic de méthamphétamine à raison de plusieurs milliers de comprimés par semaine. Les policiers ont réalisé huit perquisitions dans des résidences de Drummondville, L'Avenir et Saint-Germain-de-Grantham, ainsi que dans neuf véhicules qui ont tous été saisis comme biens infractionnels. Près de 5000 comprimés, de la cocaïne, du cannabis, 36 000 $ en argent ont été saisis et ces chiffres pourraient être appelés à grimper, l'opération étant toujours en cours. La Tribune, 22

Le fisc québécois en profite

Le nombre de contrebandiers de tabac arrêtés et la valeur des impôts qui leur sont réclamés ont fracassé des records l'an dernier, selon de nouveaux chiffres compilés par la Sûreté du Québec. A cela s'ajoute

l'explosion des taxes de ventes collectées grâce au retour des fumeurs vers le marché légal. Pour le corps policier, la démonstration est faite : la guerre à la contrebande est une excellente façon de renflouer les coffres de l'État québécois. Trois mots pour comprendre : Contrebandiers : A elle seule, la SQ a obtenu le dépôt d'accusations contre 2209 contrebandiers de tabac allégués l'an dernier, à la suite d'environ 2000 enquêtes et 2142 perquisitions. " C'est une année record ! " se félicite l'inspecteur Michel Pelletier, directeur de la lutte à la criminalité contre l'État au sein de la SQ. A ces chiffres s'ajoutent tous les suspects arrêtés par la GRC ou les corps de police municipaux comme le SPVM. Certains se concentrent uniquement sur les cigarettes, mais d'autres, comme des caïds reliés aux motards, au crime organisé asiatique, au crime organisé traditionnel québécois, à la mafia italienne, y voient une façon de diversifier leurs activités criminelles et financer d'autres trafics, comme l'importation de drogue. La Presse (Le Quotidien, 20)

Pan Am Games boss David Peterson says preparations 'in wonderful shape'

Preparing for the Pan Am Games has had its "ups and downs." So says Pan Am Games chair and pitch man David Peterson, who has had to contend with firing former CEO Ian Troop, putting out fires associated with senior officials spending money inappropriately, and going cap in hand to the province for $74 million, bringing the operations budget to $760 million. "It has had its ups and downs along the way but we are on track, we are in wonderful shape," he told a Toronto Star editorial board meeting. Peterson said the truth is "no one really wanted the games anyway," but supporters were steadfast in their determination that it was a surmountable "management challenge." "It will be the only game in town for that period of time," he said. The biggest concern is out of the hands of TO2015 and that's security, which along with transportation is the responsibility of the province. Security has been pegged at $239 million - twice the original estimate - and $61 million for transportations costs. The roughly $300 million is not factored into the $2.5 billion for the Games. The Ontario Provincial Police, which is overseeing security, acknowledges that if there is a verifiable threat against the Pan Am Games that cost could easily balloon. The traffic during the Games is also an unknown. Officials say the transportation plan for the summer games is contingent upon a 20-per-cent reduction in regular traffic. The massive month-long event is expected to draw 250,000 visitors to Toronto and area. Toronto Star

Le procès du projet Kayak fixé en août

Si de nouvelles requêtes ne viennent pas en retarder le début, le procès des individus accusés en marge du projet Kayak devrait finalement se mettre en branle le 24 août prochain. Ce procès d'une durée de huit semaines devait se dérouler au début de l'année, mais des requêtes ont fait en sorte d'en retarder le commencement. Le membre en règle des Hells Angels, Vincent Boulanger, Guy Boucher, Éric Letarte, Serge Pinard, Rock Proulx, Stéphane Rouleau et Dany Ward sont accusés de divers chefs d'accusation en lien avec le trafic de stupéfiants. La défense conteste le dépôt d'un nouvel acte d'accusation présenté hier par la poursuite. A compter du 27 mai prochain, trois semaines de requêtes préliminaires ont été retenues par la juge Julie Beauchesne de la Cour du Québec. Cinq accusés sont détenus pour la durée des procédures dans cette affaire. L'opération Kayak s'est déroulée le 12 juin 2013 à plusieurs lieux de perquisition en Estrie, dont Sherbrooke, Saint-Denis-de-Brompton, Windsor, Dudswell, Stukely Sud, Sainte-Christine et Canton de Cleveland. Plus de 235 policiers de la Sûreté du Québec, du Service de police de Sherbrooke, de la Régie de police Memphrémagog, de la Gendarmerie royale du Canada ainsi que des corps de police de Granby et Bromont avaient participé à cette frappe policière. La Tribune, 20

La présumée pirate plaide la " connerie qui a mal viré "

La présumée pirate informatique accusée mercredi s'excuse d'en avoir effrayé plus d'un en prenant le contrôle à distance de leur ordinateur, ce qu'elle considérait comme une simple blague. "Ce n'était pas dans mon intention de terroriser ou faire du mal à quelqu'un, a assuré, hier, au Journal Valérie Gignac lors d'une entrevue réalisée sur la terrasse de sa maison de Saint-Alphonse- Rodriguez. Je suis désolée, je ne savais même pas que c'était illégal [...] C'était juste une connerie qui a mal viré." La jeune femme de 27 ans a été arrêtée et accusée mercredi puisqu'elle aurait pris possession d'ordinateurs appartenant à des familles. Certains auraient été derrière leur écran lorsqu'elle les espionnait. Bien que la jeune femme était très calme lorsque Le Journal l'a rencontrée, elle a avoué avoir été ébranlée la veille lorsque la Gendarmerie royale du Canada (GRC) "est débarquée" chez elle vers 6 h du matin. Journal de Montreal

Judge acquits RCMP officer in airport taser case

Another RCMP officer who was involved in Robert Dziekanski's death at Vancouver airport has been acquitted of perjury for his testimony at a public inquiry - the last of four verdicts that saw another Mountie acquitted while two others were found guilty. Constable Gerry Rundel was acquitted Thursday in B.C. Supreme Court. The Crown had alleged the four officers who responded to the call involving Mr. Dziekanski colluded on a story to tell homicide investigators and later lied at the public inquiry. Constable Rundel, in a written statement, thanked the judge for "seeing the truth." "In Oct of 2007 four officers answered a 911 call at the airport. We responded as we were trained to. Sadly Robert Dziekanski lost his life," the statement read. Glen Orris, Constable Rundel's lawyer, said the judge found the Crown's theory lacking. "[The judge] basically said, 'on the evidence as I interpret it, the Crown's failed to prove their case,' " he said in an interview. Mr. Orris said the judge also found Constable Rundel's statements at the inquiry to have been credible. Constable Bill Bentley was the first of the officers to stand trial for perjury. All of the cases were heard by a different judge. Constable Bentley was acquitted in July, 2013, with the judge in his case ruling the Crown had "not shown that in any particular [instance] Mr. Bentley made a false statement knowing it to be false and with intent to mislead the inquiry." Globe and Mail, S3; Canadian Press (Toronto Star)

Woman's 911 call was handled properly

The RCMP is defending the way it handled a 911 call from a Nanaimo university student who was reporting that a man had tried to steal her purse and groped her. Cady Brockman, 20, said she was approached by a man wearing a balaclava just before 4 p.m. last Friday on Foster Street and Bruce Avenue in Nanaimo. The man tried to grab her purse, then pulled down her pants and groped her. She pushed the man down and he ran away. Brockman felt violated by the assault and was frustrated that when she called 911 to report the attack, she was told to call Nanaimo RCMP's nonemergency line. "I was frustrated because my emergency wasn't enough," she told the Times Colonist this week. Sally Boxall, operational communication centre manager for Island district RCMP, said she reviewed the 911 recording of the call and is satisfied with how the operator handled it. "In speaking with the caller, the operator confirmed that the incident was no longer occurring and the suspect was no longer present. Speaking in a calm manner, the caller indicated that she did not fear for her immediate safety," Boxall said. Times Colonist, A5

*** Mayor John Tory supports swapping some cops for civilians**

Mayor John Tory (open John Tory's policard) says it's time to explore using lesser-paid civilians to do some duties currently performed by uniformed Toronto police officers. "We've simply got to discuss how we are using these highly trained, expensive police officers and making sure they're being put to the best use ... for real policing matters," Tory said Thursday. For example, trained, non-police personnel could direct traffic as a more cost-effective alternative, the mayor said. "I was in Chicago a year and a half ago and saw their people who had jackets on that said 'traffic supervisor' or some such thing," Tory said. "They were people who the public recognized as having the authority to direct traffic." Across Ontario, cash-strapped municipalities are grappling with escalating policing costs, largely due to labour agreements. Tory and fellow Toronto Police Services Board members recently signed a four-year contract with the police union that gave officers an almost 9 per cent pay increase. This week, the Association of Ontario Municipalities released its "Policing Modernization Report," with recommendations to "ensure that all Ontario communities can afford policing." A key proposal calls on the province "to make legislative changes to permit the greater transfer of specific functions to civilians or other security providers where appropriate." Toronto Star

*** Politics This Morning: RCMP restricting MPs on Hill**

NDP MP Nathan Cullen raised a question of privilege yesterday after the RCMP did not allow the green House of Commons shuttle bus he was on onto the Hill at the East Block entrance, causing him to miss a vote. "They seem to be shutting down the Hill, or access to the Hill, more and more often," Mr. Cullen (Skeena-Bulkley Valley, B.C.) told *The Hill Times*. He noted that he believed the Senate deputy Speaker's motorcade was leaving the Hill precinct "and they shut the whole thing down." Mr. Cullen said that was an inappropriate reason not to allow the House bus on the Hill. "If that's the trigger for when we close off the hill, we're going to have some problems because it's just going to be too often," he said. He raised the issue in the House yesterday saying that he was "denied reasonable, timely access to the Parliamentary Precinct." He said that bells started ringing for a vote in the House when he was in the Finance

Committee meeting in 151 Sparks St. He went outside and took a shuttle back to Centre Block for the vote. The Hill Times

*** Reports of biker clubhouse spark concerns in Langford**
Parents with children at Spencer Middle School are concerned that a biker clubhouse with alleged links to the Hells Angels may be opening just steps from the school. West Shore RCMP has received reports that a Devils Army clubhouse is being constructed in the Langford neighbourhood and said the biker club is not welcome. "I'm scared, to be honest. I really think it could bring more gang violence to the West Shore," said one mother who asked not to be named. Neighbours say renovations began at 2775 Spencer Rd. about a month ago. A tall black fence blocks entry to the building and the number 41 is displayed in large text. The 41 is believed to represent D and A, the fourth and first letters of the alphabet. Hells Angels clubhouses typically display the number 81, for HA. Devils Army has been called a puppet club of the Hells Angels. The Hells Angels have denied an affiliation. A Devils Army presence has previously been reported in Campbell River. Although there's not evidence of criminal activity at the location, the RCMP said it will monitor the situation. "Maintaining public safety remains the top priority of the West Shore RCMP detachment. We will work closely with our neighbouring RCMP, municipal police forces and partner agencies to identify, investigate and disrupt criminal activity and organized crime in our communities," Insp. Larry Chomyn said. Mayor Stew Young said RCMP have informed Langford council there may be "an issue." While the city is concerned about construction happening without a permit, Young said he will leave criminal concerns to the Mounties. Times Colonist, A4

*** Ottawa set to take another step back on gun control**
An opinion piece states, "Last week the federal standing committee on public safety launched its hearings into Bill C-42, the ironically named Common Sense Firearms Licensing Act. The bill, which would loosen controls on possession permits, assault weapons and the transportation of handguns, could hardly be farther from common sense. Astoundingly, the committee is not scheduled to hear a single witness representing police organizations, or for that matter any public safety, crime prevention or legal experts - all people in a unique position to comment on the likely consequences of the proposed legislation. Instead, the hearings consist of only four hours of testimony from nine witnesses: two private groups defending gun control versus seven defending pro-gun interests. Among the many troubling changes C-42 seeks to introduce, one seemingly innocuous measure deserves special scrutiny. The legislation would open the door to regulations that limit the discretionary powers of chief firearms officers (CFO), the provincial public servants who decide on whether or not to issue a variety of licences and authorizations and on what conditions." Toronto Star, A15

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

La réussite de C-10 est un échec
Un article éditorial déclare, « La plupart d'entre nous savent qu'il y a un lien entre une cause et son effet. La criminalité par exemple. S'il suffisait de diviser le monde entre les bons et les méchants, on aurait réglé le problème depuis longtemps, mais la criminalité n'est pas un phénomène aléatoire, indépendant des conditions sociales. Au Canada, environ 12 % de la population n'a pas obtenu son diplôme d'études secondaires. C'est autre chose en prison. En 2014, le Bureau de l'enquêteur correctionnel constatait que 40 % des délinquants admis pendant l'année n'avaient pas étudié au-delà d'une huitième année. Pensez-y. Presque la moitié de ceux et celles qui aboutissent à un établissement fédéral de détention ont à peine terminé leur primaire. Le statut d'emploi, l'âge et le niveau de scolarité «sont les plus importants indicateurs de la récidive», disait aussi l'enquêteur, alors que les programmes visant à améliorer le niveau de scolarité et les compétences professionnelles facilitent la réinsertion. La récidive, comme la criminalité elle-même, n'est pas aléatoire. On peut la prévenir si on prend les bons moyens : éducation et réinsertion progressive. Cette semaine, le vérificateur général du Canada a lui aussi mis le doigt dans cette plaie que le gouvernement Harper croit pouvoir soigner avec du sel. Quand avez-vous vu ou entendu un ministre ou un député conservateur plaider en faveur de la réhabilitation des prisonniers? Jamais, car avec l'adoption du projet omnibus C-10, intitulé trompeusement «sur la sécurité des rues et des collectivités», la réhabilitation a cessé d'être une priorité. » Le Soleil, 23

Drugs seized at Collins Bay Institution
Staff at Collins Bay Institution seized a package containing 39 grams of marijuana and 92 grams of tobacco, according to a news release Thursday. The release states that the contraband was obtained in the perimeter of the medium-security unit at the prison. Correctional Service Canada estimates the institutional value of the seizure to be $5,900. To prevent drugs from entering its institutions, the correctional service uses tools such as ion scanners and drug-detector dogs to inspect buildings, personal property, inmates and visitors. A toll-free number (1-866-780- 3784) has been set up so the correctional service can receive confidential information relating to drug use or trafficking. Kingston Whig-Standard, A3

Supreme Court to hear man's appeal of mandatory minimum sentencing
The Supreme Court of Canada announced Thursday it will hear the appeal of mandatory minimum sentencing for a Vancouver drug dealer. Joseph Lloyd was convicted of possession for the purpose of trafficking after he was arrested by police two years ago for carrying fewer than 10 grams of heroin, crack cocaine and crystal methamphetamine. The amount of drugs considered possession for the purpose of trafficking is more than six grams. At sentencing, Lloyd told the court he was addicted to all three drugs, according to the Pivot Legal Society which intervened in the case at a B.C. Court of Appeal hearing. Pivot argues that mandatory minimum sentences for possession for the purpose of drug trafficking, which was introduced in 2012 as part of Prime Minister Stephen Harper's tough-on-crime agenda, have a disproportionate effect on women, young offenders, aboriginal people and people who are involved in the drug trade because of their addiction. Some people with drug addiction are trading drugs, rather than selling them, and Pivot argues a lengthy jail term for a low-level crime is an unfair punishment. Vancouver Sun, A4, * Presse canadienne (Acadie nouvelle)

Convicted murder's case being appealed to Supreme Court
The lawyer for a convicted murderer is appealing the case to the Supreme Court of Canada. Derek Hogan filed an appeal last week in the case of Steven Neville. On Feb. 1, 2013, a jury found Neville guilty of second-degree murder in the stabbing death of Doug Flynn and the attempted murder of Ryan Dwyer. It stemmed from an incident that happened Oct. 9, 2010, on Carlisle Drive in Paradise, just outside St. John's. Neville was sentenced to life in prison with no possibility of parole for 12 years. The defence appealed the conviction and, earlier this month, the Newfoundland and Labrador Court of Appeal dismissed it. The Telegram, B4

* **Top court turfs N.S. gun sentencing bid**
The Supreme Court of Canada has dismissed an appeal from the province of Nova Scotia that would have restored some mandatory minimum sentences for gun crimes. Earlier this month, the top court struck down mandatory minimum sentences for gun crimes as unconstitutional because they could constitute cruel and unusual punishment. That seemed to settle the case of Erin Lee MacDonald, a Nova Scotia man charged with several gun crimes in 2009 after he opened the door to police while holding a loaded 9-mm Beretta handgun. MacDonald was charged with possessing a loaded, restricted firearm, careless use of a firearm and possessing a weapon for a dangerous purpose. His case had the potential to shape mandatory minimum laws. He was initially sentenced to the mandatory minimum of three years in prison, but the Nova Scotia Court of Appeal struck that down as cruel and unusual punishment. MacDonald's sentence was ultimately reduced from three years imprisonment to a total of 18 days in jail and two years' probation. Chronicle-Herald, A6

* **Zoe undergoes a psychiatric assessment**
A convicted sex offender, facing new charges of break and enter and sexual assault, will be sent to an Edmonton hospital for a 30-day psychiatric assessment. The assessment for Bobby Zoe, 34, was granted in territorial court by Judge Bernadette Schmaltz on Friday. Zoe himself asked for the assessment, said his lawyer Paul Falvo in court. "The psychiatric assessment can help to determine two things," Falvo said. "One is whether the accused was or wasn't criminally responsible for his alleged offence and the second is whether he is mentally fit to stand trial." Falvo said it is the judge that ultimately makes that decision but the report from the hospital will likely be taken into account. Zoe was charged on Feb. 17 after the occupants of a downtown apartment told police they awoke early in the morning to find someone standing in their bedroom. Police say one of them was sexually assaulted and stolen items were also reported to

police. RCMP later charged Zoe with another break and enter and sexual assault that had been reported Feb 1. However, those charges were stayed last month. Zoe was sentenced to 39 months in prison in April 2012 for sexually assaulting and robbing a woman as she walked down 53 Street on Jan. 11, 2011. Yellowknifer

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Violent crime rising sharply, RCMP report says**

A 40 per cent increase in violent crimes in Surrey from the first quarter of 2014 to the first quarter of 2015 included a 46 per cent increase in sexual assaults, Surrey RCMP reports. According to crime statistics released Thursday, there were a total of 1,732 violent crimes committed in the first quarter of 2015, compared with 1,233 in the same period in 2014. That includes an increase in sexual assaults to 57 from 39 over that period, a 14 per cent increase in robberies to 168 from 148, a 29 per cent increase in assaults to 863 from 668, a 175 per cent increase in abductions/kidnappings to 11 from four (primarily due to domestic/custody disputes), a 25 per cent increase in attempted murder to five from four, and a 100 per cent increase in homicides to two from one. "The increase in attempted murder files is directly related to the spate of targeted shootings that have occurred in the city," said the RCMP in a statement. "It is important to note that not all shootings are categorized as attempted murder as intent needs to be established." There have been as many as 23 shootings in Surrey and Delta over the last several weeks, with a number of them linked to a street-level drug-trade conflict. However, the report also showed that property crimes dropped five per cent over the year, although arsons increased 146 per cent to 32 from 13. It was the first decrease in property crime in Surrey in over two years. Total criminal code offences increased seven per cent over the year, to 13,039 from 12,133. Despite the increase year-overyear, RCMP said there has been a 12 per cent drop in violent crime since the last quarter of 2014, but that robberies and assaults continue to be the biggest contributors to the city's violent crime rate. Business break-and-enters also dropped considerably - 26 per cent, to 321 from 436 - while residential break-ins were unchanged, 532 each year. Postmedia News (Vancouver Sun, A8)

*** Keep cops for 'real policing,' Tory says**

Mayor John Tory says it's time to explore using lesser-paid civilians to do some duties currently performed by uniformed Toronto police officers. "We've simply got to discuss how we are using these highly trained, expensive police officers and making sure they're being put to the best use ... for real policing matters," Tory said Thursday. For example, trained, non-police personnel could direct traffic as a more cost-effective alternative, the mayor said. "I was in Chicago a year and a half ago and saw their people who had jackets on that said 'traffic supervisor' or some such thing," Tory said. "They were people who the public recognized as having the authority to direct traffic." Across Ontario, cash-strapped municipalities are grappling with escalating policing costs. Tory and fellow Toronto Police Services Board members recently signed a four-year contract with the police union that gave officers an almost 9 per cent pay increase. This week, the Association of Ontario Municipalities published its "Policing Modernization Report." A key proposal calls on the province "to make legislative changes to permit the greater transfer of specific functions to civilians or other security providers where appropriate." Toronto Star, GT2

*** Two years later, cyberbullying law continues to ignite debate**

An overwhelming majority of complaints filed under Nova Scotia's anti-cyberbullying law have been resolved out of court, proof that it is working despite lingering criticism, supporters of the legislation say. Two years after it was passed in April 2013, the bill still faces criticism from legal experts who say it threatens freedom of expression. The legislation is the first of its kind in Canada. Two challenges aimed at striking down the controversial law are currently before the courts, and in a separate case an order under the Cyber Safety Act was overturned by the Nova Scotia Supreme Court on grounds it violated charter rights. But a member of Nova Scotia's CyberScan unit, which was established under the act to crack down on cyberbullying, said there is a side of the law the public doesn't hear about as much. Of the 559 complaints of cyberbullying filed with CyberScan, only two have proceeded to court, with the rest

resolved through informal negotiations, said Dana Bowden, one of the five investigators with the unit. Canadian Press (Maclean's, CBC News, Brandon Sun, CTV News, CHEK, Truro Daily News)

* **Cyberintimidation dénoncée: «Vous devriez vous lobotomiser avec un Magnum»**
Propos haineux, insultes, incitation à la violence ou au suicide, la militante Sophie Labelle dénonce la cyberintimidation dont sont victimes beaucoup de personnes trans qui prennent la parole sur le web. La semaine dernière, Rachel Bryk, une jeune programmeuse américaine trans très en vue, s'est suicidée après avoir subi des attaques transphobes sur internet. Certaines l'encourageaient à se suicider. Elle avait aussi des douleurs physiques dues à des maladies chroniques. «Ça me touche très personnellement, étant quotidiennement la cible de cyberintimidateurs qui ne font pas dans la dentelle», a indiqué à Métro Sophie Labelle, enseignante au primaire et auteure d'une bande dessinée en ligne traitant d'enjeux trans qui remporte du succès dans plusieurs pays et en plusieurs langues. Journal Métro

* **Canada gives short shrift to important event**
An opinion piece states, "An important gathering is being held this week at the United Nations in New York, but with the Duffy trial and the tragic earthquake in Nepal the event got little coverage in Canada and fell off the news pages. The UN Permanent Forum on Indigenous Peoples met in New York for the past 11 days, and attracted hundreds of delegates who represent 370 million indigenous people around the world. (...)Instead of a political spokesperson, such as the minister of aboriginal affairs or a parliamentary secretary, Canada was represented by an Indian Agent from the Colonial Office. It is embarrassing how backward this country has become under the current federal government. The speech by Ducros to the forum was a one-sided litany of the government's achievements, including a statement that it had "removed obstacles to concluding treaties" when, in fact, several reports have pointed to Ottawa and the Department of Aboriginal Affairs as the main impediments. She went on to state that the government had taken steps to ensure First Nations have access to clean drinking water and that it recognizes the serious issue of murdered and missing aboriginal women. Ducros didn't once mention the controversial call for an inquiry into missing and murdered aboriginal women. This was an important international forum, yet Canada was represented by someone reading a clicheridden speech that no doubt was vetted by the Prime Minister's Office." StarPhoenix, A13

* **Ending violence against aboriginal women focus of action plan**
The Aboriginal Women's Association of P.E.I. hopes an action plan with the province that came out of a roundtable February in Ottawa will make a difference in reducing higher rates of violence against aboriginal women. At the National Roundtable on Missing and Murdered Indigenous Women and Girls, the province and aboriginal groups committed to work together at the community level. Recently, Island aboriginal women's organizations met to begin discussions. Association president Judy Clark was one of six delegates from P.E.I. that attended the roundtable. She says three priority areas were determined at the conference: prevention and awareness, community safety, and policing and justice measures. CBC News

* **Nelson group raises awareness of violence against women**
Do you know this woman? Chances are you do. She is one of three women in Canada who have experienced abuse. She could be your sister, your daughter, your aunt, your mother, your friend, the clerk who often helps you in the store, or the woman across from you in your office. On average, every six days a woman in Canada is killed by her intimate partner. A sobering statistic. Think domestic violence doesn't happen in Nelson? Think again. According to Anna Maskerine, chair of the Nelson Violence Against Women in Relationships Committee, it most certainly does. The Aimee Beaulieu Transition House is often full to capacity. After 20 years of providing service in the community, the problem of violence against women shows no signs of going away. Nelson Star

* **Sexual Assault is rooted in an inherent imbalance of power**
An opinion piece states, "Sexual assault is any unwanted act of a sexual nature forced by one or more persons upon another individual. This includes unwanted touching (also known as sexual harassment) and rape. Drugs or alcohol may be used to intoxicate the victim. This includes alcohol or drugs that the victim has consumed either voluntarily or involuntarily as well as the use of anesthesia during an operation or proceedure. It's clear that men and boys are victims of sexual abuse, but 86 per cent of

victims of sexual assault who reported to police in 2004 were female. This article will focus on sexual assault as a women's and girl's issue. Statistics often bring trends to light and validate the importance of exploring specific issues like the sexual assault of women and girls. Here's well established statistics from the Ontario Women's Directorate: Over the past decade the breakdown of sexual assaults remained unchanged with 81 per cent of incidents involving unwanted sexual touching and 19 per cent involving sexual attacks." Rabble.ca

*** Should sex offenders be banned from transit?**
While judges impose limits to riding the bus by sexual assault suspects as part of release conditions, Transit Police say they don't have the resources to enforce it. Instead, when it comes to prolific offenders, some consideration should be given to either banning them from the transit system itself or imposing a condition limiting their use of transit by having them accompanied, according to Anne Drennan, Transit Police spokeswoman. "But to ban them completely from public transportation, some of the judges feel this is inappropriate," she said. This week, Vancouver man Mukesh Yasarapu was charged with two counts of sexual assault but was released with conditions, including when he's on transit he cannot sit or stand next to a female. "To say you can't stand or sit beside a female when using public transit ... is virtually impossible," she said. "You can liken it to ... handing an alcoholic a drink and saying, 'OK, you can hold this but you can't sip it.'" Drennan said while Transit Police do have a special unit dedicated to these issues, they don't have the resources to deal with it sufficiently across the system. 24 Hrs Vancouver

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Unions fight new federal screening rules on public servants**
As more than a quarter million federal government employees face credit checks and fingerprinting, one of the unions representing them is going to court to stop it. The Professional Institute of the Public Service of Canada is citing a case involving New Brunswick's J.D. Irving Ltd. The individual background checks are among new security screening standards the Treasury Board says are required to ensure the reliability and trustworthiness of civil servants handling sensitive and personal information.The new background checks apply to existing employees as well as to new hires.The Professional Institute of the Public Service of Canada has applied for an injunction to the federal court to halt the added security screening until a full legal challenge can be dealt with."We simply have no evidence from the government that such a broad, blanket application is reasonable in any way," said Isabelle Roy, the general counsel for the union, which represents 55,000 civil servants."We're simply not convinced of the rationale and reasonability for such privacy invasive measures being implemented across the board." Roy says the application for an injunction cites the 2013 Supreme Court of Canada case CEP Local 30 v Irving Pulp and Paper. In that case the top court ruled that privacy rights trump the rights of the company to initiate random alcohol testing on all employees. 'Unwarranted violation of personal privacy' Another union, the Public Service Alliance of Canada, says it also is challenging the credit check requirement. CBC.ca

OTHER / AUTRE

NIL

INTERNATIONAL / INTERNATIONAL

*** Nepal earthquake death toll hits 6,260 as government plans to compensate families**
Slowly, life edged back toward a semblance of normal in Nepal's quake-hit capital Kathmandu on Friday as residents packed up tents and moved indoors. As rescue workers continued to comb the rubble in the city for survivors, the government said it was handing out the equivalent of $1,000 US to families for each victim killed in Saturday's earthquake, and another $400 for funeral costs, according to state-run Nepal Radio. The death toll from the mammoth quake climbed to 6,260 including those who died in an

avalanche on Mount Everest, plus more than 60 elsewhere in the region. The city got a lift Thursday when two survivors, including a 15-year-old boy, were rescued after being buried in debris for five days. Associated Press (CBC News)

*** Népal - Ottawa se défend de ne pas en faire assez pour les Canadiens**

Le gouvernement canadien martèle qu'il fait tout son possible pour aider les Canadiens pris au Népal à quitter le pays ravagé par un puissant séisme. Y compris les citoyens qui sont coincés dans des régions éloignées, ont indiqué quatre ministres dépêchés au Parlement jeudi pour faire le point sur la situation. Le ministère des Affaires étrangères planche sur un plan d'opération pour localiser les Canadiens bloqués dans des régions montagneuses et qui, de ce fait, n'ont pu rejoindre la capitale népalaise Katmandou. " Nous tentons d'établir des moyens de transport traditionnels pour accéder à ces individus ", a indiqué la ministre d'État responsable des affaires consulaires, Lynn Yelich, en point de presse. Le Devoir rapportait lundi que deux jeunes Québécoises se sont trouvées coincées dans la région montagneuse de Langtang, au nord de Katmandou. Elles ont trouvé refuge en lieu sûr depuis, mais par leurs propres moyens. A ceux qui ont reproché au gouvernement d'avoir mis trop de temps à aider les Canadiens au Népal, le ministre de la Défense a rétorqué que le fédéral avait agi très rapidement. Le Canada n'a jamais eu de Haut-Commissariat dans ce pays, a noté Jason Kenney. "La raison pour laquelle les gens vont au Népal, c'est parce que c'est un petit pays très, très éloigné de la civilisation ", a-t-il fait valoir. C'est aussi pour cette raison que le Canada n'y a pas de grande mission diplomatique et qu'un seul consul honoraire, qui est aussi médecin -- le Dr Buddha Basnyat --, a d'abord fourni de l'aide médicale sur place, a expliqué le ministre. Environ 500 Canadiens se trouvaient au Népal au moment du tremblement de terre de magnitude 7,8 samedi dernier, selon les informations du ministère des Affaires étrangères. Plus d'une centaine ont quitté le pays à bord de vols commerciaux, qui ont repris à Katmandou. Et 96 personnes ont été rapatriées à New Delhi, en Inde, à bord du C-17 canadien qui a livré de l'équipement de secours au Népal. Un second C-17 devrait arriver à Katmandou vendredi matin avec à son bord 51 membres des Forces armées, notamment du personnel médical, et l'appareil pourra rapatrier davantage de Canadiens en Inde. Le Devoir, A5

*** Family worries for St. Albert couple still missing in Nepal**

Family and loved ones of a St. Albert couple unaccounted for in Nepal are holding out hope they will still be found alive. It is believed that Kathy and Bruce Macmillan were nearing the end of a weeklong hike along a trail in Langtang National Park when a 7.8-magnitude earthquake occurred around noon April 25. The Langtang Valley, directly north of Kathmandu, was among the hardesthit areas, with buildings crushed by avalanches and roads blocked. All means of communication in the region have been cut off. Edmonton Journal, A10

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
May 14, 2015 / le 14 mai 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

CSIS admits losing ground to hackers
Canada's spies admit they can't keep up with daily cyber attacks from state-sponsored hackers, according to an internal report obtained by the Star. A heavily censored "threat overview" prepared by CSIS last September stated hostile "state-sponsored" hackers are targeting everything from political positions and trade strategies to commercial data and personal information. "Hostile state-sponsored actors (are targeting) Canadian public and private computer networks daily to advance their economic, military, (and) political agendas," reads the report, prepared for **Public Safety Minister Steven Blaney**'s office. "Offensive cyber operations (are) employed with more traditional methods in support of strategic and economic objectives." A separate overview of CSIS operations, also prepared for Blaney and obtained under Access to Information law, stated CSIS is being overwhelmed by the sheer number of attacks. CSIS reported the "scale of the threat has fast outpaced (its) capacity," and the agency has been required to "prioritize" its efforts. That document rates cyber security as an "operational pressure," along with terrorist travel. Ottawa recently named China as the state sponsor behind a 2014 hack of the National Research Council's network - an attack that CSIS and Canada's electronic spy agency, the Communications Security Establishment, monitored for some time before quarantining the agency's network from government servers. But while that high-profile attack made headlines, the September 2014 threat overview shows Canada's public and private networks are targeted more often than most people realize. CSIS also identified more traditional methods of espionage in the threat assessment, including "political espionage targeting government officials and systems." Toronto Star, A1

Les services d'espionnage canadiens sont débordés

Les services d'espionnage canadiens n'arrivent plus à contenir la menace que représentent les cyberattaques au pays. Les réseaux informatiques des divers gouvernements ou du secteur privé sont quotidiennement la cible d'attaques, affirment les dirigeants du SCRS dans un document d'information qu'ils ont remis au **ministre de la Sécurité publique, Steven Blaney**, en septembre dernier. Ces cyberattaques sont souvent l'oeuvre de gouvernements étrangers hostiles qui misent sur ces agressions virtuelles pour faire mousser leurs intérêts économiques, militaires ou politiques, peut-on lire dans ce document obtenu par le quotidien Toronto Star en vertu de la Loi sur l'accès à l'information. Le **ministre Blaney** a été mis au courant de l'ampleur de cette menace par les hauts dirigeants du Service canadien du renseignement de sécurité le 18 septembre dernier. «Des acteurs qui sont parrainés par des États hostiles ciblent les réseaux d'ordinateurs publics et privés au quotidien dans le but de faire avancer leurs intérêts économiques, militaires ou politiques», soutient-on dans le document, dont plusieurs passages ont été caviardés. Les cyberpirates tentent ainsi de mettre la main sur des secrets militaires, des informations confidentielles liées à la propriété intellectuelle, des stratégies commerciales, ou encore des informations personnelles. [...] Ce n'est pas la première fois que le SCRS sonne l'alarme quant aux risques de plus en plus élevés liés aux cyberattaques. Au bureau du **ministre Blaney**, on affirme que la cybersécurité est une question prioritaire et que le gouvernement travaille étroitement avec les experts en la matière pour se protéger des intentions malicieuses des cyberpirates avant qu'ils ne frappent. Le porte-parole du ministre, Étienne Rainville, a souligné que le gouvernement a annoncé de nouveaux investissements totalisant près de 300 millions de dollars pour les forces de l'ordre et les agences de sécurité afin de combattre le terrorisme et le cyberespionnage. «***Nous avons fait d'importants investissements dans une stratégie de cybersécurité conçue pour se défendre contre les menaces électroniques, le piratage et le cyberespionnage. Le budget 2015 a réaffirmé l'engagement de notre gouvernement envers la cybersécurité en s'assurant que nos agences disposent des outils dont elles ont besoin pour faire leur travail grâce à un investissement supplémentaire***», a-t-il dit. La Presse, A15

Omnibus bill to clear RCMP of criminal charges

The Harper government moved to retroactively rewrite Canada's access to information law in order to prevent possible criminal charges against the RCMP, The Canadian Press has learned. An unheralded change buried in last week's 167-page omnibus budget bill exempted all records from the defunct long-gun registry, and also any "request, complaint, investigation, application, judicial review, appeal or other proceeding under the Access to Information Act or the Privacy Act," related to those old records. The unprecedented, retroactive changes - access to information experts liken them to erasing the national memory - are even more odd because they are backdated to the day the Conservatives introduced legislation to kill the gun registry, not to when the bill received royal assent. The date effectively alters history to make an old government bill come into force months before it was actually passed by Parliament. A source familiar with the complaint, speaking on condition of anonymity due to its sensitivity, said the government moved out of concern Information Commissioner Suzanne Legault is poised to recommend charges against the Mounties for withholding - and later destroying - gun registry documents while the legislation was still being debated. Indeed, shortly after the story broke Wednesday, Legault's office announced it would be tabling a special report Thursday detailing an investigation into the long gun registry and an access to information request. The government feels no one should face a penalty for being overly eager to enforce the will of Parliament before the legislation had been voted into law. A spokesman for **Public Safety Minister Steven Blaney** would only say the retroactive law will fix a "***bureaucratic loophole***" that allowed citizens to request heavily redacted copies of the gun registry data while the legislation to destroy the data was before Parliament. "***This clearly goes against the will of Parliament that all copies of the registry should be destroyed***," spokesman Jeremy Laurin said in an email response. "***This technical amendment re-enforces this point***." Legault's office refused to discuss any investigations, citing confidentiality provisions, or even to comment on the government's rewrite of the access-to-information law. Canadian Press, B6 (Toronto Star, National Post, Calgary Herald, Leader-Post, The Telegram, Charlottetown Guardian, Cape Breton Post, Windsor Star, Times Colonist, Red Der Advocate, Whitehorse Daily Star)

NDP decries timing of video's release

Internal RCMP documents about the release of gunman Michael Zehaf-Bibeau's video are part of a "hyperpolitical" pattern of government behaviour on its anti-terrorism legislation, the NDP says. The

documents, first disclosed by the Citizen, include an RCMP communication strategy for the public release of the video. In them, the RCMP noted that releasing Zehaf-Bibeau's video on a Friday would ensure "attention on the video will be very high over the weekend, but that the issue will die down early the following week so that the focus can be on the Bill C-51 hearings." Bill C-51 is the government's anti-terror bill, and House of Commons hearings on it started the Monday after the RCMP released the much-anticipated video recorded by Zehaf-Bibeau on his cellphone. The gunman killed a guard at the National War Memorial last Oct. 22 before being killed himself inside the Centre Block. NDP national security critic Randall Garrison said the documents have renewed concerns from opposition MPs that the government was using the video to help make the case for its anti-terrorism bill, even though the RCMP called the release and hearings "unrelated issues." "They're clearly related because the government was saying they were related," Garrison told the Citizen Wednesday. "It's part of a pattern around C-51 where everything becomes hyper-political rather than a policy question." Cabinet ministers, when asked about the timing of the video's release, said no one in the government had directed the RCMP to release the video just ahead of the C-51 hearings. "Certainly not. Never. Absolutely not," Justice Minister Peter MacKay told reporters. "We certainly don't direct the RCMP." In the House of Commons, **Public Safety Minister Steven Blaney** said he has "***full confidence in the judgment of the RCMP***" and respected the "***operational independence***" of the force. Ottawa Citizen, A10

B.C. a 'no man's land' when it comes to pot shops

As Vancouver attempts to control a proliferation of marijuana dispensaries by regulating them, other B.C. cities have taken stringent measures to stop the storefronts from popping up in the first place. Both North Vancouver District and Surrey, for instance, have passed zoning bylaws to prohibit the marijuana dispensaries, while other municipalities say their police forces, particularly the RCMP, have zero tolerance for the illegal facilities and will shut them down. [...] The federal government has handled it so incompetently, it's left the province with no direction to take," Corrigan said. The federal government has put the onus on municipalities to enforce the law around medical pot but has done nothing to crack down as a court case filed by medical pot users continues. The case was launched by medical pot users who were told they could no longer grow pot in their homes, but would have to buy it from central facilities and receive it by mail. Vancouver officials argue the situation has resulted in 80 unlicensed pot shops across the city and is proposing to regulate the storefronts by issuing $30,000 licensing fees and closing shops near schools and community centres, while allowing them in most commercial districts. But Health Minister Rona Ambrose and **Public Safety Minister Steven Blaney** recently warned Vancouver council members and Vancouver police they should crack down rather than regulate, and thereby legitimize, pot dispensaries. Vancouver Sun, A1

Crime de non-achat

Le crime de non-achat n'est pas sur le point d'apparaître au Canada. Malgré la microtempête médiatique suscitée par une interprétation des slogans conservateurs, boycotter Israël ne mènera pas du tout à la prison. A la suite des attentats de Paris en janvier dernier, le **ministre de la Sécurité publique, Steven Blaney**, manifestait au nom de la liberté d'expression. Deux semaines plus tard, un forum spécial sur l'antisémitisme était organisé à l'ONU. **M. Blaney** y affirmait que le Canada avait une politique de «***tolérance zéro***» à cet égard. Le boycottage de produits israéliens serait le nouveau visage de l'antisémitisme, soutenait le ministre. Un reporter de la CBC a demandé ce que signifiait concrètement «tolérance zéro». Une attachée de presse du Ministère lui a récemment répondu en expliquant comment le Code criminel canadien permet de punir sévèrement le discours haineux. Elle n'a pas précisé si cela référait à l'antisémitisme en général ou au boycottage ni ce que le gouvernement entendait faire avec cet arsenal juridique. Malgré tout, certains ont conclu qu'Ottawa pourrait favoriser les poursuites contre les boycotteurs. L'hypothèse a même été relayée par le Haaretz, réputé quotidien israélien, et par Glenn Greenwald, journaliste d'enquête derrière l'affaire Snowden, le scoop de la décennie. Mais cette menace ne sera pas mise à exécution. Même si le Code criminel est fédéral, c'est aux procureurs généraux des provinces que revient la décision d'intenter une poursuite. Or, aucune province n'a manifesté son intention d'aller en ce sens. La raison est simple: il n'existe pas le moindre argument juridique pour le faire. Un discours ne devient pas haineux parce qu'il est déplaisant. Même l'incitation à la diffamation ou au dénigrement ne serait pas forcément haineuse. Cette étiquette criminelle est réservée aux rares cas qui mènent à une forme «extrême» de détestation, rappelait la Cour suprême en 2013. La Presse, A24

What the media missed while it was dumping on Liz May
Dear God, please let this be the last word on Elizabeth May we hear this week: It was a bad speech. It wasn't a funny speech. And while Ottawa's magpie mainstream media outlets were obsessing over a politician's public humiliation like it was Watergate and Robocalls rolled together, actual news was happening. For instance: During the same broadcast of CBC's Power and Politics that devoted two whole segments to the Green Party leader's awkward attempts at humour, Paul Calandra - the prime minister's legendarily lachrymose parliamentary secretary - tried vainly to defend his refusal to answer a question in Parliament about how the government appoints senators ... because the issue is before the courts. [...] My point is this: Politicians say and do stupid things all the time, in professional settings, and the media frequently does little to hold them to account. Here's another example: When asked about Omar Khadr's release on bail - something against which the Harper government has fought tooth and nail, despite serious problems with his detention and prosecution, and despite the lack of any evidence he poses a risk to the public - **Public Safety Minister Steve Blaney** had this to say: "***We are disappointed by the decisions of the court, because we feel that victims should be considered in those decisions***." This statement went unchallenged by journalists. No one asked **Blaney** why, if the government feels it's so important that victims be considered in bail decisions, it did not make an amendment to that effect of the Victims Bill of Rights. The Criminal Code currently requires judges to consider the safety of a victim in bail decisions - but surely even **Blaney** can't argue Khadr poses a risk to the family of the late Christopher Speer. **Blaney**'s parliamentary secretary, **Roxanne Smith**, took up her boss's cudgel in the House. "***While Justin Trudeau refused to rule out special compensation for this convicted terrorist***," she sniped, "***and the NDP actively tries to force Canadian taxpayers to compensate him, we believe the victims of crime, not the perpetrators, are the ones who deserve compensation***." Ipolitics.ca

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Wildfire hazard in the red in Rocky forest area**
When Barry Shellian first saw the wildfire in the distance just west of Nordegg on Tuesday, he realized by the colour of the smoke just how dry it is in the West Country right now. The wildfire ranger, who was the first responder, saw black smoke instead of the often white smoke from forest fires. The seven-acre wildfire, about three km west of Nordegg in a stand of spruce trees, was brought under control. It was the 38th of 39 wildfires in the Rocky Wildfire Management Area so far in the wildfire season that began March 1. It was caused by humans. Red Deer Advocate, A1

*** Conditions ideal as wildfires grow across province**
About 40 firefighters are battling a wildfire burning out of control near Lodgepole in west-central Alberta. Richard Horne, a wildfire information officer with the province, said the fire covers about 700 hectares. On Tuesday, when it was discovered, it had destroyed about two hectares. Air tankers, helicopters and heavy machinery are being used in an attempt to bring the fire under control. Edmonton Journal, A8

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Attentat d'Ottawa et Loi antiterroriste - La GRC a orchestré la diffusion de la vidéo
Ce n'est pas un hasard si la vidéo de Michael Zehaf-Bibeau a été rendue publique à la veille de l'étude du projet de loi antiterroriste des conservateurs. La Gendarmerie royale du Canada a beau être une entité indépendante du gouvernement, elle a soigneusement orchestré la diffusion de cet enregistrement afin de s'assurer, de son propre aveu, qu'elle n'éclipse pas les débats sur C-51. Lorsque la GRC a décidé d'accepter l'invitation d'un comité parlementaire et d'y présenter la vidéo de l'auteur de l'attentat d'octobre dernier au parlement, l'opposition a rapidement soupçonné qu'elle le faisait de manière à promouvoir la rhétorique antiterroriste du gouvernement de Stephen Harper, qui venait de déposer son projet de loi C-51. Le commissaire Bob Paulson a même pris acte de cette impression. " Je sais pertinemment que le gouvernement présente de nouvelles dispositions législatives pour renforcer la lutte contre le terrorisme ", avait-il consenti au Comité de la sécurité publique, en mars dernier. " La diffusion d'une telle vidéo pourrait apparaître comme une tentative d'influencer cette démarche. Je tiens à vous assurer que ce n'est

pas mon intention '', avait souligné M. Paulson aux députés. L'Ottawa Citizen a mis la main sur un document de la GRC préparé en vue de la comparution de M. Paulson. Sa déclaration, récitée au début de la rencontre du comité de la sécurité publique, y est reproduite. De même qu'une '' stratégie de communication ''. La note -- obtenue par le quotidien d'Ottawa en vertu de la Loi sur l'accès à l'information et consultée par Le Devoir -- explique que le commissaire se présentera au comité pour présenter la fameuse vidéo enregistrée le 22 octobre, quelques minutes avant que Zehaf-Bibeau tue le caporal Nathan Cirillo et entre armé au parlement. '' L'approche proposée ci-dessous garantira que l'attention portée à la vidéo soit très élevée au cours de la fin de semaine, mais que l'enjeu se calme en début de semaine pour que l'accent soit sur les audiences du projet de loi C-51 '', stipule le document. Invité à comparaître dès la mi-février, M. Paulson a répondu le 3 mars pour témoigner le 6, soit le vendredi d'une semaine de relâche parlementaire -- alors que le comité ne devait pas se réunir. Le même comité parlementaire a étudié le projet C-51 le mardi suivant. La GRC avait en outre prévu des '' questions-réponses '' pour son patron, vraisemblablement pour le préparer aux interrogations des députés et des médias. La première : pourquoi avez-vous mis tant de temps à rendre publique la vidéo ? Réponse rédigée pour M. Paulson : '' A ce moment-ci de l'enquête, il est désormais possible de rendre publique la majorité de la vidéo pour vous aujourd'hui. J'ai profité de l'invitation de ce comité pour présenter la vidéo au moment où cela était possible et dans l'intérêt supérieur du public. '' Le Devoir, A1

Un cégépien se dit «soldat du califat»

Silencieux depuis leur disparition en janvier, deux élèves du collège de Maisonneuve soupçonnés d'avoir quitté le pays pour aller rejoindre des djihadistes outre-mer viennent de réapparaître soudainement sur les réseaux sociaux, où l'un d'eux semble maintenant s'identifier comme un «soldat du califat». Le compte Twitter d'Imad Rafai montre maintenant qu'il se définit par l'expression Jund Al-khilafah, ou «soldat du califat» en arabe. Il ne donne pas d'explication à ce sujet. Le groupe État islamique, qui se bat en Syrie et en Irak, dit avoir établi un califat, un territoire gouverné par un calife qui se veut le successeur du prophète Mahomet. Mais le nom «soldats du califat» réfère aussi à un groupe terroriste algérien, anciennement affilié à Al-Qaïda, qui a prêté serment d'allégeance l'an dernier au groupe État islamique. Imad Rafai est lui-même d'origine algérienne. En plus de son compte Twitter, le jeune homme a mis à jour son profil Facebook pour la première fois depuis le 11 janvier. Il y évoque en termes vagues son départ du Canada. «Celui qui s'enfuit de la terre de mécréance vers la terre d'Islam pour préserver sa religion en espérant la récompense d'Allah et en voulant donner la victoire à l'Islam va trouver sur terre une subsistance abondante et des bienfaits énormes. Allah, vraiment, ne manque jamais à sa promesse», dit-il, sans plus de précisions. Une des personnes qui ont «aimé» cette publication sur Facebook est Ouardia Kadem, une autre élève du collège de Maisonneuve dont la disparition avait été signalée à la mi-janvier avec une demi-douzaine d'amis de Montréal et de Laval. Depuis, elle n'avait pas donné signe de vie, elle non plus. L'Équipe intégrée de la sécurité nationale, un groupe de policiers chargés de la lutte contre le terrorisme et coordonné par la Gendarmerie royale du Canada, n'a jamais fait le point publiquement sur le sort des jeunes soupçonnés d'avoir voulu rejoindre des combattants considérés comme terroristes par le Canada. La Presse, A3 Front; * Toronto Star

*** Youth or adult?**

The case of former Guantanamo Bay prisoner Omar Khadr returns to Canada's top court for a third time on Thursday, as the federal government fights to have him declared an adult offender for crimes he committed as a 15-year-old. The dispute centres on whether the eight-year sentence a U.S. military commission handed him for war crimes should be interpreted as a youth or adult sentence. However, the arcane technical legal battle has taken on loud political overtones. "This case is another illustration of the heavy-handed approach Canada has consistently taken towards him," said Gillian Hnatiw, who represents the Canadian Civil Liberties Association, which is intervening in the case. Khadr, 28, was released on bail last week after almost 13 years in custody while he appeals his U.S. conviction, which has drawn fierce criticism from legal and human rights experts. Although he was 15 when his crimes occurred in Afghanistan in July 2002, the military commission made no distinction between juveniles and adults in sentencing him in 2010 to a further eight years behind bars. The federal government, which has consistently branded him a hardened terrorist and is separately fighting his bail, argues Khadr was really given five concurrent eight-year terms for each of the five war crimes to which he pleaded guilty. While the government concedes the sentence for the most serious charge - the murder of an American special forces soldier - can only be considered a youth sentence, it argues the other four - including attempted

murder - must be viewed as adult sentences. Telegraph-Journal, A7 (Times&Transcript, Hamilton Spectator, Edmonton Journal)

*** Man convicted in terror plot to undergo psych assessment**
An Ontario judge has ordered a mental health assessment for a convicted terrorist who plotted to derail a passenger train, saying the evaluation could help him determine the man's sentence. Justice Michael Code ordered the assessment Monday after Chiheb Esseghaier told the court he had been created by God to "warn mankind" about "hellfire" if the messages of the Qur'an weren't followed. Esseghaier and his co-accused , Raed Jaser, were found guilty in March of a terror-related conspiracy to commit murder, which carries a sentence of up to life in prison. The jury also found the men guilty of six other terror-related charges between them. Jaser is already undergoing a mental health assessment, but his lawyers will decide how much of that report to present to the court when arguments for his sentence are made. Esseghaier is self-represented, but a court-appointed lawyer who is assisting him through the legal process argued that a similar assessment ought to be ordered for the Tunisian national because his mental health was "a real issue." "This is all about fairness," said Russell Silverstein. "A psychiatrist appointed by the court would... be able to tell you whether these are all the behavioural manifestations of a religious zealot or whether there is an aspect to Mr. Esseghaier that falls under the Mental Health Act." The request was opposed by Crown prosecutors, who argued that the 32-year-old Esseghaier's extreme religious beliefs didn't warrant a mental health assessment, which would prolong the sentencing phase of the case. "Court should be really loathe to order an intrusive psychiatric assessment," Crown prosecutor Croft Michaelson said. "Your decision should primarily be based on what you yourself have observed." Esseghaier - who refused to participate in his trial because he wanted to be judged under the rules of the Qur'an - said he wouldn't mind talking to doctors because he's always eager to share his religious values. Times&Transcript, B6 (Hamilton Spectator, Waterloo Region Record); National Post; Charlottetown Guardian (Cape Breton Post)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Everyone's got an opinion on name for new bridge
How does the Good Luck Bridge sound? Or the Gordie Howe Bridge? How about the Windsor Bridge? Those are some of the suggestions made by residents who were asked by The Star to come up with some names for the new international crossing connecting Windsor and Detroit. Prime Minister Stephen Harper is expected to announce the name Thursday. The Windsor Star, A1

Suspected opium found at Hamilton airport
Border officers working at the John C. Munro Hamilton International Airport uncovered two kilograms of suspected opium hidden in a shipment labelled as shoes. In a release Wednesday, the Canada Border Services Agency called the seizure "significant." The suspected drugs were uncovered April 13 as officers inspecting a courier shipment noticed one of the cardboard boxes was "unusually heavy" and had an "earthy smell," the CBSA said. The suspected opium was found hidden in the pleats of the box. The drugs were turned over to York Regional Police, who have arrested one suspect in connection with the case. Details of that arrest, including whether the suspect is facing charges, were not immediately clear. In a statement, CBSA regional director Goran Vragovic praised the expertise of his officers. "Although our officers at all ports of entry are equipped with the latest technology to help prevent illegal narcotics from getting past us, it's their attention to detail that produces results." The Hamilton Spectator, A2

Immigration fraud preliminary set for July
A preliminary inquiry for a Dartmouth businessman facing 56 charges of immigration fraud will get underway this summer. Hector Mantolino, 52, owner and operator of Mantolino Property Services Ltd., is accused of taking advantage of 28 temporary foreign workers. The hearing against Mantolino is expected to take four days beginning July 3 in Dartmouth provincial court. Canada Border Services Agency alleges that Mantolino paid some cleaners from the Philippines as little as $3.13 an hour and told them to lie about their wages if they wanted to stay in the country. Mantolino is accused of violating the Immigration and Refugee Protection Act from July 2009 to April 2013. The Chronicle-Herald, A7

Civil forfeiture office pays cost of destroying ecstasy
B.C.'s Civil Forfeiture office has provided money for the safe destruction of 1,200 kilograms of chemicals used to make ecstasy, chemicals that were discovered recently inside an international shipping container. Agency executive director Phil Tawtel said it was the first time his office has covered the cost of destroying such precursor chemicals. "These chemicals arrived in B.C. via Port Metro Vancouver and the ship came from China," he said. Inside the container, Canada Border Services Agency workers found almost a tonne of methylamine HCL in 33 kegs and about 200 kilograms of helional in a drum. Tawtel said the chemicals "were identified by the authorities as having no legitimate use beyond creating harmful synthetic street drugs. There was no other reason to have it here." The RCMP requested a $7,000 grant to cover the cost of disposal of the chemicals by a private Lower Mainland company, Tawtel said. Postmedia News (The Vancouver Sun, A10)

10 serious crimes that could get permanent residents kicked out of Canada
Impaired driving causing bodily harm, theft over $5,000, cultivation of marijuana — under a new bill, all of these offences could send a permanent resident back to their home country without a hearing. Under the proposed Removal of Serious Foreign Criminals Act, permanent residents convicted of a serious crime will be ineligible for a record suspension — otherwise known as a pardon. The government will also be allowed to bypass the usual admissibility hearing before issuing a deportation. That means that a convicted person would no longer have an opportunity to have their deportation reviewed. A representative from Canada Border Services Agency said that removing the admissibility hearing for permanent residents "significantly streamlines the current process which means faster removals and cost savings to taxpayers." But the definition of a serious crime is broad — if a permanent resident has been convicted of a crime carrying a maximum penalty of ten years or more or has been given a sentence greater than six months, they could be sent straight home. Our Windsor

Tubes pétroliers vietnamiens: le Canada voit encore rouge
L'Agence des services frontaliers du Canada (ASFC) vient de décider d'ouvrir un réexamen afin de mettre à jour les valeurs normales, les prix à l'exportation à l'égard de certaines fournitures tubulaires pour puits de pétrole (FTPP) en provenance de divers pays, dont Vietnam. Le réexamen a été ouvert dans le cadre de l'application continue par l'ASFC des conclusions rendues le 2 avril 2015 par le Tribunal canadien du commerce extérieur à l'égard de certaines FTPP originaires ou exportées du Vietnam à l'issue d'une enquête concernant des allégations de dumping et subventionnement dommageables. Cette enquête découle d'une plainte déposée par des producteurs canadiens qui allèguent que le dumping et le subventionnement ont causé et menacent de causer un dommage à la branche de production nationale qui produit des marchandises similaires. Vietnam Plus

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

* **CRA phishing expedition suggests agency still vulnerable on security**
A security test by the Canada Revenue Agency found thousands of its employees could not resist the lure of a phony e-mail phishing scam, a discovery that suggests vulnerabilities remain at the agency more than a year after it was rocked by a major online security breach. The Globe and Mail has learned that over the first three months of this year, the agency's security and internal-affairs division sent 16,000 employees an e-mail designed to replicate the potentially dangerous messages that are common to anyone with an e-mail account. A phishing scam usually involves an e-mail that encourages a user to click on a link, which could then expose the user's computer to malicious software. The result of the CRA's test was that 78 per cent of employees did not click on the link contained in phishing attempts. However, that means roughly 3,500 employees did fall for the scam, even though they were informed ahead of time that the test would take place. Globe and Mail, A1

* **Malware attack leads GN to block employees' access to web email**
Government of Nunavut workers will no longer be allowed to access their personal web-based email accounts on government computers after a recent malware attack. Martin Joy, who heads the IT department for the Government of Nunavut, said malicious software or malware attacked one GN

computer this month after the user connected to a free web mail account and downloaded a zip file that had the malware attached. CBC.ca

LAW ENFORCEMENT / APPLICATION DE LA LOI

Un réseau de trafic de stupéfiants mis K.-O.
L'Escouade régionale mixte de la Montérégie croit avoir mis fin aux activités de trafic de stupéfiants lié au crime organisé en démantèlement un réseau de distribution et de vente de drogue en Montérégie et dans les Haute-Laurentides. Une vingtaine de personnes ont été arrêtées. Cocaïne, méthamphétamine, cannabis et près de 200 000 $ ont notamment été saisis. Quelque 200 policiers ont participé hier à la vaste opération antidrogue baptisée Mariolle. Ils ont arrêté 21 personnes, dont la p résumée tête dirigeante du réseau, René Raymond, 54 ans, de L'Ascension. Dix-neuf perquisitions ont été réalisées dans une dizaine de municipalités, dont Chambly, Mascouche, Saint-Hubert, Marieville et Terrebonne. L'enquête initiée par l'Escouade régionale mixte de la Montérégie en mai 2014 découle d'une multitude d'informations colligées par la Régie intermunicipale de police Richelieu St-Laurent au sujet d'un réseau de trafic de stupéfiants dans la région de Chambly, explique l'inspecteur Patrick Bélanger, directeur des enquêtes sur le crime organisé à la Sûreté du Québec. L'investigation des agents leur permet de croire que René Raymond agissait comme indépendant et gérait un réseau de distribution et de trafic de stupéfiants en Montérégie et dans les Hautes-Laurentides. Il aurait, toujours selon l'enquête policière, obtenu l'autorisation du crime criminalisé, soit des Hells Angels, pour avoir l'exclusivité de vente et de la distribution sur un territoire moyennant le paiement de redevances, explique l'inspecteur Bélanger. Les membres du réseau se seraient également livrés à des actes d'intimidation et de violence pour contrôler leur territoire de vente de stupéfiants, indique l'inspecteur. Incendie criminel, coups de feu tirés sur des résidences et des véhicules, agression armée, et même une tentative de meurtre auraient été commis. La Voix de L'Est; * La Presse

Fines test legal grey zone
The town of Granby doesn't often make headlines, other than the occasional story about a jogger being chased by a black bear. That all changed last week, however, when news spread of the town council's unanimous decision to make it illegal to insult police and other municipal officers online - a move applauded and panned across the country. As it turns out, however, Granby isn't the only town to make it an offence to insult the police. Sherbrooke, Shawinigan and Quebec City, for example, have similar bylaws on the books, raising the question of why so many feel it necessary to "protect" the police from verbal abuse, and why now? It's not clear just how often the bylaws are enforced and tested in court, and whether they can apply to online insults as well. In Trois-Rivières, after 2006, officers handed out more than 200 tickets per year for swearing at or insulting them. And in at least one case, in the town of Lévis, near Quebec City, a motorist was fined $150 in 2011 for his online diatribe. Antoine Cloutier-Lachance, a South Shore driver, had posted a comment on the Facebook site of a Lévis police officer: "I just wanted to thank you for the ticket the other day - "criss de trou de q !!!!!!" For towns like Granby and Westmount, where a first offence will now trigger a fine of up to $1,000, it's a question of protecting employees, say politicians. "Unfortunately, as much as there are positive aspects to social networks there are negative ones, too," said Robert Riel, deputy mayor of Granby. Montreal Gazette, A1

Cost of policing for June 4 Moncton shootings is $9M
The cost of extra policing in the aftermath of the June 4, 2014, murder of three RCMP officers in Moncton totals $9 million. Most of that will be covered by the federal and provincial governments. The full explanation of the costs and how they will be paid was publicly presented Wednesday night to members of the Codiac Regional Policing Authority. The Metro Moncton communities will be asked to pay a total of $3.5 million. CRPA financial officer Paul Van Iderstine said the authority (which is cost-shared by Moncton, Riverview and Dieppe) should be able to absorb $2 million of this in its $27.5-million annual budget, or $1 million each year for 2014 and 2015. That leaves $1.5 million for special policing costs that would be cost-shared by Moncton ($1 million), Dieppe ($300,000) and Riverview ($200,000). Van Iderstine said he is now in contact with Ottawa to see if the payments can be staggered over a three-year period. CRPA chairman Nick LeBlanc said he and other members of the board were relieved that the numbers are finally out in public view after many months of negotiations with government and police

officials. Codiac Regional RCMP constables Fabrice Gevaudan, Dave Ross and Douglas Larche were shot and killed on the evening of June 4, 2014, while responding to 911 calls of a suspicious-looking man carrying weapons. Constables Darlene Goguen and Éric Dubois were wounded... The federal government is picking up approximately $1 million under the terms of their policing agreement with the province where they share policing costs. $1.5 million worth of costs are not being billed by other jurisdictions who sent officers to Moncton. This was seen as covered under a mutual aid agreement. Van Iderstine said this agreement would mean that if another jurisdiction had a similar crisis, Codiac would be obliged to send assistance. Van Iderstine said this leaves the $3.5 million for the Codiac Region to absorb. This includes $2 million for the crime investigation and $1.5 million or 50 per cent of the overtime, meal and accommodation costs of those officers who backfilled for Codiac's regular officers when they were on leave after the emergency period. Van Iderstine thanked the RCMP, other police jurisdictions and government officials for their co-operation on what was a long process. Times & Transcript, A1 (Telegraph-Journal, A1); Chronicle Herald

Joggins Terrorized by arson

There remain more questions than answers for residents of the small Cumberland County community of Joggins who have been terrorized by arson. "We're looking for something here. Do you see a prosecution in the future?" Brian Hebert, owner of the former Odd Fellows hall that burned on May 5, asked RCMP Staff Sgt. Al Carroll. Over 200 residents who packed into the Joggins branch of the Royal Canadian Legion for a community meeting Wednesday night about the fires then looked from Hebert toward Carroll. "At the end of the day, I would say yes," said Carroll. "But I can't say when that day is." On the night of May 5, Joggins residents awoke to find their community ablaze. Three unoccupied houses, an old garage and the former Odd Fellows hall had been set on fire. The fire spread to the United Church, which was saved by over 60 firefighters from 10 departments who rushed from all over the county. "With that mass of woodwork upstairs in the church - if it had of caught," Mike Carter, fire service co-ordinator for the Municipality of County of Cumberland, told the meeting. "Well, we had a million dollars worth of trucks in close (to the church) and we would have had to make a retreat and try to save the firehall (across the road)." Chronicle Herald, A1

Mayors want regional crime unit restored

Less than six months after the successful regional crime unit folded, the mayors of Colwood, Langford and View Royal want the province to force its resurrection in response to a crime spike in the West Shore. It wasn't long after the regional crime unit - which targeted prolific offenders - disbanded at the end of 2014 that serious crime in the West Shore started to rise, said Langford Mayor Stew Young. "Everything was going great until the last three to six months, when we saw a spike in violent crimes," Young said. "It's doing so much damage to our community because it's not there." On the heels of a meeting with West Shore RCMP Insp. Larry Chomyn, Young, Colwood Mayor Carol Hamilton and View Royal Mayor David Screech will write a letter to the Justice minister and police services division asking for a meeting about West Shore's police resources and the possibility of bringing back the regional crime unit. Despite high-profile arrests of the region's most prolific property criminals, the unit folded after withdrawals by Victoria police in 2008, and Central Saanich police and Sidney-North Saanich RCMP last year. Young said the unit was disbanded without a discussion by the region's mayors to ask: "How are we going to fill this void?" He said it frustrates him that the Integrated Road Safety Unit thrives because of funding from Insurance Corporation of B.C. and traffic-ticket revenue, but a crucial unit targeting prolific offenders can fold because of money problems. In November, the province introduced amendments to the Police Act that would force municipalities to participate in integrated policing units. The change was in response to recommendations by commissioner Wally Oppal in the Missing Women Inquiry regarding better co-ordination across jurisdictions. Times Colonist, S1 Front

Napanee pair arrested in drug bust

A large quantity of crystal methamphetamine has been seized after a lengthy investigation by the Ontario Provincial Police's Organized Crime Enforcement Bureau-drug Enforcement unit. On Monday evening at approx imately 10:20 p.m., OPP and Port Hope Police Service worked together to conduct a search of vehicles parked in a car pool lot on Toronto road in Port Hope. In the vehicle, officers found 523 grams of crystal methamphetamine with an estimated street value of $52,300, more than $10,000 in Canadian currency, a blue 1992 Ford Mustang and a silver 2007 dodge Caliber. Van Phuc Luu, 38, of Toronto and

Kristopher Jerome, 24, of napanee were arrested and charged by police with one count each of trafficking a controlled substance, possession of property obtained by crime over $5,000, and two counts each of possession of a controlled substance for the purpose of trafficking. The two men remain in custody awaiting a bail hearing. The investigation continued in napanee, and, as a result, Jerome's sister, Stephanie Jerome, 26, of napanee was also arrested and charged by police. during the search, the OPP executed a search warrant at an Ann Street residence on Tuesday at approximately 1:50 a.m. Officers seized 26 grams of crystal methamphetamine, steroids and more than $10,000 in Canadian currency. Kingston Whig Standard

Investigation that jeopardizes safety
An editorial states, "Try posing as a police officer and see what happens. But apparently the other way around, cops posing as members of the media, for example, they consider fair game. Provincial police in Ontario say it's a practice they rarely use. But three media organizations, CBC, Canadian Journalists for Free Expression, and RTDNA Canada, have applied to Ontario's Superior Court to have impersonation of journalists by the police force declared a charter violation that can't be justified. A lawyer representing the media organizations claimed the method was not limited to the Ontario Provincial Police. Consider the concerns. From the point of view of the media, knowledge that such a practice exists can put genuine journalists under suspicion - and at risk. Another point is that it compromises their position, possibly making it harder to get information in certain instances... It's been successful. But it's also been criticized because of the chance that the person under investigation might embellish his or her desperate acts to impress the "gang boss." It's fair to say the public wants to see the police have the means they need to carry out successful investigations, to help keep the public safe. But let's keep in mind any investigation that resembles a fishing expedition carries a high degree of speculation - results could be questionable. But the big concern here is investigations that could jeopardize the safety of another group represents an ethical dilemma that should not be a police tool." Cape Breton Post

Trace pen on mark for valuables
Residents now have a new way to mark their possessions in case they are stolen, thanks to a Canadian-made product. Endorsed by the Ontario Association of Chiefs of Police, the Trace pen and program marks personal belongings so they can be identified by police or a pawn shop. Const. Greg Harbec, community programs officer with the Kingston Police's Community-Oriented Response and Enforcement Unit, said the pen, which retails for $39.99 online, can invisibly mark roughly 50 items. "It's cheap insurance to identify a very valuable piece of jewelry, for example, that doesn't have an identifiable mark," Harbec said. "So for a dollar, maybe a $5,000 ring can be identified and returned." Purchasers of the Trace pen register each item online at trace identified.com.If a marked item is stolen, the owner can change the item status to stolen. The same goes if the item is sold. Police and pawn shops can check for a Trace marking using a black light. "(Pawn shops) don't want to deal with stolen property, and they work with police," Harbec said. "They are reputable businesses, so they have a lot to lose." Harbec said vehicle companies have had similar technology for a number of years. He said there are similar products around the world, but Trace is unique to Canada and Ontario, and Kingston Police don't have access to other databases. Kingston Whig Standard, A6

Un réseau de trafiquants violents démantelé en banlieue de Montréal
Un réseau de trafiquants de stupéfiants qui n'hésitait pas à utiliser la **violence** pour éliminer la concurrence et faire respecter son territoire de vente a été mis hors d'état de nuire, hier, dans la grande région de Montréal. Pas moins de 200 policiers ont participé à la vaste opération, qui s'est soldée par l'arrestation de 21 personnes, dont la présumée tête dirigeante de l'organisation criminelle. Selon les autorités, le réseau était principalement actif en Montérégie et au nord de Montréal. L'enquête a également permis d'établir que le chef présumé de l'organisation, René Raymond, 54 ans, payait des dividendes aux Hells Angels afin de pouvoir exercer librement le trafic de stupéfiants sur le territoire. Journal de Montreal, 16

B.C. government wants better electronic method to monitor high-risk offenders
The B.C. government is looking for a new electronic monitoring system that will allow it to keep tabs on high-risk offenders, with the Justice Minister acknowledging the current system is "out of date." The issue came to the fore last September after the killing of 17year-old Serena Vermeersch in Surrey. The man

charged in her death, Raymond Caissie, was a high-risk offender who was not being monitored electronically. The province's monitoring system was revealed as archaic, requiring the use of a home telephone line. Jurisdictions such as Edmonton and Calgary use systems that rely on GPS instead. B.C. Justice Minister Suzanne Anton told a house committee this week that the government will be issuing a request for proposals for a new electronic monitoring system by the end of the month. Though she has defended the current system - and at times continued to do so at the committee meeting - she said the new system will be required to have a GPS component... In an interview Wednesday, Surrey Mayor Linda Hepner said she looks forward to the new system being implemented. "Any system that will allow the tracking of high-risk offenders through GPS is a good thing, in my opinion," she said. Spokesmen with both the RCMP and the Vancouver Police Department declined comment on the new system and referred inquiries to correctional officials. Globe and Mail, S1

Police probe shooting
B.C.'s Independent Investigations Office is investigating after a man was shot by a Mountie in Burnaby. The incident happened at about 1:45 a.m. Wednesday, said Kellie Kilpatrick of the investigations office. RCMP said officers were responding to a call about an intruder at a home who possibly had a knife. When they arrived, they were confronted by a man who would not comply with directions and an officer shot him, police said. The man was taken to hospital with what police said appeared to be non-life-threatening injuries. No other injuries were reported. Police said the investigations office seized a knife from the scene. Postmedia News (Vancouver Sun, A4); Canadian Press (Times Colonist, The Province)

*** Recours judiciaire possible contre la GRC**
La GRC a caché et détruit des renseignements relatifs au registre des armes d'épaule qui étaient réclamés en vertu de la Loi sur l'accès à l'information et un recours judiciaire pourrait être intenté contre le corps policier, conclut la commissaire à l'information du Canada, Suzanne Legault, dans un rapport d'enquête obtenu par La Presse. Ces conclusions pourraient d'ailleurs expliquer des amendements législatifs surprenants inclus dans le projet de loi omnibus de mise en oeuvre du budget, C-59, déposé au Parlement la semaine dernière. Ces amendements prévoient que le registre des armes d'épaule et tout fichier affilié ne seront plus accessibles par l'entremise d'une demande d'accès à l'information, et ce, de manière rétroactive au 25 octobre 2011. Le projet de loi C-59 prévoit également une immunité pour des agents de l'État pour tout acte posé durant cette période relativement à des demandes d'accès à l'information concernant le registre. Au cours des derniers jours, plusieurs personnes se sont questionnées ouvertement sur la raison de ces changements, que certains ont décrits comme une tentative du gouvernement Harper de réécrire l'histoire. La Presse, A14

*** Hells Angels, 'puppet' bikers roll into Langford**
Between 100 and 150 motorcyclists from the Hells Angels and other clubs rolled into Langford on May 2 for the opening of Greater Victoria's first biker clubhouse. The bikers were greeted with a heavy police presence, including West Shore RCMP, the Integrated Road Safety Unit, and regional, provincial and federal units dedicated to outlaw motorcycle gangs. The clubhouse is believed to belong to the Devils Army. According to the Combined Forces Special Enforcement Unit, B.C.'s anti-gang unit, the group is a Hells Angels "puppet club." RCMP Staff Sgt. Andrew Isles of the Island District management team said the opening of the new clubhouse is significant. "We're always interested in who is in our communities as far as outlaw motorcycle gangs go," Isles said. "There are some new faces here we're seeing, and we're also taking stock of who's here and who's invited." RCMP escorted about 90 bikers to Langford from Campbell River, Nanaimo and the Lower Mainland. Several traffic violation tickets were issued. Aside from the opening of the clubhouse, the bikers were also gathering for the Zeke Run. The spring ride is held in memory of Edward (Zeke) Mickle, a Nanaimo Hells Angels member who hasn't been seen since May 1993. Times Colonist, S4

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Top court to decide whether Khadr a youth or adult
The case of former Guantanamo Bay prisoner Omar Khadr returns to Canada's top court for a third time on Thursday, as the federal government fights to have him declared an adult offender for crimes he

committed as a 15-year-old. The dispute centres on whether the eight-year sentence a U.S. military commission handed him for war crimes should be interpreted as a youth or adult sentence. However, the arcane technical legal battle has taken on loud political overtones. "This case is another illustration of the heavyhanded approach Canada has consistently taken towards him," said Gillian Hnatiw, who represents the Canadian Civil Liberties Association, which is intervening in the case. Khadr, 28, was released on bail last week after almost 13 years in custody while he appeals his U.S. conviction, which has drawn fierce criticism from legal and human rights experts. Although he was 15 when his crimes occurred in Afghanistan in July 2002, the military commission made no distinction between juveniles and adults in sentencing him in 2010 to a further eight years behind bars. (...)No provisions exist for an inmate to serve both youth and adult sentences at the same time, so Ottawa classified him as an adult offender when he transferred to Canada from Guantanamo Bay in September 2012 under an international treaty to serve out his punishment. Canadian Press (Red Deer Advocate, Waterloo Region Record, Edmonton Journal, Hamilton Spectator, Telegraph-Journal, Times & Transcript, Brandon Sun), * Presse canadienne (Le Soleil, Radio-Canada)

Commitment hardly foggy
A letter to the editor states, "Re: Fog surrounds Omar Khadr case, Christie Blatchford column, May 12 Ms. Blatchford, if you find the Khadr case foggy, my suggestion is that you turn off the fog machine on which you are clearly seated. The Khadr case is foggy in the same way the case for climate change is in question. The Khadr case is indeed foggy if you persist in pretending that Guantanamo Bay military commissions are real courts and look to pleas made there to find truth. This is a position that the American government and judiciary abandoned long ago but with which our government (and Blatchford) persists. The case is foggy if you quote discredited prosecution psychiatrist Michael Welner's Islamophobic conclusions and ignore the long list of other mental health professionals who have unanimously concluded Omar Khadr does not pose a threat." Edmonton Journal, A18, Toronto Star, * Vancouver Sun, * Windsor Star, * Winnipeg Free Press

*** Khadr no victim**
A letter to the editor states, "I only have two words concerning Omar Khadr ... Convicted murderer!" Calgary Sun, Kingston Whig-Standard

*** What Khadr needs most in his new lease on life**
An opinion piece states, "With his release last week, Omar Khadr, who for so long was a distant embodiment of a heated international justice issue, has now entered our hearts and minds as a flesh and blood young man. After I saw him, I couldn't get him out of my mind. Standing with his lawyer and now host/guardian Dennis Edney, Khadr managed to sound genuine, gracious and even optimistic as he told a press conference he wanted to prove "I'm better than the person he (Stephen Harper) thinks I am." Well, we all want Khadr to be a better person than our vengeful Prime Minister thinks he is. The question is how to help him get there. Much to the displeasure of the Harper government, Khadr, freed by a judge, walked out from an Alberta jail after 12 years a prisoner, many of those years spent being tortured and held without due process at the notorious American prison at Guantanamo Bay. His government-our government-was, to its shame, the only Western nation not to call for the release of a detainee. He is appealing the verdict, claiming he pled guilty under pressure - but whatever the outcome of that appeal, he has already served his time, time that as a minor, he probably should never have served in the first place." Toronto Star

Man arrested on drug charge
A Sydney man has been remanded after he was arrested on a drug charge Wednesday. Police arrested Francis (Frank) John Abbass, 63, of Howe Street on Wednesday afternoon at the intersection of George Street and Brookland Street. He is charged with possession for the purpose to traffic in marijuana and was remanded to the Cape Breton Correctional Centre. Abbass, who was on parole regarding previous drug charges, also had his parole revoked by Correctional Services Canada. He is awaiting a future court date. Cape Breton Post, A3

Court confirms Surrey child molester's dangerous offender designation

A Surrey man who snuck into a young girl's home in the dead of night and molested her in her bedroom has lost an appeal of his dangerous offender classification. That means his sentence has no expiry date. Kyle Wayne Berkson, 40, was sentenced in 2013 in Surrey provincial court. His nine-year-old victim was sexually assaulted in her bedroom while her grandparents slept in the next room. (...)He was designated a dangerous offender in 2013. He appealed that, and lost. The appeal was heard in B.C. Court of Appeal in Vancouver. Vancouver Sun; * The Province

* **Le Canada fait bande à part**
Un article d'opinion déclare, « C'est quand même incroyable. Alors que le gouvernement Harper ne cesse de durcir ses politiques pénales, les États-Unis, pourtant les grands champions du genre, commencent à se rendre compte que les peines de prison trop longues sont contre-productives. (...)A court terme, le Canada risque de devenir, avec les dictatures du tiers-monde, le seul pays au monde à enfermer ses criminels pour la vie sans possibilité de libération conditionnelle. L'Europe avait déjà un système pénal beaucoup plus libéral - avec des peines plus courtes et sujettes à révision périodique. Si les États-Unis remettent en question la philosophie de la répression extrême, le Canada sera bientôt aussi isolé, sur cette question, que sur les enjeux climatiques. » La Presse, A25

* **Son frère lui avait fait vivre l'enfer**
L'un des frères de Chantal Demers, dont le corps a été retrouvé lundi à Saint-Raymond de Portneuf, a fait vivre l'enfer à sa soeur à l'automne 2011. Jean-Marc Demers, qui a été accusé de tentative de meurtre à l'endroit de Mme Demers, a finalement plaidé coupable à une accusation réduite de voies de fait graves en 2012. (...)Après un procès plutôt médiatisé en 2012, Jean-Marc Demers a été condamné à cinq ans de prison et le juge lui a notamment interdit de posséder une arme. Selon nos informations, il est toujours derrière les barreaux dans un pénitencier de la région de Montréal. Le Soleil (Le Nouvelliste, 9)

* **Gladue report ordered for Richard Wolfe**
A Gladue report has been ordered to look into what elements of Richard Daniel Wolfe's First Nations background might have helped contribute to his history of offending. Wolfe is awaiting sentencing on charges to which he pleaded guilty in March: Sexual assault and assault with a weapon, both of which sprang from an incident that took place in Fort Qu'Appelle on April 6, 2014. (...)The offences for which he is now awaiting sentencing arose while he was out on statutory release. A Canadawide warrant was issued (Wolfe eventually turned himself in) after he sexually assaulted a woman and beat her boyfriend with a baseball bat. Leader-Post, A7 (StarPhoenix)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Televised taunting speaks to pervasive 'rape culture'
The confrontation between a television reporter and her on-air tormentors is shining a light on the dark "rape culture" pervasive in today's society, experts say. But it will take much work to eradicate these deeply rooted misogynist beliefs. "Sexual violence against women in our world is normalized and it's excused in the media and pop culture," said Joan Tuchlinsky, public education manager for the Sexual Assault Support Centre of Waterloo Region. "When we're dealing with rape culture, it's going to take a long time to address it." On Sunday, CityNews reporter Shauna Hunt challenged several men at a Toronto FC game after sexually explicit taunts were hurled at her while she was working on-camera. It's an example of a disturbing trend that has seen the same vulgar phrase, "F--- her right in the p----," being shouted at reporters worldwide over the past 18 months. The abusers are almost always men. Their victims are almost always women. Waterloo Region Record, A1; * Globe and Mail, * Winnipeg Free Press

* **Shifting focus to women's safety**
The White Ribbon campaign is in talks with Maple Leaf Sports and Entertainment about working together to come up with strategies to make sports venues "a safe place" for working media. Officials from the campaign -- led by men dedicated to ending violence against women -- approached MLSE Tuesday morning as news spread about CityNews reporter Shauna Hunt confronting a group of male soccer fans

she said conspired to interrupt her newscast by saying "f---her right in the p----" outside BMO Field Sunday after a Toronto FC game. "Our immediate concern was they wanted to get some measures in place to make sure the stadium is a safe place for reporters," White Ribbon executive director Todd Minerson said on Wednesday. "We talked about long-term change and issues and both of us decided, 'Let's let this settle for a couple days and come and have a conversation in the next week.'" Toronto Sun, 4 (Ottawa Sun)

Justice conference explores solutions
It's easy to point a finger at the problem, and quite another to conjure up solutions to said problem. In a nutshell, this is what the three-day, Innovative Strategies in Criminal Justice: From Policy to Practice conference is all about. "All the conferences we go to on criminal justice the conversation centres around 'the plight of,' it's the plight of poor aboriginals in the criminal justice system, poor homeless, poor mentality ill -- everybody is getting screwed by the criminal justice system," said Chris Hay, executive director of the John Howard Society of Alberta, and conference organizing committee member. In total, 33 speakers, including five keynote speakers from around the world, signed on for the conference held at MacEwan University's Robbins Health Learning Centre, from May 12-14. Edmonton Sun, 17

* **Anti-racism activists seek proof of carding's impact**
A group of Toronto professionals and academics who belong to the Anti-Black Racism Network are joining a growing chorus of activists calling for an end to police carding. And the group is searching for answers as to why, in an information age, police have the technology to gather the data but don't have the statistics to defend it. "We have yet to be provided evidence that carding impacts crime in any shape or fashion," Rinaldo Walcott, an associate professor at U of T, said at a press conference Wednesday. "We have yet to be provided evidence that the database developed from carding impacts crime and its resolution in any way or shape. "We find this totally unacceptable in the age of information," Walcott said. "We believe that by ignoring available evidence, that the mayor, the Toronto Police Service and its board have clearly declared black communities collectively a public safety threat. Toronto Star, GT1

PUBLIC SERVICE / FONCTION PUBLIQUE

Clement pressures unions for sick leave deal by fall
Treasury Board president Tony Clement has further turned up the pressure on federal unions by saying he wants to reach a deal on a new sick-leave regime before the election. In an interview, Clement said he is open to further negotiations with the 18 federal unions on his contentious plan to revamp sick leave and disability management, but wants agreement by this fall. Federal election day is Oct. 19. He didn't clarify how long he was willing to continue those negotiations in the run-up to polling day. Whether negotiations fail, hit an impasse or proceed too slowly for his liking, the government is giving itself the power to impose the terms and conditions of a new sickleave regime whenever it wants. The government has been tightening the circle around unions in recent weeks after nearly a year of collective bargaining that has unfolded at a snail's pace. The big issue is accumulated sick leave, which the government wants to replace with a new short-term disability plan. The 18 unions dug in their heels from the start, signed a solidarity pact and refused to make any concessions on sick leave. They claim they're willing to fix any problems or abuses but won't budge on the existing accumulated sick-leave regime that their members want. Ottawa Citizen, A1

OTHER / AUTRE

NIL

INTERNATIONAL / INTERNATIONAL

NIL

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
May 28, 2015 / le 28 mai 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

MINISTER / MINISTRE

*** Listen up, Canada: You can't advocate free speech and criminalize dissent at the same time**
While Canadian Prime Minister Stephen Harper appears to be auditioning for a lead role in a political bromance with Benjamin Netanyahu in some epic right-wing production, he may well have overplayed his part with his latest move. As the Canadian Senate debates Bill C-51, the Conservative government's "anti-terror" bill that would give Canada's spy agency sweeping new powers and has alarmed civil libertarians, environmentalists, First Nations activists and Muslim Canadians, another frightening aspect of the Harper government's agenda has been revealed. Following the lead of Israel, where a law criminalizing participation or encouragement of BDS was recently upheld by the High Court of Justice, in a majority ruling equating boycotts with "political terror," the Canadian Conservatives are now conflating the advocacy of the boycott, divestment and sanctions campaign with hate speech. [...] But it was Canadian **Public Safety Minister Steven Blaney** who made the link explicit. In a speech at the United Nations a few days after the memorandum was signed, Canada's CBC News reported, **Blaney** linked BDS with anti-Semitic hate speech and even the attack on Charlie Hebdo – which the Conservatives claimed was an attack against free speech. The Canadian government, added **Blaney**, now has "***zero tolerance***" for BDS. Haaretz.com

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** 'Hectic' start to fire season**

Alberta's wildfire season is only three months in and already it has consumed significantly more forest than last year. So far this season there have been 720 wildfires in the province, burning just under 30,000 hectares of forest, compared to 400 fires at this time last year, which burnt about 700 hectares. All evacuation orders related to wildfires raging in Alberta were lifted as of Wednesday afternoon, but 15 wildfires are still burning out of control, including one that has been creeping toward oil and gas infrastructure near Cold Lake, Scott Long from the Alberta Emergency Management Agency told a news conference. Cenovus and CNRL both have operations in the area. As of Wednesday morning, about 250 firefighters and 10 helicopters were fighting the blaze, which is still considered out of control and is expected to keep growing in the days ahead. At least some of 150 extra firefighters coming to Alberta from other provinces are expected to be deployed to the Cold Lake fire. Edmonton Journal, A1

* **Evacuees returning as fires ease**
Thousands of Albertans are returning home as evacuations have been lifted and wildfires brought under control. A 208-hectare fire near Wabasca has been held by perimeter guards and evacuees have been told it is safe to return while 61 firefighters continue battling the blaze. Residents have been advised to listen closely to emergency notifications and be prepared to leave in case the threat returns. Evacuees are also returning to the Mortonville area, near Slave Lake, where 27 firefighters continue to battle a 138-hectare fire. Close to 5,000 people were evacuated due to wildfire threats Sunday and Monday. Calgary Sun, 24; Canadian Press (Times Colonist, Red Deer Advocate)

* **Alberta fires encroaching deeper into the oilsands**
Wildfires in northern Alberta spread farther into the oilsands area Wednesday, keeping about 10 per cent of production offline and pushing Canadian crude prices higher. A fire at Cold Lake Air Weapons Range that started Saturday expanded to cover 17,500 hectares as fire crews worked to prevent the blaze from reaching Cenovus Energy Inc.'s Foster Creek oilsands facilities, Alberta's Environment and Sustainable Resource Development agency said on its website. Another fire near the town of Chard grew to 1,400 hectares and burned in an area with "numerous pipelines and well sites." National Post, FP4

* **Hurricane season likely to be less active, says meteorologist**
There may be fewer storms forming off of Canada's East coast this year, Environment Canada meteorologist Bob Robichaud said during a press event held by Environment Canada today. This does not mean the season will necessarily be less severe, Robichaud said. "Regardless of the number of storms that are forecast, people need to prepare. Even if it's a forecast of a below average season, it only takes one storm to make it a bad season." Robichaud said there will likely be six to eleven storms this season, with up to two developing into hurricanes. Last year there were eight to thirteen storms predicted, four of which made landfall and two reaching hurricane status - hurricanes Arthur and Gonzalo. Times & Transcript, A9; Canadian Press (Cape Breton Post); Chronicle-Herald

* **New Brunswick crew off to Alberta to fight wildfires**
New Brunswick is going to help fight wildfires burning out of control in Alberta. Roger Collet, a provincial fire prevention officer with the Department of Natural Resources, said 21 firefighters are leaving on a flight to Alberta on Thursday. He said the department received a call from officials in Alberta on Tuesday requesting help. Daily Gleaner, B1

* **Fire conditions 'slowed to a steady roar'**
Hot, dry and windy weather persists throughout the province, allowing 19 fires to continue burning throughout Saskatchewan as of Wednesday. Wildfire hazards are still classified as high to extreme across Saskatchewan, provincial fire centre manager Scott Wasylenchuk said. Nine new fires were reported between Tuesday and Wednesday morning, and five are believed to be human-caused, he said. Wasylenchuk said conditions have "slowed to a steady roar," adding crews are making good progress. StarPhoenix, A4

* **West Country on high alert**
The West Country's wildfire hazard has been a good news/bad news scenario this week. Cooler temperatures, higher humidity and some rain took some of the edge off the fire hazard. However, the

unsettled weather came with lightning, which sparked seven wildfires by Tuesday night. Red Deer Advocate, C1

*** Crews foil fire in Emerald Lake area**
It was all hands on deck Tuesday evening for a small bush fire near Emerald Lake caused by a tree falling on a power line running along the highway. Firefighters from Yukon Wildland Fire Management and the volunteer fire departments of Carcross and Mount Lorne responded, along with two helicopters dispatched from Whitehorse to provide aerial support with water buckets. Located 1.5 kilometres north of Emerald Lake, the fire was contained at 0.3 of a hectare. Whitehorse Daily Star, 4

*** Little progress made on preventing wildfires: report**
B.C. hasn't made much progress in recent years on preventing catastrophic wildfires close to homes and businesses, according to a report. In 2010, the Forest Practices Board called on the B.C. and municipal governments to support efforts to remove fuel such as prescribed burns, regular tree pruning and brush removal. A followup report from the board, released Wednesday, suggests little meaningful work has been done since then. Vancouver Sun, A9

*** Derailments involving hazardous cargo raise concerns**
Trains carrying a range of cargo, including hazardous goods such as petroleum products and chemicals, derailed 124 times last year in B.C., according to federal transportation safety board summary reports based on tougher reporting criteria. Derailments involved as many as 24 cars and almost 200 metres of damaged track and occurred for reasons such as collisions with motor vehicles, spillage of coal on the tracks, broken rails or train axles, rail cars moved onto unaligned switches, unwanted emergency brakes, buildup of ice and snow, and rock slides. Some of those derailments involved relatively harmless commodities such as barley, grain, lumber, aluminum and shale, while others have the potential to cause serious human and environmental harm: hydrochloric acid, sodium chlorate, sodium hydroxide, ethanol, crude oil, glycol and diesel fuel. The 124 B.C. train derailments in 2014 compares with 110 in 2013 and a five-year average. Vancouver Sun, A5

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Le projet de loi C-51 approuvé
Le comité sénatorial qui a fait l'examen du projet de loi antiterroriste 2015 au cours des dernières semaines a approuvé le document, mais il soumet des observations au gouvernement pour considération. Le Comité permanent de la sécurité nationale et de la défense a déposé son rapport au Sénat hier. Il recommande, entre autres, de prolonger de 1 à 5 ans la période pour le dépôt d'accusations pour des infractions qui auraient été commises aux termes de la Loi sur la sûreté des déplacements aériens. Le comité propose aussi d'ajouter des photos dans un registre des personnes soupçonnées de menacer la sûreté des transports, ou qui prévoient se déplacer en avion dans le but de commettre un acte terroriste. Journal de Québec, 29

Police played on woman's obedience to pull her into terror plot
A Crown prosecutor says a husband-and-wife duo facing terrorism-related charges is "undeniably, undoubtedly and undisputedly" guilty of scheming to blow up the provincial legislature. However, defence lawyers are adamant that the couple's plot would have had no chance of success had undercover police not propelled it along. A B.C. Supreme Court jury heard closing submissions on Wednesday, which recapped nearly four months of evidence - including more than 100 hours of video and audio surveillance - presented in the trial of accused terrorists John Nuttall and Amanda Korody. They're accused of plotting to detonate homemade pressure-cooker bombs on the crowded front lawn of the B.C. legislature lawn during Canada Day festivities two years ago. They were arrested on July 1, 2013, following an elaborate RCMP sting operation and have each pleaded not guilty. In his address to the jury, Korody's lawyer Mark Jette described his client as the perfect, submissive, Muslim wife who lived an isolated life marred by poverty and drug addiction. He said she became the victim of a controlling husband and an overeager RCMP operation intent on "pulling her into their orbit." Jette asked the jury to question the likelihood that Nuttall and Korody would have been able to accomplish their alleged plot without the support and

guidance of the police. He criticized the operation's primary undercover officer as playing a heavy-handed role in guiding the accused. Red Deer Advocate, A5; The Telegram (Whitehorse Daily Star); Times Colonist

Accused: Targets or terrorists?
Whether the RCMP manipulated a Surrey couple into participating in a plot to turn 2013 Canada Day celebrations into a massacre is irrelevant, the prosecution insists. In B.C. Supreme Court Wednesday, Crown attorney Peter Eccles maintained in his final address that police conduct in the 240-officer sting didn't matter. "They blame the police - 'the police manipulated us into doing it, it wasn't us,' " Eccles mocked. "Entrapment - no, entrapment actually is not a defence that is available here ..." At that point, however, Justice Catherine Bruce interjected: "I have to interrupt you. The jury do not have to concern themselves with any issue regarding entrapment. It's not something that should concern (the jury)." Obviously irked, she said sharply that jurors should also ignore everything Eccles had said about whether the accused were acting under "duress." John Nuttall, 40, and his common-law wife Amanda Korody, 31, have pleaded not guilty to terrorism-related charges in connection with the alleged plan. Their lawyers painted a picture of poor, addicted, recent converts to Islam living on welfare - vulnerable, needy and posing little threat until the RCMP targeted them in the elaborate ruse. Eccles, however, reiterated that jurors have heard and seen everything that mattered during some 100 hours of surveillance footage and wiretaps played during the four-month trial. Vancouver Sun, A6; The Province; Globe and Mail

Military show draws peaceful crowd
The face of war has changed over the past 15 years, but its nature hasn't, say critics of the Cansec military weapons show in Ottawa. "It's the poor of the world that are always the victims of the wars these guys get rich on. That hasn't changed at all," said Matthew Behrens, co-ordinator of Homes Not Bombs, a group of peace activists who held a 10-hour protest in front of the EY Centre Wednesday. Terrorism would be less a threat if the United States and allies like Canada didn't impose military solutions to world problems so frequently, Behrens said. The al-Qaida and Islamic State terrorism launched in recent years against democracies, including Canada, is a backlash against them. If the west were less aggressive, terrorism would wane and there would be no need for a weapons show, Behrens said. This year's Cansec -- billed as Canada's premier defence trade show -- is the first since the ISIS-inspired shooting by Michael Zehaf-Bibeau, the gunman who opened fire at the National War Memorial and Parliament last October and since the discovery of alleged homegrown terrorists who wanted to join ISIS. "As long as you have an ISIS, Cansec will be successful," Behrens said. Canadians think of themselves as peaceful, but Cansec is a reminder Canada is a major manufacturer and exporter of weapons, said protester Richard Sanders. Because the Canadian government subsidies weapons-makers, its people and its government contribute to the misery wars create, Sanders said. Ottawa Sun, 10

We can dismantle the surveillance state. Here's how.
Just two short years ago, if you asked strangers on the street about mass surveillance, you'd likely encounter many blank stares. Some would remember East Germany's Stasi spy agency, or reference China's extensive Internet censorship. But few would express fear that western democratic governments like the U.S., Britain, and Canada were engaged in the mass surveillance of law-abiding citizens. That all changed in June 2013 when Edward Snowden, a contractor at the U.S. National Security Agency (NSA), blew the whistle on the spying activities of the NSA and its Five Eyes partners in Canada, Australia, New Zealand and the U.K. Since then, we've seen a long stream of revelations about how Canada's Communications Security Establishment (CSE) is engaged in extensive spying on private online activities. We learned that CSE spied on law-abiding Canadians using the free Wi-Fi at Pearson airport, and monitored their movements for weeks afterward. We learned that CSE is monitoring an astonishing 15 million file downloads a day, with Canadian Internet addresses among the targets. Even emails Canadians send to the government or their local MP are monitored - up to 400,000 a day, according to CBC News. Just last week we discovered CSE targets widely-used mobile web browsers and app stores. Many of these activities are authorized not by a judge, but by secret ministerial directives like the ones Peter MacKay signed in 2011. Ipolitics.ca

Teen accused of trying to join ISIL denied bail

An Alberta teen charged with planning to leave Canada and join the terrorist group Islamic State, or ISIL, was denied bail Wednesday. The 17-year-old was attentive as he listened to Judge Danielle Dalton's reasons for keeping him in custody. Those reasons, and the evidence presented at the hearing, are under a court-ordered publication ban. The teenager's bail hearing lasted most of last Friday, when he made his first in-court appearance since his arrest in Beaumont in March. Before then, he appeared only by closed-circuit television. It was the second time the teen has been denied bail. The first denial came from a justice of the peace shortly after his arrest. The youth, who cannot be identified, faces two terrorism-related charges after his arrest by the RCMP's Integrated National Security Enforcement Team. He is charged with attempting to leave Canada to join a terrorist group and, on the second charge, to participate in terrorist activity. Once outside the country, the youth intended to commit an offence, "namely murder, in circumstances that constitute terrorist activity," the charges state. The youth returns to court June 17. Edmonton Journal, A2; Edmonton Sun

Le PQ et la CAQ réclament des actions
Le Parti québécois et la Coalition avenir Québec (CAQ) ont demandé hier au gouvernement Couillard d'agir contre le Centre culturel islamique de l'est de Montréal et son dirigeant Adil Charkaoui, dans la foulée du témoignage du père d'une jeune fille arrêtée par la GRC de crainte qu'elle n'aille rejoindre des groupes djihadistes à l'étranger avec des amis. La Presse et le Toronto Star ont publié ce matin une entrevue avec le père de la jeune fille, qui accuse Adil Charkaoui et son centre islamique d'avoir radicalisé son enfant et de l'avoir convertie à une interprétation extrémiste de la religion. Lors de la période des questions à l'Assemblée nationale, la députée caquiste Nathalie Roy a demandé une réaction au «cri du coeur» de l'homme. «Ce que nous dit ce père de famille, c'est le gros bon sens que tous les Québécois voient. Ce père accuse ceux qui endoctrinent les jeunes. Ils ont tous fréquenté le même centre communautaire islamique où oeuvre Adil Charkaoui, et ce n'est pas le fait du hasard [...] Le gouvernement doit agir contre ces agents de radicalisation», a-t-elle lancé. «Qu'est-ce que le gouvernement attend pour agir dans le cas du Centre culturel islamique de l'Est de Montréal et d'Adil Charkaoui? Quand est-ce qu'on va faire de la prévention au Québec?», a demandé de son côté la députée péquiste Agnès Maltais. La Presse, A6 (Le Soleil)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Driver jailed in fatal collision
Audrey Goertzen says she and her five children can now move on with their lives after the man who drove through a rural stop sign and killed her husband Cory more than two years ago has been jailed and slated to be deported back to his native Nigeria. (…) Crown prosecutor Cameron Jose had argued for a three-to five-year sentence. Defence lawyer George Sirois sought a sentence of 90 days, but no more than six months, so his client could appeal any deportation order. Postmedia News (Calgary Herald, A14, Calgary Sun)

Woman who advised au pairs to lie to guards deserves jail
Prosecutors are seeking two years in jail for a Fraser Valley woman who counselled more than 100 foreign au pairs to lie to border guards about their reason for coming to Canada. (…) The Canada Border Services Agency began investigating in 2008, after officers intercepted a young woman coming from France. (…) On Oct. 12, 2010, Canada Border Services Agency officials executed a search warrant at Large's home in Chilliwack. Postmedia News (Province, A19, Times Colonist)

OPP to announce results of gun-trafficking probe
Ontario Provincial Police were expected to announce multiple arrests Thursday morning as a six-month long project targeting gun traffickers comes to an end. Project Harden culminated Wednesday with several search warrants being executed in Ottawa, Cornwall and the Montreal area. (…) The project, which attempted to disrupt a gun-trafficking route from Cornwall to Ottawa, was a joint effort headed by the OPP's organized crime and provincial weapons units and also involved Ottawa police, Cornwall police, Canada Border Services Agency, RCMP and Akwesasne police. Postmedia News (Ottawa Citizen, Standard Freeholder) (2015-05-27)

Newport lance les travaux d'expansion de son aéroport
Pendant que Sherbrooke attend toujours un mécanisme qui lui permettrait d'effectuer des contrôles de sécurité dans son aéroport, la Ville de Newport au Vermont a lancé les travaux d'expansion de son aéroport situé à Coventry. (…) M. Lachance rappelle que Sherbrooke dispose déjà de la présence de douaniers à son aéroport et que le seul point qui achoppe est celui d'offrir des services de sécurité reconnus. Selon lui, les échos laissant croire à une annonce imminente concernant la sécurité dans les aéroports non désignés sont de plus en plus persistants. Sans avoir eu de confirmation, il s'attend effectivement à une annonce avant la fin de la session parlementaire. Tribune, 5

L'aéroport international de... Mont-Joli?
Voyager vers Londres, Paris ou New York à partir de Mont-Joli? C'est le souhait de la candidate à l'investiture du Bloc québécois dans Avignon-La Mitis-Matane-Matapédia, Kédina Fleury-Samson, qui ambitionne d'internationaliser le petit aéroport du Bas-Saint-Laurent. (…) Malgré qu'un projet d'allongement de la piste à 6 000 pieds (1 829 mètres) soit toujours envisagé, ce qui permettrait des départs vers des destinations soleils à partir de Mont-Joli, les avions devraient obligatoirement passer par d'autres aéroports puisque celui du Bas-Saint-Laurent n'offrent pas de véritables services douaniers internationaux, sans compter les dizaines de millions de dollars qu'il faudrait investir dans une telle aventure. Agence QMI (Journal de Québec, Journal de Montréal) (2015-05-27)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

* **U.S. orders probe into IRS security breach**
U.S Congress is demanding answers about how identity thieves were able to steal the personal tax information of more than 100,000 taxpayers from an Internal Revenue Service (IRS) website. Senate Finance Committee Chairman Orrin Hatch has requested a confidential briefing by IRS officials by the end of next week. "It is critical that this committee fully understand what took place, what information was at risk, how this may affect tax administration, and what appropriate legislative responses may be needed to reduce the risk of this occurring again," Hatch said Wednesday in a letter to IRS Commissioner John Koskinen. The information was stolen as part of a sophisticated scheme to claim fraudulent tax refunds, Koskinen told reporters. It was taken from an online system called "Get Transcript," where taxpayers can get tax returns and other tax filings from previous years. In order to access the information, the thieves cleared a security screen that required knowledge about the taxpayer, including Social Security number, date of birth, tax filing status and street address. Associated Press (Toronto Star, B4)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Toronto police halt controversial mental health disclosures
It may have been a suicide attempt from decades ago, or perhaps a mental health crisis that prompted a 911 call. Until this week, the Toronto Police Service would release non-criminal mental health information - such as a suicide attempt that provoked police interaction - to an employer or community group running a police record check on a potential employee or volunteer working with children or vulnerable people. The disclosure of such sensitive personal health information has come under fire for years by civil and mental health rights groups, who say a growing number of Canadians lose employment and volunteer opportunities because of the discriminatory practice - particularly since the demand for police record checks by potential employers has gone up. But Toronto police have now joined the increasing number of law enforcement agencies halting the controversial disclosures, sending the message that a history of mental illness should not be automatically deemed relevant to potential employers. "This step will allow people who may have just had one terrible period of crisis in their life to have the same chance as other people to access education and employment," said Jennifer Chambers, with the Centre for Addiction and Mental Health's Empowerment Council. Toronto Star, A1

A week in, a week under attack: Chief defends carding practices
Mark Saunders jokes that if he were a fruit fly with a brief lifespan, the honeymoon he enjoyed after

becoming chief of Toronto police might seem sufficient. But "from a human perspective, the honeymoon didn't last very long - no, not at all." From the day it was announced that Chief Saunders would take over from Bill Blair, he has been under attack for defending the much-disputed practice of carding - stopping and questioning people who are not under arrest or detention and recording the details of the encounter. He isn't taking it lying down. In an interview with The Globe and Mail a week after he was sworn in on May 20, he complained that his critics are never satisfied. "Every time I've tried to say something, the term 'carding' kind of changes its meaning," he said. "It gets a little frustrating." Chief Saunders also said that while he is committed to halting random police checks of citizens just going about their business, carding suspected gang members is vital to keeping the city safe. "If it's done right, it protects people." To those who say that carding amounts to a form of racial profiling, targeting a disproportionate number of racial-minority residents, Toronto's first black police chief said: "We're not sending officers into areas because people are brown or black. We're looking at the charts. We're looking at where the violence is occurring and it's about 6 per cent of the geographics of the city. And so we're putting officers in there because that's where the violent crimes are occurring." Globe and Mail, A1

Moncton's 3K for 3 Fathers run to fund scholarships

This Father's Day will mark the second annual 3K for 3 Fathers Memorial Run, established last year to honour RCMP constables Fabrice Gevaudan, Douglas Larche and Dave Ross, who were killed in the line of duty on June 4, 2014, by Justin Bourque. On June 21, runners from across the province will gather on the Moncton waterfront. The funds raised will create scholarships for the six high schools that Codiac RCMP serve. The scholarships will be given to students who demonstrate leadership, courage and bravery. "We decided as a group this would be the right way to honour the three fallen, to create a scholarship that had the ideals they represented," said co-director Armand Doucet. "When we talk about courage, leadership and bravery, it's a pretty broad spectrum, but it really represents what they did on that day." Along with the organizing team from last year's run, which included friends and co-workers of the three officers who were killed, this year's event is being organized with the help of Nadine Larche, wife of Const. Doug Larche. "Last year's run meant a lot to all of us," said Nadine Larche in a news release. "It was a way to bring the community together. It was a place for us to be on Father's Day - which was a difficult day for all of us. This run helps us to continue moving forward. We've had our struggles during the past year, and this run is a positive place to focus energy, to focus on the good of the community and to focus on one of our husbands' passions, which is running." Last year, the event garnered a turnout of more than 7,000 runners, many holding their own satellite runs around the world. The organizing team's goal is for 1,000 runners to participate with a fundraising goal of $25,000. The cost to participate in the race is $30 for adults but free for children. Kids T-shirts are $10. Times & Transcript, A1

Body may be slain woman

RCMP say it is unclear how long it will take to determine if human remains discovered in a wooded area near Framboise, Richmond County, are those of Michelle Demers-Kennedy. Orange markers highlighted a trail Wednesday to where a burial site was located in an area off North Framboise Road. Police believe they have exhumed the remains of the 58-year-old Richmond County woman who disappeared May 3, 2013, and was reported missing 10 days later. Her eldest son, Merlin Demers-Kennedy, 32, pleaded guilty to manslaughter last week. He was originally charged with second-degree murder in his mother's death, but a psychiatric assessment later revealed a long history of suffering from paranoid schizophrenia that often went untreated. The 70-page report also indicated that his mental illness may have prevented him from forming the specific intent to commit murder… "It's around seven kilometres from here to her home," Const. Kevin MacDougall of the RCMP said as he stood near the site. RCMP say they identified the burial site earlier this week but would not say what led them there. "It's not information we're going to release. As you can appreciate, it's still before the courts," RCMP spokesman Sgt. Alain LeBlanc said Wednesday. "Whenever we have a missing person's case which turns into a homicide case, that's important for us that we find the body, and also for that family, that is what's important. I'm sure this will bring some closure to the family." Chronicle Herald, A1; Cape Breton Post, A1

Government ignored advice of lawyers: Dix

The B.C. government went against the advice of its own lawyers in 2012 when it publicly referred to RCMP involvement in the case of fired Health Ministry researchers, says NDP MLA Adrian Dix. Just

hours prior to a news conference by then health minister Margaret MacDiarmid on Sept. 6, 2012, Justice Ministry counsel advised the government not to say the RCMP was involved, Dix said Wednesday. While Dix can't provide definitive proof, and the Justice Ministry won't comment, the NDP MLA said the information was confirmed by the Justice Ministry. "People at the Ministry of Justice have told me that's the case - that they advised against [including the RCMP]," Dix said. "I think the evidence supports that that was the advice given." Dix also released previously blacked-out sections of a review of the investigation by independent lawyer Marcia McNeil last December. Those sections show the Justice Ministry provided advice "with respect to the reference to the RCMP in the news release" issued on the firings, though what counsel advised was not included in the report. At the Sept. 6 news conference, MacDiarmid announced the ministry had fired four people and suspended three without pay, and had "asked the RCMP to investigate." In the end, the fired researchers were exonerated - two were rehired, four resolved settlements and just two wrongful dismissal suits remain unresolved. Meanwhile, the RCMP never launched a formal investigation. The government said in February that it no longer wanted the RCMP to look into the issue. One of those fired was a co-op student just three days shy of completing his term. Roderick MacIsaac killed himself in December of 2012. The suggestions of an RCMP investigation increased MacIsaac's frustration and stress around allegations he knew to be wrong about a privacy breach, his family said. The RCMP reference was all propaganda and innuendo, Linda Kayfish, the dead man's sister, said Wednesday. "They wanted to strongly infer something was wrong, while at the same time provide an excuse for not having to provide any facts." Times Colonist, A1

Gun amnesty idea gets support

The city and its police service are on the same page when it comes to holding another buy-back program for illegal guns. Ward 3 Coun. Matthew Green introduced a motion asking Hamilton police to go ahead with another amnesty opportunity following the recent, high-profile exchange of gunfire at the corner of Main Street and East Avenue. Green said he feels his ward sees a troubling amount of gun violence, but added street safety is a concern across the city. Council need to "take leadership" to protect its residents, he said. Coun. Lloyd Ferguson, who is also the police board chair, said he has spoken to Chief Glenn De Caire about the amnesty idea and received a positive response. The service ran a gun amnesty program last year that resulted in 374 guns and almost 20,000 rounds of ammunition being turned over to police. Hamilton Spectator

Privacy concerns the public

Toronto Police will no longer provide information about prior mental health issues when Vulnerable Sector Screening applications are made, the Toronto Sun has learned. The policy change went into effect Monday and applies to the VSS report required from the police force when people apply for certain jobs or volunteer positions, such as teachers, daycare workers, social workers, adoptive parents and coaches for sports teams. One person's privacy can be another's lack of information on just who it is leading their children. If your child's karate instructor, dance teacher, hockey coach or scout leader once had a mental health episode, the organization, and ultimately you as a parent, will no longer be entitled to that information from any police background check. A letter dated May 20 to " stakeholders" on Toronto Police letterhead, signed by Deputy Chief Mike Federico, said the policy change is in accordance with a recommendation made by the Ontario Association of Chiefs of Police last June. So if someone has a suicide attempt in their past or was in contact with police for any mental health issue, police will no longer provide it as part of a reference check letter. Police do not do background checks on behalf of employers or organizations but for the people wanting to coach, teach, work or volunteer, Toronto Police spokesman Megan Gray explained. If in doing the check police discovered incidents with police it would be reported on as part of the letter, she said, adding the service feels it is the best way forward for people had previous mental health issues. Toronto Sun, 4

Drugs seized near Sooke school

Sooke RCMP have arrested five people in what they believe to be a "significant" drug-trafficking operation near Sooke Elementary School. Four men and a 16-year-old girl were arrested after a search warrant was executed at 11:30 p.m. Tuesday at a Lanark Road house. Police seized what they called a "substantial quantity" of illicit drugs - believed to include methamphetamine, psilocybin mushrooms, and GHB, more commonly known as the date-rape drug. Drug-trafficking paraphernalia was also seized, as well as stolen property, including items the RCMP said were linked to a break-in at a commercial

premises in Sooke. A replica handgun, machetes, knives and ammunition were also found. Because police had been alerted that there could be weapons in the house, the RCMP Island District Emergency Response Team was called in to assist in the search. The 16-year-old girl was released to the care of a guardian, while the four men remain in custody, said detachment commander Staff Sgt. Jeff McArthur. Charges have not been filed. Times Colonist, A3

Toronto police say Pan Ams won't be G20 all over again

Const. Craig Brister is standing in front of a small crowd of business owners in the St. Lawrence Centre on Toronto's Esplanade, assuring them that the Pan Am Games will not be another G20 when it comes to policing. "As soon as we start talking about all these extra officers that will be in town and all this extra security, people immediately get this idea of G20 in their mind," says Brister, an officer seconded from 32 Division to serve as the Toronto Police Service's business and community liaison for the Games. "This is a sporting event," he says. "This is family, front row. That's the big thing we're trying to push. But at the same time there needs to be a security component." That means a heightened police presence around venues, not only to secure them but to enforce no-standing zones and street closings. It also means there will be police sweeps, beginning June 26{+ }in areas such as the Pan Am Athletes Village, the 14-hectare fenced-in area in the Canary District - which is next door to the Distillery District, one of the Games' three festival sites. Brister says he hates the term "police sweeps," and it shouldn't be misinterpreted. "Officers are getting trained to do security checks," says Brister. "They tour the venues when we take possession of them. They also tour them during the Games. What they're looking for is the obvious - security problems, gaps in the security, safety issues - anything that's going to affect game play or spectator safety."... The security plan for the Games has local forces policing venues in their own municipalities, removing any confusion - which occurred during G20 planning - about who is in charge. Toronto police have cut the number of officers who can be on vacation during the two weeks of the Games nearly in half to accommodate Pan Am security. Also, 9,000 unarmed private security guards have been hired to provide access control at events. Toronto Star

*** Retroactive-law critic is nitpicking**

Treasury Board President Tony Clement says concerns over a Conservative move to retroactively rewrite the law in order to stop an investigation of alleged RCMP wrongdoing are akin to angels dancing on the head of a pin. The latest omnibus budget bill from the Harper government quietly inserted amendments, backdated to October 2011, that wipe clean any complaints about the handling of long-gun registry data before Parliament passed a bill to end the registry the following year. Clement says that since Parliament did eventually pass a law to end the registry, complaints about when that law took effect are simply arcane legal nitpicking. Federal information commissioner Suzanne Legault issued a report last week calling the move a "perilous precedent" that could be used to retroactively clear government officials of wrongdoing on everything from election fraud to spending scandals. She recommended to the attorney general of Canada in March that an investigation be launched into the RCMP's wilful destruction of registry data that was covered by the Access to Information Act - an investigation that has now been taken on by the Ontario Provincial Police. The Harper government responded by retroactively rewriting the law, backdating the amendments to the day the bill to end the long-gun registry was first introduced in Parliament, and then burying the changes this month in a 167-page budget bill that will be rammed through Parliament before the summer recess. Clement, whose portfolio includes overseeing and enforcing Canada's access-to-information law, brushed off Legault's concerns about a future government using the same after-the-fact tactic to clear itself in the face of an active police investigation. "I don't think it sets any precedent at all," Clement said Wednesday following a Conservative caucus meeting. Canadian Press (Times Colonist, A9, Telegraph-Journal, Times & Transcript); La Voix de L'Est

*** Officer sued for alleged excessive use of force**

A Whitehorse man is suing an RCMP officer for assault and unlawful arrest. Documents filed Tuesday in Yukon Supreme Court allege Stefan Brynjolfsson was punched repeatedly in the face by Whitehorse RCMP Const. Nathan Menard, causing him to fall and hit his head on the ground. He was also "violently restrained" with an armhold, he says. The altercation took place in July 2013. It left Brynjolfsson with a head injury, cuts and bruising on his face, cuts and contusions on his back and soft tissue injuries to his right elbow and shoulder, he alleges. According to the documents, Brynjolfsson and Menard knew each other previously from a Whitehorse gym. They're both trained in Brazilian jiu-jitsu. Whitehorse Star, 2

*** Mountie accused of assault says man tried to grab gun**
A Mountie charged with assault has told a judge that he became scared for his life when a drunken man tried to reach for his gun. Const. Grant Jacobson said he was trying to remove the man from a downtown Kelowna pub at closing time, but he refused to co-operate and swore at him. Jacobson, 32, told court that as he grabbed John McCormick's wrist to handcuff him from behind, the man turned around and caught him off guard. "He was either trying to assault me or trying to escape," Jacobson said Tuesday. "At that point I decided I was going to take Mr. McCormick to the ground to handcuff him." Jacobson said he grabbed McCormick around the head and shoulders and kicked out his foot. He felt a tug on the pistol on his belt and realized McCormick, 61, was going for his gun, the officer told provincial court Judge Greg Koturbash. "It's such a frightening moment ... when you feel someone trying to take your pistol away," the Mountie said. "The only thing I could think of was, 'I'm going to hit him until he stops.' And I hit him until he stopped. And his hands were clearly no longer on my pistol." Postmedia News (Vancouver Sun, Kelowna Daily Courier)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

'I wish that I could just be the next Joe on the street who nobody knows and who nobody gives a second look or thought to. That would be my ideal life'
Omar Khadr is standing in his bedroom looking out at the backyard. It is his second morning of freedom after nearly 13 years behind bars, and he's embarrassed because he doesn't know how to open the window. "Oh there we go. Well, that will come in handy," he says as he's shown where to lift the latch and fresh air fills the room. "It got hot yesterday. So that's one of the basic skills I'm going to learn, is how to open my window." Open a window. Open a bank account. Get a driver's licence. Get a library card. There are so many small skills to be learned by a man who has loomed large since he was shot and captured in Afghanistan at the age of 15 - a man who has never been allowed to speak publicly. For the first time since being granted bail earlier this month, Khadr spoke over two days in exclusive interviews for the Toronto Star and a documentary that will air Thursday on CBC-TV. Until now, Khadr has existed in caricature drawn and defined by others: victim, killer, child, detainee, political pawn, terrorist, pacifist; he has been compared both to South African freedom fighter Nelson Mandela and to serial murderer Paul Bernardo. He has been prosecuted by the Bush and Obama administrations, interrogated by Canadian intelligence agents while the Liberals were in power, vilified by the Conservative government and defended as a child soldier by prominent figures such as retired lieutenant-general Roméo Dallaire and peace activist Desmond Tutu. Toronto Star, A1, La Presse, A6/Front, Reuters (Globe and Mail), Yahoo! News); CBC News, Radio-Canada

Omar Khadr de retour sur les bancs d'école
L'ex-détenu de Guantánamo Omar Khadr a amorcé cette semaine un trimestre d'été à l'Université King's, située à Edmonton, a indiqué au Devoir son avocat, Me Dennis Edney. Le jeune homme a bénéficié de quelques semaines de quiétude, depuis la sortie médiatique suivant sa mise en liberté sous caution. La petite université chrétienne King's avait tissé des liens avec le jeune homme alors qu'il était en prison et l'avait invité, en février dernier, à venir étudier dans son campus, une fois libéré. Chose promise, chose due. Celui qui envisage une carrière dans le domaine de la santé suit actuellement des cours à King's dans le but de terminer sa douzième année scolaire, précise Me Edney. " Son éducation est l'une de ses priorités en ce moment. " La philosophie de cette maison d'enseignement est de former les étudiants à devenir des agents de réconciliation et de réhabilitation dans la société. (...)Au Canada, Omar Khadr poursuit au civil le gouvernement pour 20 millions de dollars. Le gouvernement canadien a quant à lui porté en appel la décision de libérer sous caution Omar Khadr en attendant que sa cause soit entendue aux États-Unis. Advenant une victoire du gouvernement canadien dans cette dernière situation, Omar Khadr ne retournerait pas dans un pénitencier fédéral, confirme l'avocate et titulaire de la Chaire de recherche du Canada sur la justice internationale pénale et les droits fondamentaux, Fannie Lafontaine. Une récente décision de la Cour suprême stipule en effet qu'il doit être traité comme un contrevenant mineur plutôt qu'adulte. Le Devoir, A1

Victim of released sex offender Frank Skani calls for public warnings

A Burnaby, B.C., woman who was viciously attacked in her home is demanding mandatory public warnings be issued when high-risk sex offenders are released. "Kate" - not her real name - says no one warned her a violent offender was being allowed to visit a woman staying in her basement suite. On Aug. 24, 2013, Kate was attacked by Frank William Skani - a man with two dozen convictions, many for violent sexual assault. (...)Skani had been the subject of a public warning by Vancouver police two years earlier, when he had been previously released from prison. He quickly breached his conditions, was imprisoned for a month, then released. But there was no new public warning that he was out on the streets again - and no warning that he had crossed into Burnaby, where he was being allowed overnight stays with his wife in Kate's basement suite. "He was on parole. He was supposed to be watched. Why did it happen? Why wasn't I warned?" asks Kate. "It could have stopped it from happening. Maybe if I had seen his face I wouldn't have opened the door." (...)Burnaby RCMP would only tell CBC News that when it comes to "monitoring and notifications, we would have to defer to Correction Services Canada." But Corrections Canada - responsible for prisons and prisoners - told CBC News it could not discuss the specifics of an offender's case, citing the Privacy Act. CBC News

Dorchester inmate, 33, dies at Moncton hospital
A Sydney man serving a five-year sentence at Dorchester Penitentiary died at Moncton Hospital early Wednesday morning. Matthew Ryan Hines, 33, was found unresponsive in the New Brunswick institution's medium security unit. Hines was transported to hospital by ambulance after staff members performed CPR. Hines was pronounced dead at 12:02 a.m. Nadine Boucher, spokeswoman for Correctional Service Canada, couldn't comment on the possible cause of Hines's death or any other details of the incident, including when the man was discovered unresponsive by staff. "At this time, it's under investigation," Boucher said. "Correctional Service Canada will review the circumstances of the incident. That's all we know at this time." Chronicle-Herald, A12

* **200 000 $ réclamés à ses 4 oncles agresseurs**
Après avoir courageusement dénoncé et envoyé en prison quatre de ses oncles l'ayant agressée sexuellement pendant toute son enfance, une victime décide maintenant d'aller plus loin en les poursuivant au civil pour 200 000 $. Élevées chez leurs grands-parents, dans une famille nombreuse de Grande-Rivière en Gaspésie, Guylaine et Nathalie Lebreux ont été les véritables «objets sexuels» de leurs quatre oncles. Dès l'âge de six ans, et jusqu'à leur adolescence, les deux victimes ont été utilisées pour assouvir les pulsions sexuelles de Raymond, Eudore, Élodien et Carol Lebreux. (...)Si «Raymond, Eudore et Élodien avaient un minimum de reconnaissance», Carol Lebreux a toujours nié les gestes. Ce dernier, le seul toujours en prison après avoir eu cinq ans de détention, s'est rendu jusqu'en Cour suprême pour se défendre. Or, le balancier de la justice entre la sentence et les sévices subis par les deux victimes ne sera jamais égal, selon elles. Ainsi, après plusieurs mois de réflexion, Guylaine a décidé de foncer et de poursuivre les quatre agresseurs au civil pour 50000$ chacun. Journal de Québec, 3 (Journal de Montréal)

* **Donnie Snook's trailer forfeited to the Crown**
The trailer in which disgraced former Saint John city councillor Donnie Snook made child pornography has been forfeited to the Crown. The trailer, a 2004 Starcraft Tent Trailer, was seized by police, along with numerous electronic devices and a vehicle, following Snook's arrest on Jan. 9, 2013. Crown special prosecutions prosecutor Derek Weaver presented an application to Provincial Court in Saint John on Wednesday afternoon seeking forfeiture of the trailer. Neither Snook or any representation on his behalf appeared in court for the hearing. Snook is incarcerated in prison, serving an 18-year term, having pleaded guilty to 49 child sex abuse crimes involving 17 boys, and was sentenced in 2013. The crimes occurred over a dozen years, and the victims included boys as young as five years old. Telegraph-Journal, B2

* **Un ancien Nomad sans moto**
Walter Stadnick, ancien membre des Nomads, défunt groupe d'élite des Hells Angels du Québec, ne pourra enfourcher une moto de sitôt, a tranché la Commission des libérations conditionnelles du Canada. Comme ils le font régulièrement avec les délinquants liés au crime organisé, les commissaires aux libérations conditionnelles lui ont imposé des conditions spéciales, notamment de ne pas posséder ou conduire une moto, de demeurer dans une maison de transition et de respecter un couvre-feu entre 21 h

et 6 h. Stadnick, 62 ans, a été de nouveau libéré d'office en décembre dernier, après avoir purgé les deux tiers d'une sentence de 14 ans et 7 mois pour des affaires de stupéfiants et de complots pour meurtre à la suite de son arrestation dans l'opération Printemps 2001. La Presse +, Hamilton Spectator

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Mental health to be left off background checks
In a step forward for mental-health rights, the Toronto Police Service will no longer release records of non-criminal mental health encounters with police - including suicide attempts or other psychological crises - to employers and community groups requesting background checks on potential employees or volunteers. Effective this week, the Toronto police force joins law enforcement agencies across Ontario and Canada halting a practice that civil rights and mental health groups have long been decrying as discrimination affecting a growing number of Canadians. Rights organizations including the Canadian Civil Liberties Association, the Ontario Human Rights Commission and the Information and Privacy Commissioner of Ontario have increasingly been sounding the alarm that Canadians with a history of mental illness - or even a single mental-health episode that provoked a police response - have lost employment and volunteer opportunities due to the release of non-conviction mental-health records. In a May 20 memo sent to community organizations working with children or vulnerable people, Toronto police announced that effective this week, groups making background checks under the "Vulnerable Sector Screening Program" will no longer receive information about mental-health-related contact with police. Prior to the change, Toronto police released mental-health information when asked for it by groups hiring for positions ranging from teaching to coaching to volunteering and more. Toronto Star, GT1; , * Globe and Mail

*** Men walking the walk to end violence and abuse**
The time has come for men to wake up and reclaim their traditional role as providers and protectors, says the organizer of a walk to raise awareness about abuse and violence against women. Conrad Burns, organizer of the Walk of Hope and co-founder of Rise Up Against Violence, said this year he will finally make the 360-kilometre trek from Prince Albert to Regina, thanks to the support of others along the way. (…)On Wednesday, Burns delivered his message to the chiefs and councillors attending the Federation of Saskatchewan Indian Nations spring assembly. It's time for men to reclaim their traditional role of protectors and providers, he said, adding men also need take a lead role in helping to end violence against women. StarPhoenix, A5 (Leader-Post)

*** Indigenous drumming to the rescue: a beat we might hear a lot this summer**
An opinion piece states, "Too often we are drumming for our women after they are gone. That is what Shanastene McLeod's mom and auntie said to me while they were going house to house in the North End looking for her. They're scared she will end up on the list of missing and murdered indigenous women. Shanastene is 25. Her family says she is addicted to drugs and she bounces between "crack shacks" and doesn't come home. They're scared she's being sexually exploited. Out of desperation the family did something remarkable. They put a call out to the community to bring their drums and call Shanastene home with traditional music. (…)Frustration bubbled over. I guess that's what happens when there are 1,200 missing and murdered indigenous women in Canada. This community has clearly hit their breaking point. You know what, their strategy worked. Shanastene was in the neighbourhood and she came outside." CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRE

NIL

INTERNATIONAL / INTERNATIONAL

Wide-ranging snooper's charter to extend powers of security services
David Cameron is to use the Tories' unexpected parliamentary majority to press ahead with a "turbo-charged" version of the snooper's charter that will extend the powers of the security services in response to the debate that followed surveillance disclosures by NSA whistleblower Edward Snowden. In a surprise move, the government is to introduce an investigatory powers bill far more wide-ranging than expected. The legislation will include not only the expected snooper's charter, enabling the tracking of everyone's web and social media use, but also moves to strengthen the security services' warranted powers for the bulk interception of the content of communications. The extension of the bill to "modernise the law" on tracking communications data, which was agreed within government only this week, came as the prime minister used his fresh majority to challenge the chief source of funding for the Labour party. The Guardian UK

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Federal Court ruling on CSIS retention of associated data / Décision de la cour fédérale sur la conservation des données connexes

2016-11-03 – 2016-11-04
16:00 ET

Table of Contents / Table des matières

Overview / Vue d'ensemble

On November 3, 2016 the Federal Court of Canada released its ruling on the Canadian Security Intelligence Service's (CSIS) handling of associated data. The ruling stated that CSIS had been unlawfully retaining data since the Operational Data Analysis Centre (ODAC) was created in 2006 and criticized the service for failing in its duty to be candid with the court.

In the past 24 hours, the ruling has garnered extensive national media attention, with all major print, online and broadcast outlets reporting it as a top story. The ruling was also covered internationally by wire services including *The Associated Press*, *Reuters*, *Agence France-Presse* and *The Wall Street Journal*.

Visibility was amplified due to recent news events concerning police surveillance of journalists in Quebec, polls showing Canadians see national security as one of the strengths of the Liberal mandate and the public consultation on national security that is underway in parallel. Coverage, while factual, employed highly negative language to describe the ruling, such as "scathing," "hard-hitting," and "blow." Rights groups and journalists expressed frustration at the perceived privacy infringement, particularly on social media and argued that the ruling underscored the need for greater oversight of Canada's national security agencies. Conversely, a key criticism in coverage questioned the effectiveness of an oversight committee due to partisan control. Similar concerns were voiced by NDP Justice Critic Murray Rankin in a press conference this morning.

Yesterday afternoon's technical briefing with CSIS Director Michel Coulombe and Chief General Counsel Robert Frater from the Department of Justice acknowledging the court ruling, explaining

the implications and outlining corrective measures was well-received by media, many of whom recognized the government's swift response.

Volume of coverage declined significantly following Minister Goodale's media availability this morning, when he responded to questions around the timeline of events, potential repercussions for implicated parties, safeguarding of Canadians' privacy and how the ruling could impact the service's ability to do its job. Overall, social media activity stemming from the availability highlighted the Minister's comments that he would be reviewing the issue of candor with CSIS management.

Selected Quotes / Citations choisies

Ralph Goodale - Minister of Public Safety and Emergency Preparedness

"Justice Noel did not dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could not find existing legislative authority permitting its retention and use."

"I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service."

"In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the government of Canada are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms."

"The court's insight and guidance are timely, coming in the midst of the public consultations we now have underway about Canada's national security framework."

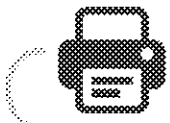
"The CSIS Act is now more than 30 years old and showing its age as global affairs, threat profiles, technology and public expectations have rapidly evolved."

Michel Coulombe - Director of the Canadian Security Intelligence Service (CSIS)

"I'll be honest, we went through our records and we really can't find a good explanation of why the court was not informed."

"That is something I will discuss with officials, (Public Safety Minister Ralph Goodale) and it is a public policy decision that the government and parliamentarians will have to make."

"I deeply regret the court's serious concerns with respect to meeting our duty of candour, and I commit to continuing my efforts, with the deputy minister of Justice, to address this concern."



Goodale says CSIS 'taking steps' to comply after court rules it broke law
The New Democrats are calling for "strong, new oversight" of the Canada's spy agency in the wake of a court decision that has found that the organization illegally kept electronic data about people for 10 years. In a news conference on Parliament Hill on Friday, NDP justice critic Murray Rankin called the judgment "very disturbing" and said it reveals "gross abuse of power by Canada's spy agency." (…) Speaking to reporters on Friday about the ruling, **Public Safety Minister Ralph Goodale** said he is taking ***"very seriously"*** the finding that ***"CSIS had failed in its duty to be candid" with the court. "(CSIS) has confirmed to me that it is taking immediate steps to address the court's decision,"*** **Goodale** said. ***"It has blocked all access to, and analysis of, any associated data while it considers its next steps to comply."*** **Goodale** also said he is asking the Security Intelligence Review Committee (SIRC) to "monitor the situation carefully to ensure compliance." SIRC is an independent review body that reports to Parliament on CSIS operations. In a ruling made public on Thursday, Justice Simon Noel said CSIS illegally held on to potentially revealing electronic data about people over a 10-year time period. The court found that the spy agency breached its responsibility to inform the court of its electronic data collection, given that the information was gathered using judicial warrants. CTV News (2016-11-04)

CSIS metadata breach: Ralph Goodale 'pursuing criticism' with spy agency management - 'I take very seriously the explicit finding … that CSIS had failed in its duty,' public safety minister says
Public Safety Minister Ralph Goodale suggested today that there may be more fallout for the senior management of Canada's spy agency after a Federal Court decision found CSIS broke the law in failing to destroy potentially sensitive information about Canadians. ***"I take very seriously the explicit finding by [Federal Court] Justice Noel that CSIS had failed in its duty to be candid with the court,"*** he told reporters before entering question period. ***"I will be pursuing that criticism with the executive management of the service,"*** he said. ***"In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the government of Canada are being effective at keeping Canadians safe, and equally that they are safeguarding our rights and freedoms, including privacy and the rule of law. "From the service and from the department of justice, a strong and timely remedial plan is required to reassure the Federal Court about the issue of candour,"*** he said. CBC News (2016-11-04)

Judge slams spy agency for keeping data illegally
Federal Court Justice Simon Noel sharply criticized the domestic spy agency, CSIS, for illegally keeping electronic data on people even though they posed no security threat. Noel said the intelligence service was not truthful with judges who were called on to authorize warrants for its data-collection program. (…) This is the second time in three years that a judge of the Federal Court has ruled that CSIS did not meet its "duty of candour" in applying for wiretaps. So far, no sanctions have been applied. In a similar ruling in 2013, Justice Richard Mosley wondered whether it would take a contempt of court proceeding to ensure that such decisions are taken seriously. (…) At a news conference, the director of CSIS, Michel Coulombe said the agency had stopped accessing and analysing the data, but did not say they would be destroyed. **Public Security Minister Ralph Goodale** said the court's ruling would not be appealed. He said he would discuss it with the security agency's management and that Canadians need to have confidence that all departments and agencies of the government are safeguarding rights and freedoms. Radio-Canada International (2016-11-04)

Goodale dit que la surveillance du SCRS fonctionne bien et fonctionnera mieux

Dans un jugement rendu public jeudi, la Cour fédérale a statué que le Service canadien du renseignement de sécurité (SCRS) avait manqué à son devoir d'informer le tribunal de ce programme de collecte de données, qui durait depuis 10 ans. Le juge Simon Noël estime que le SCRS aurait dû communiquer ses activités à la cour puisqu'elles ne concernaient pas directement la sécurité nationale. Le **ministre Goodale**, responsable de la Sécurité publique et de la Protection civile, a dit vendredi que le rapport du CSARS et l'intervention de la Cour fédérale sont la preuve que le SCRS est gardé à l'oeil. **M. Goodale** a ajouté que son projet de loi C-22 qui crée un comité de députés et de sénateurs pour surveiller les agences comme le SCRS et la GRC renforcera le système. Ce comité aura accès aux opérations en cours de ces agences alors que le CSARS ne peut que revenir sur le passé du SCRS. Par ailleurs, le **ministre Goodale** a dit avoir rappelé au SCRS son « devoir de franchise » avec les tribunaux. **M. Goodale** n'a pu dire combien de Canadiens ont vu des informations les concernant être stockées pendant 10 ans par le SCRS, mais c'est un nombre « excessif », selon lui. Presse canadienne (Radio-Canada) (2016-11-04)

Le fédéral dit avoir les espions à l'oeil
Ottawa promet d'avoir les espions canadiens à l'oeil à la suite des révélations découlant d'un jugement de la Cour fédérale rendu public jeudi. En point de presse vendredi matin au Parlement, le **ministre de la Sécurité publique Ralph Goodale** a martelé que le Service canadien du renseignement de sécurité (SCRS) a la responsabilité de respecter la loi. «***Cela est absolument fondamental pour garantir la confiance des Canadiens»,*** a-t-il déclaré. Interrogé à savoir si des fonctionnaires seront congédiés, **M. Goodale** s'est toutefois gardé de répondre directement à la question. ***«Je discuterai avec les gestionnaires du SCRS pour savoir comment ils comptent réagir au jugement en consultation avec le ministère de la Justice»***, a-t-il offert. (…) **Ralph Goodale** dit avoir été mis au courant de «l'ampleur du problème il y a quelques semaines», après avoir reçu une version préliminaire du jugement. Le **ministre Goodale** a voulu se faire rassurant, en rappelant que le Parlement souhaite bientôt mettre sur pied un comité pour surveiller les agences de sécurité. Ce comité parlementaire doit toutefois avoir plus de dents que ne le prévoient actuellement les libéraux de Justin Trudeau, a signalé le NPD. «Je pense que les Canadiens devraient être inquiets que l'agence de sécurité nationale ait menti devant la cour. C'est extrêmement préoccupant», a souligné Matthew Dubé. «Quand les agences demandent aux élus d'avoir plus de pouvoirs, le minimum qu'ils doivent faire c'est de gagner la confiance du public, et ils l'ont perdue selon moi avec un tel comportement.» Vendredi, le **ministre Goodale** a confirmé qu'il était ouvert à modifier la loi afin de rendre légal la conservation et l'utilisation des données connexes par le SCRS. TVA Nouvelles (2016-11-04)

Surveillance de journalistes: pas d'assurances sur le passé à Ottawa
Si aucune surveillance de journalistes ne se produit ***«actuellement» au niveau fédéral, le gouvernement Trudeau n'a pas demandé ni obtenu l'assurance de la GRC et du SCRS que les corps policiers fédéraux n'ont pas mis des journalistes sous surveillance au cours des cinq dernières années. «L'enjeu, c'est que ce qui se passe maintenant»,*** a dit le **ministre fédéral de la Sécurité publique Ralph Goodale** en point de presse ce matin à la Chambre des communes. Le gouvernement Trudeau n'a pas l'intention de demander à la Gendarmerie royale du Canada (GRC) et au Service canadien du renseignement de sécurité (SCRS) si des mandats de surveillance ont été émis ou si des journalistes ont été surveillés au cours des cinq dernières années. ***« L'enjeu, c'est que ce qui se passe maintenant, et nous pouvons offrir l'assurance que ce genre d'activités ne se produit pas actuellement. Je n'ai pas connaissance de choses qui se sont produites quand nous ne formions pas le gouvernement du Canada »***, a dit le **ministre Goodale.** Le gouvernement Trudeau a indiqué avoir reçu l'assurance cette semaine qu'aucune journaliste n'est surveillé «actuellement» par les corps policiers fédéraux. En réponse à une question en point de presse ce matin, le **ministre Goodale** a précisé que cette assurance des corps policiers fédéraux comprend seulement la situation actuelle. Au Québec, la Sûreté du Québec a confirmé cette semaine avoir surveillé une demi-douzaine de journalistes au cours des dernières années, certains comme le journaliste Alain Gravel (Radio-Canada) pendant plusieurs années (2008 à 2013 dans son cas). ***«La réponse, autant de la GRC que du SCRS, est que rien de la sorte ne se produit actuellement. L'enjeu au niveau fédéral n'est pas le***

même qu'au Québec, dit le ministre Goodale. [...] C'est la responsabilité du directeur du SCRS de répondre aux questions opérationnelles. Vous allez sur une pente très dangereuse quand vous invitez les politiciens à aller dans ce domaine.» (…) Le **ministre Goodale** qualifie les ***«révélations au Québec»*** sur la surveillance de journalistes de ***« très inquiétantes »*** et a l'intention de ***«réviser [les] balises fédérales en place pour s'assurer qu'elles soient assez fortes et efficaces, et nous sommes plus qu'ouverts à recevoir les représentations et les conseils du public, des organisations journalistiques et le communauté juridique pour savoir s'il faut, le cas échéant, faire des changements à nos lois.»*** La Presse (2016-11-04)

CSIS law-breaking shows need for stronger parliamentary oversight: NDP
The NDP says revelations that Canada's lead spy agency illegally kept sensitive data for years underscores the need for stronger parliamentary oversight. The New Democrats are pushing for changes to a bill that would create a committee of parliamentarians to keep an eye on the Canadian Security Intelligence Service and other spy services. NDP MP Murray Rankin says the proposed model would allow the government to arbitrarily deny crucial information to the committee. A Federal Court judge says CSIS violated the law by keeping potentially revealing electronic data about people who posed no security threat over a 10-year period. Canadian Press (Chronicle-Herald, Metro News, 680 News, Global News, Huffington Post) (2016-11-04)

What Snowden Had to Say at the McGill Videoconference
Thousands of people lined up on the McGill campus Wednesday night waiting hours for a chance to be part of a videoconference with Edward Snowden. (…) We can't trust intelligence officials to respect the spirit of the law; in fact, we can't even trust them to respect the law itself, argued Snowden. Intelligence gathering programs have broken the law more than once, he reminded, often without consequences. "What we can do," he continued, "is put processes in place to ensure that we don't have to." He believes the key of these processes is an independent judicial authority able to oversee intelligence gathering operations and prosecute them when needed. "Canada actually has the weakest intelligence oversight out of any major western country." "Now they're not the most aggressive," he conceded, "they don't have the largest scale, but.... no one is really watching." The powers of the Canadian Security Intelligence Agency (CSIS) have drastically increased in the last 15 years. Law C-51, in particular, allows them to decide under any motive – however far-fetched – who constitutes a threat to national security and can thus be spied on. "The current Prime Minister did campaign to reform [C-51] and has failed to do so," reminded Snowden. The resources to oversee the CSIS, meanwhile, have decreased. The office of the Inspector General, which used to be a major part of it, was simply cut by Stephen Harper. This left the Security Intelligence Review Committee (SIRC) as the sole entity reporting to parliament on intelligence agencies. Its members are politically appointed. CSIS is not the only intelligence gathering agency. The Canadian Border Security Agency, Global Affairs Canada and the National Defense Department all have the power to infringe on the rights of people, including the right to privacy, in certain circumstances and there is no credible authority overseeing them. Retired Deputy Director of Foreign Intelligence Kurt Jensen pleaded for changing this situation in an article published last January. "Remember the old adage of who will watch the watchers? In Canada the answer is no one," he wrote. Forget the Box (2016-11-04)

Three New Scandals Show How Pervasive and Dangerous Mass Surveillance is in the West, Vindicating Snowden
An opinion piece state, 'While most eyes are focused on the presidential race between Hillary Clinton and Donald Trump, three major events prove how widespread, and dangerous, mass surveillance has become in the west. Standing alone, each event highlights exactly the severe threats which motivated Edward Snowden to blow his whistle; taken together, they constitute full-scale vindication of everything he's done. Earlier this month, a special British court that rules on secret spying activities issued an emphatic denunciation of the nation's domestic mass surveillance programs. The court found that "British security agencies have secretly and unlawfully collected massive volumes of confidential personal data, including financial

information, on citizens for more than a decade." (…) On Thursday, an even more scathing condemnation of mass surveillance was issued by the Federal Court of Canada. The ruling "faulted Canada's domestic spy agency for unlawfully retaining data and for not being truthful with judges who authorize its intelligence programs." Most remarkable was that these domestic, mass surveillance activities were not only illegal, but completely unknown to virtually the entire population in Canadian democracy, even though their scope has indescribable implications for core liberties: "the centre in question appears to be the Canadian Security Intelligence Service's equivalent of a crystal ball – a place where intelligence analysts attempt to deduce future threats by examining, and re-examining, volumes of data."" The Intercept (2016-11-04)

CSIS collected data on citizens for past 10 years
Canada's spies for almost a decade illegally kept and analyzed data on people who posed no threat to national security, a federal court judge has ruled. In a scathing ruling, Justice Simon Noël said the Canadian Security Intelligence Service had illegally retained an unknown amount of data on "third party" and "non-threat" individuals since 2006. CSIS fed that data into a powerful database that allowed the agency to draw out "specific, intimate insights into the lifestyle and personal choices of individuals," read the heavily censored court ruling, circulated to journalists on Thursday. (…) The revelations prompted an unprecedented snap press conference by CSIS director Michel Coulombe. Coulombe told journalists the agency believed its actions were legal, from 2006 until October's ruling, but accepts Noël's findings. Coulombe could not, however, explain why CSIS believed it needed to inform the court of ODAC's existence in 2006, but failed to do so for almost 10 years. "I'll be honest, we went through our records and we really can't find a good explanation of why the court was not informed," Coulombe told reporters Thursday evening. Coulombe was clear that CSIS believed the program was useful and effective, and said he would like to keep it in operation. "That is something I will discuss with officials, (**Public Safety Minister Ralph Goodale**) and it is a public policy decision that the government and parliamentarians will have to make," the director said. In a statement, **Goodale** said the government will not appeal Noël's decision. But the minister did leave open the possibility of changing the CSIS Act to allow for such techniques in the future. **Goodale** noted the court ruling found the legislation governing CSIS was beginning to ***"show its age"*** after 30 years, and threats and investigative techniques have changed over that time. **Goodale** said he would be discussing CSIS's failure to tell the court the full truth, however, with the agency's senior management. ***"In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the (government) are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms,"*** **Goodale** wrote. Toronto Star, A1 (2016-11-04)

Le SCRS a conservé illégalement des données personnelles
L'agence d'espionnage du Canada a agi dans l'illégalité en conservant des données personnelles pendant 10 ans, a tranché la Cour fédérale. Dans un jugement rendu public hier, le magistrat Simon Noël a statué que le Service canadien du renseignement de sécurité (SCRS) avait manqué à son devoir d'informer le tribunal de son programme de collecte de données, qui opérait en vertu d'ordonnances judiciaires. Le juge Noël estime que le SCRS aurait dû communiquer ses activités à la Cour puisqu'elles ne concernaient pas directement la sécurité nationale. Colliger les données permet à l'agence d'identifier des habitudes de déplacements, de communication, de comportements et de liens qui lui seraient sinon inaccessibles, a indiqué hier le directeur du SCRS Michel Coulombe, qui dit « regretter que le SCRS a manqué à son obligation de franchise envers la Cour ». Rappelant « l'efficacité de l'analytique de données », le SCRS a l'intention de poursuivre ce programme dans le respect de la loi. Le **ministre de la Sécurité publique, Ralph Goodale**, a indiqué **« accueillir positivement »** la décision rendue dans cette affaire, et a souligné que le gouvernement n'interjetterait pas appel. Le **ministre Goodale** a dit prendre **« très au sérieux »** les conclusions du juge et a assuré qu'il ferait le suivi avec le SCRS. ***« Lorsqu'il est question de la sécurité et du renseignement, les Canadiens doivent avoir la certitude que tous les ministères et organismes du gouvernement du Canada réussissent efficacement à assurer la sécurité des Canadiens, et ce, en accordant autant d'importance***

au respect de nos droits et libertés », a indiqué le **ministre Goodale** dans un communiqué. La Presse, 10; Journal de Montréal (2016-11-04)

CSIS data program illegal, court rules
The Federal Court of Canada has faulted Canada's domestic spy agency for unlawfully retaining data and for not being truthful with judges who authorize its intelligence programs. Separately, the court also revealed that the spy agency no longer needs warrants to collect Canadians' tax records. All this has been exposed in a rare ruling about the growing scope of Canadian intelligence collection disclosed by the court on Thursday. At issue is how the federal domestic spy service has been pushing past its legal boundaries in the name of collecting data, in hopes of rounding out the holdings of a little-known Canadian intelligence facility dubbed the "operational data analysis centre." Many corporations and government agencies are now gravitating toward so-called big data computer analytics that can predict patterns of future behaviour based upon records about what has happened in the past. Spy agencies are no different, and the centre in question appears to be the Canadian Security Intelligence Service's equivalent of a crystal ball - a place where intelligence analysts attempt to deduce future threats by examining, and re-examining, volumes of data. (…) Following the ruling, **Public Safety Minister Ralph Goodale** released a statement that was equal parts stern and upbeat. ***"I will be pursuing this criticism with the executive management of the service,"*** he said. But **Mr. Goodale** added that the judges mentioned that CSIS's data-analytics program "***has yielded some useful intelligence results."*** He suggested the program could be bolstered with a few legislative changes. ***"The CSIS Act is now more than 30 years old and showing its age as global affairs, threat profiles, technology and public expectations have rapidly evolved,"*** **Mr. Goodale** wrote. Globe and Mail, A15 (2016-11-04)

CSIS broke law by keeping sensitive metadata
A Federal Court judge says Canada's spy agency illegally kept potentially revealing electronic data about people who posed no security threat over a 10-year period. In a hard-hitting ruling made public Thursday, Justice Simon Noel said the Canadian Security Intelligence Service breached its duty to inform the court of its data-collection program, since the information was gathered using judicial warrants. CSIS should not have held on to the information since it was not directly related to threats to the security of Canada, the ruling said. "Ultimately, the rule of law must prevail," Noel wrote, adding, "without it, the actions of people and institutions cannot be trusted to accurately reflect the purpose they were entrusted to fulfil." **Public Safety Minister Ralph Goodale** welcomed the decision and said the government would not appeal. CSIS crunched the data beginning in 2006 using a powerful program known as the Operational Data Analysis Centre to produce intelligence that can reveal specific, intimate details about people the spy service monitors, the judge said. The improperly retained material was metadata - information associated with a communication, such as a telephone number or email address, but not the message itself. Canadian Press (Hamilton Spectator, A8, Calgary Sun, Edmonton Sun, Kingston Whig-Standard, Ottawa Sun, London Free Press, Toronto Sun, Winnipeg Sun, Waterloo Region Record, Fort McMurray Today); Presse canadienne (Le Droit) (2016-11-04); Canadian Press (Mississaugau.com, The Record, Times Colonist, Toronto Star, CBC News) (2016-11-03)

Secret CSIS unit illegally kept data, court rules
A previously unknown unit of Canada's intelligence service has been illegally keeping data unrelated to national security threats, the Federal Court disclosed Thursday. In a hard-hitting ruling that was partly blacked out, Justice Simon Noel rebuked the Canadian Security Intelligence Service for not telling the court about a secret metadata program launched in 2006. The Operational Data Analysis Centre was unknown even to the judges who had been issuing the warrants to collect the information it mined, according to Noel's ruling. (…) **Public Safety Minister Ralph Goodale** said the government would not appeal the decision and would ask the Security Intelligence Review Committee to ***"monitor the situation carefully to ensure compliance."*** **Goodale** said he intended to speak to the CSIS executive about Noel's findings and had taken note of the court's observation that the CSIS Act was ***"now more than 30 years old and showing its age."*** The ruling touched on an issue many governments are struggling to

address: amid fears over terrorism, how far can they can intrude into the lives of citizens in the name of national security? Postmedia Network (National Post, A1/Front (Edmonton Journal, Calgary Herald, StarPhoenix, Windsor Star, Leader-Post, Ottawa Citizen, Montreal Gazette, London Free Press) (2016-11-04); National Post (2016-11-03)

Canadian spy agency put on notice
A Canadian federal court has dealt the country's spy agency a major blow by declaring it illegally kept data collected during investigations over the past decade. It has also threatened sanctions if it happens again. Although judges have previously criticised the Canadian Security Intelligence Service (CSIS) for a lack of openness, the ruling is being seen as particularly uncompromising. Federal Court Judge Simon Noel said CSIS secretly set up a special data analysis centre in 2006 to help track potential terrorism suspects. However, he said it stored and retained electronic information from people not linked to particular threats, which it was not permitted to do."CSIS has a limited mandate which does not permit the retention of associated data ... as it has done so since 2006. Therefore this retention of associated data is illegal," Judge Noel said in the ruling. (...) "The fact that CSIS could go 10 years retaining large quantities of our sensitive private information, yet we're only finding out about this now, and only as a result of a court judgement, is deeply concerning," said David Christopher of OpenMedia, an advocacy group. (...) **Federal Public Safety Minister Ralph Goodale**, who has overall responsibility for law enforcement agencies, welcomed the ruling and said the government would not appeal it. ***"I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service," Goodale*** said in a statement. Radio on New Zealand (2016-11-04)

Online national security quiz is not exactly neutral
An opinion piece state, "Making sense of the federal government's online national security quiz is not easy. The Liberal government, which during last year's election campaign had promised to scrap significant portions of the anti-terror law known as Bill C-51, now says it wants to see what Canadians have to say before acting. To that end, according to a spokesperson for **Public Safety Minister Ralph Goodale**, the government has held 27 face-to-face consultation sessions. More are in the offing. But the jewel in the crown for Justin Trudeau's very modern government is an online questionnaire. Here, the Liberal government has received 9,500 individual responses and 9,300 bulk submissions. I'm surprised it got that many. Canada's anti-terror legislation is both complicated and technical. What, for instance, is a lay person supposed to make of this question in the online quiz: "Do the current Section 38 procedures of the Canada Evidence Act properly balance fairness with security in legal proceedings?" Mind you, the online consultation does include a so-called green paper written in passably clear English that purports to describe how the current system works. But like **Goodale** himself, this green paper exudes a soothing, untroubled tone suggesting that - in the end - the law as written is pretty sensible and, at most, needs only a few tweaks." Toronto Star, A13 (2016-11-04)

Canadian Court Rules Spy Agency Illegally Kept Data Unrelated to Threats
A Canadian court issued a strong rebuke to the country's intelligence agency in a ruling released Thursday, saying the Canadian Security Intelligence Service broke the law by holding on to data that wasn't directly related to security threats. Federal Court Justice Simon Noel said CSIS overstepped its mandate when it began retaining and analyzing metadata that wasn't relevant to investigations or prosecution, or to national defense or international affairs. Metadata can include information such as a telephone number or email address but doesn't include the content of a communication. The data was sent to a CSIS program called the Operational Data Analysis Centre for processing, which the court judgment said has the ability to produce "specific, intimate details" on the life and environment of individuals under investigation. The program was launched in 2006, according to the judgment. The issue of data collection has come under greater scrutiny since former U.S. National Security Agency contractor Edward Snowden revealed that agency was conducting surveillance of U.S. citizens. (...) **Canada Public Safety Minister Ralph Goodale** said in a statement that the government doesn't intend to appeal the court's decision. Wall Street Journal (2016-11-03)

Judge raps Canada spy agency for data collection abuse
The head of the Canadian Security Intelligence Service said he agreed with a court ruling that the spy agency had held onto sensitive data beyond the time frame allowed by court warrants. CSIS director Michel Coulombe ordered all access to information dating back as far as 2006 to be denied while the agency assesses the legal impact of the decision and determines how best to move forward. "I regret that we did not meet our duty of candor to the court and I commit to continuing my efforts with the deputy minister of justice to address this concern," CSIS director Coulombe told a press conference. "All associated data collected under warrant was done so legally. The court's key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected," Coulombe said. (...) **Public Safety Minister Ralph Goodale**, meanwhile, welcomed the ruling, saying in a statement that ***"the court's insight and guidance are timely, coming in the midst of the public consultations we now have underway about Canada's national security framework."*** AFP (Yahoo! News) (2016-11-03)

Federal court ruling deems CSIS data mining actions unacceptable
The Federal Court of Canada has handed down a ruling stating that CSIS (Canadian Security Intelligence Service) illegally stored data for over 10 years. Justice Simon Noel reportedly ruled Thursday that, since the information was collected using judicial warrants, the federal agency breached its duty to inform the court of its mechanisms. The *CBC* reports that since the information was not collected to national security threats against Canada, the data should not have been retained by CSIS. CSIS published an statement which conveys that the agency accepts the decision of the court and will take steps to respond. "The Federal Court has recently ruled on the retention of associated data linked to third party information. CSIS fully accepts the Court's decision, and has taken immediate actions to respond. Given the Court's decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward," read the letter. When asked about whether Canadians would be able to rebuild their trust in the agency, chief general counsel for Justice Canada Robert Frater told the CBC that CSIS now understands its limits. Mobile Syrup (2016-11-03)

Court says Canada spy agency illegally kept data
A Canadian court ruled Thursday that Canada's spy agency illegally kept phone numbers and email addresses of people they were not directly investigating over a 10-year period and wasn't forthright with judges who authorized the intelligence gathering. Federal Court Justice Simon Noel said the Canadian Security Intelligence Service should not have kept the information since it was not directly related to threats to Canada's security. The data involves the phone numbers, email address or IP addresses of family members or friends of those the spy agency investigates. The spy agency called it "associated data." CSIS said it used metadata — information associated with a communication, such as a telephone number or email address — but not the message itself. It said the program has been in place since 2006. Spy Service director Michel Coulombe said they have halted logging, storing, and analyzing the data in question and said he "deeply" regretted the judge's findings about breach of "duty of candor." Coulombe stressed all data collection was done under warrant. He noted the issue is the retention of non-threat related data. **Canadian Public Safety Minster Ralph Goodale said he** takes it seriously the spy agency was not forthright with the courts and said he would talk to senior executives of the spy agency. **Goodale noted** the laws that govern the spy agency are 30 years old and need to be updated to reflect new technologies. ***"Justice Noel did not dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could not find existing legislative authority permitting its retention and use," Goodale said*** in a statement. News of the spy agency program comes as the provincial Quebec government announced they are calling a public inquiry into police surveillance of journalists amid revelations various forces in the province monitored reporters' phones. The province's two largest police forces said earlier this week that they had monitored the phones of six prominent journalists in 2013. Associated Press (Daily Mail UK) (2016-11-03)

Canada court deals blow to spy agency, says it kept data illegally
A court dealt Canada's spy agency a blow on Thursday, declaring it had illegally kept data collected during investigations over the past decade and threatening sanctions if the issue occurred again. Although judges have previously criticized the Canadian Security Intelligence Service, or CSIS, for a lack of openness about its operations, the ruling was particularly uncompromising... **Federal Public Safety Minister Ralph Goodale**, **who** has overall responsibility for law enforcement agencies, **welcomed** the ruling and said the government would not appeal it. ***"I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service," Goodale said*** in a statement. Most Canadian security agencies have small individual review bodies, which OpenMedia and others complain are impotent and can only look at old cases. Oversight is more robust in other nations such as Britain and the United States, where special legislative committees monitor the work of security and intelligence agencies. **Goodale**, acting amid global concerns about the reach of security agencies, promised in June to create a similar oversight committee as part of a comprehensive probe into how national security is handled. A scandal erupted this week in the province of Quebec when it emerged that police had secretly tracked phone calls received and made by six reporters. Reuters (2016-11-03)

Les espions canadiens ont outrepassé leur mandat
Le service d'espionnage canadien a outrepassé sa mission en conservant illégalement des informations sensibles recueillies en vertu de mandats, a tranché la Cour fédérale dans un jugement rendu public, jeudi. En point de presse, le patron du Service canadien du renseignement de sécurité (SCRS) a dit prendre acte du verdict. «Le SCRS accepte la décision de la cour et a pris des mesures immédiates pour y répondre», a-t-il déclaré. Je regrette profondément les graves préoccupations de la cour à l'égard de notre manquement quant à l'obligation de franchise.» Durant plusieurs années, le SCRS a caché à la Cour fédérale - qui est chargée de lui délivrer des mandats - l'existence d'un programme de récolte de métadonnées. Cela constitue, pour la cour, un manquement à l'obligation de franchise dont le SCRS doit faire preuve envers le tribunal. Agence QMI (Journal de Québec, Journal de Montréal) ; Vice News; Motherboard; Agence France-Presse (L'Orient le Jour) (2016-11-03)

Broadcast Media / Médias télédiffusés

Yesterday's ruling and subsequent reaction garnered significant media coverage on evening political shows, national news programs and led this morning's headlines.

In a panel discussion on *CBC News' Power & Politics*, former Public Safety Minister Stockwell Day was questioned on his knowledge of the service's data retention practices that began in 2006 while he was minister. This question came in follow up to CSIS Director Michel Coulombe's statement during the technical briefing that in 2006 the service wrote to the minister at the time explaining the Operational Data Analysis Centre program and that his successors were also aware of it.

CTV News provided coverage of **Public Safety Minister Ralph Goodale's** press conference in response to a Federal Court decision on CSIS data retention practices. Rough Transcript (2016-11-04)

CTV News provided coverage of the NDP reaction to the Federal Court ruling on CSIS data storage. Rough Transcript (2016-11-04)

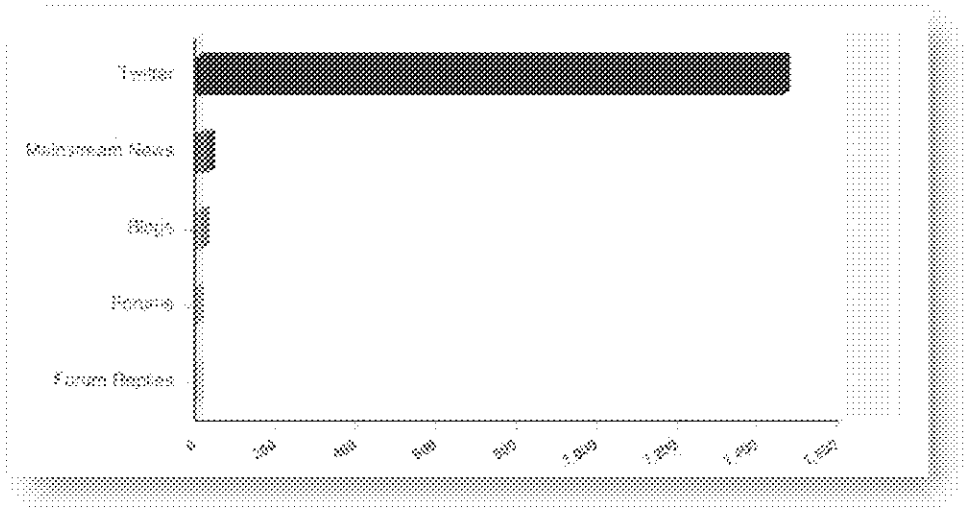
CBC News Network's Power & Politics discussed **Public Safety Minister Ralph Goodale's** response to the Federal Court's ruling regarding CSIS' retention of metadata. Rough Transcript (2016-11-03)

CBC News Network's Power & Politics interviewed Radio-Canada journalist, Marie-Maude Denis, regarding Sûreté Du Québec spying on her. CSIS's retention of metadata was also discussed during this segment Rough Transcript (2016-11-03)

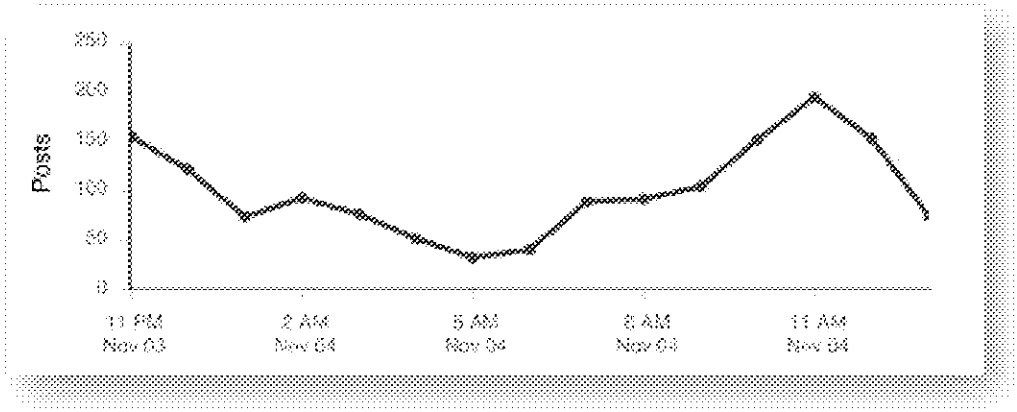
CBC News Network's Power & Politics held a panel discussion with former Public Safety Minister Stockwell Day regarding today's Federal Court's ruling on CSIS' retention of metadata. Rough Transcript (2016-11-03)

Social Media / Médias sociaux

Social media coverage regarding the ruling was extensive over the past 24 hours. There were a total of 1508 social media posts, with the vast majority on Twitter.

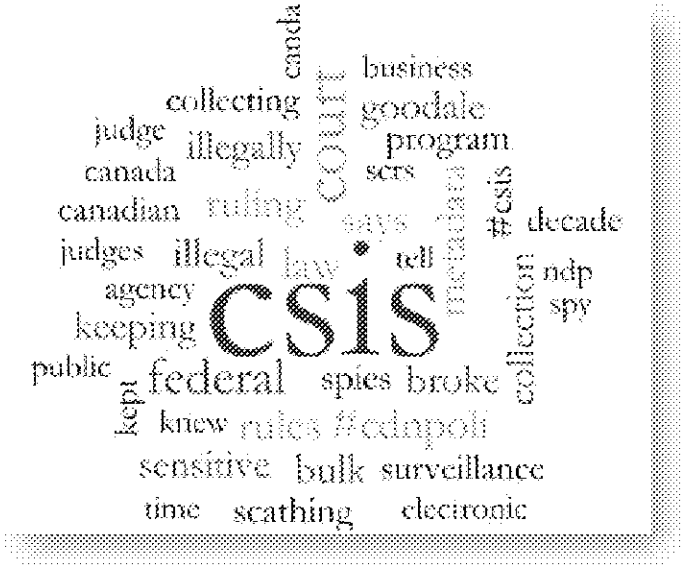


Social media coverage was consistent last night and throughout the day today, with noticeable spikes at 10:00 ET, coinciding with NDP Justice Critic Murray Rankin's press conference, and 11:00ET, coinciding with Public Safety Minister Ralph Goodale's media availability that numerous reporters live-tweeted.



Several social media users and journalists argued that CSIS cannot be trusted with the expanded powers afforded under bill C-51 and that an oversight committee is not a sufficient safeguard due to partisan control. Some posts accused Minister Goodale of defending CSIS' data retention practices under the guise of national security and demanded consequences for the government's actions, with many users calling for responsible parties to be fired.

See below for a word cloud highlighting the language used in connection with the ruling.



Tweets of note:

CTV News
UPDATED: Goodale says CSIS 'taking steps' to comply after court rules it broke law http://ow.ly/PbY7305Rkod #cdnpoli https://t.co/jqEsiMtDtR

CTV News
NDP calls for 'new oversight' after federal court rules CSIS broke law http://ow.ly/6Pkz305Rdjd #cdnpoli

Global News

Government not able to answer how many Canadians had data illegally collected by CSIS over the last decade #cdnpoli

Global News
WATCH: NDP blasts "gross abuse of power by Canada's spy agency" following judge's ruling on CSIS

Global News
Ralph Goodale "welcomes" court ruling on illegal data collection by CSIS, says agency essential to national security

CBC Politics
CSIS metadata breach: Ralph Goodale 'pursuing criticism' with spy agency management http://ift.tt/2fCGxGR #hw #c…

CBC News Alerts
Goodale also reacted to court ruling on CSIS illegally storing metadata for a decade. Said CSIS must be forthcoming and candid with court.

La Presse
Goodale dit que la surveillance du SCRS fonctionne bien et fonctionnera mieux http://bit.ly/2fjQfu1

CPAC
#QP: @MurrayRankin we need real parl. oversight for @CSIS. @RalphGoodale: #C22 provides authority to examine current operations #cdnpoli

CPAC
#QP: @MurrayRankin: Why weren't Cdns told immediately abt @CSIS spying? @RalphGoodale report filed Jan 28, that was when public was alerted

CPAC
Moments ago: Public Safety Min @RalphGoodale on ruling re: CSIS data collection: SIRC will supervise compliance; the SIRC process has worked

Matthew Dubé
Le gouvernement libéral doit révéler les détails entourant la décision sur le SCRS

Jim Bronskill
New Democrats call for more CSIS oversight following revelations of law-breaking http://www.mississauga.com/news... #cdnpoli #hw

Colin Freeze
Para 262 language hints CSIS legally leveraging CSE will get harder? "Volume of incidentally collected information..." ATTN:@NewmanRobinson

Colin Freeze
Continuing, Justice Noel does a very good job of going back to CSIS's foundational debates to remind the agency what it is and isn't.

Philippe Lagassé
Key problem for intra-executive or parliamentary oversight: how to you know what you're not being told?

Catherine Cullen
Timely: National security was perceived as a Liberal strength in the government's own poll of Canadians. More here: cbc.ca/1.3835923

Catherine Cullen
Goodale says he will pursue criticisms of the court with CSIS management. Says a strong and timely remedial plan is needed. #hw

Shirlee Engel
Goodale says CSIS Director knows very well what his expectations are going forward #cdnpoli

Shirlee Engel
Goodale says CSIS taking immediate steps to address court decision, blocked associated data while consider next step #cdnpoli

Amanda Connolly
CSIS illegal data storage 'gross abuse of power': NDP https://t.co/n0nsbX8bX1

Alison Crawford
PS Minister Goodale: the director (CSIS) understands very clearly that CSIS must be forthcoming & candid with the court and that will happen

Laura Stone
Goodale doesn't answer directly if anyone will be fired or if there will be an inquiry. Repeatedly says decision will be followed

Laura Stone
Should CSIS have access to this info? Goodale says he wants to hear arguments on all sides

Laura Stone
Was told CSIS was responding to fed court. Says he found out full scope of judgment a couple weeks ago and informed SIRC of issue

Laura Stone
CSIS and all security agencies need to comply w law, Goodale says. Judge made clear what law is

Laura Stone
Goodale says CSIS told him it's taking immediate steps to address court's decision. Has asked SIRC to monitor #cdnpoli

Chris Hall
How can you ensure Cdns not being spied on by CSIS? Goodale says SIRC blew whistle and will ensure law is complied with by the agency

Chris Hall
Goodale believes proposed Parl oversight of CSIS would plug a hole, correct a defect in Cdn security architecture.

Chris Hall
Goodale asked if anyone will be fired for failing to inform court that data retained... says he will discuss matter with CSIS execs.

Glenn Greenwald
Three new scandals show how pervasive and dangerous mass surveillance is in the west, vindicating Snowden https://t.co/uc954XVPxw

Claire Wahlen
Side note: in all this #C22, security oversight hooplah, there's too little talk about too much info/data being unnecessarily classified

Claire Wahlen
Has anyone asked @RalphGoodale whether or not people can inquire whether or not their personal info was caught up in the #csis net?

Claire Wahlen
Good Q from @alexboutilier: Did this come about from a ministerial directive? Goodale: We will never know. #csis

Tonda MacCharles
I asked #CSIS in Oct what bulk data it collected & I was told maps, foreign telephone directories & airport codes. thestar.com/news/canada/20…

Alex Boutilier

@brnfprd @ex3Tory Technically *no* oversight besides the minister, but worth noting CSIS's review body found and flagged the issue.

Justin Ling
Goodale is spinning this as a positive. It took a decade — a *decade* — for this to come to light. His argument? The system works!

Justin Ling
How many Canadians had their data captured under this program? Goodale cites operational security and won't say.

Justin Ling
Goodale says he only because aware of this massive CSIS spying campaign in early October when this judgement came out. Wow.

Justin Ling
That is not even remotely what the court told CSIS to do. They did not say: "hang on to the illegally-retained data for a bit."

Justin Ling
“This is what they call data mining. This is data mining," says Rankin. To do so, Canada needs a real committee of Parliamentarians.

Justin Ling
Murray takes aim at Trudeau's proposed intel oversight committee: he notes the high level of control that cabinet will have over it.

Justin Ling
"It's a massive breach of privacy for the Canadians involved," says NDP Justice Critic Murray Rankin on yesterday's CSIS ruling.

Michael Geist
Illegal metadata retention & dismissing oversight: how can Canadians trust their surveillance agencies? michaelgeist.ca/2016/11/lost-c…

Michael Geist
Lost Confidence: Why Trust in Canadian Surveillance Agencies Has Been Irreparably Harmed michaelgeist.ca/2016/11/lost-c…

Michael Geist
One week: police message 1000s using old geo data, journalist surveillance, court rules CSIS broke law michaelgeist.ca/2016/11/lost-c…

Christopher Parsons
And the idea that creating a new executive body, composed of parliamentarians, as a solution is frankly laughable.

Christopher Parsons
At some point, the myth that Ministerial Accountability can keep Canadian intelligence and security agencies in check must be set aside

Christopher Parsons
It’s useful to remember that CSIS has, in recent memory, conducted surveillance of provincial cabinet ministers https://t.co/wPhAKtnabp

Cathy Senay
Semaine axée #protection vie privée ,le #NPD croit que les Canadiens doivent être inquiets décision Cour #fédérale blâmant SCRS #POLCAN

Stephanie Carvin
People really underestimate how hard the Federal Court pushes back on national security agencies. (As they should.)

Ann Cavoukian
Illegal collection and retention of metadata by CSIS, for a decade, without any authorization. theglobeandmail.com/news/national/...

Kevin O'Brien
@StewartBellNP ICYMI, CSIS 2007-2008 Public Report (p19) notes existence & function of ODAC, altho not prog breadth publications.gc.ca/site/archivee-...

Lee Mathers
This brings up a good topic "Data Retention policies" for Apps and Social Networking sites: As far as I am aware the… https://t.co/M1uzH8eUbp

Murray Rankin
Security expert @cforcese recommends deleting whole sections of #C22 to remove the "triple lock" on oversight committee's access to info.

CSIS Canada
Read statement from CSIS Director regarding decision of the Federal Court https://csis.gc.ca/nwsrm/index-en.php ...

SCRS Canada
Lisez la déclaration du directeur du SCRS au sujet de la décision rendue par la Cour fédérale https://csis.gc.ca/nwsrm/index-fr.php ...

NEWS1130
Public Safety Minister Ralph Goodale says the government won't appeal a Federal Court ruling that Canada's spy agency broke the law.

Colin Freeze
Public Safety Minister @RalphGoodale --now consulting about CSIS C-51 -- says scathing ruling shows CSIS laws outdated. Time for new laws!

Matt Galloway
CSIS has been collecting & retaining electronic data on Canadians for 10 years. That's against the law. Wild story: https://t.co/9DRtnWViEB

CBC News
CSIS broke law by keeping sensitive metadata, Federal Court rules http://www.cbc.ca/1.3835472CSIS broke law by keeping sensitive metadata, Federal Court rules https://t.co/OtaWM6S9Ea

TimesTranscript
CSIS broke law by keeping sensitive metadata, Federal Court rules ow.ly/ykQS305PVzP @TJProvincial @DailyGleaner pic.twitter.com/JmZtQVkUZV

NEWS1130
CSIS broke law by keeping sensitive metadata, Federal Court rules bit.ly/2ejAmBy pic.twitter.com/TYG9MDrERk

Stewart Bell
Retention of data by CSIS "falls outside" its legislative jurisdiction, court says. http://cas-cdc-www02.cas-satj.gc.ca/

Stewart Bell
CSIS breached "duty of candour" by not disclosing Operational Data Analysis Centre launched in 2006, says court. http://cas-cdc-www02.cas-satj.gc.ca/

Stewart Bell
Important Federal Court decision on CSIS Operation Data Analysis Centre. http://cas-cdc-www02.cas-satj.gc.ca/

StewartBellNP
2/More on secret CSIS data program.

Stewart Bell
3/Court's description of CSIS data program.

Stewart Bell
4/CSIS retained metadata "indefinitely" even if not threat related, court says.

Stewart Bell
5/Federal Court's brutal judgment of the "illegal" retention of metadata by CSIS.

Stewart Bell
CSIS director responds to Federal Court ruling on illegal metadata program http://www.newswire.ca/

Michelle Lamarche
Le directeur Coulombe SCRS dit que des mesures ont été prises pour se conformer à la décision de la cour #tvanouvelles

Michelle Lamarche
Cour fédérale blâme le SCRS qui a manqué à son devoir de franchise. #polcan #tvanouvelles

Fab de Pierrebourg
Le #SCRS blâmé par la Cour fédérale pour avoir illégalement conservé des données personnelles. https://t.co/gu5OiolOG8

Christopher Parsons
People point at the US, and how NSA et al have systematically mislead the courts. This decision further reveals that CSIS does same, here

Globe and Mail
RT @Colinfreeze: Faulting #cdnpoli spies for unlawfully amassing data, court reveals #CSIS now gets tax records warrantlessly #C51 https://…

National Post
Judge blasts CSIS for not revealing secret program that has been illegally keeping metadata since 2006 natpo.st/2fmEp11 pic.twitter.com/6vSXf5mH2A

BCCLA
In scathing ruling, Federal Court says CSIS bulk data collection illegal bit.ly/2fhcErM via @globeandmail #C51 #cdnpoli

Kady O'Malley
Well, it's nice that CSIS is willing to accept the decision of the federal court on its various and sundry breaches of candour and the law.

Tonda MacCharles
CSIS program illegally spied for a decade, judge rules. The wrap by @alexboutilier https://www.thestar.com/news/canada/...

Jameel Jaffer
Canadian spies concealed far-reaching surveillance program from court tasked with overseeing them. http://www.theglobeandmail.com/news/national/...

Trevor Timm
In a scathing ruling, a federal court in Canada rules its intel agency's mass data collection program is illegal http://www.theglobeandmail.com/news/national...

Justin Ling
I've covered CSIS and CSE for years, now. This is likely the largest revelation we've ever found out about their intelligence surveillance.

Justin Ling
I'm on a tech briefing about the most recent CSIS spying revelation. This, folks, is a bombshell.

David R Brake
Seems Cdn intelligence agency CSIS is keeping comms metadata after investigations finished http://www.vice.com/en_ca/read/theres-a-secret-c... eek! #privacy

Stephanie Carvin
From last night: my piece on #YourNatlSec written before the CSIS/ODAC hoo-ha. But talks about analytical oversight.

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Federal Court ruling on CSIS retention of metadata / Décision de la cour fédérale sur la conservation des métadonnées

2016-11-03 – 2016-11-04

Table of Contents / Table des matières

Overview / Vue d'ensemble

Online, print, broadcast and social media coverage regarding the Federal Court ruling on CSIS' retention of metadata was heavy over the specified time period of November 3, 2016 – November 4, 2016. The tone of coverage was negative and factual, and was amplified by recent news events concerning police surveillance of journalists in Quebec in the lead up to yesterday's ruling.

The Federal Court ruling also garnered national and international coverage from sources such as Reuters, Wall Street Journal, Associated Press, and Agence France-Presse.

Coverage stemming from Minister Goodale's statement and comments made by the Director of the Canadian Security Intelligence Service at the technical briefing on the evening of November 3, 2016 was picked up by most media outlets.

The tone of social media coverage was negative, with many social media users expressing frustration at the perceived infringement on privacy rights. Social media users also emphasized the magnitude of the report, with many describing the decision as scathing and CSIS as unaccountable. Many privacy rights groups used the recent court decision as leverage for their case against Bill C-51.

Selected Quotes / Citations choisies

Ralph Goodale - Minister of Public Safety and Emergency Preparedness

"Justice Noel did not dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could not find existing legislative authority permitting its retention and use."

"I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service."

"In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the government of Canada are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms."

"The court's insight and guidance are timely, coming in the midst of the public consultations we now have underway about Canada's national security framework."

"The CSIS Act is now more than 30 years old and showing its age as global affairs, threat profiles, technology and public expectations have rapidly evolved."

Michel Coulombe - Director of the Canadian Security Intelligence Service (CSIS)

"I'll be honest, we went through our records and we really can't find a good explanation of why the court was not informed."

"That is something I will discuss with officials, (Public Safety Minister Ralph Goodale) and it is a public policy decision that the government and parliamentarians will have to make."

"I deeply regret the court's serious concerns with respect to meeting our duty of candour, and I commit to continuing my efforts, with the deputy minister of Justice, to address this concern."

Print and Online Media / Médias imprimés et en ligne

CSIS collected data on citizens for past 10 years

Canada's spies for almost a decade illegally kept and analyzed data on people who posed no threat to national security, a federal court judge has ruled. In a scathing ruling, Justice Simon Noël said the Canadian Security Intelligence Service had illegally retained an unknown amount of data on "third party" and "non-threat" individuals since 2006. CSIS fed that data into a powerful database that allowed the agency to draw out "specific, intimate insights into the lifestyle and personal choices of individuals," read the heavily censored court ruling, circulated to journalists on Thursday. (…) The revelations prompted an unprecedented snap press conference by CSIS director Michel Coulombe. Coulombe told journalists the agency believed its actions were legal, from 2006 until October's ruling, but accepts Noël's findings. Coulombe could not, however,

explain why CSIS believed it needed to inform the court of ODAC's existence in 2006, but failed to do so for almost 10 years. "I'll be honest, we went through our records and we really can't find a good explanation of why the court was not informed," Coulombe told reporters Thursday evening. Coulombe was clear that CSIS believed the program was useful and effective, and said he would like to keep it in operation. "That is something I will discuss with officials, (**Public Safety Minister Ralph Goodale**) and it is a public policy decision that the government and parliamentarians will have to make," the director said. In a statement, **Goodale** said the government will not appeal Noël's decision. But the minister did leave open the possibility of changing the CSIS Act to allow for such techniques in the future. **Goodale** noted the court ruling found the legislation governing CSIS was beginning to ***"show its age"*** after 30 years, and threats and investigative techniques have changed over that time. **Goodale** said he would be discussing CSIS's failure to tell the court the full truth, however, with the agency's senior management. ***"In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the (government) are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms," Goodale*** wrote. Toronto Star, A1 (2016-11-04)

Le SCRS a conservé illégalement des données personnelles

L'agence d'espionnage du Canada a agi dans l'illégalité en conservant des données personnelles pendant 10 ans, a tranché la Cour fédérale. Dans un jugement rendu public hier, le magistrat Simon Noël a statué que le Service canadien du renseignement de sécurité (SCRS) avait manqué à son devoir d'informer le tribunal de son programme de collecte de données, qui opérait en vertu d'ordonnances judiciaires. Le juge Noël estime que le SCRS aurait dû communiquer ses activités à la Cour puisqu'elles ne concernaient pas directement la sécurité nationale. Colliger les données permet à l'agence d'identifier des habitudes de déplacements, de communication, de comportements et de liens qui lui seraient sinon inaccessibles, a indiqué hier le directeur du SCRS Michel Coulombe, qui dit « regretter que le SCRS a manqué à son obligation de franchise envers la Cour ». Rappelant « l'efficacité de l'analytique de données », le SCRS a l'intention de poursuivre ce programme dans le respect de la loi. Le **ministre de la Sécurité publique, Ralph Goodale**, a indiqué **« accueillir positivement »** la décision rendue dans cette affaire, et a souligné que le gouvernement n'interjetterait pas appel. Le **ministre Goodale** a dit prendre **« très au sérieux »** les conclusions du juge et a assuré qu'il ferait le suivi avec le SCRS. ***« Lorsqu'il est question de la sécurité et du renseignement, les Canadiens doivent avoir la certitude que tous les ministères et organismes du gouvernement du Canada réussissent efficacement à assurer la sécurité des Canadiens, et ce, en accordant autant d'importance au respect de nos droits et libertés »,*** a indiqué le **ministre Goodale** dans un communiqué. La Presse, 10; Journal de Montréal (2016-11-04)

CSIS data program illegal, court rules

The Federal Court of Canada has faulted Canada's domestic spy agency for unlawfully retaining data and for not being truthful with judges who authorize its intelligence programs. Separately, the court also revealed that the spy agency no longer needs warrants to collect Canadians' tax records. All this has been exposed in a rare ruling about the growing scope of Canadian intelligence collection disclosed by the court on Thursday. At issue is how the federal domestic spy service has been pushing past its legal boundaries in the name of collecting data, in hopes of rounding out the holdings of a little-known Canadian intelligence facility dubbed the "operational data analysis centre." Many corporations and government agencies are now gravitating toward so-called big data computer analytics that can predict patterns of future behaviour based upon records about what has happened in the past. Spy agencies are no different, and the centre in question appears to be the Canadian Security Intelligence Service's equivalent of a crystal ball - a place where intelligence analysts attempt to deduce future threats by examining, and re-examining, volumes of data. (…) Following the ruling, **Public Safety Minister Ralph Goodale** released a statement that was equal parts stern and upbeat. ***"I will be pursuing this criticism with the executive management of the service,"*** he said. But **Mr. Goodale** added that the judges mentioned that CSIS's data-analytics program "***has yielded some useful intelligence results."*** He suggested the program could be bolstered with a few legislative changes. ***"The***

CSIS Act is now more than 30 years old and showing its age as global affairs, threat profiles, technology and public expectations have rapidly evolved," **Mr. Goodale** wrote. Globe and Mail, A15 (2016-11-04); Globe and Mail (2016-11-03)

CSIS broke law by keeping sensitive metadata

A Federal Court judge says Canada's spy agency illegally kept potentially revealing electronic data about people who posed no security threat over a 10-year period. In a hard-hitting ruling made public Thursday, Justice Simon Noel said the Canadian Security Intelligence Service breached its duty to inform the court of its data-collection program, since the information was gathered using judicial warrants. CSIS should not have held on to the information since it was not directly related to threats to the security of Canada, the ruling said. "Ultimately, the rule of law must prevail," Noel wrote, adding, "without it, the actions of people and institutions cannot be trusted to accurately reflect the purpose they were entrusted to fulfil." **Public Safety Minister Ralph Goodale** welcomed the decision and said the government would not appeal. CSIS crunched the data beginning in 2006 using a powerful program known as the Operational Data Analysis Centre to produce intelligence that can reveal specific, intimate details about people the spy service monitors, the judge said. The improperly retained material was metadata - information associated with a communication, such as a telephone number or email address, but not the message itself. Canadian Press (Hamilton Spectator, A8, Calgary Sun, Edmonton Sun, Kingston Whig-Standard, Ottawa Sun, London Free Press, Toronto Sun, Winnipeg Sun, Waterloo Region Record, Fort McMurray Today); Presse canadienne (Le Droit) (2016-11-04); Canadian Press (Mississaugau.com, The Record, Times Colonist, Toronto Star, CBC News) (2016-11-03)

Secret CSIS unit illegally kept data, court rules

A previously unknown unit of Canada's intelligence service has been illegally keeping data unrelated to national security threats, the Federal Court disclosed Thursday. In a hard-hitting ruling that was partly blacked out, Justice Simon Noel rebuked the Canadian Security Intelligence Service for not telling the court about a secret metadata program launched in 2006. The Operational Data Analysis Centre was unknown even to the judges who had been issuing the warrants to collect the information it mined, according to Noel's ruling. (…) **Public Safety Minister Ralph Goodale** said the government would not appeal the decision and would ask the Security Intelligence Review Committee to ***"monitor the situation carefully to ensure compliance."*** **Goodale** said he intended to speak to the CSIS executive about Noel's findings and had taken note of the court's observation that the CSIS Act was ***"now more than 30 years old and showing its age."*** The ruling touched on an issue many governments are struggling to address: amid fears over terrorism, how far can they can intrude into the lives of citizens in the name of national security? Postmedia Network (National Post, A1/Front (Edmonton Journal, Calgary Herald, StarPhoenix, Windsor Star, Leader-Post, Ottawa Citizen, Montreal Gazette, London Free Press) (2016-11-04); National Post (2016-11-03)

Canadian spy agency put on notice

A Canadian federal court has dealt the country's spy agency a major blow by declaring it illegally kept data collected during investigations over the past decade. It has also threatened sanctions if it happens again. Although judges have previously criticised the Canadian Security Intelligence Service (CSIS) for a lack of openness, the ruling is being seen as particularly uncompromising. Federal Court Judge Simon Noel said CSIS secretly set up a special data analysis centre in 2006 to help track potential terrorism suspects. However, he said it stored and retained electronic information from people not linked to particular threats, which it was not permitted to do."CSIS has a limited mandate which does not permit the retention of associated data ... as it has done so since 2006. Therefore this retention of associated data is illegal," Judge Noel said in the ruling. (…) "The fact that CSIS could go 10 years retaining large quantities of our sensitive private information, yet we're only finding out about this now, and only as a result of a court judgement, is deeply concerning," said David Christopher of OpenMedia, an advocacy group. (…) **Federal Public Safety Minister Ralph Goodale**, who has overall responsibility for law enforcement agencies, welcomed the ruling and said the government would not appeal it. ***"I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid***

with the court. I will be pursuing this criticism with the executive management of the Service," **Goodale** said in a statement. Radio on New Zealand (2016-11-04)

Online national security quiz is not exactly neutral
An opinion piece state, "Making sense of the federal government's online national security quiz is not easy. The Liberal government, which during last year's election campaign had promised to scrap significant portions of the anti-terror law known as Bill C-51, now says it wants to see what Canadians have to say before acting. To that end, according to a spokesperson for **Public Safety Minister Ralph Goodale**, the government has held 27 face-to-face consultation sessions. More are in the offing. But the jewel in the crown for Justin Trudeau's very modern government is an online questionnaire. Here, the Liberal government has received 9,500 individual responses and 9,300 bulk submissions. I'm surprised it got that many. Canada's anti-terror legislation is both complicated and technical. What, for instance, is a lay person supposed to make of this question in the online quiz: "Do the current Section 38 procedures of the Canada Evidence Act properly balance fairness with security in legal proceedings?" Mind you, the online consultation does include a so-called green paper written in passably clear English that purports to describe how the current system works. But like **Goodale** himself, this green paper exudes a soothing, untroubled tone suggesting that - in the end - the law as written is pretty sensible and, at most, needs only a few tweaks." Toronto Star, A13 (2016-11-04)

Canadian Court Rules Spy Agency Illegally Kept Data Unrelated to Threats
A Canadian court issued a strong rebuke to the country's intelligence agency in a ruling released Thursday, saying the Canadian Security Intelligence Service broke the law by holding on to data that wasn't directly related to security threats. Federal Court Justice Simon Noel said CSIS overstepped its mandate when it began retaining and analyzing metadata that wasn't relevant to investigations or prosecution, or to national defense or international affairs. Metadata can include information such as a telephone number or email address but doesn't include the content of a communication. The data was sent to a CSIS program called the Operational Data Analysis Centre for processing, which the court judgment said has the ability to produce "specific, intimate details" on the life and environment of individuals under investigation. The program was launched in 2006, according to the judgment. The issue of data collection has come under greater scrutiny since former U.S. National Security Agency contractor Edward Snowden revealed that agency was conducting surveillance of U.S. citizens. (…) **Canada Public Safety Minister Ralph Goodale** said in a statement that the government doesn't intend to appeal the court's decision. Wall Street Journal (2016-11-03)

Judge raps Canada spy agency for data collection abuse
The head of the Canadian Security Intelligence Service said he agreed with a court ruling that the spy agency had held onto sensitive data beyond the time frame allowed by court warrants. CSIS director Michel Coulombe ordered all access to information dating back as far as 2006 to be denied while the agency assesses the legal impact of the decision and determines how best to move forward. "I regret that we did not meet our duty of candor to the court and I commit to continuing my efforts with the deputy minister of justice to address this concern," CSIS director Coulombe told a press conference. "All associated data collected under warrant was done so legally. The court's key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected," Coulombe said. (…) **Public Safety Minister Ralph Goodale**, meanwhile, welcomed the ruling, saying in a statement that ***"the court's insight and guidance are timely, coming in the midst of the public consultations we now have underway about Canada's national security framework."*** AFP (Yahoo! News) (2016-11-03)

Federal court ruling deems CSIS data mining actions unacceptable
The Federal Court of Canada has handed down a ruling stating that CSIS (Canadian Security Intelligence Service) illegally stored data for over 10 years. Justice Simon Noel reportedly ruled Thursday that, since the information was collected using judicial warrants, the federal agency breached its duty to inform the court of its mechanisms. The *CBC* reports that since the

information was not collected to national security threats against Canada, the data should not have been retained by CSIS. CSIS published an statement which conveys that the agency accepts the decision of the court and will take steps to respond. “The Federal Court has recently ruled on the retention of associated data linked to third party information. CSIS fully accepts the Court’s decision, and has taken immediate actions to respond. Given the Court’s decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward,” read the letter. When asked about whether Canadians would be able to rebuild their trust in the agency, chief general counsel for Justice Canada Robert Frater told the CBC that CSIS now understands its limits. Mobile Syrup (2016-11-03)

Court says Canada spy agency illegally kept data
A Canadian court ruled Thursday that Canada's spy agency illegally kept phone numbers and email addresses of people they were not directly investigating over a 10-year period and wasn't forthright with judges who authorized the intelligence gathering. Federal Court Justice Simon Noel said the Canadian Security Intelligence Service should not have kept the information since it was not directly related to threats to Canada's security. The data involves the phone numbers, email address or IP addresses of family members or friends of those the spy agency investigates. The spy agency called it "associated data." CSIS said it used metadata — information associated with a communication, such as a telephone number or email address — but not the message itself. It said the program has been in place since 2006. Spy Service director Michel Coulombe said they have halted logging, storing, and analyzing the data in question and said he "deeply" regretted the judge's findings about breach of "duty of candor." Coulombe stressed all data collection was done under warrant. He noted the issue is the retention of non-threat related data. **Canadian Public Safety Minster Ralph Goodale said he** takes it seriously the spy agency was not forthright with the courts and said he would talk to senior executives of the spy agency. **Goodale noted** the laws that govern the spy agency are 30 years old and need to be updated to reflect new technologies. ***"Justice Noel did not dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could not find existing legislative authority permitting its retention and use," Goodale said*** in a statement. News of the spy agency program comes as the provincial Quebec government announced they are calling a public inquiry into police surveillance of journalists amid revelations various forces in the province monitored reporters' phones. The province's two largest police forces said earlier this week that they had monitored the phones of six prominent journalists in 2013. Associated Press (Daily Mail UK) (2016-11-03)

Canada court deals blow to spy agency, says it kept data illegally
A court dealt Canada's spy agency a blow on Thursday, declaring it had illegally kept data collected during investigations over the past decade and threatening sanctions if the issue occurred again. Although judges have previously criticized the Canadian Security Intelligence Service, or CSIS, for a lack of openness about its operations, the ruling was particularly uncompromising... **Federal Public Safety Minister Ralph Goodale**, **who** has overall responsibility for law enforcement agencies, **welcomed** the ruling and said the government would not appeal it. ***"I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service," Goodale said*** in a statement. Most Canadian security agencies have small individual review bodies, which OpenMedia and others complain are impotent and can only look at old cases. Oversight is more robust in other nations such as Britain and the United States, where special legislative committees monitor the work of security and intelligence agencies. **Goodale**, acting amid global concerns about the reach of security agencies, promised in June to create a similar oversight committee as part of a comprehensive probe into how national security is handled. A scandal erupted this week in the province of Quebec when it emerged that police had secretly tracked phone calls received and made by six reporters. Reuters (2016-11-03)

Les espions canadiens ont outrepassé leur mandat

Le service d'espionnage canadien a outrepassé sa mission en conservant illégalement des informations sensibles recueillies en vertu de mandats, a tranché la Cour fédérale dans un jugement rendu public, jeudi. En point de presse, le patron du Service canadien du renseignement de sécurité (SCRS) a dit prendre acte du verdict. «Le SCRS accepte la décision de la cour et a pris des mesures immédiates pour y répondre», a-t-il déclaré. Je regrette profondément les graves préoccupations de la cour à l'égard de notre manquement quant à l'obligation de franchise.» Durant plusieurs années, le SCRS a caché à la Cour fédérale - qui est chargée de lui délivrer des mandats - l'existence d'un programme de récolte de métadonnées. Cela constitue, pour la cour, un manquement à l'obligation de franchise dont le SCRS doit faire preuve envers le tribunal. Agence QMI (Journal de Québec, Journal de Montréal) ; Vice News; Motherboard; Agence France-Presse (L'Orient le Jour) (2016-11-03)

Broadcast Media / Médias télédiffusés

Yesterday's federal court ruling and the subsequent government response garnered significant media coverage on evening political shows and national news programs. Tone of coverage was negative and was amplified by recent news events concerning police surveillance of journalists in Quebec in the lead up to yesterday's ruling.

CBC News' Power & Politics held a panel discussion with former Public Safety Minister Stockwell Day, who was questioned on his knowledge of CSIS' associated data retention practices that began while he was minister. Extensive broadcast coverage continued into the morning of November 4, with all major Canadian cable news networks airing yesterday's technical briefing with CSIS Director Michel Coulombre.

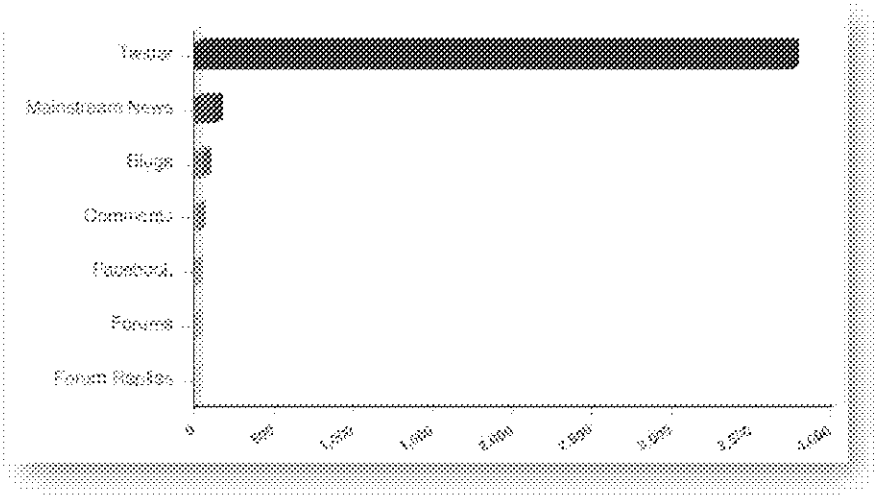
CBC News Network's Power & Politics discussed **Public Safety Minister Ralph Goodale's** response to the Federal Court's ruling regarding CSIS' retainment of metadata. Rough Transcript (2016-11-03)

CBC News Network's Power & Politics interviewed Radio-Canada journalist, Marie-Maude Denis, regarding Sûreté Du Québec spying on her. CSIS's retainment of metadata was also discussed during this segment Rough Transcript (2016-11-03)

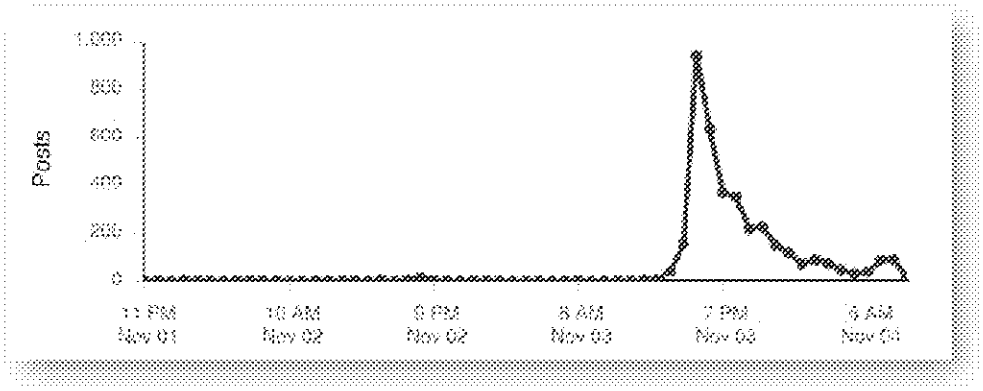
CBC News Network's Power & Politics held a panel discussion with former Public Safety Minister Stockwell Day regarding today's Federal Court's ruling on CSIS' retainment of metadata. Rough Transcript (2016-11-03)

Social Media / Médias sociaux

Social media coverage regarding the CSIS court decision was extensive over the past 48 hours. There were a total of 3963 social media posts regarding the decision, with 3,730 of those posts coming from Twitter.



Social media coverage regarding the CSIS court decision spiked considerably at 5 p.m. on November 3rd, 2016, coinciding with the release of the court decision. Approximately ¼ of all social media posts regarding the court decision occurred at this time (943 posts). Social media coverage has appeared to be declining steadily since the release but a subtle uptick in social media coverage is observed around 7:00 ET on November 4th, 2016, coinciding with the publication of online and print newspapers.



The tone of social media coverage is negative, with many social media users expressing outrage at the perceived infringement on privacy rights. Several social media users drew parallels between the illegal collection of metadata by CSIS and the surveillance of journalists by the SPVM, which has consistently garnered media attention throughout the week. Social media users also emphasized the magnitude of the report, with many describing the decision as scathing and CSIS as unaccountable. Many privacy rights groups used the recent court decision as leverage for their case against Bill C-51. See below for a word cloud indicating the words most commonly used in conjunction with social media posts regarding the CSIS court decision:

Tweets of note:

CSIS Canada
Read statement from CSIS Director regarding decision of the Federal Court https://csis.gc.ca/nwsrm/index-en.php ...

SCRS Canada
Lisez la déclaration du directeur du SCRS au sujet de la décision rendue par la Cour fédérale https://csis.gc.ca/nwsrm/index-fr.php ...

NEWS1130
Public Safety Minister Ralph Goodale says the government won't appeal a Federal Court ruling that Canada's spy agency broke the law.

Colin Freeze
Public Safety Minister @RalphGoodale --now consulting about CSIS C-51 -- says scathing ruling shows CSIS laws outdated. Time for new laws!

Matt Galloway
CSIS has been collecting & retaining electronic data on Canadians for 10 years. That's against the law. Wild story: https://t.co/9DRtnWViEB

CBC News
CSIS broke law by keeping sensitive metadata, Federal Court rules http://www.cbc.ca/1.3835472CSIS broke law by keeping sensitive metadata, Federal Court rules https://t.co/OtaWM6S9Ea

TimesTranscript
CSIS broke law by keeping sensitive metadata, Federal Court rules ow.ly/ykQS305PVzP @TJProvincial @DailyGleaner pic.twitter.com/JmZtQVkUZV

NEWS1130
CSIS broke law by keeping sensitive metadata, Federal Court rules bit.ly/2ejAmBy pic.twitter.com/TYG9MDrERk

Stewart Bell
Retention of data by CSIS "falls outside" its legislative jurisdiction, court says. http://cas-cdc-www02.cas-satj.gc.ca/

Stewart Bell
CSIS breached "duty of candour" by not disclosing Operational Data Analysis Centre launched in 2006, says court. http://cas-cdc-www02.cas-satj.gc.ca/

Stewart Bell
Important Federal Court decision on CSIS Operation Data Analysis Centre. http://cas-cdc-www02.cas-satj.gc.ca/

StewartBellNP
2/More on secret CSIS data program.

Stewart Bell
3/Court's description of CSIS data program.

Stewart Bell
4/CSIS retained metadata "indefinitely" even if not threat related, court says.

Stewart Bell
5/Federal Court's brutal judgment of the "illegal" retention of metadata by CSIS.

Stewart Bell
CSIS director responds to Federal Court ruling on illegal metadata program http://www.newswire.ca/

Michelle Lamarche
Le directeur Coulombe SCRS dit que des mesures ont été prises pour se conformer à la décision de la cour #tvanouvelles

Michelle Lamarche
Cour fédérale blâme le SCRS qui a manqué à son devoir de franchise. #polcan #tvanouvelles

Fab de Pierrebourg
Le #SCRS blâmé par la Cour fédérale pour avoir illégalement conservé des données personnelles. https://t.co/gu5OiolOG8

Christopher Parsons
People point at the US, and how NSA et al have systematically mislead the courts. This decision further reveals that CSIS does same, here

Globe and Mail
RT @Colinfreeze: Faulting #cdnpoli spies for unlawfully amassing data, court reveals #CSIS now gets tax records warrantlessly #C51 https://...

National Post
Judge blasts CSIS for not revealing secret program that has been illegally keeping metadata since 2006 natpo.st/2fmEp11 pic.twitter.com/6vSXf5mH2A

BCCLA

In scathing ruling, Federal Court says CSIS bulk data collection illegal bit.ly/2fhcErM via @globeandmail #C51 #cdnpoli

Kady O'Malley
Well, it's nice that CSIS is willing to accept the decision of the federal court on its various and sundry breaches of candour and the law.

Tonda MacCharles
CSIS program illegally spied for a decade, judge rules. The wrap by @alexboutilier https://www.thestar.com/news/canada/...

Jameel Jaffer
Canadian spies concealed far-reaching surveillance program from court tasked with overseeing them. http://www.theglobeandmail.com/news/national/...

Trevor Timm
In a scathing ruling, a federal court in Canada rules its intel agency's mass data collection program is illegal http://www.theglobeandmail.com/news/national...

Justin Ling
I've covered CSIS and CSE for years, now. This is likely the largest revelation we've ever found out about their intelligence surveillance.

Justin Ling
I'm on a tech briefing about the most recent CSIS spying revelation. This, folks, is a bombshell.

David R Brake
Seems Cdn intelligence agency CSIS is keeping comms metadata after investigations finished http://www.vice.com/en_ca/read/theres-a-secret-c... eek! #privacy

Stephanie Carvin
From last night: my piece on #YourNatlSec written before the CSIS/ODAC hoo-ha. But talks about analytical oversight.

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
October 22, 2015 / le 22 octobre 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

More changes to Parliament Hill security could be coming, says senior Mountie
A year after a rampaging gunman stormed the Centre Block, the RCMP and federal officials are still studying ways to make Parliament Hill more secure, says a senior Mountie.While it's still early, the process could lead to new, highly visible security measures on the Hill, said RCMP Assistant Commissioner Gilles Michaud."We want to make sure that we address all potential threats," Michaud said in an interview.One year ago today, Michael Zehaf Bibeau fatally shot honour guard Cpl. Nathan Cirillo at the National War Memorial before rushing into Parliament Hill's Hall of Honour, where he was killed in a hail of bullets.The RCMP was responsible for the grounds of the parliamentary precinct, while House of Commons and Senate security forces had jurisdiction inside the Parliament Buildings.A now-merged parliamentary protective service manages day-to-day security on Parliament Hill, a direct consequence of Oct. 22 intended to eliminate possible confusion.But Defence Research and Development Canada is quietly working away at two studies that could further transform security on the Hill and for about three dozen other buildings in the parliamentary precinct.One report, to be done by the end of the year, is looking at officer training, exercises and co-ordinating procedures of the newly merged security forces. The other, to be completed by April, is examining possible investments in new security facilities and equipment or other kinds of measures."I'm sure that they're looking at some aspect of how we can better screen people before they come on to the Hill," Michaud said. "Because we're doing screening of vehicles, but what about people? Is there a way that that can be done without limiting their access?"He cautioned that wouldn't necessarily mean setting up guard booths just inside the Hill gates, noting screening could be accomplished through other tools, such as security cameras — which are already being used to some extent. Canadian Press (Times Colonist); Postmedia News (Ottawa Citizen, A7)

CONTRACT & ABORIGINAL POLICING / SERVICES DE POLICE CONTRACTUELS ET AUTOCHTONES

RCMP boss says impaired driving still a problem on highways
Assistant RCMP Commissioner Roger Brown knows the ugliness of impaired driving. Brown, who has been the commander of the force in the province for two years, said he was driving to Fredericton one night from Saint John, when he stumbled upon an impaired driver. "I was driving behind a guy and the guy was so drunk behind the wheel that he passed out and the car came to a stop," Brown said in an interview. "I was Johnny-on-the-spot." Brown said he obtained the services of another officer and between the two of them, they were able to remove the individual from the car, arrest him and read him his rights. "I couldn't even lift the guy, he was that drunk." Brown said the case went to court and the blood alcohol reading was more than 400 milligrams of alcohol per 100 millilitres of blood. The legal limit is 80 mg. "This guy was on the road. He could have been driving toward you that night." Brown said drinking and driving continues to be a problem on the province's highways and he just can't understand why. "It's wrong, it kills people and that should never be." Statistics contained in the RCMP's recently released annual report revealed that nine **New Brunswickers** lost their lives last year in collisions where alcohol or drugs were involved. Daily Gleaner, A4 (Times & Transcript, A12)

Hearing set for human trafficking case
An **Airdrie** man accused of human trafficking and prostitution offences will get his chance to hear the Crown's case against him at his upcoming preliminary hearing. Javyrell Raymond Baird, 25, elected to be tried by a Red Deer Court of Queen's Bench judge alone Wednesday in Red Deer provincial court. Represented by defence counsel Greg Gordon, Baird appeared by closed circuit television from the Red Deer Remand Centre. Preliminary hearings are held to test the strength of the Crown's case to determine if a trial is warranted. Baird faces charges of trafficking a person under the age of 18 for the purpose of exploiting or facilitating exploitation, living on the avails of prostitution of a person under 18 and assault. He was arrested in Gasoline Alley June at a hotel. The Airdrie RCMP General Investigation Section and Crime Reduction Unit were investigating a report of a missing female youth. The investigation led them to believe the teen had been a victim of human trafficking. Baird remains in custody, however Gordon has scheduled a bail hearing for Oct. 26. Red Deer Advocate, C1

Man charged in hammer assault
A **Red Deer** man has been charged following a Riverside Meadows home invasion where two men were assaulted with a hammer. Police say the suspect climbed to a second-floor apartment balcony and assaulted two people inside with a hammer shortly before midnight on Friday. He climbed onto the roof of a parked vehicle to gain access to the balcony. Two men sustained bruises and abrasions but were able to push their assailant out of the apartment. The suspect then jumped from the balcony, landed on the same parked vehicle, and fled in another vehicle. The suspect was known to his victims, and Red Deer RCMP located him shortly afterward on 55th Avenue. Police executed a traffic stop and took the suspect into custody without incident. Tyrel George Jackson, 28, of Red Deer is charged with break and enter and committing a crime, two counts of assault with a weapon, possession of stolen property under $5,000, uttering threats and operating motor vehicle while disqualified, mischief under $5,000 and possession of controlled substance. Jackson appeared in Red Deer provincial court on Wednesday with a white bandage wrapped around his head. Represented by defence counsel Lorne Goddard, Jackson reserved his plea. Crown Prosecutor Blair Brandon said he is opposed to Jackson receiving bail. The matter was adjourned by judge Gordon Yake to Oct. 28 in Red Deer provincial court. Red Deer Advocate, C1; Postmedia Network (Edmonton Journal, A16)

Mounties probe shooting reports
Police are investigating reports of a drive-by shooting in **High River** that left a home and truck with bullet holes. Mounties were called to Highwood Heritage Estates, west of High River cemetery, in the town south of Calgary at 4:30 p.m. Tuesday for a possible drive-by shooting. Officers discovered bullet holes in the truck and house, but no one was injured, even though people had been home at the time. Early indications suggest the shooting was not random, and that the public is not at risk, according to RCMP. Postmedia News (Calgary Herald, A14, Edmonton Journal, A13)

A diamond detective story
Twenty-two people tried to claim a diamond ring found last spring before the rightful owner was located. According to East Hants District RCMP, a citizen found a diamond ring in a parking lot off Highway 1 in **Mount Uniacke** in early June and turned it in to the Rawdon detachment. After issuing a news release and sharing photos of the ring on social media in July, the RCMP received numerous tips from the public. Oct. 13, the RCMP in East Hants was able to confirm the rightful owner, and the ring has since been returned to a Kings County woman. Const. Dianne Hartery with the Rawdon Detachment of the RCMP said the found ring was stolen during a break-and-enter earlier this year. Hartery said she didn't want to give too many details to avoid re-victimizing the victim. Hartery did say the ring was stolen in Kings County in 2015 and that no charges are pending. The investigation into the break-and-enter is still open. More than 20 people contacted the RCMP to claim or inquire about the ring, the officer said. Cape Breton Post, A9

Moncton
Trois hommes ont été arrêtés et font face à de nombreuses accusations pour l'enlèvement d'une femme âgée de 50 ans et le cambriolage de son domicile, la semaine dernière à **Moncton**. Le 13 octobre, peu après 11 h, la police été informée qu'une femme de 50 ans avait été enlevée dans son appartement sur la rue Gordon à Moncton, plus tôt en matinée, et qu'on l'avait emmenée à Sackville. Elle a ensuite été libérée par ses ravisseurs. Elle n'a pas été blessée... Jeremy Bernard a été arrêté le 15 octobre, à Moncton, et il a comparu en cour provinciale à Moncton lundi. Il a été libéré et devrait comparaître de nouveau le 17 novembre. Meneka Weva a été arrêté le 16 octobre, à Moncton, et il a comparu en cour lundi. Il a été mis en détention et devrait comparaître de nouveau le 4 novembre. Shawn Augustine a été arrêté le 17 octobre, à Moncton, et il a comparu en cour lundi. Il a été mis en détention et devrait comparaître en cour provinciale à Moncton le 6 novembre. Les trois hommes font face à des accusations, entre autres, pour séquestration, enlèvement, agression armée, voies de fait ayant causé des lésions corporelles et braquage d'une arme à feu. La GRC poursuit son enquête. Acadie Nouvelle, 2

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

More changes to Parliament Hill security could be coming, says senior Mountie
A year after a rampaging gunman stormed the Centre Block, the RCMP and federal officials are still studying ways to make Parliament Hill more secure, says a senior Mountie.While it's still early, the process could lead to new, highly visible security measures on the Hill, said RCMP Assistant Commissioner Gilles Michaud."We want to make sure that we address all potential threats," Michaud said in an interview.One year ago today, Michael Zehaf Bibeau fatally shot honour guard Cpl. Nathan Cirillo at the National War Memorial before rushing into Parliament Hill's Hall of Honour, where he was killed in a hail of bullets.The RCMP was responsible for the grounds of the parliamentary precinct, while House of Commons and Senate security forces had jurisdiction inside the Parliament Buildings.A now-merged parliamentary protective service manages day-to-day security on Parliament Hill, a direct consequence of Oct. 22 intended to eliminate possible confusion.But Defence Research and Development Canada is quietly working away at two studies that could further transform security on the Hill and for about three dozen other buildings in the parliamentary precinct.One report, to be done by the end of the year, is looking at officer training, exercises and co-ordinating procedures of the newly merged security forces. The other, to be completed by April, is examining possible investments in new security facilities and equipment or other kinds of measures."I'm sure that they're looking at some aspect of how we can better screen people before they come on to the Hill," Michaud said. "Because we're doing screening of vehicles, but what about people? Is there a way that that can be done without limiting their access?"He cautioned that wouldn't necessarily mean setting up guard booths just inside the Hill gates, noting screening could be accomplished through other tools, such as security cameras — which are already being used to some extent. Canadian Press (Times Colonist); Postmedia News (Ottawa Citizen, A7)

Attentat à Ottawa - La GRC avait été prévenue de la menace

Un an après l'attentat qui a coûté la vie au soldat Nathan Cirillo devant le parlement à Ottawa, des documents obtenus par la CBC révèlent que la Gendarmerie royale du Canada (GRC) avait été prévenue à trois reprises d'une potentielle attaque terroriste dans les jours précédant le drame. Les autorités ne sont cependant pas à blâmer, jugent des experts qui rappellent à quel point il est difficile de contrer une menace provenant d'individus isolés. Un an après l'attentat qui a coûté la vie au soldat Nathan Cirillo devant le parlement à Ottawa, des documents obtenus par la CBC révèlent que la Gendarmerie royale du Canada (GRC) avait été prévenue à trois reprises d'une potentielle attaque terroriste dans les jours précédant le drame. Les autorités ne sont cependant pas à blâmer, jugent des experts qui rappellent à quel point il est difficile de contrer une menace provenant d'individus isolés. Le réseau anglais de Radio-Canada a dévoilé mercredi des informations contenues dans près de 1000 pages de documentation obtenues en vertu de la Loi sur l'accès à l'information. On y apprend d'abord que le 17 octobre 2014, le Centre intégré d'évaluation du terrorisme a mis en garde la GRC contre un possible " acte terroriste violent ". Il a du même coup fait passer l'indice de la menace terroriste au pays de " basse " à " moyenne ", alors que cet indicateur était demeuré inchangé pendant quatre ans. Le 18 octobre, le Groupe des renseignements criminels a quant à lui fait parvenir un rappel de sécurité. Le document d'une page prévient les autorités que le groupe État islamique (EI) " encourage activement les djihadistes de l'Occident et les nouveaux militants à lancer des attaques contre des membres des forces de l'ordre dans les pays qui combattent ses troupes ". Finalement, un troisième avis a été transmis le 21 octobre, soit le lendemain de l'attaque terroriste survenue à Saint-Jean-sur-Richelieu. Ce jour-là, Martin Couture-Rouleau a foncé avec sa voiture sur trois militaires, tuant l'adjudant Patrice Vincent et blessant un de ses collègues. Ce dernier avis produit par le Centre national de coordination du renseignement de la GRC rappelle aux policiers l'importance d'appliquer les mesures de sécurité et de prévention en lien avec les récentes menaces du groupe EI à l'endroit des forces de l'ordre. Un autre rapport qui détaille les ressources humaines déployées par la GRC en octobre 2014 indique par ailleurs que sur les 177 postes autorisés sur la colline du parlement, au moins 29 étaient vacants pendant cette période. Ce manque de ressources s'explique vraisemblablement par les coupes budgétaires imposées par le gouvernement Harper en 2012. Un rapport réalisé par la police provinciale de l'Ontario notait également en juin dernier que les compressions nuisent au dispositif de sécurité de la GRC sur la colline parlementaire. Le Devoir, A1; Agence France-Presse (Le Droit, 7) (2015-10-22); Agence France Presse (Le Journal de Québec, Le Journal de Montréal, Le Devoir (2015-10-21)

'He Stood His Ground'

Three hours into a Wednesday morning shift, the constable stood in the south corridor of Centre Block, chatting with another member of the House of Commons security force as MPs arrived for their weekly caucus meeting. A few bored journalists and camera operators congregated around the rotunda inside the Centre Block doors. The attack that killed a Canadian Forces member in Saint-Jean-sur-Richelieu two days earlier was still fresh news, and the two men - the constable in uniform, his colleague in plainclothes - speculated about whether something like that could ever happen on Parliament Hill. Then it did. "Gun! Gun! Gun!" someone yelled from the main doors, shortly before 10 a.m. Then a shot. "I smelled powder and I saw my buddy beside me draw his firearm," said the constable, a 30-year veteran of Parliament Hill security who asked not to be named. A year later, he still worries about someone targeting his family. "I said, this is tango time. We're getting hit. I'm not sure what type of attack we're getting but in hindsight I'm thinking there's a possibility the 18 are coming," he said, in reference to the Toronto 18 terror group that planned to attack Parliament and behead the prime minister... In fact, says the constable, there was no RCMP security detail in the room at the time Harper went into the closet. Until the constable arrived moments after the shooting, there were no House of Commons security there, either. Under the rules in place at the time, the prime minister's RCMP protective detail was required to wait outside of Centre Block after handing him off to plain clothes House of Commons guards. Postmedia News (Windsor Star, N1/Front, Ottawa Citizen, A1, Edmonton Journal, N1/Front) (2015-10-22); Ottawa Citizen (2015-10-21)

Securing the Hill

Could it happen again? Could worse happen? Could an attacker like rifle-wielding Michael Zehaf-Bibeau - or one who is better-trained, better-armed or with back-up, say a team of assailants - breach Parliament Hill to launch an even more deadly assault on the seat of Canada's national democracy? The question still nags as Ottawa marks the one-year anniversary of a terrible week in the country's life last October... More people have been hired to monitor more live video camera feeds around the clock. During the

attack last October, an RCMP officer in a cruiser reading a report didn't see Zehef-Bibeau run onto the grounds. Astonishingly no one at the operational centre, which monitors video feeds of all protected sites, actually saw the gunman flash on a screen as he stormed through the East Gate either. A new intelligence unit has been created within the parliamentary protective service to share and assess different threats. An armed RCMP "Quick Response Team" is permanently posted outside to respond to suspicious or emergency circumstances while other officers maintain a secure perimeter. On Oct. 22, Mounties vacated their posts to race to Centre Block so for several minutes the Hill was exposed. A vehicle screening facility at the only point of public vehicle access to the Hill is being reinforced. All Hill police and security forces will soon have the same radios and operate on the same frequency. The OPP said the lack of "interoperability" was a major problem. Commons and Senate guards, RCMP and the Ottawa police operated on different radio systems. When Ottawa cops responded to 911 calls to the War Memorial the RCMP did not know the attacker was headed their way. Commons and Senate security did not know he was out on the lawn when a Mountie screamed into her radio. The civilian forces weren't aware of the threat until it crashed through the front door. Now all Commons and Senate personnel are being security-cleared to the level of RCMP officers to receive and respond to law enforcement information on police frequencies, and the integrated service has been looped into a region-wide communications network for emergency responders known as Intersect. Toronto Star, A1 (Spectator, A5)

Interpol issues alert on Fredericton woman facing charges in Philippines

A Fredericton woman facing charges in the Philippines relating to the 2012 shooting death of her husband is now listed on the International Criminal Police Organization's (Interpol) website. Erma (Jane) Doyle, 39, has been living in Fredericton since August 2012. She came to Canada shortly after former Fredericton businessman Harry Doyle was shot and killed on Aug. 12 during a family barbecue at Palma Beach Resort in Punta Pilar, Surigao City. In August 2013, the Philippine National Police issued an arrest warrant for Doyle on a charge of parricide. She continues to live in Fredericton along with her sons, 15-year-old Joseph and Daniel who will turn three in November. Earlier this year, Philippine prosecutor A.S. Casurra requested the Canadian Embassy contact the Department of Justice to ask if it could use its influence to help expedite the process. Interpol's notification on the arrest warrant for Doyle has been sent to its 190 member countries at the request of the Philippine National Police, including the RCMP. The Daily Gleaner contacted the RCMP's head office in Ottawa for comment. None was available prior to press time. In an email, Interpol said it facilitates international police co-operation and explained that individuals listed on what it refers to as its 'Red Notice' are wanted by national jurisdictions. "Interpol's role is to assist national police forces in identifying or locating those individuals with a view to their arrest and extradition," the agency stated on Wednesday. Daily Gleaner, A1

Harper comments on Islam damaged relations with Muslims, says former CSIS analyst

Stephen Harper's comments about the threat of "Islamicism" strained the fragile trust federal officials built with Muslim Canadians in the fight against terrorism, says a former analyst with Canada's spy agency. The frequently harsh tone Harper and his cabinet members struck with Muslims created a rift the new Liberal government must work to overcome, said Phil Gurski, who spent almost 13 years at the Canadian Security Intelligence Service before moving to Public Safety Canada. Rebuilding trust will be an important element in national counter-extremism efforts by police and community groups, said Gurski, a specialist in radicalization and homegrown terrorism now working as a private threat and risk consultant. "I think now that with a new government, we have at least the opportunity to start - not with a blank slate - but to kind of reset the relationship," he said in an interview. This week marks the grim anniversary of two fatal attacks on Canadian soldiers by men with jihadist sympathies. One year ago Thursday, Michael Zehaf Bibeau shot Cpl. Nathan Cirillo, an honour guard at the National War Memorial, before rushing into Parliament's Centre Block. Zehaf Bibeau was quickly gunned down. Two days earlier, Martin Couture-Rouleau had fatally rammed Warrant Officer Patrice Vincent with a car in St-Jean-sur-Richelieu, Que. After a chase, police shot and killed the knife-wielding assailant. Gurski said security agencies need to continue investigating potential threats, but the government must also do more to support police and community-led programs to stop young people from becoming radicalized in the first place. He has distilled his insights into a book, "The Threat from Within," published this week. He praises grassroots counter-radicalization initiatives - noting such efforts work better than government-run ones - and lauds the police services active in the field, notably Toronto and Calgary. In the federal sphere, Public Safety and the RCMP have guided the efforts, with CSIS playing a background role. At Public Safety, Gurski

worked with the department's citizen engagement bureau. Canadian Press (Times & Transcript, B1) (2015-10-22); Canadian Press (CTV News, 580 CRFA, Kelowna Daily Courier, Brandon Sun, Huffington Post) (2015-10-21)

Attack changed policing in Ottawa
A year after an ISIL-inspired gunman killed an unarmed ceremonial sentry at the National War Memorial, Ottawa police now guard the guards at the vulnerable location. In some ways, the duty is emblematic of the challenges the police service of the nation's capital faces - counter-terrorism investigations fall outside the force's mandate, except that any threat of terrorism affects the city's safety. The cenotaph and Parliament Hill might be national landmarks, but they're nestled inside the City of Ottawa. Officers policing the nation's capital have always been cognizant of their special role that extends beyond the mandate of most city police forces. But in the year since the attack on the Hill, Ottawa police have had to accept that terrorismrelated threats are real - and that's changed how they police this city... Counterterrorism is the mandate of the national police force, the RCMP. But Ottawa police, while a municipal force, work to support those investigations. "A lot of information can be generated at the local level," Hinterberger said. That information can come to officers in the form of a tip from a concerned member of a religious community who wants to flag someone who has expressed radical views, or from someone who overhears a co-worker making threats against people or places. While RCMP will then lead investigations, local officers often do the grunt work. "A full-blown (counterterrorism) investigation is a tremendous effort and it requires a lot of resources," Hinterberger said. Once the RCMP launches an investigation, local patrol officers work the streets to help out. The Ottawa force has its own officers who are on loan to the RCMP's national security unit, called INSET - integrated national security enforcement teams. Postmedia News (Ottawa Citizen, A7)

Ottawa se souvient de l'attentat du 22 octobre
La cérémonie aura lieu au Monument commémoratif de guerre à Ottawa, où le caporal Cirillo est tombé sous les balles de Michael Zehaf-Bibeau, abattu plus tard à l'intérieur du parlement, le matin du 22 octobre. Deux jours plus tôt, le caporal Patrice Vincent était happé mortellement par un autre islamiste radical, Martin Couture-Rouleau, à Saint-Jean-sur-Richelieu. L'événement vise de plus à souligner le courage des premiers intervenants qui ont tenté de secourir les victimes et aux autres qui ont abattu les agresseurs pour mettre un terme à leur folie. Le gouverneur général du Canada, David Johnston, assistera à la cérémonie en compagnie d'autres dignitaires. Le 30e Régiment d'artillerie de campagne de l'Artillerie royale canadienne fera résonner 21 coups de canon, et sera suivi par le passage de CF-18 Hornet de l'Aviation royale canadienne dans le ciel de la capitale, à 11h20. Les avions traverseront la région en formation d'hommage aux disparus, à quelque 500 pieds d'altitude... La GRC n'a pas renforcé la sécurité malgré les alertes concernant de possibles attaques par des individus radicalisés, qui lui avaient été transmises moins d'une semaine avant l'attaque au parlement d'Ottawa l'an dernier, a révélé mercredi CBC. Par deux fois, les 17 et 18 octobre, la Gendarmerie royale du Canada (GRC) a été destinataire de notes prévenant d'encouragements soutenus du groupe État islamique (EI) pour mener des attaques contre des pays occidentaux dont le Canada, selon CBC qui s'appuie sur des documents obtenus dans le cadre de la Loi d'accès à l'information. La première note du service de renseignements, transmise le 17, signalait que des «actes de terrorisme pourraient se produire» et remontait de faible à moyen le niveau d'alerte pour la première fois en 4 ans. Le 18, dans une circulaire, la GRC indiquait elle-même que le groupe EI encourageait «activement les jihadistes dans le monde occidental à lancer des attaques contre des membres des forces de sécurité des pays engagés dans les combats contre nos troupes». La Presse (Le Droit); La Presse, A9 (La Voix de l'Est, 18, Le Quotidien, 16); Chronicle Herald, A16

Details to be released of major human trafficking investigation
Ontario Provincial Police have scheduled a press conference Thursday morning to reveal details of a major human trafficking investigation. A media release states several police forces were involved in the investigation nicknamed Operation Northern Spotlight including the RCMP and FBI. A human trafficking victim, a member of a child advocacy support agency, and experts in the case will also be present during the press conference. Global News

12 trafiquants arrêtés

Une large opération de l'Escouade régionale mixte (ERM) Québec visant un réseau de trafiquants qui serait lié aux Hells Angels a conduit à l'arrestation de 12 individus alors que deux suspects sont toujours recherchés.Tôt hier matin, des policiers de l'ERM Québec ont exécuté 14 mandats d'arrestation contre des trafiquants de drogue qui seraient reliés aux motards criminels Hells Angels. «Les suspects font partie d'un réseau important dans la région de Québec, avec des ramifications sur la Côte-Nord», a expliqué Ann Mathieu, porte-parole de l'ERM. Si une majorité de ces suspects ont été arrêtés hier, les autorités sont toujours à la recherche de deux individus. Il s'agit de Éric Champlain-Laroche, 39 ans, de Charlesbourg, et de Jonathan Roberge- Nöel, 29 ans, de Québec. Les autres individus arrêtés ont comparu sous des accusations de gangstérisme, complot et trafic de stupéfiants. Certains d'entre eux n'ont pas de casier judiciaire et ont été libérés en échange de conditions, mais d'autres suspects sont demeurés détenus. Journal de Québec, 15

Security experts say terror-attack warnings before Parliament Hill shootings too vague
A security expert and former RCMP officer say the trio of terror-attack warnings the Mounties received in the days preceding last year's deadly shootings on Parliament Hill were likely too general for the force to take specific actions. CBC News has reported that the RCMP disseminated separate terror warnings to officers on Oct. 17-18 and Oct. 21, each citing potential attacks on Canadians in uniform. On Oct. 22, a lone gunman did just that, killing a soldier at the National War Memorial and injuring a guard inside Centre Block on Parliament Hill. "If the threat is general, then the level of awareness is heightened, but it's hard to go beyond heightened state of awareness," said Pierre-Yves Borduas, a retired RCMP deputy commissioner. "It's always easy to second-guess after the attack." Wesley Wark, a security expert and academic at the University of Ottawa, said frequent generic warnings can even have an unintended effect. "Warnings that contained no 'actionable' intelligence ... may have been frequent enough to induce, at least in part, a cry wolf phenomenon," he said. A 1,000-page RCMP dossier obtained under the Access to Information Act also shows that so-called "enhanced patrols," ordered in the wake of two minor security incidents in Ottawa, were ended shortly before the Oct. 22 attacks. The file also shows that the RCMP unit whose duties include Parliament Hill security was chronically short-staffed in the fall of last year, by at least 29 positions, because of cuts announced in the Harper government's 2012 budget. CBC News (2015-10-21)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Mountie found not guilty of assaulting pub patron
A Kelowna cop has been found not guilty of assaulting a patron at a local pub after he refused to leave following last call. Provincial court Judge G.W. Koturbash, in a ruling handed down Wednesday, found RCMP Const. Grant Jacobson not guilty of assaulting pub patron John McCormick. McCormick, 60, according to Koturbash's decision, had been drinking at Rose's pub June 28, 2014, for up to 13 hours when he was told last call was over and it was time to leave. According to the judge, McCormick "was drunk but he said not totally wasted or stumbling." Postmedia News (Province, A13)

Stay strong and carry on
Just a month ago, the province was trying to come to grips with the tragic death of a dedicated police officer. The body of Const. Catherine Campbell, a six-year member of the Truro Police Service, was found underneath a bridge ramp off Barrington Street in Halifax. It's fitting then that the annual Atlantic Women in Law Enforcement conference is being held this week near Campbell's beat, at the Holiday Inn in Truro. "She was a member of our organizing committee, and her dedication to this conference is what gave us all the courage to continue with our planning," Sgt. Carolyn Nichols of Halifax Regional Police and president of the organization said in an email interview. "The theme of the conference is Staying Strong and Carrying On," Nichols said. "It is a reminder to all of us of the importance of taking care of ourselves and each other, to stay strong in both body and spirit and to reach out to others for support when you need it. We are fortunate to have employee assistance programs and referrals available through our agencies and unions." The 23rd annual training conference brings together 95 women to talk about topics that include investigative case studies, forensic psychology, prostitution, post-traumatic stress disorder, leveraging social media to solve and prevent crime, and radicalization within communities. "The Atlantic Women in Law Enforcement was founded on promoting teamwork by fostering

professional and inter-agency associations," Nichols said. "At the conference, we have representation from numerous provincial agencies, which gives our membership the ability to network and discuss issues which are common across all our departments." The four-day conference, which got underway Tuesday, is co-hosted by the Truro Police Service, Colchester County District RCMP, the Nova Institution for Women in Truro and Correctional Service Canada. The conference will provide informative presentations and workshops that promote professional development and provide opportunities for inter-agency networking. Chronicle Herald, A4

Manitoba RCMP staff shortages taking toll on officers, warn representatives
Staffing levels within the RCMP in Manitoba have dropped over the past two years while job vacancies have increased, creating a situation that a staff representative says is taking a toll on members. As of April 1, there were 36 vacant positions in Manitoba for regular members, according to documents obtained by CBC News under the Access to Information Act. The number of RCMP regular members in Manitoba dropped from 1,082 in April 2013, to 1,070 in 2014, to 1,055 in 2015 - a loss of 27 positions over the two-year period. Even with the smaller complement, the vacancy rate increased from 3.2 per cent in 2014 to 3.4 per cent in April 2015. By contrast, there was slightly more than a full complement in April 2013. "Typically the members who are left behind fill the gaps by taking on additional duties, working extra overtime," said Staff Sgt. Scott Bird, a staff relations representative with D Division. Bird said to maintain public safety while dealing with the shortages, officers are moved around from detachment to detachment, where they're most needed. Often it means working longer hours and spending less time with their families, he said. "We have an extremely dedicated group of RCMP members and they continually take on more and more. But they get tired ... and they're working more than they want to in some instances," said Bird. His concerns were reinforced by Rob Creasser, a media liaison with the Mounted Police Professional Association of Canada. CBC News

Mountie guilty of driving RCMP all terrain vehicle while impaired
An RCMP officer from Wollaston Lake has pleaded guilty to crashing an RCMP all-terrain vehicle while drunk and off duty. Constable Kevin Granrude was fined $1,000 and given a one-year driving prohibition. He pleaded guilty to impaired driving. A second charge of driving over .08 was withdrawn. The accident happened in the summer of 2014 when he was driving the ATV outside Wollaston at 1:30 in the morning. It was not clear to investigators why he was driving it while off duty. The RCMP launched a code of conduct investigation, but the outcome has not been made public. Granrude had more than nine years service at the time of the crash. Granrude -- who was not wearing a helmet -- was thrown from the ATV and suffered a serious head injury. He was later transferred to Swift Current. CBC News (2015-10-21)

Members of Alyssa George's family question RCMP response at inquest into in-custody death
"I can't breathe."That's what Mark Oleksiuk remembers hearing his wife Alyssa George say shortly before she was found in medical distress in her cell at the Terrace RCMP holding cells on Sept. 4, 2013. Oleksiuk, who was being held in a nearby cell at the time, appeared at the B.C. Supreme Court in Terrace on Oct. 19 to give his testimony at a public inquest into George's death. George, a 25-year-old First Nations woman, also known as Alyssa Oleksiuk, was found face-first on the floor of her jail cell 15 hours after being taken into custody on an arrest warrant. She was flown to Vancouver General Hospital for more intensive treatment, but died there on Sept. 10, 2013. CBC News (2015-10-21)

Lloydminster RCMP showcase police dog services
One of the most active members of the Lloydminster RCMP doesn't have a driver's license. He also is four years old, weighs 65 pounds, and has four legs and a tail. His name is Drax, and his partner is Constable Mark Freeman, who has been partnered with the purebred German Shephard for the past three years. On Tuesday afternoon, media were invited to view a demonstration of Drax's takedown skills and obedience training, as Freeman put his partner through the paces on the back lawn of the Lloydminster Legacy Centre, which sits behind the RCMP detachment building. "I think I have the greatest job in the world, because I get to work with a dog all day, and I have a partner with me all the time," said Freeman, who has been with the Lloydminster RCMP for the past two years. Freeman and Drax make up of 125 other Police Dog Services (PDS) across the country. Lloydminster meridian booster (2015-10-21)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

Liberals planning swift overhaul of anti-terror law
The controversial security bill rammed through Parliament by the Conservative government in the spring is expected to be overhauled without delay by the new Liberal government, say party officials and other sources. Proposed legislation to add new measures and repeal some existing parts of the law, now known as the Anti-terrorism Act of 2015, or C-51, is already being drafted and is to be tabled early in the new parliamentary session. Consultations with the public and various experts are planned before the replacement legislation is put to a final House vote. The bill was brought in by the Conservatives after the killings in October 2014 of Warrant Officer Patrice Vincent in Saint-Jean-Sur-Richelieu and Cpl. Nathan Cirillo in Ottawa by lone-wolf extremists. A key feature of the replacement legislation is expected to be the creation of a multi-party, joint House of Commons-Senate committee, sworn to secrecy and reporting to the prime minister and through him to Parliament... Public opinion polling shows many Canadians want a tighter watch over spy agencies and other federal intelligence gatherers, commensurate with their extended powers under C-51. A day after the Oct. 22, 2014 terror attack on the National War Memorial and Parliament Hill, Prime Minister Stephen Harper told the Commons that an existing government initiative to strengthen laws dealing with the surveillance, detention and arrest of national security suspects would be "expedited." Two months later, he unveiled Bill C-51, which the Conservative government used as the centrepiece of a security narrative on protecting Canadians from the Islamic State and its followers... As well, they want to narrow some of the "overly broad" definitions of what constitutes a threat to national security, including defining "terrorist propaganda" more clearly.
Current oversight and review is chiefly the responsibility of the Security Intelligence Review Committee (SIRC), which conducts after-the-fact reviews of the operations of CSIS, the country's human spy service. The activities of the electronic spy service, the Communications Security Establishment, are reviewed by a watchdog known as the Office of the Communications Security Establishment Commissioner (OCSEC). Increasingly, in the era of the Edward Snowden leaks on U.S. spying, CSE's domestic cyber-spying activities are raising privacy and legal concerns, though the agency has never been charged with law-breaking. There is no independent oversight or review of the Canada Border Services Agency, which has a dual intelligence and law-enforcement role. Nor is there dedicated, independent monitoring of the intelligence arms of the RCMP, Citizenship and Immigration Canada, the Privy Council Office, Department of Foreign Affairs, Trade and Development, and the Financial Transactions and Reports Analysis Centre of Canada. Postmedia News (Ottawa Citizen, A1, Province, A6, Windsor Star, N4, Edmonton Journal, N4) (2015-10-22); Ottawa Citizen (2015-10-21)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

NIL

OTHER / AUTRES

NIL

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 10, 2015 / le 10 novembre 2015

The Daily Media Summary can also be accessed through Newsdesk /
La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Dieppe Mountie gets major Interpol post
A New Brunswick Mountie and former commanding officer of the Codiac Regional RCMP has been elected Interpol's vice-president for the Americas. Todd Shean, who was born and raised in Dieppe,is currently an assistant commissioner and officer in charge of the RCMP's Federal Policing Special Services. This new position will be part of his regular duties with the RCMP. He was elected to Interpol's 13-member executive committee during the 84th Interpol General Assembly, which took place last week in Kigali, Rwanda. He is now one of three vice-presidents of the organization. Created in 1923, Interpol is the world's largest international police organization, with 190 member countries. In 1949, Canada became a member of Interpol and the RCMP was delegated the responsibility for administering and operating Canada's National Central Bureau, known as Interpol Ottawa. The bureau works with other countries through international criminal databases, the exchange of timely and accurate information and the coordination of international requests for assistance. Reached in Berlin, where he was attending the G7 summit on Monday, Shean said he plans to improve policing partnerships to advance Interpol's operational priorities. "We know that crime and all that goes with it is increasingly international," he said, emphasizing that it is more important than ever for law enforcement agencies to cooperate, corroborate and share information and best practices. Shean's 29-year career in law enforcement has included operational and leadership positions in tackling organized crime and financial crime, as well as in criminal intelligence and international policing. From 2005 to 2008, he led the Codiac Regional RCMP. At Codiac, he established a street crime unit, dedicated traffic section and other specialist officers in areas such as domestic violence. During that time, Metro Moncton had one of the lowest crime rates in the country. In 2008, Codiac had the best "clearance rate" among police forces in Canada for resolving serious crimes. Leading one of the largest RCMP detachments in the country, policing a bilingual city that is a microcosm of Canada, and providing services to three different municipalities were all good training, Shean said. "Codiac brings a number of different challenges. It really helps you prepare for other challenges." Shean

has also held posts in British Columbia and Florenceville. Since leaving Codiac, he has gone back and forth between Ottawa and Fredericton. His base will continue to be in Ottawa, but he maintains a home in Dieppe. "I'm a Maritimer. All my ties are there. I'll be back." Times & Transcript, A1

CONTRACT & ABORIGINAL POLICING / SERVICES DE POLICE CONTRACTUELS ET AUTOCHTONES

Man critically injured in fight
Three suspects are in custody after a man was critically injured during a confrontation between two groups of people in **Surrey** City Centre early Monday. RCMP said that at 3:20 a.m. police were called to 108th Avenue and 132nd Street following reports of screams and two groups fighting on the street. Police found one man, in his early 20s and known to police, with a serious gash to his chest. Two men and one woman were arrested and remain in custody while the investigation continues. The victim is listed in critical condition. Postmedia Network (Vancouver Sun, A4); Canadian Press (Times Colonist, A4) (2015-11-10); Vancouver Sun; CTV News Vancouver (2015-11-09)

Moose cull prompts protests
Dennis Day was all ready to protest a Mi'kmaq moose hunt that Parks Canada approved for Monday on **North Mountain in Cape Breton Highlands National Park**, but there was nothing to protest. Day, a resident of nearby Cape North, set up camp along the Cabot Trail just outside the park on Sunday night, but Mi'kmaq hunters and Parks Canada officials were still putting things in place Monday and were not expected to start hunting until Tuesday at the earliest. "I'm not even going up on the mountain," Day said Monday morning inside his roadside hut, which is equipped with a wood stove inside and a porta-potty next to it. "I'm staying right here." Day said he intends to peacefully protest Parks Canada's plan to cull up to 90 per cent of the moose population in a 20-square-kilometre area on North Mountain... However, Const. Mark Skinner of Nova Scotia RCMP said no complaints had been laid by Monday morning and police were not investigating any threats. Day said he didn't complain to police, because he didn't take an online threat he received seriously. And, he said, he has no intention of disrupting the hunt. "We just want to get our word across," he said. "I can't stress enough that this isn't against the aboriginals. This is against the park." RCMP and Parks Canada enforcement officers spent Monday morning meeting with Day and local citizens to keep things calm. Chronicle Herald, A3

Cops hunt for man
Surrey RCMP are looking for a man who allegedly tried to force his way into the home of a 15-year-old girl. Police say the man approached the teen outside her home in the 13300-block of Sutton Place around 2:15 p.m. Friday. He talked to her, then tried to go into the home uninvited. The two struggled in the doorway and the teen was able to call for help, police said. The man, described as a 25-to 30-year-old South Asian man, about 5-foot-8 with a medium build, fled in an older black car, possibly a Honda Civic. Canadian Press (Province, A8)

Brutal cas d'intimidation dans une école du Nord-Ouest
L'image du jeune Mitchell LaFrance (ci-dessus), victime la semaine dernière d'une sauvage agression près de l'école Southern Victoria High à **Perth-Andover**, est certes loin d'être passé inaperçue. Les images et propos au sujet de l'adolescent âgé de 17 ans continuent de plus belle à alimenter les réseaux sociaux. Selon le père de la victime, Tony LaFrance, l'élève de 12e année a brutalement été battu par deux élèves et a dû être transporté par ambulance à l'hôpital, après l'agression survenue mardi pendant l'heure du repas. Des propos déplacés au sujet de l'amie de coeur d'un des agresseurs seraient à l'origine de l'agression. La nuit suivant l'incident, l'homme n'a pas hésité à publier sur Facebook une photo de son enfant et d'y aller de sa version des faits. «Deux lâches lui ont sauté par-derrière. Ceci est un triste jour pour notre famille», a tout d'abord indiqué Tony LaFrance, qui a pour l'occasion créé la page Facebook "Please support anti bullying at our school", qui comptait déjà près de 1000 membres dimanche. La GRC a confirmé être intervenue à l'école Southern Victoria High mardi midi. Les parents de la victime ont indiqué sur Facebook que les présumés agresseurs avaient hérité d'une suspension de cinq jours d'école. Acadie Nouvelle, 9

Charges laid in theft of poppy donations
A man faces charges after poppy boxes were stolen in **Grande Prairie** gas station. RCMP were called to the business on Sunday. Corey Donald Muise, 23, is charged with theft under $5,000, possession of stolen property and failure to abide by probation orders. Grande Prairie is approximately 460 kilometres northwest of Edmonton. Postmedia Network (Edmonton Journal, A5); Edmonton Sun, A6 (2015-11-10); Global News (2015-11-09)

Bible Hill RCMP office undergoes renovations
The RCMP detachment in **Bible Hill** is getting an expansion and facelift. Work is underway on the project that will expand and upgrade the detachment at 283 Pictou Rd., consolidating in one building all units and offices in the Bible Hill area, an RCMP news release said. "By expanding and upgrading our current detachment facility, the RCMP is making a long-term commitment to policing services in the Bible Hill area and Colchester County in general," Staff Sgt. John Berry, Colchester District commander, said in the release. "This infrastructure project will also bring all RCMP resources in Bible Hill under one roof, which will enhance service delivery in the long run." In the first phase of the project, the original building will be expanded by about 1,200 square metres. The original structure will be renovated and upgraded in the second phase. When it is completed, the detachment will house eight RCMP units, including those now located in the nearby Agritech Park. Chronicle Herald (2015-11-09)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

'Our country benefits to this day'
Sgt. Gil Boone proudly participates in local Remembrance Day ceremonies each year with other members of the Cape Breton Regional Police Service. He is among 22 members of the Cape Breton Regional Police Service who have participated in 24 peacekeeping missions in places like Kosovo, Sierra Leone, Jordan and Afghanistan. Each Nov. 11, he is reminded of his own time overseas, but says his service hardly compares to what others have gone through... He said it reminded him of the quality of life back in Canada and the veterans who fought in wars to make sure that was possible. "The men and women that went over and fought for us, they did so much for us, and our country benefits from it to this day. People just don't seem to realize that." That's why he marches each year in a Remembrance Day parade. This year, he'll take part in commemorations on the Northside. The RCMP manages the deployment of Canadian police on peacekeeping missions, including planning and evaluating, selecting and training personnel and providing support throughout deployment. Cape Breton Post, A3/Front

Youth worker left alone with violent teen
A 15-year-old Charlottetown youth in the care of the province has been placed on probation for two years after he engaged in the unwanted sexual touching of a female youth worker. The youth, whose identity is protected under the provisions of the Youth Criminal Justice Act, has been ordered by the court to attend a sexual education program. He must undergo assessment, counselling and treatment for any underlying issue that might have contributed to the commission of this offence. That counselling could include sessions on sexual deviancy and anger management. Provincial Court Judge Nancy Orr ordered the accused to provide a sample of his DNA for the national DNA databank. She also imposed a weapons prohibition. Guardian, A1

'God didn't want me to die'
A Charlottetown youth who attempted to commit suicide by cop in the parking lot of the Charlottetown Mall was placed on probation Monday for two years on each of four weapons- related offences. The youth, whose identity is protected by the Youth Criminal Justice Act, had entered guilty pleas to possession of brass knuckles, using brass knuckles in a careless manner, using a firearm in a careless manner and possession of a weapon for a purpose dangerous to the public peace. The court was told the accused had drawn police to the rear parking lot of the Charlottetown Mall last Good Friday by placing a call to the authorities to say there was a man in the parking lot with a gun and shots had been fired. Multiple units were dispatched and when police arrived they spotted a figure with a gun, his face covered

with a balaclava... Orr ordered the accused to perform 25 hours of community service on each of the four charges. He must also provide a DNA sample for the national DNA databank. Guardian, A3

Drug probe hits jackpot
A Saskatchewan police investigation dubbed Project F-Jackpot has cashed in, with four arrests and 25 charges. "The objective of this investigation was to disrupt the criminal activity and dismantle the group of individuals involved in the distribution of cocaine and crystal methamphetamine in communities in the province of Saskatchewan," said a news release issued Monday. No one was available for an interview to provide further details. The bust was made by the Saskatchewan Combined Forces Special Enforcement Unit (CFSEU), a provincewide integrated policing task force targeting existing and emerging organized criminal groups. Members of the Regina CFSEU have been involved in Project FJackpot for the past two months. The investigation concerned alleged drug trafficking by a group operating "extensively" across the province, according to the release. Saskatoon CFSEU, the Regina Police Service and RCMP units in Saskatchewan's F Division were also involved in the project. It culminated in four arrests on Wednesday. James Edward Lloyd, 36, of Regina is charged with trafficking in cocaine, possession of cocaine, meth and oxycodone for the purpose of trafficking, possession of cannabis under 30 grams, possession of proceeds of crime exceeding $5,000, and six weapons charges. Postmedia News (Leader-Post, A1) (2015-11-10); Global News (2015-11-09)

Ils seront 25 000
De Harper à Trudeau, le contraste est saisissant en matière d'accueil des réfugiés. D'un gouvernement qui utilisait la sécurité comme prétexte pour ne pas agir, nous voilà devant un gouvernement déterminé à relever tout un défi: accueillir 25 000 réfugiés au Canada d'ici le 31 décembre.Un scénario à l'étude prévoit l'accueil de 6000 réfugiés syriens par semaine qui seraient hébergés dans des bases militaires comme celles de Valcartier ou de Trenton, selon des informations obtenues par Le Devoir. Une opération d'urgence d'envergure qui s'inspire du plan déployé en 1999 lors de l'arrivée des réfugiés kosovars au Canada.Est-ce réaliste d'accueillir autant de réfugiés en si peu de temps? ... A priori, 25 000 réfugiés, ça peut paraître beaucoup. En temps normal, le Canada reçoit 5700 réfugiés par année, pris en charge par l'État. Mais tout est relatif. Quand on sait que l'Allemagne recevra 800 000 demandeurs d'asile cette année, 25 000, ça semble très peu. Quand on sait aussi que des pays voisins de la Syrie, aux capacités beaucoup plus limitées que les nôtres, accueillent en ce moment la majorité des réfugiés syriens, on se dit que le Canada peut certainement faire mieux. Rappelons qu'en ce moment, 95% des Syriens fuyant la guerre civile sont recueillis par les pays limitrophes (Liban, Jordanie, Irak, Égypte et Turquie). Accueillir un grand nombre de réfugiés pose-t-il des problèmes de sécurité? C'est ce que prétendait le gouvernement Harper. Mais il faut encore rappeler qu'il est beaucoup plus difficile d'entrer au Canada comme réfugié que comme simple visiteur. Les demandeurs d'asile doivent obligatoirement se soumettre à des contrôles de sécurité très poussés de la GRC et du SCRS que les milliers de visiteurs qui débarquent au pays chaque jour n'ont pas à subir. La Presse

Arbitration gets the boot - Carstairs backs away from option to resolve expense-claim dispute
A former Manitoba senator has changed her mind about using binding arbitration to resolve her Senate expense-claim issues and will likely now face legal action. Sharon Carstairs, who left the Senate in October 2011, is one of 30 senators who were identified in June by the auditor general as having made what were deemed to be ineligible expense claims. Senators were given the option to repay the amount owing or go to binding arbitration with former Supreme Court Justice Ian Binnie. Those who don't repay and don't go to arbitration will be pursued in court... Former Liberal senators Rose-Marie Losier-Cool and Bill Rompkey and Conservatives Gerry St. Germain and Don Oliver also initially requested binding arbitration but have since rescinded that request. There are seven senators who still owe money from the audit who haven't sought binding arbitration, including former Manitoba Liberal senator Rod Zimmer, whose outstanding amount of $176,014 was the highest total for any of the senators identified in the audit. Zimmer's claims were related to his secondary residence as well as travel the auditor said didn't appear to be for Senate business, contracts without proper documentation, as well as gifts and taxi rides for Zimmer and his spouse in Ottawa for personal activities. All seven are among the nine whose files were referred to the RCMP to see if any criminal laws were broken. None of those senators has been charged. Winnipeg Free Press, A3

Un Néo-Brunswickois soupçonné d'agressions sexuelles
Un homme âgé de 61 ans du Nouveau-Brunswick, Jean-Marie Rodrigue, doit faire face à la justice pour des agressions sexuelles graves qui auraient été commises il y a quelques années au Québec. Les faits qui lui sont reprochés seraient survenus entre 1985 et 1998 en Beauce et en Montérégie. Le Service d'enquêtes régionales de la Sûreté du Québec (SQ), avec la collaboration de la Gendarmerie royale du Canada (GRC), a procédé à l'arrestation du suspect samedi à sa résidence au Nouveau-Brunswick. L'Acadie Nouvelle a contacté la SQ pour savoir à quel endroit avait eu lieu l'arrestation, mais un agent nous a répondu que cette information «n'est pas disponible». Jean-Marie Rodrigue doit comparaître à Saint-Joseph-de-Beauce relativement à ces accusations d'agressions sexuelles. L'enquête de la Sûreté du Québec tend à démontrer qu'il pourrait avoir fait d'autres victimes. Selon la sergente aux communications de la SQ, Ann Mathieu, le suspect connaissait les personnes avec lesquelles il aurait posé ces gestes à caractère sexuel. La Presse Canadienne (Acadie Nouvelle, 7) (2015-11-10); La Presse Canadienne (98,5 FM) (2015-11-09)

RCMP stymied in probe of Parliament Hill shooter's Winchester rifle
The RCMP believes it has "come to a dead end" in its probe of where Parliament Hill shooter Michael Zehaf Bibeau got his gun one of the most vexing questions about the events of Oct. 22, 2014. The Mounties continue to investigate several threads of what happened that day, including whether Zehaf Bibeau had accomplices, but have not gathered evidence sufficient for criminal charges. A source with direct knowledge of the police investigation provided the update to The Canadian Press on condition of anonymity due to the ongoing sensitivity of the file. On Wednesday, crowds will gather for Remembrance Day ceremonies at the National War Memorial, where Zehaf Bibeau killed honour guard Cpl. Nathan Cirillo, shooting him in the back three times with a .30-30 Winchester rifle. The attacker quickly made his way up Parliament Hill and into the Centre Block before being gunned down in the Hall of Honour, not far from then-prime minister Stephen Harper and countless MPs. The RCMP will honour 20 Mounties and former House of Commons security officers later this month in recognition of their bravery during the violent episode. Shortly before his attack, the gunman made a video in which he cites retaliation for Canada's military involvement in Afghanistan and Iraq as his motivation. Zehaf Bibeau, 32, plainly speaks of assaulting soldiers to show Canadians "that you're not even safe in your own land, and you gotta be careful." RCMP Commissioner Bob Paulson told a Commons committee in March that the Mounties considered Zehaf Bibeau a terrorist, and that he would have been charged with terrorism offences under the Criminal Code had he lived. Guardian (Prince Albert Daily Herald, Western Star, Telegram, Mississauga News, Brandon Sun); CTV News; Globe and Mail

Les Premières Nations somment Trudeau de passer aux actes
Le nouveau premier ministre du Canada doit passer de la parole aux actes, a sommé le chef d'Uashat mak Mani-Utenam, Mike McKenzie, qui invite Justin Trudeau sur la Côte-Nord pour qu'il constate «personnellement» la crise que vit sa communauté de 4000 âmes, après que cinq des leurs se soient enlevé la vie depuis 2015. Le chef McKenzie, appuyé du chef de l'Assemblée des Premières Nations du Québec et du Labrador (APNQL), Ghislain Picard, s'est adressé à la presse lundi, à la suite du déclenchement, vendredi, d'une enquête publique du coroner sur la mort de Nadeige Guanish, une jeune Innue qui a mis fin à ses jours le 31 octobre... Le chef revendique notamment le financement «adéquat» de la Sécurité publique de la communauté et la création d'une escouade mixte, avec la GRC, pour enrayer le problème de trafic de stupéfiants. Un meilleur soutien des programmes de prévention et l'amélioration des «corridors de services» entre les ressources autochtones et le réseau québécois sont aussi exigés. La Presse (2015-11-09)

Brandon boy, 16, faces terrorism-related charge
A 16-year-old boy in Brandon, Man., faces a terrorism charge for allegedly using social media to express support for the Islamic militant group ISIS. The teen has also been charged with one count of possessing child pornography. He appeared in court in Brandon on Monday, but the case was adjourned until Thursday because he had not secured legal counsel, said Manitoba's chief federal prosecutor Ian Mahon. The boy, who cannot be named under the Youth Criminal Justice Act, remains in custody. Mahon said he expects a bail application to be heard on Thursday. Not much is known about the boy. Brandon residents told CBC News he grew up in the western Manitoba city and is attending high school there. Mahon said items have been seized from the teen's home, including a computer that is closely being looked at. The

matter remains under investigation. Another Manitoban, Aaron Driver, was arrested in Winnipeg in June after he openly supported ISIS on Twitter. Although Driver is not accused of any crime, the RCMP is seeking to have his current bail conditions extended for a longer term, based on the suspicion that he might help or engage in terrorist activities. He appeared in court last week to fight the Mounties' attempts to limit his freedoms. Mahon, who is also the federal prosecutor in that case, had said the restrictions are "not punitive" but reasonable for public safety. CBC News (2015-11-09)

Nova Scotia man charged with possession for the purpose of trafficking in ecstasy
The Combined Forces Special Enforcement Unit — Newfoundland and Labrador (CFSEU-NL) received a complaint from Husky Energy regarding an offshore employee whom the company suspected was in possession of illegal drugs. CFSEU-NL initiated an investigation and learned the man was in possession of pills in a prescription bottle that did not match the prescription label, the RCMP stated in a news release. He was returning to work in the offshore and the pills were found during a routine inspection. The pills are suspected to be MDMA (ecstasy) and will be forwarded to Health Canada for further analysis, the RCMP stated. The Telegram (2015-11-09)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

RCMP to honour Hill terror heroes
The RCMP will give awards to 20 Mounties and former House of Commons security officers in recognition of their bravery when a gunman stormed Parliament Hill last year. The national police force will make the presentations during a private Nov. 23 ceremony at RCMP headquarters. The RCMP said the awards are intended to recognize the online post. 1.866.977.2737 "bravery, dedication and quick thinking" of those who were directly involved in the events of Oct. 22, 2014. On that day, Michael Zehaf Bibeau fatally shot honour guard Cpl. Nathan Cirillo at the National War Memorial before rushing into Parliament's Hall of Honour, where he was killed in a flurry of bullets. Former House of Commons sergeant-at-arms Kevin Vickers, now Canada's ambassador to Ireland, was lauded for his role in subduing Zehaf Bibeau, but there has been no formal recognition of others. The RCMP was responsible for the grounds of the parliamentary precinct during the attack, while House of Commons and Senate security forces had jurisdiction inside the Parliament nuildings. A now-merged parliamentary protective service manages dayto-day security on Parliament Hill, a direct consequence of Oct. 22 intended to avoid confusion. Times Colonist, A8 (Kingston Whig-Standard, London Free Press, Chronicle Herald); Postmedia News (Ottawa Citizen, A8); Agence QMI (Journal de Montréal, 18)

Remembrance Day ceremonies planned throughout region
Communities across southeastern New Brunswick will join Canadians across the country in pausing to remember those who have served the nation in uniform and those who made the ultimate sacrifice doing so. Here's a look at some of the main Remembrance Day ceremonies around our region. Moncton: Thousands will gather at the Moncton Coliseum for the largest ceremony in our region, organized by the Royal Canadian Legion Branch Number 6. The ceremony runs from 10:30 a.m. to noon, with a special Lest We Forget display open after the ceremony in the adjacent Agrena complex. As well, the Sunny Brae Legion will host a parade that will leave the legion, 164 Broadway St., at 10:40 a.m. and end at the cenotaph on Massey Avenue. If it rains, the ceremony moves to the Knights of Columbus Hall on Broadway. There is also the annual informal ceremony at the Victoria Park cenotaph - including veterans and anyone who has served as a police officer, firefighter or in the military - that will be held at 11 a.m. Dieppe: The City of Dieppe, in collaboration with the Dieppe Military Veterans Association, will be holding a ceremony on Wednesday, November 11, at École Anna-Malenfant to commemorate Remembrance Day. The parade, made up of veterans, cadets and members of the RCMP, will form up around 10:30 a.m. and will make its way indoors for the ceremony. Times & Transcript, A3

Troubled veterans lacking necessary support: critics
It was chilly March day when former master corporal Collin Fitzgerald - one of the country's most highly decorated Afghan war veterans - decided that the way he wanted to go out was in a spray of police bullets. It was, he believed at the time, the only thing he could do to wash away the pain of his crumbling marriage and to erase from his mind the faces of dead Taliban fighters that haunted him each night, every

time he closed his eyes. "I was done with life and everything," Fitzgerald told The Canadian Press. "And I cannot truly say to you what that feels like, but is a very hollow, shallow, cold place to be." He tried everything. Nothing worked. "Therapy. The alcohol had run its course, the (prescription) drugs had run their courses; I was done," he said. "You just want the pain to be done. I get it." But the fact he found the strength to go on living for his daughter, and to eventually face justice after holding police at bay for five hours at his home in Iroquois, Ont., south of Ottawa, was just the start of his nightmare. Fitzgerald soon encountered another chilling reality: that Canada's justice system often treats troubled veterans as threats to public safety. After an eight-month investigation, The Canadian Press has found that the federal government allowed key findings in the tragic shooting death of another troubled veteran with severe post traumatic stress disorder to gather dust. The B.C. coroner's office investigated the September 2012 RCMP killing of retired corporal Gregory Matters and made several recommendations to both National Defence and Veterans Affairs, including making mental-health professionals available to police emergency response teams who deal with troubled veterans. Letters obtained by CP, dated from the summer of 2014 and addressed to the coroner, show that both federal departments believe they are doing enough to reach and treat troubled military members. Canadian Press (Record, A3, Spectator, Times & Transcript, Daily Gleaner)

Help sought in shooting probe - Investigative unit seeks witnesses to Friday's events
The province's team of independent investigators is looking for witnesses as it probes a police shooting that killed a Winnipeg man Friday. Mark DiCesare, 24, died after being shot by officers near Kapyong Barracks following a police chase through River Heights around 1:15 p.m. Friday. DiCesare had been upset over a recent breakup with his girlfriend, a source told the Free Press. Whether DiCesare was armed as he led police on a chase Friday is part of the Independent Investigation Unit of Manitoba's probe, said executive director Zane Tessler... The unit is currently investigating several other cases, including the recent police shooting of 44-year-old Haki Sefa Sept. 20, the case of a stolen RCMP gun being used in a gang-related shooting that injured a teenage girl Oct. 24 and the apparent suicide of a murder suspect who shot himself after police tried to pull him over Nov. 2. Winnipeg Free Press, B1

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

NIL

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

NIL

OTHER / AUTRES

Missing man left financial quandary
Harold Backer, who has been missing since Nov. 3, may have left the country as a result of financial mismanagement that has cost his clients a considerable amount of money. The 52-year-old Backer, who is registered as an active mutual fund dealer with Investia Financial in B.C. and Ontario, was listed as missing last week by Victoria police. Some of Backer's clients, who asked to remain anonymous, told the Times Colonist it looks as though they have lost a substantial amount of money due to his actions.
It is unknown how many clients are affected. According to Canadian Securities Administrators, the umbrella group that brings together the country's various provincial securities regulators, Backer was an active dealer with Investia but under the terms and conditions of his registration he had agreed "to be closely supervised." The Mutual Fund Dealers Association did not return calls Monday to clarify what that meant. According to a spokesman, the B.C. Securities Commission cannot comment on whether a complaint has been made against a dealer or if an investigation is ongoing... On Monday, Victoria police announced they are working with U.S. law enforcement agencies to find Backer. "Both through our efforts and the fantastic support from our U.S. law enforcement partners, such as the Port Angeles Police Department, we continue to receive tips that we're working with now," said Det. Sgt. Kris Rice in a

statement. "Tips are important in a missing persons file like this and sometimes it is the smallest detail that helps." Times Colonist, A1

Opposition calls for action on fentanyl

Alberta's main opposition parties say Premier Rachel Notley's government has responded with indifference as deaths from fentanyl abuse have surged in the province and turned into a public-health crisis. Ms. Notley's New Democrats have defended their response to the fast-acting opioid by pointing to the creation of a committee to review mental health care in the province. However, members of the Wildrose and Progressive Conservative parties say resources need to be allocated immediately to overtaxed health and police services. In the first half of the year, 145 Albertans died from fentanyl... A pill of fentanyl costs about $20 on the streets of Alberta's major cities and is 50 times more potent than heroin. While the drug has been tied to prescription abuse in Eastern Canada, the variant found in the Prairies is believed to be produced by organized crime. What sets fentanyl apart from other opioids is how toxic it is - two milligrams are enough to kill the average person in less than 15 minutes. Globe and Mail, A11

Whistleblower to deliver address for Queen's

A man some people consider a hero and others believe is a criminal is to present the opening address at a Queen's University conference later this week. Edward Snowden, 32, the former Central Intelligence Agency employee and United States government contractor who leaked thousands of classified documents that revealed the extent of global surveillance programs operated by the U S. and its English-speaking allies, is to present the opening keynote speech at the Queen's International Affairs Association's Model United Nations Invitational on Thursday. The event is to include 250 student delegates from 15 schools across North America. Snowden, who has asylum in Russia, is to speak about cyber security at the conference via video link... Bill C-51, the Anti-terrorism Act 2015, broadened the authority of Canada's surveillance and law enforcement agencies by giving them more power to thwart suspected terrorist plots - not just gather information about them. Lauren Craik, president of the international affairs association and a third-year economics student, said the talk is to be tailored to the Canadian audience. Kingston Whig-Standard, A3

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 13, 2015 / le 13 novembre 2015

The Daily Media Summary can also be accessed through Newsdesk /
La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Screening for refugees ready to go, Liberals say
Some security screening will be conducted on Canadian soil as the Liberals push to bring in 25,000 Syrian refugees by the end of the year, Public Safety Minister Ralph Goodale says. Goodale told reporters that security checks on the refugees will be conducted both before and after the refugees begin arriving in Canada. "It will be a combination of both," said Goodale after a cabinet meeting Thursday. Security concerns were among the chief reasons the previous Conservative government advocated for moving slower on the refugee file - although Harper's former chief of defence staff, Rick Hillier, suggested those were overblown. Goodale said his officials assured him they can get the job done, despite the ambitious timeline. Goodale's portfolio includes CSIS, which does much of the screening work, as well as the Canada Border Services Agency and the RCMP. "My officials are satisfied that, to the extent that there are security issues, that they can be properly managed within the frame that the government is considering, and that Canada can fulfil the objective of receiving and settling 25,000 refugees in an expeditious way," Goodale said. Toronto Star, A1 (Record, Spectator) (2015-11-13); Toronto Star (Hamilton Spectator) (2015-11-12)

CONTRACT & ABORIGINAL POLICING / SERVICES DE POLICE CONTRACTUELS ET AUTOCHTONES

WINDSOR HOSPITAL ASSAULTS
The president of the **Nova Scotia** Nurses' Union wants a plan in place to protect her members after a nurse and security guards were assaulted in the Hants Community Hospital emergency room Tuesday night. Janet Hazelton says the occurrence, which resulted in minor injuries, is far from a rarity and needs to stop. There were 153 assaults on nurses by patients last year, she said. "When a violent patient comes

into (a hospital), we should have a plan. We should have security that are actually able to restrain patients if they have to." Thomas Steven Orman, 40, of no fixed address was arraigned in Kentville provincial court Thursday on charges of assault (twice spitting at a nurse), causing a disturbance and breach of a court order. Orman was a patient at the Windsor hospital. He has consented to a remand for a psychiatric assessment at the East Coast Forensic Hospital in Dartmouth. He returns to Windsor provincial court for a plea on Nov. 24. Hazelton said it took several serious incidents involving nurses in Ontario before the government there gave security the power to step in and restrain patients when necessary. "They're able to handcuff patients if they have to and they're allowed to physically take a patient down if they need to. They very seldom have to, but just the thought that they can is reassuring for the patients and for the nurses." A spokesman for the Nova Scotia health authority said security guards are trained to provide "hands-on assistance with aggressive patients, at the direction of clinical staff." At about 8 p.m. Tuesday, Windsor District RCMP responded to a complaint of a disturbance in the hospital's emergency room. The accused is known to police, provincial RCMP spokesman Const. Mark Skinner said. Prior to Tuesday night's police call, RCMP had received other calls about the man "but this is the call we had to act on," Skinner said. Hazelton said part of the problem is a reduction in services for people with behavioural issues. Group homes usually have zero tolerance for assaults on patients, she said, and so it usually means if a patient is kicked out of a home, they end up in an emergency department at a hospital where nurses and other staff aren't equipped to deal with situations when they escalate. Chronicle Herald, A1

Man pleads guilty to killing his mother

Ryan Ernest Roy has pleaded guilty to killing his mother. In Court of Queen's Bench in Woodstock Thursday morning, the 25-year-old pleaded guilty to second-degree murder of Phyllis Roy in **Peel**, a small community in the outskirts of Hartland. Roy, who was originally charged with first-degree murder, entered his guilty plea before Justice Tracey K. DeWare. Roy was scheduled to be in the Woodstock court to begin his preliminary hearing... Following the guilty plea Thursday morning, the family of Phyllis Roy released a media statement: "In March, our family was heartbroken when we lost our beloved Phyllis. Phyllis was a loving person who touched the lives of many people, especially her family and friends. We miss her every day. "It is difficult for anyone to lose a family member at any time. Our grief has been compounded by the tragic circumstances surrounding Phyllis's death. We greatly appreciate those in the community who have extended their kindness, thoughts and prayers to us during this difficult time. We want to thank the RCMP for their professionalism and compassion throughout their investigation. We also want to thank the members of the media who have respected our request for privacy as our family continues to deal with this tragedy. Daily Gleaner, A1

Prank with raft cost BC Ferries $40,000

A man who deployed a life raft and jumped overboard from a ferry in Active Pass last week cost BC Ferries $40,000, according to a company spokeswoman. Deborah Marshall says the cost was greater than a typical search and rescue mission because the life raft was damaged and had to be replaced. A young man was arrested after he allegedly jumped offa ferry, swam to **Galiano Island**, and broke into a house while naked. The RCMP is recommending criminal charges of break and enter and mischief under $5,000. Postmedia Network (Vancouver Sun, A12)

Northern Alberta man charged in wife's death

A man has been charged in the death of his common-law wife on a northern Alberta First Nation. Peter Noskey, 35, has been charged with manslaughter in connection with the death of Vicky Cardinal, 35, police said. Cardinal was transported from **Peerless Lake**, a community 235 kilometres east of Peace River, to hospital in Edmonton last Thursday. She died Sunday. An autopsy has been scheduled. Cardinal and Noskey lived together on Peerless Trout First Nation, police said. Postmedia Network (Edmonton Journal, A7)

Quesnel man promoted hatred

A **Quesnel** man charged with using his website to promote hatred against Jewish people has been found guilty by a B.C. Supreme Court jury. Roy Arthur Topham, publisher and editor of The Radical Press since 2008, had been charged with "communicating statements which wilfully promote hatred against an identifiable group." On Thursday morning, a 12-person jury in Quesnel found Topham guilty on one of two

counts of wilful promotion of hatred, Crown prosecutor Jennifer Johnston said. Johnston said she hadn't yet formulated her sentencing position, but a sentence for promoting hatred carries a maximum two years less a day in prison. Following a six-month investigation, Topham was arrested in his car in 2012 when he and his wife were leaving their property. Mounties searched and seized Topham's property after determining there were "reasonable grounds that the offence of promotion of hatred was committed." Topham's site hosts anti-Semitic texts including "The Protocols of the Learned Elders of Zion," "The Biological Jew" and "The Jewish Religion: Its Influence Today." Postmedia News (Province, A13) (2015-11-13); Prince George Citizen (2015-11-12)

Moose hunt on North Mountain suspended
Parks Canada temporarily suspended a moose hunt in the **Cape Breton Highlands National Park** following a confrontation between protesters and Mi'kmaq harvesters. Discussions are underway between Parks Canada and Mi'kmaq representatives to ensure that all necessary safety measures are in place before the controlled moose hunt resumes this fall. "Public safety for all involved remains the top concern of Parks Canada in this endeavour," said Coady Slaunwhite, Parks Canada public relations and communications officer. "We are working with RCMP and Unama'ki Institute of Natural Resources on public safety and security measures." At around 10 a.m. Wednesday, 30 protesters entered the restricted area moose harvest zone. Some proceeded to the staging area and confronted the Mi'kmaq harvesters. Parks Canada law enforcement branch personnel and RCMP responded. Slaunwhite said by 11 a.m., most of the protesters had left. Cape Breton Post, A7

Family holds Winnipeg vigil for woman found dead on First Nation
The family of a woman found dead on a remote, northern Manitoba First Nation this week gathered for a vigil at the steps of the Manitoba Legislature Thursday night. Krystal Andrews, 23, was found dead in an isolated area on **God's Lake First Nation** on Monday. RCMP are calling her death suspicious. CBC News (2015-11-13); CTV News (2015-11-12)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Shadowy Black Axe group leaves trail of tattered lives
Canadian police say they are fighting a new kind of criminal organization. The signs began to appear two years ago: photos on Facebook of men wearing odd, matching outfits. Then there were stories, even old police files, attached to the people in the photos: a kidnapping, a man run over by a car, brutal beatings over what seemed to be a small slight. Mapping a secret criminal hierarchy for the first time is a rare kind of detective work. So when two Toronto police officers and an RCMP analyst in British Columbia started documenting the existence of something called the "Black Axe, Canada Zone," they could not have predicted it would take them to funerals, suburban barbecue joints and deep into African history before they understood what they were seeing. The Black Axe is feared in Nigeria, where it originated. It is a "death cult," one expert said. Once an idealistic university fraternity, the group has been linked to decades of murders and rapes, and its members are said to swear a blood oath. Most often, the group is likened to the Mob or to biker gangs, especially as it spreads outside Nigeria. An investigation by The Globe and Mail that included interviews with about 20 people found that "Axemen," as they call themselves, are setting up chapters around the world, including in Canada. Globe and Mail, A1

Tragédie Lac-Mégantic: Tom Harding comparaît à nouveau
Il fait face cette fois à deux chefs d'accusation provenant des procureurs de la Couronne fédérale, à la suite de l'enquête menée par le Bureau de la sécurité dans les transports (BST), Transports Canada, la Sûreté du Québec (SQ) et la Gendarmerie Royale du Canada (GRC), un premier relatif à la Loi sur la sécurité ferroviaire, en rapport avec la tragédie elle-même, et un deuxième concernant la Loi sur les pêches et l'environnement, à la suite de la pollution du lac Mégantic. M. Harding a comparu devant le juge Paul Dunnigan, de la Cour du Québec. L'homme n'a pas eu à témoigner et est resté imperturbable. Il était le seul accusé présent, même si six autres personnes reliées à la MMA devaient aussi comparaître, soit Robert Grindrod, président de la MMA et résidant du Maine, Jean Demaître, directeur des opérations au Canada, Michael Horan, directeur adjoint aux opérations à Farnham, Lynne Labonté, directrice

générale des opérations de transport, Richard Labrie, contremaître, et Kenneth Strout, directeur des pratiques d'exportation. La Presse (La Tribune, 30); 1

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Trudeau troublé que la GRC ait voulu espionner des journalistes de La Presse
Le premier ministre Justin Trudeau juge troublantes les informations voulant que des policiers de la Gendarmerie royale du Canada aient voulu espionner les déplacements et appels téléphoniques d'un journaliste de *La Presse* pour démasquer la source qui lui avait fourni des informations sur les plans terroristes attribués à Adil Charkaoui. Estimant que la liberté de la presse fait partie des fondements d'une saine démocratie, M. Trudeau a aussi indiqué que son gouvernement examine scrupuleusement cette affaire afin de déterminer s'il y a des correctifs qui doivent être apportés. En point de presse hier à l'issue d'une réunion de son cabinet, M. Trudeau a affirmé qu'il défendrait avec énergie la liberté de la presse en tant que premier ministre. « J'ai toujours reconnu le principe et la valeur de la liberté de la presse. Une presse forte et indépendante est un fondement important d'une démocratie forte et en santé. » - Justin Trudeau « Les questions que vous soulevez feront l'objet d'un examen. Il est important de s'assurer que nous avons une presse forte et libre qui est capable de faire son travail. C'est ce que j'appuie », a affirmé M. Trudeau en réponse à une question d'une journaliste du quotidien *Toronto Star*. En français, M. Trudeau a ajouté : « Je sais que la presse joue un rôle extrêmement important dans le bon fonctionnement de notre démocratie et de toute démocratie. Je continue de vouloir défendre la liberté de la presse. « Évidemment, sur ces enjeux troublants, j'attends d'en savoir un peu plus. Mais vous pouvez être assurés que la liberté de la presse en est une que je prends très au sérieux. » La Presse, 13; Canadian Press (Times Colonist, B7, Daily Gleaner, Times & Transcript); Weekly Standard (2015-11-13); Toronto Star, A4; La Presse (2015-11-12)

3 Mounties hurt, 3 cruisers damaged during wild escape attempt
Two suspects are facing a slew of charges following a wild escape attempt through Kimberly, B.C. that left three Mounties injured and three RCMP vehicles badly damaged early Thursday morning. Authorities said the incident started while an officer was responding to a theft at a local golf course around 2 a.m. He was speaking with a security guard when a truck suddenly rammed his cruiser and took off. On its way out, the truck – which the RCMP determined was stolen – also allegedly struck a second police car that was headed to the scene. "The two police cars were able to follow it down into our downtown core," Cpl. Chris Newel told CTV News. "The suspect vehicle stopped very quickly, shoved it into reverse, and smashed into the front-end of [one of the cruisers]." Shortly after, the driver of the stolen truck allegedly lost control of the vehicle and struck a storefront – but still managed to drive off once again. Newel said the truck headed to a local ski hill next, where the officers managed to corner it, only to be rammed once again. At that point, one of the cruisers was so badly damaged it was inoperable, but another RCMP vehicle from the neighbouring detachment in Cranbrook arrived to assist in the pursuit. The stolen truck was ultimately surrounded and stopped at the ski hill's maintenance yard, but the RCMP said two suspects bolted on foot before finally being placed under arrest a short distance away. Newel said the suspects are facing "a multitude of charges," including possession of stolen property, dangerous operation of a vehicle, resisting arrest, assault, and theft. It's unclear how much it will cost to clean up the damage from the chaotic incident. "We've got three vehicles that have been probably destroyed in this incident… and some injuries to a few of our officers which, fortunately, are not serious," Newel said. The RCMP said two of the officers involved suffered back injuries and another sustained an injury to his eye. CTV News

Mounties apologize for handling of verbal racist attack
Two years after being subjected to a racist tirade by an unruly passenger a Calgary cab driver has received an apology. The apology to Sardar Qayyum comes from the RCMP, which reviewed how the verbal assault in November 2013 was handled. A video from the cab's dashcam became public last summer and shows a front-seat taxi passenger using racial slurs and telling the driver to go back to where he came from. He also implied the driver was involved in terrorism. An RCMP officer got the passenger to pay Qayyum for breaking his camera, but there were no criminal charges. Canadian Press

(Cape Breton Post, A10, Guardian); Canadian Press (National Post, A6, Calgary Herald, Edmonton Journal); Calgary Sun, A3 (2015-11-13); Calgary Herald (2015-11-12)

Man who stole cruiser caught near Thorsby
RCMP have arrested a 26-year-old man who escaped custody by stealing a police cruiser near Thorsby late last month. Jason McGinn was captured Sunday in Rocky Mountain House, police said. He escaped Oct. 26 while being transferred from Thorsby RCMP to Drayton Valley RCMP about 9 a.m. He jumped into the driver's seat of a marked RCMP car and drove away. The car was discovered a short time later abandoned near Warburg. Nothing had been removed from the car. As a precaution, there was a lockdown at Warburg School while RCMP searched the area. McGinn is expected in court in Thorsby Nov. 17 to faces 10 charges connected to his escape, including dangerous operation of a motor vehicle, assault with a weapon, mischief, escaping lawful custody, theft over $5,000 and breach of recognizance. He was originally in custody on charges of personation, possession of stolen property, driving while prohibited and many charges related to violating probation. He was to appear in court in Rocky Mountain House Nov. 18 to face this set of charges. Thorsby is 70 kilometres southwest of Edmonton. Postmedia Network (Edmonton Journal, A2); Edmonton Sun, A7; Red Deer Advocate, A3 (2015-11-13); CTV News; Global News; Edmonton Journal (2015-11-12)

Case of Edmonton man ticketed for anti-Harper sign going to higher court
An Edmonton man who was issued a $543 fine for putting a sign in his car window with an expletive aimed at former prime minister Stephen Harper says his case is being bumped up to provincial court. Rob Wells made an appearance in traffic court on Thursday, where he served notice of his intent to file a constitutional argument against the stunting ticket. He had been pulled over last August by an RCMP officer just south of Edmonton and was told to remove the sign but refused, saying it was a political statement and he had a right to have it in his window. At the time, RCMP Sgt. Josee Valiquette wouldn't comment on the sign and said police stopped Wells after receiving two complaints about erratic driving. The case was put over to Nov. 27, when Wells will appear before a provincial court judge and a later court date will likely be set. Wells devised the handmade, pink "F--k Harper" sign to voice his contempt for Harper's Conservative government. He said although some motorists gave him the thumbs up of approval, in Alberta he got more than a few birds flipped at him, including one woman who he said filed an official complaint with RCMP. CTV News

Lawyer in civil suit seeking toxicology, autopsy, ballistic reports
A lawyer representing the partner of a Tracadie man shot and killed by Bathurst Police is seeking toxicology, autopsy, scene reconstruction and ballistic reports into his death. Last July, Annick Basque launched a civil suit against the City of Bathurst and its police force following the death of her common-law partner, 51-year-old Michel Vienneau, who was killed last January. A motion to receive documents pertaining to the case was heard in French before Judge Larry Landry in the Court of Queen's Bench at the Bathurst courthouse on Nov. 12. Neither Basque nor anyone representing the city appeared in court on Nov. 12. Basque's lawyer, Charles L. LeBlanc, explained why he felt the documents should be released to him. The documents he seeks are a toxicology and autopsy report on Vienneau and a copy of RCMP documents on the case including scene reconstruction and the ballistic report. Maya Hamoud, counsel for the attorney general of New Brunswick, and Catherine McIntyre, counsel for the Department of Justice of Canada, presented their points as to why the documents should not be released. One of the reasons sited by Hamou is the possibility of interfering with a criminal case if charges are laid by the Public Prosecution Services of New Brunswick. The New Brunswick prosecution office is looking into Vienneau's death following the completion of an investigation by Nova Scotia RCMP last July. The RCMP investigated to determine if any criminal charges should be laid in Vienneau's death. Police will not reveal their findings to the public. Telegraph-Journal, A5

Affaire Vienneau
Les procureurs généraux du Canada et du Nouveau-Brunswick refusent de dévoiler, pour l'instant, le rapport indépendant de la GRC sur la mort de Michel Vienneau, abattu par un policier il y a dix mois, de même que les dossiers d'autopsie et de toxicologie. Ils invoquent qu'une divulgation prématurée pourrait nuire à d'éventuelles accusations criminelles et à un procès. Dans le cadre de sa poursuite civile contre la Ville de Bathurst, la compagne de la victime, Annick Basque, demande que ces rapports lui soient

fournis, en vertu d'une ordonnance du tribunal. La motion a été débattue en Cour du Banc de la Reine de Bathurst, jeudi matin. Au nom de la GRC, le procureur général du Canada affirme que l'inspecteur Larry Wilson, qui a mené l'enquête sur les circonstances du drame, collabore toujours avec le service des poursuites publiques du Nouveau-Brunswick quant à de possibles accusations au criminel. «Notre inquiétude est que la divulgation des documents demandés pourrait nuire à la poursuite criminelle. Nous ne disons pas que les documents pertinents ne seront pas divulgués, mais que nous ne pouvons pas le faire maintenant», a expliqué Me Catherine McIntyre au juge Larry Landry. Acadie Nouvelle, 2

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

NIL

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

In search of a better way
An opinion piece by a former soldier states ''It was chilly March day when former master corporal Collin Fitzgerald - one of the country's most highly decorated Afghan war veterans - decided that the way he wanted to go out was in a spray of police bullets. It was, he believed at the time, the only thing he could do to wash away the pain of his crumbling marriage and to erase from his mind the faces of dead Taliban fighters that haunted him each night, every time he closed his eyes. "I was done with life and everything," Fitzgerald told The Canadian Press. "And I cannot truly say to you what that feels like, but is a very hollow, shallow, cold place to be." He tried everything. Nothing worked. "Therapy. The alcohol had run its course, the [prescription] drugs had run their courses; I was done," he said. "You just want the pain to be done. I get it." But the fact he found the strength to go on living for his daughter, and to eventually face justice after holding police at bay for five hours at his home in Iroquois, Ont., south of Ottawa, was just the start of his nightmare. Fitzgerald soon encountered another chilling reality: that Canada's justice system often treats troubled veterans as threats to public safety. After an eight-month investigation, The Canadian Press has found that the federal government allowed key findings in the tragic shooting death of another troubled veteran with severe post traumatic stress disorder to gather dust. The B.C. coroner's office investigated the September 2012 RCMP killing of retired corporal Gregory Matters and made several recommendations to both National Defence and Veterans Affairs, including making mental-health professionals available to police emergency response teams who deal with troubled veterans.'' Canadian Press (Times Colonist, C1/Front)

OTHER / AUTRES

Experts defend 'big data' spying
Federal security agencies risk being overwhelmed by threats - or failing to even foresee them - unless they embrace the digital-age phenomenon of big-data crunching, warns an internal Public Safety Canada presentation. With billions of people using mobile phones and surfing the Internet, security officials are preoccupied with getting timely access to valuable information. But the recent past is littered with challenges related to information sharing and privacy, including controversy over the Conservative omnibus bill known as C-51, the presentation notes. Officials acknowledge the public might not trust government to respect privacy in the process, pointing to revelations by former U.S. spy contractor Edward Snowden about widespread surveillance of communications. "Canadians are increasingly concerned about issues of crime and terrorism, but in the post-Snowden era, public concerns about government data use may stand as a barrier to the effective use of innovative data analytics by law enforcement and security organizations," the presentation says. Big data analytics generally refers to the process of gathering and systematically sifting through millions or even billions of pieces of data - numbers, text, graphics, videos and sensor information - to glean insights that can't be detected through standard methods. Canadian Press (Toronto Star, A12, Times & Transcript, Daily Gleaner, Telegraph-Journal, Ottawa Sun, Chronicle Herald)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
January 20 2016 / le 20 janvier 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Mounties sent to help authorities in Burkina Faso
RCMP officers have been dispatched to Burkina Faso to help local authorities after more than two dozen people - including six Canadians - were killed in a terrorist attack. A government official, speaking on condition of anonymity, says the Mounties will assist officials with victim identification and paperwork so the bodies of Canadian victims can be returned home. Six Quebecers on a humanitarian mission were killed in Burkina Faso's capital of Ouagadougou last week during an attack carried out by al-Qaida. Four of the dead were from the same family: Yves Carrier, his wife Gladys Chamberland, their adult son Charlelie Carrier and Yves' adult daughter, Maude Carrier. Adam Barratt, a spokesman for Foreign Affairs Minister Stephane Dion, says the department's priority is the families of the victims. He says departmental resources in Ottawa and overseas will be used to help repatriate the victims as fast as possible. Postmedia Network (Chorincile Herald, A9, Red Deer Advocate, Guardian, Edmonton Sun, Calgary Sun, Times Colonist, Winnipeg Sun, Ottawa Sun, Times and Transcript); Journal Montreal, 13; Gazette, A3; Journal Quebec, 7

CONTRACT & ABORIGINAL POLICING / SERVICES DE POLICE CONTRACTUELS ET AUTOCHTONES

Crime Stoppers plays vital role
If you were driving past the **Lunenburg County** RCMP detachment in Cookville during the late afternoon of Jan. 8 you may have seen two hardened criminals being apprehended by detachment staff. You may also have seen those same criminals, in handcuffs and leg irons with ball and chains hampering their walking, being forced to raise the Crime Stoppers flag on the flag pole in front of the RCMP detachment. January is National Crime Stoppers Month and those two hardened criminals, Fenton Dibbin and Marlene

Mercer, are volunteers with Lunenburg County Crime Stoppers. This month, several of the volunteers with the local organization will be at retail locations in the county promoting Crime Stoppers and the work that the organization does to support local police officers in their work. Crime Stoppers is a non-profit organization that combines the public, media and police in a crime-solving effort. The simple premise of the program is to use the media to ask the public to get involved in assisting the police by identifying suspects involved in criminal activities. It is funded by donations from the public, service groups, organizations and through fund raising initiatives, emanating from the board of directors of local Crime Stoppers chapters. Postmedia Network (Chroncile Herald, S4)

Saisie de drogue à Shippagan

Deux femmes de **Shippagan**, âgées de 47 et 50 ans, ont été arrêtées à la suite de l'exécution d'un mandat de perquisition dans un appartement de Shippagan. Vendredi, vers 19 h, des agents du District du Nord-Est de la GRC, assistés par des membres de la Section de la réduction de la criminalité et de la Section des chiens policiers, ont exécuté un mandat de perquisition à Shippagan. La GRC annonce que les agents ont saisi de la marijuana, de la méthamphétamine, de la cocaïne, des produits du tabac non estampillés, de l'argent ainsi que des instruments pour l'utilisation de drogues illicites. Les femmes ont été libérées, mais devront comparaître en cour provinciale ultérieurement. Acadie Nouvelle, 7

Sex assault charge dropped against cabbie

An **Antigonish** cab driver has had one of two sexual assault charges against him dropped. William Roger MacLellan was charged in November 2014 for allegedly, on two separate occasions, groping highly intoxicated young women who took his cab home from Piper's Pub to their dorms at St. Francis Xavier University. "I've reviewed the evidence," Crown attorney Darlene Oko told Judge Laurel Halfpenny-MacQuarrie during the third day of MacLellan's trial in Antigonish provincial court. "I do not believe the court could convict him on that charge." The dropped charge stems from an alleged incident during the early-morning hours of Feb. 15, 2014, when an underage St. F.X. student claimed a cab driver had groped her breasts. The woman admitted during her testimony last October that she was drunk to the point of blacking out during the alleged assault and that she never looked at the driver and could only identify him by his voice. Testimony by RCMP officers on Tuesday focused on the remaining sexual assault charge. (...) "My cab driver molested me," the alleged victim told the 911 operator. In the background, a man could be heard telling her that she had fallen and hit her head at the pub. "That's Roger (MacLellan)," RCMP lead investigator Const. Catherine Bezaire told the court. "I know his voice." Bezaire was one of three RCMP officers who testified Tuesday to the events of Oct. 19, from responding to the St. F.X. dorm where the heavily intoxicated victim was surrounded by a growing crowd of concerned passersby, to taking her statement and searching for a dark green van driven by a non-white male. Postmedia Network (Chronicle Herald, A4)

Trial on hold over photo issue

The trial of a man charged with several sex-related and child pornography crimes had to be delayed Tuesday because some of the images in the disclosure package had not been altered to render them non-pornographic. Crown attorney Bob Morrison told Judge Alan Tufts in **Kentville** provincial court that he received a compact disc of material from the RCMP's technical crime unit Monday but found that some of the images had mistakenly not been altered. Without that, the Crown couldn't provide the disclosure package to the defence without committing the crime of distributing child pornography. The information within the package included images from a phone seized as part of the police investigation. Morrison said after court that only a few of the images were mistakenly not altered. He said there were hundreds of images that police were dealing with in the case. Robin Lee Spidle, 24, is charged with sexual touching of a minor under the age of 16, invitation to sexual touching, sexual assault, possession of child pornography, and communicating with a person under the age of 18 for the purpose of obtaining sexual services.Postmedia Network (Chronicle Herald, A7)

Lawyer lands discharge for angler caught with pot at border

A New Jersey man avoided a criminal record on Tuesday for entering Canada with 14 grams of marijuana in his vehicle last year. However, Matthew Simonelli has likely earned himself trouble crossing the border, Judge Henrik Tonning noted in **Saint John** provincial court. The judge accepted the arguments from defence counsel Charles Bryant to grant the 30-year-old, Toms River, N.J., native an absolute discharge

for possession of marijuana at St. Stephen on Sept. 9. Simonelli did not attend court, but Bryant entered a plea of guilty on his behalf. Federal Crown prosecutor Peter Thorn related in court that Simonelli and his wife crossed the border at St. Stephen and declared two expensive bamboo fishing rods. The Canada Border Services Agency officer discovered that one Ryan Mockler tried to bring these same rods into the country earlier but he was deemed inadmissible to Canada, Thorn said. Border agents searched Simonelli's vehicle and found the marijuana plus $600 U.S. in a black shoulder bag, the prosecutor said. The agents investigated further and found messages on Simonelli's cellphone "that made a reference to other drugs and pills being contained in a container or cooler," Thorn said. The border guards searched the vehicle but found nothing, Thorn said. The agents issued a civil penalty of $250 and turned the matter over to the RCMP. "There was no nefarious intent. There was no smuggling operation," Bryant said. Postmedia Network (Telegraph-Journal, B2)

Driver unaware of fatal strike on senior

Oceanside RCMP believe they have found the driver involved in a Jan. 13 incident that killed an 80-yearold woman in French Creek. Based on evidence from the scene and witness accounts, police believe a commercial truck driver unknowingly hit the woman with a piece of equipment that was sticking out from the side of the vehicle. The woman was found lying on the side of the road a short distance from her home. She was taken to Nanaimo Regional General Hospital and then airlifted to Victoria General Hospital, where she died from head trauma. Speed or alcohol do not appear to have been factors. Police said the driver is very upset and is co-operating fully. Postmedia Network (Times Colonist, A4)

Mounties arrest man after tires slashed on four RCMP cruisers

An RCMP detachment east of **Edmonton** has been going through a lot of tires. Mounties say they have arrested a man after the tires of four police cruisers were slashed at the Vegreville detachment earlier this month. Jason Larry Kotowich, who is 35, has been charged with three counts of mischief under $5,000, resisting arrest and breaching a probation order. Postmedia Network (Red Deer Advocate, A3)

Death toll from fentanyl in Calgary exceeds fatal crashes, homicides combined

More **Calgarians** lost their lives to fentanyl overdoses last year than to homicide and fatal traffic collisions combined. It will be several months yet before the final number of fentanyl-related deaths in the city for the year are made public, but it was 74 from January 2015 through to the end of September. For all of 2015 there were 34 homicides and 23 fatal traffic collisions. Staff Sgt. Martin Schiavetta says it's showing no signs of slowing down. CalgarySun.com (2016-01-19)

Sexist signs cause stir on social media

A Prince Edward Island garage manager says he has received a death threat because of a promotional sign branded "sexist and misogynistic" by some angry commenters on social media. "Women are like snowflakes. They can't drive," read the sign outside Mellish Motors in New Annan, P.E.I., a rural community just outside of Summerside, P.E.I. John Mellish, 55, and his wife say they started the business nine years ago and post a new lighthearted message to the board every Sunday. "We've always had something funny or a topic of local conversation on our sign. I've poked fun at myself, my wife, overweight people. We've been brutal to some male people. " Because of social media, this morning at 6:45 a.m., a person phoned and threatened to shoot me. I reported it to the local RCMP because I think that person needs a little bit of help if an issue like this is touching them that bad." Local residents, commenting on Facebook, backed the business for its humorous messages. Some can remember phrases on the board from last February. Toronto Star, A3

Ambulance joyride ends in charges against patient

A 21-year-old woman has been charged with dangerous driving and theft after she allegedly stole an ambulance from the Royal Alexandra Hospital Tuesday and took it on a 40-minute joyride to Duffield. The woman, a patient at the hospital, gained access to a secure ambulance bay on the east side of the central **Edmonton** hospital and made off with the vehicle at about 6 a.m., ramming it through a glassand-steel garage door on 102nd Street north of Kingsway Avenue, said Dave Weiss, executive director for emergency medical services in the north zone. The keys were in the ignition, he said. Edmonton police pursued the vehicle, tracking it using its onboard GPS system, west through Edmonton and along Highway 16 into Parkland County. The RCMP managed to stop the ambulance and arrested the woman

without incident at about 6:40 a.m. near Range Road 32 and Highway 16 in Duffield. No injuries were reported, police said. Edmonton Journal, A1

Charge laid, but cold case remains open

It took 30 years for a murder charge to be laid in the death of an elderly **Interlake** man, and RCMP still don't consider the case solved, delaying closure for the family of two men who took polygraph tests in an attempt to prove their innocence. Four months ago, RCMP laid a second-degree murder charge against Lee Norman Pischke, 50, of the RM of Grahamdale, in the death of 80-year-old Michael Kalanza, who went missing in 1985. Police also arrested a 53-year-old Winnipeg man but let him go without laying criminal charges. At the time, Manitoba RCMP said investigators believed the two were the only ones responsible for Kalanza's death. Police said the 53-year-old Winnipeg man is still not facing charges and the investigation remains open. "We are continuing on vigorously to ensure that all persons involved are held accountable for this murder," an RCMP spokesman said in an emailed statement. "To this end, we would ask that anyone with information regarding the murder of Mike Kalanza call the historical case unit tip line at 204-984-6447 or call Crime Stoppers anonymously at 1-800-222-8477." RCMP couldn't release any other details about the ongoing investigation, which has spanned three decades. The lack of closure doesn't sit well with Pischke's uncle, 67-year-old Dennis Pischke. Winnipeg Free Press, B2

RATS, In gang culture, those who talk to cops are the worst form of life

But a former Mafia associate and a senior RCMP interviewer say it's becoming much more acceptable to violate the code of the underworld and co-operate with police. Former **New York** mobster Lou Ferrante still remembers the day in 1991 that he heard the shocking news that Salvatore (Sammy the Bull) Gravano had betrayed the Gambino family and was going to testify against John Gotti Sr. "When Sammy the Bull became a rat, none of us believed it. I was the first to say: 'no way'. And a few people said, 'yeah, it's true. It's happening,'" Ferrante recalled in a recent interview. The underworld perception of ratting has percolated through other gangs as well - including B.C. groups like the Red Scorpions and United Nations. The late gangster Bal Buttar once told The Vancouver Sun he was involved in several murders, but would never help police. "I've never in my life been a rat and I'll never be one," Buttar said. Ferrante, who left the Mafia while serving an eight-year prison sentence, thinks Gravano's deal to turn on the powerful Mob boss changed the underworld perception of rats. Breaking omerta - the code of silence ingrained in Mafia culture - was considered the worst offence, more odious than murder, and punishable by death. But then came a string of American cases where powerful mobsters like Gravano struck deals to testify. Some wrote books and became celebrities. "Now I understand there are a lot of rats, not to name names, that are walking around in Howard Beach and in Brooklyn and no one's doing anything to them, so I think the whole culture has changed," said Ferrante, who turned his life around without ever co-operating with police. He has written three books, including Unlocked: The Life and Crimes of a Mafia Insider. Postmedia Network (Vancouver Sun, A1)

RCMP defend handling of root beer incident

RCMP officers believed a man was obstructing a liquor offence investigation when he refused to comply with their instructions. Const. Robert Andrew Scott Burchett, 50, and Cpl. Kevin Roger Lee Halwa, 42, both testified Monday as to why they applied the force they did on Levi Desjarlais on the evening of Aug. 20, 2011. Desjarlais has filed a lawsuit against Halwa, Burchett and Cpl. Dean Allan Purcka, 41, for the alleged assault that followed. The three RCMP officers also face assault charges. Desjarlais said he was pepper-sprayed, kneed in the groin and beaten during the altercation. "If you obstruct the police, sometimes bad things happen," said Burchett during his testimony. Burchett and Purcka were in Sylvan Lake that evening on overtime from other detachments. In the summer, the **Sylvan Lake** RCMP are provided extra money from the town to increase the police presence for the summer rowdiness. Burchett was driving in a dark blue unmarked prisoner van. He saw Desjarlais walking on the sidewalk holding what he believed at the time to be a bottle of beer. Later, Burchett would learn it was in fact root beer. Throughout direct and cross examination, Burchett said he thought Desjarlais held a beer during the incident. Postmedia Network (Red Deer Advocate, A1)

La GRC appelle à la vigilance dans une affaire de fraudeurs agressifs

Des fraudeurs sophistiqués et agressifs qui se font passer pour des employés de l'Agence du revenu du Canada visent des **Néo-Brunswickois**. La GRC dit avoir reçu plus de 100 plaintes au cours du dernier

mois. Alors que la saison des impôts approche, la GRC demande aux Néo-Brunswickois d'être sur leurs gardes contre des escrocs qui se font passer pour des employés de l'Agence du revenu du Canada (ARC). Équipés d'outils qui leur permettent d'afficher un numéro de l'ARC ou de la GRC, les fraudeurs demandent à leurs victimes potentielles de rembourser de l'impôt impayé. Avec un accent étranger, ils parlent d'un ton agressif et menacent de se rendre à la maison de leurs victimes si elles ne leur donnent pas immédiatement de l'argent par carte de crédit ou par Western Union. La fraude est répandue à travers le pays. Lundi, la GRC de l'Ontario a publié la transcription d'un échange entre un arnaqueur et sa victime dans laquelle le faux employé de l'ARC menace de faire sauter la maison de son interlocuteur (voir encadré). Acadie Nouvelle

Wig-wearing robbery suspect arrested
Police in **Surrey** said they have arrested a suspect after a man robbed a bank last month wearing an odd disguise. RCMP said they arrested a 39-year-old resident of Surrey after asking for the public's help in identifying the man following a heist near the Guildford Town Centre on Dec. 29. Police said the suspect was wearing a patterned dress, white wool sweater, a long blond curly wig and a pink tuque that partially obscured his face. Postmedia Network (Times Colonist, A2, Vancouver Sun)

RCMP searching for alleged attempted murder suspect
Police are still looking for a **Grand Rapids** man wanted for an alleged attempted murder last month. Manitoba RCMP say Alex Sanderson, 22, is considered armed and dangerous. He's wanted in connection with a Dec. 11 shooting and stabbing in Grand Rapids that left two victims with non-life-threatening injuries. Police believe Sanderson may be in Winnipeg, Brandon, Grand Rapids or Easterville and urge the public to call 911 or their local police if they see him. Winnipeg Free Press; CTV News (2016-01-19)

La police saisit 1,4 kg de cocaïne
Après avoir entamé une enquête en août 2015, des membres de l'Unité de crimes de la rue de la Force policière de **Saint-Jean** ont procédé vendredi soir à l'arrestation de deux individus et à une importante saisie de stupéfiant. Vers 22 h 15, des membres de la police régionale de Kennebecasis, de la GRC et de la Force policière de Saint-Jean ont arrêté un véhicule automobile circulant sur la route 7 en direction de Saint-Jean. Une fouille du véhicule a permis la découverte à bord d'environ 1391 grammes de cocaïne, dont la valeur de revente dans les rues de Saint-Jean peut aisément atteindre 139 000$. Les policiers ont également mis la main sur une somme de 3700 $ en argent. L'Acadie Nouvelle, 9

Seven charged in Muskowekwan home invasion
Mounties are hunting for three men after a violent home invasion on a **Saskatchewan** First Nation. Police say it happened Monday night at a home on the Muskowekwan First Nation, about 140 kilometres northeast of Regina. RCMP say seven people in disguise forced their way into the home with steel bars, baseball bats and a firearm. The six adults and two children were in the home at the time. Leader-Post; CBC News (2016-01-19)

Nunavut RCMP investigate stabbing in Pangnirtung - 22-year-old man medevaced to Iqaluit
RCMP are looking for a suspect after a 22-year-old man was stabbed in **Pangnirtung**, Nunavut, on Saturday. Police say the man was outside his home when he was stabbed. He was medevaced to Iqaluit, where he's being treated for non-life-threatening injuries. CBC News (2016-01-19)

Medical marijuana grow ups raided
On Jan. 13, Comox Valley RCMP Drug Section and General Investigation Section executed three search warrants in relation to licenced medicinal marijuana grow operations in the **Comox Valley**. Warrants were executed at a residence in Courtenay and at licenced marijuana operations in both Cumberland and Black Creek. A total of 423 plants were seized, as well as several vehicles including a motorhome, three motorcycles, a snowmobile, two automobiles and a boat, which are believed to have been purchased with proceeds of crime. ComoxValleyRecord.com (2016-01-19)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Burkina Faso Attacks: RCMP Dispatched After 6 Canadians Killed
RCMP officers have been dispatched to Burkina Faso to help local authorities after more than two dozen people — including six Canadians — were killed in a terrorist attack. A government official, speaking on condition of anonymity, says the Mounties will assist officials with victim identification and paperwork so the bodies of Canadian victims can be returned home. Six Quebecers on a humanitarian mission were killed in Burkina Faso's capital of Ouagadougou last week during an attack carried out by al-Qaida. Canadian Press (Huffington Post); Québec Hebdo; CBC News; La Presse Canadienne (L'actualité); Canadian Press (Globe and Mail) JournaldeMontréal.com (2016-01-19)

What, if anything, should Canada do after Burkina Faso? Your reactions
A senior Canadian government official told CBC News that RCMP officers have been sent to Burkina Faso to "help in whatever way they can." They will be repatriating the bodies of the six Canadians killed in last weekend's attack on a popular hotel and a cafe in Ouagadougou. Government officials, including Prime Minister Justin Trudeau, have condemned the attacks, while interim Conservative Leader Rona Ambrose used the attacks to criticize Trudeau for not doing enough to fight terrorism. We posed the question to you: what do you think of Canada's response to the Burkina Faso attacks? How should we respond? You weighed in via the discussion on CBC Forum, our new attempt to encourage a different kind of conversation on our website. Here are some of the most insightful, passionate and engaging comments we received during that discussion. CBC.ca (2016-01-19)

Weighing our privacy against security
With a spike in terrorism over the past 15 years, governments around the world have moved to enhance border security. At first it was seen in more flight security and stricter travel laws but with advances in computer technologies security agencies have turned their attention toward spying on their own citizens. Agencies like the NSA have inserted themselves into the homes of almost every U.S. family, and even share data with other countries. In light of revelations into just how widespread government surveillance is, thanks to whistleblowers like Edward Snowden, a global debate has erupted on the ethical implications. Do governments have the right to collect data on their own citizens without their consent? And should personal freedoms like privacy be sacrificed in the name of security? (...)As one who has expressed grave concern in the past about the anti-terrorism legislation enacted by the previous government, I have to point out that the expectation of privacy for citizens and residents of Canada is not the same for visitors, nor should it be. There are very different standards. In our haste to undo the covert and immoral surveillance of people going about their everyday business, we should not lose sight of the legitimate expectations of Canadians to be secure from outside threats. Entry to Canada is precisely when we should employ due diligence. (...)The RCMP must either prove the allegations against Ayaan Farah or apologize and get her employer to rehire her. Toronto Star, A12

Terror charge dropped but still no passport
Nearly two years after a court stayed charges against Mouna Diab, who had been accused of smuggling arms parts to the terror group Hezbollah, the government is still balking at granting her a passport. The National Post has learned that Diab, 30, filed a motion with the Federal Court last month, claiming Ottawa is infringing her Charter rights by refusing to act on a passport application she made in June 2014. The passport application came after the Crown abruptly dropped charges against Diab, who was arrested at Montreal's Trudeau airport in 2011. A native of Lebanon, Diab emigrated to Canada in 1993 as a seven-year-old and gained Canadian citizenship two years later. When she was charged with committing a crime for the benefit of a terrorist group, the Royal Canadian Mounted Police issued a news release alleging she was "acting under the direction of a contact person in Lebanon who is associated with Hezbollah." She faced a second charge of violating a United Nations arms embargo of Lebanon. But on April 17, 2014, a federal prosecutor requested a stay of proceedings, declaring in a brief statement that "there was no longer a reasonable prospect of conviction." Her passport had been revoked following her arrest. When she applied for a new one she was told her request required "a second level of examination" and would not be processed within the standard time. Her lawyer, Richard Prihoda, said she was interviewed for 90 minutes by two Passport Canada agents in October 2014 and was told a decision was

imminent. "Everybody keeps saying a decision is going to come soon, but here we are almost two years later, and nothing has been done," he said. He would not speculate on why her application is being held up, but described her arrest and the subsequent charges as "a tempest in a teapot." The federal attorney general has declared its intention to oppose Diab's request for a court order requiring the Department of Citizenship and Immigration to act on her application. The department would not comment when asked why Diab's passport application has been delayed. "As the matter is before the court, it would be inappropriate to comment," department spokeswoman Jessica Seguin said. This would not be the first time the government has used its passport powers against people who have come under RCMP scrutiny. The government has had the power to refuse or revoke passports on security grounds since 2004. The section was used to deny a passport to Fateh Kamel, who returned to Canada after serving prison time in France for terrorism-related offences. In 2014, Ali Sbeiti, an Iranian-trained Montreal imam, had his passport revoked and was informed he was a "subject of interest" in an RCMP national security investigation. National Post, A5

We can't go backwards on terrorism

If charity begins at home, so does national security - specifi cally at the House of Commons. Prime Minister Justin Trudeau is advised to remember this in the upcoming weeks, as Parliament resumes sitting and he has to decide whether the security measures of the previous Conservative government are too strong, too weak or just right. You know Trudeau has never discovered a security or defence scenario he considers too weak. He hypocritically voted for the Tory Anti-Terrorism Bill (C-51) while in Opposition because if there is anything Trudeau understands it is optics. With terrorist attacks, including a recent assault on Parliament Hill by an ISILinspired, lone-wolf fanatic named Michael Zehaf Bibeau, in everyone's mind, Trudeau reasoned (or at least received the correct advice) that he had better not appear too soft on terrorism with an election around the corner. Incredibly, the nattering Trudeau national media supporters now applaud Justin's "strategic" (read: cynical) decision to side with Stephen Harper. More incredibly, in the wake of outrageous terrorist attacks across Europe, and with the recent RCMP revelation that lone gunman Bibeau would have had a tough time pleading not guilty by reason of insanity in a court of law, Trudeau is prepared to pounce on the anti-terrorism act, suffi-ciently neutering its efficacy to the point of rendering it null and void. Make no mistake, the Oct. 22, 2014, attack on Parliament Hill was not an indication of how serious a terrorist attack on our government structure can be; it was an omen of worse to come should we choose to pretend that violent protest is not indigenous to Canada. Postmedia Network (Ottawa Sun, A6)

Goodale calls refugee integration crucial

Public Safety Minister Ralph Goodale says it's vital that resettled Syrian refugees are successfully integrated into Canadian towns and cities, not just from a social and cultural perspective, but from a public safety perspective. (…) At a Liberal cabinet retreat this week in New Brunswick, Immigration Minister John McCallum said the challenge is not if the target number will be met, but to find places for them to live and help them find jobs. In the face of incidents like the fire-bombing of a Peterborough, Ont. mosque and the pepper-spraying of Syrian refugees in B.C., Goodale was asked by the Star whether he worried about the ability of some Syrian refugees to integrate and the issues of radicalization that might arise in communities where Muslim youth may feel isolated or disenfranchised. (…) However, Goodale, the minister in charge of national security agencies such as the RCMP, CSIS and Canada Border Services Agency, said his first order of business is to create a watchdog committee of parliamentarians who would serve as a check and balance on those forces. Toronto Star, A10

Provinces, feds team up on drug buys

The federal government has joined Canadian provinces and territories in a bulk-buying drug program that aims to lower the cost of prescription medications. Health Minister Jane Philpott says federal drug plans will unite with the provincial and territorial pan-Canadian Pharmaceutical Alliance, which negotiates to lower prices on brand name and generic drugs. The announcement comes as the country's health ministers gather in Vancouver this week to discuss issues such as chronic diseases, drug costs and funding formulas. Philpott says in a statement that combining the negotiating power of federal, provincial and territorial governments achieves greater savings for all publicly funded drug programs, increases access to drug-treatment options and improves consistency of pricing. Federal health plans provide drug benefits to First Nations and Inuit, the RCMP, the Canadian Forces, veterans, federal inmates and

refugee protection claimants, totalling $630 million in 2014. Postmedia Network (Chronicle Herald, A8, Edmonton Sun, Times Colonist, Vancouver Sun, Times& Transcript); Toronto Star, A14

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Police puppy dies after eating rope
An RCMP plan to document the lives of two German shepherd puppies during their training has ended sadly for one of the canine recruits. The Halifax division announced Tuesday one of the pups - Helo - has died after ingesting rope and rocks. Const. Mark Skinner says the accident occurred as the puppy pursued his natural tendency to chew on objects. (…) During the media launch of the two puppies on Dec. 18, the RCMP officers training them said the dogs live at their homes. Const. Tim Reid, Helo's trainer, had said that every two weeks he and the puppy took part in a six- to eight-hour training day that included a heavy focus on tracking skills. In a few more months, had Helo lived, a fully trained dog handler would have assessed the dog's progress. Reid said Helo was the sixth puppy he'd trained and that only one had graduated to become a police dog. One of the others died of a heart attack, another returned to Innisfail to breed and two others were sold as pets. Reid had said there are about 80 people like himself across the country who are in training to make it into the RCMP dog handler program in central Alberta. An RCMP news release said Reid was saddened by the loss, and noted that condolences can be shared on the force's Facebook page in Nova Scotia and on Twitter using the hashtag RIPHelo. Postmedia Network (Chronicle Herald, A9, Cape Breton Post, London Free Press)

Puppy in training with RCMP dies
A puppy training with the RCMP died at the Atlantic Veterinary College in Charlottetown on Monday. Fourteen-week-old Helo, who was being socialized by an RCMP member in Bible Hill with an interest in becoming a dog handler, died as a result of complications following surgery. It is believed Helo ingested rocks and rope earlier this month which caused internal issues. He required three surgical procedures. "He was doing well until then," said Const. Mark Skinner, media relations officer with the Nova Scotia RCMP. "He was very young and was getting used to the world around him." Helo was born Oct. 4 at the RCMP Police Dog Service Training Centre in Innisfail, Alta., and arrived in Bible Hill in early December. Postmedia Network (Cape Breton Post, A9, London Free Press, Chronicle Herald); Metro News; Global News; CTV News; CBC News (2016-01-19)

Girls enjoy 'harm, repair' exercise
For those long removed from the lives of young teenage girls, observing their interactions can be a reminder that "Mean Girls" isn't just a movie - for some, it's a reflection of real life. To counter such meanness, Hamilton's female police officers held a Girls Leadership Day at Queen Victoria School on Forest Avenue Tuesday, focusing on what it feels like to be bullied, and what it feels like to be valued. The event was put on by Hamilton police and ProAction Cops and Kids, for girls in Grades 5 to 8. Volunteers came from the RCMP, fire department, and the military. In a "harm and repair exercise," the 83 girls involved split into groups and created an art piece paper doll representing "the perfect you." They later had to glue on mean and hurtful written statements like "nobody likes you," "you're dumb," "you're ugly," "you're stupid" and "you're a loser." As each phrase was attached, the girls were instructed to tear a piece of their beautifully adorned doll or crumple one of its body parts. It was a poignant reminder of the pain that hurtful words can cause. Postmedia Network (Hamilton Spectator, A4)

For the second consecutive day, the Selinger government has named a lake near Flin
On Tuesday, government officials announced a lake about 45 kilometres north of Flin will be named after Rhonda Commodore, a corrections officer in The Pas who died in a November 2014 crash while transporting six inmates to Dauphin. "Naming a lake in Rhonda Commodore's honour, and thereby recognizing for eternity her contributions to community safety and service, is a very special and appropriate gesture in remembering her," said Michelle Gawronsky, head of the Manitoba Government and General Employees Union, in a press release. "It is comforting that now all Manitobans, including her extended family as well as her correctional officer family, have one more reason to think of and cherish her and keep her memory alive." The naming of Commodore Lake came a day after the government

announced another lake near Flin Flon would be named after RCMP Const. Dennis Strongquill, who was gunned down while in the line of duty in 2001. Postmedia Network (Winnipeg Sun, A4)

New resource officer for Coaldale schools
Coaldale schools have a new RCMP School Resource Officer (SRO). His name is Const. Doug Sokoloski and he's all geared up since the RCMP took over policing duties from the Lethbridge Police Service on Jan. 1…"I was a community policing officer. Part of that was school resource officer and traffic and public relations were the other few main components. I have done that, of course, at the normal detachment level when I was in Raymond/Magrath – schools were part of our mandate and in Fort McMurray, as well," said Sokoloski., who has been a member of the RCMP for more than 19 years. Lethbridge Herald (2016-01-19)

Disciplinary hearings scheduled for three B.C. Mounties
Disciplinary hearings have been scheduled for three B.C. RCMP officers, all accused of disgraceful conduct. The RCMP won't give details about the allegations citing privacy, but say Corporals Correy Eggen, Nancy Joyce and Eric Irani will have public hearings. CKNW AM 980 (2016-01-19)

Man accused of shooting Kamloops Mountie slated to plead guilty
A man accused of shooting a Kamloops Mountie is set to enter guilty pleas to numerous charges this spring. Kenneth Michael Knutson faces several charges in Kamloops Supreme Court including attempted murder after an incident which left an RCMP officer critically injured and led police on a 12-hour manhunt through the Batchelor Heights neighbourhood in December 2014. Cpl. Jean-Rene Michaud was shot after he pulled over a white sedan in the early morning hours of Dec. 3, 2014. He survived the shooting after several surgeries and months in the intensive care unit. InfoTel.ca (2016-01-19)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

'Troubling' Conservative torture policy up for review
The Trudeau Liberals will review controversial directives enacted by the Harper government that allow for the sharing of information even when it might lead to torture, says the public safety minister. The "troubling set of issues" raised by the foreign information sharing policy "will be raised in the course of our consultations" on the overall national security direction of the new government, Ralph Goodale said in a recent interview with the Canadian Press. The news follows pressure from human-rights and privacy advocates to conduct a wide-ranging examination of security policies introduced by the Conservatives, whisked from office in the October election. The federal policy on foreign information-sharing has been roundly criticized for effectively condoning the torture of people in overseas prisons, contrary to international law and Canada's United Nations commitments. A four-page 2010 framework document, released under the Access to Information Act, says when there is a "substantial risk" that sending information to, or soliciting information from, a foreign agency would result in torture - and it is unclear whether the risk can be managed through assurances or other means - the matter should be referred to the responsible deputy minister or agency head. In deciding what to do, the agency head will consider factors including the threat to Canada's national security and the nature and imminence of the threat; the status of Canada's relationship with - and the human rights record of - the foreign agency; and the rationale for believing that sharing the information would lead to torture. Critics say when there is a serious risk of torture, there should be no sharing - period. The Canadian Security Intelligence Service, the RCMP, the Canada Border Services Agency, National Defence and the Communications Security Establishment, Canada's electronic spy agency, are bound by the federal policy on sharing information with foreign agencies. Postmedia Network (Kingston Whig-Standard, B3)

Torture: Ottawa veut consulter les Canadiens sur la politique de partage de renseignements
Une «série de questions troublantes» soulevées par la politique de partage de renseignements avec des pays étrangers qui peuvent conduire à la torture de citoyens canadiens innocents, «seront abordées dans le cadre de nos consultations» sur la politique nationale globale du nouveau gouvernement, a indiqué le ministre de la Sécurité Publique Ralph Goodale à la Presse Canadienne. Cette nouvelle fait suite à la

pression exercée par des défenseurs des droits de la personne qui demandent que soient examinées les politiques de sécurité mises en place par les conservateurs avant les élections d'octobre où ils ont été renversés par les libéraux. La politique fédérale sur le partage de renseignements avec des pays étrangers a été l'objet de nombreuses critiques et accusée pour avoir comme conséquence de condamner des personnes à la torture dans des prisons outremer, contrairement au droit international et aux engagements du Canada envers les Nations unies. Personne n'a oublié le cas de Maher Arar, arrêté sur la foi de renseignements transmis par la GRC le 26 septembre 2002 à l'aéroport de New York alors qu'il revenait au Canada après des vacances en Tunisie. Emprisonné en Syrie sans accusation pendant plus d'une année où il été torturé à plusieurs reprises et forcé de signer de faux aveux, il n'a été libéré que le 5 octobre 2003, après que le gouvernement syrien a admis qu'il n'avait aucune preuve contre lui. Après le rapport d'une commission d'enquête au Canada le 18 septembre 2006. le gouvernement canadien a reconnu ses torts et a offert 10,5 millions de dollars de dédommagement à Arar. 45eNord.ca (2016-01-19)

BC's health minister wants to seize opportunity to talk about effects of pot legalization
The conversation on legalizing pot in Canada has to include the medical perspective according to BC's health minister. Terry Lake is answering questions ahead of meetings with the federal health minister next week. Lake is pointing to studies which raise concern over what pot does to the brain, especially young ones. "We've got a situation now where young people are, I think, very high risk of marijuana that's out there now on growing and developing brains. This is an opportunity to create a system that protects young people and so I think we have to be very careful. You really only get to do this once." Lake understands public safety ministers will take the lead on this and doesn't think many hard solutions will come out of the meetings. He isn't ruling out the idea of selling marijuana in government liquor stores, something proposed by the BCGEU. "I think that will be something that evolves. There has been some discussion. You heard the premier of Ontario say that the liquor store model would be suitable. There are public health officials that I've talked to who say that the co-location of marijuana and liquor sales is not advisable from a public health perspective. There's a lot of discussion ongoing." News1130.com (2016-01-19)

Marijuana in Montreal: How legalization could shake up black market
In the final instalment of Daybreak's "Montreal 420" series, a retired Montreal police officer discusses how legalization could change the city's illicit drug trade. Philippe Paul spent 28 years with the Montreal Police force, most of that working on the drug and anti-gang squad. Paul is also an expert witness in narcotics trafficking cases and author of the book Coupable d'etre policier. CBC.ca (2016-01-19)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Un registre dont l'existence n'est pas justifiée
Un article d'opinion dit, « Enregistrer, immatriculer et buriner les armes à feu ne va pas rendre notre monde plus sécuritaire. Depuis 1978, le Canada possède le meilleur contrôle sur les armes à feu au monde. Toutes les personnes qui veulent se procurer une arme à feu légalement doivent se qualifier et obtenir un certificat d'acquisition et de possession. Cette démarche est le moyen que les policiers ont pour savoir si une personne peut acheter ou posséder légalement une arme à feu. C'est un processus qui se fait en moins de 60 secondes. Je connais personnellement ce procédé pour l'avoir enseigné pendant trois ans à la formation du personnel de la GRC à Montréal. J'ai pris connaissance de votre projet de loi et je m'interroge : pourquoi cet acharnement auprès de personnes qui agissent légalement ? Pourquoi avoir surtaxé les chasseurs avec des augmentations du coût des permis de 25 à 53 %, pendant que l'indice au coût de la vie était de 1,2 % ? Pourquoi créer une loi qui vous permettrait d'altérer un produit déjà marqué d'un numéro de série par le fabricant ? Où se trouve l'aspect « sécurité publique » dans cette démarche ? (...)Je suis renversé, comme tous les propriétaires d'armes au Québec, de voir mon gouvernement exploiter les chasseurs et tireurs sportifs en utilisant des prétextes fallacieux ; c'est de l'abus de pouvoir, de l'acharnement, voire du harcèlement. » LeDevoir.com

OTHER / AUTRES

Canada's weapons exports grew more than 89 per cent under Harper
Canada's arms exports shot up while Prime Minister Stephen Harper's Conservative government was in office, fuelled by higher sales to countries like Saudi Arabia, Jordan, Mexico and Austria, an analysis by iPolitics has found.(…) One of the countries where Canadian military exports rose the most during Harper's government was Jordan - a country whose human rights record has been questioned by groups like Amnesty International. Military exports jumped from only $6,580 in 2006 to $ RCMP 15 million in 2011 before falling back to $888,467 in 2013 - the year that Harper named the head of his RCMP security detail, Bruno Saccomani, as Canada's ambassador. iPolitics

Toronto police buy 51 high-powered, military-style rifles
Patrol carbines paired with less lethal sock guns to give front-line officers a choice when using force The Toronto Police Service has purchased 51 patrol carbines, high-powered rifles that will be distributed to each of the city's 17 police divisions and made available to front line officers. The force has purchased the C8 patrol carbines - a military-style, semi-automatic gun - to be paired with the "less lethal" sock guns currently being sent to each division, Toronto police spokesman Mark Pugash said Tuesday. The rollout of the weapons will be finished by the end of May. (…) Darryl Davies, a criminology instructor at Carleton University, said police are now confronting criminals and terrorists wielding high-power assault rifles with greater regularity - and their pistols and shotguns are "antiquated weapons" that are no match for an assault rifle. Following the 2014 shooting deaths of three RCMP constables in Moncton, N.B., there was harsh criticism that officers did not have the weaponry necessary to compete with convicted killer Justin Bourque's M305 semi-automatic rifle. The Mounties only had their handguns and three shotguns. Many experts said the carbine may have levelled the playing field. Davies, who recently served as a consultant to the RCMP on the feasibility of its officers using the patrol carbine, said he hopes Toronto police have a "very intensive training program" in place to ensure officers know how to use, store and maintain the weapon. Toronto Star, GT1

Civilian oversight coming to RNC and RCMP, as number of investigations spike
Justice Minister Andrew Parsons is calling for civilian oversight of police forces in this province, as CBC News has obtained new details that reveal just how often the police are being investigated in Newfoundland and Labrador. Parsons's comments come less than a week after CBC News revealed that senior members of the Royal Newfoundland Constabulary were under criminal investigation. That probe is being carried out by a civilian-led agency from Nova Scotia. Parsons says the need to shift to civilian oversight is reinforced by information contained in government briefing notes obtained by CBC News through access to information. According to those briefing materials, the RNC and RCMP were investigated 42 times in 2015 alone. CBC.ca (2016-01-19)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Sent to: RCMP DMS 1; RCMP DMS 2; RCMP DMS 3; RCMP DMS 4; RCMP DMS 5; RCMP DMS 6

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
June 02, 2015 / le 02 juin 2015

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

RCMP toxic to women, says lawyer as B.C. hearing begins for potential class-action
A lawyer arguing for a class-action lawsuit against the RCMP says the cases of hundreds of female employees alleging the force discriminated against them must be considered together. David Klein said the RCMP is toxic to women and has been for a number of years. "Day after day, week after week, year after year, they were subjected to degradation, humiliation, and demoralizing comments and behaviour. Comments and behaviour that were not adequately addressed by management," he said Monday outside B.C. Supreme Court. Klein is arguing this week that the complaints of 363 female RCMP employees should move forward collectively because that would provide a full picture of a systemic problem. "This is conduct that occurs over months or years, by multiple perpetrators, that's ignored by management at multiple locations," he said of the women. Two thirds of them still work for the force. No dollar figure has been attached to the case, but Klein said that with hundreds of cases involved, a judgment could be in the "many millions of dollars." The RCMP has taken small steps to address harassment on the force since the suit was originally filed in 2012, Klein said. But he believes there's more to be done. "They at least pay lip service to taking the problem seriously, but they're not taking the women seriously. And until they take the women seriously, until they take those claims seriously, the problem will not be solved." The hearing began three years after for Nanaimo RCMP officer Janet Merlo came forward with allegations about discrimination she experienced throughout her career, including lewd comments and actions from her male colleagues. Postmedia News (Vancouver Sun); Canadian Press (The Province, A10, Times Colonist, Red Deer Advocate, The Guardian); Presse Canadienne (Le Soleil, L'Acadie Nouvelle) (2015-06-02); CTV News; Canadian Press (News 1130; Vancouver Sun) (2015-06-01)

CONTRACT & ABORIGINAL POLICING / SERVICES DE POLICE CONTRACTUELS ET AUTOCHTONES

Pair charged with murdering man and setting his Jeep on fire
A man from B.C. and a woman from Ontario are charged with first-degree murder in a December **Strathcona County** case where an Ontario man was slain and his vehicle burned. Around 12:45 a.m. on Dec. 30, the body of Adrian Gregory, 30, was discovered inside a green Jeep that had been set on fire and left in an industrial area west of Sherwood Park. A second person, identified by police Monday as Jeremy Pershawm, was also found in the Jeep and was taken to hospital with undisclosed injuries. Police said Monday both victims had been shot before the Jeep was set on fire. The victims had been targeted, added RCMP. Investigators had asked for anyone who may have had contact with Gregory before Dec. 30 to come forward. Police said Gregory worked in Alberta for a few years. In an extensive investigation by RCMP Major Crimes Unit North and Strathcona County RCMP, a woman was arrested and charged on March 17, 2015, in Port Elgin, Ont., while a man was arrested in Chilliwack, B.C., on May 29, 2015. The woman has been released on bail in Ontario, with a subsequent court date in Strathcona County to be fixed at a later date. Postmedia News (Ottawa Sun, Calgary Sun, Kingston Whig Standard, London Free Press, Edmonton Sun); Canadian Press (Ottawa Citizen); Postmedia News (Edmonton Journal) (2015-06-02); CBC News; Agence QMI (Ottawa Sun, Edmonton Sun) (2015-06-01)

Four face charges for vandalizing property in north Halifax
Four people face charges early Saturday morning for allegedly vandalizing property with spray paint in north-end Halifax. **Halifax** Regional Police arrested three men, all 19, and a 17-year old after they allegedly spray painted signs and utility boxes at the intersection of Gladstone and North streets. All four were charged with property damage and released, and are to appear in provincial court and provincial youth court at a later date. Mounties are also investigating a report of 15 vehicles and a garage door being spray painted in Cole Harbour. Most of the cars were allegedly sprayed in orange and brown lines and sometimes a "graphic indecent image," according to an RCMP release. Police believe the incident happened between midnight Saturday and early Sunday morning. The public is urged to contact police if they know anything about any crime involving spray painting. Chronicle Herald

IHIT investigating Langley homicide, one in custody
Mounties took one person into custody after a homicide in **Langley** Monday night. RCMP officers were called around 7 p.m. to the 20300 block of Fraser Highway, where they found one person dead, according to a news release by Holly Largy, an RCMP spokeswoman. Members of the Integrated Homicide Investigation Team took control of the investigation and the area was shut down into the evening. Investigators say the homicide is likely not random, but they won't release more information until Tuesday. Postmedia News (Vancouver Sun, The Province)

RCMP seek the owner of tribal drum
RCMP are looking for the owner of a tribal drum found in **St. Albert** in March. "A tribal drum can be quite expensive, and are also held to be very valuable by their owners," RCMP Corp. Laurel Kading said Monday. She said RCMP are specifically not releasing any information to ensure it is claimed by the rightful owners. The drum was found in a case in the area of Hogan Road in St. Albert on March 13. Kading said the location means the owner may have been travelling through the area. It also possible it was stolen and then ditched. "We don't know the origin of it, but someone somewhere is missing a very nice drum," Kading said. She said the woman who handles found property for the RCMP was concerned the item would end up in a police auction, rather than back with its owner. Kading said RCMP recognize the cultural significance of the drum and have taken extra steps to ensure it is being held in a safe place and being treated in a respectful manner. Postmedia News (Edmonton Journal)

Are police properly equipped?
Several recommendations resulted from the RCMP shootings in **Moncton** a year ago. One was that police forces across the province be equipped with carbines and the training that goes with them. To see whether or not that has happened, visit telegraphjournal.com for legislature bureau reporter Karissa

Donkin's report. Jason Rideout keeps a set of horseshoes in the trunk of his car so that he's always prepared for a game and the Silver Horseshoe, the sport's equivalent of the Olympic torch, hangs in his office. So there is little wonder why Rideout was selected to lead the organizing committee after St. Stephen became the smallest community ever to host the 2015 Canadian championships. For more, visit telegraphjournal.com. The Public Safety Communication Centre, which handles 911 calls in the city, is still understaffed but is getting closer to having all positions filled, said Marven Corscadden, director of human resources and finance for the Saint John Police Force. Telegraph Journal, A2

RCMP divers discover body in river after extensive search
RCMP divers discovered a body just before 9 a.m. on Monday, in the St. Charles River in **Aldouane**, following a report of a sudden death Sunday. Police say a sudden death occurred in the early hours Sunday after a group of people were jumping off the Daigle Creek Bridge into the St. Charles River, just over an hour north of Moncton. Southeast RCMP received a call shortly before 4 a.m. on Sunday that a 23-year-old man from Pointe-Sapin had jumped off the bridge and did not resurface from the water. Cpl. Dan Melanson with Richibucto RCMP detachment said several fire departments were on scene from the initial call, as was Ambulance New Brunswick, the RCMP underwater recovery team, forensics, a canine unit and the Tri-County Ground Search and Rescue. Melanson said no one else was injured and that nothing was out of the ordinary in terms of the river's state. Times & Transcript, A6; Acadie Nouvelle, A2

Gov't may have broken law over teen's death, says B.C. grand chief Phillip
Government agencies may have broken the law by repeatedly failing to report that an aboriginal teen who died of a drug overdose in **Vancouver's** Downtown Eastside needed protection, says the head of the Union of B.C. Indian Chiefs. Grand Chief Stewart Phillip called for a police probe of workers in health care, education, policing and community agencies accused in a report of harbouring a "culture of indifference" toward aboriginal kids. The case of a 19-year-old woman identified only as Paige was highlighted in a scathing report released last month by B.C.'s representative for children and youth, who criticized the province for what she called persistent indifference by front-line workers. (…) Meanwhile, a federal government bureaucrat ordered the destruction of legal opinions over the potential of First Nations in B.C. to reach land-claim deals, Phillip claims. The allegations come days after ex-B.C. government worker Tim Duncan alleged he was told to delete emails connected to the Highway of Tears probe into murdered and missing women that were part of a Freedom of Information request. Phillip alleged a federal access to information request revealed a director with Aboriginal Affairs and Northern Development Canada ordered the destruction of the legal opinions. Canadian Press (Times Colonist); Postmedia News (Province)

Food tampering reports come from Annapolis Valley, Bridgewater - Nail found in potato salad at Woodville community barbecue
Potatoes containing metal objects continued to turn up in food tampering incidents in two different parts of **Nova Scotia** over the weekend, police reported Monday. Kings District RCMP announced it is investigating an incident where a finishing nail was found in a potato salad at a community barbecue in Woodville on Sunday. No one was hurt in the incident. RCMP said the potato salad was made by Kings Processing in Middleton, which is working with investigators to determine the source of the potatoes. Police have the nail and the partially eaten meal. CBC News (2015-06-01)

Name the RCMP foal contest begins, contest open to kids across Canada - Six RCMP foal names needed this year
The RCMP is inviting kids from across Canada to help them come up with the names for six foals who were born this spring at the RCMP breeding farm west of **Ottawa**. The foals may grow up to be part of the world-famous RCMP Musical Ride. “Every year we look forward to seeing the creative names children and young people from across the country submit for the foals,” says Superintendent Leslie Cook, Officer in Charge of the Musical Ride Branch. “The Name the Foal” contest is an annual tradition we look forward to, thanks in large part to the enthusiasm of the participants.” Beacon News (2015-06-01)

Learning the rules of the road
Members of the RCMP and EMS were at St. Joseph Elementary School on Friday for a special bike rodeo, with the goal of teaching students the importance of safe driving. The rodeo was for students in

kindergarten up to Grade 4, who went through various stations to teach them how to be safe while driving their bicycles on the road. The RCMP organized the event, and the EMS was there to do a presentation with their ambulance and sirens. "There's a lot of kids that don't know how to stop properly, they don't know they're hand signals, so it gives them a chance to get their hand signals, to learn which way is left, which way is right, to let the people behind them know which direction they're going when they're stopping, and also it helps to practice their turning because sometimes the kids aren't sure how to turn their bike properly so it works out well that way as well," said RCMP constable Debra Wenisch. Meridian Booster (2015-06-01)

The 'uncomfortable truth' about missing & murdered indigenous women
Twenty years ago, Helen Gillings' body was found in an alley on King Street. She was 19. Gillings is one of hundreds of missing and murdered indigenous women, some of whom grew up in nearby Six Nations, some of whom, like Gillings, were killed in **Hamilton**. Gillings, whom police say was a sex worker, was last seen alive at 1 a.m. entering the alley with a man the day before her body was found. Hamilton Police have a $10,000 reward advertised for clues leading to the arrest and conviction of the person responsible for Gillings' death. And Monday night, to kick off Aboriginal Awareness Month, a forum at Hamilton city hall will focus on stories like Gillings' and others — the "uncomfortable truth" about these hundreds of unsolved murders and missing persons cases. CBC News (2015-06-01)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Zehaf- Bibeau was shot 31 times
Michael Zehaf-Bibeau was shot 31 times after he stormed Parliament Hill on Oct. 22, and was finally killed by a bullet to the back of his head, according to CBC News based on a report by the Ontario Provincial Police to be released Wednesday. According to the CBC, the OPP report will conclude that Zehaf-Bibeau was alive until the final shot to the back of the head, and that the parliamentary security team followed a "justifiable" course of action. The report will reveal in "graphic detail" what happened in the time between Cirillo's shooting at the National War Memorial and Zehaf-Bibeau's death inside Parliament's Centre Block minutes later, according to sources who have seen the report and spoke to the public broadcaster. After a physical confrontation with one parliamentary security guard and a shootout with three more inside Centre Block, Zehaf-Bibeau sprinted down the Hall of Honour and hid in an alcove behind a pillar in front of the Parliamentary Library, the CBC reports. Sergeant-at-Arms Kevin Vickers then took cover on the other side of the pillar and was close enough to hear Zehaf-Bibeau breathing. Meanwhile, four RCMP officers organized themselves in a diamond-shaped formation called "immediate action rapid deployment," led by Const. Curtis Barrett, at the far end of the Hall of Honour, according to the CBC's sources. Zehaf-Bibeau turned and fired at Barrett, and Vickers dove to the ground while shooting at Zehaf-Bibeau. Barrett moved in and began firing. Zehaf-Bibeau went down, and Barrett recalled shooting Zehaf-Bibeau in the back of the head, according to the report. The OPP's report concludes that Zehaf-Bibeau was shot 31 times, according to the CBC's sources. The autopsy and ballistics report reveals that eight bullets remained in his body, four of them from the gun of Vickers. The report concludes that two of the shots would have been fatal without immediate medical intervention, including the last shot to the back of the head, CBC sources said. Postmedia News (Ottawa Citizen, A12); Canadian Press (iPolitics)

Ottawa asks court to keep files about imam secret
The government has asked the Federal Court for permission to withhold "sensitive" intelligence documents about an Iranian trained Montreal imam whose passport was revoked last year for national security reasons. Releasing the five Canadian Security Intelligence Service documents "could injure national security," the government argued in court filings that were themselves kept secret until a judge lifted the confidentiality of the case. (...) After Sbeiti challenged the decision in court, the government released official documents showing he had been described by the RCMP's Integrated National Security Enforcement Team as a "subject of interest in an ongoing investigation." (...) Federal security officials have been using passport seizures and revocations to deal with the increasing number of "high-risk

travellers'' - Canadians who have gone overseas to join such terror groups as the Islamic State of Iraq. Postmedia News (Gazette, A1, National Post, Calgary Herald, Windsor Star)

'10,000 times more powerful than morphine'

Connor was just 21 when he overdosed on fentanyl in his family's home in Calgary. He was among three students from his high school graduating class who died from overdoses, his mother, Yvonne, says. ''It blew me away because this kid absolutely loved life,'' said Yvonne, who asked that her last name not be used. ''It started as a choice, and then he got addicted to it; his personality grabbed on to it. It was a disease.'' Yvonne wants to help others from falling into the same trap. She was making plans last week to take her story into schools during the next academic year to warn students about street drugs. ''I want to tell them, don't say this can't happen to you, because it can,'' she says. Since Conner died in October 2013, fentanyl has grown into a frightening epidemic. The powerful narcotic already has been linked to 50 Alberta deaths during the first two months of this year. In many cases, the users think they are buying Oxy-Contin or heroin. They're wrong. It's fentanyl, and it's killing them. ''It's the new wave of concern in drug enforcement,'' RCMP Cpl. Eric Boechler of the B.C. clandestine lab unit says of fentanyl. In British Columbia during the past two years, there have been 150 deaths related to fentanyl, which was created in 1960 as a pain reliever. In many of the overdose deaths caused by fentanyl in B.C., the users took what would be a normal dose but, because it was spiked with fentanyl, it killed them. ''Two milligrams is a fatal dose,'' Boechler says. ''A paper-clip weighs about 1,000 milligrams. ''We've found fentanyl that's 10,000 times more powerful than morphine.'' ... Insp. Darcy Strang of the Alberta law enforcement response team says most of the pill pressing for North America is being done in Canada and then shipped south. Neither the RCMP nor the U. S. Drug Enforcement Administration would put a number on what percentage flows to the U.S. The dealers operating here are thought to be either resident Canadians or foreign nationals who have chosen to set up in this country because they can facilitate the manufacture of the product into pills. The U.S. Drug Enforcement Administration believes Mexican cartels are also involved. Postmedia News (National Post, Calgary Herald, Leader-Post)

Des écoles fouillées par les policiers

Dans le cadre d'une opération hautement inhabituelle, l'Équipe intégrée de la sécurité nationale pilotée par la Gendarmerie royale du Canada (GRC) a mené des perquisitions antiterroristes dans des établissements scolaires la semaine dernière, a appris La Presse. Les policiers ont notamment fouillé les casiers d'élèves du collège de Maisonneuve de Montréal, dont cinq ont pris l'avion vers la Turquie en janvier à destination de la Syrie. Quatre autres élèves du cégep ont été arrêtés à l'aéroport il y a trois semaines alors qu'ils s'apprêtaient à prendre un avion qui devait les amener vers le djihad en compagnie de six autres jeunes. (...) Les fouilles ont eu lieu dans le cadre d'une série de perquisitions menées mardi dernier dans la région de Montréal en lien avec la lutte contre le terrorisme. La GRC avait alors confirmé à La Presse qu'il s'agissait de «perquisitions en cours d'enquête», sans préciser si des arrestations étaient au programme. La Presse, A6 (Le Nouvelliste, 14, Le Soleil)

Commission says scam artists likely to target seniors

Scam artists are likely to seize on the trepidation of seniors in the wake of a new government policy that counts financial assets toward nursing care costs, warns the province's Financial and Consumer Services Commission. ''There is always the potential for financial scams, but the recent public discussions related to assets owned by seniors has raised the likelihood of financial exploitation and abuse,'' said commission CEO Rick Hancox. ''The trend is that scammers follow the headlines. ''You have a subject like this - where seniors' assets and how they could be used is obviously a headline story - so people come out of the woodwork.'' The Liberal government's controversial decision to include seniors' liquid financial assets, such as cash and savings, in determining how much they should pay for nursing home care has some New Brunswickers considering their financial options. Savings accounts, TFSAs, and GICs will now factor into the calculation. But retirement savings plans, the family home, car, cottage or boat will not be touched. The commission is now urging caution to seniors ''when approached by individuals offering unsolicited financial, investment or estate planning advice with respect to preserving or protecting their assets.''... RCMP spokeswoman Const. Jullie Rogers-Marsh said on Monday it's too early to say whether there will be a spike in crime involving seniors' assets, but added that the province's seniors are among the most vulnerable targets. ''People are always looking for opportunities to, unfortunately, defraud people

and they come up with these scams," Rogers-Marsh said. "What I think is important is that people are aware of them." Telegraph-Journal, A1 (Times & Transcript, Daily Gleaner)

Drugs seized from Renous prison visitor
Correctional Services Canada says staff at the Atlantic Institute in Renous confiscated a large package of drugs from a person visiting the prison. According to a news release issued by Correctional Services Canada, the seizure of the unnamed items occurred on May 17 when a visitor entered the maximum security prison. "This seizure is the result of the combined efforts of correctional officers and security intelligence officers. The contraband seized includes one vial containing two grams of hash oil," said the release. The individual was then arrested by the Blackville RCMP and may face criminal charges, the release said. Since April 2013, staff members at the Atlantic Institution have made 10 drug seizures valued at close to $104,000, which have resulted in the arrest of six visitors to the prison, the statement says. Daily Gleaner, A8

Menthol cigarette ban prompts quitting
Since the government has announced plans to ban all flavoured cigars, including menthol cigarettes, citing the legislative amendments will deter people from the harmful habit, some are saying they're right. Fin Mackay-Boyce has been smoking for six years with the past four being strictly menthol cigarettes. He says the ban will deter him from smoking altogether. "I will quit. I don't enjoy smoking regular cigarettes compared to menthols. If I'm travelling I might buy a pack if I'm craving but I think the trouble and cost of buying menthols in bulk or the dislike of normal cigarettes will keep me from smoking," he said. The prohibition on the sale of flavoured tobacco products will start on Jan. 1, 2016. Nova Scotia has implemented a similar ban, which has been challenged by Imperial Tobacco in court. The ban will also include the sale of e-cigarette and e-juices to people under 19 years of age… History shows that often prohibitions can open up illegal black markets. However, this is not a concern for the RCMP. Const. Jullie Rogers-Marsh, media relations officer with the RCMP, said the ban is currently not a concern for illegal activity. "We would look at it, and certainly keep an eye on it if there are things we need to do as a policing agency, but in general if there are ever any changes, we would certainly monitor it," she said. Telegraph-Journal, B3

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

B.C. couple fights seizure of $130,000 in civil forfeiture case
David Johnson had just pulled out of his driveway, his three-year-old son in the back seat, when RCMP officers swarmed the vehicle and drew their guns. B.C. Supreme Court heard on Monday that the officers then searched the Johnson home at the end of a quiet cul-de-sac in Surrey, B.C., and Mr. Johnson and his wife were charged with running a marijuana grow-op. The Ministry of Children and Families took their son to live with his grandparents for about three months. Criminal charges were later dropped after a judge ruled the alleged grow-op was “relatively small” at 267 plants and, at nearly three years, the case had taken too long to get to trial. But five days after the ruling, the RCMP forwarded the file to B.C.’s Civil Forfeiture Office – a government agency that has been criticized for its aggressive attempts to seize homes, vehicles and cash connected to criminal offences, even from people who are not convicted or charged. The forfeiture office began proceedings to seize $130,000 that was removed from the house during the search. And so, nearly six years after the raid, the Johnsons were back in court on Monday. “It’s very stressful,” Mr. Johnson said outside court. “It just doesn’t end.” The Civil Forfeiture Office, in its notice of civil claim, accuses the couple of using a hydro bypass to steal electricity for the marijuana grow-op. It says the search was conducted after a complaint from B.C. Hydro to the RCMP. The notice of civil claim also suggests Mr. Johnson told a neighbour and the person to whom he later sold the house that he had a grow-op. Globe and Mail

Hometown rider honoured to be part of the RCMP Musical Ride
When the RCMP Musical Ride comes to Moncton on Thursday, one rider will be performing for her friends, her family and her hometown - a hometown that lost three of its officers one year ago. Const. Tiffany Donnelly will perform in Moncton on June 4 as part of the Ride's 2015 national tour. The event is scheduled on the anniversary of the shooting deaths of three Codiac Regional RCMP officers and the

injuring of two others. Donnelly grew up in Irishtown, just outside Moncton, joining the RCMP seven and a half years ago, in 2007. "I joined for the same reasons a lot of people do. I wanted to help people, I wanted to be able to see different parts of Canada. I wanted a job that was going to be interesting and challenging," the 33-year-old said from the tour bus, which was on its way to Sussex Monday afternoon for two evenings of performances. Times and Transcript, A1 (Telegraph-Journal)

RCMP investigate shooting

A shooting that occurred in Bouctouche last Friday is under investigation, say the Southeast District RCMP. Police received a call shortly after 8:45 p.m. on May 29 of an apparent single vehicle collision on Highway 475 near Chemin Desroches in Bouctouche, an RCMP press release states. The vehicle ran off the road and was on the beach near the water. When officers arrived on the scene, a 40-year-old Richibucto man was discovered on the side of the road with a single gunshot wound, the RCMP say. He was treated at Sainte-Anne-de-Kent Hospital and later transported to the Moncton Hospital with non-life-threatening injuries. The RCMP believes this is an isolated incident and the investigation, with the assistance of the Major Crime Unit, is ongoing. Times & Transcript, A3 (2015-06-02); CBC News (2015-06-01)

Mountie charged with forgery

A Moncton Mountie who was suspended from duty in March is now charged with forgery. Codiac Regional RCMP Const. Jonathan Cormier, 36, of Moncton, is facing two charges. Defence lawyer Bruce Phillips appeared on his behalf at the Moncton Law Courts on Monday and asked for time to seek disclosure. The case returns to court July 2. The allegations against Cormier, a general duty officer, relate to incidents that occurred in February in Moncton. The charges indicate another Mountie was the target of the forgery. Cormier is charged with knowingly making a false document by forging an email document with the intent that it be acted upon as genuine by Const. Pierre Alexandre Roy. That allegedly occurred between Feb. 19 and 26. He's also charged with knowingly causing Roy to act upon a forged document by providing two forged emails as if they were genuine. Both charges are summary offences, meaning they are less serious than if the Crown had proceeded with the indictable versions. The charges were laid in court on May 4 by RCMP Staff Sgt. Stephan Pouliot, who's based in Charlottetown. New Brunswick RCMP spokeswoman Const. Jullie Rogers-Marsh told the Times & Transcript on Monday that the matter was brought to their attention in the middle of March. "The RCMP received information that a member of Codiac Regional RCMP may have committed a criminal offence while carrying out their police duties," she said. Times & Transcript, A6; L'Acadie Nouvelle

RCMP Officer to C-51 Protester: "You Could be Branded a Terrorist"

An anonymously uploaded YouTube video seemingly shot during Saturday's "Stop C-51" Rally on Parliament Hill depicts an RCMP officer telling a protester that, as a result of the coming anti-terrorism bill, he "could be branded a terrorist...whenever you're attacking the Canadian economy." The officer, whose identity is unknown at this point, goes on to answer that "when the demo's down, you become citizens again," to the question "are we considered differently when we are demonstrating?" The practical implications of Bill C-51 are a matter of great debate and have been interpreted differently by various policy makers, academics and journalists. But the fact that a working RCMP officer tasked with policing protests believes the bill has the power to temporarily revoke a protester's rights and status as a Canadian citizen is worth noting. The media relations office of the RCMP's National Division has been approached for comment, and this post will be updated with their response if it should arrive. Canadaland Show (2015-06-01)

Tragédie de Moncton : les policiers déplorent toujours le manque d'armes et de formation

Des agents de la GRC qui sont intervenus il y a un an dans le quartier de Moncton-Nord, assiégé par Justin Bourque, estiment que la police fédérale a échoué à les armer et à les former adéquatement. Trois agents de la Gendarmerie royale du Canada ont perdu la vie et deux autres ont été blessés le 4 juin 2014 lorsqu'un homme lourdement armé a tiré sur eux. Le suspect a été arrêté au terme d'une chasse à l'homme de près de 30 heures et pendant laquelle les résidents d'un quartier de la ville ont été confinés dans leurs maisons. D'après des policiers qui ont parlé à La Presse Canadienne sous le couvert de l'anonymat, ils ne disposent toujours pas de carabines semi-automatiques et craignent pour leur sécurité. Les policiers craignent qu'en s'exprimant publiquement sur cette question, ils perdent leur

emploi. Pourtant, un rapport publié il y a quelques mois recommandait justement que les policiers soient mieux outillés, qu'ils reçoivent une meilleure formation et surtout, qu'ils soient plus lourdement armés. Radio-Canada (2015-06-01)

Former CFL player set to join the RCMP in Nova Scotia
A former CFL football player will be joining the Nova Scotia RCMP by June 6. Delroy Clarke will be starting his first post as an RCMP officer in Shelburne after playing professional football for six seasons for the Toronto Argos, Ottawa Redblacks and the Edmonton Eskimos as a cornerback. Metro News (2015-06-01)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

NIL

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

RCMP seem incapable of policing themselves as hundreds of harassment complaints emerge
An editorial states, "The allegations have become sadly familiar. They've spoiled the RCMP's once-proud legacy and tarnished its brass. One woman after another has come forward, and now hundreds are claiming to have experienced gender-based harassment and discrimination while working for the Royal Canadian Mounted Police, an institution that doesn't seem capable of policing itself. The harassment complaints are outlined in legal documents and have filled pages of newspapers, for years in some cases. It's time those long-standing claims were tested in court. Several cases alleging RCMP harassment have already been tried, while others are still inching their way through the justice system, including a giant, proposed class-action case that could involve 282 or more women, should it proceed. Monday, government lawyers and counsel for the lawsuit's original plaintiff, a former RCMP constable, appeared in B.C. Supreme Court chambers for a long-awaited application hearing. A judge will determine whether the matter can go to trial. The proposed class action was initiated by veteran RCMP officer Janet Merlo, a Newfoundland native who spent her entire 18-year career as a Mountie on Vancouver Island before retiring in 2010. She anticipated none of this: the alleged behaviours directed at her; the illnesses that beset her; her husband's reactions, an attempted suicide and the break-up of their marriage; going public with her claims; the notoriety; and writing a book. Merlo told a CBC radio host Monday the class action is "probably not the best way" to manage the specific allegations she makes, and which at least 280 other former and current female RCMP members have indicated they support. "But it's the only way," she added. She is right. While the RCMP has taken steps to address harassment issues in its ranks, it hasn't - and likely can't - tackle on its own the enormity of the problem, or every concern raised by hundreds of its female members, past and present. There is, according to Merlo's lawyer, "a systemic failure within the institution." It continues to plague the police force, and the allegations keep coming..." Postmedia News (National Post, Ottawa Citizen, Vancouver Sun, Calgary Herald)

Adding insult to fatal injury
An editorial states, "When one human being kills another, the public interest is generally best served if police disseminate a timely, fulsome account of the incident. Given the immediate and reasonable concerns that some citizens may have for their safety in the aftermath of a homicide, particularly one committed in public, police information speaks to peace of mind. And police most certainly have a responsibility to keep the peace. It is difficult, therefore, to accept or even understand why a growing legion of law enforcement agencies in Alberta and elsewhere in Canada refuses to release the names of some homicide victims, including people killed by police. In this province, the latter cases are referred to the Alberta Serious Incident Response Team (ASIRT), which conducts investigations, issues findings and can lay charges against law enforcement personnel. It can also choose whether it releases the name of a homicide victim, just as the RCMP and Edmonton Police Service can choose to do. There have been 11 officer-involved deaths in Alberta so far this year, and none of the victims has been identified by ASIRT, which is conducting investigations of all 11 deaths. "It's not that we're keeping it secret. It's just that the

names aren't released," executive director Susan Hughson told Journal columnist Paula Simons. As partial justification for what can rightly be termed censorship, Hughson cited cases of socalled "suicide by cop," in which the deceased has intentionally provoked police into causing his or her own death. People who commit suicide are not considered victims of crime and are therefore not identified, as it serves no public good. But it is highly presumptuous of Hughson or any other law enforcement official to assume or decide, prior to the conclusion of a thorough investigation, that a "suicide by cop" has occurred..." Edmonton Journal, A12

Blacksmith's monument to fallen officers helps community heal

An editorial states, "It was rather inspirational, and perhaps even a bit therapeutic, to visit Paul Fontaine's blacksmith shop to see a steel monument to our fallen Mounties taking shape. When I travelled out Heritage Wrought Iron shop in MacDougall Settlement a couple of weeks ago, I stood and watched for a while as Mr. Fontaine and his son Guy lifted large fabricated pieces of cut steel onto the sculpture and then weld them into place. I stood back a few feet, trying not to look at the bright blue flame as the welding rod struck the steel to form a new bond. There's something about the smell of a welding shop, where the smoke from cutting and welding hangs in the air, that inspires creativity. Mr. Fontaine is one of the few people in our region who still practises the ancient art of blacksmithing along with the more modern craft of cutting and welding steel plates. He's been doing it for many years and told me that building a monument to the three Codiac RCMP officers who were cut down in the line of duty last June was "dream job," a chance to do something truly meaningful and different. He told me the bread and butter of his business lies in fence rails, gates and interesting architectural elements hand-crafted from wrought iron. Take a walk around his shop and you can find all kinds of interesting works that have been beaten into shape on the huge anvil from red-hot wrought iron...." Times & Transcript, A9

Alberta's cloak of secrecy

An editorial states "The instinct of Alberta's police for pettifogging, pointless secrecy has now officially reached the point of generating poetry. On May 22, the Alberta Serious Incident Response Team (ASIRT), a provincial police agency that investigates other police forces, released the results of an inquiry into the RCMP's fatal 2013 shooting of a suspect on the Cold Lake Indian reserve. The document tells the unhappy story of a former convict who had continued to lead a violent existence, but who was determined not to go back to jail. The final confrontation is explained, and justified, very convincingly. The report contains all the detail one could desire - except for names. The cop who killed a man is the "Subject Officer"; the man he killed becomes the "Affected Person." And so you get the weird mini-biography of an abstraction, written in a style almost reminiscent of Kafka or Robert Musil. "The Affected Person was a fugitive with arrest warrants for serious personal injury offences ... "(before he was Affected, naturally). "The family of the Affected Person confirmed that he was living in the bush...." "The Affected Person told the witness that something was going to happen that day...." And, climactically, "The Subject Officer commanded the Affected Person to drop the knife, and when he immediately failed to do so, the Subject Officer fired two shots, striking the Affected Person in the chest." After a couple pages of this, the verb "affect" starts to take on a sinister cast: the police have Affected you when they put a couple new holes in you. This kind of ellipticalness seems particularly characteristic of Alberta for some reason. Maybe we just notice it more. After the Mayerthorpe Mountie shootings of 2005, the RCMP's K Division memorably insisted that it could not disclose James Roszko's record of arrests, trials, or criminal convictions - it was all covered by privacy law, even after his death. Even now, the publicly accessible knowledge of those details, which were a relevant factor in a quadruple murder, is an imperfect log of horrors scraped together by reporters. (...)" Postmedia News (National Post)

Gun bill ties RCMP hands

An opinion piece states, "(...) In February of last year, the RCMP reclassified thousands of semi-automatic rifles that had entered the country as non-restricted long guns, because they were in fact prohibited given their ability to be converted into a fully automatic firearm. The decision is entirely compliant with the law, which specifically prohibits automatic firearms, and with the 1993 Supreme Court ruling that says semi-automatic firearms that can be converted to fully automatic mode are equally prohibited - these weapons being "designed to kill and maim a large number of people rapidly and effectively. They serve no other purpose. They are not designed for hunting any animal but man." These included the full range of "Swiss Arms" models and various versions of the "CZ 858" family - one of which

was used in the September 2012 shooting at the Parti Québécois election celebration in Montreal. One man was killed and another injured, but the toll could have been much higher had the gun not jammed after the first shot. Instead of applauding the RCMP for having acted in the interest of public safety, Public Safety Minister Steven Blaney echoed the complaints of the gun lobby by criticizing the RCMP for their "arbitrary" decision and announced a two-year amnesty for their owners, accompanied by a public bulletin specifically addressed to gun owners stating that "our Conservative government is on your side and will always defend the rights of honest gun owners". A few months later, new firearms classification regulations were passed, prohibiting the re-classification of firearms beyond one year after the day on which the initial classification was made." Winnipeg Free Press, A7

OTHER / AUTRES

Post-9/11 spy rules expire in U.S.
Monday marked a milestone in the United States' fight against terrorism, with the expiry of several major provisions of the controversial 2001 Patriot Act. Among the key changes: For the first time since the aftermath of the 9/11 attacks, Americans' phone records are no longer being systematically collected by the U.S. government. That phone-metadata program operated in secrecy for years, before it was among the many surreptitious programs revealed to the world by the now-fugitive whistleblower Edward Snowden. (…) What's changed? The National Security Agency immediately suspended its phone-metadata program. It's now harder for law enforcement to access business records such as hotel and credit-card information, and obtain wiretaps for investigations. Said White House spokesman Josh Earnest: "[This] introduces unnecessary risk to the country and our citizens." Canadian Press (Times Colonist)

More questions than answers about new deradicalization centre
Almost three months after Mayor Denis Coderre announced the creation of a deradicalization centre in Montreal to great fanfare, neither the city nor the police can say when it will be opened, what or where it will be, or even who is on board. Applications for the centre's director position are being accepted. But the radicalization hotline, set up the same day to receive calls from worried parents or friends, has been ringing: It has received 125 calls since March 9, and the police have intervened on three occasions, according to a statement released by the Montreal police on Monday. The hotline has also received calls for help from five "outside" sources — notably Collège Maisonneuve, the CEGEP where 11 of 17 youths who left Quebec or were arrested at the airport en route to Syria or Iraq attended classes. Montreal Gazette (2015-06-01)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à:
PS.PSPMediaCentre-CentredesmediasPSP.SP@ps-sp.gc.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
June 10, 2016 / le 10 juin 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Beef up number of Mounties abroad or lose ground on terrorism, organized crime
As the threat from terrorism and organized crime becomes more global, Canada's national police force is facing questions over whether to send more of its members abroad - in other words, take the fight to the bad guys before they land on our shores. A newly released internal report says the RCMP's "international footprint" is relatively small compared to its allies. While the RCMP has 55 liaison officers and criminal analysts abroad, Britain and Australia each have roughly twice as many. Unless the RCMP's international presence is beefed up, it runs the risk of being "unable to fully respond" to terrorism, drug trafficking, money laundering, illegal migration and cyber crime, the report warns. "The fact that combating criminality and instability in other countries leads to safer homes and communities in Canada should by now be beyond question, and ought to be both a cornerstone and raison d'etre of and for Canada's international policing efforts," says the report, completed by an RCMP analyst in late 2014 and obtained under access-to-information legislation. In an interview, RCMP Chief Supt. Eric Slinn said the number of deployments is constantly being evaluated. He noted the 55 personnel stationed abroad today are a "significant improvement" from the 38 members the force had just a few years ago. The fact that combating criminality and instability in other countries leads to safer homes and communities in Canada should by now be beyond question. "Quite candidly, I don't think we take a second seat behind anybody," he said. "We do in terms of numbers, but in our capabilities and our relationships and what we can leverage and get done, I feel very strongly we've got some solid people and we're doing a good job for Canadians." The release of the report comes at a time when public safety and intelligence officials are trying to keep tabs on roughly 180 people who left Canada and are suspected of engaging in terrorist activities abroad.
Postmedia Network (National Post) (2016-06-09)

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

'Violent sexual offender' faces new charges

A man **Yellowknife** RCMP previously warned the public about and called a "violent sexual offender" now faces 10 new charges, including sexual assault, in Pangnirtung, Nunavut. Jonah Keyuajuk was subject of the rare public warning that said he poses "a risk of significant harm to the public" in August of last year when he was being released at the end of a jail sentence. Police applied to have a judge place strict conditions on his freedom after release. Within a day of being released here last summer, he was charged with and later convicted of violating his conditions. He was sentenced in December to eight months in jail. It's not clear when or where he was released. The man with scorpion tattoos on his neck was arrested again May 22, this time in his hometown of Pangnirtung, according to Nunavut RCMP. Keyuajuk is facing charges that include sexual interference and forcible confinement. Sexual interference is when a person touches directly or indirectly a person under 16 in a sexual manner. Nunavut RCMP spokesperson Const. Lurene Dillon did not answer a question about whether RCMP warned residents in Pangnirtung about Keyuajuk. (...)An e-mailed question to Yellowknife RCMP about whether Mounties here warned police in Nunavut about Keyuajuk was not answered. Yellowknifer

Parolee ditches ankle monitor

A federal inmate released on parole earlier this month had no intention of following any of the conditions attached to his release. "I told them right from the start, I wasn't going [to Saint John] and I didn't want to leave the institution," said Andrew Donald MacKenzie in **Moncton** provincial court on Thursday. MacKenzie was arrested Wednesday on a charge of being unlawfully at large while serving a sentence and pleaded guilty. Prosecutor Eric Lalonde said the federal inmate was released on parole from a prison in the region on June 3 and he was wearing an ankle monitor to track his movement. MacKenzie was supposed to take a specified route to Saint John where he had to live while on parole. Instead, he came to Moncton and ditched his tracking device. Police were notified and found the device in the parking lot of CF Champlain shopping mall. MacKenzie was at-large for several days but on June 8 a Mountie in the street crime unit spotted him walking on Pioneer Avenue in Moncton and arrested him. Times & Transcript, A3

Relatives grateful for RCMP's work

Family and friends of a little girl who died from a devastating brain injury 12 years ago says no matter what a jury decides about the man accused of killing her, they'll finally have closure. The jury began Thursday deliberating in the case of James Paul Turpin, 37, who's accused of killing two-year-old Kennedy Corrigan in **Central Blissville** in April 2004. Deliberations will continue Friday. He was charged last year with second-degree murder, and his trial has unfolded over the past four weeks in a Fredericton courtroom. Turpin claimed Kennedy slipped in the bathtub while he had sole care of her the morning of April 2, 2004, and she struck her head. He had been dating Kennedy's mother, Connie Corrigan, in early 2004, which is why he was alone with the girl and his own three-year-old daughter in the Corrigan home on the date in question (...)Tracy O'Toole, Connie's best friend, said the family was relieved the case finally went to trial after so long. "This is what we wanted and so much more," she said. O'Toole read a brief statement from Connie Corrigan, who thanked the RCMP, witnesses and prosecutors for the work they put into Kennedy's case. Daily Gleaner, A5

Historical gravestones vandalized

Vandals toppled over and broke historical gravestones marking early Island settlers in a **Cowichan Valley** cemetery last week, RCMP say. "It's inexcusable," said Cpl. Krista Hobday from the North Cowichan/Duncan RCMP. "These are historical items dating back to the mid-1800s." Sometime between June 6 and 8, vandals pushed over 13 gravestones at the Pioneer Cemetery on the corner of Pioneer and Herd Roads, Hobday said. Two of the markers were broken. The cemetery holds the graves of the earliest settlers in the area, she said. Unfortunately, it is also known to be a party spot. "In other cemeteries, family or someone might replace the gravestones, but who is going to replace these ones? They're a piece of our history." Times Colonist, A5

Battleford RCMP warn of attempted child abduction
Battleford RCMP are investigating a report of an attempted abduction of a child from a school yard in Battleford. The alleged incident was reported to have occurred some time between 2 to 2:15 p.m. on Thursday June 9th. Police says a 10-year old child was grabbed by an arm and directed to come with the suspect to a nearby vehicle. The child screamed and the man was reported to have let go of the child and fled in the vehicle. The child was not injured during this incident. 620 CKRM

Quatre carabines et 500 plants de marijuana saisis
Un homme âgé de 33 ans a été arrêté à la suite d'une perquisition qui a mené à la saisie de quatre armes à feu et d'une importante quantité de plants de marijuana. Lundi, des agents de la GRC ont exécuté un mandat de perquisition dans une résidence de **Bairdsville**, près de Perth-Andover. La police affirme avoir saisi plus de 500 plants de marijuana à diverses étapes de croissance, ainsi que de l'équipement pour faire pousser de la marijuana, à l'intérieur comme à l'extérieur. Selon la GRC, une fois à maturité, le nombre de plants saisis aurait pu permettre de produire plus de 250 000 cigarettes de marijuana. La police a aussi saisi quatre carabines. Acadie nouvelle, 5

Des parents de Surrey demandent l'aide de la police pour sauver leurs enfants des gangs
Dix-sept familles ont déjà utilisé la nouvelle ligne d'urgence de la Gendarmerie royale du Canada (GRC) de **Surrey** qui sert à outiller les parents pour tenir leurs enfants loin des gangs de rue. La ligne téléphonique, disponible 24 heures sur 24, a fait son entrée le mois passé à Surrey. Selon l'agent Bill Fordy, l'objectif est d'offrir un outil supplémentaire aux familles de Surrey qui s'inquiètent de voir leurs enfants impliqués au sein de gangs de rue. « Plusieurs parents nous ont joints pour demander l'aide de nos agents spécialisés auprès de la jeunesse », dit-il. Depuis janvier, il y a eu plus de 40 fusillades à Surrey qui seraient, selon la GRC, causées par des groupes liés au trafic de drogues. La plupart des personnes impliquées dans les fusillades sont des adolescents et des adultes dans la jeune vingtaine. Le ministre de la Sécurité publique de la Colombie-Britannique Mike Morris, engagé dans ce projet de ligne téléphonique, espère faire comprendre aux jeunes et aux familles qu'il est possible de se sortir de l'univers des groupes criminels. La GRC a procédé à plus de 18 nouvelles arrestations lors des trois dernières semaines, mais aucune n'a mené à des accusations. Radio-Canada; CBC News (2016-06-09)

RCMP arrest and charge third teen in brutal assault north of Winnipeg
RCMP say they have arrested a third suspect in the violent assault of two workers at an addictions centre north of **Winnipeg**. During the May 29 attack Jackie Healey, a 23-year-old work placement student, suffered a fractured skull, broken teeth and blindness in her left eye. The other victim, a support worker at the facility, has extensive damage to her face, jaw and eye. Two youths, aged 16 and 17, were charged late last month with aggravated assault and robbery. Police say a third teen has been arrested and charged, but declined to provide further details. The Manitoba government has said it will conduct a workplace safety investigation into the attack at the Behavioural Health Foundation in Selkirk. Canadian Press (Brandon Sun); CTV News; CBC News (2016-06-09)

Lockdown lifted at Lethbridge's Senator Buchanan School after gun scare
Multiple people are in custody and a lockdown has been lifted at Senator Buchanan School after a report of a firearm. **Lethbridge** police said officers were on scene as of 1:45 p.m. at a home along the 600 block of 11 Street North. By 3 p.m., police were clearing the scene and said the investigation was ongoing. Police said the public no longer needs to avoid the area. Global News; Calgary Herald (2016-06-09)

Muskrat Falls entrance blocked by protesters
A group of protesters stopped traffic at the gate to the **Muskrat Falls** construction site Thursday. "[We] are trying to protect our people, our culture and our land," Jerome Jack told the CBC. Jack says he has been working for the Innu First Nation as an impact benefit agreement coordinator, but his phone has been cut off and he's uncertain of his employment. "A lot of deals were going on behind closed doors without my knowledge, without my people's knowledge, without my elders' knowledge." Jack says the First Nation was recently presented with an environmental assessment, including a caribou study, which he says was conducted by a private organization hired by Nalcor. (…)The protesters eventually let traffic out but say they will not be letting people in. "It seems to be a very peaceful protest." said Hubert Loder,

who represents the project's unionized workers. RCMP were on site to monitor the protest. CBC News (2016-06-09)

Cops seek man with info on missing girl
Police are looking for a middle-aged man who they believe may have information about the disappearance of Meykala Bali. A press release stressed the individual, described as a male between 40- and 50-years-old with stocky build and muscular arms, is not a suspect in any possible wrongdoing. Nevertheless they wish to identify and speak to him. The RCMP has received numerous tips including the unknown adult male may have information related to the missing 16-year-old Sacred Heart High School student. Yorkton This Week (2016-06-09)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Despite progress, domestic violence rates still high
Maria Hendrika has a penchant for sticking things through. If her long tenure with Regina Transition House wasn't enough, she has also been involved in the Provincial Association of Transition Houses and Services of Saskatchewan (PATHS) since its inception 30 years ago. The group was formed to provide a single voice for shelters, share best practices and set standards. (…) Saskatchewan has the "dubious distinction," as Hendrika called it, of having the highest rates of domestic violence and sexual assault as well. She wants to ensure that reports of assault are taken seriously and that there are safe ways for women to report. She would also like to see more attention paid to missing and murdered indigenous women. "This is a huge issue. People talk about murdered and missing like it's just a thing. No, these are people," said Hendrika. "These are daughters; these are wives." StarPhoenix, BR10

First Nations help with search for missing Enderby woman
Caitlin Potts and her family have been embraced by the Secwepemc people. Members of the Splatsin and other Shuswap bands gathered Tuesday to search for Potts, a 27-year-old originally from Alberta, who was reported missing in the Enderby area March 1. “This is a way to show we care for not only our people, but all people,” said Wayne Christian, Splatsin chief. (…) The search for Potts comes at the same time that the federal government is preparing for a national inquiry into missing and murdered indigenous women. “Our women are more prone to go missing than the average Canadian. Why is that?” said Shane Gottfriedson, regional chief of the Assembly of First Nations. Gottfriedson believes contributing factors are poverty and the generational impact of residential schools. “It’s up to us in our communities to look at strategies to protect our families and relatives,” he said. Salmon Arm Observer (2016-06-09)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

RCMP's BlackBerry-cracking methods could be revealed in Quebec court
A Quebec court could today pull back the curtain on secretive police techniques, including how the RCMP intercepted BlackBerry text messages to prove a murder conspiracy plot, as a judge considers whether to lift a publication ban in a case involving the Montreal Mafia. The case stems from Project Clemenza, a police operation that resulted in scores of organized crime arrests in 2014. At the time, police announced they had intercepted more than one million BlackBerry messages tied to allegations of drug trafficking, kidnapping, arson, weapons and other violent offences. (…) Chief Supt. Jeff Adam, who oversees the RCMP's Technical Investigations Services, declined to discuss with CBC News the specific methods used. But given rapid changes in technology and public concern in the post-Snowden era, as mobile developers move toward more secure "end-to-end" encryption, he says investigators are finding their jobs increasingly difficult. "What we're seeing now is … the best evidence of people conspiring to commit a crime is lost to us. And that's what we call 'going dark,'" Adam said. CBC News

Opération Malaise sur l’exploitation sexuelle d’enfants: 2 arrestations vendredi

Deux autres suspects ont été arrêtés jeudi lors d'un nouveau volet de l'opération policière baptisée Malaise qui lutte contre l'exploitation sexuelle des enfants sur Internet. La Sûreté du Québec (SQ) rapporte que Jean Simoneau, 73 ans, de Magog, et Ross Perrin, 62 ans, de Montréal, qui faisaient l'objet de mandats d'arrestation, comparaîtront au tribunal vendredi au Palais de justice de Montréal. Ces deux hommes devront faire face à des accusations en lien avec des contacts sexuels qu'ils auraient eu avec des gens d'âge mineur et pour de l'exploitation sexuelle. (…) L'Équipe d'enquêtes sur l'exploitation sexuelle des enfants sur internet (ESEI), qui a procédé aux arrestations, regroupe des enquêteurs de la Sûreté du Québec et de la Gendarmerie royale du Canada. Presse canadienne (L'Actualité, Huffington Post, La Presse)

La F1 crée 4 fois plus d'offres d'escortes
Le nombre d'annonces d'escortes offrant des services sexuels sur le «Kijiji du sexe» a quadruplé à l'approche du Grand Prix de Montréal, d'après un outil d'analyse créé par un ex-policier. Pas moins de 1000 annonces ont été placées pour la grande région de Montréal dans la seule journée d'hier sur ce site dont nous tairons le nom pour ne pas nuire aux enquêtes policières. «La promotion est moussée pour le Grand Prix. C'est vraiment la manne pour les proxénètes», explique Paul Laurier, un ex-policier de la SQ qui a créé un outil d'analyse pour traquer les *pimps*. Les mots «Montréal», «Grand Prix», «F1» et «Pornstar» apparaissent maintenant en tête de liste des mots-clés les plus utilisés, ce qui n'était pas le cas il y a une semaine à peine. (…)Les policiers attendent toutefois de pied ferme ces escortes de l'extérieur et leurs proxénètes, ainsi que les clients qui pourraient requérir leurs services. (…)On accordera une attention particulière aux mineures victimes d'exploitation sexuelle, tant dans les commerces ou les hôtels que sur le web. La frontière canado-américaine et l'aéroport de Montréal seront aussi plus surveillés qu'à l'habitude. «Nos agents peuvent déceler si une voyageuse se trouve sous l'emprise d'une autre personne qui l'accompagne. On va mettre l'accent là-dessus», rapporte Dominique McNeely, porte-parole de l'Agence des services frontaliers du Canada. Des dizaines de policiers de la GRC seront aussi présents «dans des lieux stratégiques» pour appuyer le SPVM. Journal de Montréal, 27 (Journal de Québec)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Complaint against RCMP in limbo
A young woman who went to the police station in search of an acquaintance was struck in the face and legs by RCMP officers while in handcuffs, a year-old complaint alleges - one that remains unresolved to this day. The Jan. 7, 2015 incident, which was captured on video, prompted her lawyer Gary Wool to file a complaint on the woman's behalf with the Civilian Review and Complaints Commission for the RCMP, which investigates allegations from the public of Mountie wrongdoing. The woman was charged with assault causing bodily harm to a police officer, a charge withdrawn after the Crown prosecutor viewed the video at her lawyer's request. The Lethbridge Regional Police Service in Alberta was called in to carry out a criminal investigation. The complaint filed in May of last year is based on surveillance footage because the woman doesn't have a clear memory of what happened. The complainant, who Yellowknifer has been unable to contact and whose name has been withheld in records obtained, went to the city's RCMP building on 49 Avenue after being told someone she knew was being held by police. (…)She was handcuffed and taken to the booking area. Her shoulders were being held by Const. Miranda Porr and Const. Cory Wallace and her face was about three inches from a wall. (...)Three years ago Wallace admitted to a March 2013 assault against a prisoner in courthouse cells. However, the charge was stayed in court by the Crown after the officer attended a community justice hearing. (…)The complaint was taken seriously by the complaints commission. A cover page on the report sent to RCMP Commissioner Bob Paulson in Ottawa states the allegations "may require a code of conduct or criminal investigation." Yellowknifer

ASIRT looks into gunfire, alleged bid to ram into officer's car
An investigation is underway into the circumstances surrounding an RCMP officer firing his weapon Wednesday after a police vehicle was allegedly rammed. The Alberta Serious Incident Response Team, or ASIRT, said Thursday it was conducting an investigation into the events that unfolded when Spirit River RCMP responded to a report of a suspected impaired driver. RCMP said that an officer caught up

with the vehicle, a black Ram 3500, on Range Road 61 on Wednesday afternoon. The driver allegedly turned and sped toward the officer's Chevy Tahoe. The officer got out and the pickup accelerated toward the officer. ASIRT said only that an "incident occurred" that led to the police officer firing his gun. RCMP made no mention Wednesday of the officer firing his weapon. The suspect was later arrested without injury, ASIRT said. He has not been formally charged. Edmonton Journal, A11; Global News (2016-06-09)

Mountie trades gun for horse

The face of the RCMP in the NWT has left her post in Yellowknife to join the iconic RCMP Musical Ride. Const. Elenore Sturko's last day on the job in Yellowknife was June 3. She had been the Mounties' media liaison officer for Yellowknife and the NWT since September 2014. Sturko lived in Yellowknife back in 2004 when she worked for CBC North. In 2010, she left the media organization to join the RCMP and began her policing career in Langley, B.C. She was posted back in Yellowknife in 2012. The musical ride, based in Ottawa, is performed by a full troop of 32 riders and their horses. Their performance consists of intricate figures and drills choreographed to music. Sturko said she had to go on a five-week course to determine whether she is suitable for the musical ride. (...)It is not clear who, if anyone, is going to replace Sturko as media relations officer. Yellowknifer

Edmonton holds inaugural First Responders Day to show appreciation

When bad things happen, they're the first to step up. They walk into burning buildings, while others run away. They face down dangerous criminals, pull people from twisted car wrecks, rush them to hospital. On Thursday, Edmonton said thank you by commemorating June 9 as the city's first ever First Responders Day. (...)First responders with Edmonton police, emergency medical services, fire rescue, sheriffs, peace officers, the military fire department, corrections and the RCMP were all acknowledged. CBC News (2016-06-09)

Justice dept. pledges to save money

Manitoba's most popular baby names these days are Liam and Emily, Justice Minister Heather Stefanson revealed Thursday morning. Stefanson announced the information as the minister responsible for vital statistics, as she and critic Andrew Swan kicked off a civil and relatively tame first hour of committee hearings into Stefanson's departmental budget. (...)Stefanson said the province is spending $325,000 for three RCMP officers to serve as provincial police on Sioux Valley First Nation near Brandon, after that community opted out of Dakota-Ojibway policing. Justice is spreading an additional $232,000 among five agencies providing services to victims of crime, and $44,000 will allow retired justices of the peace to help clear up backlogs in traffic court. Winnipeg Free Press, A4

Windsor Yacht Club hopes high after $850,000 harbour project

Stormy weather didn't dampen the spirits of the members of the Windsor Yacht Club as they dedicated the newly refurbished harbour and blessed the fleet for the year. A weekend of festivities officially celebrated the $850,000 renovation project's completion Arts. JASON KRYK Windsor Yacht Club commodore Chris Colthurst drops a wreath into this spring. Work included a dredging of the harbour and the addition of new breakwalls, a perimeter harbour configuration that now allows larger boats to dock, and upgraded services. On hand Sunday for the Blessing of the Fleet were many of the club's 350 members along with Windsor Coun. Ed Sleiman and representatives from the Canadian and U.S. Coast Guards, the City of Windsor Harbour Master, Royal Canadian Mounted Police, Ontario Provincial Police, Windsor Fire and Rescue and the HMCS Hunter. Windsor Star, SR5

Phone service down in Fort Liard, N.W.T., including RCMP number

Phone customers in Fort Liard, N.W.T., are experiencing a disruption to local and long distance services, according to Northwestel. In a news release, the company says emergency services have been notified and technicians are heading to the community. Cellular phone and DSL internet services have not been affected. The local RCMP phone number has also been affected by the outage — calls to (867) 770-1111 are not being forwarded to dispatch in Yellowknife. The RCMP is asking people in Fort Liard to call Yellowknife RCMP detachment directly at (867) 669-1111 for any police-related services. The operators in Yellowknife are able to contact officers in Fort Liard. Northwestel says people should be prepared to be

without service for several hours, as repairs are completed. There's no word on the cause of the disruption. CBC News (2016-06-09)

New look at RCMP space
City council will take yet another look at the overcrowded Vernon/North Okanagan RCMP premises in the downtown and the possibility of a new building. "That was talked about last council and now we'll be talking about it in the coming months," confirmed Mayor Akbal Mund. City council gets a progress report Thursday on its five-year strategic plan. Goals and timelines will be reviewed, with the RCMP at the top of a long list of items. "Definitely, we need more space for the RCMP. That's been on the radar for the past 10 years," said Mund, making it clear new premises would not come soon and that the discussion will include whether a new building was needed or an expansion of the old one. Of key concern is money. "Obviously there will be funding issues. I mean looking at building costs, probably $56 million, so it's a ways away but you do have to plan for it." In Summerland, a new detachment was funded through a provincial grant – while in Kelowna, the new $48 million structure is being funded primarily by local taxpayers. "We need to now put it into a plan and see how, eventually, we'll fund that," said Mund. When asked if an RCMP building could precede a proposed new cultural facility that would house Greater Vernon's museum and art gallery, Mund said, "definitely not." "I mean we've already passed the arts and cultural plan so that's going to proceed a lot quicker than any RCMP building will." An email to RCMP Supt. Jim McNamara about conditions in the building was not returned. Castanet (2016-06-09)

Ceremony honours Const. Carl Dixon
A former RCMP officer was recently remembered at a ceremony in Sechelt, where he spent his RCMP career serving his own community. RCMP Const. Carl Dixon, a member of the shíshálh Nation, joined the force in 1977 and spent his 20-year career working in his home community of Sechelt. Coast Reporter (2016-06-09)

Third time lucky for RCMP soccer match
The long-awaited soccer game between Special Olympic athletes and the local RCMP went off without a hitch on Thursday June 2 at the Chatelech Secondary soccer field. Last year, the game didn't happen because of a police emergency. This year, on their second try, the game was called on account of the lightning storm that hit the Coast. The third time was lucky, and players, officers and spectators all had a blast. Coast Reporter (2016-06-09)

Above and beyond: Surrey RCMP recognizes heroism and outstanding contributions
DARING rescues, dangerous encounters, dogged determination, and dedication to those less fortunate. On Wednesday, June 8, Surrey RCMP's Officer in Charge held his annual awards ceremony where heroic actions and outstanding service to the community were honoured. "Every year, we take the time to celebrate the men and women who have demonstrated tremendous heroism and outstanding service to our community," said Assistant Commissioner Bill Fordy. "This is an opportunity to highlight the excellent work being done by those in our detachment and in our community who are making this city a great place to live, work, and play." Voice Online; The Now (2016-06-09)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

Liquor board bosses, RCMP take part in planning for legalized marijuana market
Liquor board heads from across the country have quietly been meeting in New Brunswick with government officials from each province over the future sale of marijuana. The private gathering in Saint Andrews included a presentation from a top federal enforcement cop, panel discussions with industry growers, and research from policy experts in preparation for the sale, distribution and regulation of pot - now that Ottawa is moving toward legalization. The result of the multi-day meeting will now see liquor bosses move to brief their respective governments on the best practices they discussed at length with North America's top marijuana authorities. "Attendees were from the liquor boards, the Departments of Public Safety from each province and senior leaders from the beverage alcohol industry," said NB Liquor president and CEO Brian Harriman in an email. The Telegraph-Journal reported earlier this year that the NB Liquor boss has been heading research by liquor boards from across the country to prepare for

legalized pot. The annual summer meeting of the Canadian Association of Liquor Jurisdictions was then slated for New Brunswick, stretching from this past weekend until Wednesday, with an entire roster of marijuana players lined up to speak. That included RCMP Cpl. Shane Holmquist, a supervisor on the Federal Serious Organized Crime Section's marijuana enforcement team. (…)Harriman said the meeting had more than 200 attendees from across Canada. Provincial government spokeswoman Elaine Bell said it was actually the Department of Public Safety that hosted the Association of Liquor Administrations of Canada at the annual conference. "While the legalization of marijuana is a federal decision, the working group of officials from multiple departments and agencies continues its work in anticipation of legislation to be tabled by the federal government in the future," Bell said. The working group is gathering research and assessing policy implications, with a balanced focus on examining health and safety risks and identifying job and revenue-generation opportunities for the province." Prime Minister Justin Trudeau has proposed legalizing and regulating pot, also pledging to work with local authorities to come up with distribution methods, which could vary from province to province. Times & Transcript, A1 (Telegraph-Journal, Daily Gleaner)

Fentanyl a factor in more than half of fatal overdoses in B.C.
A powerful synthetic opioid that just years ago was largely restricted to hospitals and people living with chronic pain is now found in more than half of all illicit drug overdose deaths in British Columbia. From January to April, fentanyl was detected in 56 per cent of all deaths from overdoses of illicit drugs, according to new figures from the B.C. Coroners Service released on Thursday. This is up from 31 per cent last year, 25 per cent in 2014, 15 per cent in 2013 and less than 5 per cent in 2012. Health and police officials have feared for some time that illicit fentanyl, produced overseas and imported into Canada, is flooding the black market and things will get worse before they get better. A recent Globe and Mail investigation found that local traffickers can easily order the highly potent, low-cost drug online and have guaranteed shipment to Canada. It is then cut into street drugs such as heroin and oxycodone to make them go further and maximize profits. Chief coroner Lisa Lapointe said the number of deaths from illicit-drug overdoses in B.C., spurred by the growing presence of fentanyl, is now "much more significant than any other type of unnatural death in the province." From January through May this year, at least 308 people died of illicit drug overdoses - a 75 per cent increase over the same period last year (176). In comparison, for all of 2015, there were 300 deaths in incidents involving motor vehicles, and 122 homicides. "If this [illicit drug overdose] trend were to continue, we'd be looking at about 750 deaths this year," Ms. Lapointe said on Thursday. The 308 deaths represent 10.2 per 100,000 population - a rate not seen since 1998 (10 deaths per 100,000 population). The recent surge prompted B.C. health officials to declare a public health emergency in April. Globe and Mail, A1

Despite the crackdowns, marijuana entrepreneurs are betting on "edibles"
Virginia Maria Vidal started medicating with marijuana in 2003, after the birth of triplets left her with post-natal discomfort. She ran into trouble over the years, once being arrested, charged, and eventually acquitted of possessing 19 grams of pot. Even after obtaining a licence to use medical marijuana, the 45-year-old mother of six and caregiver to a grandparent with dementia found the smoke to be a nuisance and embarrassing. So she ground it into tea instead. (…) Ms. Vidal says the crackdowns aren't having a big impact on revenue – she also sells her product online and says demand is growing – but she's still worried. "It's going to be quite the battle," she says. "We need our Prime Minister to stand with us." Producing edibles in any form is illegal, however jurisdictions such as Vancouver and Victoria have chosen to ignore the law and regulate them instead. The federal laws are rarely enforced because the framework of regulations governing marijuana for medical purposes is evolving, and unlicensed producers continue to sell in stores or by mail. Last year, a Supreme Court judgment ruled that licensed patients couldn't be limited to consuming cannabis in smoking form only, but did not comment on the legality of edibles. Further, in February a federal court struck down restrictions preventing licensed patients from growing their own medical marijuana, giving the government six months to rewrite the laws. Globe and Mail

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Smoke shops not helping Dakota First Nations

An editorial states, "Earlier this week, several Dakota First Nation members who were charged for selling contraband tobacco lost a legal bid to have the case tossed out on the grounds that their people have no official treaty with Canada, and therefore the courts have no jurisdiction. As the Winnipeg Free Press reported, the two accused, - smoke shop owner Craig Blacksmith and employee Tammy Walters – were arrested during a 2014 raid by RCMP on Dakota Plains near Portage la Prairie. RCMP, the Dakota Ojibway Police Service and Manitoba Finance taxation officials seized 4,800n cartons, which amounted to 951,225 cigarettes. More than 1,840 tins of chewing tobacco, six firearms, one vehicle and an unspecified amount of cash were also seized. All told, finance officials calculated $292,572.68 of tax was avoided. (…) For anyone who has been following the ongoing and controversial issue of the non-treaty Dakota in western Manitoba, this argument – that Dakota Plains has no official treaty status in Canada, and therefore should not be subject to Canadian law – is a familiar refrain, one that has not seen much traction in our federal or provincial courts." Brandon Sun

Counterterrorism Plans Won't Be Effective Until Biases Are Addressed

An opinion piece by Monah Mazigh states, "Last federal budget, the government announced plans to create a counter terrorism office. This new initiative named as the Office of the Community Outreach and Counter-radicalization Co-ordinator would cost Canadian taxpayers $35 millions dollars. With an initial funding of $3 million in 2016-2017 and a $10 million a year in the subsequent years. According to the government, the office is supposed to "provide leadership on Canada's response to radicalization to violence." So far, no details have been disclosed about this office but Public safety Minister Ralph Goodale recently reiterated his strong commitment to it. In an op-ed, he published on "How to Fix Canada National Security Framework," he stated: "Thirdly, this summer we will launch a new national office and center of excellence for community outreach and engagement. Its purpose will be to develop and coordinate expertise in identifying those who could be vulnerable to the pressures and appeals of radicalization to violence, and to connect with them constructively in advance to head-off tragedies before they happen. As an open, pluralistic society, we need to get really good at this." As it can be understood from Mr. Ralph Goodale words, one of the tasks of the office would be to develop expertise in identifying some sort of "indicators" about people who are at risk of radicalization to violence. Indicators are defined as cognitive and behavioural changes in individuals and draw from them patterns about radicalization. For instance, someone who withdrew from his/her family or change his/her in behaviour in school in certain specific ways, these are considered as "indicators." Mr. Ralph Goodale doesn't use any word directly relating radicalization to Islam or Muslims in particular, but obviously it is everyone's mind that this office will be directed, if not entirely but in major part, for and about Muslims. And this is exactly why this approach won't be effective." Huffington Post (2016-06-09)

OTHER / AUTRES

Quebec will soon have registry

Bill 64, which requires the registration of long guns, was adopted on Thursday at the National Assembly, on the eve of the adjournment of the current parliamentary session. Since its filing last December, the bill to provide Quebec with a firearms registry did not have unanimous approval among the population, particularly in rural areas where there are many hunters. The bill passed with 99 votes in favour and eight against. There were no abstentions. About a third of the Coalition Avenir Québec (CAQ) caucus, seven MNAs, voted against the bill, as well as Sylvie Roy, a former CAQ member from Arthabaska, who became an independent. Premier Philippe Couillard imposed party discipline on his MNAs in order to pass the bill, but not the CAQ; their caucus was divided on the issue. Some Liberals and members of the PQ had reservations, but all rallied in the end, passing the bill. The bill was tabled last December by Public Safety Minister Pierre Moreau, and it was his successor, Martin Coiteux, who brought it to fruition. The gun registry, once in place, probably in 2018, will replace the federal firearms registry that was abolished by former prime minister Stephen Harper. His decision triggered concerns in Quebec. Under Bill 64, any firearm on Quebec territory must be registered with a unique number, and shall be listed in a file. Montreal Gazette, A10; Presse canadienne (Voix de l'Est, Le Quotidien, Le Soleil, La Tribune); Agence QMI (Journal de Québec); CBC News; Presse Canadienne (Journal Métro, L'actualité) ; Canadian Press (CTV News) (2016-06-09)

Activist once linked to Ottawa bank firebombing posts pro-arson anniversary message
An activist once linked to the firebombing of a bank branch in a trendy Ottawa neighbourhood has published a blog post suggesting arson is a legitimate tactic for direct action. Matthew Morgan-Brown was one of three men charged in connection with the May 2010 firebombing of a Royal Bank of Canada outlet in Ottawa's Glebe neighbourhood. The bank attack was done partly in the name of Indigenous rights. (…) Morgan-Brown tagged several people on his Facebook page post including Roger Clement, a retired civil servant who was sentenced to three-and-a-half years in prison after he pleaded guilty to the firebombing. Clement was released in March 2013 after serving about two years of his sentence. He was also visited by CSIS, Canada's spy agency, while incarcerated. The second man, Claude Haridge, a known local antiwar activist, was under surveillance following the firebombing. This led OPP investigators to find over a thousand rounds of ammunition buried by Haridge in a forested area. APTN (2016-06-09)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
July 20, 2016 / le 20 juillet 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Reports could hide true police activity
Clear gaps" in how the federal government reports invasive surveillance practices may hide the true scope of police activities, according to documents prepared for Canada's privacy watchdog. Although the number of authorized wiretaps has "plummeted" since 2002, a January briefing for Privacy Commissioner Daniel Therrien suggests those numbers may mask police surveillance practices. "It would be erroneous to infer from the drop in overall warrants issued that surveillance is affecting fewer individuals," reads the document, obtained under access to information law. "While federal authorities issued just over a hundred surveillance warrants last year (2014), they issued 792 notifications of surveillance to individuals previously targeted. From this, one can conclude more and more individuals are being named as targets in a warrant application. "With a single warrant from the Federal Court (police) may list dozens of individuals for surveillance targeting." Public Safety is required to issue a report each year about the number of warrants sought to put individuals under surveillance - "wiretap" warrants that allow police extraordinary powers to keep tabs on individuals. But police aren't just bugging the phones of bad guys anymore. New technology allows law enforcement agencies to conduct surveillance on a much wider scale. (…) Canada has also seen confirmed uses of "Stingray" technology, a device, called an IMSI catcher, that simulates a cellphone tower to force any mobile device in the area to connect to it. A recent Vice News investigation reported the RCMP has used IMSI catchers in public places for more than a decade, citing court documents. The Star requested an interview with both Therrien and Public Safety Minister Ralph Goodale for this article. Neither was available Wednesday or Thursday. But in an emailed response to the Star, a spokesman for Goodale said the minister is open to changing the system.

"Reporting is an important component of Canada's system accountability for security agencies," Scott Bardsley wrote. "We're open to consideration in this review (of national security oversight) of how to improve these elements to better achieve our two objectives (of) ensuring that our police and security agencies are being effective ... and safeguarding the values, rights and freedoms of Canadians in a plural, open, democratic society." The Guardian, A6 (The Telegram, Whitehorse Daily Star)

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

Boylston man charged after threatening RCMP with firearm
A 20-year-old man arrested after threatening citizens and RCMP officers in **Guysborough District** on July 13 has been remanded to the East Coast Forensic Hospital for assessment. William Anthony Pius George appeared in Port Hawkesbury Provincial Court on Friday. He is scheduled to be back in court on August 5 to answer to the charges. At 9 p.m. July 13, RCMP responded to a dispute on East Side Harbour Rd. where a man had broken the windows out of a residence and vehicles. Police arrived and were told by witnesses that he had threatened to kill individuals inside the residence and discharged a rifle multiple times prior to their arrival. According to RCMP, the man then threatened to kill police. RCMP officers moved the individuals inside the residence to a safe location and called in additional RCMP officers from neighbouring detachments and the Nova Scotia RCMP Emergency Response Team (ERT). The situation was resolved when the man surrendered to the RCMP just after 5 a.m., without incident. No one was injured. The individuals inside the residence and the accused are known to one another. George has been charged with uttering threats (8 counts), assault, careless use of a firearm, unauthorized possession of a firearm and mischief. Guysborough Journal

Police charge ex-boyfriend with murder
After Carol King's body was found in an abandoned farmyard near **Herschel**, Sask., her ex-boyfriend said he had nothing to do with her death. In an interview, he claimed he was "the fall guy" for the 2011 killing that rocked the small farming town. Almost five years later, that man, Joseph 'David' Caissie of Bluffton, Alta., is charged with first-degree murder. "We start with the people closest to the victim and attempt to clear them and work their way out. In this investigation, we were never able to clear Mr. Caissie," RCMP Staff Sgt. Murray Chamberlin told reporters at a news conference announcing the arrest. Carol King went missing on Aug. 6, 2011. Chamberlin said Caissie was taken into custody in Saskatoon without incident. He is also charged with offering indignity to human remains. Caissie is scheduled to appear Wednesday in Saskatoon provincial court. "We are extremely sad but extremely happy at the same time, and have a sense of relief knowing that charges have been laid," Carol King's family said in a statement. Caissie had been under the microscope of RCMP investigators for years, but had long proclaimed his innocence. Postmedia Network (StarPhoenix, A1, Leader-Post); Canadian Press (Edmonton Journal, Toronto Star, Red Deer Advocate) (2016-07-20); Global News; CTV News; Radio-Canada; 620 CKRM (2016-07-19)

Father says daughter 'fell through the cracks'
Kent Robinson just wanted his daughter to come home. Cynder Robinson, 17, lived on a northern reserve, away from family, for nearly a year. By the time he convinced her to return, it was too late. "Obviously it was a dangerous situation. I knew that right away," Robinson said. "I don't want to let it rest. I don't think my daughter should have ever been there." Cynder was found dead inside a home on the **Big Island Cree Nation** on Friday. RCMP called the death suspicious, but would not confirm a homicide investigation is underway. An autopsy was scheduled for Tuesday in Saskatoon. Cynder's father said he tried to get her to come home to Taber, Alberta for months, but because she was over 16, the RCMP and social services workers could not force her to return. "Cynder was a beautiful, beautiful soul. She just made the one mistake and it cost her life," Robinson said. Few details have emerged about what happened inside the home, but Robinson said his eldest daughter suffered from an arachnoid cyst that made her more susceptible to fatal head injuries. (...) He said he doesn't know for sure if his daughter was killed or if she died of natural causes. If someone did kill her, he wants justice, he said. "She was not a violent person. She knew she couldn't be a violent person because of her condition," he said. (...) Trevor Kahpeepatow, a Big Island band councillor, said it's not uncommon for non-band members to spend time on the reserve, although it is usually temporary. He said Cynder was a well-known face

around the reserve and that her death has hit hard. "It is a shock," he said He and the band council are working hard to make sure the reserve - which is technically a dry community - is a safe place, Kahpeepatow said, adding they are trying to get tough on the drinking rules and deal with some of the root problems in the community. StarPhoenix, A3

New Kelowna criminal gang is small but dangerous

When RCMP arrested a member of a new street gang in **Kelowna** this month, it was a significant blow to the organization. "They are what we consider a low level street gang (present) only in the immediate Kelowna area," Staff sgt. Lindsey Houghton of the B.C. Combined Forces Special Enforcement Unit says. "You can count their members on two hands." The gang came to light last week when a cache of guns, drugs and a vest bearing an unfamiliar crest was displayed to the media by local police after a warrant was executed at a home in West Kelowna. Two men and a woman were arrested and a seven-year-old child found inside the home was brought under the care of the Ministry of Child and Family Development. A 24-year-old West Kelowna woman was questioned and released. A 37-year-old West Kelowna man is expected to appear in court Oct. 13 on possible drug and firearms related charges and a 32-year-old West Kelowna man, Tyson Ashleigh Bone, remains in custody. Const. Jesse O'Donaghey said Bone is a member of a small, new gang called the Kelowna Warriors. "They've been around for about four years," Houghton confirmed on July 19. "Mostly street-level stuff like drugs but often times they are the most dangerous." Houghton says there are fewer than ten members and that membership changes quickly. "We see a lot of transiency at levels like this," he says. "They say they're in one group one day and then swear allegiance to another the next day." The vest taken from the West Kelowna home included three patches, a central logo and the name of the city and gang above and below. "In order to wear the three-piece patch you have to get the consent of whichever outlaw groups control the area. In Kelowna it's the Hells Angels." Houghton says although they likely have permission from the Angels to operate, there is no evidence of cooperation between the groups. InfoTel (2016-07-19)

Burnaby 'demoviction' protesters continue fight for affordable housing

Protesters occupying a building slated for redevelopment in **Burnaby**, B.C., are renewing their call for affordable housing as the building approaches its demise. "I hope the politicians, you know, do something or take it serious," said a man who has been living in the building who referred to himself only as Mohammed. "These are people, they are not trash on the street. They're being treated like trash."The protesters have occupied the building at 5025 Imperial Street since July 9. They previously told CBC the developer, Amacon, would begin removing hazardous materials last Monday to prepare for demolition in August. Burnaby RCMP have obtained a court injunction to clear out the group, which is operating under the name Alliance Against Displacement. CBC News

Four suspects face charges after drug bust

Four people are facing charges after Mounties seized approximately 200 fentanyl pills and other drugs during a traffic stop in southern Alberta on Sunday afternoon. **Pincher Creek** RCMP said they stopped a vehicle for a "serious traffic violation" at around 4 p.m. in the town about 200 kilometres south of Calgary. Inside the vehicle, police found a backpack containing approximately 200 fentanyl pills, three ounces of methamphetamine, nearly two ounces of crack cocaine, a small amount of marijuana and a large amount of cash. RCMP say there was also open liquor in the vehicle. Sebastion Aranzalez, 21, of Calgary, Ruairi McGinnity, 22, of Lethbridge, Christie Reed, 39, of Pincher Creek, and Sherri Lagrandeur, 40, also of Pincher Creek, are charged with possession of a controlled substance for the purpose of trafficking. Police say Aranzalez was also charged with driving with no licence and careless driving. All four were released with conditions ahead of their court appearances. Calgary Herald, A10

La GRC invite à la prudence

La GRC a demandé aux joueurs de Pokémon Go de faire preuve de «gros bon sens». Des amateurs de l'application mobile l'utilisent en conduisant pour couvrir du terrain plus rapidement et ainsi attraper plus de Pokémon, au détriment de leur sécurité et de celle des autres. La gendarme Isabelle Beaulieu rappelle que l'utilisation du cellulaire au volant est interdite au N.-B. et souligne que les agents circulent sur les routes de la province, aux aguets pour repérer les conducteurs distraits. Toute personne arrêtée en train d'utiliser un appareil électronique au volant d'un véhicule à moteur s'expose à une amende de

172,50$, en plus de voir soustraire trois points d'inaptitude à son permis de conduire. Elle demande aussi aux utilisateurs de ne pas s'introduire sur des terrains privés. Acadie Nouvelle, 5

RCMP 'apprehend' trespassing Squirtle and offer advice for playing Pokémon GO
RCMP officers in the small town of **Kindersley**, Sask., have caught a mischievous blue monster on private property and have the photos to prove it. At least that's according to a humorous post on the RCMP attachment's Facebook page addressing the latest pop culture craze known as Pokémon Go. The photo shows an RCMP officer holding a virtual image of a Pokémon character captured inside the wildly popular augmented reality mobile game, which was recently released in Canada. "In the late morning of July 18th, 2016 Kindersley RCMP were called to a possible trespasser on private property. When RCMP Cst. Hill arrived on scene of a private lot he encountered a light blue creature that resembled a turtle," the tongue-in-cheek post reads. "The little pip-squeak was very cooperative and was transported to the Kindersley RCMP Detachment where his family was called after he was taught how important it is to stay safe while playing #PokémonGo" The Kindersley RCMP is just one of several different police departments across North America responding to the new mobile app game. Players are encouraged in Pokémon Go to explore their local surroundings, including numerous real-world landmarks, in a quest to capture and battle various virtual monsters. "Yes, we have already gotten more than a handful of calls in relation to the game. We love PokemonGo just as much as you and if you feel the need to run around playing it this summer, that's cool, just be smart about it." The post ends by reminding players to always keep aware of their surroundings, respect private property and to not operate a motor vehicle while attempting to become a Pokémon master. Yahoo! News (2016-07-19)

RCMP not letting youth off the hook following prank bomb threat at Vernon mall
Police are sending a message after the latest incident of swatting — deceiving law enforcement with a phoney call — led to major disruptions at a **Vernon** mall. The prank resulted in numerous employees and patrons being evacuated from the Landing Plaza for several hours while police investigated. But it's not the first time emergency officials have been 'swatted.' Last year in Kamloops, several schools were locked down due to swatting pranks involving fake bomb threats. The same thing happened in Toronto, and a host of other cities. Sgt. Mike Moyer of Vernon RCMP says a youth was identified as the source of the prank call in Vernon and won't be let off the hook for the crime. Given the seriousness of the incident, Moyer says they will be recommending criminal charges, including mischief and possibly more, to Crown counsel. "Obviously, it scares a lot of people, especially with what's going on worldwide," Moyer says. "We, as the police, take these calls very seriously." Significant resources were deployed to the incident, including specialized RCMP units, the Vernon Fire Department, B.C. Ambulance Services and bylaw. Numerous businesses were forced to shut down, equating to thousands of dollars lost, Moyer says. And while the threat was a hoax and no one was hurt, Moyer says they want to make it clear pranks like this one are a crime and will not be tolerated. "We want to send a strong message," Moyer says. InfoTel (2016-07-19)

RCMP nab alleged drug traffickers
The **Wood Buffalo** RCMP Drug Unit arrested two individuals on July 15 after receiving a tip through Crime Stoppers of a male and female selling drugs in a Thickwood apartment building. Tristen Bradbury, 19 and Jennie Podanovitch, 19, both of Fort McMurray, were arrested Friday when they were leaving their Signal Road residence. RCMP spokesperson Cpl. George Cameron said officers opened an investigation after receiving the tip at the beginning of June. "There was enough evidence in order for the courts to grant a search warrant," Cameron said. Officers located 144 grams of cocaine, 49 grams of marijuana and 1.5 fentanyl pills after searching the apartment. Cameron couldn't give an exact amount, but estimated the drugs to be worth "thousands of dollars." Also inside the residence was a shotgun and ammunition and approximately $35,000 in cash believed to be proceeds from selling drugs. Bradbury and Podanovitch were both charged with possession of cocaine and marijuana for the purpose of trafficking, possession of fentanyl, possession of property obtained by crime, unauthorized possession of a firearm and unsafe storage of a firearm. Fort McMurray Today (2016-07-19)

Attempted child abductions in Carbon believed to be false: update
Drumheller RCMP has concluded their investigation into reports of attempted child abductions in the village of Carbon late last month and want to reassure parents in the community they believe there is no

further threat. Reports of three Carbon youth being approached and lured by two men in a vehicle were made to RCMP on June 29. After investigating and interviewing a male individual who was positively identified by RCMP, police feel the suspect holds no threat to the community and the reports may have resulted from both fabrication and fear from the three youths involved. Drumheller RCMP Constable Jason Gerard tracked down the individual and the suspect vehicle, but after interviewing him, felt the individual was incapable of the crime due to a mental illness related to an accident. "Judging from the stories from the three youths involved the stories and descriptions of the male didn't fit in. The descriptions range all around," said Cst. Gerard. Cst. Gerard said the man lives just outside of Carbon and is frequently in town. "I guess this person usually sits in town and uses the WiFi in one area of town, and he's one of those people that park in town and who people look at and think there's something weird about him. Stories can get blown out of proportion." Drumheller Mail (2016-07-19)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Zoe Saldana producing film on Canada's missing indigenous women
A new documentary by a team of Los Angeles-based filmmakers – including Avatar star Zoe Saldana – is hoping to shed light on the disappearance and murders of as many as 4,000 indigenous women across Canada. "If this exact same story were being told in a country in Africa, I think we would be paying attention to it and we would be donating money to it," said Leslie Owen, the American producer-director behind Gone Missing. "But because it's in Canada, a first world nation, we don't want to see it in our own backyard." She began researching the story in 2015, after stumbling across a news story highlighting 1,200 cases of murdered and missing women that had been compiled by police bodies from across the country. "I was like, what does that mean?" Recent months have seen the number revised upwards, with one government minister estimating the number of missing and murdered indigenous women could be as high as 4,000 women. The Guardian (UK)

Leaked document appears to give broad powers to MMIW national inquiry
There will be five commissioners sitting on a national inquiry into missing and murdered Indigenous women (MMIW) and they appear to have the power to run the inquiry as they see fit, according to the Terms of Reference (ToR) obtained by *APTN National News*. The document, watermarked "sensitive and confidential," appears to be a template for a final version. It does not name the five commissioners. The ToR document also appears to address a pivotal question asked by MMIW family members and their advocacy groups: how much power will the commission have. "Authorize the Commissioners to adopt any procedures that they consider expedient for the proper conduct of the inquiry," the ToR states. But it doesn't elaborate on how much power that is or whether the commissioners will have the power to compel people to testify. The ToR does call for the inquiry to bring the "ongoing national tragedy" of MMIW to an end and examine the "systemic causes of violence against Indigenous women and girls in Canada" and make recommendations. That means looking at the "underlying social, economic, cultural, institutional and historical causes" that have led to more than 1,200 Indigenous women and girls to be murdered or go missing in the last 30 years. APTN News

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Canada's electronic spy agency won't reveal if shared info leads to torture overseas
Canada's electronic spy agency won't say how often it shares information that could lead to someone being tortured in an overseas prison. The Communications Security Establishment – which monitors threats from foreign terrorists and spies – has censored documents that spell out the figures, even though the RCMP and Canadian Security Intelligence Service have revealed such numbers in the past. The reticence prompted Amnesty International Canada to say "much greater transparency" is needed from the Ottawa-based CSE. "At stake is Canada's compliance with crucial international human rights obligations

to prevent torture and ill-treatment," said Alex Neve, Amnesty's Canadian secretary general. The secretive CSE has been thrust into the national spotlight in recent years due to leaks by Edward Snowden, the former spy contractor who worked for the National Security Agency, CSE's American counterpart. It is also among a handful of Canadian agencies, including the RCMP, CSIS, the Canada Border Services Agency and National Defence, bound by a government instruction that allows it to share information with foreign partners – even when it means someone could be abused as a result of that exchange. Public Safety Minister Ralph Goodale said earlier this year the Liberals will review the "troubling set of issues" raised by the foreign-sharing policy, enacted by the previous Conservative government. Canadian Press (Global News)

Hells Angels a major force in B.C. despite recent loss

As B.C. Hells Angels mourn the recent death of a member of the West Point chapter, police say the biker gang remains a significant criminal force in the province. Bjorn Sylvest died July 3 while on a houseboat on the Shuswap Lake, Barb McLintock, of the B.C. Coroners Service, confirmed. "The death of Mr. Sylvest was reported to us and we are investigating," she said. Sylvest was remembered last week by his fellow Hells Angels and other friends at a service in south Surrey. And they paid tribute to the 35-year-old heavy-duty mechanic Thursday with a procession of 200 to 300 bikers riding from the White Rock Hells Angels clubhouse to the Among the mourners were bikers wearing patches of the Hells Angels, the Throttle Lockers, the Shadow Club, the Jesters, the Devil's Army, the Castaways, the Ironworkers Motorcycle Club and the Horsemen Brotherhood. While Sylvest's West Point chapter has taken a hit with his death, the Hells Angels "remain active in British Columbia and overall membership appears to have remained consistent over the last few years," RCMP Supt. Sandro Colasacco said in an interview. He said the current membership of the HA in B.C. is about 120 in nine chapters. "This number does fluctuate based on factors such as police enforcement initiatives and criminal charges," said Colasacco, intelligence officer for the RCMP's E Division. "Previous investigations have made it clear that some members of the Hells Angels are involved in illicit drug, weapons and violencerelated offences, including murder. It is for this reason that the Hells Angels and other outlaw motorcycle gangs remain a priority for the RCMP and our law enforcement partners." Postmedia Network (The Province, A4, Vancouver Sun, Times Colonist)

Une nouvelle fraude qui cible les immigrants

Pendant quelques minutes, la semaine dernière, Yoann a bien cru que le Canada allait l'expulser vers son pays d'origine, la France. Au bout du fil, un agent des services canadiens de l'immigration lui disait bel et bien que des policiers l'attendaient chez lui, prêts à l'embarquer dans le premier avion qui traverserait l'Atlantique. Sauf que Yoann a eu un doute quand il s'est rendu compte que l'employé en question ne parlait pas français et ne semblait avoir aucun collègue qui puisse s'exprimer dans cette langue. Son incertitude aura été bénéfique : le Français était bel et bien victime d'un type de fraude qui fait de plus en plus de victimes chez les immigrants installés au pays. De quatre plaintes en 2013, le nombre de signalements concernant la fraude d'immigration est passé à 1087 en 2015, selon des chiffres que le Centre canadien antifraude (CCAF) a transmis au Devoir. Depuis le début de l'année en cours, 554 Canadiens ont porté plainte pour cette raison, un chiffre qui laisse entendre que la quantité de signalements pourrait dépasser ceux compilés l'année précédente. En pertes, cela équivaut à plus de 416 000 $ depuis janvier. En général, le modus operandi des fraudeurs consiste à exiger des frais qui permettent d'éviter une prétendue expulsion du pays. " La fraude fonctionne. Les gens payent. C'est aussi simple que ça ", a répondu la caporale Josée Forest, de la Gendarmerie royale du Canada, quand on lui a demandé pourquoi les plaintes continuaient d'augmenter. Pire, les statistiques du CCAF montrent qu'environ 5 % de la population rapporte les cas de fraude. " Ce n'est pas beaucoup ", a commenté Mme Forest. Le Devoir, A3

Pot bust yields 400 plants

Police have seized five pounds of pot, 400 marijuana plants, growing equipment and cash after searching a Sturgeon County property this week. St. Albert RCMP say the amount of pot being grown could have produced hundreds of thousands of joints, which could have had a significant impact. Insp. Ken Foster said in a release he was concerned about the large amount of pot seized, noting it's indicative of a criminal trafficking operation rather than someone growing for personal use. "If these drugs were not seized, they would have impacted the well-being of our residents and our children in Morinville, Sturgeon

County, St. Albert and throughout the Edmonton region," he said. Cpl. Laurel Kading said police wanted to make clear this was a commercial operation rather than anything personal or medicinal, emphasizing the danger associated with this kind of unregulated operation. "A concern raised to me by one of our experts is there aren't any controls around those kinds of operations," she said. "You don't know if stuff has been added to make the plant grow differently, or could potentially be health hazards growing plants." Officers from several agencies worked together on the bust: St. Albert RCMP, Morinville RCMP, Fort Saskatchewan RCMP, and the Alberta Law Enforcement Response Teams. The Edmonton Police helicopter helped survey the scene during the search for officer safety. St Albert Gazette

Quarterly report: $155,770 in drugs seized by Valley police unit

The Valley Integrated Street Crime Enforcement Unit is taking thousands of dollars worth of drugs off of the streets. Kenneth Reade, acting chief of police for the Kentville Police Service, shared the unit's report for the quarter that concluded June 30 during a council advisory committee in Kentville July 11. In a three-month period, the unit executed 14 search warrants, and charged 16 people with 20 criminal code offences and 25 Narcotic Control Act violations. Twelve of the warrants were drug related and two were for Criminal Code matters. "There were $155,770 worth of drugs seized, $17,810 worth of other property seized, $22,007 in cash seized," said Reade.The quarterly report lists the drugs seized as: marijuana, cocaine, $137,000 worth of marijuana plants, hash, various prescription pills and Psilocybin. (…) The specialized law enforcement unit is comprised of members of the Kentville Police Service and Kings District RCMP and Windsor RCMP. Nova News Now

Épinglé avec 200 kg de cocaïne

Un résidant de la région de Québec est incarcéré depuis le début de février au Panama après avoir été arrêté en possession de plus de 200 kilos de cocaïne dans ce pays d'Amérique centrale. Le suspect, Steve Miller, a été appréhendé avec deux présumés complices, un Panaméen et un Colombien, lors d'une opération de la police nationale menée le 4 février dernier. L'affaire a fait les manchettes dans les journaux locaux, mais pas dans les médias québécois et canadiens. Lors de la frappe, les policiers panaméens ont découvert 212 kilos de cocaïne et quelques centaines de dollars en devises canadiennes et américaines. La drogue, qui était emballée dans des paquets d'un kilo chacun, avait été dissimulée dans un placard d'une résidence de Betania. Une camionnette, qui aurait servi à transporter la cocaïne, a aussi été saisie par les policiers. On ignore à quelle peine s'expose le présumé trafiquant québécois. La Presse a tenté plusieurs fois de communiquer avec une porte-parole du Ministère public panaméen, en vain. Ici, la Gendarmerie Royale du Canada a confirmé l'arrestation d'un Québécois pour une saisie de 212 kilos de cocaïne sans toutefois donner plus de détails. Selon nos sources, la drogue aurait été destinée aux Hells Angels québécois, en particulier ceux de la section de Trois-Rivières, une information qui n'a toutefois pas été confirmée par les principaux corps policiers du Québec. Au cours des dernières années, les Hells Angels du Québec ont planté leur drapeau ou renforcé leur influence en Amérique centrale, plaque tournante de l'importation de cocaïne vers le Canada, et dans les Antilles. En avril dernier, TVA a révélé que les Hells Angel du Québec auraient parrainé une nouvelle section que l'organisation internationale a fondée en Équateur. La Presse (La Tribune, 15, Le Nouvelliste, Le Soleil)

Who pays? New guide sets out rules for Trudeau travels

Justin Trudeau's frequent trips abroad — often with an entourage of family, officials and guests — raise tricky questions about who travels on the public dime and who does not. So the government recently "formalized" the rules, setting out who digs into their own pockets for travel expenses and who gets their bills picked up by taxpayers. One unexpected disclosure in the four-page guideline document, obtained by CBC News under the Access to Information Act, is the extent to which public money can underwrite the prime minister's personal travels, such as vacations or trips for the Liberal party. (…) In addition, one aide from the Prime Minister's Office is allowed to travel to "support" Trudeau on personal trips, again on the government dime. The principle is that the prime minister must have access to secure communications at all times, even during vacations, to respond effectively to crises, such as the recent attempted coup in Turkey. Privy Council Office spokeswoman Regine Beauplan says staff provide support during all travel by the prime minister, including "the creation of a temporary satellite equipped office that provides access to the secure equipment he needs to carry out his duties." The RCMP is responsible for all ground transportation if the Trudeau family travels for personal reasons, the guidelines say, and the government pays the entire bill without seeking reimbursement. CBC News (2016-07-19)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Former Red Deer Mountie sentenced on assault charge
A Mountie whose career started in the Red Deer city detachment has been given a conditional discharge for punching a man he had arrested on suspicion of impaired driving. Const. Eric Pomerleau, currently on administrative duties with the Brooks RCMP, was tried and found guilty before Judge Gregory Lepp in Red Deer provincial court in June on an assault charge laid after the incident, which took place at the Red Deer city detachment on Nov. 7, 2012. Sentencing arguments were heard on Tuesday, with Calgary-based Crown prosecutor Photini Papadatou asking for a fine in the range of $500 to $1,000. Papadatou stressed that a police officer in charge of a prisoner is in a position of trust and that all police officers must be held to a higher standard than ordinary citizens. Defence counsel Robb Beeman, also from Calgary, asked for a conditional discharge, which would uphold the conviction without creating a criminal record for his client. Red Deer Advocate, A2 (2016-07-20); Canadian Press (Medicine Hat News); CBC News (2016-06-19)

Conduct hearing for Mountie postponed again
A B.C. RCMP conduct hearing, which had been scheduled for Monday, was postponed for the fourth time leaving the former Osoyoos Mountie in his fourth year of paid suspension awaiting the rescheduled date. Const. Amit Goyal, who last served with the Osoyoos RCMP detachment, has been suspended with pay since at least June 2013. His hearing was originally set for 2015 before being rescheduled repeatedly, and as of Tuesday, the RCMP conduct hearing schedule website showed Goyal's hearing was set to begin in Federal Court in Vancouver on July 25. But Staff Sgt. Julie Gagnon, with the RCMP national communication service in Ottawa, confirmed Tuesday that Goyal's hearing had been adjourned again until Sept. 13. He remains suspended with pay, she said. "Every effort is made for adjudication board hearings to be scheduled in a timely manner," Gagnon wrote in an email. "However, these hearings are formal, court-like processes. Much like judicial proceedings, hearing dates, times and locations are subject to change for any number of reasons." Goyal faces five allegations under the 1988 RCMP Regulations, according to the RCMP hearing schedule. The allegations include three counts under Section 39, which prohibits members from engaging in "any disgraceful and disorderly act or conduct," and two counts of Section 45 (b), which says a member must not "knowingly or wilfully make a false, misleading or inaccurate statement or report" to a superior officer about an investigation. Goyal also faces a civil lawsuit, filed in B.C. Supreme Court last year by former Osoyoos resident Steve Condon. In the suit, Condon claimed he suffered harassment and left Osoyoos because of Goyal and the RCMP. Postmedia Network (The Province, A13, Vancouver Sun)

Mystery of Hudson Brooks shooting death sparks emotional rally
A candlelight vigil for Hudson Brooks yesterday outside the South Surrey RCMP detachment turned into a raucous protest for the 20-year-old who was shot in a police encounter a year ago. A 100-strong crowd gathered near the detachment chanting and waving "Honk for Hudson" signs. At one point the vigil took a turn for the worst when a man driving by sparked a fight and police officers had to break up an obscenity-peppered shoving match.The circumstances surrounding Brooks's shooting on July 18, 2015, remain a mystery to people who loved him, mired in investigation and shrouded in suspicion. "You ruin our lives. You make us sit there and ruin our lives. It's the worse. How did my son die? I want to know," said Brooks's mother Jennifer. All the Independent Investigations Office (IIO) has told family is that Brooks was shot at 2:30 a.m. PT by the RCMP. Another officer ended up with a gunshot wound in her leg during the incident, but the only weapons found at the scene were police weapons. Neither the IIO, nor the RCMP has revealed what happened in the moments leading up to the shooting, and why, or how a weapon was drawn on the young man described as "quirky" and "happy" by those who knew him. It remains unclear whether Brooks was armed or not, but a IIO statement released earlier this year said: "Other than police issued equipment, nothing of significance was recovered from the scene." CBC News; Global News; Peace Arch News (2016-07-19)

Man accused of ramming into RCMP cruiser released on bail

A provincial court judge agreed to unlock the door and throw away the key for a Colchester County man Tuesday. Kevin Dean Underwood, 48, was released on $1,000 bail until his return to Truro provincial court on Sept. 21 to face four charges related to ramming into an RCMP cruiser on Thursday. The conditions of his release preclude Underwood from possessing the key to or sitting in the driver's seat of any vehicle. The release conditions, read in court by defence lawyer David Mahoney and agreed to by Crown lawyer Alison Brown, also stipulate that the accused keep the peace and be of good behaviour. Underwood, whose 34 address listings have jumped from British Columbia to Kennetcook, Maitland, Truro, South Maitland, Upper Kennetcook, Five Mile Creek and Beaver Brook, is accused of twice smashing into the RCMP vehicle early Thursday afternoon on Princeport Road in southwestern Colcester County. An RCMP spokeswoman said that police were heading toward the Princeport Road area, about halfway between Truro and South Maitland and just off Highway 236, to set up a checkpoint when an officer noticed a small pickup truck with no licence plate and no box. The officer turned the cruiser around and deployed the emergency lights in an effort to pull the truck over. The pickup driver did not stop and instead turned back toward the police cruiser and rammed into it, police said. The driver then backed up and smashed into the police vehicle again. The driver tried to drive off in the pickup truck but was apprehended and arrested. The officer sustained minor injuries. Local Xpress (2016-07-19)

Cargair s'installe à Saint-Honoré

L'école de pilotage privée Cargair Max Aviation, dont le centre administratif est situé à Brossard, vient de mettre un pied à terre à l'aéroport de Saint-Honoré afin d'y former des dizaines de futurs pilotes d'origine chinoise. Le 13 juillet, l'entreprise, qui possède une quarantaine d'avions Cessna 152-172 et Piper Aztec multimoteur, a acquis la base opérationnelle d'Air Médic, spécialisée dans les transports médicaux aéroportés. Air Médic, qui continuera d'occuper le hangar, a décidé de déployer, à ce même aéroport, son nouvel hélicoptère bimoteur Agusta Westland GrandNew d'une valeur de huit millions$ équipé d'un système de lunettes de vision nocturne qui permettra d'effectuer des transports d'urgence dans un périmètre beaucoup plus étendu que le territoire de la région. Selon les informations obtenues par Le Quotidien, Air Médic a vendu pour la somme de 335 000$ sa base opérationnelle constituée d'un terrain et d'un hangar aéronautique situé au 104, rue No 1 à Saint-Honoré. (…) L'autre avantage indéniable de cet hélicoptère est que les trois systèmes de vision nocturne dont il est doté et qui sont uniquement permis à la GRC, la SQ et les Forces armées en plus d'Air Médic, permettent d'effectuer des sauvetages à toutes heures du jour entre La Tuque et les Iles-de-la-Madelaine. Le Quotidien, 2

RCMP on track with 2016-17 goals

The **Didsbury** detachment of the RCMP completed the first quarter of 2016-17 establishing priorities set by the four communities it serves in Mountain View County. The Mounties asked the towns of Didsbury, Carstairs and Cremona and Mountain View County as well as the Community Policing Advisory Committee to determine local policing priorities said detachment commander Sgt. Kim Pasloske. The detachment "is well on track" to achieve the goals set by the communities, she said. However, break, enter and theft "significantly increased" in the first quarter (April 1 to June 30). "As such, crime reduction will be a focus for this next quarter," Sgt. Pasloske said. At a media briefing July 14, Sgt. Pasloske said the detachment also took steps to increase the accuracy of the crime statistics it keeps so that year-to-year comparisons will be more helpful to understand the work of the detachment. The Town of Didsbury determined its priorities through a survey, Sgt. Pasloske said. Reduction of property crime and enforcement of laws for drug possession and distribution topped the survey. Carstairs wants increased police visibility, improved traffic safety, more police interaction with youth and crime prevention measures. Pasloske said that Didsbury and Carstairs have community peace (bylaw officers) and RCMP coordinate with them in joint operations. Didsbury Review (2016-07-19)

RCMP in Alberta county start positive ticket campaign

Young people in Sherwood Park, Alta. will be rewarded for good behaviour or helping others through a new ticketing campaign. "Strathcona County RCMP and Strathcona County Recreation, Parks and Culture have teamed up to create a positive ticket for youngsters who are observed following the law or doing a good deed in our community," Const. Chantelle Kelly said. "This could range from wearing a bike helmet, crossing at a crosswalk, picking up litter or helping a resident in need." Anyone who gets a ticket will be given single drop-in access to a rec centre (Millennium Place, Ardrossan Recreation Complex, Kinsmen Leisure Centre or Glen Allan Recreation Complex). "Together, the RCMP and Strathcona

County saw this as an opportunity to reward those who make healthy, positive choices in relation to their behaviour, decisions and actions," Sue Hutton, manager with Recreation, Parks & Culture, said. It's also an opportunity to build relationships between officers and youth, she said. The positive ticket campaign will continue all summer. Members of the Strathcona County RCMP Bike Patrol Unit and Patrol Units will be keeping an eye out for positive behaviour. Global News (2016-07-19)

Behind the scenes of the Musical Ride
Being part of an iconic Canadian symbol is unlike any experience Cst. Allison Barker has ever had. "No matter what kind of a day I've had when I get to the Musical Ride and see the people in the crowds it's all worthwhile," Barker said. "There is no better feeling than when I put on my Red Serge and climb up on that giant, black horse in his dress kit with the maple leaf on his rump." "Being part of that traditional display for our country is sheer bliss," she added, emotion catching her voice. "Getting the opportunity to do this job and share the experience with other Canadians is the happiest time." Growing up in Toronto, and spending her free time in a hunter show ring on a horse, Cst. Barker dreamed of being part of the RCMP Musical Ride. "It was always something I wanted to do," she said. "I also always wanted to be a police officer so joining the RCMP was the perfect fit." Each member of the RCMP Musical Ride has spent a minimum of two years in the field prior to joining the group. "People forget that we are police officers first and that when we are part of the ride, we are on duty," she said. (…)Sharing her love of her country and being part of a performance that is a true Canadian symbol is an experience Cst. Barker will treasure for the rest of her life. "To be part of something that is so positive is amazing," she said, her voice filling with emotion. "Even with all the rehearsals and time spent on tour it's a great experience. The hardest part of my day is when my face hurts from smiling so much." "I have the best job in Canada." Westman Journal (2016-07-19)

Community Connections wants you to fill the cruiser
Community Connections, the Revelstoke RCMP and Save-On-Foods are partnering in a fundraiser to collect donations for the food bank. The RCMP will have one of their cruisers parked outside of Save-On this Thursday, July 21 from 2–5 p.m. Officers will be collecting donations with the goal of filling up the police car and delivering the goods to the food bank. Revelstoke Review (2016-07-19)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

City urged to act on pot shops
There are growing calls to shut down or regulate Ottawa's budding marijuana dispensary business, as new - and illegal - storefronts pop up around the city. Since the beginning of July, five more dispensaries have opened or plan to shortly, boosting the number in the city to nine. They are part of a wave of marijuana stores that have been opening across the country, in defiance of federal drug laws. Ottawa Coun. Mathieu Fleury says he has asked Ottawa's police chief to enforce the law and shut them down. He and other councillors who represent urban wards have also begun to discuss whether the city should regulate where the dispensaries operate. Coun. Riley Brockington, who is upset about a cannabis store about to open across the street from a school in his River Ward, said the city can't wait to act until the federal government makes recreational marijuana legal. The umbrella group for Ottawa's Business Improvement Areas invited two police officers to a recent meeting to provide information about the pot shops. The officers gave the same answer that a police spokesperson provided to the Citizen: They are aware of the dispensaries, and are investigating. With the legalization of recreational marijuana on the horizon, these businesses are "jumping the gun," says Christine Leadman, executive director of the Bank Street Business Improvement Area. Two marijuana shops have opened on Bank Street downtown, a situation that until recently would have "been unfathomable," Leadman said. "In my mind, the city police and bylaw should be shutting them down." But she's sympathetic about the difficulty the city may have in regulating the shops. "How do you build in (bylaw) planning for a business that's illegal?" The pot dispensaries are confounding police and municipal officials across the country. The federal government has promised to introduce legislation to legalize and "strictly regulate" recreational pot next spring. Ottawa Citizen, A1 (Ottawa Sun)

Park overdose death shines light on ongoing social issues facing the City of Langley

Langley RCMP have confirmed that a man died of an apparent drug overdose in Douglas Park last Wednesday evening. The death serves as a tragic reminder of the ongoing social issues the City is struggling with. Residents living in the area took to social media that evening, saying a yellow tarp had been draped over the deceased's body and police were on scene. Drug-related deaths were declared a public health emergency in B.C. in April. Since then, overdose deaths — many tied to fentanyl — have jumped 74 per cent compared to the same time last year. Langley City Mayor Ted Schaffer told the Times he has received numerous calls from people who are concerned about homeless issues, including camps set up in municipal parks, as well as anger over the growth of petty crime in the community. "I've never had so many calls from individuals as I have right now," said Schaffer on Thursday. The City is grappling with an increased number of people living on the streets and setting up tent cities on the Nicomekl floodplain and in other locations around town. On July 12, officers from the City's bylaw department entered the growing homeless camp on the floodplain. They filled a trailer and truck with items that had been collected by the people living in the camp. "We want people to feel safe. We want to get a handle on this before it gets out of control," said Schaffer. He said last weekend he sent Langley RCMP commander Supt. Murray Power three emails about residents' concerns and asked to meet with him. He also has had recent meetings with officers in charge of policing the downtown. Langley Times (2016-07-19)

Oh Canada! 10/22 rifle mags capable of more than 10 rounds may be prohibited
A Canadian gun magazine is reporting that stores in the Great White North are pulling bonus-capacity Ruger 10/22 mags under pressure from the Mounties. Calibre, which bills itself as "Canada's Firearm Magazine" this week ran a report that the Royal Canadian Mounted Police, responsible for enforcing the national gun laws in the land of the Maple Leaf, is circulating an internal memo declaring that *all* magazines for the 10/22 capable of loading more than 10 rounds are now considered prohibited. The tip came to *Calibre* from the Moncton fish & Game Association (MFGA) who noted : From what we have been told at the moment, these large capacity magazines will fit certain specific handguns (pistols) thereby creating a situation where the pistol capacity now exceeds the 10 round limit on handguns. Individuals, who for an example, have a Butler Creek 25 round magazine for their 10/22 must now have the magazine "pinned" to 10 rounds, leave the magazine at home, or turn it in for destruction by the RCMP. This does not affect those with Remington rim fire rifles or other manufacturers. Apparently this is unique to the Ruger 10/22. Guns.com (2016-07-19)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

NIL

OTHER / AUTRES

OPP charge two men in grow-op bust
Ontario Provincial Police have charged two Ottawa men after a raid on a commercial property in Beckwith, about 45 kilometres southwest of Ottawa, led to the discovery of a large-scale marijuana grow operation. According to police, an investigation into allegations of marijuana trafficking led to the July 11 raid when the two men were arrested. Police confiscated 2,012 plants in various stages of growth, 25 pounds of marijuana buds, 26 grams of cannabis resin (hash) and hydroponic growing equipment. Facing charges related to illegally growing marijuana are Adam Gunderson-Lord, 37, and John Armstrong, 36. Ottawa Citizen, A6

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
July 21, 2016 / le 21 juillet 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Six Nations host community for AFN General Assembly
Six Nations of the Grand River was pleased to be the host community to the Assembly of First Nations 2016 General Assembly. The three day conference brought together elected officials from Canada's reserve communities to discuss key issues under the banner of gaining momentum towards a nation to nation relationship with communities and the federal government. (…) RCMP commissioner Bob Paulson was also present at the AFN to discuss how to reconcile First Nations communities and citizens in Canada and the police. Paulson said the RCMP needs to work in partnership with Canada's Aboriginal Peoples in order to improve relations between the force and the country's indigenous communities. (…) The two sides have developed a joint protocol that spells out the force's goals of working to ensure indigenous people in Canada are safe, to address diverse needs of communities and to strengthen mutual respect, Paulson said. "I'm aware this protocol is simply words on paper, and words alone will not improve things," he said. "I'm here today to pledge we will put actions to these words so we can continue the healing, continue the building and improve these vital relationships in every way possible." Last December, Paulson raised eyebrows when British Columbia Grand Chief Doug Kelly asked him a pointed question about racism within the RCMP during an AFN session in Gatineau, Que. "I understand there are racists in my police force," Paulson reportedly replied. "I don't want them to be in my police force." It was important to invite the commissioner back to the July AFN meeting to discuss how to tackle officer misconceptions; Assembly of First Nations National Chief Perry Bellegarde told the gathering. "How can we work together to make sure that air is clear, that cloud is gone?" said Bellegarde. First Nations leaders

are aware there are "always going to be issues" that play out with police locally, regionally and nationally, he added. Two Row Times; Flin Flon Reminder (2016-07-20)

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

Licensed grow-ops busted over alleged ties to organized crime
Mounties in the Okanagan executed search warrants Wednesday on two licensed marijuana grow operations in the **Vernon** area. Police say while the operations are licensed to grow, they believe those running the facilities were trafficking the product and allege there are ties to organized crime. A police news release says officers had to discharge one of their shotguns to quickly open a secured door. Four people, two men and two women, have been arrested and are being investigated on allegations of production of a controlled substance for unlawful purposes and production for the purpose of trafficking. Canadian Press (The Province, A13) (2016-07-21); CFJC Today; Global News (2016-07-20)

Shots heard was RCMP
What was thought to be a shots fired incident in **Vernon** early Wednesday morning was actually the Rcmp serving drug warrants. Police officers converged on a number of locations, including Scott road by the Vernon airport. The loud bangs heard in the area were possibly shotgun rounds used to breach doorways, said Cpl. Dan Moskaluk. Castanet (2016-07-20)

Demoviction protesters removed from apartment
A group protesting so-called demovictions in **Burnaby**, B.C., has been evicted from an empty apartment building it has been occupying for 12 days. Natalie Knight says she and other protesters were asleep when about 20 RCMP officers smashed a window and came into the building Wednesday morning. The company that owns the building had a court injunction to remove the protesters, and police took all seven people out. Three, including Knight, were arrested, but she says they were released without being charged after signing an agreement saying they will stay away from the property. Canadian Press (The Province, A8); Canadian Press (Times Colonist, Williams Lake Tribune, Vancouver Sun) (2016-07-21); CBC News; CKNW; Global News (2016-07-20)

Un restaurant ferme sous haute surveillance policière
Un autre restaurant de **Moncton** semble avoir mis la clef dans la porte, du moins, pour quelque temps. Le Moncton Pizza and Grill de la rue Main, anciennement connu comme l'Alexandria's Pizza, était la scène d'activité policière, mercredi après-midi. Au moins six agents de la Gendarmerie royale du Canada ont été aperçus montant la garde devant la pizzeria, pendant que des employés chargeaient de l'équipement de cuisine dans un camion de transport. Le propriétaire du restaurant était tenu à l'écart pendant l'opération, a confirmé un policier. Un désaccord entre partenaires d'affaires semble être à l'origine de cette fermeture. Questionné sur place à savoir si le restaurant fermait ses portes définitivement, un des déménageurs a indiqué qu'il «sera difficile de rester ouvert sans équipement pour faire la nourriture». L'Acadie Nouvelle a tenté de contacter le propriétaire, mais nos efforts n'ont pas porté leurs fruits. Acadie Nouvelle, 5

Former Hells Angel faces new charges
A former Hells Angel who was once convicted of trying to take a loaded gun through airport security is wanted by police again. New charges were laid July 5 against Villy Roy Lynnerup. The 52-year-old is facing two assault charges, one count each of uttering threats to cause death or bodily harm, dangerous operation of a motor vehicle and mischief. All offences are alleged to have occurred June 19 in **Langley**. A warrant was issued for his arrest Monday. He is described as five-foot-nine and 260 pounds with brown hair and blue eyes. Postmedia Network (Vancouver Sun, A7, The Province)

Police find 1,700 marijuana plants in Malakwa residence
Drug-related charges are being sought against two Lower Mainland residents following a police search of a **Malakwa** residence. On July 10, Sicamous RCMP, with the assistance of the Vernon Police Dog Service and the Revelstoke forensic identification unit, executed a search warrant under the Controlled

Drugs and Substances Act at a Sommerville Husted Road residence in Malakwa. Cpl. J.R. Lechky reports around 1,700 marijuana plants were found inside the house and a shop on the property. "Charges of Cultivation of Marijuana are being forwarded to Crown counsel against two individuals from the Lower Mainland," said Lechky. Eagle Valley News (2016-07-20)

RCMP ask P.E.I. to help find marijuana grow ops

Warn Islanders not to intervene but call police during growing season. RCMP is asking the public to provide assistance in locating marijuana grow operations during this year's growing season on **P.E.I.** "Often people will notice unusual activity that can be an indicator that a grow operation is nearby and officers are happy to take your information and investigate," said Cpl. Andy Cook, drugs and organized crime awareness service of the RCMP on P.E.I. He said it can be a challenge to locate marijuana plants and grow operations when so much of the Island is used for agricultural purposes. "To monitor every field is impossible so officers are asking that you report anything that you consider suspicious in order that they can investigate. It's imperative that members of the public do not investigate themselves as fields or grows are sometimes set up with traps or can even be guarded," said Cook. The Guardian; Journal Pioneer (2016-07-20)

Riot contained at Burnaby youth prison

A riot apparently broke out at the youth prison in **Burnaby** in the early morning hours on Wednesday. The Ministry of Children and Family Development has released a statement about the incident, but details are vague. "There was a serious incident at the centre involving extensive damage – some due to fire – and police and fire officials attended," the emailed statement read. "There were no injuries to residents, staff or police. Youth were contained within the centre at all times. All youth are safe and accounted for. More information will be available shortly." The NOW asked a ministry spokesperson what actually happened, and he said more details are coming. In the meantime, the NOW has put calls into both the Burnaby RCMP and the fire department, but no one has replied yet. Burnaby Now (2016-07-20)

Man accused of killing ex-girlfriend says he's innocent

Even after years of police scrutiny, Joseph 'David' Caissie says he has nothing to do with the death of his ex-girlfriend, Carol King. "He's been steadfast in his resolve that he had nothing to do with this," defence lawyer Ron Piché said outside Saskatoon provincial court on Wednesday. Piché said his client intends to plead not guilty now that he has been charged with first-degree murder in King's death. Caissie made a brief court appearance, wearing street clothes and standing before a judge for less than five minutes. He was formally accused of killing King in the Saskatchewan hamlet of Herschel in August 2011. He is also accused of offering an indignity to human remains. His next scheduled court date is Aug. 3. Caissie was arrested Tuesday in Saskatoon. "We start with the people closest to the victim and attempt to clear them and work their way out. In this investigation, we were never able to clear Mr. Caissie," **RCMP** StaffSgt. Murray Chamberlin told reporters at a news conference announcing the arrest earlier this week. Piché said he has been in contact with Caissie "for about two or three years." Neither he nor Chamberlin would specify what led to the arrest nearly five years to the day after King disappeared. "These so-called cold files, they don't seem to spare any resources to try to pursue and reach a conclusion like this. I suspect you'll all know soon enough what the case entails," Piché said. Postmedia Network (Leader-Post, A6, StarPhoenix) (2016-07-21); StarPhoenix (2016-07-20)

RCMP searching for 17-year-old Mekayla Bali

The RCMP is asking for the public's help in locating missing 17-year-old Mekayla Bali. She was last seen at a **Yorkton**, Saskatchewan bus depot on April 12th. RCMP have broadened their search to include Alberta, Saskatchewan, and Manitoba. She is described as Caucasian, approximately 5 feet, two inches tall, and 114 pounds with blonde hair and blue eyes. 660 News (2016-07-20)

Firearms seized in arrest of murdered gangster's son

Police will be looking for links between a trove of firearms seized when the son of a now-dead gangster was arrested over the weekend and a series of recent shootings, **Prince George** RCMP said Wednesday. Ryan John Moore, 25, whose father was William "Billy" Moore, was arrested Saturday after RCMP were called to a report of a domestic disturbance at a Lorne Crescent home. Kathleen Rose Slater, 26, was also arrested. After subsequently obtaining search warrants, RCMP seized four handguns

- two fully loaded and one with a silencer - along with three long guns with ammunition, various bags of ammunition; two cans of bear spray and brass knuckles. Closed circuit cameras, a large amount of cash, four cell phones, illicit drugs including methamphetamine, cocaine and marijuana and drug trafficking paraphernalia were also among the items seized. "Investigators will be looking into the possibility that these weapons have been used in other offences including the recent spike in shootings in Prince George," RCMP said in a statement. Both Moore and Slater have been charged with several firearms and drug related offences. Police described Moore as a "high priority offender." His father was the president of the Prince George Renegades Motorcycle Club who was shot to death in 2005 in an apparent gang-related execution. No one has been arrested for the murder. Court records indicate Slater hails from Surrey where, according to the Surrey Now, she was one of two people arrested in 2011 in relation to the seizure a small arsenal of guns and ammo from a pair of storage units. Prince George Citizen (2016-07-20)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Inquiry won't target police misconduct

The national inquiry into Canada's missing and murdered indigenous women will not have the authority to make findings of police misconduct or compel lawenforcement agencies to reopen cold cases, according to a draft of the terms of reference. The nine-page document, which the federal government circulated to the provinces and territories for review, says five people will be appointed to the commission, with one individual named chief commissioner. Sources have told The Globe that the following individuals are on the draft list: B.C. provincial court judge Marion Buller; former Native Women's Association of Canada (NWAC) president Michèle Audette, who lost her bid to represent the Liberals in a Quebec riding in last fall's federal election; Qajaq Robinson, a Nunavut-born civil litigation lawyer who speaks Inuktitut; Marilyn Poitras, a Métis law professor at the University of Saskatchewan; and a First Nations lawyer who served on the Human Rights Tribunal of Ontario. Justice Buller, who became B.C.'s first female First Nations judge in 1994, is said to be a contender to lead the commission. (…) The draft document, which is not dated and is watermarked "sensitive and confidential," says the commissioners will investigate and report on "systemic causes of violence against indigenous women and girls in Canada, including underlying social, economic, cultural, institutional and historical causes." (…) The Liberal government has so far committed $40-million over two years to conduct the inquiry into Canada's more than 1,181 missing and murdered indigenous women. Sources said Ottawa intends to dedicate further funding to help victims' relatives navigate the police complaints process if they question the quality of an investigation. The national inquiry will inevitably review policing - a key reason Ottawa is getting the provinces and territories to sign on to the terms of reference is to ensure matters outside federal jurisdiction, notably child welfare and provincial and municipal policing, are deemed to be squarely within the inquiry's scope. However, the draft terms of reference do not explicitly mandate the inquiry to delve into policing policies or practices. Globe and Mail, A1 (2016-07-21); CBC News; Radio-Canada; Huffington Post Québec (2016-07-20)

Three people reported missing by RCMP

Three people from Chilliwack are missing, according to local police who are seeking the public's help in locating the individuals. (…) Chilliwack RCMP is requesting the public's assistance in locating Ceda Tanner, 12, of Chilliwack. She has not been heard from since July 15, 2016. Tanner is described as: - Aboriginal female - Height: 5'5" tall - Weight: 140 lbs. - Brown hair - Brown eyes - Wearing black track pants with a white stripe, grey Batman t-shirt, and black runners. Chilliwack Times (2016-07-20)

Premiers meet with aboriginal leaders

Aboriginal leaders and Canadian premiers say there's no need to wait for an inquiry into missing and murdered aboriginal women to get to work on the issues behind the problem. "Governments don't have to wait for the outcome of the inquiry," said National Chief Perry Bellegarde of the Assembly of First Nations after a meeting with the premiers and territorial leaders Wednesday in Yukon. "Governments can make investments to end violence amongst our people, amongst indigenous women and girls, and to deal with investments in housing and education and training and daycare and shelter and detox centres and

wellness centres." The federal government is expected to release details about the inquiry shortly. The premiers are in Whitehorse for their annual summer meeting. They met with aboriginal leaders before two days of discussions about other issues, expected to include freer trade across jurisdictional boundaries. Yukon Premier Darrell Pasloski agreed improvements could be begin right away. "The federal government, the provinces, the territories, and the indigenous governments and leaders need to continue to act now, that we don't wait for the results of the inquiry before we begin to move forward. That was acknowledged by everybody in the room." Earlier in the day, provincial and territorial premiers said there is strong support for the planned inquiry. Alberta Premier Rachel Notley said individual provinces have specific concerns, but there is significant consensus among her colleagues. Quebec's Philippe Couillard said his province wants to ensure allegations of police sexual abuse of aboriginal women in his province are included. It would be better to have one inquiry rather than two parallel investigations, he said. The premiers and aboriginal leaders also discussed how to develop natural resources and their associated infrastructure, including pipelines, with the consent and participation of First Nations. Canadian Press (Times Colonist, A7, Edmonton Sun, A5, Red Deer Advocate, Toronto Sun, London Free Press, Kingston Whig-Standard, Edmonton Sun, Ottawa Sun, Calgary Sun, Winnipeg Sun, Chronicle Herald, CP24, CTV News, Our London); The Guardian (The Telegram); CBC News; Presse canadienne (La Presse)

Body found near Bella Coola identified as Dianne Pootlass
The body of a woman discovered two weeks ago near Bella Coola, B.C., has been identified as that of missing woman Dianne Pootlass. There were no signs of foul play, said a statement released by RCMP. The 41-year-old was reported missing to police after she was last seen by a family member on June 16. "An extensive air and ground search was conducted over several weeks in order to locate Dianne, but all search efforts met with negative result," wrote North District RCMP spokesperson Cpl. Dave Tyreman. Her body was located in the water in the North Bentinck Arm area by a boater on July 7. An autopsy was performed on July 11, which positively identified the deceased as Pootlass. CBC News; Coast Mountain News (2016-07-20)

Zoe Saldana making doc on Canada's missing indigenous women
A team of filmmakers including Avatar star Zoe Saldana are producing a documentary probing the disappearance of Canada's indigenous women. Gone Missing began life last year, when producer-director Leslie Owen happened upon a news story that highlighted 1,200 instances of murdered and missing women. Toronto Star (2016-07-20)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Torture - Le CSTC avare de détails
L'agence d'espionnage électronique du Canada refuse de préciser à quelle fréquence elle partage de l'information pouvant mener à la torture d'un individu dans une prison étrangère. Le Centre de la sécurité des télécommunications Canada (CSTC) -- qui analyse les menaces de terroristes et espions étrangers -- a censuré des documents présentant ces données, même si la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRS) ont déjà révélé ces chiffres dans le passé. Cette réticence a poussé Amnistie internationale Canada à affirmer que le CSTC devait faire preuve d'une " plus grande transparence ". Le CSTC a été placé sous les projecteurs ces dernières années en raison des informations coulées par Edward Snowden, l'ancien sous-traitant de l'agence de sécurité nationale américaine (NSA), l'équivalent du CSTC au sud de la frontière. Le Centre fait également partie d'une poignée d'agences canadiennes -- dont la GRC, le SCRS, l'Agence des services frontaliers du Canada et la Défense nationale -- qui ont le droit de partager des informations avec des partenaires étrangers, même si cela signifie qu'une personne pourrait être torturée par la suite. Le ministre de la Sécurité publique, Ralph Goodale, a indiqué plus tôt cette année que les libéraux se pencheraient sur les problèmes liés à cette politique de partage d'information, mise en place par le gouvernement conservateur précédent. La Presse canadienne (Le Devoir, A4) (2016-07-21); La Presse (2016-07-20)

Europol hosts Virtual Currencies Conference to fight cybercrime and money laundering

Europol's European Cybercrime Centre (EC3) organized the third Virtual Currencies Conference on 14 and 15 July at its headquarters in The Hague, which brought together over 90 experts from various regions of the world. The two-day conference aimed to strengthen the fight against the abuse of virtual currencies for criminal transactions and money laundering. In addition, it also offered opportunities for closer cooperation and new partnerships to prevent and fight cybercrime and money laundering as well as facilitate asset recovery. In attendance were representatives from law enforcement authorities, in particular from EU Member States, several US law enforcement agencies, the Swiss Police Cybercrime Division and the Royal Canadian Mounted Police. Furthermore, leading experts from several commercial and non-for-profit organisations actively involved in facilitating the lawful use of virtual currencies also took part. Experts shared their insights into criminal trends and the latest techniques used by illegal entities to hide their financial tracks and cash out criminal proceeds using bitcoins and other digital currencies. The latest cutting-edge technology solutions for tracing blockchain transactions for criminal investigations were presented. Best practices and law enforcement techniques were also shared through concrete case examples. EconoTimes

L'opération NUNAKPUT 2016 a pris fin à Fort Simpson, dans les Territoires du Nord-Ouest
L'édition 2016 de l'opération NUNAKPUT prend fin aujourd'hui à Fort Simpson (Territoires du Nord-Ouest) après deux semaines de patrouilles maritimes et d'entraînements qui ont débuté le 5 juillet. Les patrouilles et les entraînements étaient axés sur les membres du 1er Groupe de patrouilles des Rangers canadiens, ainsi que sur des exercices de recherche et de sauvetage (SAR) auxquels ont participé des militaires des Forces armées canadiennes, des employés de divers ministères fédéraux et d'un organisme civil de recherche et de sauvetage. L'importance de cet entraînement a été confirmée durant l'édition 2016 de l'opération NUNAKPUT, alors que deux incidents réels ayant donné lieu à deux opérations de recherche distinctes pour retrouver des plaisanciers perdus sont survenus près de Lutselk'e, à environ 200 kilomètres à l'est de Yellowknife. Les efforts combinés de la GRC et des équipages et appareils de l'ARC, notamment un CC-130 Hercules basé à Winnipeg et un CC-138 Twin Otter basé à Yellowknife, ont permis de localiser et de secourir les plaisanciers. L'entraînement de SAR mené cette année dans le cadre de l'Op NUNAKPUT permet de s'assurer que les FAC et leurs partenaires maintiennent leur capacité d'intervenir lors d'incidents comme ceux-ci, accroissant ainsi la sécurité et la protection des Canadiens occupant le nord du territoire. 45eNord (2016-07-20)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Mort de Michel Vienneau
Annick Basque, la compagne de Michel Vienneau, abattu par un policier municipal de Bathurst, signe une autre victoire importante. La Cour du Banc de la Reine ordonne que le dossier d'enquête de la GRC, ainsi que les rapports de toxicologie et d'autopsie de la victime, soient remis à Mme Basque. Néanmoins, dans sa décision du 11 juillet, le juge Larry Landry autorise que tout renseignement permettant d'identifier le dénonciateur à l'origine de l'intervention policière du 12 janvier 2015, de même que toute information relative aux mesures d'enquête de la GRC, soient masqués. Lors de la première audience tenue le 12 novembre, les procureurs généraux du Canada et du Nouveau-Brunswick refusaient de fournir les documents en question auxquels Annick Basque voulait avoir accès, dans le cadre de sa poursuite civile contre la Ville de Bathurst. Le procureur général du Canada affirmait que l'inspecteur de la GRC Larry Wilson, qui a mené l'enquête sur les circonstances du drame, collaborait toujours avec le service des poursuites publiques du Nouveau-Brunswick et que le dévoilement de ces documents pourrait éventuellement nuire au dépôt d'accusations criminelles. Le bureau du coroner donnait principalement les mêmes raisons pour refuser de dévoiler son rapport. Acadie Nouvelle, 5 (2016-07-21); Radio-Canada (2016-07-20)

Officer encourages residents to report tips to police
An RCMP officer in Bathurst says he may be able to shed some light on the reason why police were called recently about a suspicious vehicle at the Stonehaven wharf. RCMP Constable Jonathan Greer of the J Division Federal Operations is responsible for the RCMP's Coastal Airport Watch Program (CAWP) in the North Eastern corner of the province. He said police ask that residents tip them off to any unusual activity and that RCMP rely on calls like one made recently in Stonehaven. "Police depend on members

of the community to be our eyes and ears in their communities, to report anything they believe is suspicious in nature or 'not normal' for that area, and to help us prevent, detect and intercept individuals, vehicles and vessels," said Cst. Greer in an email. A complaint made to police recently at Stonehaven made national headlines when Louizandre Dauphin, who is black, was pulled over by RCMP after spending a few hours reading a book in his car near the Bathurst-area wharf. (...) Following the media coverage, some residents from the Stonehaven area have come out and said the racial allegation is unfair and residents in the rural area routinely report suspicious activity due to several thefts lately, and in the past number of years. Cst. Greer says "the CAWP encourages people to do exactly what the caller in this case did." He said theft isn't the only issue at wharfs and along coastal areas. "When police respond to a call of this nature, it could be to prevent a suicide, identify possible thieves, prevent a drug deal, intercept a potential importation of illegal drugs, human smuggling, etc." he said. Telegraph-Journal, A6

Halifax police assaulted at higher rate than Canadian average

For the last five years, police officers in Halifax have been assaulted at a higher rate than in any other city in Atlantic Canada, and at a far higher rate than the national average. According to an analysis of crime data obtained from Statistics Canada, from 2011 to 2015, Halifax has averaged a rate of 43.5 assaults on police officers per 100,000 people. St. John's, the next highest city in the Atlantic Canada, averaged 33. But that figure doesn't tell the whole story. While the St. John's rate of 41 assaults in 2010 was the second highest in the region; five years later their rate of assaults fell to 29. This is similar to the way rates of assault on police officers have dropped throughout Atlantic Canada. However, since 2011, Halifax's has remained relatively the same. In 2015, the rate of assaults in Halifax was 39. From 2011 to 2015 Halifax had 898 total incidents where police were assaulted. St. John's had 333. In 2011, officers in Halifax – including Halifax Regional Police and RCMP in the municipality – were 35 per cent more likely to be assaulted when compared to other Canadian regions. Five years later, the number has dropped to its lowest point at 30 per cent. Truro Daily

Pokemon Go takes N.S. by storm

From Alderney Landing and the Halifax waterfront to Peggy's Cove and Sydney, the hunt is on for Clefairy and Snorlax and Pikachu. Nova Scotian Pokemon Go enthusiasts are taking to the streets, inspired by the latest mobile digital craze over the cartoonish creatures visible only on smartphones through an app with a map-like interface - but players are urged to be careful. "There needs to be billboards with the Snorlax poster downtown. Congested sidewalks are not the place to stop in the middle of," warned Matt on the Facebook page Pokemon Go: Halifax. (...) At the RCMP, some research is underway about the game and its objectives, said Corp. Jennifer Clarke. "We would certainly encourage people to be aware of their surroundings at all times, and to be responsible with other people's private property - and to separate reality from the game, making sure they're not putting themselves in danger when they're out in the open," Clarke said. Chronicle Herald, A6

New resource for domestic violence victims in town

The town of Cochrane has hired more personnel to address a rising domestic violence problem in the community. In January, a domestic violence co-ordinator position was added to the Cochrane RCMP detachment. The new position will help assist with and review domestic violence cases in the community. “My position is here and if people have any questions with domestic violence, I am working and listening and want to help them out the best I can and if I can’t help them then I can help them find resources with the community partners we have to assist them,” said Cst. Courtney Currie, Cochrane’s first domestic violence co-ordinator. Currie has 10 years experience with the RCMP and has lived in Cochrane for the last four and a half years. She said she accepted the position because she wanted to “help people.” “I have seen where people are involved in domestic violence time and time again and I want to help them understand that it is something they shouldn’t be living with and it is not healthy in a relationship and I can understand if they want to continue in the relationship but something needs to change,” Currie said. “There is a lot of domestic violence in the area – the recession is probably not helping.” Cochrane Eagle

Police presence at west end of Salmon Arm a training exercise

It's not what it appeared to be. Reports of some type of police incident coming from passersby were, in reality, a police training exercise. RCMP officers from the Southeast District Emergency Response Team utilized buildings on a property across the Trans-Canada Highway from DeMille's Farm Market

near the Salmon River Bridge for a training exercise. The property is slated for demolition as part of a highway expansion project. Several police officers dressed in tactical gear as well as a large armoured vehicle were on the property. Sgt. Scott Lachapelle of the Salmon Arm RCMP said that the Emergency Response Team members on scene used the buildings to practise techniques for entry and other scenarios. Lachapelle said the location is used because officers do not have to be as concerned about damaging the buildings "We're not just simulating tearing a door down, we're going to try and tear it down to see how it works, so when we have to do it for real we know how it works," he said. Lachapelle and other members of the Salmon Arm RCMP observed the training exercise but did not participate. Salmon Arm Observer (2016-07-20)

Manitoba Stampede and Exhibition
The province's only professional rodeo is back in the saddle - the Manitoba Stampede and Exhibition runs this weekend, July 21-24, in Morris. Started in 1964, the Manitoba Stampede (put on by the Valley Agricultural Society) showcases classic rodeo activities such as bull riding, bronco-busting, tie-down roping, bareback riding, steer wrestling, ladies barrel racing, team roping and chariot and chuckwagon racing. The stampede also includes an agricultural fair - where patrons can learn all about the heritage of rural Manitoba - a beer garden, musical entertainment and a parade that begins Saturday at 10 a.m. This year, the RCMP Musical Ride will also be taking part, bringing 32 horses and riders that "provide the public with an opportunity to experience the heritage and traditions of the RCMP." It also raises money for local charities and initiatives across the country. The first recorded display of the Musical Ride was in 1901 in Regina - it's a performance in which horses and riders create intricate figures and do drills choreographed to music. The Musical Ride visits cities all across the country, and, in addition to the stampede, will be making 12 additional stops in Manitoba locations. Winnipeg Free Press, 8; Winnipeg Sun

RCMP Musical Ride charges into town
For the first time in 16 years, the RCMP Musical Ride will be making its return to Portage la Prairie. The cavalry will perform two shows at the PCU Centre July 26, showcasing intricate drills choreographed to music which require the utmost control, timing and coordination. Portage Daily Graphic (2016-07-20)

Flame of Hope run through downtown Whitehorse
Rachel Dawson smiles wide as she receives the freshly light Flame of Hope. The Special Olympic soccer player was the first to hold the flame at the start of the Law Enforcement Torch Run yesterday and she held it high. The torch is one-of-a-kind, carved by Owen Munro, a fellow special Olympian. It was passed hand to hand as Serge Michaud, Special Olympics Yukon and Torch Run Liason, addressed the group of about 50 law enforcement and Special Olympians in front of him. "This is the largest Law Enforcement Torch Run we've ever had in the Yukon," he said. "Congratulations all of you for signing up." (...) "Yukon Law Enforcement officers are proud to carry the torch to recognize over 90 amazing Yukon athletes with an intellectual disability" said Whitehorse RCMP Inspector, Dan Austin, LETR Director for Yukon. "Running through the streets of Whitehorse with the Flame of Hope is one of many ways we hope to increase awareness of Special Olympics Yukon." Whitehorse Daily Star, 19

City in favour of extra RCMP officer
At its Monday meeting, Courtenay council approved in principle a 2017/18 policing contract exceeding $6 million. It would provide for a full-time complement of 31.4 RCMP members — one member more than 2016/17. Courtenay is responsible for 90 per cent of the contract ($5,418,651). Comox Valley Record (2016-07-20)

RCMP begin bike patrols
Grande Prairie residents aren't the only ones enjoying the summer sun as RCMP bike patrol officers have hit the trails. This summer, residents will see officers patrolling parks, the downtown, and special events not only in an effort to curb crime, but also to build ties with the community. "It's an extension of our community policing units," said Cpl. Shawn Graham, supervisor for the bike patrol team. "It's a unit that's very visible and it's very community based, bike patrol members are visible in our park areas and they engage with local youth down there as well as other users in the park, to be visible so that (citizens) feel comfortable being at the park and (to see) that police are down there making patrols of the area." The

bike patrol has been in place for more than10 years with the core made up of five school resource officers, with the option of pulling about 10 members from a watch, if need be. Bike patrol members police in pairs and can perform traffic enforcement duties, look for lost children, and administer first aid. "Being a bike patrol officer is a really good feeling. I feel that we're able to get down into the parks where our members in the vehicles cannot. It's a great feeling of safety and security for members of the public just because we're on the trails looking out for their safety," said Const. Michelle Mosher. "We're having lots of positive comments, especially on Muskoseepi trails people have said how nice it is to see us on the trails and it makes them feel a lot better." Daily Herald Tribune (2016-07-20)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

Raiding illegal pot shops not the answer, prof believes
Sending police to shut down pot shops is a "blunt instrument" in the face of the widespread social disobedience that has propelled hundreds of the illegal businesses to open across Canada, says Osgoode Hall Law School professor Alan Young. "The criminal law is always an ineffective way to make a change in a community," said Young, a specialist in marijuana law. "It's very slow, ponderous, and by the time you get a result, the legal landscape may have changed." Ottawa city councillors and merchant groups are debating what to do about the illegal marijuana dispensaries opening in town. There have been calls for police to enforce drug laws and shut them down. Everyone is looking closely at what's happening in other Canadian cities, especially Toronto and Vancouver. Toronto police cracked down after dozens of dispensaries sprang up this spring. Since late May, police and bylaw officers have raided 47 dispensaries, arresting more than 90 people and charging them with either drug trafficking, benefiting from the proceeds of crime, or zoning infractions. Ottawa Citizen, A3

Ahead of legalization, lobbyists for the marijuana industry jostle for a say in Ottawa
In another sign that Canada's booming marijuana industry has gone corporate, dozens of companies have registered as paid lobbyists ahead of Ottawa's plan to legalize the drug's recreational use next spring. As of March 19, the federal government's lobbyist registry listed 88 paid positions with interests in marijuana or cannabis. The companies named range from small, independent businesses like Vancouver's Eden Medicinal Society to large corporations, including the Loblaws chain of more than 2,000 supermarkets across Canada. An analysis by the *Straight* revealed the vast majority of lobbyists remain focused on medicinal marijuana, while 24 can be described as focusing entirely or partly on recreational cannabis. (…) According to CAMCD president Dieter MacPherson, one reason the lobbyist registry might be short on names from the dispensary industry is because storefront operators predict Ottawa will leave nuts-and-bolts regulations for the distribution of recreational marijuana up to the provinces. "The federal government and its legalization platform is going to be setting a stage that the provinces then get to dance on," he said on the phone from Victoria. "Lobbying dollars spent at the federal level may not be as effective." Straight.com (2016-07-20)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Pot and a hard place
An editorial states, "Ottawa is now a Wild West of potrepreneurs. The city and police have been left in an awkward position by the federal Liberal government, which has sparked up a marijuana retail race but won't introduce legislation to legalize it until next spring. If legalization is going ahead, it needs to happen in a sensible, smart way. As local councillors note, we probably don't want stores - such as the nine dispensaries that have popped up across Ottawa already - selling weed across from local schools, just as we don't locate LCBOs or strip clubs there. The current situation is a mess. The recreational trade is illegal, yet there are no controls over who is peddling pot in our communities. (…) Cops are caught between the pot and a hard place. "The law is in force and it should be obeyed," Attorney General Jody Wilson-Raybould has said, meaning this commercial recreational trade is still illegal. So what are police to do? Moreover, if people are arrested, what is the Crown to do? The federal Liberals have created this frenzy of entrepreneurs, but the lag time for changing the law, and thus allowing for local regulation, is leaving cities and authorities in an untenable situation. We need clarity. The hazy approach by the feds is

only causing chaos. And it was entirely foreseeable - unless your head was in the clouds." Ottawa Sun, A18

Fentanyl is now a crisis
An editorial states, "The weekend spike in drug overdoses across Surrey's Whalley area would have been a national disaster had the subjects been victims of a mass shooting, a wild fire or a plane crash. Fraser Health medical staff faced a disaster-like 36 life-threatening cases in which people were stricken after ingesting illicit drugs likely laced with the deadly synthetic opioid fentanyl. Emergency workers handled the calamity with competence and nobody died. For their skill, they deserve thanks. The same is true for the health-care workers and police officers who then walked streets putting up warning notices, handing out pamphlets and talking to people about a growing and immediate risk. How serious is the problem? A report from the provincial coroner's service tracking detection of fentanyl in illicit drug overdose deaths shows a frightening expansion across both provincial geography - and demography. The number of overdose deaths in which fentanyl was detected jumped by 1,346 per cent from 2012 to the mid-point of 2016. For users under 19, more frequently users of other recreational drugs, the increase is 700 per cent. And the hazard is now provincewide. Of the 494 such deaths reported to the end of May, 214 were on Vancouver Island, in the Interior and across the north. Synthetics like fentanyl, 50 to 100 times more powerful - and toxic - than opiates like morphine or heroin, are increasingly popular with those who make and sell illicit drugs because they offer a cheaper ingredient which amplifies the potency of what they purvey. But lower costs and higher profits for traffickers mean vastly increased risk for unsuspecting users of street-purchased drugs. Fentanyl-implicated overdose deaths, for example, are already about 10 times the fatalities in the 2009 swine flu epidemic. The response by Fraser Health and Surrey RCMP deserves applause. But what next? If fentanyl shows up everywhere and in all forms of street drugs, everyone who ingests or injects illicit drugs is now at risk of a lethal overdose." Vancouver Sun, A10

Use Marijuana Tax Revenues To Treat Related Public Health Issues
An opinion piece by Bill Bogart, law professor at the University of Windsor, states, "The Task Force on Marijuana Legalization and Regulation is up and running. And run it will in order to have a detailed set of recommendations for its November deadline. It has lots of issues to consider as indicated by its discussion paper and beyond. Protection of children in the shift from criminalization to regulation must be paramount. Taxation raises a lot of questions. There's no doubt that marijuana, itself, and the industry and its employees, agents, etc. should be taxed. One of the main arguments for legalization and regulation is that it will impose levies on the cannabis industry, ending its illicit tax-free days. How much to tax is a critical issue: too low and the levies, even combined with other strategies, won't have much impact dampening harmful consumption; too high and the illicit market can creep back in (we've seen this happen with cigarettes). At any rate, taxation produces revenue for governments. What should be done with the flow derived from marijuana? Monies from taxes on cannabis could simply be directed to the general revenue pool of government. However, for two compelling reasons, the task force should recommend that any legislation regulating marijuana should stipulate that funds should be earmarked for public health issues related to cannabis. First, the goal of taxing drugs is to discourage harmful consumption. The money raised through those taxes will have more impact if it is used to support prevention and counselling than it will by becoming part of general revenues used for various purposes. Second, the taxes will more likely be supported by the public if they are used for these specific ends." Huffington Post (2016-07-20)

OTHER / AUTRES

Les Hells Angels sous haute surveillance
Les autorités policières des deux côtés de la rivière des Outaouais seront aux aguets, au cours de la fin de semaine, alors que plus de 500 Hells Angels et membres de clubs affiliés de partout au Canada seront à Ottawa pour le Canada Run 2016, un rendez-vous obligatoire pour ces groupes de motards, tenu aux quatre ans. Les corps policiers des villes d'Ottawa et de Gatineau, de la Sûreté du Québec (SQ) et de la Police provinciale de l'Ontario (PPO) se préparent depuis plusieurs mois à cette visite, qui aura lieu du 22 au 24 juillet. Ils se mobiliseront pour surveiller le rassemblement, faire respecter le code de la sécurité routière, recueillir des informations et rafraîchir leurs albums de photos. «Cet événement se

traduira par une forte hausse du nombre de motocyclettes sur nos routes, a précisé l'inspecteur Michel Marin de la police d'Ottawa. Il s'agit donc d'un rappel à tous les usagers de la route de partager la chaussée et de respecter les limites de vitesse.» «Ce sera tolérance zéro, a continué l'inspecteur Marin. Si nous devons effectuer une arrestation, nous la ferons en tenant compte de la sécurité des agents et des participants à l'événement.» Les Hells et leurs sympathisants se réuniront dans le secteur rural de Carlsbad Springs, dans l'est de la ville, où la présence policière sera rehaussée. Les Nomads, un chapitre des Hells Angels, possèdent une base à Carlsbad Springs. Des membres de clubs-écoles comme les Red Devils et les Gatekeepers sont aussi attendus dans la région. Le Droit, 2 (La Presse); Ottawa Sun (Ottawa Citizen); London Free Press (2016-07-21); CTV News; CFRA News (2016-07-20)

Leading member of Hells Angels arrested

André Sauvageau, 57, a leading member of the Hells Angels, was arrested in a restaurant on the South Shore Wednesday. The Sûreté du Québec said Montreal's Joint Regional Squad made the arrest as part of Projects Magot and Mastiff, joint investigations with the SQ into drug trafficking conspiracies allegedly run by the Mafia, Hells Angels and street gangs. On Nov. 19, investigators arrested or issued warrants seeking 48 people - including Leonardo Rizzuto and Stefano Sollecito, whom police described as the heads of the Mafia in Montreal. Sauvageau is expected to appear Thursday at the Montreal courthouse to face charges of gangsterism, drug trafficking and instructing a person to commit a criminal offence. The SQ says investigations are ongoing. Two people are still being sought: Jesse McCarthy, 39, of Montreal, and Patrick Williams, 41, of Mascouche. Montreal Gazette, A4; Presse canadienne (Le Nouvelliste, Le Devoir); Journal de Montréal

Number of crimes reported to police jumps for first time in 12 years

Statistics Canada says the number of crimes reported to police went up last year for the first time in 12 years. The crime severity index, which measures the volume of reports and how serious they are, rose 5% in 2015. But the agency says that's still 31% lower than it was a decade ago. The overall crime rate also rose, by 3%, but Statistics Canada notes the last time a rate increase was reported was 2003. The agency says the rise in both measurements was due to more incidents of fraud, breaking and entering, robbery, and homicide. It says there were almost 1.9 million Criminal Code incidents, excluding traffic, reported in 2015, 70,000 more than the year before. Canadian Press (Kingston Whig-Standard, London Free Press, Montreal Gazette); 610 CKTB; Global News (2016-07-20)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
August 17, 2016 / le 17 août 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

A question of balance: civil liberties, security equal in battle against terrorism: PM
An alleged terrorist plot in Ontario that created anxieties over police monitoring of suspects hasn't shaken Prime Minister Justin Trudeau's emphasis on balancing civil liberties with public safety. In his first reaction to an alleged plot that led to the death of Aaron Driver in Strathroy, Ont., Trudeau said Tuesday that balancing individual rights with keeping Canadians secure from bombing threats has to be handled with care. "Canada is a country that values its freedom (and) its basic charter rights," he said during a stop in Bridgetown, N.S., for an infrastructure funding announcement. "All Canadians expect their government to do two things: to keep Canadians safe and to defend and uphold the values and rights that all Canadians hold dear." "Getting that balance right isn't always easy in the challenging situation we now live in but it's extremely important." (...) During the news conference, the prime minister said the wider response against domestic terrorism will be rolled out by Public Safety Minister Ralph Goodale as the Liberals continue plans to reform Bill C-51. During the last federal election, the Liberals pledged to guarantee that all Canadian Security Intelligence Service warrants respect the charter, that the right to lawful protests and advocacy aren't violated, and they pledged to "narrow overly broad definitions (in Bill C-51), such as defining 'terrorist propaganda' more clearly." They also said a Liberal government would limit the Communications Security Establishment's powers by requiring a warrant to engage in the surveillance of Canadians and emphasize community outreach to battle radicalization of youths. Canadian Press (Red Deer Advocate, A8, Cape Breton Post, Telegraph-Journal); Postmedia News (Ottawa Sun, A9, Winnipeg Sun, Toronto Sun, Edmonton Sun, Calgary Sun)

Trudeau se tourne vers le comité parlementaire
Le premier ministre Justin Trudeau estime que le comité parlementaire créé pour surveiller les activités des agences de renseignement aura à évaluer l'efficacité du travail de ces agences. La semaine dernière, la Gendarmerie royale du Canada (GRC) a intercepté un jeune Canadien qui préparait une attaque terroriste. Le jeune homme était connu des autorités canadiennes, mais c'est le FBI qui a alerté la GRC alors que l'homme préparait un attentat imminent. (...) «Cette situation de la semaine dernière et des situations semblables, c'est exactement le genre de choses sur lesquelles le comité de parlementaires aura à s'exprimer, aura à réfléchir», a-t-il ajouté. Le premier ministre s'attend à ce que ce comité offre «des conseils sur la manière dont on peut encore mieux assurer la sécurité des Canadiens, comme nous avons pu le faire la semaine dernière». Presse canadienne (Le Droit, 15, La Presse+, Le Soleil) (2016-08-17); Presse canadienne (Le Devoir) (2016-08-16)

Change terror tactics
The RCMP thought Martin Couture-Rouleau was on the right track when officers met the 25-year-old radicalized convert on Oct. 9, 2014. Despite a failed attempt to travel to Syria, he seemed to be coming around. Eleven days later, he drove to a strip mall frequented by uniformed soldiers in Saint-Jean-sur-Richelieu, Que., and killed Warrant Officer Patrice Vincent. Chased by police, he crashed his car and charged officers with a knife before he was shot dead. Following a similar scenario in Strathroy, Ont., on Aug. 10, which ended with the shooting death of ISIL supporter Aaron Driver as he was allegedly about to conduct a bombing, some experts are calling for changes to the way extremists are assessed. In the Couture-Rouleau and Driver cases, the assessments were ultimately wrong. Both men had come to the attention of the RCMP but were apparently thought to have softened their views and were not being closely monitored. Former Canadian government intelligence analyst Phil Gurski said the cases point to the need for more thorough and regular assessments of extremists on the radar of security agencies. He also said authorities must assume that extremists who claim to have reformed are liars until proven otherwise. "Absent that assumption, extremists will continue to dupe well-intentioned people," he wrote in a blog post Tuesday. In an interview, Gurski said terrorist groups like ISIL encourage their followers to use deception as a tactic. "My default position is that you have not deradicalized, you have not abandoned the cause, until you prove to the nth degree the contrary," he said. (...) The Violent Extremist Risk Assessment tool currently used is a guide that rates extremists based on whether they score low, medium or high on 25 categories such as use of extremist websites, direct contact with extremists and military training. But it "has some weaknesses," Prof. Dawson said. "It shows some potential but it's got some real limitations. ... Everyone recognizes that we really need to get serious about developing better assessment mechanisms." He said the office of community outreach and counter-radicalization that Public Safety Minister Ralph Goodale has announced would likely take on the task. "They're aware of this and this is probably one of the things they're going to be pouring a lot of resources into." Postmedia Network (National Post, A1, Front, Vancouver Sun, Windsor Star, Kingston Whig-Standard, StarPhoenix, Leader-Post, Montreal Gazette, Ottawa Citizen, London Free Press, Edmonton Journal, Calgary Herald)

Police chiefs want access to passwords
Canada's police chiefs want a new law that would force people to hand over their electronic passwords with a judge's consent. The Canadian Association of Chiefs of Police has passed a resolution calling for the legal measure to unlock digital evidence, saying criminals increasingly use encryption to hide illicit activities. There is nothing currently in Canadian law that would compel someone to provide a password to police during an investigation, RCMP Assistant Commissioner Joe Oliver told a news conference Tuesday. Oliver said criminals - from child abusers to mobsters - are operating online in almost complete anonymity with the help of tools that mask identities and messages, a phenomenon police call "going dark." "The victims in the digital space are real," Oliver said. "Canada's law and policing capabilities must keep pace with the evolution of technology." The chiefs' proposed password scheme is "wildly disproportionate," because in the case of a laptop computer it would mean handing over the "key to your whole personal life," said David Christopher, a spokesman for OpenMedia, a group that works to keep the Internet surveillance-free. "On the face of it, this seems like it's clearly unconstitutional." The police chiefs' resolution comes as the federal government begins a consultation on cybersecurity that will look at issues including the best way to balance online freedoms with the needs of police. The consultation runs until Oct. 15. Police demands for access to online communications and the concerns of civil libertarians about privacy rights have created tensions around the globe in recent years. The issue came to fore last year

when the U.S. Federal Bureau of Investigation went to court in a bid to crack the password of a terror suspect's iPhone following a mass shooting in San Bernardino, Calif. Canadian Press (Red Deer Advocate, A7, Guardian, Telegram, Chronicle-Herald, Cape Breton Post, Toronto Sun, Hamilton Spectator, Waterloo Region Record, Edmonton Sun, Toronto Star, Edmonton Journal, Leader-Post, Ottawa Citizen, National Post, times & Transcript); Canadian Press (Calgary Sun,A3, Calgary Herald); Presse canadienne (Acadie-Nouvelle, 12, Le Quotidien, La voix de l'est, Le Soleil) (2016-08-17); Presse canadienne (L'Actualité) ; Canadian Press (CTV News, News 1130, iPolitics); CHED 630 AM (2016-08-16)

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

King may have been on the move

Denecho King is believed to have hid in several locations throughout the city prior to being found in a housing unit on Sissons Court Saturday morning, police say. "We can confirm that we suspect he was moving to different locations during the three-day search, thus the police activity that was all over **Yellowknife**," RCMP civilian member Marie York-Condon stated in an e-mail Tuesday. The force declined an interview request. King, 23, had escaped Wednesday from the North Slave Correctional Centre. He was found in a home on Sissons, an area with multiple rowhouses, by police through "investigational techniques" and tips from the public. Between 25 to 30 RCMP officers were involved at the height of the search, police have stated. "We followed up on any and all sightings reported around the city, and followed the investigational leads," York-Condon stated. "Ultimately, this led us to King at the residence where he was apprehended." RCMP officers were going door to door around 8 a.m., Sissons Court resident Leroy Mantla said. Police confirmed King was in a unit and a crisis negotiator established contact with the occupants. How many people were inside remains unclear. By 9 a.m., officers with weapons drawn could be seen around the buildings as more officers arrived. About 30 minutes later, an officer began giving instructions to King over a loudspeaker. After about 30 minutes more, King left the unit through the front door and was led away in handcuffs to a waiting police truck. "Through the hard work and professional conduct of our RCMP members, we were able to bring this search to a successful conclusion without incident," Yellowknife RCMP detachment commander Insp. Matt Peggs stated in a news release. Northern News; Yellowknifer; Yellowknifer

Home searched by RCMP in terrorism investigation no longer of interest to police

A **London** family that has been in the hot seat for nearly a week -- since police swooped in and searched their Northwest London home without a warrant in connection with a terrorism investigation last week -- is in the clear. "As it stands, we have no ongoing interest in 43 Blanchard (Cres.)," RCMP spokesperson Louise Savard wrote in an email to the Free Press Tuesday. A day earlier, the RCMP would not answer any questions about their investigation of that home, an investigation they made public by announcing the address at a national news conference last Thursday. The family who lives there had "no communication" from the RCMP since their home was searched — without a warrant — and cleared the night terrorism suspect Aaron Driver died in a confrontation with police in Strathroy, their lawyer told the Free Press Monday. London Free Press (2016-08-16)

19K found inside Hamilton man's car on Trans-Canada Highway

A man from Hamilton, Ont., faces criminal charges after RCMP in **Manitoba** pulled a car over for speeding, only to find "stacks of cash" exceeding $19,000 in cash along with some marijuana inside. RCMP say they stopped a 2007 Cadillac on the Trans-Canada Highway near Headingley, which is just west of Winnipeg, around 1 p.m. CT on Aug. 11. Officers found a small quantity of marijuana and "stacks of cash in excess of $19,000" inside the vehicle, RCMP said in a news release Tuesday. Both the money and the car were seized. Police say they believe the cash was obtained through criminal activity. An RCMP spokesperson says the vehicle is being held as part of the investigation, which will determine whether or not it came from proceeds of crime. CBC News; Global News; Winnipeg Free Press; Radio-Canada (2016-08-16)

Peterborough plane crash probe continues, RCMP now involved

City police continue to work with the **York** Regional Police and the Transport Safety Board as the investigation into Friday morning's plane crash on Lansdowne St. continues. The RCMP is also involved, city police report. The level of local police involvement will be determined as the investigation continues, city police say. Peterborough Examiner (2016-08-16)

Surrey RCMP request public help to locate Maya Singh
Surrey RCMP are requesting the public's assistance in locating a high risk missing female, Maya Singh, who was last seen on August 10 (Wednesday) as she left her home in Surrey for another family's residence. It wasn't discovered until August 13 (Saturday) that she didn't make it to her destination and was reported to police as missing. Maya Singh is described as a 68-year-old South Asian Fijian female, 5'3 in height, 155 pounds with black shoulder length hair and brown eyes. She was last seen wearing a black-and-white striped hoody, pink top, and plaid pajama pants. Maya Singh was also seen carrying three large purses / handbags (see photos). Investigators of Surrey RCMP Missing Person's Unit have located surveillance photos from August 10, the day she was last seen. The photos come from a business in the 12100-block of 72nd Avenue in Surrey. Indo-Canadian Voice (2016-08-16)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

MMIW Red Dress Campaign heading to Prince George
There will be empty red dresses hanging in parts of the city on October 2nd, honouring missing and murdered indigenous women. Local organizer Tammy Meise saw the Red Dress display while in Vancouver in 2014. She wants to give a voice back to local women who've gone missing, especially one. "One of my childhood best friends, Kari Anne Gordon, she was murdered and she has become a statistic. When I saw the red dress project it impacted me, it literally took my breath away ... us that are mothers, that are sisters, that are daughters, that are aunties, have family and friends that have gone missing. When you actually talk to people and start making connections, it's actually amazing how it affects so many people." Meise presented the event to Council on Monday night. Councillors unanimously supported the event and met her request of waiving the Lheidli T'enneh Memorial Park liability costs and covering the Park rental fees. Council also gave Meise permission to hold a candlelit vigil at the Park that night and many, including Councillor Terri McConnachie, promised to be there. My Prince George Now (2016-08-16)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Driver killed by gunfire: Father: ISIS supporter's funeral won't be held at mosque in London, spokesperson says
An ISIS supporter who died during a confrontation with an RCMP tactical team outside his home in Strathroy, Ont. was killed by a police bullet, his family said Tuesday. Wayne Driver said an autopsy had determined that his son Aaron had been shot two times and that one of the bullets had struck his liver and travelled to his heart. The other hit his spleen, he said. The 24-year-old was allegedly in the final stages of preparing a terrorist attack on Aug. 10 when a police Emergency Response Team surrounded him. He detonated an explosive device and police opened fire. Following the incident, the RCMP said it was unsure whether Driver had died as a result of his own bomb or police bullets but the father said the autopsy had put that question to rest. "It was the police officer's bullet that killed him," the father told the National Post. "The bomb that exploded he could have walked away from with minor to severe injuries they said." (...) In his first reaction to the alleged terror plot, Prime Minister Justin Trudeau said a wider response to domestic terrorism would be rolled out by Public Safety Minister Ralph Goodale. "All Canadians expect their government to do two things: To keep Canadians safe and to defend and uphold the values and rights that all Canadians hold dear," he said during a stop in Bridgetown, N.S. "Getting that

balance right isn't always easy in the challenging situation we now live in but it's extremely important." Kingston Whig-Standard, B1/FRONT

Public Safety Minister Goodale Outlines Intention to Combat Radicalization
Public Safety Minister Ralph Goodale says Canada must do better to be a leader in understanding and countering violent radicalization. Goodale says the death of Aaron Driver in Strathroy, who was suspected of planning a terrorist attack, demonstrates the need for *"continued vigilance"* in responding to threats posed by those who have been radicalized to the point of wanting to harm or kill innocent people. While there are no official plans in place, he says the federal government is working to create a new national office for community outreach and engagement that will help combat radicalization. There is no word on when the office will open, or if multiple locations will be established across the country. Goodale made his comments after visiting a centre in Montreal on Monday that works to prevent radicalization leading to violence. Last Thursday, the RCMP revealed that it was the FBI and not the Mounties who discovered a video that led them to Aaron Driver in Strathroy, who police said had threatened to detonate an explosive in an urban centre. Driver died Wednesday night after a confrontation with police that saw a bomb detonated in a taxi cab that was called to take him to Citi Plaza in London. An investigation continues to determine if Driver died from the blast or from a police bullet. AM980 (2016-08-16)

Family tries to clear the air about ties with aspiring terrorist Driver
As Aaron Driver put the finishing touches on a planned terrorist attack last week, he gave no hint anything was wrong, except for confiding that he was feeling ill. "He says, 'I'm not feeling good.' He's sick. He coughs and says, 'I want to go to a hospital,' " a 60year-old friend recalled. A cook for his congregation, he had befriended Mr. Driver when the 24-year-old loner showed up at the local mosque in London, Ont., last year. For initiating this friendship, the cook felt at first like a good neighbour - until last Wednesday. That's when a police intervention made the cook and his family feel like suspected accomplices. As authorities scrambled to neutralize the threat posed by Mr. Driver, they also used some heavy-handed tactics to isolate the family's home. Female family members say police snipers even pointed a laser-scoped rifle at them as they exited their house with their hands up. Three days earlier, Mr. Driver had been at that very house, where the family says he was showing a gentler facet of his personality. On that Sunday, "he trimmed the bushes in the back, the roses and daisies," the cook's 52-year-old wife recalls. She was explaining that her husband and Mr. Driver had bonded over odd jobs. "He was a polite, well-mannered kid, very quiet and shy," she said. Speaking to The Globe and Mail in an hour-long interview, the family members, who knew Mr. Driver by his Islamic name of Harun, say they can't reconcile the police allegations with their interactions with the young man they knew. They asked to remain anonymous to minimize any further fallout from being publicly linked to an Islamic State-inspired extremist, but wanted to speak out to clear up any lingering misconceptions that they were privy to Mr. Driver's ideas or aims. Media reports and senior RCMP officers publicly mentioned the family's address as a secondary search site last week, but police now say it was a red herring. "That was an address that we had some understanding Aaron Driver had a connection to ... so we wanted to follow up," RCMP Superintendent Harvey Seddon said. Declining to discuss specific police tactics or weaponry in an interview, he said "the family doesn't need to be concerned about any cloud of suspicion. Globe and Mail, A1

Muslim rites for terror suspect
The family of the Strathroy terrorism suspect killed in a clash with police last week is making arrangements to give him a Muslim burial Thursday Members of Aaron Driver's family were in London this week and contacted the London Muslim Mosque, asking about funeral protocol, a spokesperson said. "They did reach out to us, inquiring about the protocol for a Muslim funeral. We gave them the lay of the land," said Nawaz Tahir. "We will help and support the family as much as we can." The funeral neither will be held at the mosque, nor have an imam presiding over it, but is expected to be a private family affair, Tahir said. It's scheduled for what would have been Driver's 25th birthday. Driver, 24, an ISIS sympathizer, was shot dead last Wednesday after detonating explosives in a taxi outside his sister's Strathroy home. Police moved in after being alerted by the U.S. Federal Bureau of Investigation to a martyrdom video Driver had made, vowing to attack a major Canadian urban centre. Until Tuesday, police hadn't said whether Driver was killed by the blast in the taxi or by police gunfire. An autopsy concluded he died of a gunshot, police confirmed. Driver's activities, including communicating with ISIS members, had put him on a federal watch list while he was living in Manitoba and led to him being placed under a court-

ordered peace bond that banned him from computer and cellphone communication and required him to live with his sister in Strathroy. Postmedia Network (London Free Press, A1, Front, Winnipeg Sun, Toronto Sun, Ottawa Sun, Edmonton Sun, Calgary Sun); Canadian Press (Red Deer Advocate, A8, Winnipeg Sun, Ottawa Sun, Toronto Sun, Times Colonist, Edmonton Sun, Calgary Sun, Daily Gleaner, Times & Transcript); Presse canadienne (Le Droit) (2016-08-17); National Post; CBC News; Canadian Press (London Free Press, Kingston Whig-Standard, CTV News); Radio-Canada (2016-08-16)

Expansion urged for programs that combat radicalization
After RCMP thwarted a major terror threat in Ontario last week, Mohamed El-Rafih knew that his community anti-radicalization initiatives were more urgently needed than ever. El-Rafih is best known in Calgary's Muslim community as the creator of an anti-radicalization program that he calls Fostering Youth Inclusiveness (or FYI). The program is a day camp for children aged five to 12 that aims to fight radicalization by tackling the feeling of isolation that some Muslim children experience while trying to integrate into Western society. Now, El-Rafih is gathering a group of local politicians, police, religious leaders and Muslim community members on Thursday to see how his programs can be expanded and brought to high schoolage youth. "The purpose behind this meeting is to look at the messaging (we've come up with), and to get everybody's opinion on ... whether it is going to help us against radicalization," said El-Rafih. "There's messaging for Muslims and there's a message for non-Muslims. The message for Muslims is on how there could be misinterpretations on misguided imams and misguided leaders that could make youth vulnerable to radicalization." (...)El-Rafih expects the Calgary police, RCMP and Darshan Kang, Liberal MP in the Calgary SkyView riding, to attend Thursday's meeting, and hopes their input can help craft an effective message that will help to prevent the radicalization of teenage Muslims. Postmedia Network (Calgary Herald, A11, Edmonton Journal, Calgary Sun)

Terrorism propaganda case referred straight to trial
The Public Prosecution Service of Canada says the case against a Fort St. John man charged with four terrorism-related offences will go directly to trial. Spokeswoman Elizabeth Armitage said the case of Othman Ayed Hamdan will proceed by direct indictment, meaning there will not be a preliminary inquiry. Hamdan was arrested in July 2015 and accused of posting Islamic State propaganda online. An RCMP statement at the time alleged the propaganda included inducement and instructions to commit murder in the name of jihad. None of the allegations has been proven in court. Hamdan was originally charged with three terrorism related charges in provincial court, but Armitage said those charges have been stayed. B.C. Supreme Court documents show he is now charged with counselling to commit murder for a terrorist group, counselling to commit assault causing bodily harm for a terrorist group, counselling to commit mischief for a terrorist group and instructing a person to carry out a terrorist activity. Canadian Press (Times Colonist, A5)

American Involvement In Canadian Terror Cases Must Be Questioned
While watching last week's RCMP press conference in the aftermath of Aaron Driver's death, many questions invaded my mind but were left unanswered. The RCMP's narrative of the events that transpired was repeated over and over in the media with very little questioning. Mike Cabana -- the deputy commissioner of the RCMP who stood alongside his colleagues in the conference room at the RCMP headquarters, apparently nervous and uncomfortable answering some questions -- is the same Mike Cabana that was involved in the case of Maher Arar. (...)By contrast, Ottawa resident Mohamed Harkat has been the object of a security certificate due to suspicions that he is an Al-Qaeda sleeper agent for more than a decade. Today, he continues to face the threat of being deported to torture by the Canadian government, and has worn a GPS electronic bracelet for more than six years while living under what amounts to house arrest. All his visitors must report to Canada Borders Services Agency (CBSA) and he must obtain the authorization of the CBSA to leave his house. For years, he couldn't use the Internet or even get near a computer. Huffington Post (2016-08-16)

Transfert d'armes en Libye
Le gouvernement fédéral a transmis à la Gendarmerie royale du Canada (GRC) les conclusions d'un rapport de l'Organisation des Nations unies (ONU), qui révèle qu'une entreprise canadienne aurait opéré le transfert illicite de véhicules blindés vers la Libye. En mars, un rapport de l'ONU a avancé que l'entreprise ontarienne Streit aurait transféré en 2012 des véhicules blindés de ses installations des

Émirats arabes unis vers la Libye, pourtant sous un embargo commercial qui y interdit la vente d'armements. Selon le comité de l'ONU concernant la Libye, tout transfert de véhicule blindé vers le pays de l'Afrique du Nord devrait être interdit. En 2014, des membres de ce comité ont rencontré des représentants de Streit, qui se sont défendus d'avoir agi illégalement. Or, selon la CBC, qui a eu accès à des avis de livraison et des reçus de vente, l'entreprise canadienne aurait continué de vendre des véhicules blindés à la Libye et au Soudan du Sud après avoir été avertie par l'ONU. Le Devoir, A5 (2016-08-17); Radio-Canada (2016-08-16)

Terrorisme : une audience à Fort St. John déplacée à Vancouver pour des raisons de sécurité
L'audience préliminaire d'un résident de Fort St. John qui fait face à des accusations de terrorisme a été déplacée à la dernière minute à Vancouver pour des raisons de sécurité. Othman Ayed Hamdam est confronté à six chefs d'accusation pour entre autres la publication en ligne de propagande du groupe armé État islamique et d'incitation à commettre un crime au nom du djihad. L'entrepreneur de 33 ans est détenu à Fort St. John depuis juillet 2015. À l'époque, la communauté musulmane locale avait dit ne pas connaître cet homme qui n'avait selon elle jamais fréquenté la mosquée. L'audience préliminaire doit décider si suffisamment d'éléments ont été réunis par la Gendarmerie royale du Canada (GRC) pour que le dossier de M. Hamdam soit présenté en Cour provinciale. Si ce procès avait lieu, il s'agirait du second cas de ce genre dans une affaire terroriste en Colombie-Britannique depuis l'adoption de la loi antiterroriste C-51. Celle-ci accorde davantage de pouvoirs au Service canadien du renseignement de sécurité pour contrecarrer des complots de grands actes de violence. Radio-Canada; Canadian Press (Globe and Mail) (2016-08-16)

Revocation of airport-security clearance was unfair
A government decision that stripped a woman of her airport-security clearance and put her out of work more than two years ago was unfair, incomprehensible and unreasonable, a Federal Court judge has ruled. In ordering the minister of transport to take another look at the case, Judge Susan Elliott slammed the government for treating Ayaan Farah in a shoddy fashion. The advisory group that recommended revoking the clearance did not carefully review documents, Elliott said in her written decision, while the director general of aviation security failed to "ensure the critical facts upon which she relies are very clear." Elliott quashed the revocation, saying the government had hidden behind the Privacy Act and failed Farah badly - especially in light of the "gravity of the consequences" to her. Farah expressed delight with the ruling, saying she hopes it will help others caught in a similar situation. "I hope this brings light to the fact that Transport Canada needs to do a better job regarding security-clearance decisions - cancelling people's clearance," Farah said in an interview Tuesday. "Transport Canada needs to change its policy." In April 2014, Transport Canada told Farah the RCMP had reported her having contact with criminals only identified as subjects A, B, and C. Police claimed that two of the individuals used Farah's car to go to a funeral for a known gang member - although she was not in the car and did not attend the service. RCMP also said police interacted with her while she was in A's company, but she said she had no memory of being stopped by police. She also said she did not know who the criminals were, although her lawyer suggested one might have been her brother. Canadian Press (Times Colonist, A8, Chronicle-Herald, Kingston Whig-Standard, Waterloo Region Record, Leader-Post, Ottawa Citizen, Calgary Herald)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Driver hits RCMP car in Nanaimo detachment parking lot
RCMP are investigating after a driver steered their car into the rear parking lot of the Nanaimo detachment and collided with a police car Tuesday morning. Few details have been released but police said after entering the parking lot at about 8:30 a.m., the driver accelerated and hit a dumpster, knocking it aside and narrowly missing two officers, who were on foot. The vehicle then continue and collided with a police car that had three officers inside. Global News; Nanaimo News Bulletin (2016-08-16)

Free Our Finest hopes to raise $20,000 to support athletes training for Special Olympics
Law enforcement officers in the Red Deer area will once again demonstrate their dedication to Special Olympics by hoisting members atop scaffolding outside Walmart at Parkland Mall. Three officers will camp on scaffolding about five metres high, located to the left of the Walmart entrance, from 9 a.m. on

Friday to 4 p.m. on Sunday for Free Our Finest fundraising event. Participating agencies include RCMP, Alberta Corrections and Alberta Sheriffs. Committee member Brad Cotmen said the goal this year is to raise $20,000 and that money will stay in the Red Deer area to assist local athletes. "It's an extremely worthwhile event. All proceeds go to support Special Olympics for their training, their coaches, attending different events," Cotmen said. People can get their pictures taken with an old West-style prison trailer and other law enforcement vehicles, view demonstrations and take part in water fights, attend a barbecue lunch, buy merchandise, and make donations. Red Deer Advocate, A2

Musical Ride a great opportunity
An editorial states, "When the agricultural societies in Lincoln and West Lincoln merged, there were a lot of critics out there questioning the move. Much of the debate was sentimental and understandably so. The move meant a new chapter would begin for the two organizations which each had a tremendous history and presence in their respective communities. It also meant significant change, including the sale of the Beamsville Fairgrounds and the move of the fair from downtown Smithville to the current agriplex on the edge of West Lincoln... If you can't make it to RCMP Musical Ride be sure to save the date and make it to the fair Sept. 8-11. It will be a great chance to see this new facility and enjoy a community tradition." Niagara This Week (2016-08-16)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

NIL

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

How will PM tackle terror? Just watch him
An opinion piece states, "So far on terrorism, Justin Trudeau is more or less the prime minister Stephen Harper told us he would be. On the very day Trudeau became leader of the Liberal Party of Canada, in April 2013, he sat in Ottawa for an interview with Peter Mansbridge of the CBC. Two bombers had just detonated their home-brew contraptions at the Boston Marathon, killing three and wounding hundreds. How would you respond if you were prime minister, Mansbridge asked. "Over the coming days," Trudeau replied, "we have to look at the root causes." That language seemed custom- designed to ruffle Conservative feathers. But Trudeau was not done. "There is no question that this happened because there is someone who feels completely excluded. Completely at war with innocents . . . And our approach has to be, where do those tensions come from?" (...) In a long weekend news release, Goodale first reassured Canadians that the police had done their job well and that Canada's threat level is no higher than it has been for a year and a half. Then he added: "We have also budgeted for a new national office and centre of excellence for community outreach and counter-radicalization. "We need to get really good at this - to preserve our diversity and pluralism as unique national strengths." So if you want a government that conveys any view other than utter condemnation, this new Liberal government's language will seem wildly complicated. Goodale remains unbowed. "We need to know how to identify those who could be vulnerable to insidious influences that draw certain people - especially young people - toward extremism leading to violence," he wrote. "We need to understand what positive messages can counteract that poison." Toronto Star, A1

Kudos and questions in terrorist takedown
An editorial states, "Canada came very close to suffering a terrorist attack last week, but countless lives were saved when police disrupted the plan. The wouldbe terrorist, Aaron Driver, who was living in Strathroy under what was basically a restraining order, was killed. How he died isn't yet clear. The Ontario Provincial Police are investigating whether he died by police gunfire or from a bomb that went offin the back of a taxi, injuring the cabbie who had picked up Driver at the house in which he lived. The RCMP acknowledged the tragic outcome but noted correctly that had Driver not been stopped, the carnage would have been far, far worse. So let's take a moment to give our police and security authorities - whose actions are often challenged - full credit. In a fine example of cross-border co-operation, the operation began with a tip from the FBI, which had come across a martyrdom video. (...) Questions remain, of

course. We don't know how the FBI got the video, for example. Some wonder about the peace bond Driver was under and why an electronic monitoring bracelet had been removed. There's a tricky balance between monitoring for terrorism and respecting civil liberties; he had never been charged or convicted of a dangerous crime. Even if he had, severe conditions, particularly imprisonment, can further fast-track extremist tendencies. There are dicey political and policy issues ahead. The Liberals remain committed to reforming the Tories' anti-terrorism bill, C-51, but this incident adds complications. And the task has barely begun, although a bill to create a new national security oversight committee has been tabled." Kingston Whig-Standard, A4

Don't overestimate terrorist threat to Canada

An opinion piece states, "Last Wednesday Canada experienced another brush with global terrorism, when Aaron Driver was killed during a violent encounter with police in the sleepy southern Ontario town of Strathroy. No one but Driver was killed in the incident, but the fear-mongers were quick to tell Canadians that the intent of this deranged Islamic supporter of Daesh (also known as Islamic State, ISIS, and ISIL) was to commit mass murder during a workday rush hour. Scary stuff. According to the official version of events, it was the FBI that first discovered that Driver had made a recent martyrdom video and was about to launch an attack. It had to be the FBI because the Canadian Security Intelligence Service insists that it does not spy on Canadians. Driver had long publicly declared his sympathy for the Daesh cause and, as a result, had been arrested prior to signing a peace bond to secure his release. (…) First of all, Driver was a troubled youth who found popularity among Daesh sympathizers online. He was not a hard-core member of the Daesh evildoers. He had never even been to the Middle East, and the congregation at his local mosque tried to correct his skewed take on the Islamic faith. He did make some sort of bomb, but if the result was that exploding it in his own lap failed to kill him and left the taxi driver largely unhurt, it really wasn't much of a bomb. The intelligence and security services-both Canadian and American in this case (because Canadians don't spy on Canadians)-worked efficiently together. Driver did not get to carry out a terror attack. He was killed before he could even attempt the attack. No one was terrorized by his actions. Yet after Driver's death we were told of all the carnage he "would have" created, therefore making it imperative to impose stricter security measures and better monitoring to keep the public safe. (…) Canada remains very, very safe." Hill Times

Rift between Muslims and police deepens

An opinion piece by Amira Elghawaby, the communications director at the National Council of Canadian Muslims, states, "The past few weeks have deeply shaken whatever trust exists between Canadian Muslim communities and law enforcement agencies. First, news and video footage of the heartbreaking and unjustifiable death of a mentally ill Canadian-Somali man in Ottawa as a result of a police intervention. Then, a B.C. Supreme Court judge ruled that the RCMP were the key architects of a terrorism plot that was used to entrap two marginalized individuals who had recently converted to Islam. Both of these cases have spotlighted some troubling excesses in our country's security establishments. They further underscore the need for Canadians to continually question the unequal power balances in our society that can and do sometimes lead to violations of the human rights and dignity of fellow community members. (…) "We need a fundamental and transformative cultural change to policing attitudes and practices," argued criminology professor and policing expert Darryl Davies in a recent Ottawa Life Magazine article. The same conclusion might be drawn from the RCMP's role in manufacturing a terrorist plot, which points to deep flaws in how security agencies operate. Justice Catherine Bruce's ruling in the case against John Nuttall and Amanda Korody should serve as a wake-up call for our elected leaders. "There must be a balance between the need to protect the public from crime and what is tolerable police conduct in a free and democratic society," wrote Justice Bruce. There is clearly an urgent need for adequate checks, balances, and oversight of those who hold incredible power and authority. With the federal government's current consultations on the Anti-terrorism Act, the time for Canada to properly balance civil liberties with public safety is now. Trust is fundamental to our collective well-being. We need more of it, not less. As the authors of a 2016 Kanishka research study of Canadian Muslim concerns around counterterrorism policies discovered in their interviews, citizens are losing faith in the state." Toronto Star, A13

How much do we really know about the Canadian intelligence community?

An opinion piece states, "The Trudeau government is set to review the activities of Canada's spy agencies at a time when it appears Bill C-51 has empowered many of the more than 20 agencies and departments with surveilling powers to violate the Canadian Charter of Rights and Freedoms. Last year American whistle-blower Edward Snowden proclaimed that Canadian intelligence agencies have the "weakest oversight" in the Western world and compared the Canadian government's Bill C-51 to George W. Bush's post-9-11 U.S. Patriot Act... There should be an inquiry into the events that led to Driver's death. In essence he was "engaged and killed" for an action he had not yet carried out. Moreover, it appears the young man was under close surveillance by at least two different countries, making it difficult to imagine that authorities could not see it coming. However, putting aside those important questions for the moment, one thing is clear: the event gave Minister of Public Safety Ralph Goodale justification for the continued delay of the Liberals' election promise to reform C-51... Mapping the issue is helpful. Different agencies report to different ministries. The RCMP and CSIS, for example, report to the Minister of Public Safety, while The Canadian Security Establishment (CSE) reports to the Minister of National Defence. The Independent (Newfoundland & Labrador) (2016-08-16)

Countering extremism
A letter to the editor states, "Re: Young terror supporter had troubled upbringing (Aug. 30). I am absolutely shocked that the RCMP identified a homegrown extremist originally from Winnipeg who was planning to attack a public area in Canada. It is quite scary, in fact, to see the power of social media and how it is being manipulated to serve the interests of ideological extremist recruiters. Aaron Driver, a 24-year-old living in a town in Ontario, had shown support for ISIS in the past and was thus being monitored. I am thankful this situation did not escalate to an attack and was mitigated immediately. Although there may be many solutions to homegrown extremism, the most effective one is having a true and powerful counter-narrative. One example of such a narrative is the Ahmadiyya Muslim Youth Association, which is known for giving back to society through blood drives, food drives, city cleanups and much more. These counter-narratives will help put an end to homegrown extremism and continue to make Canada great..." Winnipeg Free Press (2016-08-16)

Fighting crime in the digital age
An opinion piece states, "This week, top police officials from coast to coast have descended on our nation's capital for the 111th annual Canadian Association of Chiefs of Police conference. The topic that will shape their discussion, Public Safety in a Digital Age: Real Victims - Real Crime, is timely, given that we're at an important societal juncture. So much of our daily lives now take place online: our wealth passes through jurisdictions in the form of ones and zeros; the most intimate details of our lives, whether they are held by government or industry, rest on servers located somewhere around the globe; and our critical infrastructure, whether it is managed by the public or private sector, is operated digitally. Given the recent media coverage of data breaches and many people's personal experiences with fraudulent phishing schemes, it's understandable that we, as consumers and citizens, want to erect the highest walls possible around our valuable digital assets. This is a natural human reaction, but it isn't a realistic societal response, given the magnitude of our online world." National Post, A8

OTHER / AUTRES

Mario Harel s'affaire déjà à la tâche
Le directeur du Service de police de la Ville de Gatineau, Mario Harel, est devenu le «chef des chefs» de police, d'un océan à l'autre. A peine 24 heures après son élection unanime à la tête de l'Association canadienne des chefs de police (ACCP), M. Harel s'est prononcé mardi sur les enjeux qui marqueront son mandat de deux ans, se réjouissant au passage de l'oreille attentive du nouveau gouvernement fédéral. M. Harel est passé de vice-président à numéro un de l'organisme représentant plus de 1000 membres, lors du congrès de l'ACCP, qui se termine à Ottawa ce mercredi. Il compte profiter de son siège pour marquer des points sur la colline parlementaire. «Avec l'arrivée du nouveau gouvernement, dit M. Harel, il y a un dialogue avec l'ensemble des décideurs qui touchent la sécurité publique. (Le gouvernement) écoute nos enjeux et on écoute ceux du gouvernement. Il y a une bonne communication avec les autorités. On sent qu'il y a une écoute et on sent un désir d'améliorer le cadre législatif dans le but d'améliorer la sécurité publique.» M. Harel sera président lorsque le gouvernement Trudeau

légalisera la marijuana, l'an prochain. Ce dossier fait partie des préoccupations à court terme de l'ACCP. Le Droit, 5

Deux fois plus de crimes contre des groupes religieux
Graffitis nazis sur une synagogue, tête de porc devant une mosquée, homosexuels agressés : plus de 250 crimes haineux ont été commis au Québec en 2014, dont près d'une centaine à Montréal. En un an, les crimes ciblant un groupe religieux ont doublé dans la province. Les communautés juive et musulmane sont préoccupées par le phénomène, mais n'observent pas de flambée sur le terrain. Le nombre de crimes haineux perpétrés au Québec était relativement stable dans les dernières années, et même en baisse au Canada. Or, 257 délits haineux ont été rapportés en 2014, un bond de 39 % par rapport à l'année précédente, a révélé le ministère de la Sécurité publique (MSP) dans un volumineux document rendu public lors de l'étude des crédits, en avril dernier. Depuis 2010, il n'y avait jamais eu plus de 200 crimes haineux pendant une année. Cette récente augmentation est « majoritairement attribuable à la hausse des délits motivés par la haine contre certaines religions », selon le MSP. En effet, ces crimes ont doublé entre 2013 et 2014 (48 contre 94). D'autre part, 80 crimes étaient guidés par la haine contre la « race ou l'ethnie » et 27 par l'orientation sexuelle de la personne. Le Ministère prévient toutefois qu'une « grande prudence est de mise dans l'interprétation des données [_] considérant qu'il est parfois complexe d'établir le caractère haineux d'un délit ». Les données de 2015 n'ont pas été compilées. À Montréal, 113 crimes haineux ont été répertoriés l'an dernier, une hausse de 24 % en un an. Pourtant, au moment de présenter la nouvelle escouade vouée aux crimes et incidents haineux, en mai dernier, le chef Philippe Pichet évoquait plutôt une moyenne d'environ 70 crimes haineux chaque année dans la métropole. Il avait aussi spécifié que le phénomène n'était pas en hausse. La Presse+

Windsor police host forum to fight sex slavery
Police, social service groups and others in the battle against human trafficking emerged from a roundtable discussion in Windsor Tuesday calling for a provincewide task force to fight the growing scourge. Progressive Conservative MPP Laurie Scott from Haliburton-Kawartha Lakes-Brock, who introduced the private member's bill known as Saving the Girl Next Door Act, said there are victims in virtually every city, neighbourhood and high school. "This is one of the largest growing crimes in Ontario, Canada and globally," said Scott, who travelled to Windsor for the discussion. "We have to recognize it's happening in our neighbourhoods and we have to help our children from these horrific situations." Windsor police hosted the roundtable, which brought together officers, community organizations and others with a stake in the fight against human trafficking. Scott, whose Bill 158 has passed second reading, said more than 90 per cent of victims in this country are Canadian-born. Scott added that Ontario has been designated as a hub for human trafficking in Canada, with 65 per cent of all cases occurring in the province. Shelley Gilbert from Legal Aid Windsor during a Windsor Police Service hosted roundtable discussion on Human Trafficking with community partners and MPP Laurie Scott from Haliburton-Kawartha Lakes-Brock. Windsor Star

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 1, 2016 / le 1 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Montreal journalist ' spied on ' by police

A Montreal journalist whose iPhone was monitored by police for months says he was outraged to discover he had been " spied on " as part of what he calls an effort to identify his sources. " I was living in the fiction that police officers wouldn't dare do that, and in the fiction that judges were protecting journalists - and this type of police intrusion ," Patrick Lagace, a columnist for La Presse, said in an interview Monday " Clearly, I was naive ." The French-language newspaper said it learned at least 24 surveillance warrants were issued for Lagace's phone this year at the request of the Montreal Police ' s special investigations unit. That section is responsible for looking into crime in the police force. Three of those warrants reportedly authorized police to get the phone numbers for all Lagace ' s incoming and outgoing texts and calls, while another allowed them to track the phone ' s location via its GPS chip. The surveillance was ordered as part of an internal probe into allegations police anti-gang investigators fabricated evidence. Five police officers were arrested this summer and two were charged as a result. Lagace said police told him they obtained the courtauthorized warrants because they believed the target of one of their investigations was feeding him information. Canadian Press (London Free Press, N3, Leader-Post, Vancouver Sun, Edmonton Journal, Ottawa Citizen, Windsor Star, StarPhoenix, Waterloo Region Record, Calgary Herald, National Post); Montreal Gazette; Le Devoir; Globe and Mail; Toronto Star; La Voix de l'Est

Montreal Cops Have Tracked a Journalist's Cellphone for the Past Year

Montreal police, investigating the possibility of crooked cops on the force, obtained warrants to surveil a journalist's iPhone, and even obtained permission to use his GPS chip to track his whereabouts at all time. But the federal minister of public safety, Ralph Goodale, stopped short of discouraging police forces

from going to the courts to obtain judicial orders against journalists. Asked directly by NDP Member of Parliament Matthew Dubé on Monday about whether he'll issue a directive to create more formal rules around how police deal with journalists, Goodale would only say that *"we take the freedom of the press in this country very, very seriously."* Dubé raised the question after on Monday after Montreal newspaper La Presse published details on surveillances warrants, at least 24 in total, obtained to surveil journalist Patrick Lagacé. The MP also referenced another case, where federal police are working to obtain chat records from a VICE journalist's cell phone, as evidence that action needs to be taken. Vice News (2016-10-31)

SPVM: le ministre Coiteux est surpris par une procédure contre un journaliste
Le ministre de la Sécurité publique, Martin Coiteux, a exprimé sa surprise, lundi, en apprenant que la police a surveillé les appels téléphoniques d'un journaliste. M. Coiteux a entamé des vérifications pour établir si les procédures ont été respectées par le Service de police de la ville de Montréal (SPVM). «J'ai été très surpris et c'est pour ça qu'on fait des vérifications», a-t-il dit. La ministre de la Justice, Stéphanie Vallée, effectuera également une évaluation des procédures qui ont mené un tribunal à accorder à plusieurs reprises un mandat au SPVM, cette année... À Ottawa, le ministre de la Sécurité publique, Ralph Goodale, a affirmé que la situation est toujours délicate quand le journalisme et les enquêtes policières se rencontrent. «Il s'agit d'un cas qui relève des compétences provinciales, mais la position fédérale est d'affirmer que la liberté de presse est une valeur canadienne fondamentale», a-t-il dit. La Presse Canadienne (L'actualité) (2016-10-31)

Affaire Lagacé : Goodale prêt pour «une discussion sérieuse» sur les règles policières
À la lumière de l'affaire Patrick Lagacé, le ministre fédéral de la Sécurité publique Ralph Goodale se dit « certainement prêt à avoir une discussion de politique sérieuse » et « à entendre les représentations » des médias sur la façon dont les forces policières devraient concilier leurs enquêtes avec la protection des sources journalistiques et la liberté de presse. Le ministre Goodale, qui n'a pas voulu commenter le cas de Patrick Lagacé mais qui se dit « profondément préoccupé par ce genre de dossier », s'assurera prochainement auprès du commissaire de la GRC Bob Paulson que les directives fédérales en vigueur sont respectées dans les faits. Depuis 2003, une directive ministérielle demande aux forces policières de porter une « attention spéciale » au statut des médias dans le cadre d'enquêtes sur la sécurité nationale. « Au regard de ce dossier au Québec, qui est sous juridiction provinciale, c'est une question qui doit être posée [à la GRC]. Je n'ai pas encore eu l'occasion de le faire [hier], mais je le ferai [prochainement]. C'est une question juste de demander [à la GRC] de s'assurer que la directive ministérielle qui requiert un très haut standard soit appliquée dans les faits », dit le ministre Goodale en entrevue à La Presse. Le ministre Goodale, qui croit que la liberté de presse est « une valeur fondamentale » au Canada, n'a pas voulu s'avancer à savoir si des changements législatifs sont nécessaires afin de protéger la liberté de presse dans le cadre d'enquêtes policières. « Nous devons traiter de cet enjeu sérieusement et je suis certainement prêt à entendre les représentations [des médias et d'associations de journalistes comme la FPJQ] sur ce qui pourrait être un meilleur ensemble de règles », dit le ministre Goodale... La Sûreté du Québec a saisi en septembre l'ordinateur d'un journaliste du Journal de Montréal à la demande du Conseil de la magistrature en rapport avec un dossier traité par le conseil. Le ministre Goodale, qui n'a pas voulu commenter sur ces cas précis, fait valoir que « les cas vont suivre leur cours pour voir s'ils respectent les critères de la Cour suprême » en matière de protection du matériel et des sources journalistiques. La Presse (2016-10-31)

We're spied on more often than you think, journalists groups say
Canadians may be used to hearing about police tapping journalists' phones in China, or tailing them down the street in Turkey. But in Montreal, Canada? Unfortunately, say organizations like Canadian Journalists for Free Expression, it is happening a lot more than we think. "It's something we've been suspecting for a long time – that when this kind of power is in the hands of the police they will abuse it," said Tom Henheffer, executive director of CJFE. "I used to be cautious about drawing parallels with Canada and dictatorships like Turkey, China, Russia or Egypt. But the difference has started to erode, especially when it comes to privacy rights"... Montreal Gazette (2016-10-31)

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

Man arrested after costume gun scare at Camosun

What's thought to be a poorly-thought out Halloween costume caused a scare at Camosun College's Lansdowne campus Monday afternoon when a man was spotted in army fatigues and what looked to be a pistol strapped to his leg. A 28-year-old man has been arrested and **Saanich** police are recommending one charge of possession of a weapon for a dangerous purpose. Police responded to several reports of a man with a handgun on the Lansdowne campus around 3 p.m. Officers were on scene within four minutes and quickly arrested a man, said Saanich police spokesman acting Sgt. Jereme Leslie. A replica hand gun was seized. "We would like to remind people that carrying an imitation firearm is extremely dangerous, even at Halloween," Leslie said. "Responding to this incident put many people at possible risk." It's unclear if the man is a Camosun student. The man will appear in court in mid-December. (…) Victoria police took 12 people into cells for public intoxication between noon on Friday and noon on Monday, according to department spokesman Bowen Osoko. West Shore RCMP arrested two people for public intoxication Saturday night. Times Colonist, A3

Woman killed by son had informed police she was afraid of him

Statement heard at sentencing of Michael McCormick, who pleaded guilty to manslaughter. Ten days before she was killed, Pamella Dyer told police she was afraid of her adult son, Michael McCormick, because crystal meth made him delusional. "He thinks I'm not his mother, that I'm out to get him," Dyer told RCMP in a video recorded statement on July 10, 2014. "He's using meth," she said on the recording, played in **Victoria** Supreme Court Monday. "And when he is in that state, he is as strong as an ox and he has no mind." On July 20, 2014, Dyer, 64, was found lying dead in her Sooke home, at 2227 French Rd. McCormick was arrested and charged with second-degree murder on Sept. 17, 2014. McCormick, 38, was in B.C. Supreme Court for a sentencing hearing on Monday after pleading guilty to manslaughter in his mother's death. He entered the guilty plea on Oct. 11. Prosecutor Ruth Picha told Justice Brian Mackenzie that the Crown is seeking a prison sentence of 12 to 15 years. Picha said McCormick's addiction to crystal meth and personality disorders led to bizarre behaviour. But psychiatric examinations determined McCormick is not mentally ill. Times Colonist, A1/Front

Vader reversal cold comfort for McCann clan

"This has gone on a long time, to say the least," Justice Denny Thomas said with a grimace. That's an understatement. On Monday, Thomas vacated Travis Vader's two second-degree murder convictions, which he had handed down Sept. 15. In effect, he reversed himself and found Vader was not guilty of murder. But Thomas wasn't done. He then found the Alberta man guilty of two counts of manslaughter in the deaths of Lyle and Marie McCann, the **St. Albert** seniors who disappeared west of Edmonton while on a camping holiday in June 2010. (…) A more likely sentence, suggested Sankoff, could be around 15 years. Crown prosecutor Ashley Finlayson seemed sanguine Monday. "We felt justice would be done," he said calmly outside the courthouse. It may not look like justice to everyone. After 6-1/2years of blunders by the RCMP, the Crown prosecutors office and the trial judge, this case has taxed public patience and diminished public confidence in the administration of justice in Alberta. Edmonton Journal, A1/Front; * Globe and Mail

Jury watches video recording of Morningstar's police interview

Devin Morningstar told police investigators during a jailhouse interview, a video recording of which was shown to jurors Monday, that Marissa Shephard sent her young son away hours before Baylee Wylie was killed, telling people at her house she was worried for his safety. (…) In the video, played in Court of Queen's Bench, Morningstar was crying and unintelligible at times at the start of the video as he spoke to two police officers from the RCMP Major Crime Unit who visited him in jail two days after his arrest for murder. In the Dec. 20 video, Morningstar said he participated in the attack on Wylie but didn't kill him. "I know I deserve a punishment, but I did not murder that guy," he told **Codiac** RCMP Sgt. Jim MacPherson when the video was played for the jury Monday morning. "Who did?" asked the investigator. "Tyler," said the murder suspect. Times & Transcript, A1, Front

Inquest into police shooting death of Felix Taqqaugaq begins in Igloolik: Man was shot in his own home after officers say he threatened them with a weapon
More than four years after Felix Taqqaugaq was shot and killed by RCMP officers in his own home, his family and the community of **Igloolik**, Nunavut, will get some answers starting today. Taqqaugaq died March 20, 2012. A coroner's inquest into the death begins Tuesday morning in Igloolik and is scheduled to run until Nov. 11. It's a mandatory inquest since the death was police-related. Nunavut Chief Coroner Padma Suramala will preside over the inquest, which will detail the events surrounding Taqqaugaq's death, and the findings from the subsequent investigation by the Ottawa Police Service. The details of the investigation, which was completed last year, have not yet been made public. In March 2012, Taqqaugaq phoned in to the community radio station in Igloolik and started ranting. Family members said he suffered from mental health issues. After the rant, someone in the community called the RCMP and police went to his house to check on him. CBC News

RCMP nab 10 men for prostitution-related offences in Moncton
The **Codiac** RCMP arrested 10 men, aged 25 to 80, for attempting to obtain sexual services in Moncton in two separate busts earlier in October. The RCMP carried out two police operations Oct. 14 and 27 in the area of Dufferin Street targeting individuals attempting to buy services from sex trade workers. CBC News; CTV News (2016-10-31)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Indigenous and Northern Affairs Minister speaks at Trinity College: Bennett talks Nation-to-Nation, endangered languages, re-Indigenizing urban spaces
Federal Indigenous and Northern Affairs Minister Carolyn Bennett spoke at Trinity College on October 28. The event was part of a series called Conversations with the Chancellor Bill Graham; it consisted of a brief introduction made by Trinity Provost Mayo Moran, a discussion period, and a question and answer period. A reception was held when the formal event finished. (…) The preservation of Indigenous languages was also discussed; Bennett reiterated that the endangered languages and the extreme importance of Indigenous education are the responsibility of the government. Throughout the conversation, specific examples of Indigenous concerns and issues arose. There was discussion on pipelines, the United Nations Declaration on the Rights of Indigenous Peoples, missing and murdered Indigenous women and girls, as well as the Trans-Pacific Partnership deal. (…) In terms of resolution, Bennett said that the government must change their "urban-Aboriginal strategy." Bennett explained how this relies on a "commitment to reconciliation." Varsity (U of T)

Alberta trucking company says racist slur sticker 'a joke'
A photo taken of a truck with a sticker above the front grill has gone viral on social media as a result of its derogatory language towards indigenous women. The sticker, which read "One Squaw Too Many," was spotted in the area of Grande Cache, Alta. and has some wondering if charges should be laid for hate speech. Grande Cache RCMP confirmed they received a complaint about the truck and have dealt with the matter, declining to go into anymore detail. No charges have been laid against the company. Sandra Jansen, MLA for Calgary-North West who shared the post on social media, said when she saw the post it made her blood boil. "There's absolutely nothing funny about this when across the country we're defining the parameters of the Missing and Murdered Indigenous Women Inquiry and talking about some serious endemic problems." she said. Metro News

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

'We are seniors, why you hit me and my wife?': Elderly couple speak out about RCMP arrest
The elderly couple caught on camera being violently arrested by Coquitlam RCMP last week is speaking out. The incident happened on the evening of Oct. 26 after police were called to a strata meeting that allegedly got out of control. The video, which was posted on YouTube, appears to show an officer

dragging a man down a staircase while another officer arrests a woman, who appears to fall at one point... Myung Ju Lee and his wife, Kap Su Lee, told Global News they spent the night in the hospital after ending up with bruises, cuts and scrapes as a result of the incident. "[The police] walked up and did not say anything. Just walked up and grabbed us," Myung Ju Lee said. Lee claims the strata meeting was not over and there had been no screaming or fighting when police entered and grabbed him and his wife... Lee believes the police officers involved should not only apologize but lose their jobs. Additionally the couple wants compensation for their physical and mental anguish due to the incident. The couple have given a statement to Coquitlam police and will be getting a lawyer. Global News (2016-10-31); AM 730

Complaints about elderly B.C. couple's arrest prompt federal investigation
Days after troubling footage emerged of Mounties arresting an elderly couple in Coquitlam, B.C., a federal agency is launching an investigation into the officers' conduct. The Civilian Review and Complaints Commission for the RCMP said it has received more than a dozen complaints from people expressing concerns about the YouTube video, which at one point shows an officer dragging a senior down a stairwell. "We've received approximately 15 complaints from concerned citizens," said Richard Evans, senior director for the independent agency. "Some were present at the scene and some were not." The incident, which took place after a heated strata meeting at a Best Western hotel, is already being investigated by the New Westminster Police Department, which will decide whether to recommend charges against the officers involved. But the Civilian Review and Complaints Commission's probe could potentially lead to changes in RCMP policy moving forward, Evans said. "Our investigation is designed to make findings and recommendations about [officers'] conduct to inform better policing practices," he told CTV News. "Issues like: Did they have the authority to arrest? Was the appropriate use of force used? Were the RMCP members there properly trained? Were they properly supervised? Was there a language issue?" CTV News

Ex-tax auditor acquitted in corruption case
One of the eight Canada Revenue Agency auditors charged in connection with an RCMP investigation into alleged corruption at the taxman's offices was acquitted at the Montreal courthouse Monday. Quebec Court Judge Christian Tremblay found Luigi Falcone not guilty on all four counts he has faced since 2012, when charges were laid against him in Project Cloche. The charges involved allegations that Falcone, 54, of Laval, Que., solicited a $50,000 bribe from a man who owned a restaurant in Notre-Dame-de-Grâce at the time. The owner, Mario Agostini, alleged that Falcone falsely claimed he had looked at his file at the Canada Revenue Agency, found out it was going to pursue him for $250,000 in undeclared revenue and warned he might go to jail. Agostini testified that he turned down Falcone's offer after consulting a lawyer and an accountant. Six witnesses testified for the Crown during the trial in February. Falcone gave evidence in his own defence. "Mr. Agostini is not credible and (was) unreliable concerning some of his testimony," Tremblay said before acquitting Falcone, who worked for CRA in 1990-2009. The judge even raised the possibility that Agostini misunderstood Falcone after asking his advice on what to do about the actual audit his restaurant was about to be subject to. Leader-Post, N6 (Windsor Star, National Post, Gazette)

Ottawa terror suspect granted bail again after allegedly breaching conditions
An Ottawa terror suspect has been released from custody after he was charged with breaching some of his bail conditions while awaiting the outcome of his case. The RCMP arrested Tevis Gonyou-McLean in August on a terrorism peace bond for his alleged support of ISIL and was later granted bail on several conditions that included wearing a GPS monitoring device on his ankle and a ban on possessing any terrorist logos. On Oct. 25, the 24-year-old was arrested again after police allege he failed to report to the John Howard Society's bail supervisory program and reside at his pre-approved address, and that he damaged his ankle bracelet, thereby allegedly committing mischief. But his Ottawa lawyer, Biagio Del Greco, said the breaches were the result of a "miscommunication" and said the damage to the bracelet occurred while his client was in police custody and was unintentional. None of the breaches were related to alleged terrorist activity. Ottawa Citizen (2016-10-31)

Former military members who were discharged over sexuality launch class-action suits

People discharged from service because of their sexuality say they suffered extreme psychological trauma from the experience. Frustrated by inaction from Ottawa, former members of the Canadian military who were discharged because of their sexuality are launching class-action lawsuits against the federal government. The plaintiffs seek redress for members of the Canadian Forces and the federal public service "who were investigated, targeted, sanctioned and/or who were discharged or terminated by the Government of Canada because of their sexual orientation, gender identity or gender expression," according to a statement of claim deposited Monday in Quebec Superior Court. (…)Beginning in the 1950s, security agencies sought to identify suspected homosexuals serving in the military and public service, including government agencies such as the CBC and the National Film Board. The investigations continued until the 1990s, when the Mulroney government ordered an end to the practice. At one point, the RCMP had the names of 9,000 people on file. Those targeted were subject to dismissal, demotion or other punishment. Many simply left the military or the public service rather than face investigation. Ms. Roy was dismissed from the military in 1984, after being labelled a sexual deviant because she is a lesbian. Globe and Mail

Les visages de la radicalisation
«Je suis là pour m'excuser.» Devant nous, un grand baraqué. Rempli de remords. La Fédération des Québécois de souche, c'est lui. Ou plutôt, c'était lui, quand il cultivait le nationalisme blanc, vraiment blanc. «Je suis le fondateur, le seul et unique. C'est parti de ma tête.» Et elle était rasée, cette tête, à l'époque skinhead. Lui, c'est Maxime Fiset, de Québec, aujourd'hui étudiant universitaire… qui a déjà pensé faire sauter une bombe comme celle du marathon de Boston. Il a aussi été modérateur pour un site Web très raciste. Lundi, il est sorti de l'ombre pour dire qu'il a tout balancé. La radicalisation violente, «c'est plus proche de nous qu'on pense», prévient-il. Il était rendu à un tel point que les policiers l'ont arrêté pour propagande haineuse. (…) C'était avant l'État islamique. C'était les talibans, Al-Qaida. Mubin Shaikh étudiait la religion. Il avait 19 ans. Il est parti du Canada en voyage initiatique au Pakistan. Pas dans des camps. Juste un voyage de jeune croyant, raconte-t-il. Et il a rencontré ses nouveaux voisins, des talibans de la ville de Quetta. «Ils sont encore là.» Il a appris quoi? «Que pour être un vrai musulman, il faut combattre. Au retour, il a rejoint d'autres extrémistes ici. Il a recruté dans des mosquées, des conférences islamistes. Puis il y a eu le 11 septembre 2001, les tours de New York qui tombent. Ça, c'était trop pour lui. Il est parti pour la Syrie (bien avant la guerre). «J'ai appris le vrai islam.» Revenu au Canada, il a vu un de ses amis se faire arrêter. Il a alors appelé les services secrets : «Ils m'ont recruté pour être agent infiltrateur. Pendant deux ans, j'ai été infiltré.» Il a aussi travaillé pour la GRC. L'arrestation du groupe des 18 de Toronto, inspiré par Al-Qaida, c'est un peu lui. Il jure que cet épisode policier est derrière, qu'il se concentre sur son doctorat en psychologie en Angleterre. Son sujet : comment contrer et prévenir l'extrémisme. La Presse

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Fort McMurray first responders recognized for battling 'The Beast'
Darby Allen still thinks about the wildfire that swept through Fort McMurray. The Wood Buffalo fire chief has good days and bad; the evacuation of 80,000 people from the city still plays on his mind, the thought of, "Could we have done more?" Monday was one of the good days, as he and his fellow first responders were recognized at the Alberta legislature for their work during the disaster. (…) In addition, companies without a firefighting plan or a lack of firefighting equipment on-site could also face a fine of $10,000 per offence. There will also be an increased focus on handing out tickets for careless use of campfires. Peace officers, forestry, fish and wildlife and conservation officers and RCMP officers will be able to hand out tickets from $150 to $1,000. Roughly 70 per cent of wildfires in the last five years were caused by people and RCMP have said they believe the Fort McMurray fire was caused by human activity. Edmonton Sun

Reticle range operating in 'soft opening' mode
Construction on a firing range north of Brockville is well under way, and the "world-class" training facility will be ready for a Spring 2017 opening, officials said Friday. Ottawa-based Reticle Ventures Canada Inc. is in the midst of building an instructional facility, unique in Canada, at the Brockville-1000 Islands Regional Tackaberry Airport in order to support first responders, law enforcement and select national security agencies and is in a "soft-opening phase right now." said the company's lawyer Bryce Geoffrey.

"We've built our 50-metre range," Geoffrey said, adding the Ontario Provincial Police, Royal Canadian Mounted Police and other law enforcement agencies have already been practicing on the firing ranges since early fall. "Things are going well. It's all going to be done in the spring." The site plan for the project includes a new 6,480 square-metre (21,600 sq.ft.) airplane hanger construction, a portable office, a future training facility building, a 50-metre outdoor firing range and "an identified sound barrier." Reticle plans to have federal security agencies as its clients, including the Canada Border Services Agency and Department of National Defence, as well as conservation officers, registered security companies, the Commissionaires of Canada and other clients. Reticle officials have said the aim is to run "a public safety and national security training facility." Brockville Recorder (2016-10-31)

RCMP not to blame for death of suspect who shot Golden Mountie: Police watchdog
The suspect who led police on a manhunt after shooting a Mountie near Golden died from head trauma and RCMP action or inaction was not to blame, B.C.'s police watchdog says. The provincial Independent Investigations Office launched a probe to determine whether there was any connection between the officers' actions and the death of Sheldon Kyle Thunderblanket, 40. Investigators concluded "there is no causal connection between death of the male affected person and actions or inactions of police," according to a Independent Investigations Office media release. Info News (2016-10-31)

RCMP vehicle involved in serious crash
An RCMP vehicle was involved in a serious crash Monday afternoon at one of the city's most notorious intersections. Emergency crews were called to the corner of Kenaston and McGillivray Boulevard for what appeared to be a two-vehicle crash. A light standard was seen sitting atop the police cruiser in the southbound lane of Kenaston. Front and side airbags were deployed. A van ended up in the westbound lane of McGillivray. No word yet on injuries. The intersection was highlighted eariler this year as having the second highest number of collisions in the city with 2,298 crashes between 2005 and 2014. Winnipeg Free Press; CTV News; CBC News (2016-10-31)

RCMP mourns one of its own
Insp. Tony Perry was found dead Friday morning in Happy-Valley-Goose Bay. Perry, who is originally from Deer Lake, joined the RCMP in 1988 and served in Nova Scotia until July 2015, when he was transferred to Newfoundland and Labrador. Most recently, Perry worked as a negotiator between police, aboriginal leaders and protesters at the Muskrat Falls hydroelectric project site. Foul play is not suspected. Western Star (2016-10-31)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

Nil

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Liberté de presse et protection des sources journalistiques - Les élus doivent passer aux actes
Un article d'opinion state, « Nous, dirigeants des principales salles de rédaction de Montréal, tenons à exprimer notre indignation et notre inquiétude face à l'espionnage électronique du journaliste Patrick Lagacé par la police de Montréal. Il est inacceptable que des enquêteurs aient pu obtenir accès aux données téléphoniques et à la géolocalisation d'un journaliste sans autre motif que d'identifier des sources journalistiques à l'intérieur du corps de police. Ce n'est pas le seul cas d'intrusion injustifiée des autorités policières dans le travail des journalistes. En juin, le premier ministre Justin Trudeau avait qualifié d"' inacceptable '' la filature par la GRC des journalistes Joël-Denis Bellavance et Gilles Toupin, de La Presse. Puis en septembre, l'Assemblée nationale a adopté à l'unanimité une motion pour '' rappeler l'importance du principe de protection des sources journalistiques '' après que la Sûreté du Québec eut perquisitionné l'ordinateur du journaliste Michaël Nguyen, du Journal de Montréal. Dans les trois cas, les élus ont soit dénoncé l'intervention policière, soit s'en sont dits fortement préoccupés. Des actions concrètes sont nécessaires pour protéger les sources journalistiques formellement. C'est essentiel pour la liberté de la presse, un droit fondamental consacré par la Charte canadienne des droits

et libertés et reconnu par la Cour suprême du Canada. La procédure pour obtenir un mandat de surveillance contre un journaliste doit être plus contraignante pour les corps policiers ». Le Devoir, A9

A bad precedent
An editorial states, "''Are you a journalist?'' tweeted American whistleblower Edward Snowden on Monday. ''The police spying on you specifically to ID your sources isn't a hypothetical,'' he warned. ''This is today.'' Snowden was referring to the case of Patrick Lagacé, a columnist at Montreal's La Presse newspaper, who revealed that police have been spying on him for months, tracking his whereabouts using his cellphone and monitoring his calls and texts. Montreal police suspected that a target of one of their internal investigations was leaking information to Lagacé and so applied for - and, bizarrely, received - a series of warrants to monitor the columnist. The state spying on a journalist suspected of no wrongdoing, in an apparent attempt to identify his sources, is unprecedented in Canadian history and poses a troubling threat to freedom of the press." Toronto Star, A10

OTHER / AUTRES

Faire notre travail
Tout a commencé par un texto de l'éditeur adjoint de La Presse, Éric Trottier. « Faut que je te parle, jeune homme. » C'était jeudi en fin d'après-midi, je venais de finir une répétition pour l'enregistrement de Deux hommes en or, l'émission que je coanime à Télé-Québec. Je rappelle donc Éric. Sur le bruit de fond caractéristique des conférences téléphoniques, il m'annonce qu'il est avec Patrick Bourbeau, l'avocat de La Presse. Me Bourbeau m'explique les détails de l'affaire. Les quatre policiers arrêtés en juillet_ Mon nom qui apparaît sur le radar des enquêteurs_ Une demande faite à un juge_ Un de nos procureurs qui parle à celui de la Couronne. Et mon téléphone, espionné pour ses métadonnées pendant six mois. Pendant six mois, la police de Montréal a pu avoir accès à tous les numéros qui entraient dans mon téléphone, à tous ceux que je composais. Pour des appels ou pour des textos. Si vous m'avez appelé entre le 13 janvier et le 7 juillet, si je vous ai appelé, si nous avons échangé des textos : la police de Montréal le sait. Ce fut plus fort que moi : dans le hall du Monument-National, j'ai lâché un gros juron du terroir québécois qui commence avec un T et qui finit avec un K. En majuscules. J'étais sous le choc. Sans être expert du droit des médias, j'ai tout de suite anticipé ce qui s'est confirmé par la suite : la police qui obtient le droit d'espionner un journaliste de la sorte, c'est du jamais-vu au Canada. Ça ne s'est pas vu pour trouver les sources d'articles traitant de sécurité nationale, de l'armée canadienne, de terrorisme. Mais le SPVM, lui, a obtenu le droit inusité de m'espionner pour des affaires de crimes de droit commun qui sont, dans le grand ordre des choses, stupéfiantes de banalité. La Presse, 4

UBC researchers create new method to classify dangerous sex offenders
UBC researchers have developed a new classification system that could help police solve sex crimes. Using classified anonymous police case files and court records, researchers at UBC's Okanagan campus uncovered new subtypes of high-risk sexual offenders that could give police insight into the behaviour of convicted sex offenders who have been released into the community. ''These are offenders who have an extremely-high probability of reoffending, but they have timed-out of the system and are released,'' says Kimberly Kaseweter, a PhD student at UBC. ''A lot of people don't understand that these high-risk sexual offenders are often treated the same way as non-violent offenders, once released, in regards to community supervision and treatment.'' Kaseweter, and UBC Okanagan psychology Professor Michael Woodworth, worked with former RCMP Staff Sergeant and psychologist Matt Logan, who helped facilitate access to the classified case files. Using details from the crime scenes, Kaseweter and Woodworth used a statistical technique called Latent Class analyses to uncover three distinct groups of these offenders--coercive child molesters, sadistic rapists, and stranger-focused offenders. Kaseweter says they used details of the crime scene and statistical models to reveal profiles that police can use to help identify the type the offender they are looking for. Then by using additional variables, such as use of weapon, violence, and sadism, police can narrow the search for probable suspects. EurekAlert! (2016-10-31)

Law enforcement agencies around the world collaborate on international Darknet marketplace enforcement operation

A globally coordinated law enforcement action against the buyers and sellers of illicit drugs and other illegal activities using Darknet global marketplaces was conducted Oct. 22 to 28. "Operation Hyperion" was initiated by U.S. federal law enforcement, the Five Eyes Law Enforcement Group (Australia, Canada, New Zealand, the United Kingdom and the United States) and members of Europol, the European Union's law enforcement agency, as the first step in developing a more unified global law enforcement response to the growing usage of the Darknet by individuals seeking to buy and sell illicit drugs and other illegal goods and services... Operation Hyperion resulted in a number of law enforcement leads on cases related to the buying and selling of illicit drugs and other goods on the Darknet. This operation will also help law enforcement agencies continue to combat the trafficking of illicit goods and services on the Darknet through the identification of new smuggling networks and trends... International partners included Europol the United Kingdom's National Crime Agency; Australian Federal Police; New Zealand Police and New Zealand Customs Service; Canada's Royal Canadian Mounted Police, Canada Post and Canada Border Services Agency; The Netherlands; French Customs National Intelligence and Investigations Directorate; Finnish Customs; Swedish Police Authority and Swedish Customs; Ireland's Garda National Drugs & Organised Crime Bureau; and Spain's Guardia Civil. U.S. Immigration and Customs Enforcement (2016-10-31)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 4, 2016 / le 4 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Justin Trudeau says police surveillance of journalists 'troubling' in free democracy
Prime Minister Justin Trudeau called reports about surveillance of journalists in Quebec "troubling" Thursday and said he has received assurances from the RCMP and CSIS that no actions are taking place on their part that infringe the rights of reporters... Public Safety Minister Ralph Goodale said while he does not normally comment on any operations, he confirmed the activities being reported in Quebec are *"not applicable"* at the federal level. CBC News (2016-11-03)

UPDATE: Quebec to hold public inquiry into police surveillance of journalists
As Quebec announced plans Thursday to hold an inquiry into freedom of the press and police surveillance of journalists, Prime Minister Justin Trudeau said spying on reporters is not happening at the federal level. The Quebec government said a public inquiry will be held against the backdrop of revelations that various forces monitored reporters' phones. A panel of experts announced earlier this week will now have all the powers typically granted to a commission of inquiry, including being able to compel witnesses to testify, said Justice Minister Stephanie Vallee... Meanwhile, the controversy reverberated in Ottawa, where Trudeau said surveillance of journalists was not taking place. Trudeau told reporters he immediately contacted RCMP and CSIS leadership after news broke about the Quebec surveillance... In an interview on Montreal radio station 98.5FM, provincial police director Martin Prud'homme said he's asked lawyers to unseal the warrants to provide details about them... Vallee and Public Security Minister Martin Coiteux said the admission by provincial police played a part in the decision to expand the mandate. "Until yesterday (Wednesday), the epicentre, as far as I could tell, was primarily the SPVM (Montreal police)," Coiteux said. "But yesterday, we learned that the Surete du Quebec (provincial police) had also conducted such investigations involving journalists." Canadian Press

(Globe and Mail, CTV News); La Presse ; Agence QMI (Canoe) ; Presse Canadienne (Journal Métro) (2016-11-03)

Leader says feds are not tracking journalists' phones
Prime Minister Justin Trudeau said today that reporters' mobile phones are not being tracked at the federal level. He said he received assurances to that effect from the heads of the national police force, the RCMP, and the domestic spy agency, CSIS...The leader of the opposition New Democratic Party, Tom Mulcair said in the House of Commons that he had raised the issue of police spying on reporters earlier this year and he asked the public safety minister whether he would hold a public inquiry at the federal level. The minister said no, but it was unclear whether that was no, there would not be an inquiry or no, spying was not going on at the federal level. RCI (2016-11-03)

Espionnage de journalistes: Trudeau ouvert à revoir le Code criminel
Le gouvernement fédéral doit s'interroger sur ce qu'il peut faire pour mieux protéger les sources journalistiques, affirme le premier ministre canadien Justin Trudeau, dans la foulée des nouvelles révélations d'espionnage de journalistes de la part de la Sûreté du Québec (SQ). M. Trudeau affirme cependant que les Canadiens peuvent être rassurés quant aux pratiques en vigueur à la Gendarmerie royale du Canada (GRC) et au Service canadien du renseignement de sécurité (SCRS). En conférence de presse jeudi midi, M. Trudeau a été interrogé sur la possibilité que son gouvernement revoit l'article 193 du Code criminel, évoqué par la SQ mercredi pour justifier l'espionnage des communications de six journalistes québécois en 2013. « Je sais que dans un monde où il y a quand même des dangers, nous nous devons d'être responsables dans notre fonctionnement », a-t-il ajouté. « Mais c'est fondamental à nos valeurs, à notre identité, en tant que pays libre et juste, que les journalistes puissent faire leur travail d'informer les Canadiens et donc de protéger leurs sources confidentielles. » M. Trudeau a par ailleurs révélé qu'il avait communiqué avec le commissaire de la GRC et les responsables du SCRS dans la foulée de cette affaire pour s'assurer qu'« aucune activité de ce type [ne] se passe au niveau fédéral ». Radio-Canada ; La Presse ; CBC News; Vice News; Toronto Star; National Post; Times Colonist; Canoe (2016-11-03)

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

Former Mountie on trial in Moncton for impaired driving
Arresting officer says Ronald Cleveland suggested he 'pretend that you never found me'. Former RCMP sergeant Ronald Cleveland is on trial in **Moncton** on a charge of impaired driving dating back to an incident in the early hours of March 21, 2014. Cleveland was released from the RCMP on a medical discharge earlier this year. Testifying Thursday, Const. Joel Arsenault described how uncomfortable he was arresting a superior officer. "Up until June 4, that was the worst day of my career," Arsenault said, referring to the day a few months later when three Codiac RCMP officers would be shot and killed by a lone gunman. Arsenault testified the RCMP had received a call about a possible drunk driver. The caller gave a license plate number that was traced back to Cleveland. Arsenault said he recognized his fellow RCMP member's name. CBC News

Halloween snatch and grab in Kelowna
A cashier in **Kelowna** was the victim of a snatch and grab on Halloween night. Shortly before 10 p.m., Monday, Oct. 31 a man entered the Esso in the 2300 block of Highway 97 North and asked for a pack of cigarettes, according to a Central Okanagan Crime Stoppers media release. "When the clerk turned to get them, the man reached under the lottery ticket glass and grabbed a tray of $3 lottery tickets," it says. Roughly 55 tickets including Crossword, Bingo, Lucky Lines, Holiday Homes and Solitaire were stolen. The suspect is between 30 and 35 years of age with a short beard and wearing beige pants. He also had on a grey hoodie with orange writing on the front. Infotel

Police seek details on suspect: RCMP-led homicide unit releases photo of 21-year-old man in hopes of gaining information from public

Homicide investigators are still trying to piece together the past of a young man who they believe drifted between Alberta and British Columbia before allegedly stabbing an **Abbotsford** high-school student to death in a random attack that has shocked the conservative suburb. On Thursday morning, the Lower Mainland's RCMP-led homicide unit released a photo of the 21-year-old suspect, which was captured by the security camera of a local Abbotsford business and shows the suspect just hours before he is alleged to have entered Abbotsford Senior Secondary School barefoot on Tuesday afternoon and stabbed two female students. In the photo, the slim young man wears running shoes, blue jeans, a camouflage hoodie and a backpack. Police are hoping the photo prompts more information from the public about the suspect, about whom they say they know very little. Spokeswoman StaffSergeant Jennifer Pound said the young man, who is in jail facing second-degree murder and aggravated assault charges, had no apparent connection to the community, the school or the two girls he is accused of stabbing. Globe and Mail

New Brunswick RCMP's first e-joints seizure earns man 2 years in prison
An **Ottawa** man was sent to prison on Thursday after being caught trafficking marijuana and e-joints in southeastern New Brunswick. Stephane J. André Fournier, 40, pleaded guilty in Moncton provincial court in late January to possessing marijuana, hydromorphone and cannabis resin. The prosecutor withdrew three counts of trafficking those substances. Judge Alfred Brien followed a joint recommendation on Thursday for two years in prison. Prosecutor Patrice Deschenes told the court that a Mountie pulled over a vehicle on the Trans-Canada Highway in River Glade on Oct. 7, 2015. Upon approaching the vehicle, the officer smelled fresh cannabis and further investigation resulted in the seizure of three briefcases containing 12 kilograms of marijuana, several e-joints or electronic marijuana vapour cigarettes that contained cannabis resin, along with some hydromorphone pills. He admitted to police he was transporting the illegal substances from Ottawa to Nova Scotia for re-sale. The defence told the court the offender committed the crimes out of economic necessity. "Clearly this was a bad decision on your part," said Brien. New Brunswick RCMP said after the arrest that it was their first seizure of e-joints in this province. Times & Transcript

Man killed in tanker explosion near Red Deer, Alberta
A 35-year-old man was killed by an explosion while working in an industrial park on the northwest edge of **Red Deer** Thursday afternoon. Blackfalds RCMP said it happened at around 1:40 p.m. at the Burnt Lake Industrial Park at J Moore Enterprises. A single tanker exploded, RCMP said, destroying the tanker and killing the man. Global News; 660 News; CTV News (2016-11-03)

200 fentanyl pills seized in Saskatoon drug bust
Police said they have seized fentanyl pills and charged three people following a drug bust in **Saskatoon**. The bust happened after members of the Saskatoon integrated drug enforcement team spotted what they believed to be a drug transaction in the area of Taylor Street and St. George Avenue on Wednesday afternoon. Police arrested two men and said they seized 100 fentanyl pills and over $1,500 in cash. A home in the 100-block of Girgulis Crescent was then searched, where police said they seized an additional 100 fentanyl pills. Two men, 20 and 22, are facing charges of possession for the purpose of trafficking. The 22-year-old man is also facing charges of trafficking fentanyl and possession of the proceeds of crime. An 18-year-old woman is also charged with possession for the purpose of trafficking. Global News (2016-11-03)

RCMP release photo of homeless man charged in high school murder
Homicide investigators have released a photo of the 21-year-old man charged in the stabbing death of an **Abbotsford** high school student in hopes the public will come forward with information. Staff Sgt. Jennifer Pound says the photo of Gabriel Klein was captured on closed-circuit surveillance just hours before a deadly attack at Abbotsford Senior Secondary. Thirteen-year-old Letisha Reimer was killed after being attacked by a barefoot intruder in the school's atrium. Her 14-year-old friend, who cannot be named because of a publication ban, was seriously injured and remains in hospital. CTV News (2016-11-03)

Edmonton judge stays sex charge over unexplained loss of evidence by RCMP
An **Edmonton** judge has tossed out a sexual assault charge against an Edson-area man as a result of the “unexplained” loss by the RCMP of an audio-recorded statement from the alleged victim. In a ruling released this week, Court of Queen’s Bench Justice Denny Thomas issued a judicial stay of the 2015

sexual assault charge against the 21-year-old accused man. "Balancing the societal interest of having a full trial on the merits of this charge before a jury and the right of the accused to make full answer and defence, I conclude that this is one of those 'clearest of cases' where a stay should be granted to respect the rights of the accused," said Thomas in his written decision, The man had sought a stay of the charge, arguing the "unexplained" loss of key evidence by the Mounties was so prejudicial to his right to make full answer and defence that he would not get a fair trial. The Crown had conceded that the loss of the complainant's audio statement meant the prosecution had not met their disclosure obligation and it was therefore a breach of the accused's Charter rights, but had argued there was other evidence available to the defence which would have mitigated the prejudice to him. Edmonton Journal (2016-11-03)

Alberta vehicle theft suspect arrested after leading police on low-speed skid steer chase
Police have arrested a suspect in connection with a string of thefts of trucks, trailers and construction equipment east of **Edmonton**. The arrest came after a man driving a construction vehicle led Vegreville RCMP on a low-speed chase. It all began last Saturday around 4:45 p.m., when Mounties got a call about a suspicious man who had just parked a truck and trailer in a field southwest of Mundare. Police did a check and discovered the truck and trailer had been stolen from a business in the Nisku industrial park south of Edmonton. The person who called police then said the man who had dropped off the truck was leaving the scene in a John Deere skid steer, which was later determined also to have been stolen. RCMP found a man driving the skid steer on Range Road 17-0 and attempted to arrest him. The man fled in the equipment which, according to John Deere's website, has a maximum travel speed of about 20 kilometres per hour. Police said at one point during the low-speed pursuit, the driver attempted to ram a police vehicle. Global News (2016-11-03)

Ten drug dealers in dial-a-dope network allegedly operated by Mohamed Abdi Yusuf caught in Brooks, Alberta bust
Seven suspected drug dealers have been arrested and warrants have been issued for three others as ALERT (Alberta Law Enforcement Response Teams) shut down a drug trafficking network operating in Brooks, Alberta. ALERT's Medicine Hat organized crime team conducted the investigation in response to community concerns related to cocaine trafficking. ALERT worked hand-in-hand with RCMP Brooks and **Medicine Hat** Police Service on the three-month investigation. ALERT alleges that the group was operating as a dial-a-dope network with Mohamed Abdi Yusuf, 40, as the suspected ringleader. The group played a significant role in cocaine trafficking within Brooks and the project implicated the suppliers and street-level dealers. A total of 10 men are facing 20 drug-related charges. "This dial-a-dope group presented a challenge for uniformed members to investigate. However, by virtue of the partnership with ALERT and their specialized skill sets and resources, we were able to deliver a coordinated response and provide a safer community," said Sgt. Raimo Loo, RCMP Brooks. Indo-Canadian Voice

Needles found in chocolate bars
Sewing needles were found in two large-sized chocolate bars collected by **Cochrane** youth while trick-or-treating, Oct. 31. Cochrane RCMP are investigating the incident and in the meantime are asking people to step forward if they have been the victim of the tampering of candy during the annual Halloween costume dash for candy. According to the Cochrane RCMP, the complainant had been checking their children's Halloween candy and found a sewing needle in a large O'Henry bar and another sewing needle in a large Kit Kat bar. They had been trick-or-treating on the west side of Gleneagles. The exact location of where the bars were received is still under investigation and if there are any other incidents with tampered candy the RCMP are strongly encouraging it to be reported to help narrow down where this could have taken place at. Cochrane Times (2016-11-03)

Search for missing Codroy Valley hunting guide into 2nd day
A ground search will continue Thursday for a 49-year-old man who became separated from his hunting group Tuesday afternoon on **Newfoundland's** west coast. RCMP said a helicopter search continued until midnight Wednesday, and will be back in the air Thursday, weather permitting. Barachois Ground Search and Rescue, a Joint Rescue Co-ordination Centre helicopter and RCMP assisted in the search, which began shortly after the man was reported missing at 1 p.m. Wednesday. CBC News (2016-11-03)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Thunder Bay cops face probe for all missing persons cases

Review broadened to focus on interaction with indigenous community. All indigenous missing persons and death investigations will be under the microscope of the Ontario police watchdog as it expands its "systemic review" of the Thunder Bay Police Services, looking for discriminatory conduct. The sweeping review, to be conducted by the Office of the Independent Police Review Director, was formally unveiled on Wednesday and begins immediately. The issue of police racism toward indigenous people has galvanized the country in wake of greater exposure to the issue of murdered and missing indigenous women and girls. Many indigenous families have not been satisfied with how police authorities handled their initial complaints about their loved ones, and how they followed up on them. Those concerns spill over into all aspects of the justice system and in cases of other indigenous death investigations. The incarceration of Adam Capay in segregation in a Thunder Bay cell for four years, without a trial, is a stark reminder of human rights inequalities. The systemic review will focus on the interaction between the police and indigenous people in Thunder Bay; if indigenous people have been "over-policed" or "under-policed," and if investigations have been carried out in a discriminatory manner, said Gerry McNeilly, the Independent Police Review director. Toronto Star; CBC News

Chief urges communities to live violence free

While the national inquiry into missing and murdered Indigenous women inches forward, leaders from the Esk'etemc First Nation are not waiting to make positive changes in their community and others.
"We choose to be proactive," Esk'etemc Chief Charlene Belleau told attendees at the recent First Nations Health Council caucus, held in Williams Lake last week. Despite the inquiry being called, Belleau said she feels like nothing has changed in the way missing and murdered Indigenous women cases are treated and feels communities themselves must choose to live violence-free. "Somehow it's our responsibility to do something about it." So far, that desire for change has translated into physically assisting in the search for missing woman and girls such as helping the Splatsin First Nation at Enderby search for Caitlin Potts June 7. Potts, originally from Alberta, was reported missing March 1. William Lake Tribune (2016-11-03)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

LGBTQ Canadians Sue Government for Decades-Long Witch Hunt

In a Canadian military interrogation room in 1990, strapped to a polygraph machine and sensing unseen observers behind a two-way mirror, 21-year-old Canadian sailor Todd Ross finally broke down in tears and said out loud what he'd been unable to say even to himself: He was gay. The military gave Ross an ultimatum: accept an honourable discharge or perform "general duties"—grunt work—for the rest of his career. (…) According to government records, the RCMP spent decades following World War II investigating, surveilling, and questioning suspected gay and lesbian public servants, including members of the military, about their sexual orientation. At one point, the RCMP amassed a list of 9,000 people deemed suspect and subject to investigation. The Canadian government would often employ a device that would measure sweat and sexual reaction to certain words, phrases, and images—dubbed internally as the 'fruit machine'—to vet suspected LGBTQ government employees. The project was created through a government grant at the Carleton University Psychology Department. Vice News (2016-11-03)

Liberal government may not compensate men convicted under anti-gay laws, FOI suggests

Government officials say Canada's looming effort to purge criminal convictions for consensual homosexual acts could cost $4.1 million and face "nightmarish" bureaucratic hurdles, Daily Xtra has learned. Nevertheless, public servants told the government they would have been able to start the process by September 2016, according to documents released under access-to-information laws, raising questions as to why the review still hasn't started. On Feb 27, 2016, Prime Minister Justin Trudeau announced he would seek a posthumous pardon for Everett Klippert, who was labelled a dangerous offender for consensual gay sex. The next day, his spokesman said the government will review all convictions of "buggery" and "gross indecency" laws prior to 1969, when they were restricted to mostly

non-consensual activity. The government has only said publicly and to bureaucrats to look into cases before 1969, but there's no mention of afterwards. In 400 pages of exchanges obtained by Daily Xtra, Parole Board of Canada employees say roughly 6,000 sentences could be reviewed, with an RCMP search showing the oldest dating back to October 1939. "A manual review of each file would be needed to determine the circumstances surrounding the convictions," according to one memorandum. However, the Parole Board said in the documents that it would be ready, "to post information on its website for September 1, 2016 to inform individuals with the specific convictions that they may apply for clemency." The documents suggest the Liberals are interested in modelling an Australian program that involves cost-free reviews of convictions for people who feel they were charged because of homophobia, but bars them from any compensation. The documents also reveal that over 300 Canadians convicted under either charge have requested pardons on their own since 2000, with a success rate of 98 percent. The government did not respond to Daily Xtra's request for comment on the documents, which date from February to July 2016. The lack of a timeline and plan of action has frustrated activists...According to the documents, Public Safety Minister Ralph Goodale was leaning toward replicating how the Australian state of Victoria is expunging records. Daily Xtra (2016-11-03)

Feds holding Twitter consultation on national security
Public Safety Canada is holding a Twitter chat Thursday night to hear what Canadians think about national security and its responsibility to Canadians. The department in charge of the RCMP, the Canadian Security Intelligence Service and its oversight body, and the Canada Border Services Agency is asking people to tweet them using the hashtag #YourNatlSec starting at 8 p.m. ET to discuss accountability in national security. The social media discussion comes the same week the House public safety committee is starting its review of bill C-22, which will amend some of the laws changed under the Conservatives' highly contentious C-51. Public Safety Minister Ralph Goodale isn't participating in the Twitter chat. New Democrat justice critic Murray Rankin says he wants as many people as possible to participate. "Any effort to get Canadians engaged is great," he said. The department is holding national security townhalls across the country until Dec. 15. It's also is accepting input on its website too. CTV News (2016-11-03)

Feds forbid construction of new embassies on Sussex Drive
The federal government is forbidding the construction of new embassies on Ottawa's Sussex Drive following a stark RCMP assessment of the potential for "violent events" in the high-profile neighbourhood. Countries with diplomatic missions already located on the well-known boulevard include the United States, France, Kuwait, Saudi Arabia and South Africa. It is also home to Rideau Hall, where the Governor General lives, as well as the prime minister's residence at 24 Sussex. Justin Trudeau and his family are living in a house on the Rideau Hall grounds while federal officials consider badly needed renovations to the traditional address of Canada's leader. Foreign Affairs Minister Stephane Dion was advised of the ban on new embassies in January by Daniel Jean, then his deputy minister, records released under the Access to Information Act show. Jean has since been named national security adviser to the prime minister. "A recently concluded RCMP security assessment advises against any additional foreign embassies being located along Sussex Drive," says Jean's memo to Dion, obtained by The Canadian Press. "As a result, the department will no longer be approving requests by diplomatic missions to acquire land in the affected zone." Canadian Press (Daily Commercial News) (2016-11-03)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

$100M radio network for first responders goes live
With the flip of a lever on a silver control box, a $100-million, state-of-the-art digital radio network for New Brunswick's first-responders went live on Thursday. It's called the New Brunswick trunk mobile radio project and it will allow 3,400 police, firefighters, paramedics, forest rangers, school bus drivers, and snowplow operators now - and up to 8,000 in the future - to communicate clearly, quickly, and easily. It replaces a 30-year-old system that lacked coverage in some parts of the province and didn't allow different agencies to talk to each other. (...)Larry Tremblay, RCMP assistant commissioner for J Division, said the new radio system will make communications between agencies smoother, more reliable and give wider coverage. "I can say this new system will enhance the safety of our police officers when they are

out on call, as well as the safety of other first-responders assisting them," he said. "Every call we answer carries risks for all involved and this new system will help reduce that risk by ensuring better communication." New Brunswick Fire Chiefs Association president Dan McCoy said information is one of the most important requirements when responding to a call. Daily Gleaner

Nanaimo sheriff rushed to hospital after exposure to fentanyl
The potentially lethal drug has become so rampant and led to so many fatal overdoses that the province has declared a health emergency and this incident reminds front line workers of the risk they run everyday. In the war on Fentanyl, Const. Justin Ickringill has gotten closer than any officer wants to be to the potentially lethal drug. "I was immediately light headed and dizzy," says the Nanaimo RCMP officer. "I had a racing heart and it caught me by surprise. (…)Monday a Nanaimo deputy sheriff became the latest front line worker to experience an accidental exposure to it. When conducting a gloved search of a prisoner at the RCMP detachment before transport to court she was exposed to the crystal-like substance in the pocket of a jacket being searched, and quickly became ill. "She was taken to the hospital in Nanaimo and the doctor determined that it was in fact Fentanyl that she was exposed to," says Dean Purdy of BCGEU's Corrections & Sheriff's Unit. "So from our standpoint it's a big concern for us because we would like to see some interim measures put into place so that we can try and prevent this." RCMP say fentanyl has now made its way into everything from marijuana, to cocaine and heroin. Chek News

Des francophones de la GRC intentent une action collective
Des francophones de la Gendarmerie royale du Canada veulent intenter une action collective contre leur employeur en raison de la discrimination et du harcèlement qu'ils disent subir à cause de leur langue. «Les opportunités d'avancement sont de beaucoup diminuées pour des policiers francophones, alors que dans l'autre sens, un unilingue anglophone peut accéder à un haut grade», s'insurge Paul Dupuis, un retraité de la police fédérale, à l'origine de ce recours. Cet ancien sergent d'état-major, qui a aussi été président de l'Association des membres de la police montée du Québec (AMPMQ), n'est pas tendre envers son ex-employeur. Dans la demande déposée au palais de justice de Montréal, il affirme avoir été victime «d'une campagne de harcèlement systématique» à cause de son militantisme pour ses droits linguistiques et de ses revendications pour créer un syndicat au sein de la police fédérale. «Après une campagne de harcèlement prolongée [...] M. Dupuis s'est senti de prendre sa retraite en 2016», peut-on lire dans le document de cour. Journal De Montreal; La Presse

Amnesty International calls for more police in Fort St. John, northeast B.C.
Resource development contributes to crime, putting Indigenous women and girls most at risk, Amnesty says. A new report from Amnesty International says police in northeast B.C. are not equipped to deal with the high rates of crime in the region, particularly when it comes to violence against Indigenous women and girls. The report also calls on RCMP to increase Indigenous cultural knowledge for its officers, and renews Amnesty's demand for the Site C dam project to be stopped. The report titled Out of Sight, Out of Mind provides an overview of the ways in which resource development in B.C.'s Peace River region — including fracking, coal mining and hydroelectric dams — affect vulnerable populations. "There is a downside to the scale of resource development in the northeast and the people who live there," said Craig Benjamin, who helped prepare the report for Amnesty. "Particularly, Indigenous women and girls are bearing a very heavy burden for hosting these products in their region." CBC News (2016-11-03)

Province, federal government in talks over RCMP staffing levels in Sask.
Conversations are ongoing between the two levels of government on the issue of RCMP staffing in Saskatchewan. In September it was reported that our province was under served by as much as 25 per cent. 980 CJME (2016-11-03)

RCMP nets handguns and rifles in amnesty
Gun owners responded to a what RCMP called a gun amnesty by turning in more than two dozen firearms to the local detachment. Kamloops RCMP wrapped up the program earlier this week. Cpl. Jodi Shelkie said five handguns were turned in, along with 27 rifles and shotguns, five pellet guns and five boxes of ammunition. Kamloops This Week; Merritt Herald (2016-11-03)

P.E.I. variety show to salute military, RCMP past and present

Military and RCMP members past and present will be feted with a special fundraiser variety show held at Holland College in Charlottetown next Wednesday. A crew of 60 people, including 40 performers, are putting together Salute!, which will raise money for the P.E.I. Military Family Resource Centre (MFRC). CBC News (2016-11-03)

Tax rate in Chilliwack jumping 3.5% to fund more RCMP
The public has been screaming for more police in Chilliwack to deal with rampant property crime. City council is taking a major leap forward in this direction hiring 10 new RCMP officers for 2017, as well as two RCMP information officers. Chilliwack Progress (2016-11-03)

Former Mountie on trial in Moncton for impaired driving
Former RCMP sergeant Ronald Cleveland is on trial in Moncton on a charge of impaired driving dating back to an incident in the early hours of March 21, 2014. Cleveland was released from the RCMP on a medical discharge earlier this year. CBC News (2016-11-03)

Regina and Saskatoon getting more police officers
Funding for targeted police initiatives rolled into Saskatoon and Regina on Thursday. The province is giving $4.6 million to Regina for 39 new police officers and $4.8 million for 42 police officers in Saskatoon. Leader-Post (2016-11-03)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

Nepean pot shop case highlights hazy enforcement rules for police
A knife point robbery didn't do it. Neither did a truck crashing through the store's front window. Nothing seemed to be able to shut down CannaGreen, a marijuana dispensary in a Nepean strip mall this summer, until the owner of the building slapped an eviction notice on the front of the store. But even then the bailiff hired to enforce the order said the owner of the pot shop got back into the store and kept selling. And that's when Ottawa police came on Wednesday to help the bailiff enforce the eviction and arrested a man for trespassing. Ottawa police have said they are hesitant to enforce trafficking charges against dispensaries, given the fact that they could be thrown out of court once federal legislation comes into effect. But the CannaGreen situation may provide the blueprint for how neighbourhoods and police deal with the proliferation of unregulated pot dispensaries that have popped up in the capital after the federal government signaled its intent to legalize marijuana: where the criminal laws are murky, municipal bylaws and provincial regulations can be used to shut stores down. CBC News

Calgary to ask Ottawa for a slice of pot pie
When marijuana legalization hits Canada in spring 2017, Calgary hopes it gets a cut of the new tax revenue that's sure to follow. On Thursday, a council committee approved official positions that the city will present to Ottawa as the federal government begins making decisions about how pot legislation should be crafted. Those policy positions include making sure the city has control over licensing, that people are allowed to grow a limited amount of cannabis at home, and that Calgary get a slice not just of any marijuana tax, but of all sin taxes. CBC News (2016-11-03)

Legal pot could boost economy
An editorial piece states, “It’s possible, even likely, that at some point next year, Ontarians will be able to search store shelves for ‘purple haze’, ‘blue dream’ and ‘kosher kush’ marijuana alongside their VQA merlots, sauvignon blancs and moscatos. Work is well underway to lay the foundation for marijuana legalization in this country, with legislation expected in the spring. Pot advocates have long argued legalization could give our economy a lift. A new report suggests that lift could surpass anyone’s wildest prophecy. A study produced by the Deloitte firm – titled Recreational Marijuana: Insights and Opportunities – suggests a legal marijuana industry in Canada could be worth an incredible $22.6 billion – more than the sales of wine, spirits and beer combined. Deloitte’s research values the recreational retail market for weed at between $5 billion and $8.7 billion annually. Tack on between $12.7 billion and $22.6 billion for the ancillary market (growers, specialty product makers, testing labs and security) and you have

what Deloitte calls "a bold new landscape" for businesses and governments. But that's not all." Simcoe (2016-11-03)

Canada's Budget Office Estimates Cannabis Market Worth Hundreds of Millions During Flagship Year

According to Canada's Parliamentary Budget Office, sales tax revenues from legal cannabis could be between $356 million and $959 million once the drug is legalized nationwide, as is expected this spring. The figures are based on legal per gram prices between $7.48 and $9.34 with only federal and provincial sales tax applied. Parliamentary Budget Officer Jean-Denis Fréchette notes that the office expects the revenues to, eventually, climb into the billions of dollars and that the new sector will create both new revenues and expenses for the government. "Different products, such as edibles and concentrates, may require entirely different approaches to taxation," the report states. "These variations, along with others, each have different implications for market incentives and fiscal revenues." The PBO projects that in 2018 — the likely first year of legal sales — Canadians will consume between 378 and 1,017 metric tons of cannabis and that the legal market will be largely driven by individuals who consume the drug daily or weekly. The office suggests that between 3.4 million and 6 million Canadians will consume cannabis at least once after it is legalized nationally. Ganjapreneur (2016-11-02)

Medical marijuana group one step closer to business

As Canadians reacted to news that Shoppers Drug Mart is exploring the possibility of selling medical marijuana in the near future, an independent retailer is finalizing the last steps in opening a medical marijuana dispencery within the Camrose area. Grant Gillott, the chief executive officer of htKa group — the acronym stands for honour, truth, knowledge and action — made a presentation to the Rotary Club of Camrose Oct. 17, discussing what the plans are heading forward. htKa have purchased a 66 acre lot outside the city limits, which Gillott said will leave lots of room for expansion as the market allows. "We see that as something that's almost inevitable," said Gillott. "We didn't want to get into a small site with a single building and try to do expansion and then have to go back through the application process." To reach the stage of owning land, htKa had to become certified with Health Canada in a five step process. The third step was to go through security clearance, that Gillott said took 22 months before they reached an 11 month review process, that they are currently finishing up. Now Gillott is ready to move forward, break ground and be licensed, and he hopes to be ready to go within the next 18 months. While many Canadians are still skeptical about the legalization of medical marijuana, Gillott said there are bussiness opportunities as as legal companies start moving forward. Camrose Canadian (2016-11-03)

Calgary wants seat at table when marijuana is legalized in Canada

The City of Calgary wants to make sure it has a seat at the table when marijuana is eventually legalized in Canada. The Trudeau government plans to introduce legislation in the spring of 2017. AM 640 (2016-11-03)

City mum on pot shop plans as council inquires about restrictions

Riley McGee is clearing the air: Marijuana for Truama isn't a one-stop pot shop or a dispensary. On Wednesday, city councillors asked if new pot dispensaries should be restricted like liquor stores, which would mean they wouldn't be able to locate near schools... He said Marijuana for Trauma won't get into the dispensary business when it becomes legal, noting the company went through a rezoning process to open at its current location. Metro News (2016-11-03)

Letter: Marijuana legalization could go up in smoke

A letter to the editor states, "To all you fellow human beings out there who may happen to read this — I do hope you will do what's right and speak out about the unfairness pertaining to this subject..." Penticton Western News (2016-11-03)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Muslim Toronto Police chaplain's views troubling

An opinion piece states, "He says Muslim women should obey their husbands. He even suggests a wife should make herself available and "not withhold this right from her husband without a valid excuse." Further to his dictates on wives' sexual obligations to their husbands, he argues that some scholars agree that if a woman "refuses without a valid reason, then she has committed a major sin." He even insists that women must seek permission from their husbands whenever they want to leave the house because the man is the "main decision-maker of the home." These are not edicts issued by Wahhabi clerics in Saudi Arabia, or by jihadis from ISIS or al-Qaida. The source is right here in Canada. Musleh Khan is the new Muslim chaplain hired by the Toronto Police to bridge gaps between law enforcement and the Muslim community and to provide religious and moral support to Muslim officers. The police union is justifiably concerned about his comments, made in a 2013 webinar entitled "The Heart of the Home: The Rights and Responsibilities of a Wife." Of course, people offended by these comments understand the importance of a relationship that requires both parties to respect each other's wishes. They are enlightened enough to see that Khan's comments promote a kind of sexual tyranny..." Postmedia Network (Toronto Sun, Edmonton Sun, Winnipeg Sun) (2016-11-03)

RCMP treatment of senior couple brutality
A letter to the editor states, "Just viewed the video again and brutality is the only way to describe dragging an old man down stairs by his feet. As for the treatment of the woman, it was stupidity. Neither of these are characteristics that should be tolerated in Canada's "finest". For comparison, look at video of the Kinder Morgan or Carmanah protests and what do you see? Protesters being "carried" by at least two officers — not dragged by their heels. This situation is an astounding revelation and, when tied to the recent sexual harassment/assault issues the RCMP have experienced, suggests that some authority, much higher than tiny New West's police force, should be conducting a pervasive review of the RCMP." Cowichan Valley (2016-11-03)

Commission d'enquête sur la surveillance des journalistes: à quoi s'attendre?
Un article d'opinion déclare « La mise en place de la commission devrait permettre de connaître l'étendue du problème et les manières d'y remédier... Le fait qu'un ministre de la Sécurité publique puisse, comme ce fut le cas en 2013 pour Stéphane Bergeron, appeler directement le grand patron de la SQ Mario Laprise pour s'enquérir d'une possible enquête -- même s'il ne savait pas que l'investigation toucherait ensuite des journalistes -- est troublant... » L'actualité (2016-11-03)

Here's what investigative journalists actually do
An editorial states, "On Thursday, Quebec announced a full public inquiry into freedom of the press and police surveillance of journalists, against the backdrop of revelations that various provincial police forces had extensively monitored reporters' phones - one of them for five years. Several of the reporters whom Quebec police spied on in recent years specialize in what's referred to as "investigative journalism." Here are some examples where digging by reporters has made a difference: Alleged police abuse: Last fall, Radio-Canada's Enquête investigative show aired a report alleging Sûreté du Québec officers in Val-d'Or subjected indigenous women to violence and other cruel behaviour and paid for sexual favours with money and cocaine. In the wake of the report, eight SQ officers were put on administrative leave and Quebec named a civilian observer to oversee the Montreal police investigation of the alleged abuse..." Ottawa Citizen (2016-11-03)

Police surveillance scandal
An opinion piece states, "Investigative journalism that made a difference. Several of the reporters who Quebec police forces spied on in recent years specialize in investigative journalism. Here are five cases where digging by reporters has made a difference. Alleged police abuse: Last fall, Radio-Canada's Enquête investigative show aired a report alleging Sûreté du Québec officers in Val-d'Or subjected indigenous women to violence and other cruel behaviour and paid for sexual favours with money and cocaine. In the wake of the report, eight SQ officers were put on administrative leave and Quebec named a civilian observer to oversee the Montreal police investigation of the alleged abuse..." Montreal Gazette (2016-11-03)

OTHER / AUTRES

Auditor General flags 'unacceptable' Phoenix pay glitches, PS pension costs
Auditor General Michael Ferguson turned the spotlight on the pay problems of Canada's public servants and the risks of the growing liabilities of their pension plans with the present low interest rates in his latest audit observations on the federal government's books. Ferguson, who audits the government's financial statements, gave the 2016 Public Accounts a clean audit, but he flagged the delays and errors of the Phoenix pay system as "unacceptable" and praised the government for re-examining the assumptions in determining pension liabilities in the face of prolonged low interest rates. Ferguson uses these notes or observations in his audit opinion to highlight issues for MPs to watch. Ferguson, along with senior bureaucrats from Treasury Board and Finance appear at the Commons public accounts committee Thursday to discuss the Public Accounts. On pensions, Ferguson's 2014 report urged the government to re-examine the design of the three defined-benefit plans for Canada's public servants, military and RCMP to ensure it can manage risks that could affect the long-term affordability and "sustainability" of the plans (…) Ferguson said he will be watching the impact of Phoenix in his upcoming audit of the 2017 financial statements. He is also undertaking a major investigation into Phoenix and the whole pay transformation project — at the request of Public Services Minister Judy Foote — to find out how the project went off the rails. It's unclear when that report will be completed. Ottawa Citizen (2016-11-03)

Court says Canada spy agency illegally kept data
A Canadian court ruled Thursday that Canada's spy agency illegally kept phone numbers and email addresses of people they were not directly investigating over a 10-year period and wasn't forthright with judges who authorized the intelligence gathering. Federal Court Justice Simon Noel said the Canadian Security Intelligence Service should not have kept the information since it was not directly related to threats to Canada's security. The data involves the phone numbers, email address or IP addresses of family members or friends of those the spy agency investigates. The spy agency called it "associated data." CSIS said it used metadata — information associated with a communication, such as a telephone number or email address — but not the message itself. It said the program has been in place since 2006. Spy Service director Michel Coulombe said they have halted logging, storing, and analyzing the data in question and said he "deeply" regretted the judge's findings about breach of "duty of candor." Coulombe stressed all data collection was done under warrant. He noted the issue is the retention of non-threat related data. Canadian Public Safety Minster Ralph Goodale said he takes it seriously the spy agency was not forthright with the courts and said he would talk to senior executives of the spy agency. Goodale noted the laws that govern the spy agency are 30 years old and need to be updated to reflect new technologies. "Justice Noel did not dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could not find existing legislative authority permitting its retention and use," Goodale said in a statement. News of the spy agency program comes as the provincial Quebec government announced they are calling a public inquiry into police surveillance of journalists amid revelations various forces in the province monitored reporters' phones. The province's two largest police forces said earlier this week that they had monitored the phones of six prominent journalists in 2013. Associated Press (Daily Mail UK); Reuters; Canadian Press (Mississaugau.com, The Record, Times Colonist, Toronto Star); CBC News; National Post; Wall Street Journal; Globe and Mail; Agence QMI (Journal de Québec, Journal de Montréal) ; Vice News; Motherboard; Agence France-Presse (L'Orient le Jour) (2016-11-03) (2016-11-03)

Edward Snowden Calls Police Spying on Quebec Journalists a 'Threat to Democracy'
In a speech to 600 people at McGill University in Montreal on Wednesday night, Edward Snowden described police spying on Quebec journalists a "threat to the traditional model of our democracy." Though it had been announced months ago, the timing of Snowden's conference was strangely appropriate. The event took place just hours after *La Presse* revealed the Sûreté du Québec (SQ), which is the provincial police force, had put at least six prominent journalists under surveillance. Two days earlier, the same Montreal daily had broken the story that its own star columnist, Patrick Lagacé, had been spied on by the Montreal police force (SPVM). Appearing live from Russia, where he's been living in exile since exposing top secret information about US intelligence and surveillance programs, Snowden did not mince words when discussing the behaviour of Quebec police. (…) Snowden reiterated that citizens should be leery of authoritarian measures defended by governments that argue their very survival

is under threat from terrorists. "There's no real evidence this is actually the case, but the politics of this fear have reshaped the way our laws are getting passed." Canada's Bill C-51, whose adoption in 2015 generated reams of criticism from legal experts and ordinary citizens worried about how it would erode Canadians' privacy and individual rights, was one such example, he said. During the election, Prime Minister Justin Trudeau promised to amend the law, most notably by scrapping some "problematic elements" like the overly vague proscription against terrorist propaganda and by "guaranteeing that all actions undertaken by the Canadian Security Intelligence Service are consistent with Canada's Charter of rights and freedoms." Motherboard

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 7, 2016 / le 7 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Skepticism about peace bonds after arrest of alleged ISIL supporter for second time in two weeks
An alleged ISIL supporter has been arrested in Ottawa for the second time in less than two weeks for violating the conditions of his release, raising new questions about terrorism peace bonds. Police picked up Tevis Gonyou-McLean, 24, on Saturday morning — just five days after a judge had freed him from custody following his arrest for multiple previous breaches of his release conditions. "He was arrested, I believe, yesterday morning on breaches," his lawyer Biagio Del Greco said in an interview Sunday. He said there were two alleged breaches this time, one of them for a curfew violation. The 24-year-old was required to observe a 10 p.m. to 6 a.m. curfew and wear an electronic GPS ankle bracelet. He appeared in court over the weekend and the matter was adjourned to Tuesday. The case is the latest to prompt concerns about terrorism peace bonds, which the RCMP has been using to restrict the activities of extremists and prevent them from leaving Canada to join terrorist groups... There have been 18 arrests on terrorism peace bonds since the beginning of 2015, according to the Public Prosecution Service of Canada. Nine terrorism peace bonds are pending in Ontario, Quebec and B.C. Two are currently active. In Toronto, Kadir Abdul, the brother of an ISIL fighter believed to have died in Syria, signed a peace bond in July after he was arrested in Turkey. An Edmonton youth is also subject to a terrorism peace bond. On Aug. 10, another Canadian arrested on a terrorism peace bond, Aaron Driver, 24, was killed by a police tactical team as the extremist convert was attempting to leave his home in Strathroy, Ont. to commit a suicide bombing. Public Safety Minister Ralph Goodale later said the Driver case showed the limits of the effectiveness of terrorism peace bonds and that changes may be needed, including mandatory de-radicalization counseling. National Post; Vancouver Sun

Another arrest for alleged ISIL supporter

An alleged ISIL supporter has been arrested in Ottawa for the second time in less than two weeks for violating the conditions of his release, raising new questions about terrorism peace bonds. Police picked up Tevis Gonyou-McLean, 24, on Saturday morning - just five days after a judge had freed him from custody following his arrest for multiple previous breaches of his release conditions. "He was arrested, I believe, yesterday morning on breaches," his lawyer Biagio Del Greco said in an interview Sunday. He said there were two alleged breaches this time, one of them for a curfew violation. The 24-year-old was required to observe a 10 p.m. to 6 a.m. curfew and wear an electronic GPS ankle bracelet. He appeared in court over the weekend and the matter was adjourned to Tuesday. (…) There have been 18 arrests on terrorism peace bonds since the beginning of 2015, according to the Public Prosecution Service of Canada. Nine terrorism peace bonds are pending in Ontario, Quebec and B.C. Two are currently active. In Toronto, Kadir Abdul, the brother of an ISIL fighter believed to have died in Syria, signed a peace bond in July after he was arrested in Turkey. An Edmonton youth is also subject to a terrorism peace bond. On Aug. 10, another Canadian arrested on a terrorism peace bond, Aaron Driver, 24, was killed by a police tactical team as the extremist convert was attempting to leave his home in Strathroy, Ont. to commit a suicide bombing. Public Safety Minister Ralph Goodale later said the Driver case showed the limits of the effectiveness of terrorism peace bonds and that changes may be needed, including mandatory de-radicalization counselling. Posmtedia Network (National Post, A5, Ottawa Citizen, Leader-Post, London Free Press)

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

Second foreign student sent home after gun threat

The second international student under investigation related to an alleged gun threat at Seycove secondary has been sent back to his home country. **North Vancouver** school district confirmed Wednesday that his student visa had been revoked and he has flown home under the supervision of the homestay agency acting as his custodial guardian. Another student was arrested on Oct. 25 when he allegedly threatened to "bring a gun to school and do harm to a teacher." The student was sent home less than 24 hours later. Later, on Oct. 26, police recovered a gun somewhere off of school grounds. Police had requested charges of possession of a prohibited firearm and uttering threats for the second boy, although the Crown declined. "Because Crown didn't approve charges, there is no more criminal investigation happening. It will still try to be determined how the gun surfaced," said Cpl. Richard De Jong, North Vancouver RCMP spokesman. "We still have a concern, obviously as police, how a young person can have access to a gun." Police could confirm that the gun did not come from any of the homestay families. All other aspects of the investigation aren't being disclosed, De Jong said. Both students were subject to background checks by the school district as well as screening by the Canada Border Services Agency and Citizenship and Immigration Canada, according to Deneka Michaud, North Vancouver school district spokeswoman. North Shore News (2016-11-04)

School stabbing tragedy sparks security calls in SD62

The brutal, senseless slaying of a student at **Abbotsford** secondary last week has sent shock waves throughout school districts across the province and beyond, said Jim Cambridge, superintendent for the Sooke School District. "Although it's an unusual event, everyone was just shocked by the randomness," Cambridge said regarding the attack on Nov. 1. that killed Letisha Reimer, 13, and seriously injured her 14-year-old friend. "It hits a nerve with every parent and educator in the province, because we treat student safety so seriously. Our hearts and prayers go out to those families." He has spoken to several parents that have expressed their anxiety about school safety since the attack. School District 62 is fortunate in that regard because a former RCMP officer has been in charge of school security for a number of years and goes over security plans regularly, Cambridge said. In addition, the district holds annual lockdown drills, as well as earthquake and fire drills and goes over hold and secure and parent release procedures of part of its overall emergency preparedness plan. Goldstream News

Latest Surrey Shooting Leaves Two Indo-Canadian Men Dead

Vikram Toor and Ashim Raza were killed Friday night in a brazen shooting in the Fraser Heights area of **Surrey** next to an elementary school. Police believe the homicide is independent from other recent acts

of violence in the Lower Mainland. Two young Indo-Canadian men were killed after a drive-by shooting in Surrey Friday night, and police believe the incident is independent from other recent acts of violence around Metro Vancouver. The Integrated Homicide Investigation Team (IHIT) has identified the victims as Vikram Toor, 24, and Ashim Raza, 19. Surrey RCMP responded to calls of shots fired at about 7:20 p.m. at 110th Avenue and 159th Street in the Fraser Heights area. One of the men died at the scene and the other was taken to hospital, then died from his injuries. Investigators are still trying to determine if the shooting was targeted. (…) One neighbour told CTV News violence has been escalating in the area. "We only live half a block away from here, our kids go to school here," she said. "We thought we'd moved 16 years ago to a very nice neighbourhood, and a couple of years ago a man was killed right there." Bouquets of flowers were placed at the scene of the shooting on Saturday. More than 50 shootings have occurred in Surrey this year. Link Paper

Woman's death in custody exposes indigenous policing issues
Lena Anderson took her own life as she sat alone in the back of a police truck on the **Kasabonika Lake** First Nation on a cold late afternoon in February, 2013. Five members of a coroner's jury are now being asked to determine how she met her end – a mandatory procedure in Ontario when someone dies in police custody. Regardless of their findings, Ms. Anderson's case, along with the horrific deaths of two young men being held in a jail on the Kashechewan First Nation in 2006, serve as stark reminders that the right to a minimum standard of policing, and a basic level of security, do not exist everywhere in Canada. Indigenous communities with their own culturally sensitive police forces have no law to set requirements for officer training, mandatory equipment, use of force or codes of conduct. "At any given time, we have communities with no police, we have communities with one police officer working alone," Terry Armstrong, the chief of the Nishnawbe-Aski Police Service (NAPS), told the inquest. "If you were to ask me right now if it's safe, it's not safe." As it stands, indigenous policing is just another government program financed by Ottawa and the province of Ontario. The only way the communities of the Nishnawbe Aski Nation (NAN) will get security "backed by the rule of law" is if NAPS is covered by the Ontario Police Services Act, Mr. Armstrong said. Without the act, First Nations residents cannot demand that sufficient resources be applied to the job of keeping them safe. Detachments can be decrepit shacks – or non-existent. Police are not required to have radios or access to investigative services. There is nothing to say a lone officer should not be on call seven days a week, around the clock. Globe and Mail

Stolen semi found stuck in slough with murder suspect inside: Saskatchewan RCMP
A 26-year-old man is now facing a second-degree murder charge after RCMP launched a suspicious death investigation in Saskatchewan. At around 4:20 a.m. CT on Wednesday, RCMP received a complaint about a semi that had been stolen from a farm yard north of Kerrobert, Sask. The complainant also provided a description of a suspect. A short time later, another complaint was received by police about a sudden death at a residence in **Kerrobert**. Members attended and found Johan Klassen Sr., 53, deceased. Investigators determined the death was suspicious in nature and identified a person of interest who matched the previous description given. Kindersley RCMP said they immediately began searching for the semi and quickly found it stuck in a slough northwest of Luseland, Sask. The vehicle was in approximately 1.2 metres of water, about 30 metres from shore. The man inside the semi refused to exit. RCMP immediately contained the scene to ensure public safety and the emergency response team (ERT) was deployed to the scene to assist. At around 2 p.m., the man was taken into custody without incident. Sughar Daily; CTV News; 650 CKOM; Star Phoenix (2016-11-04)

Bomb threat Romeo jailed, ordered to pay $89,100
P.E.I. man who called in a bomb threat to Walmart in **Charlottetown** because he wanted his girlfriend to get the day off was sentenced to 60 days in jail and ordered to pay $89,100 in restitution. Logan Richard Arsenault, 19, appeared before Chief Judge Nancy Orr in provincial court in Charlottetown Friday after previously pleading guilty to calling in the bomb threat. In handing down the sentence, Orr said we don't live in a society where that type of behaviour is considered a joke. "It's never been a joke," she said. Arsenault used a payphone in Stratford on Aug. 2 to call in the bomb threat, saying he knew people who worked at the store and they needed to get out. The store was evacuated and closed for about six hours while Charlottetown police, an RCMP explosives unit, Island EMS and firefighters responded. NG News (2016-11-04)

Man charged for gym mischief
A man has been arrested in relation to a break-in that ended in the vandalism of a local school gymnasium. The incident took place in the early morning of Aug. 29, when a man entered Lakeland Ridge School, and was caught on surveillance video pulling a fire extinguisher off the wall. He then used the extinguisher to spray down the school gym, causing what the RCMP noted as "several thousands of dollars' worth" of repairs made necessary by the damage. A suspect turned himself into police on Oct. 29. Charges are pending against the 19-year-old man, from **Sherwood Park**, for one count of mischief under $5,000. He is scheduled to appear in Sherwood Park Provincial Court on Wednesday, Nov. 30 at 9:30 a.m. The man's identity has not been released by Strathcona County RCMP. Sherwood Parknews (2016-11-04)

Lawrencetown man arrested after indecent act complaints
A **Lawrencetown** man has been arrested and charged after RCMP received complaints about a man committing indecent acts in front of children. Annapolis County District RCMP started an investigation after receiving a complaint Tuesday afternoon about a man masturbating while fully undressed in front of a window as children walked by. A second similar complaint was received at about 8:30 the next morning. Assisted by the RCMP Internet Child Exploitation Unit and RCMP Technological Crime Unit, officers executed a search warrant at a Sunvalley Street residence. They arrested Chester Terry Thibodeau and charged him with three counts of committing an indecent act. Thibodeau has been remanded into custody after appearing in Annapolis Royal Provincial Court Thursday. He is scheduled to return Nov. 14 for a bail hearing. Chronicle Herald; Metro News (2016-11-04)

RCMP investigating separate indecent act incidents
A woman was shaken up but not injured when she was grabbed while jogging in **Spruce Grove** Thursday afternoon. RCMP said the woman was running near the soccer field on Heatherglen Drive around 4:30 p.m. when she was approached by the male suspect. She told police he talked to her briefly before grabbing her buttocks and shoulder and touching her face. He's described as 5'10", with a medium build and dark skin. The victim said he was wearing a black Nike jacket, black pants, a black hat, and thick black sunglasses. iNews 880 (2016-11-04)

Police seize drugs, handgun, cash during Sooke raid
Police seized drugs, a handgun, body armour and cash during a raid on a suspected drug house in Sooke. **Sooke** RCMP teamed up with the RCMP Island District General Investigation Section to execute a search warrant on a home in the 6700 block of Eustace Road in Sooke early Thursday. The raid followed a several-month investigation into drug trafficking. Police said they seized several ounces of cocaine, several pounds of psylocibin mushrooms, drug trafficking paraphernalia, a pistol and loaded magazine, a ballistic vest and more than $7,000 in cash. A 30-year-old man was arrested as a result of the investigation, and faces charges of possession of a controlled substance for the purpose of trafficking, unsafe storage of a restricted weapon, unlawful possession of body armour, and possession of prohibited weapons. The suspect remains in custody, but is expected to be released on bail. "This joint investigation has curtailed the activity of a high volume, and diversified drug trafficker who deals primarily to other dealers and users within the community of Sooke." said Staff Sgt. Jeff McArthur. Sooke News (2016-11-04)

Conception Bay South man arrested after child-luring investigation
A **Conception Bay South** man is facing charges of child luring after a five-month investigation. The 28-year-old man was arrested Friday without incident as a result of the investigation by the Combined Forces Special Enforcement Unit, an investigative unit comprising members of both the RCMP and the Royal Newfoundland Constabulary. CBC News (2016-11-04)

Felix Taqqaugaq inquest: Boy, 8, still afraid of RCMP after witnessing shooting
The coroner's inquest into the death of Felix Taqqaugaq went into the weekend with its most emotional testimony yet. The 30-year-old, diagnosed with schizophrenia, died in 2012 after being shot by police in his home in **Igloolik**, Nunavut. Neighbour Jacobie Amaroalik, who saw the whole incident through his window, struggled to get through his nearly two hours of testimony Friday. Speaking in Inuktitut through an interpreter, he broke down on the witness stand when he spoke about the impact the shooting has had

on his eight-year-old son, who also witnessed some of the events. "My young son does not want to go to school anymore. He knows the RCMP helps the breakfast program at the school and he does not want to see them," Amaroalik testified, sobbing. "It was very terrible for my young son because after seeing this incident, he would get a toy gun and pretend to shoot at the cops ever since then." CBC News (2016-11-06)

Fin de l'alerte Amber: deux enfants et leur mère retrouvés en Colombie-Britannique
La Gendarmerie royale du Canada (GRC) en Colombie-Britannique a mis fin à son alerte Amber après que deux enfants et une mère eurent été retrouvés sains et saufs à **Sicamous**, en Colombie-Britannique. L'alerte avait été déclenchée vendredi soir et les deux enfants, un garçon et une fillette, ont finalement été retrouvés à une station-service de Sicamous. La mère a été arrêtée. «L'enquête se poursuit et des accusations devraient être portées contre elle. Les enfants vont être réunis avec leur famille», a indiqué la GRC. Agence QMI (Journal de Montreal); CBC News (2016-11-05)

Manitoba RCMP respond to increase in road fatalities
Manitoba RCMP are reporting that nine people have died this past week on Manitoba roads and that officers are doing there best to not ever have this rate of fatalities repeated... RCMP say that everyone has a role to play and that Manitobans must wear their seatbelts, slow down and drive sober. Manitoba RCMP also recognize that enforcement is a critical part to changing driving behaviour, this year, there has been more enforcement and more impaired drivers taken off our roads. My Steinbach (2016-11-05)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Sexual abuse haunts children in indigenous communities
Child sexual abuse is a disturbing reality in many of Canada's First Nations, Métis and Inuit communities, research is beginning to show. Extensive interviews with social scientists, indigenous leaders and victims undertaken over the past few months by The Canadian Press show that the prevalence of sexual abuse in some communities is shockingly high. Only now are prominent indigenous leaders speaking out publicly for the first time about the need for communities to take a hard look. The impact of childhood sexual abuse is expected to be a central issue raised when hearings begin early next year for the inquiry into missing and murdered aboriginal women. An interim report is due in November 2017. "Throughout the (pre-inquiry) hearings on missing and murdered indigenous women and girls, we certainly found the incidents of child abuse and the association of child abuse was very, very frequent, in both the descriptions of the victims and in the perpetrators," said federal Indigenous and Northern Affairs Minister Carolyn Bennett. Canadian Press (Toronto Star, A1, Ottawa Sun, Times & Transcript)

CBC adds oldest Manitoba case so far to MMIW database: 56 years later, still no answers: Flora Muskego was found frozen to death in 1960 near Norway House
Flora Muskego was found frozen to death in a snow drift near Norway House First Nation 56 years ago. Her family is still wondering what happened to the 22-year-old on Thursday, December 9, 1960. There was a small newspaper clipping from 1960 in the Winnipeg Free Press stating when Muskego was found and that she was last seen just the day before. It also said a coroner's inquest was pending on the police investigation. Muskego is buried in Norway House today. As part of continuing CBC's coverage of missing and murdered Indigenous women and girls, Muskego is the latest case to be added to its database and oldest case uncovered by CBC in the province of Manitoba. Sylvia Grier, 64, of Saskatoon remembers her aunt. "I remember how beautiful she was," said Grier, also a Norway House community member. At the young age of eight, Muskego introduced Grier to make-up. Grier remembers her aunt wearing beautiful clothes and always having nice shoes. CBC News (2016-11-04)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Animal Rights Groups, the KKK, and ISIS—the RCMP's New Guide To Extremism

For the past few years, the Canadian government has faced accusations that it's been asleep at the switch when it comes to stopping youth from being programmed by violent extremist groups. The Royal Canadian Mounted Police are striking back at that notion with a 140-page guide to radicalization, extremist groups operating in Canada, and terrorist groups abroad. The agency's Terrorism and Violent Extremism Awareness Guide, which was officially unveiled in October, "is intended for first responders, parents, colleagues or friends of persons at risk alike and is meant to help the reader to better understand and recognize the growing phenomenon of radicalization to violence." A large chunk of the report is just compiling resources on radicalization, offering different models that try to explain how someone might come around to violence and extremism based on their social, religious, and political beliefs. But the report also sheds light on exactly which domestic groups the RCMP are keeping an eye on. The report's language borrows heavily from internal security and intelligence assessments prepared by groups like the Canadian Security Intelligence Service and the Integrated Terrorism Assessment Centre... The RCMP also warns about the Internationalist Resistance (IR), which it describes as an "extremist anti-capitalist group." The classification is interesting, because the RCMP has spent the better part of a decade investigating a small group of Quebec Communists, accusing them of making up the central cell of the IR, and for carrying out three bombings throughout Quebec from 2004 to 2010. A VICE Canada investigation raised questions about that investigation and whether the RCMP really has the right culprits. The RCMP report also names Skinheads Against Racial Prejudice and Red and Anarchist Skinheads, both committed to anti-fascism and anti-racism, as being two radical groups. Vice News (2016-11-04)

Feds to appoint border crossing adviser

The federal government is set to appoint a special ministerial representative to look at border crossing issues faced by First Nations. In a joint letter written in response to a Senate committee study, Indigenous Affairs Minister Carolyn Bennett, Immigration Minister John McCallum and Public Safety Minister Ralph Goodale say the adviser and First Nations will discuss significant and complex challenges. It also says the resolution of these issues will require a "horizontal approach" involving several departments and agencies. The ministers say the results of the engagement between the representative and First Nations will shape the work of an interdepartmental committee of senior officials. The Senate committee on aboriginal peoples outlined border crossing issues in its June report. The committee said some First Nations believe they should have the right to freely cross the Canada-U.S. border, based on the 1794 Jay Treaty between Britain and the U.S. Canadian Press (Inside Ottawa Valley, CBC News); Presse Canadienne (Journal Métro) (2016-11-04)

Espionnage de journalistes - Ottawa ferme les yeux sur le passé

Aucun journaliste n'est actuellement surveillé par la GRC et le SCRS... mais Ottawa n'a pas idée si cette situation a pu se produire dans un passé récent. Le ministre de la Sécurité publique, Ralph Goodale, ne l'a pas demandé. Et il n'a pas l'intention de le faire : c'est le présent qui compte, dit-il. Pour M. Goodale, " la question porte sur ce qui se passe maintenant et nous pouvons offrir l'assurance que ce genre d'activité n'a pas lieu. Je ne sais rien sur les événements qui se sont produits lorsque nous [les libéraux] ne formions pas le gouvernement ", a indiqué le ministre en point de presse. Questionné à savoir s'il demanderait directement au patron du Service canadien du renseignement de sécurité (SCRS) si des mandats de surveillance ont pu être lancés dans les cinq dernières années, Ralph Goodale a répondu que c'était précisément la " responsabilité du directeur de répondre aux questions opérationnelles "... Lors de la période de questions, M. Goodale a indiqué trouver " très inquiétantes " les révélations qui ont marqué la semaine au Québec -- l'espionnage de plusieurs journalistes par le Service de police de la Ville de Montréal (SPVM) ou la Sûreté du Québec (SQ). Le Devoir, A7; La Presse, 1 (2016-11-05)

Retour sur une semaine sombre pour la liberté de presse

Pour les trois journalistes de Radio-Canada, il s'agit de tous leurs appels de novembre 2008 à octobre 2013, confirme la SQ. Cette procédure ne prévoyait pas d'écoute électronique. La SQ cherchait à faire la lumière sur des fuites d'éléments d'enquête provenant de l'écoute électronique en 2008 et 2009 du président de la Fédération des travailleurs du Québec (FTQ) de l'époque, Michel Arsenault - qui s'est plaint en 2013 de ces divulgations dans les médias... Jeudi, il a dit s'être assuré auprès de la Gendarmerie royale du Canada (GRC) et du Service canadien du renseignement de sécurité (SCRS) que de telles « activités » ne se passent pas « au niveau fédéral ». Rappelons que deux journalistes de La Presse ont été espionnés en 2007 par des agents de la GRC. Radio-Canada (2016-11-05)

'Unregulated field' of private police needs greater oversight, report warns
Private police have exploded in numbers in recent years, but Canada is lagging behind other countries in tracking their often-covert activities - something that experts warn could compromise privacy and public safety if growth continues unchecked. "There is little or no governance or oversight of private security firms in Canada, no mechanisms that require standardized reporting by private security firms, and only minimal standards in place for licensing, training and discipline of the various positions within the private security industry," reads a research report prepared for Public Safety Canada. Provincial and federal statutes, including privacy rules, govern surveillance and the collection and use of information. But the report finds lax licensing requirements and a lack of oversight are failing to keep the activities of private investigators, analysts and guards in check. "This has a number of consequences, including an inability to ensure that private security companies are not vulnerable to organized crime, unethical and/or illegal behaviour," the report said. The report, released to CBC News, comes amid news reports about questionable surveillance and data collection activities of Canadian police and spy agencies. Two Quebec police forces have come under fire for tracking the cellphones of journalists, while a federal court condemned the Canadian Security Intelligence Service for illegally retaining the metadata of people not under investigation. The report finds a "potential" for private security to play an important role in community safety. But it warns of the dangers of an expanding role in the national security apparatus that falls largely under the radar. Curt Griffiths, a criminologist at B.C.'s Simon Fraser University who co-authored the report, called the growing business of private security an "unregulated field." CBC News (2016-11-06)

Laws on protecting journalists' sources not being followed, says retired justice John Gomery
The creation of a commission of inquiry into spying by Quebec police on journalists is a necessary step, but the public shouldn't expect it to solve the problem, says retired Quebec Superior Court justice John Gomery. Gomery, who led the commission of inquiry into the federal sponsorship scandal between 2004 and 2006, said such bodies are essential to help restore public confidence in the rule of law. "A public inquiry is a good way to find out what happened, but as far as developing policy for the future, I'm not sure it's the best way to go," he told CBC News. Gomery said one of the commission's useful functions will be to shed light on the role played by justices of the peace in the growing scandal. CBC News (2016-11-04)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Minister sides with RCMP on background checks
The justice minister of the NWT sides with the RCMP when it comes to giving information beyond criminal records to potential employers seeking background checks. Louis Sebert's remarks followed a demand from Yellowknife Centre MLA Julie Green for a stop to the practice. "Two days after getting (a) job, my constituent was let go. He has never been convicted of a criminal offence but the forms supplied by the RCMP detailed the things he was not convicted of," Green told the house. "My constituent lost a job he desperately needed because the police issued a form which confirms he has no criminal record, but which also says there is "adverse information" on file. This is not a conviction, it's a suspicion. This is outrageous." She asked Sebert if he would apply that principle to the Mounties and their policy. "The short answer is no. This act ... has been in force for 16 years now. I assume that Charter challenges have not been made or failed," Sebert said. NWT News

Mounties are recruiting
The RCMP is hiring. The Royal Canadian Mounted Police (RCMP) is recruiting police officers from all backgrounds who are physically fit, up for a challenge and ready to make a difference wherever they're posted. A career presentation will be held 6 p.m. Thursday, Nov. 24 at the RCMP Headquarters, 450 University Ave., Charlottetown. The presentation will offer the opportunity to meet with recruiters and hear real life career experiences from police officers who wear the RCMP uniform. A recruiting officer will also outline the process to apply, the benefits and rewards of a career in policing, provide advice and answer questions. There are approximately 18,500 police officers across Canada who work for the federal police

force of Canada. The RCMP is unique in the world providing policing services at the international, federal, provincial and municipal levels. Guardian, A4

Twilling ate RCMP Members Prepare Time Capsule
Members of the Twillingate RCMP detachment are creating a time capsule as they prepare to move into a new building in 2017. Constable Greg Bowie thought of the idea as a way to show future residents of the area a brief overview of the RCMP in Twillingate in 2016, as well as some information about the town that they serve. In the not too distant future the Twillingate RCMP will be ready to move from what is currently the oldest detachment in Newfoundland, to the newest. The idea of a time capsule seemed quite fitting for the occasion. Currently, the capsule will include a letter from Bowie with a brief history about himself and the other members he serves with. He plans to also include a current RCMP shoulder flash, a 2016 loonie, RCMP pin as well as newspaper clippings, both local and national from present day. They would also like to include photos or small mementos reflecting current life in Twillingate/Durrell. Bowie said the capsule is going to be very compact, as it will be packaged in a coffee can, therefore any donated items need to be small enough to fit inside. Pilot NL (2016-11-04)

Policing concerns in rural Saskatchewan prompt meeting of ministers - 'Public safety continues to be our challenge,' says Minister of Justice Gord Wyant
Saskatchewan's minister of justice says he went to the federal minister responsible for the RCMP over rural policing concerns. Gord Wyant said he and Minister of Public Safety Ralph Goodale agreed to have further meetings to discuss adequate RCMP deployment and resources allocated to this matter. "Public safety continues to be our challenge," said Wyant, adding that comments and concerns from the public prompted the meeting with the Saskatchewan MP. "We need to make sure that not only is the proper protection there, but people feel they are being protected," said Wyant. He said Goodale is doing a review of vacancy management. "I think that was a big concern that was expressed in rural Saskatchewan," said Wyant. CBC has reached out to Goodale for comment. CBC News; Radio-Canada (2016-11-04)

Quebec Mounties seek to launch discrimination lawsuit against RCMP
The association that represents RCMP members in Quebec is seeking to certify a class action lawsuit against the force on behalf of members across the country, alleging systemic harassment and discrimination against members by superiors. “There’s some cases that have been done privately but on behalf of all members, this has never been done,” said Frederic Serre, media officer for the Quebec Mounted Police Members Association. “You’re looking at power trips and unfortunately there’s a lot of it within the force … That’s what we’re trying to point out with this action.” Serre said that although it’s an association representing Quebec Mounties that’s seeking to launch the suit, the class action is meant to represent all RCMP members across Canada — not just those in Quebec or francophones. iPolitics; Global News (2016-11-04)

City of Richmond: Volunteer cops need gun training
The amount of time Richmond’s volunteer RCMP auxiliary constables are on the beat has dropped by 70 per cent this year, over 2014, after Mounties were ordered to have direct armed supervision of the complementary force and end all ride-along duties. Now, Richmond city council wants Ottawa to reinstate unsupervised duties for the unarmed auxiliary force and allow for firearms familiarization training. “We would like to see the auxiliary force back to what they used to be. It’s been a great resource to augment our police force,” said Coun. Bill McNulty. The city is backing a proposal by the Union of B.C. Municipalities to introduce a three-tier training program that would allow auxiliary constables to increase the number of duties they perform — such as public ceremonies, bike patrols and traffic and crowd control — without supervision. Richmond News (2016-11-04)

Grey OPP hosting counterfeit money detection seminar
Grey County OPP, together with the Bank of Canada and the Royal Canadian Mounted Police (RCMP), will be hosting a ‘Bank Note Counterfeit Detection Training’ session on Nov. 22 in Owen Sound. Businesses, together with the general public, are invited to attend this free training session to learn more about the security features on Canadian and US money; what to do should you receive a suspicious bank note; and discover tips and techniques for verifying and counting bank notes during cash transactions. All attendees will receive free training materials. Simcoe.com (2016-11-06)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

MLA calls for clear direction from GNWT on legal marijuana
Kam Lake MLA Kieron Testart is calling on the territorial government to establish clear guidelines on legal marijuana. Testart said that the government needs to be proactive ahead of proposed federal legislation that would make legal the consumption and regulated sale of pot. "The market is adapting to pending changes, drawing in national and international investment that is already roughly created a medical marijuana industry valued at $200 million," Testart recently told the house. "Marijuana is now considered by the business community as a commodity of great potential, and not an illicit drug; nothing exemplifies this more than the announcement by Shoppers Drug Mart, Canada's largest pharmacy trade ... having formally applied to be a distributor of medical marijuana." Testart asked Health and Social Services Minister Glen Abernethy how the GNWT intends to manage marijuana sales once the law changes, including issues like age restrictions which could be as young as 19 or as old as 25. NWT News

Local Ottawa politicians applaud raids on marijuana dispensaries
Local politicians in Ottawa are applauding the closure of a string of marijuana dispensaries operating illegally in the city. Police arrested nine people and raided seven pot shops this week after mounting complaints from community members and councillors. "I'm happy with the level of response that OPS has put in," said Jody Mitic. "We were kind of tightening the screws a little bit on the [police] chief." CBC News (2016-11-05)

Police hope pot shop raids
Ottawa police raided six marijuana dispensaries Friday morning, closing a big chunk of the city's pot shops in one fell swoop... The targeted shops are operated by a B.C.-based outfit that moved into Ottawa this summer, opening dispensaries called Green Tree, WeeMedical and CannaGreen. Ottawa Citizen, A2 (2016-11-05)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Current threat scenario is serious, requires a more adult conversation
An opinion piece states, "One of the great Canadian novels of the 20th century was Two Solitudes by Hugh MacLennan. It is the story of the troubles between Canada's two European founding nations-the French and the English (both had been preceded by the First Nations thousands of years earlier). The phrase "two solitudes" has entered Canadian English as a synopsis of the relations between the English and the French. Different languages, different backgrounds, different cultures, different ways of seeing the world. I couldn't help but think of this as I sat in a meeting room last Friday in the offices of the Canadian chapter of the Internet Society in Ottawa. I had been invited to a discussion on the intersections of rights and freedoms and the controversial C-51, the anti-terrorism bill that significantly increases some of the powers and capabilities of Canada's security and law enforcement agencies. I was the only person with any experience in those latter organizations (CSIS and CSE). The others in attendance were privacy advocates and lawyers. It was of no surprise to me that these participants, after paying what I saw as "lip service" to the necessity that our spies and cops have the tools to stop threats like terrorism, were uniformly critical of any more capabilities. I found myself time and time again disagreeing with their comments and realized how woefully ignorant they were of what CSIS and the RCMP do and how they do it, as well as why." Hill Times

It's not easy being a journalist's unnamed source in the Information Age
An opinion piece states, "Were I in a position of authority, I would probably hang up if contacted by a journalist. Not because I don't think people in positions of authority should speak to journalists - I do, and I'm grateful to all the people in positions of authority who haven't hung up on me over the years... In Canada, Mounties investigating a document leak have targeted journalists, and last week, reporters at La Presse in Montreal and at Radio-Canada discovered Quebec police, hunting for leakers in their own ranks, have been tracking and tapping their communications. (We have no idea how many other

journalists have been surveilled, but it's safe to assume it happens.)... Glenn Cowan, GRA Quantum's Canadian CEO, says such software allows phone, video or email communication without leaving any record: no metadata, no communications link to analyze, no tracking log, nothing...Cowan stresses that his firm does not regard law enforcement as a "threat actor," to use the language employed by the super-secret Communications Security Establishment in its advice to government employees on how to protect their communications..." CBC News (2016-11-05)

Should Canadian journalists assume they're being secretly watched by police?
An opinion piece states, "Journalists rely on whistleblowers to report wrongdoing, and whistleblowers trust journalists to keep their identities secret to protect their jobs, their families and sometimes even their personal safety. It's a relationship that's fundamental to holding those in power to account. That's why what happened this week was so remarkable. Not one but seven Quebec journalists, including some who work for CBC's French-language service Radio-Canada, learned they have been the subjects of secret surveillance by police in Quebec...The first revelation came Monday, when La Presse columnist Patrick Lagacé revealed that Montreal police confirmed they had been collecting metadata from his cellphone, effectively keeping tabs on every incoming and outgoing call...On Friday, I tweeted out what I believe many journalists were thinking upon hearing the news. A number of people responded that secret surveillance by police in Canada is something journalists should not only assume but accept. Goodgodmadge wrote: "Oh come on now, let's not be naive!" Some investigative journalists do work under the assumption that their conversations are listened to or their emails privately traced. But is there a danger in making that assumption? DS: So, Patrick, let me ask you first of all: What has this cost you? To have this level of surveillance of your activities? PL: A certain loss of innocence, I'd say. I really was living in this fairy tale - where journalists are not special citizens but you cannot spy on journalists as easily as what we've seen in this case..." CBC News (2016-11-05)

The worst part about the spying spree - it was legal
An opinion piece states, "Connect the dots between Quebec's police corps and the half-dozen or more investigative journalists who were put under surveillance over the past decade and you will find a gaggle of judges potentially derelict in their gatekeeping duties. In each of the spying episodes that have come to light over the past week, the police had to convince a judge to sanction the surveillance and, in some cases, to do so more than once..." Toronto Star (2016-11-05)

Spying eyes
An editorial states, "Taken in isolation, either case is concerning. But this week, we actually had two major law enforcement misconduct issues surface. The Canadian Security Intelligence Service, it turns out, has been collecting unrelated information it received as part of terrorism investigations (and was supposed to destroy), and instead loaded it into database systems that its legal overseers weren't even told existed. Meanwhile, in Quebec, police services were tracking some reporters' calls and texts for periods as long as five years, in an effort to catch and punish police whistleblowers. There's a huge problem here. And it's an oversight problem..." The Telegram, A15 (2016-11-05)

Surveillance des journalistes - La nouvelle chasse aux sorcières
Un article d'opinion déclare, « Le professeur Stéphane Leman-Langlois est un spécialiste de la police, du renseignement, du terrorisme, des technologies et du contrôle social. Il a récemment collaboré au livre "Transparent Lives" sur la surveillance au Canada. Il enseigne à l'Université Laval.\r\nAvez-vous été surpris par les récentes révélations sur l'ampleur de l'espionnage des journalistes québécois ? Pas du tout. Chaque fois que je parle de surveillance depuis des années et que je dis aux journalistes qu'ils sont les premières cibles, la plupart d'entre eux lèvent les yeux au plafond parce qu'ils n'y croient pas. Ils me traitent de parano parce que je suis dans les études de la surveillance. Je suis certain que le phénomène est d'une ampleur bien supérieure à ce qui vient d'être dévoilé. Je pense que les révélations de la SQ -- arrivées très, très rapidement et concernant, comme par hasard, des écoutes datant d'anciens directeurs de ce corps de police -- sont faites pour détourner l'attention. Mais bon, il va y avoir une commission d'enquête et, si elle peut lever des pierres, on va en trouver bien plus, de ces histoires de surveillance... » Le Devoir, B1 (2016-11-05)

Why spying on the press hurts democracy

An opinion piece states, "Revelations this week that two Quebec police forces spied on journalists by secretly monitoring their smartphones was widely condemned in Canada and abroad as an outrageous attack on press freedom. Critics from Edward Snowden to domestic and international media groups decried the police tactics as a spectacular assault in a country that is widely considered to be a gold standard for democracy..." Ottawa Citizen, B5 (2016-11-05)

OTHER / AUTRES

Ottawa police raid pot shops across city
Ottawa police have arrested at least one person during Friday morning raids at marijuana dispensaries across the city. The raids at the Wee Medical Dispensary Society shop at 358 Rideau Street, and the Green Tree Medical Dispensary shops at 290 Montreal Road, 256 Bank Street and 352 Preston Street come following a volume of complaints about the growing number of dispensaries across the city. One person was seen being escorted out of the shop on Montreal Road by police and shuttled into a cruiser. Ottawa police tweeted that there were operations underway "at several locations in Ottawa" but refused to comment further "so as not to jeopardize ongoing investigations." The federal government has promised to introduce legislation to legalize marijuana by the spring of 2017 but possession, production and trafficking of marijuana remains illegal. CBC News; Ottawa Sun (2016-11-04)

Armed robbers hit Stittsville pot shop
One of Ottawa's remaining marijuana dispensaries was robbed at gunpoint on the weekend.
The robbery at Magna Terra Health Services on Iber Road in Stittsville on Saturday came after police raids last week closed seven of the 17 illegal pot shops in town. Three men robbed the dispensary at about 7:30 p.m. on Saturday, escaping with three large garbage bags of cannabis products and some cash, Ottawa police StaffSgt. Jamie Harper said. Two of the men concealed their faces with hoodies or neck warmers, and one had a silver handgun, he said. Store employees were not injured. "Obviously this was a planned attack," Harper said. He compared it to pharmacies that are robbed for fentanyl and other drugs with street value. "There is always a criminal element out looking for this type of product." There have been at least four robberies of Ottawa dispensaries this fall, as thieves target the dried weed, cannabis cookies, brownies and cash in the stores. Magna Terra in Stittsville has more security than other dispensaries do. Ottawa Citizen, Front/A1

Health Canada disputes police story on fentanyl
Police were alerted by both phone and mail in July that there was liquid fentanyl in Hamilton, says Health Canada. The statement is in direct contradiction to police claims that the vice and drug unit were notified the week of Oct. 31 about the lab results and that they were not physical documents that landed on an officer's desk. Torstar (Hamilton Spectator, A1; The Record) (2016-11-05)

Five arrests in Fentanyl bust
Five people were arrested and $20,000 in Fentanyl seized after a year-long investigation **in** St. Catharines. Since November 2015, members of the Niagara Regional Police St. Catharines street crime unit have been conducting a drug investigation involving two individuals who were allegedly responsible for selling large amounts of Fentanyl in the city... In total, $20,000 in Fentanyl was seized in addition to $1,450 in cash. St Catherines Standard (2016-11-05)

Ottawa Citizen
If you're coming to Ottawa for Canada Day this year, would you mind sending us your RSVP? Despite the anticipation around the July 1, 2017, celebration of the country's 150th anniversary - and likely the biggest Canada Day bash the national capital has ever seen - no one involved in its preparations seems to know just how many people might actually show up to for the party. Millions of dollars are being spent on the event, which is sure to pack downtown Ottawa for the crowning event of a year of various celebrations. That will affect everything from traffic flow to business to public transit, and it will require a big police presence to maintain public safety. (...) The Ottawa Police Service has produced an internal estimate for 2017 Canada Day attendance, but a spokesman said that estimate won't be released to the public. He said the RCMP should be able to provide an official number, but the Mounties refused to comment on

expected crowds or how the national police force is preparing to deal with them. RCMP spokeswoman Annie Delisle referred all questions about Canada Day attendance to Canadian Heritge. Ottawa Citizen

Montreal police were issued warrants to listen to journalists' conversations
Montreal police sought, and obtained, warrants to listen to the private conversations of two journalists at the French-language newspaper La Presse, according to court documents seen by the journalists. The revelation adds a new dimension to the ongoing controversy about police surveillance of journalists in Quebec. CBC News; Montreal Gazette; Canadian Press (CP24; iPolitics; Toronto Sun); Global News (2016-11-05)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 10, 2016 / le 10 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Nipawin RCMP issue Amber Alert for 7-year-old Sask. girl believed to be taken by father

Nipawin RCMP have activated an Amber Alert for seven-year-old Nia Eastman believed to have been taken by her father Adam Jay Eastman, 45, Wednesday night. RCMP said Nia was to be returned home to her mother by 7:00 p.m. A vehicle believed to be operated by her father was located on a rural property east of Smeaton, Sask., near Snowden around 10:00 p.m. Neither Nia nor Adam were found with the vehicle. Officers are searching the vicinity. Police have described Nia as 3'9" with shoulder-length blonde hair. She was last seen wearing pink eyeglasses, purple long-sleeved shirt with butterflies, pink skirt and purple leggings with silver trim at the bottom. 650 CKOM; Global News; Toronto Star; CBC News

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

Jury finds python owner not guilty in deaths of New Brunswick boys

A jury has found a New Brunswick man not guilty of criminal negligence causing death after his African rock python escaped its enclosure and killed two young boys three years ago. Four-year-old Noah Barthe and Connor Barthe, 6, died during a sleepover in Jean-Claude Savoie's apartment in August 2013. (…) Matchim said an investigation by the RCMP and two subsequent reviews concluded that charges were not appropriate. He said he received that assurance in writing. The lawyer said a new lead investigator was then appointed and suddenly is client found himself facing a charge. (…)He responded to the earlier testimony of RCMP officers about the python's aggressive behaviour after it was captured - hissing and

lunging at the glass of the enclosure. "A snake that responds like that is a very aggressive snake," he said. "It was an extreme response to human presence. This animal was dangerous." Truro Daily

Nanaimo city council calls for RCMP to investigate Mayor

If there was still any hope of Nanaimo council healing from their very public fractures, this new scandal will end that. "Well this is a really strange situation obviously and a situation that is really complex," says Coun. Bill McKay. As city council openly calls for RCMP to investigate Nanaimo Mayor Bill McKay for alleged corruption. "When you hide something everyone assumes its corruption and that's the allegation," says Coun. Jerry Hong. "Until he comes forward and presents it and shows it otherwise that's what the allegations are." It's the latest in a saga of dysfunctional chapters in this council's story that was seen publicly for the first time last March, when 7 city councillors signed a letter calling for McKay's resignation "You know the public asked why we did it. These are some of the things why," says Hong. Chek

First Nations police service recommends its own disbanding at suicide inquest

The suicide of a First Nations woman in the back of a police truck is causing Canada's largest Indigenous police service to do some soul searching. The Nishnawbe Aski Police Service, which covers 34 First Nations in northern Ontario, told an inquest into Lena Anderson's death that it has neither the resources nor the legal foundation to do its job properly. So it took the drastic step on Wednesday of asking the jury at the inquest to recommend the police force be disbanded if Ontario does not bring it under the province's Police Services Act by March 31, 2017. "Enough is enough," said Nishnawbe Aski Police Service (NAPS) board chair Mike Metatawabin. "We can't do this all the time where you promise something and then turn around and say you can't do it." Ontario's Ministry of Community Safety and Correctional Services says it plans to introduce legislation in the spring that will "modernize" the Police Services Act and that it is consulting with First Nations on "exploring a legislative framework for First Nations policing." CBC News

Four cattle dead after chased by four-by-four

Okotoks RCMP are looking for help to catch individuals responsible for the death of four cattle after they were chased by a vehicle on a rural property in the DeWinton area. Sometime on Oct. 7 someone opened the gate to a property west of Macleod Trail where the animals were grazing. The suspects drove a four-by-four vehicle onto the ranch land and used it to chase cattle for an unknown length of time."It looked like someone had come in and chased them," said Heather Mills, who owned the animals with her family. "From what we could see it looked like they had brought them up the fence line where we had a catch pen. I don't know if they were trying to steal them or if it was a cruel joke." She said they want people to be aware and watchful for anything suspicious. Mills said the loss of four animals will impact their farm. The cattle were insured, but they are working to see how much they will receive. "This is livelihood and it affects everyone in the long run if people are injuring animals," she said. "There isn't a large margin at the end of the day for what farmers get off their cattle." Mills said she and her husband received a phone call from someone living on a neighbouring property that there was a dead cow. They were in Calgary at the time and received a second call soon after about a second animal. Upon arriving, Mills she said they counted their herd and realized another was missing. After euthanizing another, in total four animals were dead. Western Wheel

Two men facing charges in kidnapping in mountain resort town of Jasper, Alta.

RCMP say two men have been charged after an armed kidnapping in Jasper Alta., on Saturday. Mounties say the complainant has taken into a vehicle by two males armed with firearms, but managed to jump out of the moving vehicle and ran into a nearby business for help. He was taken to hospital and treated for non-life threatening injuries. A few hours later, RCMP in nearby Hinton conducted a high-risk traffic stop and took one male into custody while another man turned himself in at the local detachment two days later. Otto Richard Latimer, 21, and Nathan Rodney Shevalier, 29, are charged with forcible confinement, uttering threats to cause death, possession of a weapon for a dangerous purpose and theft under $5000, along with additional charges for Shevalier. Lethbridge Herald

Details emerge of unsolved murder in Penticton

Details have emerged in civil court about an unsolved murder in Penticton that happened over a year ago. The ex-wife of the man shot to death in a motel last June is fighting to receive the life insurance

payout. Darren Leadbeater, 36, was reported as the victim of a June 4, 2015 shooting at the Golden Sands Resort Motel by Penticton RCMP, who have not put forward a suspect or any findings since. So far the only details that have materialized are through a Supreme Court lawsuit filed by Leadbeater's former spouse Leanne Bishop. According to public court documents obtained by the *Western News*, Manulife Financial was initially withholding the $205,000 life insurance policy Leadbeater had through his employer, with the only beneficiaries being Bishop and her children. The reasoning Manulife offered in their response to the claim was "(Manulife) sought confirmation from the authorities and/or police that (Bishop) was not involved in the death of Leadbeater." Penticton Western News (2016-11-09)

'I was trying to stop him': RCMP officer apologizes for shooting Felix Taqqaugaq
The RCMP officer who shot Felix Taqqaugaq in his Igloolik home in 2012 apologized to Taqqaugaq's family at a coroner's inquest on Tuesday. Const. Jason Trites testified by video from Halifax, and in responding to a question from Taqqaugaq's father, asked by the family's lawyer, he said he hopes the family gets closure from this inquest into his shooting death by police four years ago. "I just hope that they realize that nobody joins the RCMP in the hopes of ever shooting somebody," Trites said. "I've talked to many members who have gone their entire careers without pulling their pistol, and I envy them because I live with this every day." Trites said he's done his best to keep the incident from affecting him professionally, but he replays the shooting in his mind in his downtime when he's not on the job. "I just hope the family knows that they're not the only ones that were hurt by this," Trites said. "The things that I deal with, do affect my personal life. I'm definitely not the same person as I used to be before this incident." CBC News (2016-11-09)

Parks Canada issues wolf advisory after 'freaky' encounter at B.C. beach
Brent Woodland was almost finished his normal run with his dogs at dusk on Wickaninnish Beach, near Ucluelet, B.C. last week, when he saw something moving on the sand dunes. It was a large wolf, bigger than his 40-kilogram dogs, standing just two metres away. "It was stalking us. I don't know how long it had been watching us," said the 36-year-old Ucluelet resident. And it didn't back down, until a 911 call brought RCMP sirens blaring. After Woodland's wolf encounter, and two others that day in the Long Beach area of Pacific Rim National Park Reserve, Parks Canada has issued a wolf advisory and warning for the area, including advice on how to react to the aggressive, habituated wolves that seem a little too comfortable around people. CBC News (2016-11-09)

Mint employee guilty of smuggling $165K of gold in rectum
A former Royal Canadian Mint employee has been found guilty of smuggling $165,000 worth of gold from the building on Sussex Drive — apparently in his rectum, an Ottawa judge ruled Wednesday morning. Leston Lawrence "clearly had the opportunity" to steal the gold because he often worked alone and the security cameras would not have caught him slipping gold pucks into his pocket, Justice Peter Doody ruled. (...) Under RCMP surveillance, he was seen visiting the Ottawa Gold Buyers store at Westgate Mall on March 9, 2015. The RCMP found Lawrence sold a 24-karat gold puck to the store for $7,966.27, and had previously sold 17 similar pucks to the store for a grand total of $138,172.46. The RCMP also seized four gold pucks — roughly the diametre of golf balls with a total value of $27,278.84 — from Lawrence's bank safety deposit box on March 11, 2015, the ruling detailed. CBC News (2016-11-09)

Nanaimo RCMP seize 44 firearms during amnesty month
Mounties in Nanaimo say residents turned over 44 guns to authorities during a province-wide amnesty month. Half of the guns turned over were handguns, while the others were rifles and shotguns, police said. Hundreds of rounds of ammunition were also seized by Mounties. CTV News (2016-11-09)

Police raid controversial pot dispensary in Whitewood, Sask.
The owner of a controversial marijuana dispensary in Whitewood, Sask. is facing a string of charges after police raided his business on Tuesday. Jerry Matthew Martin, 45, sparked debate in his community last year after contributing funds from his medical marijuana dispensary to local emergency services, a kids' camp and facilities including the town library. At about 10 a.m. on Tuesday morning, Broadview RCMP launched a raid on both the business, Martin Medical Services, and a residence. Whitewood is 175 kilometres east of Regina. CBC News (2016-11-09)

First Nations police service recommends its own disbanding at suicide inquest
The suicide of a First Nations woman in the back of a police truck is causing Canada's largest Indigenous police service to do some soul searching. The Nishnawbe Aski Police Service, which covers 34 First Nations in northern Ontario, told an inquest into Lena Anderson's death that it has neither the resources nor the legal foundation to do its job properly. So it took the drastic step on Wednesday of asking the jury at the inquest to recommend the police force be disbanded if Ontario does not bring it under the province's Police Services Act by March 31, 2017. "Enough is enough," said Nishnawbe Aski Police Service (NAPS) board chair Mike Metatawabin. "We can't do this all the time where you promise something and then turn around and say you can't do it." Ontario's Ministry of Community Safety and Correctional Services says it plans to introduce legislation in the spring that will "modernize" the Police Services Act and that it is consulting with First Nations on "exploring a legislative framework for First Nations policing." CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Calls for justice, communication, and cultural display at Amnesty Forum
While it wasn't a full house, the audience was engaged at Amnesty International's public forum in Fort St. John on Friday, Nov. 4. The forum acted as a venue to discuss the findings of Amnesty's report Out of Sight, Out Of Mind: Gender, Indigenous Rights, and Energy Development in Northeast B.C., and had five panelists on stage as voices for various aspects of the report. (…) Calls for justice for missing and murdered indigenous people were also raised. Inspector Mike Kurvers, detachment commander for the Fort St. John RCMP, spoke about the role of police in the community, particularly in dealing with the shadow population of transient workers who come through the area to work in the oil patch. "We are aware of it, we understand it, but from a police perspective it hasn't impacted the detachment to date. We still get the same number of calls and … treat each call on its own merits," Kurvers said. Alaska Highway News

Raising awareness of missing and murdered indigenous women in Canada
Brad Firth (Caribou Legs) has worn through 15 pairs of running shoes in five months. That is because he is running across the country from Vancouver to Newfoundland to raise awareness about the missing and murdered indigenous women in Canada. This run recently brought him to Shelburne County. The number of unsolved cases is high and is a problem. Firth's own sister was murdered and his idea to run across the country began in her memory but quickly spread to include all murdered and missing indigenous women. He runs in full warrior makeup. He said the reactions he's had by people have been wide and varied. (…) He said the biggest thing he would like to see destroyed is indifference surrounding the plight of the missing and murdered women. "How can we understand that indifference... how do we make our home safe again?" he said. "The more we honour the circle of life the more the circle of life honours us." Coast Guard (Nova News Now)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Surveillance: Thomas Mulcair veut que Goodale et Wilson Raybould s'expliquent
Le chef néo-démocrate, Thomas Mulcair, demande aux ministres de la Sécurité publique, Ralph Goodale, et de la Justice, Jody Wilson-Raybould, de rendre des comptes devant le Comité permanent de la sécurité publique sur la surveillance des citoyens et des journalistes. De passage à Montréal, mercredi, M. Mulcair a exigé que les deux ministres s'expliquent sur la tentative du ministère de la Justice d'empêcher que ne soit rendue publique l'information voulant que le Service canadien de renseignement de sécurité (SCRS) ait illégalement recueilli et conservé des données personnelles de citoyens canadiens pendant une décennie. Cette activité a récemment été jugée illégale par le juge Simon Noël de la Cour fédérale. Lors d'un point de presse devant l'édifice du quotidien La Presse, dont les journalistes Joël-Denis Bellavance et Gilles Toupin ont été illégalement surveillés par la GRC en 2007, M. Mulcair a

également demandé au ministre Goodale de préciser devant le comité la nature des activités des services policiers fédéraux visant des journalistes. Thomas Mulcair a noté que Ralph Goodale, tout comme le premier ministre Justin Trudeau, ont affirmé qu'il n'y avait aucune surveillance de journalistes «actuellement» et que M. Goodale a précisé que les policiers ne font «pas exactement» la même chose à Ottawa que ce qui a été mis au jour au Québec. Presse canadienne (L'Actualité) (2016-11-09)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Court told of cop's data hunt

Repeated bids to access police data that was allegedly sold by a city cop were described in court Wednesday by another officer. Staff Sgt. Jasbir Kainth told court he zeroed in on five days between March 10 and July 5, 2010 in which Det. Gerard Brand allegedly dug up information on people sought by a lending company trying to track down deadbeat debtors. He was paid $2,300 by the lending firm, contends Edmonton-based Crown lawyer Leah Boyd. "Were there any entries queried by Mr. Brand on that date?" asked Boyd, referring to June 16, 2010. (...) Kainth said he also sought out Brand's access record to the RCMP computer database shared with city police. "I asked for an audit of Brand's CPIC queries," he said, referring to the system known as the Canadian Police Information Centre. Two computers were seized from Brand's home along with other records to be analyzed. He's also accused of providing information on four people obtained through his employment for a friend. Calgary Sun, A18 (Calgary Herald)

Surrey mayor wants three tiers for RCMP auxiliary policing program

Surrey Mayor Linda Hepner said the city favours the third of three options governing the future of the RCMP's Auxiliary Constable Program. This option, which Hepner said is also the favoured choice of the Union of B.C. Municipalities, presents a three-tiered system which she says "allows us the broadest range of services." "I think it's a better option for both the city and the volunteers," Hepner told the Now. "It may very well take them into a career of law enforcement." The three options the RCMP is considering include settling with the status quo, setting up a community corps programs, or adopting a three-tiered program that would incorporate both options one and two. In January Surrey's roughly 80 volunteer cops – the largest contingent of roughly 1,500 auxiliaries across Canada – learned from RCMP headquarters in Ottawa that they would no longer be able to ride with Mounties, receive firearms familiarization training, and that their uniforms will be changed to better distinguish them from regular officers. Now Newspaper

Are Sask. RCMP detachments operating without backup? Minister wants to know - Sask. should have 925 RCMP working, under terms of agreement

Saskatchewan's Minister of Justice says anonymous sources within the RCMP have told him that some detachments in the province are operating without the expected numbers of officers. Gordon Wyant said Wednesday he has heard similar complaints, about RCMP staffing levels, from rural residents and leaders. Wyant said Saskatchewan's policing agreement notes 925 officers should be providing service in the province, but he has been told about staff shortages in some detachments. The shortages relate, he said, to unfilled vacancies. "Vacancies [in detachments] where there are a number of officers deployed, yet a number were on parental leave, sick leave, training or retirement leave, those kinds of things which weren't being back-filled," he said. "Those are the kinds of things that we became worried about. So, we've initiated a discussion with **the [federal] Minister of Public Safety."** CBC News (2016-11-09)

Rural municipalities eager for new policing strategy after Boushie shooting

Three months to the day after the shooting death of a 22-year-old indigenous man inflamed tensions across Saskatchewan, the province's rural municipalities say they want to work with government and the RCMP on a new policing strategy. Those discussions are expected to begin next week, when Saskatchewan Association of Rural Municipalities (SARM) representatives meet with Justice Minister Gordon Wyant, SARM president Ray Orb told reporters Wednesday in Saskatoon. "We know there are issues out there, so we need to address that," Orb said, referring to concerns about rural policing raised following the Aug. 9 death of Colten Boushie in a Biggar-area farmyard. Star-Phoenix (2016-11-09)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

Tuesday's vote saw more U.S. states legalize pot: Why Canada could benefit
There could be an upside for Canada now that several U.S. states have decided to legalize marijuana, according to one of the architects of Canada's pot policy. On Tuesday night while Americans were electing Donald J. Trump as their next president, several states also had ballot questions about whether to legalize pot for recreational use. California, Nevada and Massachusetts all said yes. All three states plan to have possession of small quantities of marijuana legalized by Jan. 1, 2017. That means by early next year, more than one in five Americans will live in a state where marijuana is legal for adult use. So what does it mean for Canada? Bill Blair, parliamentary secretary to the minister of justice and former Toronto police chief, told CBC News he sees a couple of benefits. "I think we will have an opportunity to learn from them and I think there's also some encouraging signs that they'll be more investment in research and more information about how this can be safely and healthfully regulated," said Blair. Canadian officials have already taken a look at how legalization has worked in Colorado and Washington state as the Trudeau government prepares to table its own legislation in spring of 2017. Oregon, Alaska and Washington, D.C., have also already legalized the drug. With 97 per cent of the vote in, Maine voters were separated by less than a percentage point, leaning towards legalization. California's move is significant because it's the most populous U.S. state, clocking in at around 39 million people. CBC News

Latest U.S. marijuana votes could bolster Canada's legalization effort: law prof
Canada's effort to craft a legalized marijuana regime could be boosted by the move of four more U.S. states to approve recreational use of the drug, says a Halifax law professor. As it designs a new system, the Liberal government must address the fact Canada is a signatory to three international conventions that require criminalization of the production and possession of cannabis. (...) Currently someone convicted of simple possession of up to 30 grams of marijuana is eligible to apply for a pardon, now known as a record suspension, five years after their sentence is completed. An internal Public Safety Canada briefing note, released under the Access to Information Act, says the issue of record suspensions will be "important to consider during the marijuana legalization discussions." The federal task force's report *"may include recommendations on past convictions,"* said Scott Bardsley, a spokesman for Public Safety Minister Ralph Goodale. Until new legislation comes into effect, current laws and rules remain in place, Bardsley added. Canadian Press (Times Colonist)

No sale for medical marijuana business in St. John's
The owner of Health Cannabis on Water Street in St. John's says he has been put on notice by the Royal Newfoundland Constabulary: sell marijuana and risk criminal charges. The warning comes despite the federal government's promise of new legislation to come in spring 2017 - expected to legalize the business of marijuana and possession for more than just medical use. "They called my landlord a couple of days ago," said David Ferkul, who spoke with The Telegram Wednesday afternoon. "Then he gave us a number. I phoned them back. They waited a couple of days and I finally got the call today." He said the caution was also delivered in writing. A business for patients: Ferkul said Health Cannabis is a "members only" spot, with membership being limited to medical marijuana licence holders. The location is only open on weekends and potentially some other, unusual hours. "The new federal law states that you have to receive your (prescription) marijuana through mail order from one of the 36 licenced producers," he said, referring to a list of producers licenced by Health Canada (the list is available on the regulator's website). Telegram, A5

B.C. pot grower seeing green as more states legalize marijuana
As California, Nevada, Maine and Massachusetts appear set to join the growing list of states that have legalized recreational pot, one of B.C.'s biggest medical marijuana producers is seeing big opportunities in the American market. After several successful ballot initiatives south of the border this week, B.C. will soon be the only West Coast jurisdiction between the Bering Sea and Tijuana where toking up is still restricted to medical use. But the people behind Tilray, the federally licensed cannabis production facility on Vancouver Island, aren't concerned about losing their edge to rivals south of the border when Canada eventually legalizes pot. "I think Canadian companies have a huge advantage based on the very tight regulatory framework that exists in the medical cannabis program in Canada," Tilray president Brendan

Kennedy said Wednesday. That tight framework may have squeezed out many entrepreneurs interested in jumping into the legal medical marijuana business, but the lack of competition has allowed licensed producers like Tilray to grow quite large. Vancouver Sun, A5

Pot dispensary owner charged with trafficking after two raids in Whitewood
A marijuana dispensary owner has been charged with a range of offences after Broadview RCMP conducted two raids in Whitewood, about 175 km east of Regina, on Tuesday. An RCMP brief said that marijuana and property, including cellphones, computers, cash and three vehicles, were all seized during raids on a business - not named by RCMP but known to be Martin Medical Services on the 600 block of 3rd Ave. in Whitewood - and a private residence. Jerry Matthew Martin, 45, is charged with offences relating to the "operation of an unlawful marijuana dispensary," RCMP said. These include the trafficking and possession of marijuana and cannabis resin, possession of the proceeds of crime, trafficking in the proceeds of crime and laundering the proceeds of crime. After an appearance at provincial court in Broadview on Wednesday, Martin was released to reappear on Nov. 23. Martin and his lawyer, the Vancouver-based medical marijuana advocate Kirk Tousaw, could not be reached for comment. Star Phoenix, A7 (Leader-Post)

Mountain High: Jasper, Lake Louise lead country in marijuana charges
There's no denying it, Jasper loves its pot. According to a recent RCMP report, for every 100,000 people that visited Jasper last year there were 3,024 incidents involving the possession of cannabis. That puts Jasper in the second top spot in Canada for the most marijuana busts per capita, following Lake Louise with 3,675 incidents last year. "I thought it was surprising that we reached second in Canada, but right now we're pretty committed to getting drugs off the street—whichever drugs they might be," said Cst. Patrick Vallee, the media liaison officer for the Jasper RCMP detachment. According to Vallee, during the past few years the number of search warrants obtained by the local RCMP has increased, which in turn has led to an increase in drug seizures. Jasper Fitzhugh (2016-11-09)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Zero tolerance for job horrors
An opinion piece states, "'To all the women who have been impacted by the force's failure to have protected your experience at work, and on behalf of every leader, supervisor or manager, every commissioner: I stand humbly before you today and solemnly offer our sincere apology.'' Those words, uttered by RCMP Commissioner Bob Paulson on Oct. 6, put on the public record what far too many female Mounties already knew for decades to be true: They were victims of workplace sexual harassment and abuse, some to such a degree careers were cut short and personal lives were ruined. The apology and accompanying multi-million-dollar financial settlement was preceded by separate class action lawsuits filed by two former RCMP officers, representing hundreds of women. Linda Davidson said she was sexually harassed by a male supervisor, when she was a young officer. Her legal claim stated she continued to face such attitudes as she rose through the ranks to become an inspector. Janet Merlo said she had to deal with sexist attitudes while on the force, even to the point of a manager asking why she didn't "keep her f---legs closed" when he learned she was pregnant. Both reported having to put up with sexual innuendos, comments and pranks. But both also said they blamed a minority of former colleagues for fostering such a toxic work environment. As the national police force took its first steps toward closure, a similar issue would come to light in Calgary." Winnipeg Sun

Where There's Smoke There's Fired?
An opinion piece states, "The federal Liberal government's winning election campaign included marijuana legalization. Working towards delivering on its platform, it has created a task force to provide advice on the design of a framework to legalize, regulate and restrict access to marijuana. But a review of the backgrounds of those appointed to the task force panel reveals there is no representation from safety-sensitive industries or anyone with expertise in occupational health and safety. This is problematic for the oil and gas industry, and for all industries with safety-sensitive workplaces. Employers have significant legislative obligations to ensure the safety of their workers. The Alberta Occupational Health and Safety Act outlines the legal obligation to maintain a safe work environment and to ensure the safety of workers.

There are similar obligations in occupational safety legislation in all provinces. These obligations must be taken into consideration when developing the policy framework to legalize marijuana." Alberta Oil

OTHER / AUTRES

Nil

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 16, 2016 / le 16 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

'I don't know that we can help you': RCMP boss 'consumed' with 'inability' to investigate in digital world

The RCMP is lobbying the Prime Minister's Office for new powers to bypass digital roadblocks in cases where national security threats and other "high priority" suspects hide online and operate anonymously beyond the reach of police. "I can safely say that there's criminal activity going on every day that's facilitated by technology that we aren't acting on," RCMP Commissioner Bob Paulson told CBC News and the Toronto Star in an exclusive interview. The problem is a major focus for Paulson, and one that only gets more urgent as technology advances and suspects find new ways to cover their digital tracks. "Because of our inability - and the future inability - to protect Canadians, both from garden variety criminality and from the national security threat, I see that as really significant," Paulson said. "I'm consumed with trying to make sure that we're able to mitigate the threat." But privacy advocates and civil liberties groups remain unconvinced that effort requires expanded investigative powers for police. (...) On June 23, the RCMP sent Prime Minister Justin Trudeau's national security adviser a briefing note that says Canada lacks strategies and laws to address the technological limitations of police investigations. The RCMP argues the U.S., Australia, the U.K. and New Zealand - members of our Five Eyes intelligence alliance - do much more than Canada to help their police forces deal with high-tech obstacles like encryption, and interception and storage of digital information. CBC News

Mounties lobbying for more power

The RCMP is lobbying Prime Minister Justin Trudeau for more powers - including access to digital information without warrants - to investigate suspects who are hiding behind uncrackable encryption on their digital devices, a Toronto Star/CBC investigation has found. "I can safely say that there's criminal

activity going on every day that's facilitated by technology that we aren't acting on," RCMP Commissioner Bob Paulson told the Toronto Star and CBC in an exclusive interview. "We're losing our ability, if we haven't lost it entirely, to bring the traditional investigative response to technologically facilitated crime because of the misunderstanding, in my view, of the privacy threat." The RCMP has reached a point, Paulson said, that Canadians should "think about where you go with that complaint because I don't know that we can help you." "And that's a terrible thing for a person who's in charge of a police force to say when citizens, when companies, when corporate Canada, or indeed when the government comes to us and says, 'Hey, we've been victimized on the Internet.'" An RCMP briefing document sent June 23 to Trudeau's national security adviser compares Canadian law enforcement's digital investigative capabilities with four western countries - and Canada stands alone. Toronto Star, A10

Protéger les sources, à la source
Un article d'opinion dit, « Le gouvernement fédéral profite pour l'instant du fait que les projecteurs sont braqués sur les patrons politiques des deux corps policiers impliqués dans le scandale de la surveillance des journalistes au Québec pour se tenir sur les lignes de côté. Le resserrement de la procédure pour l'obtention de mandats visant des journalistes et la commission d'enquête finalement mise sur pied par le gouvernement Couillard, ainsi que l'examen des procédures à la police de la Montréal (SPVM) demandée par Denis Coderre ont une portée limitée. C'est le gouvernement Trudeau qui a en main les leviers pour apporter des correctifs en amont en se basant sur les principes mis de l'avant par la Cour suprême. Un regroupement de journalistes, dont le chroniqueur Patrick Lagacé, à l'origine des récentes révélations là-dessus, l'a compris et interpellera justement aujourd'hui le gouvernement fédéral afin qu'il joue pleinement son rôle. C'est que la réponse du gouvernement libéral nous laisse jusqu'à maintenant sur notre appétit. Bien sûr, M. Trudeau parle de faits « troublants » et de son « ouverture » à apporter des correctifs au besoin. Le ministre responsable de la GRC et du Service canadien du renseignement de sécurité (SCRS), **Ralph Goodale**, trouve ça « ***inquiétant*** » et il rassure en disant que ses services ne se sont pas livrés à de telles pratiques, ce que les patrons des agences ont réitéré. Il considère que le cas Lagacé relève des compétences québécoises, ce qui n'est qu'en partie exact. Oublié par **M. Goodale**, l'épisode de la surveillance de deux autres journalistes de La Presse par la GRC dans l'affaire Charkaoui nous laisse croire qu'aucun corps policier n'est à l'abri d'un dérapage. En plus des voeux pieux exprimés par messieurs Trudeau et **Goodale**, le gouvernement libéral mise sur la vaste consultation sur la sécurité publique qui doit prendre fin à la mi-décembre pour obtenir des pistes de solution. On nous dit au bureau du **ministre** que « ***tout est sur la table*** ». Il faut savoir que nulle part dans les deux documents qui amorçaient la consultation il n'est question spécifiquement des sources journalistiques. C'est par la bande que ces sources seraient éventuellement mieux protégées, soit quand il est question que « tous les mandats du SCRS respectent la Charte canadienne des droits et libertés ». Et encore, on ne vise pas la GRC ici et on parle des mandats obtenus dans le cadre d'opérations liées à la sécurité nationale, rien à voir avec ce qui nous occupe actuellement. » Le Devoir, A3

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

Several charged in Medicine Hat ALERT bust
Eight people have been arrested, and three have been charged following a lengthy drug trafficking investigation in **Medicine Hat and Tilley**. On Nov. 8, the Medicine Hat Police, Brooks RCMP and members of the Alberta Law Enforcement Response Team team seized a pair of firearms, ammunition, cocaine and methamphetamines. ALERT also searched a rural residence outside of Tilley and seized more meth and another handgun. As a result of both searches, ALERT seized: 44-calibre handgun; 22-calibre rifle; Various rounds of ammunition; 57 grams of methamphetamine; 14 grams of cocaine; 34 cartons of contraband cigarettes; $3,550 cash proceeds of crime. In total, 20 charges have been laid against three people, with charges pending against another five. Calgary Herald, A11

RCMP follow up on new lead as they hunt for 'armed and dangerous' man in northwest Alberta
Police in **northwestern Alberta** are renewing a plea for help from the public as they continue a three-week-old search for an elusive man they consider "armed and dangerous." Peace Regional RCMP say Malcolm Henry Testawits is wanted on multiple charges including assaulting a police officer and robbery.

On Tuesday, Mounties said officers were investigating a theft of gas outside Brownvale, Alta. At around 1 a.m., they received a tip Testawits "may be connected to the theft and may possibly be in a specific rural area in the Grimshaw/ Peace River area." According to police, when officers followed up on the tip, they were unable to locate the man. Global News (2016-11-15)

Almost half of all cigarette butts at UBC are contraband

B.C. remains a significant market for untaxed contraband cigarettes, a study by the Western Convenience Stores Association shows. The majority, which are manufactured on First Nations reserves in Eastern Canada, are finding their way to students at B.C. high schools and universities. Every year the association conducts a study of contraband or illegal cigarettes found in B.C., Alberta, Saskatchewan and Manitoba to judge how pervasive the industry is in Western Canada. In B.C. it examined butts discarded at 50 locations, including government offices, universities, colleges and schools. (…) However, Andrew Klukas, president of the Western Convenience Stores Association, said the high prevalence of contraband cigarettes found at universities and schools shows students opt for cheaper products and the purveyors are specifically targeting youth. Unlike in the 1990s when high federal tobacco rates spurred the illegal importation of cigarettes from the U.S., mostly through the Akwasasne, Kahnawake and Six Nations reserves in Ontario and Quebec, most of the unbranded tobacco is now manufactured on those reserves, Klukas said. (…) The RCMP and Ontario and Quebec's provincial police have conducted frequent raids alleging the industry is tied to gangs and money-laundering. Klukas said despite its flat growth, B.C. is tied with Manitoba with the highest rates of contraband tobacco use in Western Canada. Saskatchewan has the lowest rate, at 11.7 per cent. But Alberta has also seen a significant growth over the last year, from nine per cent to 12.3 per cent, largely because of the slumping economy there and the Alberta government's decision to add $10 to the price of a carton in 2015, he said. The association estimates B.C. misses out on about $100 million annually in tax revenue. The contraband market is also a vector for criminal gangs to distribute other illegal products, he said. "RCMP inform us that there are over 100 criminal gangs in the distribution of these products and once they are out there, once you have a distribution network, it is not limited to just tobacco. Tobacco is the easy way to start a distribution network because the penalties are relatively low." Vancouver Sun, A1

Fentanyl can be deadly, new campaign warns

Dr. Brendan Hanley, the territory's chief medical health officer, and his team have launched a "Fentanyl can be deadly" awareness campaign to promote knowyoursource.ca and prevent fentanyl-related overdoses. There have been two fentanyl-related deaths in the **Yukon**, Hanley said today. The website originated with an initiative led by the Vancouver Police Department. Fentanyl is a synthetic opiate narcotic, a prescription drug used primarily by cancer patients in severe pain. It is roughly 50 to 100 times more toxic than morphine. The new campaign is in conjunction with National Addiction Awareness Week (Nov. 13-19). "Drug-related overdoses and deaths have become a very serious concern in Yukon," Hanley said in a statement. The campaign includes participation by the RCMP, Kwanlin Dün First Nation, Council of Yukon First Nations, the Blood Ties Four Directions Centre, FASSY, Many Rivers, the Yukon Hospital Corp. and territorial alcohol and drug services branch. They are working to raise awareness and provide education on the danger of fentanyl, which is also commonly prescribed for patients suffering from chronic pain, and other high-potency opioid drugs. Whitehorse Star, 3

Window shutter shot at S. Rutland Elementary over weekend

RCMP recovered evidence at South Rutland Elementary School showing damage to a window screen was caused by a small caliber firearm. On Nov. 14, shortly after 8 a.m., the **Kelowna** RCMP received a mischief report after school official's observed damage to the rear of South Rutland Elementary School in the 200 block of Mallach Road. School officials said the damage occurred sometime over the past weekend, between end of the school day on Thursday Nov. 10 and before the start of the school day of Monday Nov. 14. The damage was contained to a metal rolling shutter, which covers a classroom window at the rear of the school. RCMP made a full examination of the scene, with the assistance of both Police Dog Services and the Integrated Forensic Identification Services and recovered evidence that the damage caused is consistent with a small caliber firearm. Lake Country (2016-11-15)

Crime rides wave of theft

Kelowna's crime rate is up this year, thanks in large part to preventable property crimes. That was one of the conclusions reached during the RCMP's quarterly report to city council Monday. Kelowna's well-documented crime rate jumped in 2015, and acting top cop, Insp. Brent Mundle, said calls for service jumped during the third quarter of this year. Calls for service increased nearly 8.9 per cent – more than 3,900 – over 2015. Mundle said the biggest concern centres around property crime. Castanet (2016-11-15)

Police investigating death of seven-year-old Nia Eastman in Choiceland

An Amber Alert issued on Thursday had a tragic result with the discovery of the body of seven-year-old Nia Eastman, just hours after the body of her father, Adam Jay Eastman, was found near Snowden. Nia's body was found in a home in **Choiceland** shortly after noon on November 10, just a block from WM Mason School where she attended Grade One. Nia was reported missing after her father failed to return her home to her mother on November 9. He had picked her up after school and was to have returned her by 7 pm. Eastman's body was found on a quarter-section of land along Highway 55 near Snowden, dead of self-inflicted injuries. Federal Minister of Public Safety Ralph Goodale issued a statement on Nia's death on Thursday afternoon. "It was with great sadness that I learned that Nia Eastman was found deceased by the RCMP today following an Amber Alert," said Goodale in the statement. "It is heartbreaking to lose a child, and nothing can ever make that right. I wish to extend my heartfelt condolences to Nia's mother and family, her community and all those who have been touched by this tragedy. We are all grieving together this most terrible loss." Melfort Journal (2016-11-15)

Nia Eastman, father died by murder, suicide: RCMP

Autopsies on seven-year-old Nia Eastman and her father have determined the causes of death were homicide and suicide. In a statement released Tuesday, the RCMP said the specific causes of death will not be released, but there is no evidence anyone else was involved. Adam Jay Eastman was found dead on Nov. 10, the same day RCMP issued an Amber Alert to find seven-year-old Nia Eastman. She was later found dead inside a residence in **Choiceland, Sask**. Police say no charges will be laid. More to come... CTV News (2016-11-15)

Government of Saskatchewan app for smartphones doesn't issue Amber Alerts

The **Saskatchewan** government's emergency notification app for smartphones does not notify the public when an Amber Alert is initiated. The app notifies the public for emergency situations such as boil water advisories, tornado warnings and freezing rain. But according to a government spokesperson, although the app is capable of issuing missing person information, the administration of the Amber Alert program falls under the RCMP's jurisdiction. The government says for Amber Alerts to be included in the app, the RCMP would have to give them permission. The RCMP was expected to issue a statement on the matter on Tuesday. Canadian Press (Star-Phoenix) (2016-11-15)

RCMP need another 48 hours to review new Don Dunphy evidence

RCMP say they need more time to conduct interviews about new evidence relating to the death of Don Dunphy. The Dunphy commission said in a statement on Tuesday afternoon that RCMP say they will need another 48 hours to complete interviews regarding the new information, which was announced last week. On Nov. 8, the release of police reports into Dunphy's death were delayed after the commission said it found "new information" about the incident. Police cited concerns over "tainting" this new evidence, and asked the commission to delay the public release of the five reports expected to be issued last week. CBC News (2016-11-15)

Canada-wide warrant issued for murder suspect

RCMP issued a Canada-wide warrant for a man wanted for a murder in **Maskwacis**, near Ponoka. Officers responded to reports of a fight in which two men were attacked with edged weapons in the early morning hours of November 11, 2016. One man suffered non-life threatening injuries while the other man later died in hospital in Ponoka. A Canada-wide warrant has been issued for 26-year-old Allan Joseph Soosay for the following criminal offences: - Second Degree Murder; - Assault with a Weapon; - Assault Causing Bodily Harm. CTV News (2016-11-15)

Rash of crimes has Hay River wondering if more youth activities are needed - Community's youth centre shut down 2 years ago
The **Hay River** youth centre was a place for kids, even those who came from unstable home situations, to be kids. "It was a support network, but it was also just an outlet for them to shoot pool, play video games, hang out, use the skateboard park," says Kevin Wallington, who used to run the centre... It is unclear given the lack of available data whether crime has risen overall in Hay River following the youth centre's demolition, although the RCMP says it has seen an increase in property crime over the past 10 days. The RCMP was asked to provide crime numbers to help establish whether the current crime rate is out of the ordinary. The police instead referred CBC News to the Town of Hay River. The town, in turn, recommended CBC News contact the RCMP. CBC News (2016-11-15)

Before practice, the real thing for Arrowsmith Search and Rescue
Last week, area search and rescue teams were looking forward to some training at **Little Qualicum Falls** on Sunday. Little did they know they would be needed for a real-life rescue on Saturday in the hills above Nanoose Bay. A Victoria man was tired, cold but not seriously hurt after being rescued at Bonnell Falls. Arrowsmith Search and Rescue's Ken Neden told The NEWS the man was hiking with a friend on a trail near the falls and proceeded down a muddy slippery section with the aid of a rope that was in place... Neden said the man's friend called the RCMP for help who then called Arrowsmith Search and Rescue to assist at 3 p.m. Saturday. Parksville Qualicum Beach News (2016-11-15)

Mental-health workers to join Mounties in cars
Mental-health workers soon will be riding shotgun in some **Kelowna** police cars. A new policing initiative aims to pair such workers with RCMP officers in a bid to better help street people avoid criminal entanglements, city council heard Monday. Full details of the program, similar to ones already operating in some B.C. cities, will be announced soon, Kelowna RCMP Acting Supt. Brent Mundel told council. Councillors praised the RCMP for trying to work with social service agencies to curb what appears to be a local crime rate that's once again on a worrying rise. "The collaboration you're working on is phenomenal," Coun. Ryan Donn told Mundel. Coun. Gail Given said Kelowna's street population seems to have "grown quite considerably" during the past year. Dealing with challenges that flow from an increasing homeless and drug-involved population is the "top priority" for city council, Mayor Colin Basran said. Daily Courier (2016-11-14)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

B.C. limits on federal probe vex advocates
The B.C. government has issued an orderin-council that some legal advocates fear places new restrictions on the national inquiry into missing and murdered indigenous women. Attorney General Suzanne Anton said the order-in-council confirms the province's support for the inquiry by giving commissioners the power to examine relevant matters within B.C. "It gives them the authority that a provincial commission of inquiry would have," she said. But West Coast Women's Legal Education and Action Fund and the B.C. Civil Liberties Association both expressed concern Tuesday that the B.C. order comes with conditions attached. "I'm happy that they've committed to participating," said Kasari Govender, executive director of West Coast LEAF. "I'm less happy about the additional restrictions they placed on the terms of reference." She said the federal terms of reference already made clear that the inquiry will not reopen specific cases. The B.C. government's additional terms go beyond that by indicating that the commission "may not inquire into any matter respecting the exercise of prosecutorial discretion," she said. Times Colonist, A4

Officer guilty in wrongful arrest of First Nations woman
An Edmonton police officer has been ordered to participate in a reconciliation process with the First Nations woman he wrongfully arrested and charged in 2014. Const. David Olsson entered a guilty plea Tuesday to one charge of neglect of duty at a disciplinary hearing. It followed an investigation into the April 17, 2014, arrest and charging of Arlene Sams. Sams said in an interview she was in a bad state

when Olsson arrested her. She was intoxicated and struggling to cope after a recent assault. She said she was also on medical leave from her job as a land surveyor with the Government of Alberta, after being the target of racist bullying. (…) Sams was supported at the hearing by an aunt, activist Lewis Cardinal and Muriel Stanley Venne, founder of the Institute for the Advancement of Aboriginal Women. Venne said she sees parallels in Sams' case and the overarching issue of missing and murdered indigenous women. She said the incident reflects law enforcement's "overall indifference to aboriginal women" and speaks to the need for change. Postmedia Network (Edmonton Journal, A1, Edmonton Sun)

'Caribou legs' brings message to Paqtnkek
Inside the Paqtnkek First Nation community centre gymnasium, Nov. 2, there were eight red dresses being held up on a small stage like banners. One of the people holding a dress was Brad Firth, of the Gwichin First Nation in Inuvik, who people may know better as 'Caribou Legs.' Firth is on the final stretch of a run, which began in Vancouver, which will soon end in Newfoundland. Another red dress was being worn by Maryanne Junta, 16, of Eskasoni First Nation. Before 'Caribou Legs' took the microphone, Maryanne spoke about The Red Dress Project, and its role in raising awareness for missing and murdered Indigenous women. "The red dresses are a reminder of the staggering number of women who are no longer with us," she said." (…) The number of missing and murdered Indigenous women in Canada varies, from report to report, with some putting the number at more than 1,100; others at more than 4,000. Robyn Bourgeois of St. F.X.'s Coady International Institute, who has made missing and murdered Indigenous women central to her research, explained the discrepancy in the numbers. "You're going to see variance everywhere on this topic. If you're only looking at official police reports, you will find that the RCMP didn't record race, before 1980, and we cannot accurately know if someone is indigenous or not, unless it is stated in the report," Bourgeois said. Chronicle Herald, L16

Families, searchers focus of Instagram project
Writer Katherena Vermette's poetry and film about indigenous-led Winnipeg activists in the core North End neighbourhood is engaging a growing Instagram audience in an experimental National Film Board project. Each day since the beginning of October, "What Brings Us Here" has featured portraits of indigenous-led safety patrollers on North End streets and Drag the Red volunteers searching the river for evidence about unsolved missing person cases. Each photo is accompanied by the voices of volunteers, many of them family members of missing and murdered women and men. Postmedia Network (StarPhoenix, A3, Leader-Post)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Liberté de la presse: Trudeau doit agir au lieu de parler, dit un journaliste de Vice
Oui, Ben Makuch a entendu le premier ministre du Canada Justin Trudeau réitérer l'importance de la liberté de la presse dans la foulée des révélations des dernières semaines sur la demi-douzaine de journalistes québécois surveillés par les corps policiers. Sauf que le journaliste de Vice se bat depuis février 2015 devant les tribunaux contre la GRC qui veut saisir son matériel journalistique sur un présumé terroriste. «On m'a envoyé une citation à comparaître sous [le gouvernement] Harper et je suis allé en cour sous Trudeau. Rien n'a changé. Je ne vois pas de différence [entre les deux gouvernements]», dit Ben Makuch en entrevue avec La Presse. «En campagne, [Justin Trudeau] a dit que le journalisme était important et devait être respecté, mais les corps policiers fédéraux m'ont, sous sa surveillance, amené en cour pour que je donne de l'information et du matériel journalistique, dit le journaliste de 28 ans. [...]. Il n'est pas intervenu, il n'a rien dit.» L'histoire commence en février 2015, alors que Vice reçoit la visite de la Gendarmerie royale du Canada. La GRC veut obtenir ses entrevues et son matériel journalistique concernant un présumé terroriste du groupe État islamique, Farah Mohamed Shirdon, ancien résidant de Calgary qui a fait l'objet de nombreux reportages de Vice en 2014 et qui fait maintenant face à un procès criminel par contumace. Vice conteste la saisie du matériel journalistique. La Presse

Aaron Driver's device a killer, cops say
The cab driver who unknowingly picked up a bomb-carrying terrorist in Strathroy for a trip to London says he's alarmed, but not completely surprised, by new reports the explosive device was deadlier than initially suspected. "I realized that (its danger) at the time. All I know it was one hell of a big bang," former

Strathroy cab driver Terry Duffield said. An RCMP bomb analysis shows that the blast from the device, on its way to downtown London and perhaps Toronto, would have caused a high risk of death to anyone within 1.5 metres of the explosion and varying risks of injury up to 7.8 metres away. Injuries could have included lung damage and ruptured ear drums. That assessment doesn't include the impact from bomb fragments or the 139 ball bearings reportedly embedded in the device. "If what they're saying is true, I wouldn't be here talking to you today (if the bomb fully detonated). They would have went right through the seat," Duffield said. The RCMP did not answer questions from The Free Press. London Free Press (2016-11-15)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Edmonton man killed for stealing from gang members, murder trial told
A member of the White Boy Posse street gang ordered the 2012 execution of an Edmonton man because he was stealing drugs from gang members, a prosecutor told a jury Tuesday. Joshua Petrin, 31, is charged with first-degree murder in the death of Bryan Gower, 35, whose body was found on a country road near Lloydminster in September 2012. Two other men have already pleaded guilty in the killing. In his opening address to the jury, Crown prosecutor Jeff Rudiak told the jury of seven women and five men that Gower's murder was directed by Petrin. (…) RCMP Const. Lee Popescul testified when he arrived at the scene, he found Gower on the ground beside a black truck and a large pool of blood around his head. The trial is scheduled to last two weeks. CBC News; Postmedia Network (Edmonton Sun, A7, Edmonton Journal)

Suspicious package prompts evacuation of Red Deer RCMP headquarters
Police are investigating after a suspicious package was brought into the Red Deer RCMP's downtown detachment Monday, prompting road closures and a late-night evacuation. A section of 51st Avenue between 46th Street and 47th Street was closed for several hours after a resident discovered the suspicious package and brought it into the downtown headquarters. The explosives device unit was called in, and all non-essential staff were evacuated from the building. Officers canvassed the neighbourhood to advise businesses of the ongoing investigation. Officers "neutralized the device" shortly after 10 p.m. but police say they have yet to determine whether or not it was explosive. No one was hurt in the incident. The incident prompted RCMP to issue a reminder to the public. They say suspicious packages should be reported to police immediately, and should never be moved or touched. CBC News (2016-11-15)

Constable Amit Goyal in fourth year of paid suspension, conduct hearing delayed again
It's another delay of a conduct hearing for a Mountie into his fourth year of paid suspension. The conduct hearing for Constable Amit Goyal, formally of the Osoyoos RCMP detachment, has been postponed again until December, thanks to new information that's come to light. Goyal is in his fourth year of paid suspension, and this is the sixth time his RCMP conduct hearing has been rescheduled… Goyal was once an RCMP whistle-blower in a case that saw several senior Mounties criticized by superiors. CKNW (2016-11-15)

Fight involving Mounties in Prince Rupert, B.C., sparks internal probe
RCMP in Prince Rupert, B.C., have launched an internal investigation after cellphone video surfaced online apparently revealing a confrontation between officers and two teenagers. Police in the north coast city confirm in a news release that they responded to reports of a fight in progress shortly before 1 a.m. on Nov. 12. An ambulance was called when officers found an injured 16-year-old boy but they also say the teen became combative and tried to fight the attendants and police. According to police, an 18-year-old female bystander joined the fight and was taken into custody. Sgt. Jagdev Uppal says video of the incident has been distributed on social media and investigators are now trying to locate the person with the video and also want to speak with any other witnesses. A public complaint about the police response was filed on Nov. 14 and the RCMP release says an internal probe has begun. CBC News (2016-11-15)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

Marijuana and driving worries former Mountie
New Brunswickers and Canadians alike have every reason to be concerned that roads could become more dangerous with the legalization of marijuana, says a retired RCMP assistant commissioner. Roger Brown, who spent three years as this province's top cop, said he doesn't believe the system or technology is in place to be able to do roadside checks to find out when people are at a certain limit with regard to the drug. "An impairment is an impairment, whether it be drugs or alcohol," Brown said in an interview. "I just don't think, right now, that we're in a position to be able to actually determine that yet." Legislation to legalize marijuana is expected to be introduced by the federal government in the spring of 2017. Daily Gleaner, A2

UWindsor prof says Canada should 'permit, but discourage' all drugs
An opinion piece states, "Last week, several American states voted to legalize recreational marijuana and Canada is expected to issue guidelines to do the same. But University of Windsor law professor Bill Bogart says Canada is not going far enough to end the War on Drugs. In his latest book, Off The Street: Legalizing Drugs, Bogart says Canada should move to "permit, but discourage" all recreational drugs. He spoke with Windsor Morning host Tony Doucette. In your book, you argue the War on Drugs has been a failure for both the economy and society. Why? The central goal of the war [on drugs] has been suppression of drug consumption and we know that goal has not been achieved. Meanwhile, the war has imposed enormous collateral costs. We put people in jail simply for taking a substance. We allow a market to be run by thugs. They sell tainted substances that make people sick and even kill them. Governments are deprived of a revenue stream from an industry — and it is an industry — and children are terribly exploited in any number of ways." CBC News

Legalized pot industry could import U.S. talent
Americans wishing to flee a Donald Trump presidency could work in Canada's soon-to-be-legalized pot industry, say two immigration lawyers who dedicated a how-to podcast for our neighbours to the south. Canada is the first G7 country that has committed to legalizing marijuana, announcing at the United Nations earlier this year that it would introduce new legislation by the spring of 2017, even though doing so would breach three international treaties signed by previous Canadian governments. A federal task force led by Canada's former deputy prime minister Anne McLellan is expected to report back by the end of November with recommendations on how to move forward. Many startup companies will be seeking the expertise required to get their businesses off the ground as Canada inches closer to legalizing marijuana, immigration lawyers Betsy Kane and Mark Holthe said. According to Kane, who is with the firm Capelle Kane in Ottawa, Canadian companies could easily tap into U.S. talent in a variety of occupations found under NAFTA. Pharmacists, biologists, chemists, biochemists, horticulturalists, plant breeders and even soil scientists will soon find themselves in "huge demand," Kane said. "These type of professionals should be seeking out opportunities immediately and in the next year because I think there is a lot of demand and these people will get immediate work permits with a simple offer from many of these startup marijuana companies." Ottawa Citizen, A5 (Ottawa Sun)

Marijuana could help treat drug addiction, mental health
Using marijuana could help some alcoholics and people addicted to opioids kick their habits, a UBC study has found. "Research suggests that people may be using cannabis as an exit drug to reduce the use of substances that are potentially more harmful, such as opioid pain medication," says the study's lead investigator Zach Walsh, an associate professor of psychology at UBC's Okanagan campus. This comprehensive systematic review of research on the medical cannabis use and mental health also found some evidence that cannabis may help with symptoms of depression, PTSD and social anxiety. However, the review concluded that cannabis use might not be recommended for conditions such as bipolar disorder and psychosis. EurekAlert

Canopy Growth becomes Canada's first marijuana unicorn, worth $1 billion
Medical marijuana producer Canopy Growth Corp. has become the first Canadian company in the sector valued at more than $1 billion after strong quarterly results sent the stock on a tear. The company was trading hands at $11.16 per share when stock markets closed in Toronto on Monday. That values the

company at almost $1.3 billion. As recently as July, the company was worth less than a third of that. But that was before seven U.S. states voted last week to legalize some form of either recreational or medical marijuana. (…) During a conference call to discuss the company's quarterly results, CEO Bruce Linton emphasized the company's efforts to expand its production capacity to keep up with demand. CBC News (2016-11-15)

CAA wants to prepare the public for stoned drivers
The Canadian Automobile Association is lobbying for a government-funded public education program to warn of the dangers of cannabis-impaired driving before Canada legalizes recreational pot. Police will also need more funding to learn how to recognize and investigate drug-impaired drivers, says the CAA. The Liberal government has promised to introduce legislation legalizing recreational marijuana next spring and a committee report on the process is expected at the end this month. The CAA helped fund a study by the Ottawa-based Traffic Injury Research Foundation that suggests legalization will pose "incredible challenges" for managing pot-impaired drivers. The study is sure to inflame the escalating propaganda war over marijuana's harms and benefits, because it is premised on the assumption that access to legal cannabis will increase traffic accidents. The CAA commissioned a poll that found almost two thirds of respondents are worried roads will become more dangerous after legalization. CTV News (Civilized.life) (2016-11-15)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Government accountability in short supply
An editorial state, "Earlier this year the provincial Liberal government backed away from creating a Municipal Auditor General (MAG). This was after the former NDP government had set aside some $300,000 for creating and staffing such a service. A MAG had the approval of the Union of Nova Scotia Municipalities as well as the Cape Breton Regional Municipality (CBRM). In Richmond Co., ongoing investigations by the RCMP, the provincial Ombudsman and a Grant Thornton forensic audit all confirm the need for provincial oversight of municipal spending and expensing practices. MAG received enthusiastic support across Nova Scotia from taxpayers and many municipal leaders, including CBRM Mayor Cecil Clarke. Supporters believe the public would be better informed about irregularities, waste and corruption in the financial operations of their municipal governments. In addition to the Richmond Co. case, there have been cases of theft, fraud and corruption within some of the province's 50 municipalities. And still, many will likely go undetected." Cape Breton Post, A8

Washington offers look at pot future
An opinion piece states, "The first guy through the pot shop door Wednesday morning figured he had good reason to buy a joint. "I woke up to Trump as president," he said. Which, according to Washington state law, is a perfectly valid reason for getting high. Unlike Victoria, where the patrons of our three dozen or so (cough cough) medical marijuana dispensaries are supposed to be suffering from some sort of ailment, recreational pot is legal across the strait. It has been since the summer of 2014.That offers a glimpse of what Canada, where a federally appointed task force is due to report this month ahead of legalization legislation expected in the spring, might look like soon. The biggest surprise? The age of the consumers. Marijuana use by teens might not have changed, but the same can't be said of grey-hairs willing to buy, now that it's legal. "A lot of people are in their mid-50s to 70s," says Kelsi Hutchins, behind the counter at Mr. Buds, one of the three marijuana retailers allocated to Port Angeles by the state licensing authority. Patrons include plenty of Vancouver Islanders. "We're the closest store to the ferries," Hutchins says. "Probably 15 to 20 per cent of customers are tourists. Canadians especially." Prince George Citizen

OTHER / AUTRES

Spy agency kept court in the dark about data
Canada's electronic spies were asked to brief the Federal Court on their intelligence-gathering activities, the Star has learned. But the Communications Security Establishment (CSE) declined to meet with

federal judges earlier this year, saying an ongoing constitutional challenge prevented them from doing so. The request came from the same judge that found CSE's partner agency, the Canadian Security Intelligence Service (CSIS), illegally kept information on innocent people for almost a decade. In a strongly worded ruling released this month, Justice Simon Noël found CSIS kept the court in the dark about a program to retain and analyze data about innocent people between 2006 and 2016. The ruling gave an unprecedented look at CSIS's Operational Data Analysis Centre, which for years had been storing data about "non-threat" individuals. While the information was intercepted legally, the court ruled it was illegal for CSIS to keep and analyze it indefinitely. The ruling came out of a briefing on the program by Noël for judges who approve CSIS warrants. In documents obtained by the Star, CSE chief Greta Bossenmaier was told that Noël requested a general educational briefing from her agency around the same time. But because of a constitutional challenge launched by the B.C. Civil Liberties Association (BCCLA) against CSE's intelligence activities, currently before the court, the agency declined Noël's invitation. Toronto Star, A10

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 21, 2016 / le 21 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Digital encryption is here to stay, says report from U.S. lawmakers

As Canadian police push for more power in the online world, documents obtained by the Star suggest that privacy-protecting encryption software is here to stay. A memo prepared for Daniel Therrien, the federal privacy commissioner, stated it would be difficult for any one country to weaken or ban encryption technology. The document, obtained under access to information law, summarizes a report from the U.S. committee on homeland security. "Encryption tools very much are now ubiquitous, globally distributed and irrevocable, which plainly no piece of domestic regulation or lawmaking will undo, given that two-thirds of encryption products are produced and sold by non-U.S. firms," the memo reads. In other words, if the bad guys want to hide their tracks, they'll have plenty of options even if Canada or the U.S. attempts to weaken or ban encryption. The RCMP are making a very public push for more powers to obtain Canadians' private information from telecommunication companies and to decode encrypted messages. RCMP Commissioner Bob Paulson told a joint Star/CBC investigation it has reached the point where if a citizen is a victim of a crime online, he's not sure the Mounties can help. But the report from the U.S. homeland security committee, summarized for Therrien in the memo, states that weakening encryption would probably compromise public safety rather than improve it. North of the border, meanwhile, the federal Liberals are examining Canada's national security framework, including such issues as encryption and warrantless access to Canadians' private information. Public Safety Minister Ralph Goodale, who is leading that consultation, has remained neutral on the issue pending the results of the exercise. "We have invited everyone with a view to come forward with their perspective. "Obviously, the police perspective is being advanced with a good deal of vigour and enthusiasm from their perspective of law enforcement," Goodale told the Star last week. Toronto Star, A1

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

'We've always been seen as a threat,' says former N.W.T. premier of RCMP surveillance revelations

A recently revealed program of police surveillance across Canada is "alarming" and a "threat to our own security," says former **N.W.T.** premier Stephen Kakfwi. He's "not surprised," however, to hear that more than 300 protesters, 89 of whom are Indigenous, were being watched by RCMP as part of surveillance program called Project SITKA, launched in 2014...Police Response. "When the RCMP is in receipt of information that indicates an individual or individuals are involved in a crime or may pose a threat to the safety and security of others, we are duty-bound to investigate. The RCMP did not specifically target Indigenous protestors," writes Cpl. Annie Delisle, Media Relations Officer for the RCMP. CBC News (2016-11-20)

Mi'kmaq woman concerned about Project SITKA

A Mi'Kmaq woman from **Elsipogtog** is concerned that her name is on a "watch list" compiled by RCMP intelligence services in the wake of a year-long investigation of dozens of Indigenous protesters, called Project SITKA. Amy Sock, a former defence attorney, mother, and an active member of Idle No More worries her time on the front lines of anti-shale gas protests in 2013 may have landed her on the list, although the RCMP refuses to say whether she is or not. CBC News (2016-11-20)

Man wanted by RCMP arrested on Muskowekwan First Nation

A man who was wanted by the RCMP on several outstanding warrants has been arrested. Darryl Raymond Longman was located by **Punnichy** RCMP at a residence on Muskowekwan First Nation on Sunday.He was taken into custody at 3 p.m, according to a press release. On Nov. 19, the RCMP had issued a release asking for information on Longman's whereabouts. The RCMP said Longman was known to frequent Regina, Muskowekwan First Nation and George Gordon First Nation. On Oct. 3, 2015 Longman was arrested and charged with dangerous operation of a vehicle, driving while being chased by police, driving drunk, refusing to provide a breath sample, driving without a drivers license and stealing a vehicle. Longman also had additional outstanding warrants for his arrest in connection with an incident which happened on June 6. He was charged with assault, assault with a weapon, uttering threats and failure to comply. Leader-Post; CTV News (2016-11-20)

Surrey RCMP searching for missing 15-year-old girl

Surrey RCMP are asking for the public's assistance in locating a missing 15-year-old girl. Police say Trinity McKenzie was last seen on Friday, Nov. 7 at home in Surrey. Family and police are now concerned for her health and well-being. Global News (2016-11-20)

Red Deer's top cop talks about tackling drugs, organized crime

It's no secret that drugs and organized crime are driving much of the crime activity in Red Deer. In part two of our feature story, new **Red Deer** RCMP Superintendent Ken Foster says he is condifent these troublesome issues can be dealt with effectively. Red Deer News Now (2016-11-19)

RCMP investigate daylight shooting in Burnaby

There is a heavy police presence in a south **Burnaby** neighbourhood following reports of a shooting. Nearby residents reported hearing shots fired around 11:30 a.m. One victim has been taken to Royal Columbian Hospital, and RCMP say a possible second victim may have also been treated in hospital. The incident occurred in the 7100 block of 14th Avenue, situated several blocks from the Edmonds SkyTrain tation and one block from an elementary school. Global News; CKNW (2016-11-19)

Punnichy, Sask. RCMP on lookout for 2 wanted men

Saskatchewan RCMP is asking the public for help locating two separate wanted men. Darryl Raymond Longman, 48, has outstanding warrants for his arrest. On Oct. 3, 2015, he was charged with Criminal Code offences such as operation of a motor vehicle while being pursued by a peace officer operating a

motor vehicle, impaired operation of a motor vehicle and taking a motor vehicle without consent. Global News; CTV News; CBC News; Leader-Post (2016-11-19)

RCMP request that Albertans please report their moldering dynamite
There may be something explosive lurking amongst the rolls of baler twine and tractor parts in that old barn down on the farm. According to **Alberta** RCMP, there is a large but unquantified amount of degraded and deteriorated dynamite on properties across the province as a result of historic rules that permitted farmers and ranchers easy access to explosives. Edmonton Journal; Agence QMI (TVA Nouvelle) (2016-11-19)

Four face drug charges following police search in Harbour Landing
Four adults are facing cocaine trafficking charges after police executed a Controlled Drugs and Substances Act search warrant in **Regina**'s Harbour Landing neighbourhood Wednesday. Regina's Combined Forces Special Enforcement Unit (CFSEU), with the assistance of the RCMP Integrated Organized Crime Unit, seized cocaine, cash and a loaded hand gun. Danieol Johnson, Kendall Robinson, Ali Mahdi and Mohammed Osman are all charged with possession of cocaine for the purpose of trafficking and proceeds of crime over $5,000. Leader-Post, A4 (2016-11-19)

Break-in at Manitoba Hydro compound
Steinbach RCMP are currently investigating a recent report of a break, enter and theft to the Manitoba Hydro compound located in the City of Steinbach, Manitoba. My Steinbach (2016-11-19)

Codiac RCMP locate both missing persons in Moncton
Police say both the 17-year-old boy and 23-year-old woman reported missing Nov. 17 in separate incidents in **Moncton** have been located. The boy had left the Moncton City Hospital of his own accord that day. The woman was located Saturday afternoon. Codiac RCMP thanked the public for their assistance. CBC News (2016-11-19)

Leduc RCMP appeal to public for help finding woman missing since Nov. 3
Leduc RCMP issued a plea to the public for information on a missing woman Saturday. Mounties said Deanna Millington left her family home in Leduc, Alta. on Nov. 3 and has not been seen since. Police said they are concerned for the woman's well being. Global News; CTV News (2016-11-19)

RCMP warn of email fraud
The RCMP has issued a warning about a recent email scam targeting businesses that perform wire transfers. That scam often involves businesses whose executives' email accounts are compromised or imitated. The fraudster then sends emails to an unsuspecting employee telling them to wire large sums of money to foreign accounts. Charlottetown Guardian, A3 (2016-11-19)

Inquiry into Don Dunphy death delayed by anonymous letter
Police are asking for the public's help in finding the author of an anonymous letter about the shooting death of Donald Dunphy. A press release from the RCMP says they found out about the letter on the evening of Nov. 7 from the inquiry into Dunphy's death and began investigating its contents and source the next morning. "The RCMP was informed by the commission of inquiry respecting the death of Donald Dunphy the new information in the form of an anonymous letter had come forward regarding the death of Mr. Dunphy. The following morning the RCMP obtained the letter and began an investigation into its origins and content," said RCMP Superintendent Pat Cahill at a news conference Friday. CBC News; VOCM News (2016-11-18)

RCMP testify in Burnaby school bookkeeper's trial
Police decided to focus on investigating questionable cheques instead of missing cash at Alpha Secondary between 2008 and 2010 because cash is harder to track, according to the RCMP's chief investigator in the case. Const. Anna Taylor testified Wednesday at the trial of former Alpha Secondary bookkeeper Jodi Fingarsen, who is accused of defrauding her **Burnaby** school of about $67,000 using cheques either fraudulently generated, signed or deposited. During her investigation, Taylor interviewed school staff who also complained of missing cash collected for things like school trips, dry grad

celebrations and Advanced Placement exams. "They did bring up the cash as well," said Taylor, "but from the police perspective, tracing physical cash is more difficult." Defence lawyer John Banks, however, suggested Taylor didn't investigate the missing cash because Alpha's system for collecting and accounting for cash was flawed. Burnaby Now (2016-11-18)

Swift Current RCMP looking for two missing teens
Swift Current Municipal RCMP are looking for two missing teenagers who haven't returned home or attended school this past week. Fourteen-year-old Amber Padley was reported missing to RCMP on Wednesday, Nov. 9. She's described as Caucasian, five feet six inches tall and 120 pounds with brown hair and blue eyes. Fifteen-year-old Austin Doerksen was reported missing to RCMP on Friday, Nov. 11. He's described as Caucasion, six feet two inches tall and 180 pounds with blonde hair and hazel eyes. CJME News (2016-11-18)

Missing girl found
Nakayo Poucette has been located and is safe. **Cochrane** RCMP were requesting assistance from the public to find a missing 16-year-old from Morley. Nakayo Faith Poucette, 16, from Stoney Nakoda First Nation was last in Morley on Nov. 7 when she attended a birthday party at her grandmother's residence on the reservation. Poucette was seen leaving the party with another young male under non-suspicious circumstances, according to the RCMP. Poucette is believed to be out in Morley and the RCMP do not think she is in any danger, according to Sgt. Darleen White with the Cochrane RCMP. Cochrane Eagle (2016-11-18)

RCMP charge teen in fake terrorist threat in Yellowknife but give no details
RCMP have arrested and charged a teen in **Yellowknife** in a fake terrorist threat. Mounties say the criminal charge resulted from an investigation by Alberta RCMP K Division that began on Nov. 1. Northwest Territories RCMP spokeswoman Marie York-Condon says no details about the hoax can be released, but may come out in court. She says the youth has been released on conditions and will appear at a later date in youth court in Yellowknife. York-Condon also says the next court date may not be released "considering the size of the community that the court is in and the amount of youth that may be appearing in court." She says there was no public safety risk when the alleged threat came to light. Canadian Press (CTV News) (2016-11-18)

IIU Investigates Arrest Involving RCMP Dog
Manitoba's police watchdog is investigating after a robbery suspect was brought down by an RCMP dog in Portage la Prairie on Wednesday. Mounties were called to an armed robbery in the city west of Winnipeg and arrested three people, however one man got away. Officers let the dog loose to chase after the man. The Independent Investigation Unit (IIU) did not go into details, but the suspect received an injury to his leg once the dog caught up to him. 680 CJOB (2016-11-18)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

'That was just my destiny'
Sharon Acoose remembers being groped as a child by an uncle who paid her in pocket change for her trouble - the earliest roots of a life scarred by sex work, drug use and jail time. "He would give me a quarter ... or a nickel or a dime, whatever he had," Acoose, 63, recalled during an interview with The Canadian Press. "You wouldn't believe all the candies that I bought." Despite the longest of odds, she managed to turn her life around, eventually becoming a professor of social work. Countless others who followed a similar trajectory are no longer alive to tell the tale. To this day, that same cycle is repeating itself with alarming frequency in indigenous communities across Canada, a CP investigation has found. And with its insidious links to suicide, violence and mental health problems, the issue of child sexual abuse is poised to be a key theme in next year's long-anticipated national inquiry into the tragic phenomenon of murdered and missing indigenous women. (...) Indeed, experiences of sexual and physical abuse among indigenous women and girls are so pervasive they are expected to overwhelm

next year's national inquiry, where commissioners will examine and report on the systemic causes of the violence. (...) In May 2014, the RCMP documented 1,181 murdered and missing women between 1980 and 2012. A year later, it said 32 additional aboriginal women had been murdered and 11 more had disappeared since it first reported on the issue. The force also cited an "unmistakable connection" between homicide and family violence. Aboriginal women are vulnerable precisely because they're aboriginal and women, said Dr. Yvonne Boyer, a Canada Research Chair at Manitoba's Brandon University. Boyer co-authored a report on trafficking of aboriginal women for the Public Safety Department in May 2014 that noted many of its participants suffered sexual abuse as a child, contributing to a pattern of exploitation that carried on into their adult years. Canadian Press (The Guardian, A8, Waterloo Record, Times & Transcript, Chronicle Herald, National Post, City News, Battlefords News-Optimist, Hamilton News, Weyburn This Week) (2016-11-21); (2016-11-21); Canadian Press (Ottawa Citizen; iPolitics; Mississauga.com; Waterloo Chronicle); Presse Canadienne (La Presse, Le Devoir) (2016-11-20)

UN urges Canada to work on barriers that still face women
A new report from the United Nations is calling on Canada to get to work on a number of barriers still facing women when it comes to gender equality and urging the government to take more concerted steps to stop violence against indigenous women and girls. The review - typically conducted every four or five years - by the Geneva-based Committee on the Elimination of Discrimination against Women covered a range of issues, from the gender pay gap to poverty and violence against women, as well as the use of solitary confinement in prisons. Prime Minister Justin Trudeau, who often calls himself a feminist, has said improving relationships with indigenous communities and working toward gender equality are key priorities for his government. And the report did note some progress, namely the equal representation in the federal cabinet. But the committee cited a range of concerns, among them the "continued high prevalence" of gender-based violence, particularly against indigenous women and girls. It also highlighted the "very low" number of cases of violence against women reported to police by victims, and low rates of prosecution and conviction against perpetrators. The report, posted on its website Friday, came as prosecutors in Quebec said no charges would be laid against police officers in Val-d'Or, after 21 indigenous women and seven men filed complaints against police that included sexual assault and excessive use of force. "It's difficult enough when you're dealing with violence in your personal life," said Francyne Joe, the interim president of the Native Women's Association of Canada. "If you can't go to police expecting to be protected, that's going to lead to such despair and depression and anger ... and disrupt any growing positive relationship with the policing system." Globe and Mail, A12

Caribou Legs reaches St. John's
Brad Firth - better known as Caribou Legs - was part-way through a run spanning five provinces last year, on a mission to protect lakes and rivers, when he got a call that would change his life. got some bad news from back home. That phone call was actually about my sister's death. So I was hit with this really sad story, and it took me a couple of hours to regain my strength, my balance, and continue running, because I didn't want to run any more," Firth said. After finding out his sister had been killed, he just wanted to go home and grieve - "not the right way, but I wanted to grieve angrily, because - just the way my sister died." (...) Caribou Legs, with the support of groups such as Sisters in Spirit, Warriors Against Violence and Culture Saves Lives, decided to set out on the road again. This time it would be to honour women, shine a spotlight on the country's missing and murdered indigenous women and girls, and prevent violence against women. The Telegram, A5; VOCM

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Apology for anti-homosexual persecution should include compensation, government told
Ottawa's apology to Mounties, soldiers and other public servants whose careers were destroyed by anti-homosexual witch hunts will have to be accompanied by compensation, experts say. Prime Minister Justin Trudeau appointed Edmonton Centre MP Randy Boissonnault as a 'special advisor for LGBTQ issues' earlier this week with the goal of arranging an official apology to the thousands of gay and lesbians who were persecuted in the latter half of the 20th century. "We do not have a timeline to announce at this stage," Cameron Ahmad, press secretary to the Prime Minister's Office, said in an email

to iPolitics. The apology will have to include some form of compensation, said Matt James, an associate professor at the University of Victoria who specializes in political apologies and the Canadian Constitutionalism. James said he would not be surprised if representatives from the agencies involved in the persecution - the RCMP and Canadian Armed Forces - had a chance to vet the apology. "I'd be very interested to see, for example, if the apology attempts to make any kind of excuse in terms of national security or that these were things that other security agencies were doing at the time," he said. "I would expect [it's something] the RCMP or military representatives would want to see in there and something I expect the representatives in the LGBTQ community would not want ... So there will be some interesting choices the government will have to make around that." The government announced in April it would apologize and offer redress to LGBTQ employees of the federal public service and the Canadian Armed Forces persecuted by the RCMP. Many were charged with gross indecency before homosexuality was decriminalized in 1969. After decriminalization, federal government workers suspected of being gay or lesbian were often denied promotions or security clearances that would advance their careers. Military members could be dishonourably discharged from the service until 1992. Upwards of 9,000 people were affected. iPolitics

Un camp islamique financé par la Ville de Montréal

Montréal a versé 10 850 $ à une association islamiste pour prendre en charge 30 enfants réfugiés syriens même si elle est soupçonnée par la GRC d'avoir financé des groupes terroristes. Des jeunes syriens âgés de 5 à 14 ans, dont certains ne parlaient pas français ont été accueillis cet été au camp Sindbad organisé par le Centre communautaire Laurentien, une section de l'Association musulmane du Canada (MAC). Le MAC est l'antenne la plus officielle des Frères musulmans, rappellent deux experts. En janvier 2015, Le Journal révélait, d'après des documents de cour produits par la GRC, que MAC avait versé près de 300 000 $ à l'International Relief Fund for the Afflicted and Needy-Canada (IRFAN). En 2011, Revenu Canada a révoqué le statut d'oeuvre de bienfaisance de cet organisme, puis le fédéral l'a déclaré organisation terroriste en 2014. Il reproche à l'IRFAN d'avoir envoyé 14,6 M$ au Hamas entre 2005 et 2009. Le Hamas, un autre groupe terroriste selon Ottawa, vise la libération de la Palestine de l'occupation israélienne et l'instauration d'un gouvernement islamique. Malgré son interdiction, la GRC dit avoir aperçu en mars 2014 un collecteur de fonds de l'IRFAN dans les bureaux de MAC à Montréal. Le Journal de Québec, 25 (Le Journal de Montréal)

Legal changes in the works on opioid crisis

The federal government is eyeing a number of legislative changes to address Canada's opioid crisis, Health Minister Jane Philpott said Saturday at the conclusion of a summit examining the issue. The federal government is actively trying to turn the tide of the crisis, Philpott added, noting it will require a whole-of-government approach. "This is a topic I have been working with alongside the minister for public safety, the minister of justice and the minister of foreign affairs," she said. "In the coming months, there are a number of pieces of legislation that are going to address matters related to the opioid crisis and certainly we will do the work necessary." Addiction, overdose and deaths related to opioid use were the focus of discussions for health experts and ministers who gathered in Ottawa for a two-day summit to look at a national approach. On Saturday, B.C. Health Minister Terry Lake urged the federal government to waste no time in taking additional action to address Canada's opioid crisis, including setting up a nationally coordinated surveillance system to track overdoses and other drug-related harm. The province also wants the federal government to look at tools to stop the flow of fentanyl from China by stepping up diplomatic negotiations. "They need to properly equip the Canadian Border Services Agency and the RCMP with the tools and resources needed for border control and to get fentanyl off the streets," Lake said in a Saturday statement. British Columbia says 622 overdose deaths have happened in that province since January - more than double the number of people who died in car crashes last year. Waterloo Region Record, A3 (CTV News) (2016-11-21); Postmedia Network (Toronto Sun, A11; The Province, Vancouver Sun); Canadian Press (The Province, Vancouver Sun, Toronto Star, Times Colonist) (2016-11-20); Canadian Press(Maclean's; iPolitics; Global News; CTV News; Chronicle Herald); CBC News; Presse Canadienne (La Presse) (2016-11-19)

'This is all a work in progress'

The first time Donovan Locke had to perform an intervention with an aspiring extremist, the 14-yearold in question had been caught spouting white supremacist views at a Toronto high school. The parents were

notified, along with the Toronto Police Service, where Locke is an acting staff sergeant and a coordinator of a new project attempting to address radicalization in Canada's largest city... After police shot Islamic State of Iraq and the Levant supporter Aaron Driver as he was leaving his home in Strathroy, Ont., to conduct a suicide bombing Aug. 10, Public Safety Minister Ralph Goodale said there was *"little national coherence"* to counter-radicalization efforts in Canada and re-committed the government to opening an office to co-ordinate them nationally. Toronto has been quietly experimenting with its own approach, the National Post has learned. Launched as a pilot project by the Toronto police and the city, it has been kept under wraps until now. But in interviews with the Post, key officials spoke for the first time about what they were doing. "One of the things we chose to do here was not to engage the media," said James Ramer, Toronto's deputy police chief. But, "We're at the point now that we do want to advertise it." National Post, A6 (2016-11-19)

Taxpayers would have to foot bill for new high-tech police powers, wireless industry says
Canada's top telecommunications industry group says any government move to force its members to install equipment to intercept digital traffic and store data to aid police investigations would have to be covered by taxpayers. "We have always submitted that there should be a mechanism for the government to cover the costs or possibly law enforcement," said Kurt Eby, director of regulatory affairs and government relations for the Canadian Wireless Telecommunications Association. "Every time the government looks to add a layer such as this, there is going to be cost incurred." The federal government is holding public consultations on Canada's Anti-Terrorism Act, which includes proposals for new investigative powers for police to gather digital evidence... RCMP Commissioner Bob Paulson says nearly 70 per cent of telecommunications companies can't comply with interception orders from the courts. CBC News (2016-11-19)

ComicCon could help you become a spy
Do you enjoy going to ComicCon ? What about giveaway sunglasses or free popcorn ? More importantly: Can you keep a secret ? Then a job as a digital spy might just be for you. Or, at least, that ' s what the Communications Security Establishment (CSE) has in mind as it seeks the best and brightesttechies. An old-fashioned popcorn machine and free pairs of CSE-branded shades were part of the display at a government job fair Thursday at Ottawa ' s Shaw Centre. At the event, where the hashtag # secureyourfuture was prominently displayed, other agencies - including Public Safety Canada, the Canadian Security Intelligence Service (CSIS), the Canadian Forces, the Correctional Service of Canada and the Canada Border Security Agency - competed to woo curious job-hunters, more than one of whom was spotted eating a banana. Though the Royal Canadian Mounted Police displayed Batman-like combat gear on a mannequin, it was, subjectively, hard to compete with CSE ' s popcorn and shades. A CSE rep explained the agency had tried recruiting at a ComicCon event for the first time in Montreal this summer - you know, because a lot of, uh, tech-savvy people attend ComicCon. Postmedia Network (London Free Press, N4; Calgary Herald, National Post, * National Post) (2016-11-19)

Your cellphone password could hold the key in legal battle over collecting evidence
Here's the scenario: Police believe there is evidence on your cellphone or computer that could assist them in a criminal investigation. They ask that you provide your password or encryption key so they can search for clues. Currently, there is no law compelling you to comply with that request. But police in Canada, frustrated by evidence trails that lead to digital dead ends, are calling for a law that would make it a criminal offence to say no to a police officer carrying a judicial warrant. It's an idea designed to accomplish through a legal order what police are increasingly unable to accomplish technologically — getting inside digital devices containing what they believe is crucial evidence in criminal investigations. "It's a very radical proposal in Canadian law," said Micheal Vonn, executive director of the B.C. Civil Liberties Association. "It changes the basic nature of how we go about achieving the ends of criminal investigation, by compelling the person who is under investigation to participate in the investigation." Many privacy advocates — and even some in law enforcement — call the idea an abuse of both privacy protections and the rights of Canadians against self-incrimination. Police supporters counter that public safety — and the ability of police to respond to serious crimes — is already being dramatically eroded by disappearing evidence. Liberal Public Safety Minister Ralph Goodale: "(Police) are certainly concerned about the effect of new technology in an age accelerating digitization. They're concerned whether or not their legal tools are sufficient to cope with what they now have to deal with . . . .

Others in the academic community, in the open media community, have put forward the contrary opinion. And that's what this consultation is intended to solicit, and we will have to weigh all of that carefully to make sure that in our response, we produce a position that is consistent with Canadian's expectations." Toronto Star/CBC News (2016-11-18)

The McAdam file: Bribery, Chinese gangsters and betrayal
Brian McAdam was a seasoned Canadian diplomat when he was posted to Hong Kong in 1989. He became the high commission's immigration control officer two years later, and soon uncovered what he believed was a major scandal. Members of Chinese criminal gangs, known as Triads, were applying to enter Canada as entrepreneurs under the country's business immigration program. And many were getting visas. "What was very, very disturbing to me was I kept seeing all these connections of these people to certain people — politicians — in Canada, and the odd name in our embassy," McAdam says. He started writing reports — there were ultimately 32 — documenting the names of the gangsters who were getting into the country and related concerns. The reports caused panic in the immigration minister's office and at headquarters in Ottawa, McAdam alleges. "I was exposing incredible negligence. I was exposing incredible corruption. And I was exposing the flaws in our whole immigration system. "People in Ottawa didn't want to investigate anything. They just shut their eyes to everything." Most of his reports were destroyed, he says. McAdam returned to Ottawa in 1993, lured by the promise of a job in a new organized crime unit at Foreign Affairs. But when he showed up for work, the job didn't exist. He alleges the personnel manager urged him to take a retirement package, though he was just 51. Days later, he went on sick leave and never returned to work. In 1996, RCMP Cpl. Robert Read began investigating McAdam's allegations that employees at the Hong Kong mission had received bribes and that Triad criminal gangs had infiltrated an immigration computer system. After finding gaping holes in earlier RCMP investigations, Read urged his superiors to authorize a thorough investigation, but was taken off the case. Concerned that his bosses were suppressing his findings, Read went to the media with his concerns in 1999, which led to his dismissal from the RCMP in 2002. McAdam's allegations also sparked a joint RCMP-CSIS investigation known as Project Sidewinder, which probed the threat posed by the purchase of Canadian companies by Triad members or associates with links to the Chinese Intelligence Service. Ottawa Citizen (2016-11-18)

Why Spy on Reporters When You Can Spy on CEOs?
An opinion piece states, "Canadians have been shocked to learn that police in this country have for the second time this year admitted to spying on reporters. What makes the recent disclosures most ironic is not that police officers were the ultimate targets, or that spying was approved in the absence of an actual judge—but that much of the meta-data sought by Montreal police may have already existed on a government server, and could have been obtained without a warrant, thanks to the enactment of the Anti-Terrorism Act (known as "Bill C-51"). In fact, in his latest annual report to Parliament, Canada's Privacy Commissioner identified 58 such instances where Canadians' information was collected and shared without prior judicial approval in the first six months of this year alone. Whether it's the Communications Security Establishment (CSE) illegally collecting and sharing Canadians' metadata with foreign intelligence partners, the RCMP, Vancouver, and Toronto Police departments each individually mopping up entire city blocks full of cell phone information with Stingray surveillance devices, or the Canadian Security Intelligence Service (CSIS) building a secret database and intentionally concealing its existence from Federal Court Judges, Bill C-51 has emboldened all manner of police and security services to push the envelope and end-run Canada's Privacy Act." VICE News (2016-11-18)

Money-laundering watchdog cites 'significant' deficiencies at 100-plus B.C. real estate firms
Canada's anti-money laundering watchdog found "significant" or "very significant" levels of non-compliance at more than half of the B.C. real estate companies it examined over a four-and-a-half year period, its records show. The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the federal agency mandated to detect and combat money laundering, examined about 220 real estate companies in B.C. between 2012 and mid-2016, finding 112 companies with "significant" levels of non-compliance and five with "very significant" non-compliance, according to records obtained by Postmedia News through an access to information request. In the past year, FINTRAC has ramped up scrutiny of real estate - particularly in B.C. In an operational brief this week intended for banks and real estate professionals, the agency highlighted the Canadian housing market's vulnerability to money laundering.

The 12-page FINTRAC brief also notes the "minimal" filing of suspicious transaction reports in Canadian real estate, with 127 reports filed on five million sales over 10 years. Vancouver Sun (2016-11-18)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Changing perceptions: How this Winnipeg artist's dramatic billboards aid police training
In early 2015, KC Adams' black and white portraits of indigenous people hung around the city on billboards, bus shacks and bulletin boards, demanding our attention. The twinned photos featured people scowling and hurt as Adams hurled racial insults at them, then smiling and radiant as she reminded them of happier times. The models self-selected their own labels on their second portraits: epithets like mother, dream chaser, soccer player and taxpayer... Metro: Do you have plans for a Perception round two? Do you think our city could still use more of a push in that direction? Adams: "I think we need to be constantly reminded about our responsibilities on truth and reconciliation and I think the work could potentially... be used as a tool maybe in educational systems. Interestingly enough, I was contacted in British Columbia by the RCMP training unit where they train their new recruits. Metro News (2016-11-20)

RCMP Biography Will Please Mountie Fans And Concern Critics
To hear biographer George Garrett tell it, Stirling McNeil was a character straight out of a 1930s movie. The handsome hero, a Manitoba kid, loses his factory job to a Depression-era layoffand joins the RCMP. He goes on to patrol the frozen north on 700-milelong dog sled trails, bringing sometimes rough but always fair justice to the trappers, miners and First Nations residents of Canada's north while establishing a reputation for even-handed treatment of all, old world courtliness and devotion to the law and the RCMP. He pioneers the use of airplanes for law enforcement in the north and rubs shoulders with a colourful gallery of fellow officers, felons and raffish local characters. Vancouver Sun, E7 (2016-11-19)

Mounties won't be charged after Surrey suspect suffers broken hip
The Criminal Justice Branch says three RCMP officers will not be charged after a suspect in Surrey suffered a broken hip. The branch says police were called to a basement suite in on Feb. 28, 2015, after reports that a tenant was "trashing" the unit. A statement from the branch says Mounties found an apparently intoxicated man who was naked, bleeding and swearing in a room littered with broken glass and furniture. The branch says the man initially complied with police and agreed to leave the residence, but then began pushing the officers who had to take him to the ground so he could be restrained. The statement says suspect's nose and forehead were cut after his head hit the ground, but an injury to his right hip wasn't immediately obvious, though it was later determined that he needed surgery. Potential charges of assault were considered, but the branch says the available evidence does not meet the standards to approve any charges. Canadian Press (Vancouver Sun; Info News) (2016-11-19)

Kamloops Mountie honoured for saving the life of his brother in blue
A member of the Kamloops RCMP was among 56 men and women who were recognized at the annual Police Awards in Victoria last night. Cst. Steve Marcil was honoured by Lieutenant Governor Judith Guichon and Solicitor General Mike Morris for his actions in saving the life of Corporal J.R. Michaud, who was shot during a traffic stop two years ago in Batchelor Heights. Marcil says, while the incident was unusual, it's all in a day's work for an RCMP member. CFJC (2016-11-18)

D'ex-agents de la GRC estiment avoir subi des représailles à la suite de gestes déplacés de supérieurs
Deux anciens agents de la Gendarmerie royale du Canada (GRC) dénoncent à leur tour les injustices du système de discipline interne du corps policier. En plus des disparités entre les infractions commises et les sanctions reçues, ils affirment que les plaignants sont souvent traités comme des parias par la GRC et que des plaintes infondées seraient parfois utilisées pour se venger entre employés. Il y a quelques années, la carrière de Linda Davidson dans la GRC semblait atteindre des sommets. Elle avait même été affectée à la protection du premier ministre de l'époque Stephen Harper, à Ottawa. Mais elle soutient, dans son témoignage à Radio-Canada/CBC, avoir plutôt vécu l'enfer, victime d'une agression sexuelle au travail par l'un de ses supérieurs. Radio-Canada (2016-11-18)

Un premier groupe d'entraide pour les veufs et les veuves à Moncton
Il est difficile d'imaginer ce qu'on peut ressentir à la perte d'un conjoint. Trouver un groupe d'entraide afin de mieux vivre son deuil est vital pour certains. Or, ce genre de groupe n'existait pas à Moncton jusqu'à aujourd'hui. Soaring Spirits Moncton Vivre avec le deuil a été mis sur pied par deux veuves, Christelle Léger et Nadine Larche. Mme Larche a perdu son conjoint, il y a plus de deux ans, lors de la fusillade du 4 juin 2014 à Moncton. Pour la mère de trois filles, le deuil est encore une épreuve difficile à surmonter, et ce, même si les choses semblent s'améliorer. «On peut dire que ça va mieux. Évidemment, j'ai encore des journées très difficiles. Comme maintenant, j'ai une petite fille malade à la maison toute seule. Il y a encore des journées difficiles, mais ça va mieux, ça va mieux», a confié Mme Larche à l'Acadie Nouvelle. Nadine Larche a été en mesure de trouver des appuis dans la grande famille de la GRC, rencontrant, lors de cérémonies, d'autres endeuillés avec qui elle a été capable de tisser des liens. Acadie Nouvelle (2016-11-18)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

Marijuana tycoon says Canopy could survive 25 per cent Trudeau tax rate
The head of Canada's first publicly-listed marijuana producer said his company could still turn a profit even if Prime Minister Justin Trudeau's government decides to tax legal recreational weed at rates as high as 25 per cent. A task force is due to report this month on how Canada can build a legal weed market that squeezes out organized crime, protects minors, ensures quality and adds to revenue through taxes. Bruce Linton, chief executive officer of Canopy Growth Corp., says lawmakers will probably choose to control the distribution of recreational marijuana through government-run outlets such as liquor stores. "We can probably carry a tax burden of 25 per cent or so and end up in the consumers' hands on a still cost-competitive basis, with a superior product," Linton said in an interview at Bloomberg's Ottawa newsroom. Canopy, based in Smiths Falls, Ont., became the first marijuana producer to trade on a major North American stock exchange when it graduated to the Toronto Stock Exchange in July. It became the first publicly traded Canadian producer of the drug in 2014. The company's share price more than doubled this month, bringing its market value past $1.6 billion, on better-than-expected earnings and after U.S. elections widened the scope for legal marijuana. Canopy already produces medical marijuana under an existing legal regime. Linton says the company, which operates out of a former chocolate factory, can shift production to serve the recreational market when Trudeau's government makes that legal. Part of the appeal of the legal variety will be its quality control, Linton says. "When it's lawfully available from a reliable supply chain, which we know we can trust and believe in, there are a lot of people who might discontinue the use of say a glass of wine or a beer and try this." Canopy can also generate new formulations of medical marijuana to sell through pharmacies as legalization moves ahead, Linton said. Loblaw Cos., owner of the Shoppers Drug Mart pharmacy chain, has signalled it wants to sell medical marijuana. Postmedia Network (Leader-Post, B6, StarPhoenix, Vancouver Sun)

Ottawa pot dispensaries back in business after police raids
At least two illegal marijuana dispensaries in Ottawa have reopened after police raids closed them down earlier this month. Seven shops were shut down following complaints about the growing number of dispensaries in the city. Two Green Tree Medical Dispensary locations visited by CBC News on Sunday were open for business, although shop attendants refused to provide any sort of comment. "It's a reality," said Rideau-Vanier Coun. Mathieu Fleury. "Until we have the federal framework in place and better coordination provincially ... it's going to be that game of closing and opening." Fleury said he knows there are concerns in his ward about the illegal dispensaries and their effect on the community and people shouldn't stop giving their input on the issue because some of the dispensaries have reopened. "We have to continue to monitor, to enforce. Especially based on community complaints and community feedback and information gathering." On Nov. 4, two marijuana shops in Fleury's ward were raided by police but that hasn't deterred others from getting into the business. He said he's aware of two new shops that have opened recently but still thinks the raids were a good idea. "There's huge gains from the raids that have been put in place. I know that's contentious to say but the perception that these locations were offering legal marijuana is now clear that it is not. That element has been clarified." The federal government has promised to introduce legislation to legalize marijuana by the spring of 2017, but the possession, production and trafficking of marijuana remains illegal. CBC News

Feds closer to new policy on medical pot for vets
The Trudeau government is getting closer to having a new policy on medicinal marijuana for our veterans, who take the drug to treat conditions like PTSD. The veterans affairs department has been reviewing the issue of medical pot after concerns were raised earlier this year that the department is compensating vets for up to ten grams of marijuana a day. News 1130

Legal pot in Canada could sell for $5 a gram — or less
Uncle Ike's Budget Bud is the cheapest pot we've found anywhere. A product line of a Seattle, Wa.-based marijuana retailer, it lives up to its name at US$99 an ounce. That works out to $4.76 a gram Canadian, and it would put the cost of a joint in the $1.50-$2 range. Global News (2016-11-20)

Legalizing marijuana isn't apt to bring a windfall for governments
An opinion piece states, "Several economic myths have surrounded the legalization of marijuana. This has maintained the illusion that it would be a bonanza for federal and provincial treasuries because of the supposed enormous tax revenues that legalization would generate. The Parliamentary Budget Office in Ottawa is to be congratulated for blowing up some of these myths in its report, published this month,on projected marijuana tax revenues following legalization in Canada in 2017 or 2018..." Montreal Gazette (2016-11-20)

Du pot légal près de chez vous
D'ici à ce que le Canada arrive à la conclusion de sa longue démarche visant à légaliser la marijuana, les amateurs de cannabis du Québec, plus précisément ceux de la Beauce, pourraient avoir accès à une source légale de marijuana à des fins récréatives à quelques minutes de chez eux. La Presse (Le Soleil, 3; Le Quotidien) (2016-11-20)

Où acheter la marijuana une fois sa consommation légalisée?
Si la consommation de cannabis devient légale au Canada, la vente de cette substance devrait être bien encadrée, suggère un nouveau rapport de l'Institut national de santé publique du Québec. « On ne peut pas imaginer de distribution libre à but lucratif comme n'importe quel produit qu'on vend », affirme Réal Morin, médecin-conseil et coordonnateur du chantier cannabis à l'Institut. Le Dr Morin croit que la vente du cannabis devrait être confiée à une « agence gouvernementale de type monopole d'État ». En entrevue à l'émission 360 PM, il a précisé que cette organisation devrait avoir la prévention comme principale préoccupation et non pas une mission économique comme c'est le cas d'autres sociétés d'État. Radio-Canada (2016-11-20)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

RCMP overstating 'surveillance lag'
An opinion piece states, "The RCMP has been lobbying the government behind the scenes for increased surveillance powers on the faulty premise that their investigative powers are lagging behind those foreign police services. The centre piece of the RCMP's pitch is captured in an infographic that purports to show that foreign governments are legislating powers that are more responsive to investigative challenges posed by the digital world. On the basis of this comparison, the RCMP appears to have persuaded the federal government to transform a process intended to curb the excesses of Bill C-51 into one dominated by proposals for additional surveillance powers. The RCMP's lobbying effort misleadingly leaves an impression that Canadian law enforcement efforts are being confounded by digital activities. For example, in its comparative sample (which includes Australia, New Zealand, the United Kingdom and the United States) Canada is presented as the sole country lacking a legal obligation compelling Internet companies to design their services around state surveillance requirements. In fact, Canada already imposes this obligation on mobile service providers in spectrum licences. Furthermore, communications providers demonstrated to the government in 2013 that their networks are generally becoming intercept-ready even in the absence of a legal obligation to do so. The RCMP also misrepresents the legality of foreign surveillance powers. For example, a proposal to require the retention of communication interaction data is presented as "under discussion" in the U.K. In fact, this power has been found unconstitutional by the

U.K. divisional court and is currently on appeal to the EU's highest court, which has already struck down its predecessor legislation." Toronto Star, A11

Native policing

A letter to the editor states, "Re Either Fund Native Police, Or End Them (editorial, Nov. 15): While I expect the editorial questioning the skills and capacity of "native police" after the in-custody suicide of Lena Anderson was well-intentioned, may I point out that many indigenous Canadians have died in the custody of well-funded mainstream non-indigenous police forces? Take for example, Solomon Uyarasuk, a young Inuk man in Iglulik who, after being taken into RCMP custody in 2012, died alone in his cell where he had been left naked, but for his belt. Despite inquiry after inquiry into the deaths of indigenous people in custody, many of which have stated that hanging points should not exist in cells, he was left alone with a belt and a hanging point. Clearly, upstream solutions to complex mental health and societal problems are needed, but these repeated in custody scenarios are appallingly grievous." Globe and Mail, A10

Canada's national security oversight is among the weakest in the world: former human rights advocate

An opinion piece by Steven Zhou, Toronto writer and human rights advocate, states, "There doesn't seem to be much that Canada's intelligence and spy agencies can't do these days-and that includes breaking the law. While much of world remains anxious about the future of a Donald Trump presidency, Canadians should refocus their attention back home, and they should start with the country's bloated national security state. Experience shows that most of a country's establishment systems have likely transcended partisan lines and will remain immune to changes in political personality. National security seems to be one of these categories and its pervasive entrenchment within post-9/11 democracies has been demonstrated both in and outside of American borders. The Canadian security apparatus is a good example of how partisan changes usually have minimal impact on the larger system. There is no Canadian Edward Snowden to shed light on the extensive surveillance and policing machinations of CSIS or the Communication Security Establishment (CSE)... A federal court made national news last week by rebuking CSIS for essentially hiding a giant database full of private information belonging to law-abiding Canadians who pose no threat to public safety. Its watchdog group, the Security Intelligence Review Committee (SIRC), had previously asked CSIS to disclose the existence and full capabilities of this database to the courts, but the spy agency refused and kept things secret for a whole decade. The revelation has been an embarrassment for Public Safety Minister Ralph Goodale, who's been conducting a national consultation on how to reform Canada's security regimes. When asked why CSIS kept the database a secret from the courts, agency director Michel Coulombe simply said that he had no good explanation... There's precisely one person, the CSE Commissioner Jean-Pierre Plouffe, who's supposed to overlook the entire slew of intelligence-related activities that are carried out by the agency on a regular basis... Minister Goodale has promised swift action, but until those words actually manifest themselves into serious institutional change, then Canada will still remain the country with perhaps the weakest national security oversight in the Western world." CBC News (2016-11-20)

Give all officers training in mental-health skills

A letter to the editor states, "Re: "Police seek budget for mental health officers," Nov. 17. We do not need two mental health officers, we need the existing force, and all new recruits, trained in basic mental health and communication skills, as well as violence prevention. You need to have coverage for all times of the day, and two officers wouldn't cut it. As most normal police/civilian interactions are stressful, these courses would help here as well. With proper training, willing officers can help change the stigma of mental illness..." Times Colonist (2016-11-20)

Ottawa should be careful on expanded police powers

An editorial states, "Crime, like everything else, has been transformed by the digital age. Fraudsters, child pornographers and terrorists, among others, are becoming ever more expert in using digital technologies to commit their offences and cover their tracks. Not surprisingly, this has created new challenges for law enforcement. Police chiefs across Canada claim investigators do not have the tools to keep up. Many say concerns about privacy have scuttled their attempts to convince politicians to provide them with the cyber-surveillance powers they need to do their job. As Bob Paulson, commissioner of the Royal Canadian

Mounted Police, puts it, "We're losing our ability, if we haven't lost it entirely, to bring the traditional investigative response to technologically facilitated crime because of the misunderstanding, in my view, of the privacy threat." This week, Paulson shared with reporters from the Star and CBC News case files he says demonstrate the obstacles his force faces, an attempt to help the public understand the need for new police powers the federal government is currently floating... And that's to say nothing of security agencies themselves. The recent revelation that the Canadian Security Intelligence Service illegally spied on people suspected of no wrongdoing is a timely reminder that expanded powers must be accompanied by expanded oversight... In recent decades, and in particular with the passing of the overreaching Bill C-51, the trend has been to expand the powers of the security establishment without offering counterbalancing privacy protections or safeguards against abuse... The public consultation now underway won't mean much unless Canadians understand, yes, the challenges police face, but also the risks of their proposed remedies, including the threats to personal privacy and security posed by an ever-expanding surveillance state." Toronto Star (2016-11-18)

Ottawa should be careful on expanded police powers
An editorial states "Crime, like everything else, has been transformed by the digital age. Fraudsters, child pornographers and terrorists, among others, are becoming ever more expert in using digital technologies to commit their offences and cover their tracks. Not surprisingly, this has created new challenges for law enforcement. Police chiefs across Canada claim investigators do not have the tools to keep up. Many say concerns about privacy have scuttled their attempts to convince politicians to provide them with the cyber-surveillance powers they need to do their job. As Bob Paulson, commissioner of the Royal Canadian Mounted Police, puts it, 'We're losing our ability, if we haven't lost it entirely, to bring the traditional investigative response to technologically facilitated crime because of the misunderstanding, in my view, of the privacy threat.' This week, Paulson shared with reporters from the Star and CBC News case files he says demonstrate the obstacles his force faces, an attempt to help the public understand the need for new police powers the federal government is currently floating. The cases are no doubt disturbing, tales of child abusers and wannabe terrorists evading justice. But while they clearly illustrate new and thorny police challenges, they do not establish that the requested powers are necessary or proportionate or to what extent they would endanger privacy or even weaken security. Paulson is right that an informed public discussion about these difficult issues is necessary and that the evolving nature of cyber-crime is an important part of that discussion. But a closer look at the requested powers shows that Paulson's story is not the whole story." Toronto Star (2016-11-18)

The RCMP needs you scared - and the media seems happy to help
An opinion piece states "Long before email, metadata and GPS tracking, King Louis XIII's hatchetman Cardinal Richelieu said: 'If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged.' Nothing's changed. The RCMP is back at the back door, lobbying the government for greater powers to access digital evidence - and now they're using the media to make their case. Recently, the RCMP self-selected 10 investigation files and fed summaries to the CBC and Toronto Star. Details that could compromise ongoing investigations (or be used by journalists to fact-check) were redacted. Both media outlets dutifully gave the Mounties the headline they wanted - one about how child predators, drug gangs and terrorists are escaping justice. The RCMP's proposed solution is, of course, more police power. It's always more police power. The RCMP wants laws that would compel suspects to hand over passwords, grant warrantless access to subscriber information and require telecommunication providers to build back-door intercept capabilities into their networks." iPolitics (2016-11-18)

OTHER / AUTRES

Pas d'accusations à Val-d'Or, deux à Schefferville, le DPCP s'explique
Jeudi, il a été révélé qu'Alain Juneau a été accusé d'agressions sexuelles contre des femmes autochtones ; des gestes qu'il aurait posés à Schefferville, entre 1992 et 1994, au moment où il travaillait comme policier pour la Sûreté du Québec (SQ) sur la Côte-Nord. Le DPCP devrait en faire l'annonce dans sa conférence de presse. Et il appert aussi qu'un policier autochtone de Schefferville ferait l'objet d'accusations, selon ce qu'a appris Radio-Canada. Octobre 2015, le Québec sous le choc. Rappelons

qu'en octobre 2015, la diffusion de témoignages accablants de femmes autochtones de Val-d'Or, disant avoir été victimes de violence sexuelle et d'abus de pouvoir de la part de policiers de la SQ, avait secoué l'ensemble du Québec. Ces révélations de l'émission Enquête de Radio-Canada avaient conduit le ministère de la Sécurité publique du Québec à confier au Service de police de la Ville de Montréal (SPVM) le soin d'enquêter sur les comportements allégués d'agents de la SQ. Le DPCP a par la suite analysé 37 dossiers qui lui avaient été remis par le SPVM. Presse canadienne (Radio-Canada, Huffington Post); CBC News; TVA Nouvelles; La Presse; Le Devoir (2016-11-18); Globe and Mail, A3; Leader-Post, N3; Ottawa Sun, A16; Postmedia Network (London Free Press, N3; Montreal Gazette, Edmonton Journal, Windsor Star, Vancouver Sun, Calgary Herald); * Le Droit, 29 (2016-11-19)

Hamilton's horror - Cops not naming names in child abuse scandal telling
One lone name stood out on the press release outlining those charged in the monstrous serial molestation of a little Hamilton girl. Can I remind you, she's seven. And while he was not directly connected to the little girl, the only name on that release was Geoffrey Burnet. And so far, he's the only one we have. According to cops, the girl's mother's boyfriend was allegedly offering her for sale on Craigslist. Seven people were arrested - no names. In the case of the mom and her boyfriend it's easy to see why there were no names. Postmedia Network (Winnipeg Sun, A7; Calgary Sun, Edmonton Sun) (2016-11-20)

Surge in domestic handgun trafficking
Danny Santapaga, a self-employed financial adviser, bought 14 guns on 10 different occasions over seven months. Plumber Graham Jovanovic purchased nine firearms over five weeks. University student Justin Green obtained 23 handguns during a 22-month period, including 15 from one store. Security guard Andrew Winchester acquired 47 handguns in a six-month buying binge. Hamilton Spectator (2016-11-19)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 21, 2016 / le 21 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Digital encryption is here to stay, says report from U.S. lawmakers
As Canadian police push for more power in the online world, documents obtained by the Star suggest that privacy-protecting encryption software is here to stay. A memo prepared for Daniel Therrien, the federal privacy commissioner, stated it would be difficult for any one country to weaken or ban encryption technology. The document, obtained under access to information law, summarizes a report from the U.S. committee on homeland security. "Encryption tools very much are now ubiquitous, globally distributed and irrevocable, which plainly no piece of domestic regulation or lawmaking will undo, given that two-thirds of encryption products are produced and sold by non-U.S. firms," the memo reads. In other words, if the bad guys want to hide their tracks, they'll have plenty of options even if Canada or the U.S. attempts to weaken or ban encryption. The RCMP are making a very public push for more powers to obtain Canadians' private information from telecommunication companies and to decode encrypted messages. RCMP Commissioner Bob Paulson told a joint Star/CBC investigation it has reached the point where if a citizen is a victim of a crime online, he's not sure the Mounties can help. But the report from the U.S. homeland security committee, summarized for Therrien in the memo, states that weakening encryption would probably compromise public safety rather than improve it. North of the border, meanwhile, the federal Liberals are examining Canada's national security framework, including such issues as encryption and warrantless access to Canadians' private information. Public Safety Minister Ralph Goodale, who is leading that consultation, has remained neutral on the issue pending the results of the exercise. "We have invited everyone with a view to come forward with their perspective. "Obviously, the police perspective is being advanced with a good deal of vigour and enthusiasm from their perspective of law enforcement," Goodale told the Star last week. Toronto Star, A1

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

'We've always been seen as a threat,' says former N.W.T. premier of RCMP surveillance revelations

A recently revealed program of police surveillance across Canada is "alarming" and a "threat to our own security," says former **N.W.T.** premier Stephen Kakfwi. He's "not surprised," however, to hear that more than 300 protesters, 89 of whom are Indigenous, were being watched by RCMP as part of surveillance program called Project SITKA, launched in 2014...Police Response. "When the RCMP is in receipt of information that indicates an individual or individuals are involved in a crime or may pose a threat to the safety and security of others, we are duty-bound to investigate. The RCMP did not specifically target Indigenous protestors," writes Cpl. Annie Delisle, Media Relations Officer for the RCMP. CBC News (2016-11-20)

Mi'kmaq woman concerned about Project SITKA

A Mi'Kmaq woman from **Elsipogtog** is concerned that her name is on a "watch list" compiled by RCMP intelligence services in the wake of a year-long investigation of dozens of Indigenous protesters, called Project SITKA. Amy Sock, a former defence attorney, mother, and an active member of Idle No More worries her time on the front lines of anti-shale gas protests in 2013 may have landed her on the list, although the RCMP refuses to say whether she is or not. CBC News (2016-11-20)

Man wanted by RCMP arrested on Muskowekwan First Nation

A man who was wanted by the RCMP on several outstanding warrants has been arrested. Darryl Raymond Longman was located by **Punnichy** RCMP at a residence on Muskowekwan First Nation on Sunday.He was taken into custody at 3 p.m, according to a press release. On Nov. 19, the RCMP had issued a release asking for information on Longman's whereabouts. The RCMP said Longman was known to frequent Regina, Muskowekwan First Nation and George Gordon First Nation. On Oct. 3, 2015 Longman was arrested and charged with dangerous operation of a vehicle, driving while being chased by police, driving drunk, refusing to provide a breath sample, driving without a drivers license and stealing a vehicle. Longman also had additional outstanding warrants for his arrest in connection with an incident which happened on June 6. He was charged with assault, assault with a weapon, uttering threats and failure to comply. Leader-Post; CTV News (2016-11-20)

Surrey RCMP searching for missing 15-year-old girl

Surrey RCMP are asking for the public's assistance in locating a missing 15-year-old girl. Police say Trinity McKenzie was last seen on Friday, Nov. 7 at home in Surrey. Family and police are now concerned for her health and well-being. Global News (2016-11-20)

Red Deer's top cop talks about tackling drugs, organized crime

It's no secret that drugs and organized crime are driving much of the crime activity in Red Deer. In part two of our feature story, new **Red Deer** RCMP Superintendent Ken Foster says he is condifent these troublesome issues can be dealt with effectively. Red Deer News Now (2016-11-19)

RCMP investigate daylight shooting in Burnaby

There is a heavy police presence in a south **Burnaby** neighbourhood following reports of a shooting. Nearby residents reported hearing shots fired around 11:30 a.m. One victim has been taken to Royal Columbian Hospital, and RCMP say a possible second victim may have also been treated in hospital. The incident occurred in the 7100 block of 14th Avenue, situated several blocks from the Edmonds SkyTrain tation and one block from an elementary school. Global News; CKNW (2016-11-19)

Punnichy, Sask. RCMP on lookout for 2 wanted men

Saskatchewan RCMP is asking the public for help locating two separate wanted men. Darryl Raymond Longman, 48, has outstanding warrants for his arrest. On Oct. 3, 2015, he was charged with Criminal Code offences such as operation of a motor vehicle while being pursued by a peace officer operating a

motor vehicle, impaired operation of a motor vehicle and taking a motor vehicle without consent. Global News; CTV News; CBC News; Leader-Post (2016-11-19)

RCMP request that Albertans please report their moldering dynamite
There may be something explosive lurking amongst the rolls of baler twine and tractor parts in that old barn down on the farm. According to **Alberta** RCMP, there is a large but unquantified amount of degraded and deteriorated dynamite on properties across the province as a result of historic rules that permitted farmers and ranchers easy access to explosives. Edmonton Journal; Agence QMI (TVA Nouvelle) (2016-11-19)

Four face drug charges following police search in Harbour Landing
Four adults are facing cocaine trafficking charges after police executed a Controlled Drugs and Substances Act search warrant in **Regina**'s Harbour Landing neighbourhood Wednesday. Regina's Combined Forces Special Enforcement Unit (CFSEU), with the assistance of the RCMP Integrated Organized Crime Unit, seized cocaine, cash and a loaded hand gun. Danieol Johnson, Kendall Robinson, Ali Mahdi and Mohammed Osman are all charged with possession of cocaine for the purpose of trafficking and proceeds of crime over $5,000. Leader-Post, A4 (2016-11-19)

Break-in at Manitoba Hydro compound
Steinbach RCMP are currently investigating a recent report of a break, enter and theft to the Manitoba Hydro compound located in the City of Steinbach, Manitoba. My Steinbach (2016-11-19)

Codiac RCMP locate both missing persons in Moncton
Police say both the 17-year-old boy and 23-year-old woman reported missing Nov. 17 in separate incidents in **Moncton** have been located. The boy had left the Moncton City Hospital of his own accord that day. The woman was located Saturday afternoon. Codiac RCMP thanked the public for their assistance. CBC News (2016-11-19)

Leduc RCMP appeal to public for help finding woman missing since Nov. 3
Leduc RCMP issued a plea to the public for information on a missing woman Saturday. Mounties said Deanna Millington left her family home in Leduc, Alta. on Nov. 3 and has not been seen since. Police said they are concerned for the woman's well being. Global News; CTV News (2016-11-19)

RCMP warn of email fraud
The RCMP has issued a warning about a recent email scam targeting businesses that perform wire transfers. That scam often involves businesses whose executives' email accounts are compromised or imitated. The fraudster then sends emails to an unsuspecting employee telling them to wire large sums of money to foreign accounts. Charlottetown Guardian, A3 (2016-11-19)

Inquiry into Don Dunphy death delayed by anonymous letter
Police are asking for the public's help in finding the author of an anonymous letter about the shooting death of Donald Dunphy. A press release from the RCMP says they found out about the letter on the evening of Nov. 7 from the inquiry into Dunphy's death and began investigating its contents and source the next morning. "The RCMP was informed by the commission of inquiry respecting the death of Donald Dunphy the new information in the form of an anonymous letter had come forward regarding the death of Mr. Dunphy. The following morning the RCMP obtained the letter and began an investigation into its origins and content," said RCMP Superintendent Pat Cahill at a news conference Friday. CBC News; VOCM News (2016-11-18)

RCMP testify in Burnaby school bookkeeper's trial
Police decided to focus on investigating questionable cheques instead of missing cash at Alpha Secondary between 2008 and 2010 because cash is harder to track, according to the RCMP's chief investigator in the case. Const. Anna Taylor testified Wednesday at the trial of former Alpha Secondary bookkeeper Jodi Fingarsen, who is accused of defrauding her **Burnaby** school of about $67,000 using cheques either fraudulently generated, signed or deposited. During her investigation, Taylor interviewed school staff who also complained of missing cash collected for things like school trips, dry grad

celebrations and Advanced Placement exams. "They did bring up the cash as well," said Taylor, "but from the police perspective, tracing physical cash is more difficult." Defence lawyer John Banks, however, suggested Taylor didn't investigate the missing cash because Alpha's system for collecting and accounting for cash was flawed. Burnaby Now (2016-11-18)

Swift Current RCMP looking for two missing teens
Swift Current Municipal RCMP are looking for two missing teenagers who haven't returned home or attended school this past week. Fourteen-year-old Amber Padley was reported missing to RCMP on Wednesday, Nov. 9. She's described as Caucasian, five feet six inches tall and 120 pounds with brown hair and blue eyes. Fifteen-year-old Austin Doerksen was reported missing to RCMP on Friday, Nov. 11. He's described as Caucasion, six feet two inches tall and 180 pounds with blonde hair and hazel eyes. CJME News (2016-11-18)

Missing girl found
Nakayo Poucette has been located and is safe. **Cochrane** RCMP were requesting assistance from the public to find a missing 16-year-old from Morley. Nakayo Faith Poucette, 16, from Stoney Nakoda First Nation was last in Morley on Nov. 7 when she attended a birthday party at her grandmother's residence on the reservation. Poucette was seen leaving the party with another young male under non-suspicious circumstances, according to the RCMP. Poucette is believed to be out in Morley and the RCMP do not think she is in any danger, according to Sgt. Darleen White with the Cochrane RCMP. Cochrane Eagle (2016-11-18)

RCMP charge teen in fake terrorist threat in Yellowknife but give no details
RCMP have arrested and charged a teen in **Yellowknife** in a fake terrorist threat. Mounties say the criminal charge resulted from an investigation by Alberta RCMP K Division that began on Nov. 1. Northwest Territories RCMP spokeswoman Marie York-Condon says no details about the hoax can be released, but may come out in court. She says the youth has been released on conditions and will appear at a later date in youth court in Yellowknife. York-Condon also says the next court date may not be released "considering the size of the community that the court is in and the amount of youth that may be appearing in court." She says there was no public safety risk when the alleged threat came to light. Canadian Press (CTV News) (2016-11-18)

IIU Investigates Arrest Involving RCMP Dog
Manitoba's police watchdog is investigating after a robbery suspect was brought down by an RCMP dog in Portage la Prairie on Wednesday. Mounties were called to an armed robbery in the city west of Winnipeg and arrested three people, however one man got away. Officers let the dog loose to chase after the man. The Independent Investigation Unit (IIU) did not go into details, but the suspect received an injury to his leg once the dog caught up to him. 680 CJOB (2016-11-18)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

'That was just my destiny'
Sharon Acoose remembers being groped as a child by an uncle who paid her in pocket change for her trouble - the earliest roots of a life scarred by sex work, drug use and jail time. "He would give me a quarter ... or a nickel or a dime, whatever he had," Acoose, 63, recalled during an interview with The Canadian Press. "You wouldn't believe all the candies that I bought." Despite the longest of odds, she managed to turn her life around, eventually becoming a professor of social work. Countless others who followed a similar trajectory are no longer alive to tell the tale. To this day, that same cycle is repeating itself with alarming frequency in indigenous communities across Canada, a CP investigation has found. And with its insidious links to suicide, violence and mental health problems, the issue of child sexual abuse is poised to be a key theme in next year's long-anticipated national inquiry into the tragic phenomenon of murdered and missing indigenous women. (...) Indeed, experiences of sexual and physical abuse among indigenous women and girls are so pervasive they are expected to overwhelm

next year's national inquiry, where commissioners will examine and report on the systemic causes of the violence. (...) In May 2014, the RCMP documented 1,181 murdered and missing women between 1980 and 2012. A year later, it said 32 additional aboriginal women had been murdered and 11 more had disappeared since it first reported on the issue. The force also cited an "unmistakable connection" between homicide and family violence. Aboriginal women are vulnerable precisely because they're aboriginal and women, said Dr. Yvonne Boyer, a Canada Research Chair at Manitoba's Brandon University. Boyer co-authored a report on trafficking of aboriginal women for the Public Safety Department in May 2014 that noted many of its participants suffered sexual abuse as a child, contributing to a pattern of exploitation that carried on into their adult years. Canadian Press (The Guardian, A8, Waterloo Record, Times & Transcript, Chronicle Herald, National Post, City News, Battlefords News-Optimist, Hamilton News, Weyburn This Week) (2016-11-21); (2016-11-21); Canadian Press (Ottawa Citizen; iPolitics; Mississauga.com; Waterloo Chronicle); Presse Canadienne (La Presse, Le Devoir) (2016-11-20)

UN urges Canada to work on barriers that still face women
A new report from the United Nations is calling on Canada to get to work on a number of barriers still facing women when it comes to gender equality and urging the government to take more concerted steps to stop violence against indigenous women and girls. The review - typically conducted every four or five years - by the Geneva-based Committee on the Elimination of Discrimination against Women covered a range of issues, from the gender pay gap to poverty and violence against women, as well as the use of solitary confinement in prisons. Prime Minister Justin Trudeau, who often calls himself a feminist, has said improving relationships with indigenous communities and working toward gender equality are key priorities for his government. And the report did note some progress, namely the equal representation in the federal cabinet. But the committee cited a range of concerns, among them the "continued high prevalence" of gender-based violence, particularly against indigenous women and girls. It also highlighted the "very low" number of cases of violence against women reported to police by victims, and low rates of prosecution and conviction against perpetrators. The report, posted on its website Friday, came as prosecutors in Quebec said no charges would be laid against police officers in Val-d'Or, after 21 indigenous women and seven men filed complaints against police that included sexual assault and excessive use of force. "It's difficult enough when you're dealing with violence in your personal life," said Francyne Joe, the interim president of the Native Women's Association of Canada. "If you can't go to police expecting to be protected, that's going to lead to such despair and depression and anger ... and disrupt any growing positive relationship with the policing system." Globe and Mail, A12

Caribou Legs reaches St. John's
Brad Firth - better known as Caribou Legs - was part-way through a run spanning five provinces last year, on a mission to protect lakes and rivers, when he got a call that would change his life. got some bad news from back home. That phone call was actually about my sister's death. So I was hit with this really sad story, and it took me a couple of hours to regain my strength, my balance, and continue running, because I didn't want to run any more," Firth said. After finding out his sister had been killed, he just wanted to go home and grieve - "not the right way, but I wanted to grieve angrily, because - just the way my sister died." (...) Caribou Legs, with the support of groups such as Sisters in Spirit, Warriors Against Violence and Culture Saves Lives, decided to set out on the road again. This time it would be to honour women, shine a spotlight on the country's missing and murdered indigenous women and girls, and prevent violence against women. The Telegram, A5; VOCM

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Apology for anti-homosexual persecution should include compensation, government told
Ottawa's apology to Mounties, soldiers and other public servants whose careers were destroyed by anti-homosexual witch hunts will have to be accompanied by compensation, experts say. Prime Minister Justin Trudeau appointed Edmonton Centre MP Randy Boissonnault as a 'special advisor for LGBTQ issues' earlier this week with the goal of arranging an official apology to the thousands of gay and lesbians who were persecuted in the latter half of the 20th century. "We do not have a timeline to announce at this stage," Cameron Ahmad, press secretary to the Prime Minister's Office, said in an email

to iPolitics. The apology will have to include some form of compensation, said Matt James, an associate professor at the University of Victoria who specializes in political apologies and the Canadian Constitutionalism. James said he would not be surprised if representatives from the agencies involved in the persecution - the RCMP and Canadian Armed Forces - had a chance to vet the apology. "I'd be very interested to see, for example, if the apology attempts to make any kind of excuse in terms of national security or that these were things that other security agencies were doing at the time," he said. "I would expect [it's something] the RCMP or military representatives would want to see in there and something I expect the representatives in the LGBTQ community would not want ... So there will be some interesting choices the government will have to make around that." The government announced in April it would apologize and offer redress to LGBTQ employees of the federal public service and the Canadian Armed Forces persecuted by the RCMP. Many were charged with gross indecency before homosexuality was decriminalized in 1969. After decriminalization, federal government workers suspected of being gay or lesbian were often denied promotions or security clearances that would advance their careers. Military members could be dishonourably discharged from the service until 1992. Upwards of 9,000 people were affected. iPolitics

Un camp islamique financé par la Ville de Montréal

Montréal a versé 10 850 $ à une association islamiste pour prendre en charge 30 enfants réfugiés syriens même si elle est soupçonnée par la GRC d'avoir financé des groupes terroristes. Des jeunes syriens âgés de 5 à 14 ans, dont certains ne parlaient pas français ont été accueillis cet été au camp Sindbad organisé par le Centre communautaire Laurentien, une section de l'Association musulmane du Canada (MAC). Le MAC est l'antenne la plus officielle des Frères musulmans, rappellent deux experts. En janvier 2015, Le Journal révélait, d'après des documents de cour produits par la GRC, que MAC avait versé près de 300 000 $ à l'International Relief Fund for the Afflicted and Needy-Canada (IRFAN). En 2011, Revenu Canada a révoqué le statut d'oeuvre de bienfaisance de cet organisme, puis le fédéral l'a déclaré organisation terroriste en 2014. Il reproche à l'IRFAN d'avoir envoyé 14,6 M$ au Hamas entre 2005 et 2009. Le Hamas, un autre groupe terroriste selon Ottawa, vise la libération de la Palestine de l'occupation israélienne et l'instauration d'un gouvernement islamique. Malgré son interdiction, la GRC dit avoir aperçu en mars 2014 un collecteur de fonds de l'IRFAN dans les bureaux de MAC à Montréal. Le Journal de Québec, 25 (Le Journal de Montréal)

Legal changes in the works on opioid crisis

The federal government is eyeing a number of legislative changes to address Canada's opioid crisis, Health Minister Jane Philpott said Saturday at the conclusion of a summit examining the issue. The federal government is actively trying to turn the tide of the crisis, Philpott added, noting it will require a whole-of-government approach. "This is a topic I have been working with alongside the minister for public safety, the minister of justice and the minister of foreign affairs," she said. "In the coming months, there are a number of pieces of legislation that are going to address matters related to the opioid crisis and certainly we will do the work necessary." Addiction, overdose and deaths related to opioid use were the focus of discussions for health experts and ministers who gathered in Ottawa for a two-day summit to look at a national approach. On Saturday, B.C. Health Minister Terry Lake urged the federal government to waste no time in taking additional action to address Canada's opioid crisis, including setting up a nationally coordinated surveillance system to track overdoses and other drug-related harm. The province also wants the federal government to look at tools to stop the flow of fentanyl from China by stepping up diplomatic negotiations. "They need to properly equip the Canadian Border Services Agency and the RCMP with the tools and resources needed for border control and to get fentanyl off the streets," Lake said in a Saturday statement. British Columbia says 622 overdose deaths have happened in that province since January - more than double the number of people who died in car crashes last year. Waterloo Region Record, A3 (CTV News) (2016-11-21); Postmedia Network (Toronto Sun, A11; The Province, Vancouver Sun); Canadian Press (The Province, Vancouver Sun, Toronto Star, Times Colonist) (2016-11-20); Canadian Press(Maclean's; iPolitics; Global News; CTV News; Chronicle Herald); CBC News; Presse Canadienne (La Presse) (2016-11-19)

'This is all a work in progress'

The first time Donovan Locke had to perform an intervention with an aspiring extremist, the 14-yearold in question had been caught spouting white supremacist views at a Toronto high school. The parents were

notified, along with the Toronto Police Service, where Locke is an acting staff sergeant and a coordinator of a new project attempting to address radicalization in Canada's largest city... After police shot Islamic State of Iraq and the Levant supporter Aaron Driver as he was leaving his home in Strathroy, Ont., to conduct a suicide bombing Aug. 10, Public Safety Minister Ralph Goodale said there was *"little national coherence"* to counter-radicalization efforts in Canada and re-committed the government to opening an office to co-ordinate them nationally. Toronto has been quietly experimenting with its own approach, the National Post has learned. Launched as a pilot project by the Toronto police and the city, it has been kept under wraps until now. But in interviews with the Post, key officials spoke for the first time about what they were doing. "One of the things we chose to do here was not to engage the media," said James Ramer, Toronto's deputy police chief. But, "We're at the point now that we do want to advertise it." National Post, A6 (2016-11-19)

Taxpayers would have to foot bill for new high-tech police powers, wireless industry says
Canada's top telecommunications industry group says any government move to force its members to install equipment to intercept digital traffic and store data to aid police investigations would have to be covered by taxpayers. "We have always submitted that there should be a mechanism for the government to cover the costs or possibly law enforcement," said Kurt Eby, director of regulatory affairs and government relations for the Canadian Wireless Telecommunications Association. "Every time the government looks to add a layer such as this, there is going to be cost incurred." The federal government is holding public consultations on Canada's Anti-Terrorism Act, which includes proposals for new investigative powers for police to gather digital evidence... RCMP Commissioner Bob Paulson says nearly 70 per cent of telecommunications companies can't comply with interception orders from the courts. CBC News (2016-11-19)

ComicCon could help you become a spy
Do you enjoy going to ComicCon ? What about giveaway sunglasses or free popcorn ? More importantly: Can you keep a secret ? Then a job as a digital spy might just be for you. Or, at least, that ' s what the Communications Security Establishment (CSE) has in mind as it seeks the best and brightesttechies. An old-fashioned popcorn machine and free pairs of CSE-branded shades were part of the display at a government job fair Thursday at Ottawa ' s Shaw Centre. At the event, where the hashtag # secureyourfuture was prominently displayed, other agencies - including Public Safety Canada, the Canadian Security Intelligence Service (CSIS), the Canadian Forces, the Correctional Service of Canada and the Canada Border Security Agency - competed to woo curious job-hunters, more than one of whom was spotted eating a banana. Though the Royal Canadian Mounted Police displayed Batman-like combat gear on a mannequin, it was, subjectively, hard to compete with CSE ' s popcorn and shades. A CSE rep explained the agency had tried recruiting at a ComicCon event for the first time in Montreal this summer - you know, because a lot of, uh, tech-savvy people attend ComicCon. Postmedia Network (London Free Press, N4; Calgary Herald, National Post, * National Post) (2016-11-19)

Your cellphone password could hold the key in legal battle over collecting evidence
Here's the scenario: Police believe there is evidence on your cellphone or computer that could assist them in a criminal investigation. They ask that you provide your password or encryption key so they can search for clues. Currently, there is no law compelling you to comply with that request. But police in Canada, frustrated by evidence trails that lead to digital dead ends, are calling for a law that would make it a criminal offence to say no to a police officer carrying a judicial warrant. It's an idea designed to accomplish through a legal order what police are increasingly unable to accomplish technologically — getting inside digital devices containing what they believe is crucial evidence in criminal investigations. "It's a very radical proposal in Canadian law," said Micheal Vonn, executive director of the B.C. Civil Liberties Association. "It changes the basic nature of how we go about achieving the ends of criminal investigation, by compelling the person who is under investigation to participate in the investigation." Many privacy advocates — and even some in law enforcement — call the idea an abuse of both privacy protections and the rights of Canadians against self-incrimination. Police supporters counter that public safety — and the ability of police to respond to serious crimes — is already being dramatically eroded by disappearing evidence. Liberal Public Safety Minister Ralph Goodale: "(Police) are certainly concerned about the effect of new technology in an age accelerating digitization. They're concerned whether or not their legal tools are sufficient to cope with what they now have to deal with . . . .

Others in the academic community, in the open media community, have put forward the contrary opinion. And that's what this consultation is intended to solicit, and we will have to weigh all of that carefully to make sure that in our response, we produce a position that is consistent with Canadian's expectations." Toronto Star/CBC News (2016-11-18)

The McAdam file: Bribery, Chinese gangsters and betrayal

Brian McAdam was a seasoned Canadian diplomat when he was posted to Hong Kong in 1989. He became the high commission's immigration control officer two years later, and soon uncovered what he believed was a major scandal. Members of Chinese criminal gangs, known as Triads, were applying to enter Canada as entrepreneurs under the country's business immigration program. And many were getting visas. "What was very, very disturbing to me was I kept seeing all these connections of these people to certain people — politicians — in Canada, and the odd name in our embassy," McAdam says. He started writing reports — there were ultimately 32 — documenting the names of the gangsters who were getting into the country and related concerns. The reports caused panic in the immigration minister's office and at headquarters in Ottawa, McAdam alleges. "I was exposing incredible negligence. I was exposing incredible corruption. And I was exposing the flaws in our whole immigration system. "People in Ottawa didn't want to investigate anything. They just shut their eyes to everything." Most of his reports were destroyed, he says. McAdam returned to Ottawa in 1993, lured by the promise of a job in a new organized crime unit at Foreign Affairs. But when he showed up for work, the job didn't exist. He alleges the personnel manager urged him to take a retirement package, though he was just 51. Days later, he went on sick leave and never returned to work. In 1996, RCMP Cpl. Robert Read began investigating McAdam's allegations that employees at the Hong Kong mission had received bribes and that Triad criminal gangs had infiltrated an immigration computer system. After finding gaping holes in earlier RCMP investigations, Read urged his superiors to authorize a thorough investigation, but was taken off the case. Concerned that his bosses were suppressing his findings, Read went to the media with his concerns in 1999, which led to his dismissal from the RCMP in 2002. McAdam's allegations also sparked a joint RCMP-CSIS investigation known as Project Sidewinder, which probed the threat posed by the purchase of Canadian companies by Triad members or associates with links to the Chinese Intelligence Service. Ottawa Citizen (2016-11-18)

Why Spy on Reporters When You Can Spy on CEOs?

An opinion piece states, "Canadians have been shocked to learn that police in this country have for the second time this year admitted to spying on reporters. What makes the recent disclosures most ironic is not that police officers were the ultimate targets, or that spying was approved in the absence of an actual judge—but that much of the meta-data sought by Montreal police may have already existed on a government server, and could have been obtained without a warrant, thanks to the enactment of the Anti-Terrorism Act (known as "Bill C-51"). In fact, in his latest annual report to Parliament, Canada's Privacy Commissioner identified 58 such instances where Canadians' information was collected and shared without prior judicial approval in the first six months of this year alone. Whether it's the Communications Security Establishment (CSE) illegally collecting and sharing Canadians' metadata with foreign intelligence partners, the RCMP, Vancouver, and Toronto Police departments each individually mopping up entire city blocks full of cell phone information with Stingray surveillance devices, or the Canadian Security Intelligence Service (CSIS) building a secret database and intentionally concealing its existence from Federal Court Judges, Bill C-51 has emboldened all manner of police and security services to push the envelope and end-run Canada's Privacy Act." VICE News (2016-11-18)

Money-laundering watchdog cites 'significant' deficiencies at 100-plus B.C. real estate firms

Canada's anti-money laundering watchdog found "significant" or "very significant" levels of non-compliance at more than half of the B.C. real estate companies it examined over a four-and-a-half year period, its records show. The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the federal agency mandated to detect and combat money laundering, examined about 220 real estate companies in B.C. between 2012 and mid-2016, finding 112 companies with "significant" levels of non-compliance and five with "very significant" non-compliance, according to records obtained by Postmedia News through an access to information request. In the past year, FINTRAC has ramped up scrutiny of real estate - particularly in B.C. In an operational brief this week intended for banks and real estate professionals, the agency highlighted the Canadian housing market's vulnerability to money laundering.

The 12-page FINTRAC brief also notes the "minimal" filing of suspicious transaction reports in Canadian real estate, with 127 reports filed on five million sales over 10 years. Vancouver Sun (2016-11-18)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Changing perceptions: How this Winnipeg artist's dramatic billboards aid police training
In early 2015, KC Adams' black and white portraits of indigenous people hung around the city on billboards, bus shacks and bulletin boards, demanding our attention. The twinned photos featured people scowling and hurt as Adams hurled racial insults at them, then smiling and radiant as she reminded them of happier times. The models self-selected their own labels on their second portraits: epithets like mother, dream chaser, soccer player and taxpayer... Metro: Do you have plans for a Perception round two? Do you think our city could still use more of a push in that direction? Adams: "I think we need to be constantly reminded about our responsibilities on truth and reconciliation and I think the work could potentially... be used as a tool maybe in educational systems. Interestingly enough, I was contacted in British Columbia by the RCMP training unit where they train their new recruits. Metro News (2016-11-20)

RCMP Biography Will Please Mountie Fans And Concern Critics
To hear biographer George Garrett tell it, Stirling McNeil was a character straight out of a 1930s movie. The handsome hero, a Manitoba kid, loses his factory job to a Depression-era layoffand joins the RCMP. He goes on to patrol the frozen north on 700-milelong dog sled trails, bringing sometimes rough but always fair justice to the trappers, miners and First Nations residents of Canada's north while establishing a reputation for even-handed treatment of all, old world courtliness and devotion to the law and the RCMP. He pioneers the use of airplanes for law enforcement in the north and rubs shoulders with a colourful gallery of fellow officers, felons and raffish local characters. Vancouver Sun, E7 (2016-11-19)

Mounties won't be charged after Surrey suspect suffers broken hip
The Criminal Justice Branch says three RCMP officers will not be charged after a suspect in Surrey suffered a broken hip. The branch says police were called to a basement suite in on Feb. 28, 2015, after reports that a tenant was "trashing" the unit. A statement from the branch says Mounties found an apparently intoxicated man who was naked, bleeding and swearing in a room littered with broken glass and furniture. The branch says the man initially complied with police and agreed to leave the residence, but then began pushing the officers who had to take him to the ground so he could be restrained. The statement says suspect's nose and forehead were cut after his head hit the ground, but an injury to his right hip wasn't immediately obvious, though it was later determined that he needed surgery. Potential charges of assault were considered, but the branch says the available evidence does not meet the standards to approve any charges. Canadian Press (Vancouver Sun; Info News) (2016-11-19)

Kamloops Mountie honoured for saving the life of his brother in blue
A member of the Kamloops RCMP was among 56 men and women who were recognized at the annual Police Awards in Victoria last night. Cst. Steve Marcil was honoured by Lieutenant Governor Judith Guichon and Solicitor General Mike Morris for his actions in saving the life of Corporal J.R. Michaud, who was shot during a traffic stop two years ago in Batchelor Heights. Marcil says, while the incident was unusual, it's all in a day's work for an RCMP member. CFJC (2016-11-18)

D'ex-agents de la GRC estiment avoir subi des représailles à la suite de gestes déplacés de supérieurs
Deux anciens agents de la Gendarmerie royale du Canada (GRC) dénoncent à leur tour les injustices du système de discipline interne du corps policier. En plus des disparités entre les infractions commises et les sanctions reçues, ils affirment que les plaignants sont souvent traités comme des parias par la GRC et que des plaintes infondées seraient parfois utilisées pour se venger entre employés. Il y a quelques années, la carrière de Linda Davidson dans la GRC semblait atteindre des sommets. Elle avait même été affectée à la protection du premier ministre de l'époque Stephen Harper, à Ottawa. Mais elle soutient, dans son témoignage à Radio-Canada/CBC, avoir plutôt vécu l'enfer, victime d'une agression sexuelle au travail par l'un de ses supérieurs. Radio-Canada (2016-11-18)

Un premier groupe d'entraide pour les veufs et les veuves à Moncton
Il est difficile d'imaginer ce qu'on peut ressentir à la perte d'un conjoint. Trouver un groupe d'entraide afin de mieux vivre son deuil est vital pour certains. Or, ce genre de groupe n'existait pas à Moncton jusqu'à aujourd'hui. Soaring Spirits Moncton Vivre avec le deuil a été mis sur pied par deux veuves, Christelle Léger et Nadine Larche. Mme Larche a perdu son conjoint, il y a plus de deux ans, lors de la fusillade du 4 juin 2014 à Moncton. Pour la mère de trois filles, le deuil est encore une épreuve difficile à surmonter, et ce, même si les choses semblent s'améliorer. «On peut dire que ça va mieux. Évidemment, j'ai encore des journées très difficiles. Comme maintenant, j'ai une petite fille malade à la maison toute seule. Il y a encore des journées difficiles, mais ça va mieux, ça va mieux», a confié Mme Larche à l'Acadie Nouvelle. Nadine Larche a été en mesure de trouver des appuis dans la grande famille de la GRC, rencontrant, lors de cérémonies, d'autres endeuillés avec qui elle a été capable de tisser des liens. Acadie Nouvelle (2016-11-18)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

Marijuana tycoon says Canopy could survive 25 per cent Trudeau tax rate
The head of Canada's first publicly-listed marijuana producer said his company could still turn a profit even if Prime Minister Justin Trudeau's government decides to tax legal recreational weed at rates as high as 25 per cent. A task force is due to report this month on how Canada can build a legal weed market that squeezes out organized crime, protects minors, ensures quality and adds to revenue through taxes. Bruce Linton, chief executive officer of Canopy Growth Corp., says lawmakers will probably choose to control the distribution of recreational marijuana through government-run outlets such as liquor stores. "We can probably carry a tax burden of 25 per cent or so and end up in the consumers' hands on a still cost-competitive basis, with a superior product," Linton said in an interview at Bloomberg's Ottawa newsroom. Canopy, based in Smiths Falls, Ont., became the first marijuana producer to trade on a major North American stock exchange when it graduated to the Toronto Stock Exchange in July. It became the first publicly traded Canadian producer of the drug in 2014. The company's share price more than doubled this month, bringing its market value past $1.6 billion, on better-than-expected earnings and after U.S. elections widened the scope for legal marijuana. Canopy already produces medical marijuana under an existing legal regime. Linton says the company, which operates out of a former chocolate factory, can shift production to serve the recreational market when Trudeau's government makes that legal. Part of the appeal of the legal variety will be its quality control, Linton says. "When it's lawfully available from a reliable supply chain, which we know we can trust and believe in, there are a lot of people who might discontinue the use of say a glass of wine or a beer and try this." Canopy can also generate new formulations of medical marijuana to sell through pharmacies as legalization moves ahead, Linton said. Loblaw Cos., owner of the Shoppers Drug Mart pharmacy chain, has signalled it wants to sell medical marijuana. Postmedia Network (Leader-Post, B6, StarPhoenix, Vancouver Sun)

Ottawa pot dispensaries back in business after police raids
At least two illegal marijuana dispensaries in Ottawa have reopened after police raids closed them down earlier this month. Seven shops were shut down following complaints about the growing number of dispensaries in the city. Two Green Tree Medical Dispensary locations visited by CBC News on Sunday were open for business, although shop attendants refused to provide any sort of comment. "It's a reality," said Rideau-Vanier Coun. Mathieu Fleury. "Until we have the federal framework in place and better coordination provincially ... it's going to be that game of closing and opening." Fleury said he knows there are concerns in his ward about the illegal dispensaries and their effect on the community and people shouldn't stop giving their input on the issue because some of the dispensaries have reopened. "We have to continue to monitor, to enforce. Especially based on community complaints and community feedback and information gathering." On Nov. 4, two marijuana shops in Fleury's ward were raided by police but that hasn't deterred others from getting into the business. He said he's aware of two new shops that have opened recently but still thinks the raids were a good idea. "There's huge gains from the raids that have been put in place. I know that's contentious to say but the perception that these locations were offering legal marijuana is now clear that it is not. That element has been clarified." The federal government has promised to introduce legislation to legalize marijuana by the spring of 2017, but the possession, production and trafficking of marijuana remains illegal. CBC News

Feds closer to new policy on medical pot for vets
The Trudeau government is getting closer to having a new policy on medicinal marijuana for our veterans, who take the drug to treat conditions like PTSD. The veterans affairs department has been reviewing the issue of medical pot after concerns were raised earlier this year that the department is compensating vets for up to ten grams of marijuana a day. News 1130

Legal pot in Canada could sell for $5 a gram — or less
Uncle Ike's Budget Bud is the cheapest pot we've found anywhere. A product line of a Seattle, Wa.-based marijuana retailer, it lives up to its name at US$99 an ounce. That works out to $4.76 a gram Canadian, and it would put the cost of a joint in the $1.50-$2 range. Global News (2016-11-20)

Legalizing marijuana isn't apt to bring a windfall for governments
An opinion piece states, "Several economic myths have surrounded the legalization of marijuana. This has maintained the illusion that it would be a bonanza for federal and provincial treasuries because of the supposed enormous tax revenues that legalization would generate. The Parliamentary Budget Office in Ottawa is to be congratulated for blowing up some of these myths in its report, published this month,on projected marijuana tax revenues following legalization in Canada in 2017 or 2018..." Montreal Gazette (2016-11-20)

Du pot légal près de chez vous
D'ici à ce que le Canada arrive à la conclusion de sa longue démarche visant à légaliser la marijuana, les amateurs de cannabis du Québec, plus précisément ceux de la Beauce, pourraient avoir accès à une source légale de marijuana à des fins récréatives à quelques minutes de chez eux. La Presse (Le Soleil, 3; Le Quotidien) (2016-11-20)

Où acheter la marijuana une fois sa consommation légalisée?
Si la consommation de cannabis devient légale au Canada, la vente de cette substance devrait être bien encadrée, suggère un nouveau rapport de l'Institut national de santé publique du Québec. « On ne peut pas imaginer de distribution libre à but lucratif comme n'importe quel produit qu'on vend », affirme Réal Morin, médecin-conseil et coordonnateur du chantier cannabis à l'Institut. Le Dr Morin croit que la vente du cannabis devrait être confiée à une « agence gouvernementale de type monopole d'État ». En entrevue à l'émission 360 PM, il a précisé que cette organisation devrait avoir la prévention comme principale préoccupation et non pas une mission économique comme c'est le cas d'autres sociétés d'État. Radio-Canada (2016-11-20)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

RCMP overstating 'surveillance lag'
An opinion piece states, "The RCMP has been lobbying the government behind the scenes for increased surveillance powers on the faulty premise that their investigative powers are lagging behind those foreign police services. The centre piece of the RCMP's pitch is captured in an infographic that purports to show that foreign governments are legislating powers that are more responsive to investigative challenges posed by the digital world. On the basis of this comparison, the RCMP appears to have persuaded the federal government to transform a process intended to curb the excesses of Bill C-51 into one dominated by proposals for additional surveillance powers. The RCMP's lobbying effort misleadingly leaves an impression that Canadian law enforcement efforts are being confounded by digital activities. For example, in its comparative sample (which includes Australia, New Zealand, the United Kingdom and the United States) Canada is presented as the sole country lacking a legal obligation compelling Internet companies to design their services around state surveillance requirements. In fact, Canada already imposes this obligation on mobile service providers in spectrum licences. Furthermore, communications providers demonstrated to the government in 2013 that their networks are generally becoming intercept-ready even in the absence of a legal obligation to do so. The RCMP also misrepresents the legality of foreign surveillance powers. For example, a proposal to require the retention of communication interaction data is presented as "under discussion" in the U.K. In fact, this power has been found unconstitutional by the

U.K. divisional court and is currently on appeal to the EU's highest court, which has already struck down its predecessor legislation." Toronto Star, A11

Native policing

A letter to the editor states, "Re Either Fund Native Police, Or End Them (editorial, Nov. 15): While I expect the editorial questioning the skills and capacity of "native police" after the in-custody suicide of Lena Anderson was well-intentioned, may I point out that many indigenous Canadians have died in the custody of well-funded mainstream non-indigenous police forces? Take for example, Solomon Uyarasuk, a young Inuk man in Iglulik who, after being taken into RCMP custody in 2012, died alone in his cell where he had been left naked, but for his belt. Despite inquiry after inquiry into the deaths of indigenous people in custody, many of which have stated that hanging points should not exist in cells, he was left alone with a belt and a hanging point. Clearly, upstream solutions to complex mental health and societal problems are needed, but these repeated in custody scenarios are appallingly grievous." Globe and Mail, A10

Canada's national security oversight is among the weakest in the world: former human rights advocate

An opinion piece by Steven Zhou, Toronto writer and human rights advocate, states, "There doesn't seem to be much that Canada's intelligence and spy agencies can't do these days-and that includes breaking the law. While much of world remains anxious about the future of a Donald Trump presidency, Canadians should refocus their attention back home, and they should start with the country's bloated national security state. Experience shows that most of a country's establishment systems have likely transcended partisan lines and will remain immune to changes in political personality. National security seems to be one of these categories and its pervasive entrenchment within post-9/11 democracies has been demonstrated both in and outside of American borders. The Canadian security apparatus is a good example of how partisan changes usually have minimal impact on the larger system. There is no Canadian Edward Snowden to shed light on the extensive surveillance and policing machinations of CSIS or the Communication Security Establishment (CSE)... A federal court made national news last week by rebuking CSIS for essentially hiding a giant database full of private information belonging to law-abiding Canadians who pose no threat to public safety. Its watchdog group, the Security Intelligence Review Committee (SIRC), had previously asked CSIS to disclose the existence and full capabilities of this database to the courts, but the spy agency refused and kept things secret for a whole decade. The revelation has been an embarrassment for Public Safety Minister Ralph Goodale, who's been conducting a national consultation on how to reform Canada's security regimes. When asked why CSIS kept the database a secret from the courts, agency director Michel Coulombe simply said that he had no good explanation... There's precisely one person, the CSE Commissioner Jean-Pierre Plouffe, who's supposed to overlook the entire slew of intelligence-related activities that are carried out by the agency on a regular basis... Minister Goodale has promised swift action, but until those words actually manifest themselves into serious institutional change, then Canada will still remain the country with perhaps the weakest national security oversight in the Western world." CBC News (2016-11-20)

Give all officers training in mental-health skills

A letter to the editor states, "Re: "Police seek budget for mental health officers," Nov. 17. We do not need two mental health officers, we need the existing force, and all new recruits, trained in basic mental health and communication skills, as well as violence prevention. You need to have coverage for all times of the day, and two officers wouldn't cut it. As most normal police/civilian interactions are stressful, these courses would help here as well. With proper training, willing officers can help change the stigma of mental illness..." Times Colonist (2016-11-20)

Ottawa should be careful on expanded police powers

An editorial states, "Crime, like everything else, has been transformed by the digital age. Fraudsters, child pornographers and terrorists, among others, are becoming ever more expert in using digital technologies to commit their offences and cover their tracks. Not surprisingly, this has created new challenges for law enforcement. Police chiefs across Canada claim investigators do not have the tools to keep up. Many say concerns about privacy have scuttled their attempts to convince politicians to provide them with the cyber-surveillance powers they need to do their job. As Bob Paulson, commissioner of the Royal Canadian

Mounted Police, puts it, "We're losing our ability, if we haven't lost it entirely, to bring the traditional investigative response to technologically facilitated crime because of the misunderstanding, in my view, of the privacy threat." This week, Paulson shared with reporters from the Star and CBC News case files he says demonstrate the obstacles his force faces, an attempt to help the public understand the need for new police powers the federal government is currently floating... And that's to say nothing of security agencies themselves. The recent revelation that the Canadian Security Intelligence Service illegally spied on people suspected of no wrongdoing is a timely reminder that expanded powers must be accompanied by expanded oversight... In recent decades, and in particular with the passing of the overreaching Bill C-51, the trend has been to expand the powers of the security establishment without offering counterbalancing privacy protections or safeguards against abuse... The public consultation now underway won't mean much unless Canadians understand, yes, the challenges police face, but also the risks of their proposed remedies, including the threats to personal privacy and security posed by an ever-expanding surveillance state." Toronto Star (2016-11-18)

Ottawa should be careful on expanded police powers
An editorial states "Crime, like everything else, has been transformed by the digital age. Fraudsters, child pornographers and terrorists, among others, are becoming ever more expert in using digital technologies to commit their offences and cover their tracks. Not surprisingly, this has created new challenges for law enforcement. Police chiefs across Canada claim investigators do not have the tools to keep up. Many say concerns about privacy have scuttled their attempts to convince politicians to provide them with the cyber-surveillance powers they need to do their job. As Bob Paulson, commissioner of the Royal Canadian Mounted Police, puts it, 'We're losing our ability, if we haven't lost it entirely, to bring the traditional investigative response to technologically facilitated crime because of the misunderstanding, in my view, of the privacy threat.' This week, Paulson shared with reporters from the Star and CBC News case files he says demonstrate the obstacles his force faces, an attempt to help the public understand the need for new police powers the federal government is currently floating. The cases are no doubt disturbing, tales of child abusers and wannabe terrorists evading justice. But while they clearly illustrate new and thorny police challenges, they do not establish that the requested powers are necessary or proportionate or to what extent they would endanger privacy or even weaken security. Paulson is right that an informed public discussion about these difficult issues is necessary and that the evolving nature of cyber-crime is an important part of that discussion. But a closer look at the requested powers shows that Paulson's story is not the whole story." Toronto Star (2016-11-18)

The RCMP needs you scared - and the media seems happy to help
An opinion piece states "Long before email, metadata and GPS tracking, King Louis XIII's hatchetman Cardinal Richelieu said: 'If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged.' Nothing's changed. The RCMP is back at the back door, lobbying the government for greater powers to access digital evidence - and now they're using the media to make their case. Recently, the RCMP self-selected 10 investigation files and fed summaries to the CBC and Toronto Star. Details that could compromise ongoing investigations (or be used by journalists to fact-check) were redacted. Both media outlets dutifully gave the Mounties the headline they wanted - one about how child predators, drug gangs and terrorists are escaping justice. The RCMP's proposed solution is, of course, more police power. It's always more police power. The RCMP wants laws that would compel suspects to hand over passwords, grant warrantless access to subscriber information and require telecommunication providers to build back-door intercept capabilities into their networks." iPolitics (2016-11-18)

OTHER / AUTRES

Pas d'accusations à Val-d'Or, deux à Schefferville, le DPCP s'explique
Jeudi, il a été révélé qu'Alain Juneau a été accusé d'agressions sexuelles contre des femmes autochtones ; des gestes qu'il aurait posés à Schefferville, entre 1992 et 1994, au moment où il travaillait comme policier pour la Sûreté du Québec (SQ) sur la Côte-Nord. Le DPCP devrait en faire l'annonce dans sa conférence de presse. Et il appert aussi qu'un policier autochtone de Schefferville ferait l'objet d'accusations, selon ce qu'a appris Radio-Canada. Octobre 2015, le Québec sous le choc. Rappelons

qu'en octobre 2015, la diffusion de témoignages accablants de femmes autochtones de Val-d'Or, disant avoir été victimes de violence sexuelle et d'abus de pouvoir de la part de policiers de la SQ, avait secoué l'ensemble du Québec. Ces révélations de l'émission Enquête de Radio-Canada avaient conduit le ministère de la Sécurité publique du Québec à confier au Service de police de la Ville de Montréal (SPVM) le soin d'enquêter sur les comportements allégués d'agents de la SQ. Le DPCP a par la suite analysé 37 dossiers qui lui avaient été remis par le SPVM. Presse canadienne (Radio-Canada, Huffington Post); CBC News; TVA Nouvelles; La Presse; Le Devoir (2016-11-18); Globe and Mail, A3; Leader-Post, N3; Ottawa Sun, A16; Postmedia Network (London Free Press, N3; Montreal Gazette, Edmonton Journal, Windsor Star, Vancouver Sun, Calgary Herald); * Le Droit, 29 (2016-11-19)

Hamilton's horror - Cops not naming names in child abuse scandal telling
One lone name stood out on the press release outlining those charged in the monstrous serial molestation of a little Hamilton girl. Can I remind you, she's seven. And while he was not directly connected to the little girl, the only name on that release was Geoffrey Burnet. And so far, he's the only one we have. According to cops, the girl's mother's boyfriend was allegedly offering her for sale on Craigslist. Seven people were arrested - no names. In the case of the mom and her boyfriend it's easy to see why there were no names. Postmedia Network (Winnipeg Sun, A7; Calgary Sun, Edmonton Sun) (2016-11-20)

Surge in domestic handgun trafficking
Danny Santapaga, a self-employed financial adviser, bought 14 guns on 10 different occasions over seven months. Plumber Graham Jovanovic purchased nine firearms over five weeks. University student Justin Green obtained 23 handguns during a 22-month period, including 15 from one store. Security guard Andrew Winchester acquired 47 handguns in a six-month buying binge. Hamilton Spectator (2016-11-19)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 23, 2016 / le 23 novembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

Big Brother et « Five-eyes »

La consultation sur la sécurité nationale menée par le gouvernement Trudeau tire à sa fin et deux événements récents appellent les Canadiens à la plus grande vigilance pour la suite des choses. L'affaire de la surveillance des journalistes au Québec et le jugement de la Cour fédérale sur la collecte et la rétention de données personnelles par le Service canadien du renseignement de sécurité (SCRS) montrent bien que l'équilibre entre la sécurité et la protection de la vie privée reste au centre des préoccupations devant les demandes incessantes de pouvoirs accrus des autorités. Les libéraux ont promis en campagne d'« annuler les dispositions problématiques » du projet de loi C-51 adopté en vitesse après les attaques d'octobre 2014, législation qu'ils avaient appuyée avec réserve. Ils ont inclus cet engagement dans une consultation plus large basée sur un livre vert qui lance les discussions. Le gouvernement est déjà passé à l'action sur un aspect de la consultation, soit la supervision politique des agences et organismes chargés de la sécurité nationale. Le projet de loi C-22 prévoit la formation d'un Comité parlementaire sur la sécurité nationale et le renseignement. Tenus au secret, ses membres auront un accès sans précédent au Canada aux informations sur les opérations liées à la sécurité nationale. Le ministre de la Sécurité publique, Ralph Goodale, a expliqué son empressement en indiquant que le Canada était une « anomalie » en la matière par rapport à ses partenaires de ce club du renseignement qu'est le « Five-Eyes », qui regroupe aussi les États-Unis, la Grande-Bretagne, l'Australie et la Nouvelle-Zélande. Il s'est d'ailleurs rendu en début d'année à Londres, se disant inspiré par le modèle britannique, qui a le grand mérite selon lui de ne pas avoir donné lieu à des fuites qui auraient pu mettre en danger la sécurité nationale. La participation du Canada aux échanges du groupe Five-Eyes est d'ailleurs un élément central du contexte dans lequel les nouvelles normes canadiennes sur la sécurité nationale seront définies. C'est un aspect que les Canadiens doivent garder à l'esprit quand ils

évaluent les positions des autorités compétentes et des défenseurs de la vie privée. Étant donné l'attirance britannique du ministre Goodale, l'adoption jeudi dernier à Londres du projet de loi sur les pouvoirs d'investigation mérite l'attention. Fait intéressant, d'autres dispositions de la même loi se retrouvent parmi les hypothèses soumises aux Canadiens par le ministre Goodale dans son livre vert. C'est ainsi que les fournisseurs britanniques de services de communication (FSC) devront conserver pendant une année les données de navigation en ligne de leurs clients et que les enquêteurs pourront accéder sans mandat aux données de connexion. Les FSC seront contraints d'aider les autorités lors d'interceptions ciblées, en plus de devoir retirer sur demande leur propre chiffrement des données. Le Devoir, A3

Senator tables bill to protect source confidentiality

The relationship between a journalist and a confidential source is sacrosanct, according to a Parliamentarian who wants to enshrine that relationship in law. Amid a scandal over revelations that police in Quebec spied on several journalists, Conservative Senator Claude Carignan has introduced a private member's bill that aims to keep police from ferreting out reporters' sources. "It's a fundamental principle. It's very important to protect the journalist and also the whistleblower," Mr. Carignan, the Senate's opposition leader, told reporters in Ottawa on Tuesday. While Quebec recently announced a commission of inquiry into press-freedom issues, Prime Minister Justin Trudeau has resisted calls for a Canada-wide inquiry. But Mr. Carignan said Parliament cannot afford to wait. Bill S-231, the Journalistic Sources Protection Act, seeks to "protect the privilege of journalistic sources, and secrecy," he said. Last year, the RCMP ordered a Vice News reporter to surrender materials related to conversations with a Canadian member of the Islamic State. And the Mounties briefed Public Safety Minister Ralph Goodale last year about the fact that some detectives had shadowed a Quebec reporter who obtained a leaked CSIS document. Globe and Mail, A4

Watchdog wants rules for spies sharing info

Other national security agencies may be taking the same broad view of the law that led CSIS to illegally keep data on innocent people for almost a decade, the federal privacy watchdog says. Privacy commissioner Daniel Therrien said he's calling on Parliament for clearer rules about how spy- and law-enforcement agencies obtain, retain and destroy information on Canadians. Therrien said information-sharing powers granted in Bill C-51, the former Conservative government's controversial spying bill, need restrictions on what agencies can share and how long they can keep the information. "Security agencies, with (Bill C-51 powers) and with the absence of rules around retention, for instance, would be able to collect and retain information that they don't really need," Therrien told the Star outside a House of Commons committee Tuesday. "I don't dispute that CSIS needs to analyze information in order to do their job ... but once the analysis has been completed and the vast majority of people about whom they're collecting information are found not to be a threat, and that's the case, then they should destroy that information." "I don't think that's the kind of country we want, where the security services of the country hangs onto information on vast amounts of people in case it might be helpful one day," Therrien added. In his testimony before the access to information, privacy and ethics committee, Therrien noted Canadian spy agencies misusing powers is not a "theoretical" issue. He noted that CSIS was recently found by a federal court to have illegally kept data on an unknown number of innocent Canadians between 2006 and 2015. Therrien's comments come as the governing Liberals are in the midst of a wide-ranging review of Canada's national security agencies and issues of oversight for spies. They also come as Canada's national police force, the RCMP, are publicly arguing for expanded investigative powers in the online world. A spokesperson for Public Safety Minister Ralph Goodale said the minister looks forward to the Commons committee's report on Bill C-51's information-sharing powers and appreciates Therrien's insight into these issues. Toronto Star, A10

Territorial government preparing for federal marijuana legalization

The territorial government has formed an inter-departmental working group to prepare for the eventual legalization of marijuana across Canada. The group is also in discussions with the federal government, according to Department of Justice spokesperson Sue Glowach. The task force was established by the minister of Justice and Attorney General of Canada, the minister of Public Safety and Emergency Preparedness and the minister of Health, according to Glowach. She stated the task force's mandate is to inform the federal government's commitment legalize and regulate marijuana. The report is expected to

be released to federal ministers by the end of the month ahead of next April's anticipated marijuana legalization legislation. "The information on potential systems for production, distribution, promotion and taxation provided in the report should make it possible to determine what the role of the ... territories will be," she stated. Yellowknifer

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

Surrey's top cop concerned by ages of suspected shooters

The officer in charge of the **Surrey** RCMP says he's troubled that nine young people have been arrested in connection with a shootout in south Surrey. "To say anything other than the fact that they are youths would probably be saying too much," said Chief Supt. Dwayne McDonald. "I don't want to risk identifying them but youths involved in crimes such as that is definitely a concern for me and for the Surrey RCMP and for the city of Surrey." Several shots were fired in a hotel parking lot early Monday morning near King George Boulevard and 11th Avenue. One person was cut by broken glass but no one was seriously hurt. McDonald says he's heard false reports about the accused. "It was reported that some of the youths or many of the youths involved in yesterday's incident were part of our Wrap Program and that is not the case," he said. CBC News (2016-11-23); Times Colonist (2016-11-22)

Crime on decline in Surrey

Surrey's new top cop wants to change the perception that his expanding city is a hotbed of crime. "I believe, having lived and worked in Surrey for a number of years, the perception of crime in Surrey tends to be that crime is high," Chief Supt. Dwayne McDonald said Tuesday during a keynote address at a Surrey Board of Trade luncheon. "That's something that I want to address as an officer in charge." McDonald, appointed officer in charge of Surrey's RCMP detachment last month, pointed to the recently released third-quarter crime statistics as one reason for optimism. "We have work to do, but I'm pleased by the results," he said. According to the latest police statistics, there's been a 13 per cent decrease in violent crime, a slight decrease in property crime, a 38 per cent decrease in robberies, a 21 per cent drop in business break-and-enters, and a 17 per cent curtailment in incidences of theft under $5,000. Residential break-and-enters are up, however, and McDonald said that's an area police need to target. Province, A12 (Vancouver Sun)

Surrey police deny suspects were part of Wrap program

Surrey police deny that any suspects in a shooting Monday were participants in an anti-gang program for youth. On Monday, Kash Heed, a retired police officer and former B.C. MLA who served as minister of public safety and solicitor general, said a source had informed him that of the nine people arrested following a shootout in the parking lot of the Pacific Inn Resort and Conference Centre, five were students in Surrey schools and a person alleged to have had a gun was in Grade 8. Heed said three of the accused were involved in the Wraparound (Wrap) Program, a Surrey RCMP and school district initiative that works with at-risk youth to help them stay out of gangs and the criminal lifestyle. But following a keynote address Tuesday at the Surrey Board of Trade, Surrey RCMP Chief Supt. Dwayne Mc-Donald told reporters that none of the suspects was involved in Wrap. "It was a bit disappointing," Mc-Donald said. "It was factually inaccurate yesterday. It was reported that some of the youth or many of the youth involved in yesterday's incident were part of our Wrap program, and that is not the case. I won't get into too many details on that other than to say that that's inaccurate." As many as 20 shots were fired between two vehicles on Monday and one person was treated for minor injuries. Vancouver Sun, A11

Two tech initiatives launched to help keep Surrey safe

The **Surrey** RCMP and the City of Surrey on Tuesday announced the launch of two new technology initiatives under the City's new Public Safety Strategy. These initiatives will allow residents and businesses to become more engaged and play a larger role in keeping Surrey safe. The new Surrey RCMP App is a convenient, one-stop-shop for mobile device users to access information and resources on emerging crime trends, Surrey RCMP events, crime mapping, crime prevention and contact information. Users will also be able to view missing persons, most wanted persons, and photos of

unidentified suspects right from their phones to assist police and the community. Voice Online (2016-11-22)

Surrey launches public registry of CCTV cameras to cut crime
The City of **Surrey** has started rolling out its public safety strategy in collaboration with the RCMP and one of the latest additions could involve your home or business security camera. They're calling it Project IRIS and the idea is people will sign up online and tell the RCMP where their CCTV cameras are located. Police can then use that database to quickly track down security footage in the event of a crime. "I can tell you from experience that it is very common for most residents to have them and almost every business now," says RCMP Chief Superintendent Dwayne MacDonald. News 1130 (2016-11-22)

City of Surrey, RCMP prepare to launch 135A Street cleanup
Locals call it "the strip"; a notorious stretch of 135A Street between 106th and 108th Avenues where trafficking in drugs, sex, and stolen goods is commonplace. Now, the city and the RCMP are preparing to launch a comprehensive effort to address the various issues plaguing the area. "When we talk about 135A, we're really talking about a series of social issues," says Chief Superintendent Dwayne McDonald. "Certainly there is criminal activity that's involved there, but we're really dealing with a population which is venerable." McDonald stresses their approach will be more than law enforcement, and efforts will be made in collaboration with community partners to transition residents into the services they need. One of area's biggest issues is drug abuse. Of the 36 overdose cases reported in Surrey in the span of 48 hours this summer, most came from 135A Street. News 1130 (2016-11-22)

Police bust fentanyl lab in city's S.W
Two men have been charged after police busted a fentanyl powder reprocessing lab. **Calgary** police evacuated an apartment building in the 0-100 block of Westpark Link S.W. last week after officers found signs of the lab. Police initially entered the building on a search warrant for what was believed to be a heroin trafficking investigation. The RCMP Clandestine Laboratory Enforcement and Response Team was brought in to identify and remove the substances found in the residence. No one was injured as a result of the investigation. Police found 11 grams of methamphetamine, more than 26 gram of power cocaine, 65 grams of crack cocaine, 263 grams of fentanyl powder and 645 fentanyl pills as part of the search. Calgary Sun, A19 (Edmonton Journal, Calgary Herald) (2016-11-23); Canadian Press (Medicine Hat News); Calgary Herald (2016-11-22)

Alarm raised on fentanyl after overdose death
A **Nova Scotia** woman is raising awareness after her 21-year-old granddaughter's fentanyl overdose. Charly Ann Torikka, a young mother and Maple Ridge, B.C., resident, was found dead in bed by her boyfriend on Nov. 6. An autopsy report revealed fentanyl-laced cocaine was in her system, and her father used the media to warn others in B.C. about the drug. Now, the girl's grandmother, Lynda Koile, is doing the same on the East Coast. (…) RCMP spokeswoman Cpl. Jennifer Clarke said the department now has a supply of Naloxone, a drug that reverses or blocks the effects of opioids. "(It) is being distributed to employees across the province in stages. The first to receive the Naloxone kits are the employees who are the most likely to come into contact with it, then to those employees who are at a lower risk of contact," she wrote in a late October email. "We are actively rolling them out to the rest of the division." Chronicle-Herald, A1

Investigation into child's death delayed
A police investigation into the death of a four-year-old girl who died in care is waiting on paperwork, said an RCMP spokesman Tuesday. "There are different agencies involved here," said Sgt. Jack Poitras of **Edmonton**'s K Division. "Investigators are waiting for reports to come in." He said he couldn't release further information on what the reports are and doesn't know the timeline for the investigation. Serenity died on Sept. 27, 2014, while in kinship care, being looked after by family members. Her death prompted a review of the case by Alberta's child and youth advocate, who found that no workers had checked on Serenity or her two older half-siblings in almost a year before she died, despite reports she was unwell, malnourished and bruised. Medical records obtained by Postmedia showed Serenity weighed 18 pounds when she died. She was suffering from hypothermia and had multiple bruises, including around her genitals, when she arrived at hospital. Her hymen was gone. The Alberta medical examiner's report on

her death was completed almost two years after her death before being given to the RCMP, who asked that the report not be released. Poitras said the autopsy report will be withheld until the investigation is concluded. He added that due to the different agencies involved with children in care, it isn't uncommon for investigations to be delayed. Edmonton Sun, A9 (Calgary Herald, Edmonton Journal)

Youth charged over alleged terror threat
A youth arrested Thursday in **Yellowknife** faces a charge of making a hoax terrorism threat, RCMP stated in a news release. The youth, who cannot be identified, lives in the territory. An investigation started Nov. 1 that included the RCMP's Integrated National Security Enforcement Team in Alberta determined the threat was a hoax. It's unclear what the hoax allegation involves and RCMP aren't elaborating. "The rest of the information will come out in the court process," RCMP spokesperson Marie York-Condon stated in an e-mail. The youth's next court date was not known. Yellowknifer

Athol man arrested on child pornography charges
A 24-year-old Athol man has been charged with offences allegedly related to child pornography. The RCMP's Provincial Internet Child Exploitation Unit has charged Darryl Wayne Baxter with luring a child and six counts of breach of conditions. On Nov. 18, police searched a home in **Athol** and arrested Baxter at the scene without incident. He was held in custody pending an appearance in Amherst Provincial Court Tuesday. Chronicle-Herald, A5

Search for Chris Metallic continues four years later
Four years after a 20-year-old man was reported missing, **Sackville** RCMP continue to investigate the disappearance of Chris Metallic, and police officers will conduct new searches in the Sackville area in the coming days in hopes of getting more information that could help find him. Metallic was reported missing on Nov. 25, 2012, following a party at a residence in Sackville. A few days after his disappearance, footwear belonging to him was located off the Haute-Aboujagane Road. We continue to receive information about the disappearance of Chris Metallic. By conducting these new searches we will be following up on some of that information in order to see if it provides any more information about what happened to Chris. Sgt. Paul Gagné. Metallic is described as aboriginal, measuring six feet tall, and weighing about 180 pounds at the time of his disappearance. He has short, dark, black hair and was last seen wearing a shiny bright blue sweater and jeans. "We continue to receive information about the disappearance of Chris Metallic," says Sgt. Paul Gagné with the Sackville RCMP. "By conducting these new searches we will be following up on some of that information in order to see if it provides any more information about what happened to Chris." Times & Transcript, A8 (Guardian)

Claims of attacker in clown mask could lead to charges in Port Hardy
Port Hardy RCMP are preparing to bring mischief charges against a 19-year-old man suspected of clowning around with the law. The move follows a month-long investigation of a reported October assault where the man said he had been set upon by someone wearing a clown mask. Police allege the report was false and misled the detachment. The incident mirrors the "creepy clown" phenomenon in Canada and the United States that has seen people dress up as clowns to scare or surprise others. Victoria police had an experience with the phenomenon when a man possibly disguised with a clown mask was arrested in October for a burglary at Frank White's Dive Store. Port Hardy RCMP Cpl. Stuart Foster said every report received by the detachment is taken seriously. "Investigations such as these, where there are no witnesses and [they] allege a violent offence, are especially difficult and time-consuming to investigate," Foster said in a statement. He said specialized RCMP units were brought to Port Hardy to help investigators. "It is not only a waste of resources, it is a criminal offence and one for which we will seek charges," Foster said. Times Colonist

Jury Hears Of Suspected
An ex-girlfriend of an accused gangster boss killer told an **Edmonton** jury Tuesday she saw her boyfriend give a suspected gun to one of his drug thugs a few days before the killing. Testifying at the first-degree murder trial of Josh Petrin, Karissa Dow, 24, told jurors she dated Petrin from 2010 to November 2012 culminating in the birth of their daughter following his arrest. 'Patched' member Dow testified that Petrin, 33, revealed to her that he was a "patched" member and a "boss" with the "drug-dealing" White Boy Posse street gang and said he has a WBP tattoo on his arm. (…) Under cross-examination, Dow told

defence lawyer Markham Silver that she never saw Petrin hand anything to Halbauer and agreed she does not know what he might have given him. She also agreed that drugs were sometimes stashed in the same places where guns were. Dow also said in crossexamination that she was pressured to speak with the RCMP and told jurors that one Mountie threatened to have her jailed and to have her newborn baby taken away. She clarified to Rudiak that the officer told her after Petrin's arrest that they could take away her child. She also said the officer told her friends she was going to deliver the baby while in jail. She added her daughter was never taken away and she was never charged. Postmedia Network (Edmonton Sun, A5, Edmonton Journal)

Denecho King murder case moves to preliminary inquiry

A preliminary hearing for a man charged with second degree murder and attempted murder began Monday, almost two years after police found two men seriously injured in a downtown apartment building. John Wifladt, 39, succumbed to his injuries while Colin Digness, who is in his early 40s, was medevaced to **Edmonton** for further medical treatment. Denecho Noel Calvin King, 24, was charged with second degree murder and attempted murder months after police responded to the early morning incident Dec. 14, 2014, at the Sunridge Place apartment building on 51A Avenue. Eleven days have been set aside for NWT Territorial Court Judge Robert Gorin to hear evidence in the case and to decide whether it is strong enough to proceed to trial on the charges police announced against King on May 1, 2015. The Crown may call up to 40 people to testify, defence lawyer Jay Bran has previously said. Crown prosecutor Alex Godfrey was expected on Tuesday to call paramedics who transported the two men to hospital as the hearing continued. A publication ban was imposed on testimony and exhibits, such as photos of items in the apartment. The ban means little can be reported about what occurred. The preliminary inquiry began with testimony from five RCMP officers Monday in Courtroom 4, one of the smallest courtrooms in the building. There was added security, with two RCMP officers keeping watch. A third RCMP officer in a suit watched from the gallery as evidence was given. King also faces a charge in connection with an escape from the North Slave Correctional Centre on Aug. 10. King, wearing grey sweatpants, a white T-shirt with a graphic print, remained in leg shackles during the hearing as he sat beside his lawyer. He listened without any obvious reaction to the testimony of five RCMP officers, slumping in his chair as the hearing wore on through Monday afternoon. The public gallery remained largely empty on the first day of the hearing. Yellowknifer

Sask. community up in arms over RCMP carbine training

Drew Erickson thought he knew what he was getting into when he built his home in Stone Pointe Estates in 2011. Stone Pointe is an up-scale neighbourhood located east of **Regina**. The community has about sixty-five homes, many valued at more than a million dollars. For the last two summers, it has also had some very noisy neighbours. Across the road is the Regina Wildlife Federation and its gun range. At first, Erickson's family heard what they expected: small caliber fire and the odd shotgun. That all changed one summer morning in 2015. "We awoke, about a quarter after seven, to what sounded like automatic rifle fire, very loud, rapid succession." According to the Regina Police Service which uses the same weapon, C8 Carbines are noisier than typical rifles or shotguns because the projectile travels faster than the speed of sound. The gun fire could be heard in Emerald Park and White City two kilometres away. Erickson, who lives just a few hundred metres away, says it's like living in a war zone. He said the gunfire woke his wife, who is from South Africa, and sent her into a panic. "When she heard that noise when she was a kid, that meant somebody nearby was in peril," Erickson explained. It's not just his wife either. When the matter was brought before the RM by Erickson and a group of concerned community members, it was mentioned some members of the group had immigrated to Canada from a war-torn country. Erickson said a man and his wife heard the gunfire on their first day in the community. "She effectively thought she was back in a war zone," he said. "This is not why they came to Canada. This is not why they came to live in a rural community." Erickson says closing doors and windows does little good. He says the RCMP needs to find another range, away from the community. "Our community is at the point where we've done our time, we've taken our turn, this is two summers in a row, and if it's a third it's unnaceptable." CBC News

Body of missing Trail, B.C., senior found - Ida Cragnolini had dementia and had gone missing in the past

The body of a 70-year-old woman with dementia has been found. Ida Cragnolini went missing in **Trail B.C.** on Sunday, according to the RCMP. RCMP, search and rescue teams and members of the public

had been searching for Cragnolini after she left her residence near the Waneta Plaza shopping mall Sunday morning. She was last seen around 4 p.m. PT in the east Trail area. Her body was located before noon on Tuesday in the Miral Heights area not far from where she was last spotted, according to a family friend. CBC News (2016-11-22)

Nunavut police plan "comprehensive review" of coroner jury findings
The **Nunavut** RCMP plans to review and consider recommendations made by the recent coroner's inquest in Igloolik, reporting back to the Nunavut Coroner next year on progress made towards change. That news came in a Nov. 21 news release from the RCMP V Division in connection to the 25 recommendations made by a coroner's jury which looked into the March 2012 death of Felix Taqqaugaq in Igloolik. That news came in a Nov. 21 news release from the RCMP V Division in connection to the 25 recommendations made by a coroner's jury which looked into the March 2012 death of Felix Taqqaugaq in Igloolik. Nunatsiaq Online (2016-11-22)

Three busted as RCMP raids 'sophisticated' drug lab in Ajax
Three men are facing charges after the discovery of what police are describing as a "sophisticated" drug lab in **Ajax**. Investigators spent three days removing chemicals used in the production of ketamine from the residence, at 4 Bunting Court, RCMP said. A search warrant was executed at the house Nov. 18, Mounties said. Some of the chemicals found in Ajax have been linked to a company investigated by the RCMP earlier this month, police said. Two men associated with that company have been charged with selling chemicals knowing they would be used to produce illegal drugs. Inside Halton (2016-11-22)

RCMP Turn to Public to Help Solve Homicide From 2007
RCMP are turning to the public for clues in the 2007 killing of a grandmother in **Portage La Prairie**. Charlene Ward was discovered dead in her home more than nine years ago. On October 31, 2007, Ward went out with friends to Cat & Fiddle Nite Club in Portage La Prairie. She then returned to her home with friends for a party that ended at 8:00 AM the next morning. Ward's body was found about 45 minutes later in her home on 5th Avenue NE. RCMP ruled Ward's death a homicide but to date, no one has been arrested. Officers believe someone has information related to this crime and are asking anyone who can help find Ward's killer to contact them at the RCMP tipline. AM 900 CHML (2016-11-22)

Virden team's Mountie jerseys raise hundreds for charity
A **Manitoba** Junior Hockey League team in Virden, Man. thought their new jerseys would make people smile but had no idea how big of a hit they would actually be. Styled after a Mountie uniform, the Virden Oil Capitals' wore Red Serge shirts, black pants with yellow stripes and brown socks to mimic RCMP dress uniforms on Nov. 12. It was the second year in a row the team temporarily changed their jerseys to honour first responders in the province. "It seemed like the perfect fit," said Brandi Pollock, marketing coordinator with the Virden Oil Capitals, about the decision to recognize RCMP officers. "They came out and you could just see the looks on people's faces ... a lot of excitement." Now for sale on eBay, the team's special uniforms have more than a dozen bids each and are selling for hundreds more than the original asking bid of $80. CBC News (2016-11-22)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Aboriginals seek inquiry into alleged abuse by police
Premier Philippe Couillard has promised to meet with indigenous leaders to discuss ways to investigate alleged "systemic racism" in Quebec. "We're aware of the enormous trauma in aboriginal communities, we're not trivializing it ... we'll find concrete ways to bring some answers," the premier said. Couillard made the remarks Tuesday at the National Assembly, where a dozen women stood wearing small, red felt dresses pinned to their shirts, reminiscent of the red square worn by student protesters in 2012. They said the red dress symbolizes the murdered and missing aboriginal women. The Couillard government has suggested that Canada's national inquiry into missing or murdered indigenous women is a sufficient vehicle for examining alleged abuse of aboriginal women by police forces. But on Tuesday, aboriginal

women argued Quebec's problems will be lost in a national inquiry. Montreal Gazette, A10; Le Devoir; TVA Nouvelles; La Presse Canadienne (L'actualité, Radio-Canada); La Presse; Huffington Post Québec

Anti-violence campaign to begin Friday
A coffee house, panel discussions, the Take Back The Night march and a family day are all part of the list of events on tap for this year's 12 Days to End Violence Against Women campaign. Set for Nov. 25 to Dec. 6, the annual campaign that's organized by a variety of local groups aims to draw attention to the issue of violence against women. Panelists will include Patricia Bacon, a human sexuality expert and executive director at the Blood Ties Four Directions Centre; Mark Rutledge, a White Ribbon Yukon member and father; and Sara Tillett, a counsellor at Golden Horn Elementary School. That will be the first of two panel discussions included in the campaign's schedule. The other one will focus on missing and murdered indigenous women in Canada and is scheduled for noon on Dec. 5 at Yukon College. Whitehorse Daily Star, 5

Elsipogtog hoops player takes a knee in support of missing and murdered aboriginal women
Quentin Sock has some personal experience with the issue of missing and murdered aboriginal women and girls. The 30-year-old student athlete at St. Thomas University, a member of the Elsipogtog First Nation, and the men's basketball team at the school, was one of the organizers of an awareness campaign/protest at the Tommies' Atlantic Collegiate Athletic Association basketball home game against the University of Kings College Blue Devils earlier this month in Fredericton. Before the playing of the national anthem prior to the game, the entire Tommies team quietly took a knee. Sock and team co-captain Jeremy Speller, a native of the Gesgapeplag First Nation in Quebec, bowed their heads and raised a red shawl, a symbol of the plight of missing and murdered aboriginal women across the country. They did so with the blessing of the university president, Dawn Russell, and the university community. Literature handed out with the program, quoting the Native Women's Association of Canada and the Government of Canada, noted that 16 per cent of all women murdered in Canada between 1980 and 2012 were of aboriginal descent and notes that, "the RCMP has identified that there may be 1,181 missing and murdered Aboriginal women and girls." Times & Transcript, D3

Aboriginal women repeat calls for inquiry into alleged abuse by police
Premier Philippe Couillard has promised to meet with indigenous leaders to discuss ways to investigate alleged "systemic racism" in Quebec. "We're aware of the enormous trauma in aboriginal communities, we're not trivializing it ... we'll find concrete ways to bring some answers," the premier said. Couillard made the remarks Tuesday at the National Assembly, where a dozen women stood wearing small, red felt dresses pinned to their shirts, reminiscent of the red square worn by student protesters in 2012. They said the red dress symbolizes the murdered and missing aboriginal women. "It's the province's responsibility to launch an independent inquiry," said Donna Larivière of Quebec Native Women, who categorically rejected the recent conclusions of a Montreal police investigation into Sûreté du Québec officers alleged to have abused aboriginal women in Val-d'Or. Montreal Gazette; CBC News (2016-11-22)

Enquête nationale : la relation entre les autochtones et les forces de l'ordre sera analysée, assure Michèle Audette
La commissaire de l'enquête nationale sur les femmes et les filles autochtones disparues et assassinée, Michèle Audette, assure que la relation entre les autochtones et les forces de l'ordre sera analysée par la commission. Depuis que le Directeur des poursuites criminelles et pénales (DPCP) a rendu publique sa décision de ne pas accuser les six policiers suspendus de Val-d'Or, plusieurs membres des Premières Nations réitèrent leur demande de tenir une commission d'enquête indépendante québécoise sur la relation entre leurs communautés et les forces de l'ordre. La commissaire Michèle Audette a accordé une entrevue à Annie-Claude Luneau mardi après-midi. Elle assure que l'étude des relations entre les peuples autochtones et les représentants des forces de l'ordre sera étudiée lors de la commission d'enquête nationale sur les femmes et les filles autochtones disparues et assassinées. Radio-Canada (2016-11-22)

The girls on Commercial Drive
The number of Missing and Murdered Indigenous Women (MMIW) continues to rise in Canada, and one local woman is working to educate the valley. Sherry Tinsley, owner of A Cut Above in Valemount, has

four red dresses and one empty post in the field beside her store on Commercial Drive. Rocky Mountain Goat News (2016-11-22)

'He's still a coward': Six Nations man who strangled woman pregnant with his baby leaves court a free man
Kent Owen Hill walked out of court a free man on Monday after pleading guilty to manslaughter and being sentenced to time served in the death of Tashina General and her unborn child... In an agreed statement of facts read by Brant County Crown attorney George Orsini, court heard that General met Hill when she was 16 and dating another player on the Six Nations lacrosse team... Orsini said the crime had a significant impact not just on Six Nations but on "other First Nations communities in this country." "They consider Tashina one of those missing and murdered aboriginal women." National Post (2016-11-22)

Aboriginal women repeat calls for public inquiry into police abuse
A dozen aboriginal women traveled to the National Assembly on Tuesday with small, red felt dresses pinned to their shirts, reminiscent of the red square worn by student protesters in 2012, and a message for parliamentarians. They said the red dress symbol is to remember all the murdered and missing aboriginal women. "It's the province's responsibility to launch an independent inquiry ... because we're talking about criminal acts," said Donna Larivière of Quebec Native Women, who categorically rejected the recent conclusions of a Montreal police investigation into Sûreté du Québec officers alleged to have abused aboriginal women in Val D'Or. Quebec's Director of criminal and penal prosecutions decided to forgo charges against the Val D'Or police but charged two retired SQ officers from Schefferville, as a result of the police investigation. "We don't believe in police investigating police," Larivière said. The Couillard government said last week it will let the national inquiry into missing or murdered indigenous women and girls continue the work. But on Tuesday, aboriginal women argued Quebec's problems will be lost in a national inquiry. Montreal Gazette (2016-11-22)

To Remember the Missing and the Murdered (and to Inspire New Music), a Marathon of One
In British Columbia, they call it the Highway of Tears. A 450-mile stretch of road along the Trans-Canada Highway has claimed the lives of dozens of young women, many of them indigenous, who have disappeared on this road or were murdered nearby. Across Canada, the numbers of missing and murdered indigenous young women over the last several decades is exponentially higher, with estimates as high as 4,000. It was the type of news that was hard to ignore in Manitoba, where Tracie Léost, the featured subject of a new video for Cass McCombs's "Run Sister Run" quickly became outraged. "Every second day it seemed like there was another story about a young First Nations female who had gone missing or murdered," Léost remembered recently by phone from Winnipeg, where she is now studying social work at the University of Regina. "And our prime minister at the time, Stephen Harper, denied that there needed to be an open inquiry into it. I kept bringing it up to my indigenous studies teacher until finally he said to me, 'If you want to see changes, why don't you do something about it?' " And so, in August 2015, Léost, a track and field athlete, set out on a four-day solo journey on foot, covering 115 kilometers in a solo run to raise awareness about what she viewed as an unsettling epidemic. Vogue (2016-11-22)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Rendu malade par le pot, il menace Trudeau
Favorable à la légalisation du cannabis, le premier ministre Justin Trudeau a été victime de menaces de mort d'un jeune Montréalais en proie à des troubles psychiatriques aggravés par la marijuana, cet été. «La drogue, je ne veux plus en prendre», a dit ce dernier devant un tribunal après avoir été déclaré criminellement nonresponsable de ces délits, puis enfermé dans un hôpital du-rant deux mois. Selon une décision récente de la Commission d'examen des troubles mentaux, le Montréalais, dont l'identité n'a pas été rendue publique, a acheminé un courriel au bureau du premier ministre, le 10 juin dernier. «Je te jure, Justin, je commence à m'entraîner pour te tuer si tu ne fais rien pour mon cas», a-t-il écrit dans un message confus. Sans réponse, il a ensuite téléphoné au bureau de M. Trudeau et réitéré ses menaces avant d'être arrêté par la GRC. Journal de Montréal, 15

Border agency touts drug, gun seizures

Loaded guns, stolen vehicles, child pornography, weed, booze and tobacco are all things that have been seized by the Canadian Border Services Agency in Atlantic Canada in the last quarter. The agency processed about three million travellers at its 50 service locations in the Atlantic region from April to October 2016. Details of its activities were released Tuesday. On Oct. 3, border officials at the the St. Stephen 3rd Bridge port of entry in New Brunswick searched a motorhome and found four tasers, five pepper spray canisters, a loaded 9mm handgun and a loaded .357 Magnum, which are prohibited weapons in Canada. A traveller got $2,300 in fines after pleading guilty the next day to failing to report weapons and providing untrue statements under the Customs Act. "It is important that anyone travelling to Canada understand that undeclared and prohibited firearms are not allowed in our country," said Calvin Christiansen, CBSA director general for the Atlantic region said in a news release. "We welcome our United States neighbours but remind them to leave their guns at home." On their way to inspect a vessel with three foreign nationals arriving in Shelburne, CBSA officials received a tip that a number of bags containing wine, rum, tobacco and marijuana were found in the woods in the region. Officers were able to determine that the bags belonged to the individuals on the vessel, and each traveller was charged with three offences under the Customs Act: non-report of alcohol, tobacco and marijuana; making false statements; and smuggling. They each pled guilty to non-reporting. Fines of $2,500 (for the captain), $1,000, and $500 were charged to the travellers. Total seizures from the hidden bags and boat totalled 39.9 litres of alcohol, 0.79 kg of tobacco and 17.46 grams of marijuana. CBSA officers, along with members of the Internet Child Exploitation unit of the Integrated Halifax Regional Police/RCMP Criminal Investigation Division unit, discovered child pornography on an electronic device belonging to a crew member while searching a vessel Aug. 16. Chronicle-Herald, A4

2 men charged with conspiracy to smuggle person into U.S. plead not guilty

Two New Brunswick men charged with conspiracy to smuggle a person across the Canada-United States border this summer have pleaded not guilty. Richard Cyr, 50, of Baker Brook, appeared in Edmundston provincial court on Monday and Oneil Devost, 67, of Edmundston, a well-known local country music singer, was represented by his lawyer. Both accused are scheduled to return to court on Jan. 24, 2017, to set a trial date. The charges are related to an incident in July when authorities became aware a 46-year-old woman had entered the United States illegally by crossing the St. John River from the Baker Brook area with a paddle boat, RCMP have said. CBC News (2016-11-22)

Accused UN killer tells undercover cop he dreamed about his arrest

Cory Vallee, a United Nations gang member and accused killer, had a dream he was going to be arrested the day before Mexican police raided his Guadalajara house and took him into custody. Vallee described the dream to an undercover cop posing as a criminal and planted in the accused killer's cell at the Richmond RCMP detachment on Aug. 17, 2014. A secretly recorded video of the conversation was played for B.C. Supreme Court Justice Janice Dillon at Vallee's murder trial Tuesday. "I started packing the day before I got arrested because I had a dream that I got arrested. I swear to God," Vallee said to the cop, whose identity is shielded by a court order. "I had a dream that someone was coming in my house and I woke up and thought I saw a shadow and they were trying to arrest me. It was like a nightmare." He said he started packing all his clothes, books and DVDs the same day. So when police arrived and shouted his name the following day, "everything was in boxes." Replied the undercover cop: "That is f-king trippy." The jail cell conversation took place about 2:40 a.m. after Vallee had been escorted back to Canada by two other RCMP officers. Vallee met the undercover cops at Vancouver airport when they were all placed in the same Canada Border Services Agency holding cell early on Aug. 17. He also said that going to jail won't be so bad, since he had already cut offall contact with family and friends years earlier when he went on the run. Vancouver Sun, A11 (Province), 1

First there was phishing, now we have 'smishing': Spammers are now texting us

If you received a text in the past day or so that dangles the dubious possibility of a big inheritance coming your way, don't worry. You're not alone. Island RCMP say it's just the latest installment of an annoying trend that's known as 'smishing.' "They're fishing for replies," said Cpl. Troy MacLean of Kings district RCMP. "With email, it's called phishing. With text messages, it's smishing." The suspect text appeared in recent days. With generous use of all-caps, the text appears to have been written by someone named Gordon Freeman. And Gordon, for whatever reasons, says he wants to share money with you. "It's urgent

please contact me for an unclaimed benefit payment," reads part of the text. "Ignore it," said MacLean. "Do not respond." Unfortunately, too many people do. About 200 people have been scammed more than $2 million so far this year, according to the federal government's Canadian Anti-Fraud Centre website. CBC News (2016-11-22)

Neutraliser Vito Rizzuto avant qu'il ne soit trop tard
« Lorsque nous avons débuté Colisée, Vito Rizzuto commençait à entrer dans une phase de légitimité. La façon dont il gérait ses investissements et dont il voyait son futur, nous avions le sentiment que si nous n'allions pas le chercher à ce moment, il serait devenu intouchable cinq ou dix ans plus tard. Seulement avec ses placements, il n'aurait plus eu besoin d'être impliqué dans les affaires criminelles », affirme James Malizia. L'actuel commissaire adjoint à la GRC était inspecteur à la Division C (Québec) de la police fédérale au début des années 2000. Il venait de terminer le dossier de Charles Guité, acteur du scandale des commandites, lorsqu'il est devenu le patron de l'Unité mixte d'enquête contre le crime organisé (UMECO). La GRC avait alors mis le parrain de la mafia canadienne, Vito Rizzuto, en tête de liste de ses priorités. La Presse+ (2016-11-22)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Late Mountie honoured at YMCA Peace Breakfast
Peace was everything Lisa Gallagher's late husband fought for. Gallagher, addressing the annual YMCA Peace Breakfast on Tuesday morning, spoke to an audience of Metro Moncton politicians and volunteers about the legacy of her husband, former Codiac RCMP Sgt. Mark Gallagher, and what he taught her. Mark Gallagher died in Haiti in January 2010 when a devastating earthquake hit the country. He died the same day he arrived in the Caribbean nation to serve a six-month stint with a UN mission that was training a national police force. The retired RCMP member had spent the holiday season with his wife and two kids, but felt he still had more to give, and wanted to return to Haiti. "It was only that morning he was leaving, I realized what a brave man he had become," Lisa Gallagher said of her husband of 31 years. During her talk, Gallagher spoke at length about the idea that peace comes from respecting each person and understanding that they have value. Daily Gleaner, B3 (Times & Transcript)

Moncton woman sentenced for kicking Mountie in head
A Moncton woman will spend the next 18 months on probation after assaulting police officers and saying Justin Bourque should have shot more of them. Lia Olivia Chase, whose adoptive father is a retired Mountie, was in court for sentencing on six charges, including two counts of assaulting police, resisting arrest, uttering death threats and two counts of breaching an undertaking by consuming alcohol. Judge Irwin Lampert ordered her to take anger-management counselling, avoid drugs and alcohol, do 30 hours of community service and write a letter of apology to Codiac Regional RCMP. "I would only describe your behaviour as disgusting and disgraceful," said the judge. "To say that about the RCMP, after what's happened in this community in the last couple of years? And your father is a retired RCMP member?" Chase made no comment to the court when given the chance during her sentencing. The prosecutor told the court the incident occurred on Sept. 19, 2015 in Moncton. Her partner called police after a domestic incident, saying she was assaulting him and tearing up the apartment. When they arrived he said she was gone and he didn't want to pursue the matter. Police learned the woman was "wandering the streets intoxicated" and set out to find her. They heard she was hiding in Victoria Park but she fled when they approached. She fell and they found her lying on the ground, barefoot and crying. Times & Transcript, A6

Ex-RCMP recruiter charged with sex assault
A Winnipeg woman has filed a lawsuit alleging a former RCMP recruiter sexually assaulted her in his home. Court records confirm former Const. Michael Adam Timmer, 34, has been criminally charged with one count of sexual exploitation in connection with the alleged August 2014 incident. According to a statement of claim filed last week, the then-17-year-old female met Timmer at a career fair in January 2014. A month later, Timmer - whose image was used on RCMP recruitment posters, the lawsuit alleges - invited the teen to apply to attend a RCMP youth camp in Regina, where Timmer was to act as a chaperone. The teen attended the youth camp the following August. Within days of returning home, Timmer texted her and the two made arrangements to meet for coffee. As the coffee date ended, Timmer

kissed the teen "without her invitation or consent," the lawsuit alleges. Later that week, Timmer invited the teen to a party at his house. "Upon her arrival , it became apparent to (her) that no one else had been invited," says the lawsuit. Timmer then led the teen to his bedroom where he sexually assaulted her, the lawsuit alleges. The lawsuit also names the RCMP as a defendant, alleging the police service breached its position of trust by exposing the woman to "sexual conduct and harm" and took no steps to uncover the alleged abuse. "The RCMP in particular, in placing Timmer in charge of recruits and displaying him on the poster for recruiting as an inducement to the public, had a duty to investigate his character and personality and failed to do such," the lawsuit alleges. Winnipeg Sun, A5

Investigators examining death of man in Prince George jail
An investigation has been launched into the death of a man found unresponsive in a jail cell in Prince George. RCMP say officers responded Sunday night to reports of an intoxicated man causing a disturbance. He was arrested and taken to the police detachment, where he was placed into a cell. RCMP say the unidentified man was found unresponsive during a check at about 2 a.m. Monday and that emergency crews were called. Paramedics took over resuscitation efforts but the man was pronounced dead shortly before 3 a.m. The Independent Investigations Office is now looking into the case in an effort to determine whether there is a connection between police actions and the man's death. Vancouver Sun

Taser-armed police should carry automated defibrillators: Inquest
RCMP members who are equipped with Tasers should also carry an automated defibrillator and be properly trained to operate the device. That was one of the recommendations coming out of a coroners inquest that looked into the death of a Chilliwack man in 2015. Kevin Mukuyama died after police were called to an Oak Street home in February of last year, following reports that a man with a knife was acting irrationally. While attempting to arrest the 42-year-old man, police said, a struggle broke out and a "conducted energy weapon" was used to subdue him. Mukuyama died in hospital of "acute cocaine toxicity during restraint," the coroners report said, complicated by an underlying heart disease. Following a three-day inquest in Burnaby, the coroners jury issued a total of 14 recommendations. Among those was a call for better training of RCMP officers when responding to similar incidents. It called for a requirement that, "all officers certified to use a CEW be simultaneously trained in advanced emergency first aid, specifically including the use of an AED (automated external defibrillator)." Chilliwack Progress (2016-11-22)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

Territorial government preparing for federal marijuana legalization
The territorial government has formed an inter-departmental working group to prepare for the eventual legalization of marijuana across Canada. The group is also in discussions with the federal government, according to Department of Justice spokesperson Sue Glowach. The task force was established by the minister of Justice and Attorney General of Canada, the minister of Public Safety and Emergency Preparedness and the minister of Health, according to Glowach. She stated the task force's mandate is to inform the federal government's commitment legalize and regulate marijuana. The report is expected to be released to federal ministers by the end of the month ahead of next April's anticipated marijuana legalization legislation. "The information on potential systems for production, distribution, promotion and taxation provided in the report should make it possible to determine what the role of the ... territories will be," she stated. Yellowknifer

Pour ou contre la légalisation de la marijuana?
C'est au printemps 2017 que le gouvernement Trudeau déposera son projet de loi pour légaliser la marijuana à des fins récréatives. D'ici le 30 novembre, le Groupe de travail sur la réglementation et la légalisation de la marijuana, présidé par Anne McLellan, déposera ses recommandations au gouvernement. Plus de 30 000 commentaires ont été émis depuis le début des consultations, dont 500 de différentes organisations. Pour ou contre la légalisation de la marijuana? Les partisans (Line Beauchesne, professeure de criminologie à l'Université d'Ottawa, et Philippe Hurteau, chercheur à l'Institut de recherche et d'informations socio-économiques) en débattent avec les opposants (Jean-Pierre

Chiasson, médecin spécialisé en toxicomanie et fondateur de la Clinique Nouveau Départ, et Claude Carignan, leader de l'opposition officielle au Sénat). Radio-Canada (2016-11-22)

La consommation de cannabis bondit de 25 % chez les Québécois et les Québécoises
Au moment où le processus de légalisation de la marijuana pour 2017 semble bien enclenché au Canada, des données publiées par l'Institut de la statistique du Québec (ISQ) révèlent que la consommation de cette drogue chez les personnes de 15 ans et plus a bondi au Québec de 25 % entre 2008 et 2015, passant de 12 à 15 %. L'étude de l'ISQ précise que cette hausse est surtout attribuable à la consommation dite « occasionnelle », soit une personne ayant consommé du cannabis moins d'une fois par mois ou d'une à trois fois par mois au cours des 12 mois ayant précédé l'enquête. L'enquête révèle par ailleurs que c'est dans la population des 18 à 24 ans que l'on retrouve la plus forte proportion de consommateurs occasionnels. Radio-Canada (2016-11-22)

Reining it in - Canada puts in new rules for prescribing medical marijuana to veterans
The Canadian government is slashing the limit on how much veterans can be prescribed under federal rules, from 10 grams per day to just three, and putting a hard cap on how much marijuana should cost, at $8.50 a gram. That brings the rules in line with Health Canada recommendations, and may help curb runaway costs for the Veterans Affairs Canada drug insurance program. VICE News wrote last week that the program was facing staggering cost overruns, while fears abound that veterans were being prescribed far more marijuana than needed. "This is just our starting point," promised Veterans Affairs Minister Kent Hehr in making the announcement. He blasted the previous government for dispensing marijuana to veterans "with no policy in place. "It's time to change that." The new rules are not absolute. Veterans who are currently receiving more than the three grams will be able to continue getting the drugs until May 21 of the coming year, and any veteran who wishes to continue receiving more of the plant will need a special exemption. Vice News; 45e Nord (2016-11-22)

Three of the seven Ottawa pot shops raided by police are back in business
Three of the seven pot shops that were closed by police in raids earlier this month have reopened. The WeeMedical Dispensary on St. Laurent Avenue was back in business Tuesday, after its sister Green Tree stores on Preston Street and Montreal Road opened on the weekend. The stores are low on stock, carrying only a few jars of dried weed. All of their cannabis products were seized by police during the raids on Nov. 4. The seven raided dispensaries were all operated by a B.C.-based outfit. The other four remain closed, including one on Bank and Hunt Club that was evicted by the landlord after the clerk sold pot from a hole carved into a boarded-up storefront. Both Green Tree stores were selling weed to customers over the age of 19 on Monday who filled out a form listing their name, address, doctor's name and "medical conditions." The form includes a waiver that customers use the products at their own risk and Green Tree is not liable for damages. Ottawa Citizen (2016-11-22)

Cannabis, dépendance et développement du cerveau
Un rapport final sur la légalisation de la marijuana sera remis aux ministres fédéraux avant la fin du mois. À l'occasion, Radio-Canada a abordé la question avec un infirmier spécialisé en toxicomanie. Jean Clermont-Drolet est en faveur d'une loi fédérale qui légaliserait et encadrerait l'utilisation du cannabis. Le cannabis thérapeutique qu'il juge d'ailleurs extrêmement utile chez certaines personnes qui souffrent de maladies chroniques. L'alcool est beaucoup plus dangereux que la marijuana en termes de dépendance, selon l'infirmier. Il explique que la consommation d'alcool remplace à long terme des substances produites naturellement par le cerveau, ce qui crée des symptômes « très physiques » lors d'un sevrage. Radio-Canada (2016-11-22)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Big Brother sleeps easy
An opinion piece states, "The revelation that Montreal police secretly monitored several journalists' smartphones for months, ostensibly in hopes of discovering the source of internal information leaks, has brought home for many people the troubling reality of government snooping. The fact that thousands of students recently lined up to watch whist leblower Edward Snowden at a video conference at McGill

University is another sign of the public's growing concern about respect for the right to privacy. Indeed, it is not just journalists who are targeted by electronic surveillance. Revelations about the National Security Agency (NSA) in the United States also touch Canadians, since in the age of the Internet and social networks, telecommunications knows no borders. It is reasonable to imagine that practically all our communications could be intercepted, filtered and recorded by governments. This is now the world in which we live. Thanks to Snowden's revelations, Canadians know our federal government is actively helping the United States with surveillance programs of its own. For example, it was revealed in April that the RCMP had decrypted about one million private messages from BlackBerry smartphones. In addition, we know that the number of communications intercepted in Canada grew by a factor of 26 in 2015, without the authorities giving any reasons. This opacity is at the heart of the problem: "Big Brother" is completely lacking in transparency. A Federal Court ruling revealed recently that the Canadian Security Intelligence Service (CSIS) had acted illegally by conserving personal data for 10 years. It is alarming to discover just how unclear the limits imposed on surveillance agencies and police forces are. It is probably this lack of clarity that allowed Montreal's police force and the provincial Sûreté du Québec to put so many journalists under watch for such specious reasons." National Post, A11

De la colère à l'action

Un article d'opinion note, « S'il veut faire toute la lumière sur les violences subies par les femmes autochtones, le gouvernement Couillard doit commencer par ouvrir les yeux. Depuis une semaine, son plan d'action se résume ainsi : se cacher derrière la commission d'enquête fédérale, et ne pas faire grand-chose en même temps. M. Couillard a d'abord proposé une vague « table de concertation ». Mais avant de lancer cette idée, il aurait dû consulter les communautés touchées. Acculé au mur, il accepte maintenant de le faire. Il a parlé hier avec le chef de l'Assemblée des Premières Nations du Québec et du Labrador, et d'autres entretiens sont prévus dans les prochains jours. La pression augmente pour déclencher une enquête judiciaire québécoise sur les relations entre les femmes autochtones et les policiers (violences sexuelles, abus de pouvoir et autres formes de discrimination). Québec refuse de bouger, en invoquant que le fédéral fait déjà ce travail avec la nouvelle commission d'enquête lancée sur les femmes autochtones tuées et disparues. Cette excuse ne convainc pas. Certes, la commission fédérale se penchera entre autres sur le Québec, et son mandat inclut maintenant les violences sexuelles. Mais le Canada est un vaste pays, et le temps de la commission sera limité. Le gouvernement Couillard pourrait rétorquer que la commission pourra compléter cet examen, car les causes sont en partie déjà connues. Mais si c'est le cas, cela signifie qu'on les connaît aussi déjà assez pour trouver des solutions ! Or, Québec n'a encore rien proposé pour mieux former les policiers et protéger les femmes. Le refus de Québec aurait également été plus crédible si les policiers étaient eux aussi prêts à agir. Mais contrairement à la Gendarmerie royale du Canada, la Sûreté du Québec (SQ) refuse de reconnaître la discrimination envers les autochtones. » La Presse, 2

OTHER / AUTRES

NIL

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
December 28, 2016 / le 28 décembre 2016

The Daily Media Summary can also be accessed through Newsdesk / La Revue de presse quotidienne peut également être accédée via InfoMédia

TOP STORIES / ACTUALITÉS

RCMP wary of Hells Angels' return to Maritimes
Andy Cook knows the Hells Angels, and what they bring with them. The bespectacled RCMP corporal has crossed paths with Canada's most notorious outlaw biker gang before, during stints in Ontario and British Columbia, and he is not happy they are setting up in Prince Edward Island, where he works now. "It doesn't sit well with me for them to be here," said the 20-year veteran Mountie. "I've seen them in action and they bring violence with them and they bring drug trafficking with them." The Angels were without a beachhead in the Maritimes since police smashed the former Halifax chapter in 2001. The raid led to the imprisonment of four of its seven members and the closing of the chapter after the clubhouse was seized by justice officials. But the gang has begun to re-assert itself, cementing its presence mainly through affiliate or so called "puppet clubs" in Nova Scotia, New Brunswick and P.E.I. A New Brunswick chapter of the Nomads is now "full patch H.A.," said Cook. Canadian Press (Chronicle Herald, A1, Montreal Gazette, Vancouver Sun, The Guardian, Cape Breton Post, Leader-Post, Windsor Star, National Post, Edmonton Journal, Calgary Herald, Daily Gleaner, Telegraph Journal, Times & Transcript, Ottawa Citizen); Globe and Mail

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

Wildfire, fentanyl top mountie issues

Claire Theobald sat down with deputy commissioner Marianne Ryan, commanding officer of the Royal Canadian Mounted Police in **Alberta**, to discuss the challenges faced and triumphs achieved by RCMP officers in 2016, and where their focus will be in 2017 (…) Q Is there any one event (from 2016) that stands out in your mind? A The (Fort McMurray fire) evacuation was absolutely outstanding. It felt like we were in a tinder box … I don't think anyone predicted the devastation the fire would take in Fort McMurray (…) Q The RCMP are no strangers to drug crimes, but this year saw the rise of deadly opioid abuse, including fentanyl and carfentanil. A I liken the fentanyl crisis to reverse Russian roulette, where the chamber is loaded and there is one blank. That's what you are playing with when you are involved in illicit drug use … do you want to keep playing that game? Q How is the RCMP addressing this opioid crisis? A On a national and international level, we are working with China and the (Canada Border Services Agency) on the illicit importation of what we call precursors, which are the chemicals used to make fentanyl. We've been involved through the ALERT teams in several high-profile seizures. It is a multi-faceted challenge and it is not just a law-enforcement issue, it is a community issue, and we continue to view it as a big priority for us and for all law enforcement in Alberta (…) Q The RCMP conducts surveillance on individuals identified as terrorist threats, but how else is the RCMP getting ahead of the issue? A Another key component that has proven to be a big success for us is the outreach program, and that's where we have highly skilled officers who can go into communities, establish that trust and respect, and develop those relationships so that people in the communities would be more open to talk to police about their concerns and the what-ifs. Q Technology seems to be as much of a blessing as it is a curse for the RCMP, creating new investigative tools while also opening new avenues for crime. Going forward, how is the RCMP keeping up with the growing issue of cybercrime? A Apart from fentanyl, it is going to be one of our biggest challenges. Postmedia (Calgary Herald, A5; Edmonton Journal, Calgary Sun, Edmonton Sun) (2016-12-27)

Yukon RCMP dealt with community tragedies and triumphs in 2016 - From horrific murders to the royal visit, the police saw life in the territory first hand

RCMP officers in Yukon faced various challenges in 2016, but also did much they can be proud of according to Supt. Brian Jones, the Officer in Charge of Criminal Operations for the **Yukon** RCMP. Jones said the past year was particularly tragic for the community of Watson Lake. "Unfortunately Watson Lake had a summer that I think many of the individuals in that community would like to forget," said Jones. In July an 11-year-old boy was killed after a collision with a vehicle. His death came just a week after the alleged murder of Watson Lake resident 36-year-old Andy Giraudel. A 22-year-old man was charged in his death. CBC News (2016-12-26)

RCMP warn of contaminated drugs

Three people in Fort Chipewyan overdosed on illegal drugs believed to be laced with fentanyl, police say. "There is a possibility that there are contaminated drugs on the street," Cpl. Erika Laird with the **Wood Buffalo** RCMP said Tuesday. On the night of Dec. 22, Fort Chipewyan RCMP were called to help a person suspected of overdosing. Just a few hours later, early on Dec, 23, Mounties were called to another suspected overdose, this time involving two people. All three received medical attention and have since recovered. Investigators believe all three had consumed another illicit drug without knowing it was contaminated with fentanyl, an opioid that can be 100 times more potent than morphine. Between January and September this year, 338 Albertans died from opioid-related overdoses. Fentanyl was responsible for 193 of those deaths. Postmedia Network (Edmonton Journal, A6, Edmonton Sun)

Possible changes coming to emergency services in Metro Edmonton

A new way of looking at policing, and the prospect of handling fire on a regional basis are two changes emergency services that could see in metro **Edmonton**. It's one of many ideas the mayors will work through after being mandated by municipal affairs minister Danielle Larivee. "In the mandate review for the regional board, they've asked us to take a closer look at regional services," Mayor Don Iveson confirmed in his annual year end interview with 630 CHED. (…)For police Iveson said it could be a mix, with RCMP working at Edmonton's new borders, and the Edmonton Police Service handling the vast majority of the city. "Sounds like it takes 16 RCMP officers to police the annexation area that we would potentially inherit through that process and Edmonton Police Service, because they deploy resources differently has said they need 60 rather than 16." "Perhaps in the more rural areas of the south side of the

city, maybe even in the north east where it's still more rural maybe it makes sense for us to contract with RCMP if they're able to deploy and cover that at a lower cost." News Talk 770

RCMP investigate suspicious death on Paul Band First Nation
Mounties were asking for tips from the public Monday night after a person was found dead on a First Nation west of Edmonton. A body was found in the area of Sundance Road on the **Paul Band First Nation** about 2:15 p.m. Monday, police said in a news release. Stony Plain RCMP said the death was suspicious, and have called in the Edmonton major crime unit to investigate. An autopsy is scheduled to take place in the coming days. Postmedia (Edmonton Journal; Edmonton Sun); CBC News (2016-12-27)

RCMP looking for missing Innisfail teen
Mounties out of **Innisfail** are looking for a 15 year old girl not seen since 10:30 Tuesday Morning. RCMP say they are worried about Starla Neufeld. They think she may have an injury and could require medical attention. Neufeld is 5'4" and about 125 lbs with a slim build and shoulder lenght reddish brown hair. She was last seen in Innisfail wearing a black hooded sweatshirt. 630 CHED (2016-12-27)

One of 2 missing females found by Surrey RCMP
Surrey RCMP have found one of the two young women who went missing over the holidays. The 15-year-old was found safe and sound, police say. Police continue to look for 24 year-old Ilse Mackie. CBC News (2016-12-27); Radio-Canada (2016-12-26)

Police ask for help to find missing Moncton teen
Codiac RCMP are seeking the public's help in finding a 15-year-old boy who has been missing since Thursday. Zackery Hill of Moncton was last seen by his family on Dec. 22. In a police press release, Hill is described as 5'2, weighing 104 pounds with green eyes and light brown hair. Mounties have been trying to locate him through known friends and acquaintances, but have not had any success. Anyone who has seen Hill since Dec. 22, or has information as to his whereabouts, is asked to call the RCMP. Times and Transcript, A4 (2016-12-26)

Colten Boushie shooting in review
The top crime story in the province in 2016 erupted in August on a farm in the rural municipality of Glenside. The shooting death of Colten Boushie, a 22-year old from **Red Pheasant First Nation**, sparked outrage among First Nation people and caused a social media firestorm...The case fueled racial tensions from the beginning, starting with a news release from the RCMP that described an initial confrontation on the property. Battlefords News-Optimist (2016-12-26)

Un policier récompensé pour son rôle dans la Grande traversée
La Gendarmerie royale du Canada (GRC) a récemment récompensé le bénévole responsable de la sécurité pour la Grande traversée (LGT), ce relais pan-canadien de jeunes cyclistes organisé par une équipe de bénévoles et le Conseil scolaire francophone de la Colombie-Britannique. Le gendarme Ivan Provost, le coordonateur national de la sécurité de la Grande traversée, a reçu une citation du commandant de la **Division C** de la GRC pour son dévouement. Encore une fois cette année, une équipe de bénévoles dévoués s'affairent à préparer un nouveau tracé de la Grande traversée (LGT) pour permettre à 280 jeunes de parcourir environ 300 kilomètres à vélo en trois jours. Pour la cinquième Grande traversée, le relais commencera à Victoria pour finir au Nouveau-Brunswick. Cela veut dire des dizaines et des dizaines de municipalités et de villes parcourues. Le gendarme Ivan Provost, des Laurentides au Québec, est responsable de faire approuver le trajet de la Grande traversée chaque année. Pour ce faire, il accomplit des mois de travail bénévole. « Ivan c'est notre liaison entre les villes, les municipalités, les provinces, les services de police et l'équipe qui fait l'itinéraire de LGT », explique le fondateur de la Grande traversée, Laurent Brisebois. Radio-Canada (2016-12-26)

RCMP make multiple arrests in child abduction investigation
On December 20, 2016, just before 5:30pm, **Blue Hills** RCMP were dispatched to a call of an abduction of an 11-year-old girl in Brandon, Manitoba. Police were provided a description of a vehicle, and within minutes, officers had located the vehicle heading eastbound at the intersection of Highway 1 and Highway 5. My Steinbach (2016-12-25)

New top cop spent part of childhood in Yukon
When he was in the sixth grade, Scott Sheppard used to bang on the door of the Whitehorse RCMP detachment and ask officers for stickers to put on his bike. "I sort of took on that iconic school kid's dream of one day being a Mountie," says Sheppard, who was recently named the new commanding officer of **Yukon** RCMP ("M" Division). The appointment, he says, "closes the loop in many ways." Sheppard, who's from B.C., but lived in the Yukon for two years as a child (his father worked here as a welder), always wanted to join the RCMP. Twenty-seven years ago, he was hired on in Kamloops. His first posting was in Manitoba. Over the years, Sheppard has received a Queen's Jubilee medal for his work. He has also presented on Olympic security programming to officials from the United Nations, Geneva, and INTERPOL. Whitehorse Star, 3 (2016-12-24)

Year-end warrant blitz nets Red Deer RCMP dozens of offenders
A year-end campaign to clear outstanding warrants by **Red Deer** RCMP netted 36 wanted offenders this week. During the sweep, police checked 199 people and residences, executing 83 warrants and laying 117 charges for offences ranging from aggravated assault to drug offences and theft, said Insp. Gerald Grobmeier. CBC News (Yahoo News); Red Deer Advocate (2016-12-24)

Investigation continues
Police believe the bomb threat in September that led to a provincewide evacuation of schools in **P.E.I.** originated in the U.S. RCMP Staff Sgt. Kevin Baillie told The Guardian Friday that the RCMP is working with law enforcement south of the border to try to establish exactly from where and from whom the bomb threat was made. "To date, we haven't laid any charges - certainly not ruling out that at some point we couldn't have the evidence to lay a charge - but to date we haven't positively identified who is responsible for the bomb threat," says Baillie. Police received a fax threatening bombs in multiple P.E.I. schools would be detonated on Sept. 21. Guardian (2016-12-24)

Two charged after police seize cocaine and pot
Police seized cocaine, marijuana and drug trafficking paraphernalia after searching a property in **southwest Edmonton** on Thursday. RCMP officers seized 253.3 grams of cocaine after executing a search warrant on a vehicle in southwest Edmonton. They subsequently arrested two people. At a residence, police then seized an additional 385.5 grams of cocaine, eight grams of marijuana, Canadian currency and items related to drug trafficking. Mounties from the Stony Plain, Spruce Grove and Enoch drug sections were involved in the joint investigation. Postmedia Network (Edmonton Journal) (2016-12-24)

RCMP allege influence peddling
Newly unsealed court documents give a greater glimpse into the extent of the RCMP's investigation into the **Winnipeg** police headquarters scandal. The $214-million downtown project has been the subject of a two-year investigation by RCMP, which began when officers executed a search warrant in December 2014 at Caspian Construction, the company contracted to build the police headquarters. The project included $79 million worth of cost overruns and was completed after three years of delays. In files presented by Mounties to a judge in order to obtain financial records, RCMP allege Armik Babakhanians, owner of Caspian Construction, used his relationship with the city's former project director on the project to influence the hiring of "his close associates." RCMP Const. Christopher Haskins, in a sworn affidavit, alleges Babakhanians and associates Peter Chang and Patrick Dubuc agreed to offer project director Ossama AbouZeid a $600,000 reward "for showing favour" to the trio. Postmedia Network (Winnipeg Sun) (2016-12-24)

Man faces child pornography charges
Police have charged a **Plympton** man with possession and distribution of child pornography. On Thursday, the RCMP Internet child exploitation unit executed a search warrant at a home in Plympton and arrested 55-year-old Daniel Joseph Melanson. Melanson has been charged with the distribution of child pornography, possession of child pornography, unsafe storage of a firearm and unauthorized possession of a firearm. Chronicle Herald (2016-12-24)

Comox Valley RCMP issue gift cards not tickets
"Good afternoon how are you? I'm Perry with the **Comox Valley** RCMP traffic section, do you have your driver's licence with you?" asked Comox Valley RCMP Constable Perry Snyder who had a driver pulled over near the 5th Street bridge in Courtenay. CHEK News (2016-12-24)

RCMP investigating suspicious death in Cambridge Bay - Police received report of deceased female in community Friday morning, treating death as suspicious
RCMP in **Cambridge Bay** are investigating after a woman was found deceased in the community Friday morning. According to an RCMP news release, officers received notice of a possible deceased female in the Nunavut community at about 10:30 a.m. Friday. Police then attended the location, confirmed the deceased female, and opened an investigation. In the release, police say they are treating the death as suspicious. Iqaluit's "V" Division Major Crime Unit and the Forensic Identification Unit, as well as the office of the chief coroner, will be assisting Cambridge Bay RCMP with the investigation. CBC News (2016-12-23)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Panama Papers to pesticide problems: 10 memorable I-Team stories from 2016
... Unresolved: Investigating MMIW - Partnering with the CBC Indigenous Unit and our CBC colleagues across Canada, we took a closer look at 34 cases involving the deaths or disappearances of Indigenous women in which foul play had been ruled out. The families of the women didn't agree with those assessments, and as our investigations unfolded we found more unanswered questions. In fact, the one thing these cases seemed to have in common was that they all begged for more in-depth investigation. CBC News Winnipeg (2016-12-26)

Weighill talks crime, marijuana and MMIW in year-end interview
For the first time under Chief Clive Weighill's tenure, crime in Saskatoon is going up. This city has the highest murder rate in the country and thefts and break-ins are spiking. The StarPhoenix sat down with the city's police chief to talk crime and what's next for 2017... As the past president of the Canadian Association of Chiefs of Police, you've been tapped to be the liaison for the inquiry into missing and murdered indigenous women. What is the issue as you see it, and where should the inquiry go? A: Certainly it has caught the national attention because of the awareness and the issue itself. This is a huge issue, not only with missing and murdered indigenous women and girls, but also with men. This is a problem we've got in Canadian society with a huge marginalized population. There are reasons for that - the residential schools, colonization. But we are all left here now trying to deal with this. We have to start looking forward. I think one of the main things we have to look at is the root causes. What is causing this? In my opinion, it's poverty, it's (lack of) housing, it's racism, it's disadvantage. It's putting women and girls in vulnerable situations. So if we can't come to grips and solve those root causes we are going to continue to investigate cases of missing and murdered indigenous women..." StarPhoenix (2016-12-24)

PM wants 'huge issues' addressed
Much more needs to be done to confront the crime of sexual abuse of children in indigenous communities, says Prime Minister Justin Trudeau, who anticipates the national inquiry into missing and murdered indigenous women and girls will reveal "huge issues" that must be addressed. "I think part of what that national inquiry is going to reveal is there are deep challenges that we have to address that go beyond just lack of adequate policing or enforcement or justice systems," Trudeau said during a year-end roundtable interview with The Canadian Press. "There are huge issues that we have to work with as partners with indigenous leadership, indigenous communities." The issue of missing and murdered women is symptom of a constellation of social ills but a dominant theme is rampant childhood sexual abuse, say victims - including 59-year-old Bernie Williams, who wants the inquiry's commissioners to confront head-on what many say has been an open secret in indigenous communities for decades. Canadian Press (Chronicle Herald; Whitehorse Daily Star; Record; StarPhoenix) (2016-12-24)

Top 10 stories of 2016: First Nations fight for missing murdered women, other issues
The year 2016 saw local First Nations bands raising several issues and continuing to fight for their rights on numerous fronts. It's a fight that shows no sign of ending but this year in the Central Okanagan there were several events that raised the public profile. The Okanagan Indian Band held a rally over missing and murdered women, the Okanagan Nation Alliance re-introduced salmon into Okanagan Lake and the Westbank First Nation saw a historic change in leadership, making First Nations one of our top stories of 2016, coming in at No. 8. Capital News (2016-12-24)

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

Terror tip ignored: Canuck cops jail man who warned of Berlin attack
A man who warned the RCMP that terrorists were set to launch an attack in Berlin - three days before a truck plowed into a German Christmas market - was jailed when his claim was dismissed as a "hoax." Stephen Clements, who spent five days in jail before receiving bail, was charged with hoax of terrorist activity last Saturday. Two days later the Berlin terror attack killed 12 people. Did the 57-year-old tipster have legitimate information about the impending horrific attack - or was it just a guess? "That would be one hell of a coincidence," one veteran GTA officer, who asked not to be identified, said Friday after learning of the man's arrest. Multiple sources confirmed a man contacted the German Consulate in Toronto on Dec. 16 claiming a terror attack was going to occur over the weekend. Postmedia Network (Winnipeg Sun; Ottawa Sun; Brantford Expositor) (2016-12-24)

Province's first anti-human trafficking director brings first-hand experience to the job
Ontario's first director of its anti-human-trafficking office brings to the job not only nearly two decades of work history in tackling the issue, but first-hand insight, having lived through the experience herself. "I was trafficked at 13," Jennifer Richardson says in an interview. "For three years. Across pretty much every province in Canada, and into the U.S. a little bit, by a quite organized group." Her own experience as a survivor of sex trafficking - where she endured physical and emotional abuse, along with manipulation - led her into the field. Her exit occurred in Montreal, after the police intervened in the wake of an assault (…) Human trafficking is defined as recruiting, transporting or exercising control over a person to exploit them, typically through sexual exploitation or forced labour. The majority of trafficking cases in Canada are domestic, rather than cross-border, and most reported domestic cases are sex trafficking, according to the RCMP. Ontario has about 65 per cent of the human-trafficking cases reported to police in the country, and the RCMP has said the province is a major hub for trafficking in Canada. The human cost is steep, as trafficking can inflict serious and long-term trauma on survivors. In response, the Ontario government said in June it will spend up to $72-million over four years in a new anti-trafficking strategy, becoming the third province in Canada to adopt a plan to fight human trafficking. Globe and Mail, A11 (2016-12-27)

Parents of Canadian man held hostage in Afghanistan speak out about new video
The parents of a Canadian man held hostage in Afghanistan say a recently released video of their son and his family marks the first time they've seen their two grandchildren, who were born in captivity. Canadian Joshua Boyle and his American wife, Caitlan Coleman, were kidnapped in 2012 while backpacking in northern Afghanistan. In the video uploaded to YouTube earlier this week, Coleman -- sitting next to her husband -- urges government on all sides to reach a deal to secure the family's freedom. Canadian Press (Guardian) (2016-12-24)

Liaisons dangereuses
Selon les recherches de notre Bureau d'enquête, l'une des visites de l'espion russe Evgueny Buryakov au pays correspond à un événement de l'Association d'affaires Canada-Russie-Eurasie, vouée à la promotion des liens économiques entre les deux nations. En mars 2013, il s'est rendu à Toronto pour une rencontre de cette organisation, en tant que représentant de la banque d'État russe Vnesheconombank, selon une infolettre retrouvée en ligne. Le but de son voyage était de «négocier avec des membres et des compagnies qui ont des projets en Russie et sont intéressées à collaborer», selon le document de

l'Association, connue sous son acronyme anglais CERBA. Agence QMI (Journal de Québec; Journal de Montréal); Agence QMI (Journal de Québec; Journal de Montréal) (2016-12-24)

Fears Growing Islamic State Successfully Weaponizing Refugees
Western security officials are increasingly worried that the Islamic State terror group may be a step ahead of their renewed efforts to stop terrorist infiltration of their countries... "When it comes to refugees being radicalized after they come to a host country, this is quite low in number, actually," according to Mubin Shaikh, a terrorism expert who has previously worked with the Canadian Security Intelligence Service. Voice of America News (2016-12-24)

The 'app of choice' for jihadists
When the Islamic State was seeking volunteers for a holiday killing spree in Europe, it sent word over its favourite social-media channel: the messaging service known as Telegram. "Christmas, Hanukkah, and New Years Day is very soon," began a Dec. 6 posting on one of the terrorist group's usual Telegram bulletin boards. "So let's prepare a gift for the filthy pigs/apes." ... The words and images flew across the globe over a network that terrorist leaders describe as ideal for their purposes: one that is highly discreet, with its heavy encryption and secret chat rooms, but also highly permissive, allowing violent jihadist groups to exchange ideas and spread propaganda with minimal interference. The same conclusion has been reached by terrorism analysts who say Telegram is now overwhelmingly preferred by extremist groups such as the Islamic State, in part because the company has failed to adopt the aggressive measures used by its competitors to kick terrorists off its channels. Canadian Press (Record) (2016-12-24)

'Cornbread Mafia' toast?
Canadian cops have arrested Kentucky crime kingpin, Johnny Boone, after he was on the run for eight years. Boone had been accused of running a marijuana empire in rural Kentucky, producing an estimated 182 tonnes... The U.S. Marshals released the following statement: "On December 22, after an extensive eight-year fugitive investigation into the location of John 'Johnny' Boone, information was developed that led the U.S. Marshals Service to a small town outside of Montreal, Canada. "This information was passed on to law enforcement in Canada and Boone was arrested today by Canadian law enforcement officials in Montreal." Sun Media Corporation (Toronto Sun) (2016-12-24)

Trois hommes de Saint-Jérôme arrêtés en Ontario avec trois tonnes de tabac de contrebande
Trois Québécois de Saint-Jérôme ont été arrêtés en Ontario cette semaine avec en leur possession trois tonnes de tabac haché fin de contrebande. Mardi, les membres du Groupe de travail régional de Cornwall (GTRC) ont intercepté un fourgon quittant une propriété riveraine de South Glengarry, en Ontario. Les trois hommes de Saint-Jérôme ont alors été appréhendés, ont annoncé les autorités vendredi matin. Jonathan Boulay, 22 ans; David Dore, 33 ans; Nancy Slavinsky, 42 ans comparaîtront à la Cour provinciale de Cornwall le 31 janvier 2017. Ils ont été libérés sur engagement. S'ils sont reconnus coupables, chacun d'eux pourrait se voir infliger une amende minimale de près de 800 000 $ pour les accusations de ressort fédéral et d'environ 1,4 million $ au provincial ou d'une peine d'emprisonnement. Le GTRC est une force policière mixte composée de la Gendarmerie Royale du Canada, de la Police provinciale de l'Ontario et du ministère des Finances de l'Ontario. Agence QMI (Journal de Montreal, TVA Nouvelles) (2016-12-23)

Lang tops Postmedia's list of best politicians
Yukon Senator Dan Lang has been named the best politician in 2016 by Postmedia in a recent column published across Canada in all SunMedia publications. "A lot of Canadians think senators don't do anything and that the Senate should be abolished," columnist Anthony Furey wrote. "They might change their tune if they knew more about what some of the hardworking members of the Upper Chamber were up to in 2016. "For example, Daniel Lang, the Conservative Senator representing Yukon. "Throughout the year, Lang was a tireless advocate on the terrorism file in his capacity as chair of the Senate Standing Committee on National Security and Defence. "He drew attention to the fact the RCMP knows about dozens of wannabe jihadists suspected of breaking the law but who, for some reason, haven't being charged. "'Why isn't anyone being charged for being involved in these activities?"' asked Lang, during committee testimony by CSIS head honchos. "'Why are we leaving them on the street? ... Am I missing

something here?' "Just the other week, Lang embarked on a campaign to get his colleagues' backing to amend Liberal legislation removing the government's power to strip dual nationals of their citizenship, if they're convicted of terrorism," Furey wrote. Whitehorse Daily Star, 4 (2016-12-27)

Les soldes d'après Noël, une mine d'or pour les fraudeurs
C'est le temps des soldes d'après Noël, une période de l'année où les consommateurs se tournent beaucoup vers Internet pour profiter des meilleures aubaines. Mais il n'y a pas que pour les consommateurs que les opportunités sont alléchantes. Les fraudeurs aussi en profitent! La nouvelle tendance, profiter de la hausse du nombre de transactions en ligne et cibler les acheteurs inattentifs ou pressés, pour leur soutirer des informations personnelles, estime la Gendarmerie royale du Canada (GRC). « Internet ouvre un éventail de possibilité pour les fraudeurs », explique le coordonnateur de l'escouade contre la fraude à la GRC, Guy-Paul Larocque. « On voit des anciennes fraudes recyclées grâce aux technologies du jour. Les chiffres sont de plus en plus alarmants. » La technique la plus commune est l'hameçonnage, un courriel bidon qui ressemble en tout point à celui d'un commerce, ou d'une institution financière et qui demande au destinataire d'entrer des informations personnelles. Radio-Canada (2016-12-27)

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

Riding along again: RCMP changes policy on volunteers
The RCMP is pledging to reinstate some volunteer auxiliaries to their former role — but the policy will change depending on local departments' wishes. Earlier this year RCMP prevented auxiliaries from going on ride-alongs with regular officers and barred them from taking part in traffic stops, citing safety concerns. On Thursday, RCMP announced the program will re-launched — with certain changes. Auxiliaries will be divided into three 'tiers' of responsibility. Local RCMP divisions in consultation with provincial and territorial governments will chose local volunteers' level of participation and responsibility. That flexibility makes sense, says Coralee Reid, who represents the RCMP in Yukon. "Given the diversity of our country, locations where the RCMP operate and and different threat environments, a one-size-fits-all model was not feasible," she writes. The change is supported by Yukon Senator Dan Lang, who had criticized the RCMP for scaling back volunteers' roles. "I didn't understand from the get-go why the RCMP were doing what they were doing. Any costs are incurred by the provincial or territorial government, so the cost of the program to the RCMP was negligible," he says. Lang says auxiliaries provide important local knowledge, which is especially important to new members of the RCMP. CBC News (2016-12-23)

Officials under pressure to improve rural policing
The man who speaks for rural Saskatchewan has a target in his sights for 2017. Ray Orb, president of the Saskatchewan Association of Rural Municipalities (SARM), wants a way to gauge whether RCMP service improves in the next six to 12 months, and a plan for how to make sure it happens. "We have to have some kind of benchmark ... and see if what we're doing is actually working," Orb said in a recent interview. When it comes to policing the province's vast and sparsely populated expanses, Orb and a host of other public officials are under pressure. Rural residents say they feel increasingly vulnerable to the prying hands of thieves. What are normally widespread and very public complaints in recent months about slow RCMP response times and the Mounties' lack of visibility have added intensity and urgency to routine discussions on whether the RCMP is performing to expectations (…) Meanwhile, federal Public Safety Minister Ralph Goodale has also been drawn into the ongoing discussion, having met recently with the province's justice minister. Orb said he also hopes to bend Goodale's ear. However, Goodale isn't commenting to the press while an RCMP resourcing review launched in August continues its work. A final report is expected this winter. Underlying all this is a sense that something has to be done to quell the vigilante mood that's taking hold in rural Saskatchewan, evident with the launch of the Facebook page Farmers with Firearms. Postmedia (Leader-Post, A1; StarPhoenix) (2016-12-27)

Family of Mission woman left to die after RCMP mistake continues legal fight
The family of a woman who was murdered in Mission eight years ago has launched a fundraiser to support a legal fight they say is significant to all Canadians. “It’s a very important issue because it affects

every Canadian's rights to life," said Rosemarie Surakka, mother of Lisa Dudley. On the night of Sept. 18, 2008, Dudley and her partner, Guthrie McKay, were shot as they sat watching television in the living room of their home. The shooting was a drug-related hit targeting Dudley. A neighbour called police to report the gunshots, and an RCMP officer responded. He drove around without getting out of his car or speaking to the person who called 911. In 2011, the officer was reprimanded and docked one day of pay. A neighbour discovered the couple four days after the shootings. McKay was dead and Dudley was paralyzed. She died on the way to the hospital. A civil claim filed by Surakka against the Attorney General of Canada and the B.C. government alleges that Dudley was deprived of her right to life and security of person — which is guaranteed under Section 7 of the Canadian Charter of Rights and Freedoms — because the RCMP failed to properly respond to the 911 call the night Dudley and McKay were shot. Postmedia (Vancouver Sun, Vancouver Province) (2016-12-27)

Inside the RCMP's Underwater Recovery Team

They work in a murky world, where they are often sent out to search by touch alone. And a day's work can involve hunting for bodies - the victims of accidents or crimes - lost in lakes, rivers or the ocean. The members of the RCMP Underwater Recovery Team form a specialized unit that is on call across the Maritimes and beyond. Not for the faint of heart It's a small team with six members and more being trained, made up of regular officers who are called on whenever a search is needed in water. In the past year, that's involved about 20 call-outs. "Primarily we look for missing people or missing items underwater whether it's related to investigation [or] a piece of evidence," said RCMP Cpl. Mark Bishop. CBC News (2016-12-27)

Police not responsible for crash injuries

Sidney-North Saanich RCMP officers were not responsible for the injuries of a man involved in a fiery crash Friday, the province's police watchdog has found. Marten Youssef, spokesman for the Independent Investigations Office of B.C., said his office has given Sidney-North Saanich RCMP the go-ahead to continue investigating the case. Times Colonist, A4 (2016-12-27)

Crossfield to get full-time enhanced police officer

A full-time enhanced police officer will be heading to Crossfield in 2017. Within the 2017 operating and capital budget, Crossfield town council allocated funds for short-term enhanced policing and sent a request to Airdrie RCMP K-Division for a full-time position to open mid-year. The full-time officer would be a three-year commitment and Crossfield Chief Administrative Officer Ken Bosman said the town has been preparing financially for when it reaches a population of 5,000 and takes over its own policing. "It has always been part of our plan to gradually ramp up our enhanced policing budget," he said. "When we hit 5,000 people, it's not a big shock to the system (because) we're already there." The plan, Bosman said, was to have extended shifts that lined with the town's Peace Officer so there would be one or the other scheduled every day. Rocky View Weekly (2016-12-27)

Independent reviews sent to Crown

The Independent Investigations Office has sent two reports to the Crown for consideration of charges about separate and unrelated deaths involving RCMP officers. The office says one case involves the Jan. 29, 2015, shooting of Waylon Edey, 39, of Yahk. He died during a traffic stop in Castlegar. The other case involves Jacobus Jonker, 53, who died six days after an incident while he was in custody in Smithers on Feb. 15, 2015. He had been arrested at his home in Smithers a day earlier, but the IIO says he became unco-operative while in custody and lost consciousness during a struggle with officers. He died in a Victoria hospital on Feb. 21, 2015. Vancouver Sun, A7 (2016-12-26)

Indo-Canadian Mountie Cleared Of Misconduct Allegations

An Indo-Canadian RCMP officer facing allegations of misconduct has been cleared after being suspended with pay for more than three years. RCMP Const. Amit Goyal was serving in Osoyoos, B.C., when he was accused of five allegations under the RCMP Act, including making false or misleading statements to a member of a superior rank, reported Canadian Press. A statement from E Division Deputy Cmdr. Craig Callens says he withdrew the allegations after reviewing information from Goyal's lawyer that provided different theories that couldn't be disputed because of contradictory expert information. The Link (2016-12-24)

2016 a challenging year for the Fredericton Police Force
It was a year of challenges for the Fredericton Police Force. From firings to ongoing suspensions to rehirings, the city's 103-member department was seemingly pushed to its limit (…) Three RCMP officers were killed June 4, 2014, while responding to a report of a man with firearms in a residential neighbourhood in Moncton. Seventeen members of the Fredericton Police Force were deployed to the Codiac incident during an extensive search for the killer. Improved communications was one of the recommendations contained in the report on the murders prepared by retired RCMP assistant commissioner Alphonse MacNeil. "When you look at a province of 700,000-plus people and a lot of rural area and a lot of interagency co-operation that's required, that radio system is beautiful," Fitch said. "It's a huge, huge accomplishment." Daily Gleaner, A1 (2016-12-27)

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

The imitation game
A number of handguns sit on display at the Wascana Pistol Club. There are real firearms, as well as the air guns modelled after them. They include a Beretta 92 FS and a Colt Governmental 1911. Club president Kelly Moens and club member David Schmidt issue a challenge, asking which ones are the real deal. It's not so easy. (…) Air guns designed to look like real-life models of firearms are frequently brought up as a concern by police, but they are legal. (…) Det.-Cpl. Rich Fraser with the Regina Police Service estimates that 25 per cent to 30 per cent of the guns that get confiscated by police are air guns. Fraser is a member of the National Weapons Enforcement Support program (NWEST), which is a partnership between provincial and municipal police forces to combat gun crime in Canada. Fraser catalogues all firearms seized by Regina police. Despite the number of guns he sees, Fraser said air guns modelled after real firearms are "very convincing." Some air gun imitations of revolvers even include cartridges that store ammo, making it look like the gun is loaded with bullets. Police have also seen air guns made of clear plastic painted to look more real. Postmedia Network (Leader-Post, A1, Star Phoenix, Edmonton Sun, Calgary Sun)

Grip of drug addiction shapes new ideas to reduce risk of deadly fentanyl
Watching an addict fill a syringe with puddle water, former senior RCMP officer Raf Souccar imagined a radical shift in how Canada could deal with people in the grip of drug addition — by providing them with medical-grade heroin and giving them a chance to survive. "I've always thought of these people as victims," he said, recalling the scene in Vancouver's Downtown Eastside, where the man added heroin to the dirty water and injected the contents into his arm. "I've seen a guy injecting with a needle he was sharpening on the side of the curb," said Souccar, a former RCMP deputy commissioner who spent 35 years fighting the illicit drug trade and is now concerned about the death toll from the fentanyl overdose crisis, which has killed hundreds of people in Canada this year. The country's two supervised-injection sites, including Insite, are both in Vancouver. Addicts are provided with clean needles and a nurse who watches over them as they shoot up their own drugs. People who unwittingly overdose on fentanyl-laced substances are given another drug, naloxone, to reverse the effects and then sent to hospital. Souccar said addicts should be given medical-grade heroin along with housing and mental-health services to save overall health-care costs and money for policing, courts and incarceration. "I'm not advocating drug use. I'm saying in the situation of people who need help, we need to find a way to help them with quality-control products," Souccar said from Ottawa. Canadian Press (Edmonton Sun, A13, Calgary Sun, Chronicle Herald)

Vancouver boosts fines for pot shops but defiant retailers still selling
A steady surge in illegal pot shops has prompted many cities to turn to law enforcement to try and clamp down. In Toronto and Ottawa, police tried co-ordinated raids to crack down on illegal pot shops. In Montreal, police recently raided six marijuana storefronts - the day after they opened. But Vancouver's latest approach is different than many other cities, with local officials turning to zoning rules, licence fees and hefty fines to try and control the marijuana boom. Earlier this year, Vancouver became the first city in Canada to draft a set of bylaws that would regulate pot shops in the absence of federal laws, which are expected to be tabled next year. But the rules seeking to limit the city's growth of medical marijuana

businesses, brought in on June 24, have so far had limited success. (...)According to officials, the number of marijuana-related businesses grew by 100 per cent per year from mid-2013 to mid-2015. In the first six months of 2015 alone, the city said, the number of pot-related businesses increased from 60 to 100. CBC News

Quarter of adults would try pot if legal: poll
If marijuana is legalized in this province, nearly one-quarter of Manitoba adults say they're prepared to get some. Rich or poor, NDP or Progressive Conservative, man or woman, young or middle-aged - tens of thousands are likely to try some pot. The *Winnipeg Free Press*/Probe Research Inc. survey asked, "If marijuana becomes legal in Canada, how likely would you be to use it even just once?" Twenty-four per cent - nearly one-quarter of a million adult Manitobans - said they would be likely to use it. "That's a significant market," said Probe research associate Mary Agnes Welch. "It's a little more than I thought." Between one-quarter and one-fifth of respondents said they're open to using legalized marijuana. Those most likely to use it were renters (38 per cent), men between the ages of 18 and 34 (37 per cent) and those with some post-secondary education (32 per cent). More men (28 per cent) than women (20 per cent) and more Winnipeg residents (28 per cent) than rural Manitobans (19 per cent) would use it once, and more 18- to 34-year-olds (32 per cent) than 35- to 54-year-olds (26 per cent) would use it once. Those least likely - 15 per cent - were over the age of 55. Winnipeg Free Press

From dime bag to money bags, businesses look forward to recreational marijuana
It's Sunday afternoon and Toronto's Centre for Social Innovation is packed full of marijuana enthusiasts perusing tables of goods. Everything from marijuana-infused barbecue sauce to medicated body rubs is available at Green Market, where artisans peddle their various craft cannabis products. Such events, which sell to patients and casual users alike, operate within a foggy regulatory environment. Selling marijuana is illegal unless you are a large-scale producer licensed under Health Canada's medical marijuana regime. However, licensed producers are only permitted to sell dried cannabis flower and oils, in spite of a Supreme Court ruling last year that said Canadians have a right to access medical marijuana in all of its forms. "We only carry products that are inaccessible in the current legal medical program," says Lisa Campbell, Green Market co-founder and a marijuana consultant at Mobile Revolutions. "So for patients we are the only place they can find edibles - it's not available from any licensed producer." The year ahead is expected to be a pivotal one for Canada's burgeoning marijuana industry, as the federal government is planning to table legislation in the spring that will lay out the ground rules for a legal, recreational market. Canadian Press (Daily Gleaner, D4, Telegraph Journal)

Pot enforcement won't change until marijuana is legalized, says Regina police chief
Regina Police Chief Evan Bray says there are no plans to let up on policing marijuana while it's still illegal. Bray said there has been discussion about its impending legalization, one of the Liberal promises made in the 2015 federal election. But the law will continue to be enforced in Regina until it changes, according to the police chief. "Today, the law still says that [marijuana]'s illegal to possess," he said in a year-end interview with CBC News. Bray said police exercise discretion when it comes to the issue and will continue to do so. If someone was a danger to themselves or others, such as being behind the wheel of a vehicle while impaired by drugs, he said police would act on the matter. CBC News (2016-12-27)

Hazy Outlook - Work cut out for province on marijuana legalization
After two days of legal marijuana immersion therapy, Alberta's justice minister admits more questions than answers remain on how the province rolls out pot reforms. But a federal task force's recently unveiled recommendations - calling for cannabis sales outside liquor stores, mail order retail and a minimum age of 18 - have cleared some of the smoke. While an October trip to Denver - the epicentre of Colorado's cannabis legalization - was useful, what Alberta's post-prohibition landscape looks like remains dependent on Ottawa's still hazy blueprint, says Kathleen Ganley. What's clear, she says, is that the deepest anxieties centre around the welfare of the province's youngest citizens - and motorists - as the feds prepare to table legislation in the spring. "Our biggest concerns are to ensure the safety of our roads and children," said Ganley, calling Colorado's experience a mixed bag. "Things certainly didn't descend into disorder or solve all the world's problems." Because no cannabis equivalent exists to the roadside breathalyzer that measures alcohol impairment, it appears police will have to rely on their own

skills of observation in weeding out stoned drivers, she said. Postmedia Network (Edmonton Sun, A11; Calgary Herald) (2016-12-26)

Legal pot could spark Canada-U.S. conflicts - From border security issues to existing anti-drug treaties legalization will have fallout
Their position on marijuana is hardly the only difference between Canada's prime minister and the president-elect of the United States. But when Justin Trudeau's government introduces legislation to legalize cannabis this spring, it could spark problems between Canada and the U.S., particularly since Donald Trump has indicated he will keep pot illegal at the federal level. Here's a look at what could change in Canada-U.S. relations once Canadians start lighting up legally... Earlier this year, Public Safety Minister Ralph Goodale said Canadians banned from entering the U.S. because they've admitted to using pot was a "ludicrous situation" that needed to be addressed. Scott Bardsley, a spokesperson for the minister, said Goodale will continue to discuss with American officials the need for Canadians to be treated appropriately when they are entering the U.S. Canadian Press (Toronto Star, A33) (2016-12-26)

Lacing dog treats with cannabis is a growing business
Even for a puppy, Kat Donatello's black Labrador, Austin, was hyperactive. After experimenting with natural supplements on her older dog, Donatello slipped a special biscuit to Austin. "It just kind of took the edge off of him," she recalled. Hamilton Spectator (2016-12-26)

Legal pot will bring difficult challenges for police, says expert
The impending legalization of marijuana will be a "tough" cultural shift for police forces in 2017, according to a Fredericton crime expert. Michael Boudreau, a professor with the criminology and criminal justice department at St. Thomas University, said law enforcement will have to embrace a new culture when it comes to dealing with marijuana. Telegraph-Journal (Telegraph-Journal; Daily Gleaner; Times & Transcript) (2016-12-24)

Perth County OPP test new devices to help identify impaired drivers
Police are testing new devices to identify drug impaired drivers. Whether or not the impending legalization of recreational marijuana use will have an impact on drug-impaired driving remains to be seen. However, the timing of a pilot project to detect drug impairment could give police new resources as legislation legalizing recreational cannabis is introduced in Parliament this spring. The pilot project is being tested by OPP, including Perth County, Toronto, Vancouver, Gatineau, Halifax, and Yellowknife police forces as well as North Battleford RCMP. Police are testing two units that collect oral fluids. The Alere DDS2 website says the hand-held machine can detect up to six different drugs from one oral fluid sample. The Suretec DrugWipe claims reliability greater than 95% with test results in eight minutes or less. Stratford Beacon Herald (2016-12-23)

Don't legalize pot before figuring out how to deal with stoned drivers: poll
Over 80 per cent of Canadians think that it would be a mistake to legalize marijuana before we have a reliable system for testing stoned drivers, a poll shows. Driving while impaired by a drug is just as illegal as driving drunk, but testing drivers for cannabis is more challenging than testing them for alcohol. As well, there's no consensus about where a bloodstream limit for THC should be set for drivers. "Until Canadians are convinced that the legalization of marijuana isn't going to make our roads less safe, we should just put the brakes on legalizing marijuana until we've got this figured out," said Sean Simpson, vice-president of Ipsos Public Affairs, summarizing the poll's findings. Global News (2016-12-23)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Does the loss of 755 B.C. lives to drug overdoses justify a public inquiry?
An opinion piece states, "In the summer of 2010, *Maclean's* magazine published an astonishing story about the RCMP's approach to supervised-injection sites. It outlined how the previous autumn, the Mounties and the B.C. Centre for Excellence in HIV/AIDS were in discussions to hold a joint news conference. There, they would each "declare their agreement that research shows the 'benefits' and 'positive impacts' of supervised injection sites for intravenous drug users", according to journalist John

Geddes. (…)The senior Mountie in B.C. at the time—then deputy commissioner Gary Bass—reportedly told Dr. Julio Montaner that RCMP headquarters in Ottawa would not permit the news conference to go ahead. The B.C. Centre for Excellence in HIV/AIDS subsequently filed a complaint to the Commission for Public Complaints Against the RCMP. This concerned the Mounties' efforts to discredit the centre's research. (…)According to *Maclean's*, senior B.C. RCMP officers were prepared in 2009 to acknowledge peer-reviewed research about supervised-injection sites. This research says, among other things, that these facilities save lives. However, someone in Ottawa appears to have prevented this public statement from being made." The Georgia Straight (2016-12-27)

Ragoût de «pot» de cochon?
Un article d'opinion par Dr Sylvain Charlebois note « Le pot est à la mode ces jours-ci, surtout à Ottawa. Un groupe de travail a récemment présenté un cadre de législation possible pour un Canada qui permettrait la consommation de la marijuana pour l'ensemble de la population. Pratiquement, depuis le lendemain de la victoire des libéraux à l'automne 2015, l'ensemble du secteur agroalimentaire attentait avec impatience les recommandations de ce groupe et le rapport déposé au début décembre n'a certes pas déçu l'industrie. Ce que plusieurs ne réalisent pas encore, c'est que le cannabis représente une petite mine d'or pour les secteurs de la transformation et de la distribution alimentaire au pays. Selon une étude publiée par Deloitte en octobre, le marché de la marijuana, une fois légalisé, pourrait générer plus de 22 milliards de dollars au Canada. C'est plus que les ventes combinées de vin, de bière et de spiritueux sur l'ensemble du territoire. Les ventes de cannabis à l'état pur représenteraient environ 8 milliards de revenus supplémentaires d'ici quelques années. Mais selon la même étude, plus de 14 milliards de revenus supplémentaires émaneraient de produits dérivés du cannabis. C'est énorme. Il est fort possible que 5 à 7% des produits alimentaires vendus au Canada d'ici 10 ans puissent contenir du cannabis, incluant le prêt-à-manger. Qui sait, une autre façon de déguster le ragoût de pattes de cochon, le pâté chinois, la tourtière ou bien les pets de soeur! » Le Quotidien, 12 (Le Nouvelliste, Le Droit)

Inside fentanyl crisis
An opinion piece by Staff Sgt. Conor King from the Victoria Police Department states, "I spent Christmas 2015 sitting at my kitchen table, smartphone in hand, tracking overdose deaths across Greater Victoria. Eight people had died in seven days, three in the preceding 24 hours. Two of them died on the street, one in a parkade, the rest at home. This included Miranda, the 22-year-old daughter of one of my co-workers at the Victoria Police Department. She died in her bedroom a few hours after opening Christmas presents with her mom and stepdad. In the weeks before Christmas, I had watched the number of overdoses rise across the city. We call it a cluster. It wasn't the first one I'd seen. That happened in the spring of 2013. (…) I called my friends at the RCMP. They invited me to an urgent meeting at their headquarters. Fifty cops and crime analysts from across Western Canada crowded into a briefing room. The U.S. Drug Enforcement Administration sent a team of chemists from Washington, D.C. That's not normal. I braced for bad news. On an oversized smartboard, we examined maps dotted with overdose clusters. Communities across North America were seeing overdoses spike. The chemists explained it was illicit fentanyl, cheaper than heroin and lethal in minute quantities. One held up a 500-milligram Tylenol tablet and said: "If this was fentanyl, it could kill 250 people." (…)People take enormous risks smuggling heroin. That risk is a strong deterrent. But what I was hearing from the RCMP was this: Unlike heroin, fentanyl is produced with ease by unscrupulous chemical companies in China and other countries, advertised on the Internet and shipped by commercial mail." Times Colonist, A1

Let's unite on opioid war
An editorial states, "If Alberta had as many drunk driving deaths as it did from opioids - 338 for the first nine months of the year, half of those tied to fentanyl - there would be all-party support for an enhanced strategy to put a stop to the carnage. There is a growing chorus of voices, though. Liberal Leader Dr. David Swann, who headed the NDP's mental health review, has been steadfast in his view the province needs to declare a public health emergency to combat the crisis. And now one of Alberta's top cops is pushing for more action. In an interview with the Canadian Press, Calgary Police Chief Roger Chaffin said the province has to take more aggressive action dealing with the "demand side" for the drugs. "We need to get these people out of the lifestyle they're in and get them into more healthy lifestyles, improve their families, improve their wellness in this community," he said. To him, that means more treatment spaces." Edmonton Sun, A14 (Calgary Sun)

Press freedom in Canada eroded by post-9/11 obsession with security
An opinion piece states "Canada's news media are still living under the entrenched legacy of Stephen Harper - like everything and everyone else in this country. The previous prime minister ushered in what the Paris-based press freedom organization Reporters Without Borders (known by its French acronym, RSF) refers to as a 'Dark Age' of Canadian journalism. Even with a change at the executive level, old habits that characterize the legacy of such an age haven't left Canada's institutions... The scary contrast here is with the increasing threat to investigative reporting or meaningful journalism in general in a post-9/11 age of heavy-handed security laws. This kind of legislation has created much more legal space for law enforcement and intelligence agencies to operate, sometimes virtually with impunity, in ways that, according to organizations like the Canadian Civil Liberties Association, 'violate the Canadian Charter of Rights and Freedoms.' Such a climate calls for more scrutiny by the press when it comes to monitoring centres of power. Yet Canadians are witnessing the exact opposite trend." CBC News (2016-12-26)

Jessica's favourite things from 2016 - Canada shifts its stance on personal data security
An opinion piece states "This past November, it came to light that the Canadian Security Intelligence Service (CSIS) had been illegally collecting Canadian data for over a decade. The federal government chastised the agency for its actions, and handed down a ruling stating that the intelligence service had breached its duty to inform the court of its mechanisms. The information had been collected for reasons other than national security threats, and therefore, should not have been retained by CSIS in the first place. This report accompanied several others in 2016 detailing the relationship between federal regulators and Canadian data. News that a Quebec police station tracked the smartphones of six journalists made headlines around the world and attracted commentary from history's most famous whistleblower, Edward Snowden. The reaction to these stories by federal courts and regulators demonstrates a more modern perspective on data than we've seen from Canadian governments in the past. It's encouraging for many Canadians to see that the legacy left by Bill C-51 needn't be a permanent one..." Mobile Syrup (2016-12-26)

Quebec's indigenous inquiry isn't quite what was sought
An opinion piece states, "Often a public inquiry is what the opposition demands when it has no ideas of its own to propose. And often it's the response of a government to pressure to Do Something. There has been pressure on the Couillard government to hold a public inquiry into allegations of abuse of indigenous women by police in Val-d'Or since the Radio-Canada investigative program Enquête first reported them in October 2015. The pressure, led by Quebec indigenous leaders, became more intense in the past month... Finally, last week, the federal commission of inquiry into missing and murdered indigenous women and girls, created in September, said it could not conduct the investigation into the situation in Val-d'Or on which the Couillard government had been counting. The federal commission suggested that instead Quebec conduct its own "complementary" inquiry. At that point, the Couillard government gave in. When the government announced the terms of the inquiry this week, aboriginal leaders were pleased. They may, however, have got more than they bargained for - or less..." Montreal Gazette (2016-12-24)

Les méritas 2016
Un article d'opinion note « En cette fin d'année, je distribue généreusement les méritas aux gens de la scène politique qui se sont démarqués. Comme les enfants qui n'ont pas été sages sont susceptibles d'être déçus par le père Noël, les oubliés dans ma liste peuvent toujours rêver de faire mieux... l'an prochain... RALPH GOODALE. Méritas Gardien du fort. Les questions de sécurité ne semblent pas être la force du toujours positif Justin Trudeau. Face à la menace terroriste ou dans la sélection des réfugiés, le vieux routier Goodale apparaît comme une force rassurante. Je suis convaincu que sa sagesse se fait aussi entendre au Conseil des ministres.... » Agence QMI (Journal de Québec, 16; Journal de Montréal) (2016-12-24)

What should we expect from security intelligence services?
A blog post by Phil Gurski states "Earlier this morning the suspect in the Berlin Christmas market attack that killed 12 and wounded dozens more was shot to death by Italian police in Milan. An international manhunt ended successfully with the killing of Anis Amri, a Tunisian refugee who had spent time in Italy before moving on to Germany. He was known to Italian authorities for his violent behaviour while

imprisoned for vandalism. German authorities had sought to deport him to Tunisia but were hampered by questions over his nationality. He had also been on German intelligence radar for months. Islamic State has issued a video of Amri pledging allegiance to IS leader Abu Bakr al-Baghdadi. As is usual in the aftermath of terrorist attacks, questions are being asked about why the attack had not been foiled. German agencies in particular have been criticised and their capabilities are under scrutiny. The same happened in the wake of the Brussels attacks as well as here in Canada after the October 22, 2014 rush on Parliament Hill by Michael Zehaf-Bibeau. Inquiring minds want to know: just what the hell are our intelligence and law enforcement agencies doing with the billions we give them? I find all this hand wringing and armchair quarterbacking interesting – and hypocritical. Yes, I have a clear bias as someone who worked in security intelligence for three decades but if I try to see this as an interested outsider (which, truth be told, I am now that I have retired from CSIS), I still can't support the criticism levied on my former colleagues, both here and abroad." Borealis Threat and Risk (2016-12-23)

What legal weed needs: marijuana and the law
An opinion piece states "Against a background of considerable buzz, the Liberal government's task force on the future of marijuana in Canada has now released its much-anticipated report, A Framework for the Legalization and Regulation of Cannabis in Canada. The report provides helpful recommendations on how to responsibly legalize and regulate recreational marijuana use. The report is ambitious in scope, addressing everything from the packaging of edibles to the height of homegrown plants to environmental stewardship. It has been well-received, and for good reasons: While it may not be perfect, the report goes some way to redefining marijuana as matter of public health and not of criminal law. Now comes the hard part. The Trudeau government, along with the provinces, must now move from theory to practice and create a comprehensive legislative regime." iPolitics (2016-12-23)

OTHER / AUTRES

'It just shocks me'
Calgary's police chief says the Alberta government has to take more aggressive action on fentanyl if it wants to help addicts and families who are being destroyed. "It is a crisis," said Calgary Police Chief Roger Chaffin in an interview with The Canadian Press. "Look at the numbers of deaths. Numbers of homicides and traffic fatalities don't come anywhere near the deaths associated with these drugs." In the first 10 months of 2016, 338 Albertans died from opioid-related overdoses, with fentanyl linked to 193 of those deaths. "People are going to keep arguing about whether this is a crisis or not. It just shocks me," Chaffin said. "We're wasting all our energy arguing about whether this should be called a public health crisis or not. Spend your energy fixing the problem." Chaffin said there is a huge demand for highly addictive opiods such as fentanyl - a drug used as a painkiller for terminally ill cancer patients and 100 times more powerful than heroin - or its more powerful cousin carfentanyl. Reducing the supply increases the price and make its users more desperate, he said. Postmedia Network (The Guardian, A5, Whitehorse Daily Star, Red Deer Advocate, Leader-Post, Windsor Star, Montreal Gazette, National Post, Ottawa Sun, Vancouver Sun, Ottawa Citizen, Times Colonist, Waterloo Record, Edmonton Journal, Calgary Sun, Kingston Whig-Standard, Times & Transcript, Hamilton Spectator, Toronto Star, Globe and Mail); Postmedia Network (Calgary Herald, Calgary Sun)

'Perfect storm' testing police
A lagging economy and the presence of potent drugs and addictions in Calgary translated to a "perfect storm" in 2016 for the city and its police officers, according to Chief Roger Chaffin. The police chief cites drugs as the biggest issue the service faced during the past year - and one that has affected the very nature of policing. "You see highly motivated criminality around these drugs that's cause for many, many public safety concerns, and safety concerns for our officers," Chaffin said in an interview. Those concerns have put the local police service in situations it hasn't seen in its history, he added. The fact that officers fired their weapons in 10 separate incidents in 2016, including five fatal scenarios, is reflective of that different environment, according to the chief. Calgary Herald, A1

La SQ démantèle un premier laboratoire de fentanyl au Québec

La SQ a démantelé pour la première fois samedi dernier un laboratoire d'encapsulage de fentanyl. Les résultats d'analyse ont confirmé mardi qu'il s'agit bien de cette drogue " puissante et dangereuse ", a déclaré un porte-parole de la Sûreté du Québec (SQ). Un kilogramme de la substance a été saisi, deux cents grammes d'alprazolam, ainsi que deux presses à comprimés et une machine à encapsuler. Des saisies ont d'abord eu lieu à Longueuil, Boucherville et Saint-Roch-de-Richelieu, avant de mener les 35 policiers de cette escouade vers le laboratoire à Potton en Estrie. (…) Une recherche dirigée par Kate Smolina, de la Faculté de médecine de l'Université de la Colombie-Britannique, révèle que, de 2005 à 2012, la proportion de la population prenant des opioïdes pendant une période prolongée est passée de 2,0 à 2,4 %, ce qui représente une hausse relative de 19 %. " 2 %, ça peut paraître peu, mais c'est en fait considérable. En Colombie-Britannique, cela se traduit par environ 100 000 [personnes] ", explique Mme Smolina. Le Devoir, A3

Hausse des incendies criminels liés à la mafia

Les incendies criminels liés à la mafia montréalaise ont augmenté à Montréal en 2016, en particulier depuis le début de l'automne, laissant ainsi croire que le crime organisé italien connaît une autre période de recrudescence des luttes intestines qui la secouent depuis environ 10 ans. En cette année qui se termine, les enquêteurs de la section des incendies criminels de la police de Montréal ont par ailleurs été également très occupés avec plusieurs incendies qui ont éclaté dans des immeubles désaffectés, tellement qu'un nouveau bureau d'enquête vient d'être créé pour endiguer le phénomène. «Actuellement, selon notre analyse, je lis qu'il y a une lutte entre deux groupes de la mafia, dont le clan Rizzuto. C'est surtout lui qui est visé. On dirait que l'on veut tasser les Rizzuto, et ce sont des messages que l'on veut envoyer», a expliqué à La Presse le commandant de la section des crimes majeurs et économiques du SPVM, Juan Vargas. Voix de l'Est, 11

Chief looking out for patrol cops

As the year draws to a close, Brian Fitzpatrick sits down with new Regina Police Service Chief Evan Bray to find out how he's settling into his new role (…) But image aside, he must now oversee a staff of 586, getting them to buy into his plans from the bottom up. He said that making sure patrol units - what he calls the "core function" of the service - are adequately supported, and communicated with, will be one of his main 2017 goals (…) With surging methamphetamine use and the gun-based crime wave that has come with it, Bray said he wants to refocus on the travails of the men and women who "are being asked to make split-second decisions, and then ultimately are at risk every day and night that they come to work." These decisions are being made within a worsening environment. Yearly attempted murders have jumped from eight in December 2015 to 31 as of last month (…)From January to November there were 126 violent incidents involving a firearm, versus just 67 over the same months in 2015. On just one Tuesday in November, police responded to four gun-related incidents. Bray said patrol units often find their numbers dragged on by specialist units - plainclothes units, investigative units, etc. - meaning a force can easily lose sight of what its primary job is. For most RPS officers, it's not meeting the press in a fancy room. Postmedia (StarPhoenix, A1/FRONT; Leader-Post) (2016-12-27)

Police in Quebec City shoot, kill armed man

Quebec's police watchdog is investigating after a 39-year-old man died and a police officer was injured by a machete during a chase in Quebec City overnight Monday. According to the province's independent investigations bureau (BEI), around 2:30 a.m. police in Lévis initiated the chase and called Quebec City and Sûreté du Québec officers for assistance. Police laid down a spike strip but it didn't stop the car (…) The man proceeded to get out and struck an officer with a machete. Her injuries were minor. At least two police officers then opened fire on the man. He was pronounced dead in hospital. The BEI, which probes deaths or serious injuries involving police, has asked three members of the Montreal police force to assist with the investigation. CBC News; La Presse Canadienne (La Presse) (2016-12-27)

Une année marquée par des tragédies

L'année 2016 aura connu sa part d'événements tragiques et d'interventions policières, ce que les médias classent sous la rubrique des «faits divers»… Le mois d'octobre se termine, le 31, par un coup de tonnerre dans les médias: on apprend que le chroniqueur Patrick Lagacé, de La Presse et du 98,5 FM, a fait l'objet de 24 mandats de surveillance par lesquels le Service de police de la Ville de Montréal (SPVM) a eu accès aux métadonnées de son téléphone cellulaire et obtenu la possibilité de connaître sa position

par le biais du GPS. Les informations déboulent dans les jours suivants et on apprend finalement qu'une dizaine de journalistes ont fait l'objet de surveillance du SPVM ou de la Sûreté du Québec (SQ). L'affaire prend une telle ampleur que le gouvernement du Québec se voit obligé de décréter de nouvelles directives pour encadrer la délivrance de mandats et déclenche une commission d'enquête publique sur les pratiques policières, la délivrance de mandats et les interventions politiques auprès des corps policiers. Le Soleil, 22 (2016-12-26)

Guns, drugs, cash seized in 'significant' raid
London police say they're alarmed by the number of weapons seized in a jaw-dropping raid that netted three guns, hundreds of rounds of ammunition and more than $30,000 in illegal drugs Friday. Cops swooped down on Fleming Drive - site of a St. Patrick's Day riot in 2012 near Fanshawe College - and officers in the guns and drugs section raided a home. Sun Media Corporation (London Free Press) (2016-12-24)

Four Mississauga robberies solved with GTA-wide gang sweep: Police
Four retail robberies in Mississauga are among the 37 police say they have solved with a multi-jurisdictional investigation that saw 16 suspects arrested and warrants issued for another three. Mississauga.com (2016-12-23)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Ellis2, Andrew (PS/SP)

From: COMDO / COMDO (PS/SP)
Sent: Wednesday, October 19, 2016 7:27 AM
To: Bergeron, Marianne (PS/SP); Haddad, George (PS/SP)
Subject: RE: cyber??

Thanks. I will include in Cyber.

I think this one should go in NS Consultation (came out last night and we included in TN, but I think it is worth re-including in the this morning's DMS):

Snowden says Trudeau afraid to kill anti-terrorism bill
Whistleblower. Hero. Traitor. Patriot. These words and more have been used to describe former cybersecurity contractor Edward Snowden, who in 2013 copied and distributed thousand of documents to reporters and whose stories of Western intelligence agencies — including Canada's Communications Security Establishment (CSEC) — shook the world. This morning Snowden told the the annual SecTor cyber security conference in Toronto that Prime Minister Justin Trudeau want to amend the controversial Bill C-51 anti-terrorism law and not repeal it because he "is afraid of being attacked for being soft on terrorism." Speaking by video from Russia, where he fled to avoid prosecution by U.S. authorities, Snowden said the legislation, needs three fixes: First, a judicial body should have oversight over federal intelligence agencies that has the power to prosecute authorities that have broken the law. Second, because intelligence agencies are trading personal information of citizens "like baseball cards" citizens should be told if the data sharing hasn't led to an arrest for criminal activity. And finally, what Snowden called the criminalization of speech through vague definitions of terrorism should be taken out of C -51. A lot of what police call terrorism is the activity of what he called "common criminals" or those who are trying to make a political point but don't constitute a "super criminal threat." IT World Canada (2016-10-18)

From: Bergeron, Marianne (PS/SP)
Sent: Wednesday, October 19, 2016 7:20 AM
To: Haddad, George (PS/SP); COMDO / COMDO (PS/SP)
Subject: cyber??

http://ww2.infomedia.gc.ca/ps-sp/2016/10/19/203004775

Marianne Bergeron
Communications Advisor
Public Safety Canada / Government of Canada
Marianne.Bergeron@canada.ca / Tel: 613-949-9932

Conseillère en communications
Sécurité publique Canada / Gouvernement du Canada
Marianne.Bergeron@canada.ca / Tél : 613-949-9932

Ellis2, Andrew (PS/SP)

From: COMDO / COMDO (PS/SP)
Sent: Monday, July 27, 2015 7:50 AM
To: Lavoie, Ericka
Subject: RE: EM & Cyber

I highlighted the item in yellow as it may have been picked up in another section, perhaps LE?

From: Lavoie, Ericka
Sent: Monday, July 27, 2015 7:50 AM
To: COMDO / COMDO (PS/SP)
Subject: RE: EM & Cyber

Hello,

Just to check, is there a reason the article on silent scanners is highlighted in yello? Thanks

---

From: COMDO / COMDO (PS/SP)
Sent: Monday, July 27, 2015 7:47 AM
To: Lavoie, Ericka; Bue, Richard; Charbonneau, David
Subject: EM & Cyber

** Item highlighted in yellow may have been picked up in LE?

NATIONAL SECURITY

File breach at electronic spy agency prompts mandatory privacy training
Canada's electronic spy agency introduced mandatory privacy awareness training for all employees in March following an internal breach involving personal information. When Greta Bossenmaier became chief of the Communications Security Establishment in February, the ultra-secret eavesdropping outfit was under intense public scrutiny over alleged spying on citizens. But less than two months into the job, Bossenmaier was informing the spy agency's staff of a privacy violation inside its own walls. "I seriously regret that we are in this situation and never want it to be repeated," Bossenmaier told employees in a March 20 email. "As such, we must use it as a learning opportunity so that we can prevent any further incidents from occurring." Documents leaked in 2013 by former American spy contractor Edward Snowden revealed the U.S. National Security Agency — a close CSE ally — had quietly obtained access to a huge volume of emails, chat logs and other information from major Internet companies, as well as massive amounts of data about telephone calls. As a result, civil libertarians, privacy advocates and opposition politicians have demanded assurances the CSE is not using its extraordinary powers to snoop on Canadians. The agency insists it scrupulously follows the law in protecting Canadians' privacy. Canadian Press (City News)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

***Water shortage a wake-up call: Expert**
On a sunny afternoon in Stanley Park, cricket players run on parched yellow grass. A majestic fountain in the middle of Lost Lagoon sits dormant. A little girl approaches an inactive splash pad, squealing when its user-activated geysers suddenly gush water. Vancouver, often admired for its lush greenery and occasionally mocked for its torrential rain, has turned a dry, dusty brown as a savage drought sweeps Western Canada. And as residents adapt to the harshest water restrictions imposed in 12 years, experts and officials warn it's time to get used to turning off the taps. When asked how the province stacks up to other parts of the world in terms of water conservation, University of British Columbia watershed management profess or Hans Schreier doesn't mince words. "We're terrible," he says. "We're terrible, seriously. We are the second biggest water users. We have never worried about water. We have terrible regulations." "There are going to

be more floods and more drought," he warns. "We should start thinking about adapting to these conditions." Metro Vancouver chair Greg Moore says the region has been monitoring water for a century and this week marks only the second time it has had to impose Stage 3 restrictions. "We haven't seen this type of drought and consumption of water in our history," says Moore, who is also mayor of Port Coquitlam, a suburb east of Vancouver. Canadian Press (Kingston Whig-Standard, B1; Globe and Mail, Edmonton Journal, Leader-Post, Star Phoenix, Windsor Star, Edmonton Sun, London Free Press, Red Deer Advocate, Times and Transcript, Telegraph-Journal)

*** Wise to plan for drier West**

An editorial states "After a run of several wet years that saw several major flood emergencies, the spring and summer of 2015 have seen Saskatchewan literally dry up. The signs have been everywhere - evacuees fleeing huge wildfires in northern forests, parched and stunted crops in the grain belt, and brown, patchy lawns and "green spaces" in the cities. Reginans were asked to temporarily reduce their water use by 25 per cent a few weeks ago when the Buffalo Pound water treatment plant struggled with unusual algae blooms and water conditions on the lake that supplies this city and Moose Jaw with clean water. Saskatchewan isn't alone - drought conditions have also hit Alberta farmers and British Columbia is enduring recordbreaking heat and sparse rainfall that have resulted in more than 1,300 wildfires and led to significant water use restrictions in normally rainy Vancouver. "For sure, this is something we can expect to see with increasing regularity," Howard Wheater, director of the Global Institute for Water Security at the University of Saskatchewan recently warned." Star Phoenix, A6 (Leader-Post)

*** Silent Scanners**

Citizens who like listening in on police, fire department and ambulance calls are out of luck, now that most emergency services communications in Cape Breton are conducted on fully encrypted radios. The scanners have gone silent, for the most part, with the introduction of the second generation of Trunk Mobile Radio (TMR2) communications. Being unable to monitor police traffic can be dangerous for citizens, said one longtime listener who didn't want to be named. "You don't know what's going on in the city unless you have a scanner," said the citizen, who lives in Sydney's north end. "No offence to radios or newspaper, but you don't hear everything that goes on." Cape Breton Regional Police spokeswoman Desiree Vassallo said police haven't heard any complaints from citizens about the encryption system. She said police need secure communications, especially during sensitive operations when police don't want suspects or the public to know exactly where they are. Chronicle-Herald, A3

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

***Greece had secret plan for instant drachma switch**

A secret cell at the Greek finance ministry hacked into government computers and drew up elaborate plans for a system of parallel payments that could be switched from euros to the drachma at the "flick of a button." The disclosures caused a political storm in Greece and confirm just how close the country came to drastic measures before Prime Minister Alexis Tsipras gave in to demands from Europe's creditor powers, acknowledging that his own cabinet would not support such a dangerous confrontation. Yanis Varoufakis, the former finance minister, told investors that a five-man team worked for months on a contingency plan to create euro liquidity if the European Central Bank cut off emergency funding to Greece, as it in fact did after talks broke down and the ruling Syriza party called a referendum. London Daily Telegraph (Ottawa Citizen, C2; Edmonton Journal, Calgary Herald, Star Phoenix, Leader-Post, The Province, Windsor Star, Vancouver Sun)

*** Cracking down on hackers bad for innovation**

An opinion piece states "Every week seems to bring a new hacking story - the massive hacking attack on the U.S. government's databases and the attacks on the U.S. health-care system are just two of the bigger stories - so it's perhaps no surprise that the knee-jerk reaction is to take the fight directly to the hackers. By making the penalties tougher, by expanding the scope of federal anti-hacking statutes and making it easier to prosecute wrongdoers, it'll convince hackers that it's just not worth the risk, right? The problem is that simply toughening the laws on hackers by extending their scope and reach or extending the prison sentences of hackers is not going to help catch the real hackers - the criminalized, anonymous hackers who operate in places such as China. Instead, they're more likely to ensnare the likes of hacktivist heroes such as Aaron Swartz. Getting tough on hackers by extending the definition of what a hacker is would theoretically mean that people who even so much as retweet or click on a link with unauthorized information could be committing a felony. Moreover, the white hat hackers (the "good guys") could be ensnared as well, since their work, at its core, is indistinguishable from that of the black hat hackers (the "bad guys"). And that could have a chilling effect on innovation." Hamilton Spectator, A15

***Your car could be hacked, and that's no prank**

An editorial states " It's a scenario out of a Stephen King novel: A driver cruising along a busy highway suddenly finds his car taken over by an outside force. First it's just the radio, the wipers and the air conditioning behaving chaotically. Then - as an 18-wheeler bears down at high speed - the transmission shuts down. As you've no doubt noticed, more and more

everyday objects are being rigged with sensors and connected to the Internet. By 2020, 50 billion such devices may be online. This phenomenon, known as the Internet of Things, promises all sorts of benefits to companies and consumers alike. But many of the manufacturers involved have little experience with digital security, and few customers know how to properly protect their cars (or toothbrushes) from malicious hacking. As a result, commonplace items such as baby monitors, room locks and medical devices have already been hacked. Manufacturers should expect this to continue, and prepare for it to get worse before it gets better. That means making cybersecurity something more than an afterthought when designing new products. It also means being upfront with consumers about exactly what those products are doing and sharing online. Bloomberg (Hamilton Spectator, A14)

***Security is a private matter**

The Ashley Madison hack is the latest in a series of high profile data breaches that have plagued businesses and consumers. Other targets include Target, Home Depot, Sony, and JP Morgan Chase, to name but a few. Ashley Madison's customers are targets of cyber extortion. Hacker group The Impact Team claims to have breached the website's computer systems, gaining access to troves of sensitive personal information about its users. The Toronto-based service gained notoriety as a website that facilitates "discreet encounters between married individuals," boasting close to 38 million members. It has been threatened with the public disclosure of information on its users unless it shuts down. Reports have claimed the hackers are former employees of Ashley Madison, who used their insider knowledge to gain access to the personal data. But the hack could have been accomplished just as easily by utilizing a "zero day" attack, or simply because of lax security (as is often the case in data breaches). Companies, not their users, are ultimately responsible for the security of their websites. But there are several measures users of Ashley Madison could have taken to protect themselves. Winnipeg Sun, 14

Ellis2, Andrew (PS/SP)

From: COMDO / COMDO (PS/SP)
Sent: Wednesday, October 19, 2016 7:33 AM
To: Despard, Sean (PS/SP)
Subject: RE: One-off and/or include in this morning's product

Perfect. Agreed.

Thanks!

From: Despard, Sean (PS/SP)
Sent: Wednesday, October 19, 2016 7:33 AM
To: COMDO / COMDO (PS/SP)
Subject: RE: One-off and/or include in this morning's product

Since the article was in yesterday's 2pm, I feel like sending out a one-off now would be of little benefit. My thoughts on one-offs is that it should be for breaking or relatively recent news items. So, it would have made sense to have sent it out yesterday.

That said, we're going to top story the National Post piece this morning (same one that was in yesterday's 8pm product).

- Sean

From: COMDO / COMDO (PS/SP)
Sent: Wednesday, October 19, 2016 7:17 AM
To: Despard, Sean (PS/SP)
Subject: RE: One-off and/or include in this morning's product

Snowden says Trudeau afraid to kill anti-terrorism bill
Whistleblower. Hero. Traitor. Patriot. These words and more have been used to describe former cybersecurity contractor Edward Snowden, who in 2013 copied and distributed thousand of documents to reporters and whose stories of Western intelligence agencies — including Canada's Communications Security Establishment (CSEC) — shook the world. This morning Snowden told the the annual SecTor cyber security conference in Toronto that Prime Minister Justin Trudeau want to amend the controversial Bill C-51 anti-terrorism law and not repeal it because he "is afraid of being attacked for being soft on terrorism." Speaking by video from Russia, where he fled to avoid prosecution by U.S. authorities, Snowden said the legislation, needs three fixes: First, a judicial body should have oversight over federal intelligence agencies that has the power to prosecute authorities that have broken the law. Second, because intelligence agencies are trading personal information of citizens "like baseball cards" citizens should be told if the data sharing hasn't led to an arrest for criminal activity. And finally, what Snowden called the criminalization of speech through vague definitions of terrorism should be taken out of C -51. A lot of what police call terrorism is the activity of what he called "common criminals" or those who are trying to make a political point but don't constitute a "super criminal threat." IT World Canada (2016-10-18)

From: Despard, Sean (PS/SP)
Sent: Wednesday, October 19, 2016 7:17 AM
To: COMDO / COMDO (PS/SP)
Subject: RE: One-off and/or include in this morning's product

What's the article?

From: COMDO / COMDO (PS/SP)
Sent: Wednesday, October 19, 2016 7:16 AM

To: Despard, Sean (PS/SP)
Subject: One-off and/or include in this morning's product

This came out last night and was included in TN… That said, I'm thinking it is worth reincluding in this morning's product. Could also one-off?

Just wanted to bounce this off someone.

Let me know your thoughts.

Toni

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre/CentredesmediasPSP (PS/SP)
Sent: Friday, January 16, 2015 7:37 PM
To: Today's News / Actualités (PS/SP)
Subject: RT - CBC News - Power and Politics: Debate between national security experts Ray Boisvert and Errol Mendes on measures to track terror threats - 2015-01-16 - 18h25 ET

Rough Transcript

Station: CBC News – Power and Politics
Time/Heure: 18h25 EST
Date: 2015-01-16

Summary: *CBC News' Power and Politics featured a debate between national security experts Ray Boisvert and Errol Mendes on measures to track terror threats.*

>>> Hannah: Police say peace bonds are useful tool to help track terror suspects but they also say the legal requirements for obtaining them are so high that they are rarely granted. In fact, peace bonds have been ordered only eight time against terror suspects since 2001. And CBC news has learned that police tried but failed to get one for martin Couture-Rouleau weeks before he used his car to run down two soldiers in Quebec. Royal officer was killed in that attack. Comes with conditions, not owning weapons or restricting travel or associating with certain individuals. As the federal government prepares to table new anti-terror laws should it lower the bar for peace bonds to give police new powers or is it prudent to restrict their use to protect civil liberties? Joining me now to debate that, (Errol Mendes) Professor of International and Constitutional Law at the University of Ottawa. And by Skype from Toronto, Ray (Boisvert) is the former assistant director of intelligence at CSIS. He is now CE of ISAC integrated strategies. I want to start with you. What was your reaction to our story by our colleague Chris Hall that a prosecutor felt there wasn't enough evidence for a peace bond for martin Couture-Rouleau.

>> Interview: I wasn't shocked or surprised. Part of the issue, that's been a relatively long standing piece of criminal code of Canada related tool set. It has been very rarely used in the context of national security and in fact that part of the problem. I think there is probably lack of understanding, a lack of knowledge around national security issues amongst prosecutors because many crown councils deal with average day, every day things from high end to low end, from homicide to common assaults. Not that often are they sieged with this kind of complexity of an issue. So I think the threshold was probably difficult to achieve just naturally because you are dealing with whole bunch of new substance matter for the officers involved to convince the crown let alone convince judge subsequently p. I think that's part of the problem. But ultimately I think there is some potential to add this and to use it more frequently in that tool set. Aiming to sort of reduce the risks around terrorism.

>> Hannah: You want today jump in there.

>> Interview: Oh, absolutely. I'm confused as to why the prosecutor refused because you know, as you said, they have been eight bail bonds which were issued, six to the 18 terrorists in Toronto. And two which eventually were charged with major criminal offense. And when you look at the six that were given to the 18, they were fairly easily obtained, and brain Saunders who is the director of public prosecutions when he appeared before the senate security committee basically actually said that as far as he is concerned, the threshold that's in the law actually is lowered as far as he is he concerned. He actually said that as far as he is concerned, if he is convinced the judge can give it, he will give it. He will give his opinion. So I'm confused as to whether or not it's not a question of the law being changed, it's a question of whether the prosecutors did their job properly and whether the police presented the evidence properly.

>> Hannah: Now, Ray I see you nodding your head there.

>> Interview: I think it's a very fair comment. Both ends. A try apartheid system. Law enforcement officers bring forward information or charges against individuals. Prosecutors have to be satisfy adrenal chance of success and there is due process. Number of thing. There is a bit of check and balance, naturally in the system. And then thirdly convince judge that the evidence is compelling beyond a reasonable doubt and so on. I'm not a lawyer but ultimately I think in the first part

when the police are faced by the prosecution there is a gap. I think knowledge gap. May be simply a complex and I had velocity. I worked with criminal prosecutors in a previous life. I spoke to a number of them, not that long ago at western university at a seminar because they had a group in Ontario had no exposure to national security cases from espionage to terrorism. And I think they were probably pretty representative of the whole.

>> Hannah: So seems like it's a knowledge gap. So how do you fix the knowledge gap. Is it nor training?

>> Interview: Knowledge on the part of perhaps even parliament because when kneejerk reaction to say we need harsher laws. Where is the evidence? Amazing that the CBC had to produce this knowledge before we knew about it. That tells us that we are not being told the full story about what actually happening out there. And if, for example, the gaps where there is a gap of knowledge between the prosecutors and the police, let's fix it. To have a kneejerk reaction, harsh draconian laws, that could be done as a political ploy, to say we are strong on terrorism and the opposition may be weak on terrorism which I hope is not the case that's making political something which should not be made political. The safety of all Canadians at stake. Should find out based on the evidence what's needed and if the evidence produces that there is a need for changing of law so be it.

>> Hannah: Ray, you were talking about a knowledge gap there. Do you think you new legislation is needed? You I'm taking from what you are saying no?

>> Interview: I'm taking that we need to know the facts and need to know what the evidence is be we have this kneejerk reaction whenever there is a major incident we are going to toughen our laws.

>> Hannah: Sorry about that, Ray.

>> Interview: Fair enough. At the end of the day though you can't quite often prove a negative. A number of very effective national security cases that brought to bear and reduce some of those impacts. In other cases been tragic consequences such as we saw in Ottawa in October. Ultimately though as a practitioner, and I guess more narrowly from my perspective when I worked in that area i need as many flex and I believe diverse tools that I can get my hands on. As far down as perhaps some peace bond or control mechanism, something akin to if that Canadian travels overseas and we have reason to suspect that they are going to engage in violent activity, in other words commit murder in a horrible end need to be able to track them. I would call that draconian law. I think reflection of 21st century I think what we are facing right now. Take parts out, which part of the laws are we talking about and what kind of requirements are out there in terms of the intelligence organizations, what kind of laws and how do you apply those laws? The previous segment made that point very well. How do the judges fly that law properly?

>> Hannah: We were talking about the case in France, there was a kid who was drinking, said things, you know, I hope the same thing happens to you and got four years in prison. I don't think anybody would sit here and go that's probably something
--

>> Interview: Absolutely. And yes we face a big problem in terms of the foreign fighters, and we have to figure out how do we have kind of exit controls to make sure that we are not getting more and more of these people who go and come back. We need the evidence. And we don't need to just have kneejerk reactions wherever time there is an incident, we say let's have harsher laws.

>> Hannah: The problem with evidence, ray, and you might be able to come in on this too, problem with evidence, a lot of that evidence they are not giving.

>> Interview: This is part of the problem. We saw that through the security certificate process. We have seen in other trial. I know when I was involved in counter terrorism program trying to move intelligence into useable evidence is a big challenge. We came up with a whole bunch of ad hoc ways. One of the laws being proposed is help address that. I can't see any harm in that. Bring things out in the light of day and into the courts of law.

>> Hannah: Absolutely and if evidence is needed and you need more tools to get your evidence, no one disagrees with that. Because we don't want twelve journalists killed in our country just because they have had a cartoon printed. That being said, however, we absolutely need to figure out what is needed before we come to jump to conclusions and the last thing I would say is that i really hope that this is not being made into a political tool just to say we are tougher than the other parties. If that's the case, then we have to be careful as to what actually is being proposed.

>> Interview: And I think that's what the opposition clearly saying as well. Ray, just quickly, France is bringing in new anti-terror legislation. British Prime Minister David Cameron says intelligence agencies should have the power. So what do you respond to that?

>> Hannah: Well, you I'm hoping it's a question of as said about closing gaps. Some real conscious, concrete gaps that will affect security outcomes.

>> Interview: This is for encrypted internet communications.

>> Interview: Yeah, and I think ultimately that gets right down into the nugget of one of the most contentious issues, especially in the age of post Snowden revelations. So I'm of the view the end of the day security overseas will have to get at certain types of information, irrespective of what cloud it is sitting on irrespective of jurisdiction so they can connect dots hopefully prevent something from happening. This idea been perverted. A lot of scaremongering about the state listen to every conversation, every e-mail. It's poppycock. It is what it is. Going to be a difficult debate to have. I think that's what the French are talking about as much as anything.

>> Hannah: Thank you for having this debate on "Power & Politics" today. Appreciate your time.

>> Interview: You are very welcome.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at PSMediaCentre/CentredesmediasdeSP@ps-sp.gc.ca.
Questions? Veuillez communiquer avec nous au PSMediaCentre/CentredesmediasdeSP@ps-sp.gc.ca.

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre/CentredesmediasPSP (PS/SP)
Sent: Wednesday, February 25, 2015 4:35 PM
To: Today's News / Actualités (PS/SP)
Subject: RT: CBC News - CSE monitoring e-mails - B.C. Civil Liberties Association - 2015-02-25 - 16h17 ET

Rough transcript

Station: CBC News
Time/heure: 16h17 ET
Date: 2015-02-25

Summary: *CBC News reports documents that have just emerged from U.S. whistleblower Edward Snowden reveal the agency has monitored millions of e-mails Canadians send to Ottawa. The B.C. Civil Liberties Association, says these new documents reveal the agency stores Canadian e-mails for days, months, some cases years. The Communications Security Establishment says it respects Canadian's privacy and insists anything it looks at and stores is used in its mission to protect government networks.*

A CBC news exclusive is raising questions today over how your e-mail correspondence with the federal government is monitored. New details are emerging about the activities of canada's electronic spy agency. Documents that have just emerged from u.S. Whistleblower edward snowden reveal the agency has monitored millions of e-mails canadians send to ottawa. With more on what's behind this, here's david seglins.

>> You'll need to register online.

>> Reporter: Pass ports, taxes, writing your m.P. So much of canadian's communication with government these days done online. All that traffic means that, for canada's electronic spy agency, it is a huge job defending ottawa against cyber attacks.

>> To complete your report online, simply log on

>> Reporter: Cbc news for the first time has seen top-secret documents obtained by the u.S. News site the intercept and show how widespread the monitoring is. In 12010, for example, they scanned each and every document to and from government. They screened the attachment looking for bugs, malware and hackers trying to break in. 400,000 e-mails screened every day. About 400 would trigger automated alerts. And analysts take a closer look. Of those, an average fourz each day prompt a warning to a government department or canada's allies.

>> There's much more that the canadian public should be told upfront.

>> Reporter: Michael vaughan, a lawyer with the b.C. Civil liberties association, says these new documents reveal the spy agency stores canadian e-mails for days, months, some cases years.

>> How long is this data being cam chured? Who actually has access it to while it's holding.

>> It's relevant to canadians.

>> Reporter: But this professor of computing says holding on to day that for the day that you discover you've been hacked.

>> You really want to go back and see how big a problem did this cause? How much did we lose because of this attack that we only just noticed?

>> Reporter: C.S.E. Says government systems are constantly threatened by malware, hackers and enemy nations. The agency says it respects canadian's privacy and insists anything it looks at and stores is used in its mission to protect government networks. Dave seglins, cbc news, toronto.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at psmediacentre/centredesmediasdesp@ps-sp.gc.ca.
Questions? Veuillez communiquer avec nous au psmediacentre/centredesmediasdesp@ps-sp.gc.ca.

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre/CentredesmediasPSP (PS/SP)
Sent: Wednesday, February 25, 2015 4:35 PM
To: Today's News / Actualités (PS/SP)
Subject: RT: CBC News - CSE monitoring e-mails - B.C. Civil Liberties Association - 2015-02-25 - 16h17 ET

Rough transcript

Station: CBC News
Time/heure: 16h17 ET
Date: 2015-02-25

Summary: *CBC News reports documents that have just emerged from U.S. whistleblower Edward Snowden reveal the agency has monitored millions of e-mails Canadians send to Ottawa. The B.C. Civil Liberties Association, says these new documents reveal the agency stores Canadian e-mails for days, months, some cases years. The Communications Security Establishment says it respects Canadian's privacy and insists anything it looks at and stores is used in its mission to protect government networks.*

A CBC news exclusive is raising questions today over how your e-mail correspondence with the federal government is monitored. New details are emerging about the activities of canada's electronic spy agency. Documents that have just emerged from u.S. Whistleblower edward snowden reveal the agency has monitored millions of e-mails canadians send to ottawa. With more on what's behind this, here's david seglins.

>> You'll need to register online.

>> Reporter: Pass ports, taxes, writing your m.P. So much of canadian's communication with government these days done online. All that traffic means that, for canada's electronic spy agency, it is a huge job defending ottawa against cyber attacks.

>> To complete your report online, simply log on

>> Reporter: Cbc news for the first time has seen top-secret documents obtained by the u.S. News site the intercept and show how widespread the monitoring is. In 12010, for example, they scanned each and every document to and from government. They screened the attachment looking for bugs, malware and hackers trying to break in. 400,000 e-mails screened every day. About 400 would trigger automated alerts. And analysts take a closer look. Of those, an average fourz each day prompt a warning to a government department or canada's allies.

>> There's much more that the canadian public should be told upfront.

>> Reporter: Michael vaughan, a lawyer with the b.C. Civil liberties association, says these new documents reveal the spy agency stores canadian e-mails for days, months, some cases years.

>> How long is this data being cam chured? Who actually has access it to while it's holding.

>> It's relevant to canadians.

>> Reporter: But this professor of computing says holding on to day that for the day that you discover you've been hacked.

>> You really want to go back and see how big a problem did this cause? How much did we lose because of this attack that we only just noticed?

>> Reporter: C.S.E. Says government systems are constantly threatened by malware, hackers and enemy nations. The agency says it respects canadian's privacy and insists anything it looks at and stores is used in its mission to protect government networks. Dave seglins, cbc news, toronto.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at psmediacentre/centredesmediasdesp@ps-sp.gc.ca.
Questions? Veuillez communiquer avec nous au psmediacentre/centredesmediasdesp@ps-sp.gc.ca.

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre/CentredesmediasPSP (PS/SP)
Sent: Wednesday, January 28, 2015 9:45 AM
To: Today's News / Actualités (PS/SP)
Subject: RT: CBC News - Exclusive look into Communications Security Establishment Canada's alleged monitoring of global file-sharing - 2015-01-28 - 09h12 EST

Rough Transcript

Station: CBC News
Time/Heure: 09h12 EST
Date: 2015-01-28

Summary: *CBC News provided an exclusive look into the Communications Security Establishment Canada's alleged monitoring of global file-sharing.*

>> CBC news has learned that Canada's little-known electronic spy agency is conducting mass surveillance on the world's internet file-sharing sites in its search for terrorists. Top-secret documents obtained by US whistleblower Edward Snowden reveal that Canada's communications security establishment, known as CSEC, is in fact watching millions of uploads and downloads of movies, photos, and music every day. While the agency insists it is not directly targeting Canadians, Dave Seglins tells us the program is raising questions about just how far Canada and its allies go in monitoring the net.

>> It's called project Levitation and according to these new documents, Canada is watching 102 of the world's internet file sharing sites, the kind used to share things like music, movies, and photos. Canada's sifting through ten to 15 million uploads and downloads every day, looking for extremists accessing propaganda videos, instructions on how to build a bomb. This surveillance expert reviewed the documents for CBC.

>> Canadians need to understand and have a debate about the extent which it's okay for their government to be watching everything they do. Is it okay in the pursuit of radical extremists and defending Canadians from possible harm that the government sets up a giant digital x-ray machine over everything that we do? Because that's effectively where we're headed right now.

>> Reporter: CBC got these documents from journalist Glenn Greenwald who first broke the Edward Snowden stories. He says this is an example of Canada taking the lead among its allies in conducting mass surveillance.

>> You could be finding a terrorist, although probably much more likely, you're finding a scientist or a journalist or a lawyer working on a case relating to some of those issues or a student who's interested in those issues or a citizen who's reading about them, so you subject huge numbers of people to all kinds of very invasive surveillance based upon suspicion that is completely unfounded.

>> Reporter: CSEC says it's within their legal mandate to find foreign terrorists. The agency says it's not targeting Canadians and if a Canadian citizen is incidentally caught up in the surveillance, they have measures in place to protect their privacy.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre/CentredesmediasPSP (PS/SP)
Sent: Wednesday, January 28, 2015 9:45 AM
To: Today's News / Actualités (PS/SP)
Subject: RT: CBC News - Exclusive look into Communications Security Establishment Canada's alleged monitoring of global file-sharing - 2015-01-28 - 09h12 EST

Rough Transcript

Station: CBC News
Time/Heure: 09h12 EST
Date: 2015-01-28

Summary: *CBC News provided an exclusive look into the Communications Security Establishment Canada's alleged monitoring of global file-sharing.*

>> CBC news has learned that Canada's little-known electronic spy agency is conducting mass surveillance on the world's internet file-sharing sites in its search for terrorists. Top-secret documents obtained by US whistleblower Edward Snowden reveal that Canada's communications security establishment, known as CSEC, is in fact watching millions of uploads and downloads of movies, photos, and music every day. While the agency insists it is not directly targeting Canadians, Dave Seglins tells us the program is raising questions about just how far Canada and its allies go in monitoring the net.

>> It's called project Levitation and according to these new documents, Canada is watching 102 of the world's internet file sharing sites, the kind used to share things like music, movies, and photos. Canada's sifting through ten to 15 million uploads and downloads every day, looking for extremists accessing propaganda videos, instructions on how to build a bomb. This surveillance expert reviewed the documents for CBC.

>> Canadians need to understand and have a debate about the extent which it's okay for their government to be watching everything they do. Is it okay in the pursuit of radical extremists and defending Canadians from possible harm that the government sets up a giant digital x-ray machine over everything that we do? Because that's effectively where we're headed right now.

>> Reporter: CBC got these documents from journalist Glenn Greenwald who first broke the Edward Snowden stories. He says this is an example of Canada taking the lead among its allies in conducting mass surveillance.

>> You could be finding a terrorist, although probably much more likely, you're finding a scientist or a journalist or a lawyer working on a case relating to some of those issues or a student who's interested in those issues or a citizen who's reading about them, so you subject huge numbers of people to all kinds of very invasive surveillance based upon suspicion that is completely unfounded.

>> Reporter: CSEC says it's within their legal mandate to find foreign terrorists. The agency says it's not targeting Canadians and if a Canadian citizen is incidentally caught up in the surveillance, they have measures in place to protect their privacy.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre/CentredesmediasPSP (PS/SP)
Sent: Wednesday, January 28, 2015 9:45 AM
To: Today's News / Actualités (PS/SP)
Subject: RT: CBC News - Exclusive look into Communications Security Establishment Canada's alleged monitoring of global file-sharing - 2015-01-28 - 09h12 EST

Rough Transcript

Station: CBC News
Time/Heure: 09h12 EST
Date: 2015-01-28

Summary: *CBC News provided an exclusive look into the Communications Security Establishment Canada's alleged monitoring of global file-sharing.*

>> CBC news has learned that Canada's little-known electronic spy agency is conducting mass surveillance on the world's internet file-sharing sites in its search for terrorists. Top-secret documents obtained by US whistleblower Edward Snowden reveal that Canada's communications security establishment, known as CSEC, is in fact watching millions of uploads and downloads of movies, photos, and music every day. While the agency insists it is not directly targeting Canadians, Dave Seglins tells us the program is raising questions about just how far Canada and its allies go in monitoring the net.

>> It's called project Levitation and according to these new documents, Canada is watching 102 of the world's internet file sharing sites, the kind used to share things like music, movies, and photos. Canada's sifting through ten to 15 million uploads and downloads every day, looking for extremists accessing propaganda videos, instructions on how to build a bomb. This surveillance expert reviewed the documents for CBC.

>> Canadians need to understand and have a debate about the extent which it's okay for their government to be watching everything they do. Is it okay in the pursuit of radical extremists and defending Canadians from possible harm that the government sets up a giant digital x-ray machine over everything that we do? Because that's effectively where we're headed right now.

>> Reporter: CBC got these documents from journalist Glenn Greenwald who first broke the Edward Snowden stories. He says this is an example of Canada taking the lead among its allies in conducting mass surveillance.

>> You could be finding a terrorist, although probably much more likely, you're finding a scientist or a journalist or a lawyer working on a case relating to some of those issues or a student who's interested in those issues or a citizen who's reading about them, so you subject huge numbers of people to all kinds of very invasive surveillance based upon suspicion that is completely unfounded.

>> Reporter: CSEC says it's within their legal mandate to find foreign terrorists. The agency says it's not targeting Canadians and if a Canadian citizen is incidentally caught up in the surveillance, they have measures in place to protect their privacy.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Monday, March 23, 2015 8:43 AM
To: Today's News / Actualités (PS/SP)
Subject: RT: CBC News - Exclusive re. Canada's electronic spy agency & cyber warfare capabilities & its expanding powers w/ Bill C-51 - 2015-03-23 - 08h00 EDT

Follow Up Flag: Follow up
Flag Status: Completed

Rough transcript

Station: CBC News
Time/heure: 08h00 EDT
Date: 2015-03-23

Summary: *CBC News reported on Canada's electronic spy agency and its cyber warfare capabilities and how those powers may expand if Bill C-51 is passed.*

>> Heather: Good morning. I am Heather Hiscox. We begin this hour with new revelations about Canada's electronic spy agency.

>> Canadians may be surprised to learn about the capability Canada has.

>> Heather: Documents obtained by CBC News shows the depth of Canada's cyber tool box and its use around the world. The plan to expand Canada's ISIS mission. We look ahead as hearings resume on Parliament Hill on hand cuff laws... It is whether you like it or not. It is virtual battlefield where bill C-51 would allow the disruption of terror activities at home. CBC News has documents that reveal Canada has a powerful arsenal for cyber warfare. And the documents also show it is being used to spy on computer networks around the world.

>> The US, Britain. Now proof that Canada's security establishment is also in on international hanging and cyber warfare. These top secret documents obtained by Edward Snowden and analyzed by CBC and the US news site intercept shows that Canada has been hacking into networks in the Middle East and Mexico and other areas. But doing much more, from implanting bugs in computers to disrupting entire networks, cell phones, even attacking a country's infrastructure.

>> Canada may be surprised to learn about the cape believes Canada has. But ultimately it should come as no surprise that Canada would have these capabilities as a highly developed country that's at the apex of the national security pyramid.

>> The documents say Canada has yet to use some of the most destructive weapons, like those used in other areas but there are others that could be used, especially if bill c-51 passes, tools to disrupt communications, divert money transfers, all in a bid to disrupt terrorists or a threat to national security. Dave Seglins, CBC News, Toronto.

>> Heather: As Dave mentions, Bill C-51 would give more powers to Canada's spy agencies. Canada's lawyers are the latest to speak out against the legislation.

>> We will ask judges, the guardians of the constitution and the charter to authorize violations of charter in their absence and it is quite shocking.

>> Heather: Representatives of the Canadian bar are expected to appear before the Bill c-51 hearing this week.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at psmediacentre/centredesmediasdesp@ps-sp.gc.ca.
Questions? Veuillez communiquer avec nous au psmediacentre/centredesmediasdesp@ps-sp.gc.ca.

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Thursday, January 28, 2016 12:59 PM
To: Today's News / Actualités (PS/SP)
Subject: RT: CBC News - press conference by Minister of Public Safety Ralph Goodale and Minister of National Defence Harjit Sajjan - 2016-1-28, 12h30 ET

Follow Up Flag: Follow up
Flag Status: Completed

Rough Transcript

Station: CBC News
Time/Heure: 12h30 ET
Date: 2016-1-28

Summary: *CBC News provides live coverage of a press conference by Minister of Public Safety Ralph Goodale and Minister of National Defence Harjit Sajjan.*

Taking you live unfolding in Ottawa. **Minister of Public Safety Ralph Goodale** on the screen and also Minister of National Defence Harjit Sajjan talking about sharing information with Canada's security allies. We will listen in live.

>> -- We are following the existing procedures in terms of review and disclosure. Today sirq released the annual report with respect to cis. And the commissioner released the report with respect to the security establishment and the communication security establishment within dnd. These are two annual reports that relate to events of more tharn a year ago. And they should have been filed last year, but that process was interrupted because of the election campaign and the fact that parliament was not sitting for a protracted period of time. And they are filed now. And so we have the overview reports on two of our major security intelligence agencies. And minister sajjan and I are here to respond to your questions

>> Reporter: We found out about the metadata sharing of information in 2013, that is when it was discovered. It was stopped at the beginningover 2014, but Canadians have not found out about this until today in 2016.

Was this because the former conservative government was not willing to share this information with Canadians?

>> I can't answer the question the reasons behind what the former government's reasons were, but when this was brought to my attention after meeting with the minister of international defence, and I also met with the commissioner directly. And have taken appropriate action. This is one of the reasons we have provided a technical brief on this. And we have accepted all the recommendations that the commissioner has laid out.

>> Reporter: What information have you stopped sharing?

>> I didn't hear the question.

>> Reporter: What kind of metadata.

>> The exact kind of metadata in the technical brief, because of the software deficiencies, that has been ceased since that at that time and will not be reactivated until we have the assurance that the safeguard of that privacy will be kept.

>> Reporter: We know that they were sharing information they weren't supposed to and Canadians' private data made it into foreign hands. We no a lot more of that thanks to Edward Snowden. Will you consider legislative measures to stop them from this data collection in the future?

>> It is important to note that the type of metadata that we are talking about, no content is included in that. And the important work that metadata in terms of identifying the type of threats that posed to Canada not just from a

counterterrorism perspective and also over 100 million types of malicious cyber attacks that come onto our Canadian institutions. And what they prevent and I have accepted all the recommendations. And we will be letting that go to plan.

>> Reporter: Is the only accountability mechanism, are you confident that the collection methods and backbone or mass collection apply with Canadian law?

Are you comfortable with the way they collect the data?

>> The collection is done in accordance with the national defence act. One of the important aspects for Canadians to know is the actual deficiency was identified by officials themselves who proactively brought that to the attention of the commissioner. And that is how seriously it is taken.

(Question inaudible)

>> Reporter: Is collecting mass information at least according to the reports that we have, mass information from all onned the world and that have to include Canada data. Are you comfortable with practices that tap the infrastructure of the internet?

>> This is the first time that there is a technical brief. And the first ever in history. And if we have more technical questions, they will be happy to answer that for you.

>> And if I could, let's put this all in the context where we find ourselves as a new government. We have undertaken a complete review of the security intelligence framework. That review will be proceeding over the next weeks and months. The objective here is to make sure that our security and policing agencies are effective in keeping Canadians safe. And secondly, that they are properly respecting Canadian rights and freedoms. And this review will result in a number of changes, including the creation of a parliamentary mechanism which is never existed before.

>> Reporter: On that issue, though, the report shows that cis is collecting metadata, and it is not destroying it. They do have a time frame before it gets rid of it cis is refusing to do so. Will you order them to stop this?

>> The work -- firstover all, it is important to recognize that cirq made it very clear that csis has followed the laws and direct ifrs that they are -- directives that they are supposed to.

In terms of the particular provision on metadata, what the criticism was that they had, according to cirq, they had not properly informed the federal court of the methodology they were using. For the, they conducted a seminar to assure the court so they were fully apprised of all the information that was necessary with respect to metadata. Csis has complied with the recommendation.

(Question inaudible)

>> Not to my knowledge, no.

(Question inaudible)

>> Well a certain type of metadata that we were talking about, we want to make sure that the software updates actually does what it's supposed to do. And that is why we passed off that portion of metadata sharing. It is very important that we do protect the privacy of Canadians while we actively look at the protection side from the counterterrorism work done. And as I stated, there are over 100 million types of malicious cyber attacks that occur on the infrastructure.

>> Reporter: What do you have to see to be convinced to start sharing again?

>> This is something we will have to present and will be some discussion on the type of computer software and the testing that will be done. Once I am satisfied, the commissioner will also be notified as well. And that appropriate comment will be started.

>> I wanted to make the point that in the review of the entire frame work, one of the people that we have consulted with and will continue to consult with closely is the privacy commissioner.

He all through this process will offer very valuable advice.

>> Reporter: Give us an idea of how many people, if you may, farnd you know, how many people, how many Canadians, would have been impacted by this?

>> We can't give you the actual number. By us trying to dig into that answer itself, we in itself will be violating the law and digging up that type of information.

(Question inaudible)

>> Reporter: Is there any guarantee that some of the information didn't end up in hands of countries that we would not voluntarily share with?

>> The agreements that we have in place are solid. We have the same type of agreements that will not be going to outside that realm. And more importantly, we do not share our -- we do not spy on each other's data.

>> Reporter: And any frustration with the metadata not being available for three years? Have they expressed concern that this is impeding their operations?

>> No, our allies are actually very supportive of the work that we do on a daily basis. It is ongoing and to invest to the agreement and very important agreement in the community in place.

>> Reporter: With the cabinet committee in place, you wl be giving authorization or review

>> The parliamentary committee. Off tau cabinet committee, too.

>> Reporter: Can you tell us what the structure or format will be? And will it lead to further authorizations that the report said was weather centering into some of the possible privacy concerns?

>> Obviously I can't discuss cabinet committee activity. That would be a violation of my oath as a councillor, but the cabinet committee structure is designed to insure at the highest level there is that kind of examination, knowledge, and oversight that needs to be provided.

It is one of the most senior committees of cabinet. And it will discharge the responsibilities properly on bhafr of all Canadians.

(Question inaudible)

>> Reporter: Will he have a plan to take with him next week to Rome about dealing with ISIS?

>> I am in discussions all the time with the minister regarding other options. And wefr discussions on this. We knows how I am thinking through the process. And there is ongoing discussions on that. Thank you.

>> Thanks, ministers.

>> Suhana: Lots of questions from or thors. And we were -- from reporters. Answers from the minister of defence harjit sajjan and Ralph Goodale about sharing metadata. There were software discrepancies and deficiencies regarding private information of Canadians being shared amongst other allies. And that has now been stopped. There is also a complete review that is coming from Ralph Goodale of that whole Canadian security framework. Still, not a lot of questions answered about how many Canadians was chaired. If you are not familiar with the term metadata, it is data about data to make it easier to summarize the basic information. But Cameron Macintosh knows way more than I do and joins us with more. What stood out for you?

>> Reporter: Well, I am learning about it. This is the information that the electronic communications around the world and will tell it where to go and an email or I.P. Address. And the Canadian security establishment, which is Canada's eyes and ears around the world to gather foreign intelligence tracks metadata.

The mandate is to not share information. And in 2013, it found some information that it was sharing with the five eyes -- the U.S., U.K., Australia, and new Zealand, and in some circumstances information that could have identified Canadian, not the content of the message, but to identify Canadians wasn't being properly minimized. And that information wasn't being removed from that information that went out to our partners. In 2013 this was discovered within the Canadian security establishment and stopped in 2014 and is becoming public today from the commissioner who oversees the Canadian security establishment and a ban on sharing this type of information will remain in place. And in speaking with

the minister for public safety saying they are looking to strike a parliamently committee to review all of Canada's security agencies and how they are operating.

>> Suhana: Thank you, cam. Cameron Mcintosh in ottawa. And Steve miles is back with a look at the markets.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: ps.pspmediacentre-centredesmediaspsp.sp@Canada.ca

Sent to: !INTERNAL

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre/CentredesmediasPSP (PS/SP)
Sent: Wednesday, January 28, 2015 5:18 PM
To: Today's News / Actualités (PS/SP)
Subject: RT: CBC News (Power & Politics) - Report on CSE's Project Levitation and interview with Canadian Privacy Commissionre Daniel Therrien - 2015-01-28, 17:04 ET

Rough Transcript

Station: CBC News – Power & Politics
Time/Heure: 17:05 ET
Date: 2015-01-28

Summary: *CBC News – Power & Politics reported on the Communication Security Establishment's Project Levitation, which is used to track terrorist activity online. Following this CBC News interviewed Daniel Therrien, the Privacy Commissioner of Canada regarding Canadians concerns about online privacy. Mr. Therrien was also asked questions regarding the upcoming anti-terrorism legislation to be tabled Friday.*

>> Evan: ... CBC News has learned that Canada's electronic spy agency is part of a five-country effort that sifts through millions of online videos and documents every day looking for extremist plots. Revealed in a document obtained by U.S. whistle blower Edward Snowden. Leading the CBC coverage of this, joining me live from Toronto now, Dave Seglins, can you outline briefly how this system works and what it's been finding?

>> Okay. So Canada spy agency access to huge numbers of data bases, data bases that whoever collected it, whether it was the NSA, the UK, we don't know. But they can go to file sharing sites but they're looking specifically for jihadi videos. Hostage videos or instructions on how to build a bomb. They scour millions upon millions. People accessing or sharing that kind of extremist literature or material. Then they can use these other data bases. It's not just this one set of data, but other data bases to piece together a person's internet history, Facebook ID. What this reveals is not just this program levitation, but the five eyes have capacity to recreate lots of internet history about you and I and anyone in the world.

>> Evan: Right. And so we heard about this debate about the meta data. Should Canadians be concerned about things like project levitation?

>> Well, the problem in all of this -- I mean, the goal is good most analysts would say. Let's track down the extremists. But does it go too far? Meta data isn't just useless information. It can be used to piece together people's behaviours, who you're talking to. It's actually quite revealing. The problem in all of this is that the law is really outdated. Operates under a law thrown together in a month after 9/11. Where did they get that law? Orders and council dated in the early 1990s. Quickly wrote it into legislation. Never -- most people in the early 90s didn't have an e-mail address or cellphone or Facebook or all of that. So there were all sorts of vague gaping holes in the law. It's not specific. All it says is do foreign intelligence, don't direct it at Canadians. Never contemplated the nuance of this kind of capability. Here where in 2015. Through the rear view mirror of time we find out the spy agencies have been using this meta data. The question is is it time for the law to be revisited? Number one to give a clearer sense of mandate, but on the oversight, is there a way more people -- Canada alone, the other one of the five eyes that doesn't have some sort of parliamentary or politician oversight. So I think the opposition parties are screaming for this. Certainly a number of security experts that we've talked to, cyber experts say it's high time Canada does this. The government is moving ahead to introduce new legislation, maybe about expanding powers. No word on what they're going to do on the over sight and law end of things.

>> Evan: That's where the rubber hits the road here. The government is about to introduce new legislation on security and this obviously gives us new insight into what exactly they're doing on that side. Thanks for that, Dave.

>>> Canadians are clearly concerned about their online security. The proof, the latest public opinion poll conducted by Canada's privacy watchdog, let's go to the source for that sitting next to me. Good to see you, sir.

>> Good evening.

>> Evan: Canada's security agency is working with five eyes and at their discretion they're supposed to be tracking extremists and terrorists, we just don't know the range of what they're doing. How concerned are Canadians about their privacy and this balance between security and privacy?

>> I think what the poll says is that Canadians are concerned at unprecedented level as to their privacy. 90% of Canadians are concerned and a 3rd of Canadians are extremely concerned about their privacy rights. That's a huge increase from our previous polling. And roughly 7 out of 10 Canadians feel they're losing control over their information.

>> Evan: 7 out of 10. 73%.

>> Evan: Half of the Canadians in this service know about surveillance for the purposes of national security. Most of those people felt those agencies should explain those activities to Canadians. I guess the question is are we being transparent enough about what we're doing?

>> So the percentage of people who want more transparency is actually 90%. 90% of Canadians wish their government to be more transparent. Clearly there needs to be an effort in that respect. And of course we have said a number of times, including after the events in October that although there are oversight mechanisms in Canada for CSIS, the RCMP, that the over sight regime needs to be enhanced to cover other agencies as well.

>> Evan: You heard this project we're just hearing about, project levitation, anti-terror project, sifting through millions of videos and documents. So-called metadata. As the privacy commissioner, what question does something like that raise for you?

>> This is a project about the collection of foreign intelligence which is governed by a separate regime, legislation that applies to C.S.E.C. C.S.E.C. has a lawful mandate to intercept foreign communications. And there is an over sight body that has reviewed activities similar to this. I'm not sure about this particular program, but that has regularly concluded that C.S.E.C. operations are lawful as they pertain to foreign intelligence. For intelligence in Canada, certainly these methods raise questions as to whether it is appropriate to collect bulk information, massive surveillance with a view to identifying new threats to national security. That is a very complicated and difficult question. You may remember that about a year ago, President Obama actually raised similar issues and tasked people in the U.S. administration to try to determine whether it is possible for the government to identify new security threats without going through massive surveillance or what he called bulk information. And our various views expressed on whether that is possible or not, certain experts view that. It is not possible other things that civil liberties should prevail. This is a very complicated issue, obviously. I would say maybe to end on this point that I look forward to the courts actually eventually looking at these issues. Currently two challenges under the charter to the C.S.E.C. legislation, which allows for this massive surveillance, which allows for surveillance based on administrative authorization as opposed to judicial authorization. So these issues are currently before the courts at the trial level. But eventually we should get judgments from the higher courts on this very important question.

>> Evan: I should say as the government is expected to table its anti-terrorist legislation on Friday, the U.S. Ambassador was on this program last week, saying we're encouraging the Canadian government for more sharing information. The Canadian governments collecting data on foreign people, right. But maybe the U.S. is collecting the same on Canadians and that's the sharing. So you just don't know what that means. How concerned are you? We're going into very important legislation. What are the key questions you have now going into the new anti-terror legislation on Friday?

>> Two main ones. First, you raise the issue of transparency and oversight. The legislation we haven't seen obviously. But apparently based on media reports will enhance information sharing between the departments. We'd hope to see enhanced information sharing comes with enhanced transparency and over sight. Point one. Point two: it is understandable that the government would want to monitor individuals who may be suspect of terrorism, but it's quite another thing to collect information and to share information about ordinary Canadians. People who are not suspected of anything with a view to identifying new threats. So that issue of what will happen under this legislation to sharing of information about non-suspects with a view to identifying new threats will be certainly something that I will look to.

>> Evan: One last question on oversight. We heard Dave talk about it. How robust is Canada's oversight on what our security intelligence agencies are doing compared to the UK or the United States? Do we need better oversight?

>> We have oversight for CSIS, RCMP. We do not have oversight for other agencies like the border services agency, who since 2001 are now involved. And we do not have parliamentary oversight. I think we're lagging behind.

>> Evan: Right. But the oversight -- not robust enough you think?

>> It's less robust than in other countries. An appointed body, not full time. Do you think that needs to be more robust?

>> When I say it's comparatively less robust, I'm referring to the fact that certain agencies are not covered like the border service agency and the fact that there's no parliamentary over sight.

>> Evan: That's dangerous.

>> Well, we certainly can do better and there are commissions of inquiry obviously after 9/11 that have recommended to consistently increase oversight. I'd encourage the government to look at these.

>> Evan: Your new poll shows Canadians are concerned. A top concern.

>> Concerned and want more transparency.

>> Evan: A very important issue. We'll be speaking about this a lot on Friday when the new legislation comes out. Thank you so much for that.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at PS.PSPMediaCentre-CentredesmediasPSP.SP@ps-sp.gc.ca.
Questions? Veuillez communiquer avec nous au PS.PSPMediaCentre-CentredesmediasPSP.SP@ps-sp.gc.ca.

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Monday, November 21, 2016 4:04 PM
To: Today's News / Actualités (PS/SP)
Subject: RT: CTV News - Interview w/ former CSIS & RCMP agent re. CSIS briefing notes on Russia/Chinese interest in Canadian state secrets - 2016-11-21 - 11h15 ET

Rough Transcript

Station: CTV News
Time/Heure: 11h15 ET
Date: 2016-11-21

Summary: *CTV News interviewed former CSIS and RCMP agent Ron Miles regarding CSIS briefing notes that identify Russian and Chinese interest in Canadian state secrets.*

>> Marcia: Canada's spy agency is warning that Russia and China are interested in our country's state secrets. Briefing notes from CSIS say the two countries are targeting classified information, as well as government officials and systems. For more on this I'm joined by Ron Miles, a former CSIS agent and former RCMP security service agent. He's with us this morning from Montreal. Good morning, thanks for being on our program.

>> Ron Miles: Good morning. It's a pleasure.

>> Marcia: So CSIS rarely identifies security threats by name. Why do you think they're openly calling out Russia and China?

>> Ron Miles: Well, a security service normally works in the shadows and it doesn't get a lot of publicity, to possibly they are looking for a little bit of good publicity. Russia and more lately China have been very aggressive in hacking, in spying on north America and the west in general. So possibly he's trying to build up a consensus amongst the population so that we become more aggressive in our defence.

>> Marcia: What would Russia and China want from Canada? What sort of information would they be seeking?

>> Ron Miles: Well, Canada is part of the western world, and the demands that, let's say, the old KGB or the Russia and China intelligence agencies, what would they want from us ranges from the classical military intelligence to -- influence. For instance, if you had somebody in the Canadian external affairs or in the American state department, they could influence the way that country decided it was going to handle a particular issue. More recently you have in the American election Russia's been accused of trying to influence the outcome of the election by leaking e-mails it supposedly hacked from Hillary Clinton, from Bernie Sanders. So they have a lot to gain by this spying to influence what's going on in the west.

>> Marcia: Are western countries spying on them?

>> Ron Miles: Oh, absolutely. I think the revelations of Edward Snowden showed that the west is just as aggressive against the east as the east against the west.

>> Marcia: All right, Ron Miles, former CSIS agent and former RCMP security service agent, thank you.

>> Ron Miles: Thank you very much. Have a good day.

>> Marcia: You too.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at ps.pspmediacentre-centredesmediaspsp.sp@Canada.ca.
Questions? Veuillez communiquer avec nous au ps.pspmediacentre-centredesmediaspsp.sp@Canada.ca.

Sent to: !INTERNAL; !INTERNAL 2; RCMP Breaking News

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Friday, September 23, 2016 3:40 PM
To: Today's News / Actualités (PS/SP)
Subject: RT: CTV News - Interview with cyber security expert Chester Wisniewski regarding a report from Public Safety Canada warning about cyberthreats - 2016-09-23, 15:00 ET

Rough Transcript

Station: CTV News
Time/Heure: 15:00 ET
Date: 2016-09-23

Summary: *CTV News interviewed cyber security expert Chester Wisniewski regarding a report about Public Safety Canada warning about cyber threats.*

>> Todd: Also coming out of Ottawa today, we're hearing that major infrastructure technology here in Canada might be at risk of internal cyber attacks. That's according to internal memos from **Public Safety Canada** that were obtained by the Canadian Press. The notes warn operators of things like electric grids, transportation hubs, insiders might be able to cripple some of them if a virus was in their digital systems. The reason why someone on the inside would do this is because of a disgruntled employee. Someone angry with their employer. For more on this, let's bring in Chester Wisniewski, he is coming from Vancouver, and he's a cyber security expert. Good to have you on, Chester. What do you make of the insider threat?

>> Well, I hope it is just a good warning to remind companies to harden their infrastructure and it's not related to any specific intelligence that they have, that something might happen. But what we see often with national critical infrastructure like power grids and things, they are sort of built like a candy bar. They have the hard outside shell to resist foreign nation states hacking them, and all this kind of thing. But once you get on the inside, it's a soft gooey centre, and it's very easy for someone on the inside to take them apart.

>> In layman' terms when we talk about transportation hubs, electrical grids, the key infrastructure systems here, what might we see?

>> Well, you know, again, you know it may not event be disgruntled employees, as you mentioned at the start if a nation state wanted to disrupt Canadians lives, taking down the telecommunication grid would be a good way to do this. You consider tens of thousands of employees at every one of the companies, you could maybe find someone to buy off and would have access to systems they shouldn't. What **Public Safety Canada** is aiming for is to make the infrastructure more resilient by making sure that the inside of the systems only provide access to those that are required to access, rather than just (indiscernible) all of their staff.

>> Todd: I'm also curious what you think in terms of protection. You know, we had the huge hack against Yahoo coming out. That they announced on Thursday. We're hearing about this internal threats, as well, here in Canada. Can you defend yourself against this kind of thing?

>> Well, you're never going to be able to stop it entirely, right. When you have determined human adversaries who are really trying to get in and steal your information or disrupt your infrastructure, I don't think you can ever eliminate that as a threat. What we are trying to do is balance the risk here, and the government is looking at the risk and realizing there's not enough security on the inside of the critical infrastructure companies, perhaps. In order tower the risk, we need to take it more seriously, and invest a lot more money in it.

>> Todd: In terms of the controls over employee, too, if you start to talk about internal risks, internal threats, Chester, again what can we possibly do on that? How can you tell if someone is a threat?

>> Well, yeah. It's very difficult. I mean obviously you know with Ed Snowden and the NSA is a perfect example. They do lot of screenings. It's not like they don't do a background check when you go to work for a security agency. It's not like

someone causing harm. The key component is compartmentalization. Just because I work for the hydro authority doesn't mean I should be able to access all of the parts of the system or all databases, because I'm in the computer department, doesn't mean access to all accounts and all things. By compartmentalize things, you limit the risk that a person with malicious intent.

>> Todd: Chester, thank you for coming on from Vancouver.

>> Thank you.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at ps.pspmediacentre-centredesmediaspsp.sp@canada.ca.
Questions? Veuillez communiquer avec nous au ps.pspmediacentre-centredesmediaspsp.sp@canada.ca.

Sent to: !INTERNAL; !INTERNAL 2

Ellis2, Andrew (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Thursday, January 28, 2016 3:49 PM
To: Today's News / Actualités (PS/SP)
Subject: RT: CTV News - SIRC annual report and the CSE Commissioner's annual report - 2016-1-28, 15h07 ET

Rough Transcript

Station: CTV News
Time/Heure: 15h07 ET
Date: 2016-1-28

Summary: *CTV News reports on the SIRC annual report and the CSE Commissioner's annual report.*

>>> Two watchdog reports are out today that are raising some alarms and red flags. They concern our country's security agencies, such as CSIS, Canada's primary spy agency, and also the CSE, Communications Security Establishment, which monitors communications. Among the findings that the electronic spy agency broke privacy laws by sharing information about Canadians with foreign partners and the CSE is not supposed to be doing that. Let's go to Mercedes Stephenson standing by in Ottawa with more on this. She certainly knows surveillance in this country, knows these agencies. Let's talk about the key findings here in these reports, Mercedes, the highlights for you.

>> Mercedes: So, Todd, let's start with the CSIS report. It properly identified insider threats. Think of Edward Snowden, people who might take secrets from inside and either sell them to another country, or put them on-line, like he did, and basically what they found is CSIS did not deal adequately with some incidents, one in particular, where there may have been somebody working for the agency who actually posed a threat to some of those national secrets, so they're saying they need to do more to make sure those secrets are safeguarded. Also finding some questions about the legal relationship between cis and the department of foreign affairs, something they're currently investigating under the cis act. Switching gears, let's take a look at the cse report. This is the one on signals intelligence for things like phone calls ande-mails. Now CSE belongs to the Department of National Defence, Todd, and under that they have a mandate to intercept foreign signals intelligence.

Part of what they collect is called metadata. That's basically information about who is sending messages, receiving them, where they might be coming from, but it's not the actual internal message itself. If you think about when you send an envelope in the mail, it would be the equivalent of reading the outside of that envelope. But here's the problem, in scooping up all the metadata that CSE does to evaluate, find threats to the country, sometimes Canadians' information gets caught up in that. That's exactly what happened in this case, and then it was transmitted to the so-called five eye, allied countries that we share intelligence with, like Australia and the United States. So back in 2014, the government quietly suspended that intelligence sharing, but Todd, it hasn't resumed yet because they're not satisfied that the appropriate safeguards are in place.

>> Todd: You and I have been having a conversation for years about these agencies, what they do, what they don't do, what they're allowed to do, what we know they are actually doing. How transparent are these agencies?

>> Mercedes: They're not transparent at all. I mean, we have a situation here where you have two watchdogs overseeing them, but particularly in the case of cis, the committee that is tasked with overseeing them can't have access to classified information. So you can imagine when you're talking about a spy agency, that's pretty limiting in terms of what they're able to get. It's only things the agency declassifies, and that in part is why the government has promised they're going to put together a parliamentary committee which will consistent of parliamentarians from the senate and the house of commons to oversee these agencies. That's what the United States, the U.K. And so many other countries do so you have actual elected officials able to hold people to account. The problem is that they're going to have to find a way to ensure secrets don't leak out of there, and also to provide a security clearance, Todd, for the people who are on this committee, because that's the only way they're going to be able to look at some of this classified information and assess it.

>> Todd: Very interesting, Mercedes Stephenson in Ottawa, thanks again for this.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: ps.pspmediacentre-centredesmediaspsp.sp@Canada.ca

Sent to: !INTERNAL

Globe and Mail
Leaked Snowden document shows how 'sigint' nabbed a Canadian al- Qaeda operative
Saturday, 10 December 2016
Byline: Colin Freeze

Ottawa - Communications intercepted by U.S. and British spy agencies led to the arrest of the first al-Qaeda-inspired terrorist caught in Canada, according to a newly leaked document.
The memo, circulated within the U.S. National Security Agency more than a decade ago, provides a rare and detailed look at the world of intelligence-sharing.

In early 2004, a cell of British terrorists was caught scheming to explode a bomb in London. After Scotland Yard launched "Operation Crevice" to round up the conspirators , Canadian police simultaneously moved to arrest an Ottawa software engineer.

Momin Khawaja had helped build detonators for the conspirators. The suspects, including Mr. Khawaja, were twentysomething Westerners whose families had hailed from Pakistan. They had travelled to a terrorist training camp in that country and emerged from it wanting to bomb Britain for its role in the invasions of Iraq and Afghanistan.

Evidence included discussion of close co-operation between British and Canadian police. But prosecutors glossed over how "signals intelligence" (or sigint) captured long before the bust had laid a foundation for detectives.

The details are revealed in a document flowing from Edward Snowden, the fugitive former American contractor who took volumes of files from the NSA in 2013 to leak them to the media.

The Intercept, a news site, has extensive access to the Snowden archive. It has started publishing memos that circulated within the NSA "signals intelligence directorate" in the early 2000s.

The April, 19, 2004 NSA memo titled "SIGINT contribution to Operation Crevice" reads as follows:

"Since March 2003, the U.K.'s Security Service and police had been investigating an AQ (al-Qa'ida) support network based in the U.K. with links to a senior AQ operational planner in Pakistan."

The memo goes on to describe a British mastermind who had wanted to "mount an attack in the U.K. using a large improvised explosive device" and his "Pakistan-based contact [who] was attempting to obtain nuclear material for use in the device."

The eventual evidence at trials was that the British police who unfurled the plot discovered a storage shed containing a large bomb made of ammonium- nitrate, an explosive substance sold commercially as a fertilizer. No evidence of any capability to make a nuclear-material "dirty bomb" surfaced in any

courtroom, although some British media have reported that spies had caught wind of terrorists talking about that possibility.

The leaked memo says the NSA and its British counterpart, known as GCHQ, worked quickly to map out the conspirators' communications before providing investigative leads to Pakistani, British and Canadian agencies.

"Call records analysis and reporting expanded Security Service's network knowledge and helped to identify new telephone numbers of key targets in the U.K.," it says. "C2C (computer-to-computer) analysis provided new leads on a Canada-based individual within the network."

This was an allusion to Mr. Khawaja, who lived with his parents and whose day job was fixing computers for Canada's Foreign Affairs department.

Mr. Khawaja became the first terrorist to be arrested, tried and convicted under the Anti-Terrorism Act that Parliament passed in 2001. He is serving a life sentence.

The leaked NSA memo, which is to be officially declassified in 2032, says that "well over 100 Sigint reports were issued on Operation Crevice." Most came from GCHQ but "the NSA reporting contributed significant pieces to the jigsaw."

A Canadian agency called the Communications Security Establishment is a close NSA and GCHQ ally, but the Operation Crevice memo makes no mention of it. At that time, the Canadian agency was beginning to get secret authorizations from cabinet ministers to expand its powers.

CBC News
Trade tribunal looking into weather supercomputer contract
Monday, 12 December 2016
Byline: Alison Crawford

A trade tribunal is conducting an inquiry into how the federal government handled the purchase of a powerful new weather-forecasting supercomputer for Environment Canada.
Computer company Hewlett-Packard Canada alleges the government's IT department, Shared Services Canada, wrongly invoked a national security exception in the procurement process.

Hewlett-Packard is the latest in a long list of Canadian companies to allege the federal government routinely imposes such exceptions for no good reason.

"Government contracts are a huge business in Canada. This is a real market that a lot of businesses in Canada depend on to survive," said Chris McLeod, an Ottawa lawyer who specializes in international trade and public procurement.

A national security exception means buyers are exempt from trade rules that require all bidders to be treated equally and may mean equipment must be made in certain countries and data must be stored or processed within Canada.

Hewlett-Packard has also asked the Federal Court to determine if Shared Services Canada (SSC) applied the exception appropriately.

"The NSE (national security exception) applies to all procurements for SSC relating to email, networks and data centres ... by invoking a blanket NSE, Public Services and Procurement Canada has improperly and unlawfully sought to immunize itself from scrutiny and compliance with the procurement rules set out in domestic and international trade agreements," the company said in its submission.

Shared Services Canada says it cannot comment because the matter is before the courts.

Hewlett-Packard was among four qualified companies invited to bid on leasing the federal government a new supercomputer, storage cloud, storage networks, processors and software, over 8½ years with an option to renew the contract for 30 months. The contract includes two upgrades as well as maintenance and support.

In its Federal Court filing, Hewlett-Packard said it was told in June that its bid was non-compliant and had been disqualified.

Last week, CBC News reported SSC secretly awarded the $430 million contract to IBM Canada in May.

Blanket approval for exceptions

According to government documents and e-mails filed at Federal Court, SSC asked for and received blanket approval in the spring of 2012 to invoke a national security exception on virtually all its big purchases. That means procurements are excluded from the obligations of all domestic and international trade agreements signed by Canada, "including those that may come into force in the future," according to the internal government correspondence. The stated goal was to protect the IT supply chain from cyber threats.

The initial pitch for such a ban was made by Benoît Long, who was a senior executive at SSC.

"There is a significant risk that potential suppliers with relationships with foreign intelligence agencies hostile to Canada could tamper with system components (whether hardware or software) in advance of delivery to the Crown in order to facilitate future covert access," he wrote to Tom Ring, former assistant deputy minister of Public Works.

What followed was a high-level meeting with senior executives from Canada's spy agencies CSIS and CSEC, the Privy Council Office, Treasury Board and Shared Services. Two invitees from DND were absent but they, like all the others, signed attestations saying they agreed to the idea of invoking a blanket exception.

Soon after, Ring approved the plan.

"I agree to invoke the national security exception for all purposes to exempt the procurement of goods and services related to the Government of Canada's electronic mail (email) network, and data centre infrastructure, systems and services from the application of Canada's domestic and international trade agreements, including those that may come into force in the future," Ring wrote in his response to Long.

Ever since, SSC and Public Services and Procurement Canada have invoked national security exceptions on a whole host of federal contracts -- everything from night-vision binoculars and a new federal government email system, to data storage and supercomputers.

Tide could be turning

Not only do national security exceptions permit SSC and Public Services and Procurement Canada to limit who may bid on a contract, they also prevent people from seeking redress from any trade tribunal.

"All the rules go out the window and your ability to challenge these procurements goes out the window," lawyer McLeod told CBC News.

For years, companies in the same situation as Hewlett-Packard sought redress from the Canadian International Trade Tribunal (CITT), only to be told it had no jurisdiction when a national security exception had been invoked. After several years, though, the tribunal started to make noises about the integrity of the competitive procurement system.

"There's a potential that government actors may use the national security exception to avoid rules that they would otherwise be subject to instead of simply following their rules, even when there's no national security risk at play," said McLeod.

Tribunal is unhappy

In February 2016, the tribunal indicated it had had just about enough, when Toronto IT firm Eclipsys Solutions complained it was unfairly excluded from bidding on a SSC contract. While the CITT conceded it had no jurisdiction, the tribunal made it abundantly clear it wasn't happy about it.

"Opposing nothing more than the NSE applicability as a complete response to a supplier's grounds of complaint is an empty and silent response indeed; it leaves potentially unanswered doubts lingering as

to the transparency and fairness of the impugned procurement," wrote the tribunal's presiding member Serge Fréchette.

"The tribunal is concerned that relying on an authorization that is already several years old and is both 'blanket' in nature and open-ended into the future (i.e: with no specified end date) increases the risk that the NSE will be invoked automatically or by rote, or without proper considered justification, or altogether inappropriately."

Ground-breaking victory

McLeod's own client, M.D. Charlton, had also been excluded, by virtue of a national security exception, from a federal contract to provide the RCMP with night-vision binoculars.

And in August, McLeod successfully established for the first time that the government had improperly invoked a national security exception. The tribunal found the government "breached the trade agreements by failing to properly tailor the scope of the exception."

"There are lots of national security exceptions that are legitimate ... I'm the first one to say that. There are also situations where the national security exception invocation goes too far, [beyond] what's needed," McLeod said.

London Times
Prepare for cyberspace Pearl Harbor, warn experts
Saturday, 10 December 2016
Byline: Deborah Haynes

London - The potential for a "cyberspace Pearl Harbor" is growing as countries such as North Korea, Iran and Russia test the boundaries of internet warfare, security experts said last night.
Britain, the United States and their allies are also building and testing cyberweapons but, unlike with conventional arsenals, no one knows for sure what damage their adversaries can inflict with computer codes that their cyberwarriors have written.

Adding to the opaqueness of cyberwarfare, there are no international rules or principles governing the way that countries should behave in cyberspace, other than the overriding belief among western powers that all actions should adhere to international law.

The absence of agreement on when a cyberattack becomes an act of war has empowered nations to fire cyberweapons at each other in tit-for-tat skirmishes that only come to public attention when something too big to hide happens. "It is not quite conflict. It is not quite war," a former senior western intelligence official said. "It is the exchanges of fire across the border. It is really not helpful."

North Korean hackers, who are among the best in the world, recently used software to steal secrets from the South Korean military unit responsible for fending off cyberattacks, a major embarrassment for South Korea.

Iran, or "state-affiliated groups", apparently targeted the computers of an agency that runs Saudi Arabia's airports last month, wreaking havoc.

Even the US election campaign was alleged to have been affected by cybermeddling, thought to be linked to Russia, with huge leaks of data from the Democratic National Committee designed to undermine Hillary Clinton's presidential hopes. President Obama ordered a review into election hacking by the Russians yesterday.

John Bassett, a former senior official at GCHQ who now sits on the international advisory group PS21, a think tank, said: "Because you are apparently able to get away with it via cyber, people are willing to chance their arm far more.

"Eventually my concern is that one of these things goes horribly, horribly wrong and something dreadful happens, like someone unintentionally takes down the intensive care unit of a hospital."

One apocalyptic scenario would be using a computer virus to destroy a nation's entire electronic infrastructure, even making -- for a country such as Britain, France or the US -- nuclear weapons explode in their silos.

"We are a very, very long away from any evidence that the worst is at all achievable," Mr Bassett said. "Rather more credible is something very bad happening, such as a nation's air defences being taken down. That is where you get on to the cyber Pearl Harbor."

General Sir Richard Barrons, a former military officer and a leading authority on war in the information age, said: "Cyberspace could deliver strategic harm to the homeland and vital interests. People need to organise for that in a way that they have never had to in history."

Financial Post
Fintech as a Force for Social Good
Saturday, 10 December 2016
Byline: Adam Nanjee

Ottawa - For enterprises concerned about network security, identity verification has become a top-of-mind issue in an era of ubiquitous cyber- crime. But for millions around the world with no valid identification, standard computer access and identity authentication measures such as passwords pose a formidable barrier to not just public services, but also to the formal economy and traditional financial institutions.

When BioConnect, a Toronto-based biometric firm, launched seven years ago, its goal "was to solve the big problem of identity" posed by entities like banks that require customers to provide traditional paper documents to open accounts, explains vice president of strategic marketing and global alliances Bianca Lopes. She cites two telling statistics: according to CISCO, there are now 50 billion digitally connected devices globally, but there are also 2.5 billion human beings who are not considered people because they don't have ID. "These people can't enter the system," says Lopes.

BioConnect's technology suite allows the firm's customers to use a range of biometric identifiers - facial expressions, iris patterns, even cardiac rhythms - to identify users. Lopes sees the technology as key to providing mobile banking services in developing countries where many people have a smart phone but no physical way of connecting to a financial institution. "The technology allows these systems to see these people, so they can become part of the economy," she adds.

For Canada's rapidly globalizing financial technology (fintech) sector, such stories reveal the ways in which these mobile technologies produce both new revenue streams and social dividends.

Fintech firms have the capacity and the technology to develop widely accessible, competitive services that support socially positive activities instead of just boosting the banking sector's profit margins, says Canada>Sponsored>Brand&utm_content=YoungMoneyMoneyFintechAsAForceForSocialGo od-Sponsored-brand&utm_term=FinancialPost" target="_blank">Mogo (www.mogo.ca) founder Dave Feller. "Platforms that provide consumers with features like real-time updates on their Canada>Sponsored>Product&utm_content=YoungMoneyMoneyFintechAsAForceForSocial Good-Sponsored-creditscore&utm_term=FinancialPost" target="_blank">credit scores (www.mogo.ca) result in an overall financial awareness and produce social benefits in the form of fewer personal bankruptcies and reduced consumer debt. The more financially fit we are, the more likely we are to contribute," says Feller. "It has a ripple effect on society."

Outside Canada, the potential is even greater, particularly among the estimated

two billion people globally that currently have no access to banking services, according to the World Bank. While traditional banking services are unattainable, mobile banking is certainly within the realm of possibility. California-based market research firm, The Radicati Group, projects that 84 per cent of the world's population will be using mobile technology by the end of 2018.

"What if these people could access financial services online or through mobile devices?" asks Dinaro Ly, director of MaRS FinTech. "The result would be increased financial literacy and improved social inclusion on an international scale," he adds.

In order to go global, fintech ventures need access to international advisors who can help them gain an understanding of the local business landscape, assess market fit, and secure customer opportunities

Goldmoney, a fintech platform with a broad social goal, already has international traction. For several decades, gold has held its value much more consistently than all sorts of currencies, both strong and weak (while it fluctuates, overall gold has risen 10% per year against the Canadian dollar for 15 years running).

But gold hasn't been widely available as an investment vehicle in developing nations because it trades in minimum denominations that preclude small purchases, says Darrell MacMullin, CEO of Goldmoney Network. MacMullin's firm enables users to create savings accounts through which they can buy even a few cents worth of gold at a time. Founded in May 2015, the fintech startup now has 1.3 million accounts in 150 countries, with combined deposits worth $1.9 billion. George Soros was an early investor. "He liked the idea of providing upward mobility for two billion people around the world," says MacMullin."

Impak Finance is hoping to take the fintech-driven social dividend concept one step further. The firm, which was founded a year ago, will allow consumers to open savings accounts and direct their funds to organizations or companies that require loans to finance a range of socially or environmentally beneficial activities and businesses. "The project is to create a bank that will be a catalyst for the social impact ecosystem," says co-founder Paul Allard, adding that it will begin lending funds next year and introduce consumer savings accounts in 2018.

The company, which has raised $1 million in lending capital since October, relies on a more holistic risk algorithm to evaluate the creditworthiness of borrowers, but it also provides depositors with a say in the sorts of firms that they'd like to back. "You choose the sector where you want to see your money at work," he says, citing sectors such as cleantech or bio-agriculture.

Canadian fintech firms have some novel solutions, but if they hope to have greater social impact, they must leverage international partnerships.

As a global innovation hub, MaRS is a gateway to international markets for Canadian companies. Take the recently announced partnership between MaRS and NTT Data, the systems arm of the Japanese telecom and information technology giant, which promises to provide local fintech firms access to the Japanese market.

Under this partnership entrepreneurs working in the fintech sector will be invited to participate in a global business challenge that offers startups the opportunity to present solutions to economic problems like population decline and aging, environmental destruction, depletion of resources, and the rising cost of healthcare.

Winners will receive business development support from NTT Data to run a proof of concept, with the objective of commercializing their technology in the Japanese market.

"In order to go global, fintech ventures need access to international advisors who can help them gain an understanding of the local business landscape, assess market fit, and secure customer opportunities," says Ly.

In addition to partnering with NTT Data in Tokyo, MaRS has established a network of co-working spaces in key locations such as San Francisco, New York, Singapore, London, Shanghai, Tokyo, Sao Paulo and Hong Kong to give Canadian startups a base in these vital markets.

This story was created by Content Works, Postmedia's commercial content division, on behalf of Mogo.

Motherboard Blog
Terror Scanning Database For Social Media Raises More Questions than Answers
Saturday, 10 December 2016
Byline: Sarah Jeong

Ottawa - On Monday, Facebook, Microsoft, Twitter, and YouTube announced a new partnership to create a "shared industry database" that identifies "content that promotes terrorism." Each company will use the database to find "violent terrorist imagery or terrorist recruitment videos or images" on their platforms, and remove the content according to their own policies.
The exact technology involved isn't new. The newly announced partnership is likely modeled after what companies already do with child pornography. But the application of this technology to "terrorist content" raises many questions. Who is going to decide whether something promotes terrorism or not? Is a technology that fights child porn appropriate for addressing this particular problem? And most troubling of all--is there even a problem to be solved? Four tech companies may have just signed onto developing a more robust censorship and surveillance system based on a narrative of online radicalization that isn't well-supported by empirical evidence.

How the Tech Industry Built a System for Detecting Child Porn

Many companies--for example, Verizon, which runs an online backup service for customers' files--use a database maintained by the National Center for Missing and Exploited Children (NCMEC) to find child pornography. If they find a match, service providers notify the NCMEC Cyber Tipline, which then passes on that information to law enforcement.

The database doesn't contain images themselves, but rather, hashes--digital fingerprints that identify a file. This means that service providers can scan their servers without "looking" at anyone's files. Thanks to PhotoDNA, a technology donated by Microsoft, the hashes are made using biometric information inside the photos and videos, meaning that cropping or resizing the files won't necessarily change the hash value being used.

Monday's announcement marks the first time companies have sought to use this kind of technology to combat "terrorist content online." It's an odd match. The hash matching system appealed to many aspects of the fight against child pornography. For one thing it allowed companies to scan for files without finding out anything about non-matching files--so, arguably, without violating anyone's privacy, except with respect to possession of child porn. It also protected people from having to look at child porn in order to identify it--the very act of looking at child porn so it can be removed from the internet can be traumatic to the employees who are policing content on platforms.

Applying the Hash System to Terrorism

Neither of these specific upsides to the hash identification system seem to apply to "terrorist content," since the partnership appears to be aimed at publicly posted social media. (I asked Facebook via email whether the hash identification system would be applied to private messages between users, but did not hear back from the company). Furthermore, the companies have stated in their press release that a person on the other end will be looking at the content before taking it down. The press release implies, but does not explicitly say, that matching hits will not be provided to government officials, the way that hits for child pornography are.

Indeed, one of the useful things about the child pornography hash identification database is that it's managed by a single entity with specific knowledge and experience in the content at issue--that is, NCMEC. The industry database for "terrorist content" that's being proposed will be composed of hashes added by each platform, as they remove content as consistent with their own policies.

Facebook removes "content that expresses support" for groups involved in terrorism or organized crime. Even "supporting or praising leaders of those same organisations, or condoning their violent activities" is banned from the platform. So for example, a video that praises ISIS might get taken down by Facebook. The Facebook employee or contractor taking it down might choose to hash the video, and share the hash through the database. The database will flag the same video when it's uploaded on YouTube.

YouTube's terrorism policy, however, is different from Facebook's- -it prohibits terrorist recruitment videos and other content that intends to incite violence. Theoretically, the same video that gets banned from Facebook might pass muster on YouTube. And just because it's in the database doesn't mean that it'll automatically get taken down.

But Facebook, Twitter, and YouTube have all been vigorously criticized for their seemingly haphazard and inconsistent application of their existing policies, whether with respect to nudity, harassment, or copyright infringement. Identifying "terrorist content" implicates just as many tricky questions of judgment.

A video of a guy in a ski mask beheading an American journalist seems like a pretty straightforward case scenario, but the world is a lot more complicated than just ISIS and not-ISIS. Hamas is not only a major

political party that wins parliamentary elections in Palestine, it's also been designated as a terrorist organization by many countries, including the United States. The Kurdistan Workers' Party (sometimes called the PKK, short for Partiya Karkerên Kurdistanê) is also designated as a terrorist organization by the United States, even as the US has provided air support for their ground forces to fight ISIS.

"To me, you've built a hammer and now you're asking the world to look for nails."

If the State Department can't be consistent on who's a terrorist and who's not a terrorist, is it really a good idea to entrust that decision to tech companies that are strangely baffled by human nipples?

These worries aren't just speculative. Facebook has, in the past, been criticized for its apparent censorship of Palestinian journalists.

Experts worry that the inflammatory way that society and the media deals with terrorism, combined with a corporate-driven takedown process will result in illegitimate censorship. "To me, you've built a hammer and now you're asking the world to look for nails," said Andy Sellars, director of the Boston University / MIT Technology and Cyberlaw Clinic. "This is a system that encourages over-reporting."

Although the press release emphasizes that the database only flags content, and removal will not be automatic, Sellars said that he didn't see a world where tech companies would hesitate to remove content flagged as "terrorism- promoting."

And flagging content based on hashes focuses on the content, not the context or the message sent. Sellars pointed out that child pornography "is really the only place where media is contraband by its very definition." An ISIS recruitment video, on the other hand, shifts in meaning and effect when being shared by journalists, or by social scientists studying extremism.

This point is echoed by others. Hugh Handeyside, a staff attorney at the American Civil Liberties Union (ACLU) said, "This kind of digital hash system has been used to identify child pornogrpahy but child pornogrpahy and so called terrorism content are not really comparable. The first is always illegal, the second may be news."

And in a January 2016 interview for On the Media, John Horgan, a professor of psychology at Georgia State University who specializes in studying terrorist behavior, said: "Pedophilia and terrorism are quite different. I mean, there is no clear sense of what involvement in terrorism is. Terrorism can involve anything from browsing radical sites to donating money to questionable sites, to far more extreme activity of wanting to go overseas to become a foreign fighter or constructing bombs." (I emailed Horgan for further discussion but he did not respond in time for this article's publication).

Does "Content Promoting Terrorism" Lead to Actual Terrorism?

Technology built to address child porn might be a bad fit for combating "terrorist content," but even more troublingly, there isn't consensus on whether terrorists are converted by extremist content on the internet. In fact, there's a lot of evidence that says they aren't.

Handeyside at the ACLU said that "decisions about what constitute terroristic content are often based on theories about radicalization and violence that research and studies have debunked."

Horgan is similarly critical of the narrative of online radicalization. He said that there is no single profile of a terrorist, or what makes someone into a terrorist. In fact, it seems that "radicalization" might not even be part of the process.

"There is increasing evidence that suggests that people who become involved in terrorism don't necessarily hold radical views. At least not to begin with," Horgan said in January. "In many cases we see people's radical views developing as a result of spending time in a terrorist group. ... There are lots of examples of individuals I've interviewed who have said, 'Well, I didn't realize why I became involved in this movement until ... I wound up in prison.'"

'How dare you spend all of your time just engaging in social media. You need to get up off your backsides and come out here and join the fight.'

ISIS is certainly very active on social media, and their presence on platforms created by US companies may be alarming for people who otherwise feel like they are distant from the ongoing conflict abroad. But ISIS's social media presence doesn't necessarily translate to real world effects.

Horgan said that even ISIS acknowledges that for many of its supporters, their involvement both begins and ends online. "One of our researchers, Charlie Winter, discovered several senior female jihadis based in Syria complain to foreign supporters here in the United States, to say to them, 'How dare you spend all of your time just engaging in social media. You need to get up off your backsides and come out here and join the fight.'"

Potential Law Enforcement Exploitation of the Database

Monday's press release implies that the partnered companies are not going to be giving the government unfettered access to scan their platforms using the hash database.

"No personally identifiable information will be shared ... And each company will continue to apply its practice of transparency and review for any government requests," the press release reads. But it stops short of explicitly stating that it won't, for example, comply with a Foreign Intelligence Surveillance Act (FISA) order similar to the one that got Yahoo to build a scanner that searched the emails of all customers.

Indeed, in that particular case, an anonymous official told The New York Times that the government was scanning for a "digital signature" of a "communications method used by a state-sponsored, foreign terrorist organization" in the emails of all Yahoo mail users. It's not known whether the FISA order was for a hash value. (In fact, other sources have told Motherboard that the description given to the Times was wrong, and that the Yahoo scanning tool was more similar to a rootkit).

Facebook and Google have been criticized in the past for allowing the National Security Agency access to their users' data under the PRISM program, as exposed in the Snowden documents. Ever since the backlash around those revelations, many tech companies have become much more wary about their cooperation with the United States government--a development sometimes referred to as "the Snowden effect."

But even if you can now count on companies to resist forking over information without a legally binding government order, that doesn't say the government can't get a legally binding order that that gives it access to the newly constructed terror-image database and accompanying scanning capabilities.

Sellars, and other lawyers familiar with the law around electronic surveillance, say that a warrant to, for example, scan all of Facebook for a particular image, would lack "particularity"--a requirement under the Fourth Amendment, which bars unreasonable search and seizure. However, a FISA order might be a different story. The Electronic Frontier Foundation has, and continues to argue, that such orders would be unconstitutional, and there is some debate as to whether FISA or any law could legitimately authorize the order at issue in the Yahoo mail case. But the Yahoo mail case, and other ongoing cases raise troubling precedents for what the courts have allowed to pass muster.

"The ability to transfer this idea from the particular context of identification on online platforms, to a tool of surveillance, is perhaps the scariest thing," said Sellars. Whether and to what extent the government can hijack the technology that Silicon Valley is building for its own use remains to be seen. It's not clear that the law allows law enforcement or intelligence agencies to be able to scan entire social media platforms for particular images or videos. The only thing we know is that it's not just technically possible, but that four companies have partnered to build out the infrastructure to do it.

Le Monde
Archives Snowden : quand DGSE et DGSI étalaient leur rivalité
Saturday, 10 December 2016
Byline: Jacques Follorou

Paris - Les services français ont parfois préféré travailler avec les Britanniques et les Américains plutôt qu'entre eux
Dans l'ombre de la stratégie antiterroriste française se joue une autre guerre. Loin des déclarations gouvernementales assurant que l'ensemble de la communauté du renseignement unit ses forces, la rivalité historique entre les deux principaux services français, la Direction générale de la sécurité

extérieure (DGSE) et la Direction générale de la sécurité intérieure (DGSI) n'a, en réalité, jamais cessé. Au point de privilégier parfois les liens avec des services étrangers à la coopération entre directions françaises du renseignement.

" Les cousins ", comme ils s'appellent eux-mêmes, se jalousent depuis un siècle. Mais depuis 2008, début du programme d'investissement massif de la France dans la création d'une plate-forme nationale de renseignement technique gérée par la DGSE et mutualisée aux principaux services secrets français, la DGSI (qui s'appelait jusqu'en 2014 la Direction centrale du renseignement intérieur, DCRI), n'a eu de cesse de vouloir s'émanciper de la DGSE dans son utilisation des moyens techniques du renseignement.

Dépendante techniquement, la DGSI l'était aussi sur le plan humain : que pouvaient faire ses policiers face aux ingénieurs X-Télécoms de la direction technique de la DGSE? L'actuel patron de la DGSI, Patrick Calvar, a milité auprès des parlementaires comme du gouvernement pour finir par obtenir les moyens de diversifier ses recrutements, notamment en direction des ingénieurs ou d'informaticiens.

En 2015 et début 2016, ces querelles de territoires apparaissaient toujours lors du suivi des suspects par la DGSE et la DGSI. Ces deux services, malgré les alertes de l'autorité de contrôle des interceptions administratives, " branchaient " ou " débranchaient " des cibles dans le plus grand désordre, sans que l'information circule.

Bernard Bajolet, patron de la DGSE, confirmait, lors d'un colloque coorganisé, fin 2015, par la CIA, aux Etats-Unis, " le besoin d'une parfaite coopération entre les services pour se débarrasser des angles morts, en particulier pour le suivi des suspects à l'intérieur et à l'extérieur des frontières " . Un sujet sensible, puisque l'un des frères Kouachi, impliqué dans l'attaque contre Charlie Hebdo, avait ainsi pu disparaître des radars.

Statut de " senior sigint "Pour défendre son pré carré, la DGSE défend son titre officiel de leader, en France, en matière d'interceptions techniques (également appelé " senior sigint "), que le gouvernement lui a attribué en 2008.

De nouveaux documents extraits par Le Monde , en collaboration avec le site The Intercept , des archives d'Edward Snowden, ex-consultant de l'Agence nationale de sécurité (NSA) américaine confiées à Glenn Greenwald et Laura Poitras, montrent que les deux principaux services français ont été très empêtrés dans leur rivalité. Conséquence : ils ont parfois privilégié une coopération bilatérale avec la NSA ou avec son homologue britannique, le GCHQ, à celle qu'ils devaient avoir entre eux.

Une note de la NSA qui annonce la visite " le 18 juin 2013, de 9 heures à 14 heures " de Bernard Bajolet, nommé à la tête de la DGSE en avril 2013, illustre la volonté du renseignement extérieur d'interdire à la DCRI tout contact avec la NSA. Il est précisé qu'il souhaite rencontrer les principaux responsables de la NSA et évoquer son statut de " senior sigint ". En janvier 2014, M. Bajolet enfonçait le clou dans un texte paru dans la RevueDéfense nationale rappelant à qui voulait l'entendre que " la DGSE assure le rôle de chef de file national (senior sigint) en matière renseignement électronique " .

Car la DCRI a noué, comme la DGSE, d'étroites relations bilatérales avec des services étrangers, notamment le GCHQ. Celles-ci sont régulièrement évoquées dans la lettre d'information interne du GCHQ, dénommée " Frelnet ", frappée d'un très haut niveau de classification, " Top -Secret Strap 1 ", et consacrée aux relations avec les services secrets alliés.

" C'est regrettable "Plusieurs lettres du GCHQ en 2009 et début 2010 se félicitent des " échanges avec la DGSE " . La direction technique de la DGSE, dit que le GCHQ est " très désireuse de démontrer son savoir-faire " et note qu'elle " regrette parfois que l'on n'aille pas plus loin " . Il faut donc, mentionne l'un de ces lettres internes, faire en sorte de " répondre techniquement aux attentes de la DGSE " .

La DCRI n'est pas pour autant laissée pour compte. Bien au contraire. Visiblement à l'insu de la DGSE, le service secret technique britannique a monté, avec la DCRI, des " opérations de contre-espionnage " , dont une, qualifiée de " majeure " , contre une puissance étrangère.

Les moyens techniques très puissants des Britanniques ont été associés au savoir-faire de la DCRI sur le sol français. Elle serait, selon les informations du Monde , toujours en cours et considérée comme stratégique au regard des enjeux de sécurité international actuels. La DGSE n'en aurait appris l'existence que bien plus tard, selon une source gouvernementale.

Pour échapper aux regards de la DGSE, la DCRI a joué la carte de la NSA pour obtenir l'historique des communications d'un suspect ayant séjourné à l'étranger. Elle adressait alors sa requête à l'agence américaine qui lui retournait la réponse dans un cadre de coopération judiciaire via le FBI américain. C'est par ce biais que la NSA, à la demande de la DCRI, a livré, en 2012, l'ensemble des données de connexions à l'étranger de Mohamed Merah.

En février 2016, interrogé par Le Monde , le préfet Bernard Squarcini, chef de la DCRI de 2007 à 2012, admettait, sans fournir de détails : " C'est regrettable mais en matière de coopération, les services français coopèrent mieux avec leurs homologues étrangers qu'entre eux. "

South China Morning Post
E-commerce sites on mainland most targeted by hackers
Monday, 12 December 2016
Byline: Zen Soo

Beijing - Greater China is facing an increasing number of cyberattacks on online transactions, with e-commerce websites being the most vulnerable, according to a recent cybersecurity report.
The increasing number of attacks on e-commerce websites come as the trend of cross-border e-commerce continues to grow, with more consumers shopping online for the best deals, according to cybersecurity firm ThreatMetrix's "Cybercrime Report Q3 2016".

According to ThreatMetrix data, fraudulent log-in attempts comprise about 11.8 per cent of e-commerce transactions in Asia-Pacific, compared to 4 per cent in the finance industry as hackers become more interested in gathering user data to exploit people's identities down the road.

E-commerce sites often make it easy for customers to log in or create an account, forgoing extra layers of security such as two-factor authentication to create a frictionless shopping experience, said Alisdair Faulkner, chief products officer and co-founder of ThreatMetrix.

He added that e-commerce sites are often "sitting ducks" for such hackers because users often give such sites a wealth of personal information, including addresses and phone numbers, allowing hackers to compile "dossiers of information" for later use.

"With your identity, [hackers] could access your medical record, insurance, even your bank accounts. They could collect enough information, impersonate someone's identity and apply for a loan at a bank ... or commit tax fraud," he said.

These same e-commerce sites often lack strong authentication measures for customer log-ins, and often do not inform users about data breaches.

"E-commerce sites can't force customers to have more security," Faulkner said, adding that additional security measures may put off customers from buying from the merchant.

This is particularly true in countries like China, where more than 600 million people use smartphones. Merchants today often make it easier to create accounts or log in on their mobile devices, where screens and keyboards are much smaller than on a desktop computer.

In particular, the greater China region faces an extremely high number of automated bot attacks, which can be combined with identity or device spoofing in large scale cyberattacks, according to the report.

"There are no uniform standards around privacy ... we don't have the same level of guidelines for people's identities and how it's protected [compared to financial information] because data is typically treated as not encrypted whereas credit card data is," Faulkner said.

He said that credit card data is much less valuable than identity and personal information, because hackers only make a one-time gain from credit card fraud whereas impersonating an identity may be more lucrative in the long run.

The Asia-Pacific region sees more than 200,000 identity abuse attacks daily, according to ThreatMetrix data, an increase of about 50 per cent from last year.

"Anybody in Asia could be getting these attacks - they just don't experience it directly," Faulkner said.

He added that companies like ThreatMetrix compile digital profiles of mobile devices and how they are used to help companies and merchants determine if transactions are legitimate or suspicious.

Suspicious transactions would get flagged by ThreatMetrix in real-time, allowing companies to manually review them and decide if they should allow a transaction to go through.

CBC News
Federal government's Canada.ca project 'off the rails'
Tuesday, 13 December 2016
Byline: Staff reporter

The federal government's bid to merge 1,500 departmental and agency websites into a single site, Canada.ca, is a year behind schedule and almost 10 times over budget. And experts warn it is on track to be another failed government IT project, like the Phoenix pay system.
"It's gone off the rails. It's a disaster," said one government source with knowledge of the project who spoke on condition of anonymity.

CBC spoke with a number of government workers who are also familiar with the project in different departments and they all expressed similar evaluations.

The Canada.ca initiative was launched in 2013 with the goal of making it easier for people to find and use government information online. A $1.54-million contract for a new content management system, where all government websites would be moved, was awarded to Adobe in 2015.

The original deadline to have all active web content moved to the single portal was this month. But in June, it was pushed back to December 2017, which was the initial deadline for the migration of all archived content.

The contract with Adobe is now above $9.4 million, according to government figures.

The actual migration of the websites is up to the departments themselves and is to be done within existing budgets and staffing. Since 2015, eight of the largest departments have budgeted or spent more than $28 million on this project.

Those departments include: Employment and Social Development; Immigration, Refugees and Citizenship; Health; Environment; Canada Revenue Agency; National Defence; Fisheries and Oceans; and Global Affairs.

According to the government, only 10,000 web pages have been moved to date. There are more than 17 million Government of Canada web pages in total.

"If it's cost them already 10 times their existing budget to migrate only 0.05 per cent of the content for the Government of Canada, we're talking about it ultimately costing hundreds of millions of dollars. It's not a small price ticket," said Mike Gifford, CEO of Ottawa-based web development company Open Concept, who has written articles criticizing the government's approach to Canada.ca.

New deadline 'impossible'

Based on the current timeline, Gifford said he thinks the December 2017 deadline is unrealistic. He's not alone.

"Absolutely impossible to achieve," said Timothy Lethbridge, who teaches software engineering and computer science at the University of Ottawa. "And I'm sure many people inside the project know it."

There's also a good chance of the project failing altogether, Lethbridge said, because large IT projects are exponentially more complex. "As a project of this size gets bigger, the probability of failure goes up."

If the government spread the work out over a number of years and spent a billion dollars, it might be able to make the migration a success, Lethbridge said. But he questioned whether taxpayers would be getting value for money at that point.

This is not the first large government IT project to run into problems.

The government will spend at least $50 million this year to try to fix problems with the new Phoenix pay system, which has seen thousands of public servants underpaid, overpaid or not paid at all.

The initiative to transform the government's email system has been stalled for months because of problems with new software.

And Shared Services Canada, the agency created in 2011 to modernize IT-related services in government, has been slammed for its many missteps, particularly by the auditor general.

"There's a trend," said Robin Galipeau, managing partner of OpenPlus, a content architecture company. "There's definitely something going on there. Large renewal projects in IT are failing in government."

OpenPlus, along with Dell and Microsoft, submitted a bid to create the new CMS for Canada.ca.

Ministers refuse to comment

According to OpenPlus Chief Technology Officer Joel Brockbank, the federal government continues to erroneously believe there are one-size-fits-all software solutions for its IT goals.

"There never is," he said. "It's like your cross-trainer running shoes. It's not good for anything that you do."

The key to not having large IT projects fail, Brockbank said, is to simply not do them. Instead, such projects should be done in stages or "bite-size chunks."

None of the ministers whose departments are involved in the Canada.ca migration project were willing to comment when contacted by CBC News.

Treasury Board President Scott Brison, Social Development Minister Yves Duclos and Public Services and Procurement Minister Judy Foote all declined requests. As did Michel Laviolette, the director general of Service Canada, and John Messina, the federal government's chief information officer.

"That tells me they have something to hide," said Debi Daviau, president of the Professional Institute of the Public Service of Canada, the union representing many of the government's IT workers.

"If they're unwilling to be transparent about the decisions they make, that calls those decisions into question."

Yonhap News Agency
Military investigators raid cyber command in hacking probe
Tuesday, 13 December 2016
Byline: Staff reporter

Seoul - Military investigators have raided South Korea's cyber command as part of their investigation into the first hacking of the command's intranet that is being blamed on North Korea, military officials said Tuesday.
"The Defense Security Command is thoroughly looking into how the cyberattacks took place, what confidential information has been leaked and if there was any professional negligence," a military official told Yonhap News Agency.

He confirmed that military prosecutors were overseeing the raid while the Defense Security Command was collecting documents in a raid to the cyber command on Tuesday.

In September, the defense ministry recognized that a total of 3,200 computers, including 700 linked with the intranet, were contaminated with malware a month after the latest cyberattack took place.

The ministry found in October some military documents were hacked while refusing to provide details. The computer used by Defense Minister Han Min-koo also turned out to have been compromised.

Last week, the ministry said the IP addresses linked to the attack were traced to a location in China that has been used by North Korean hackers.

As one of the military's two integration servers was jointly linked to the internet and the intranet, it allowed the hackers to gain access to the intranet, it said.

The cyber command separated the affected server from the whole network to avoid the spread of viruses in October, two months after the initial hacking attempt was made in August.

It marked the first time that the data of South Korea's cyber command has been compromised. South Korea set up the command in January 2010 as part of its efforts to counter external hacking attempts on the country's military.

North Korea -- which has thousands of cyberwarfare personnel -- has a track record of waging cyberattacks on South Korea and the United States in recent years, though it has flatly denied any involvement.

Yonhap News Agency
Acting President Hwang redoubles calls for robust cyberdefense
Tuesday, 13 December 2016
Byline: Song Sang-ho

Seoul - South Korea's Acting President and Prime Minister Hwang Kyo- ahn on Tuesday redoubled calls for robust cyberdefense against North Korea, saying cyberwarfare with the provocative state has already begun.
Following a suspected hacking by Pyongyang of Seoul's cybercommand intranet, Hwang and South Korean security officials have repeatedly stressed the need to prepare against the North's surreptitious cyberattacks which could be as devastating as physical military strikes.

"As evidenced in the recent hack of the (South's) defense ministry, North Korea has attempted to mount cyberattacks on major government facilities, and (this shows) cyberwarfare has already begun," he said during the first regular Cabinet meeting since he took over as acting president last Friday after President Park Geun-hye was impeached over a corruption scandal.

"Related ministries, including the ministries of defense and future planning, must devise thorough measures to prevent any recurrence (of hacking incidents) and take special caution not to allow any minor mistakes to threaten our security," he added.

The defense ministry said last week that a total of 3,200 computers, including 700 linked with the intranet, were infected with malware in August. The computer used by Defense Minister Han Min-koo was also affected, officials said.

In recent years, Seoul has been pushing to bolster its cyberdefense capabilities as Pyongyang has launched a host of attacks on South Korean corporate and government websites by mobilizing its specially trained personnel, including those based in China and other foreign countries.

The reclusive regime has denied responsibility for its cyberattacks including the latest one, upbraiding Seoul for "fabricating" claims about online attacks.

Hwang, in particular, ordered the government to check the nation's financial, traffic, broadcasting and energy networks, and other major national facilities to verify if they are exposed to any cybersecurity threats.

On the economic front, Hwang said that the country's economic fundamentals remain strong as Seoul has striven to maintain a consistent policy despite political uncertainties sparked by the corruption scandal.

The acting president also urged economic officials to keep close tabs on the financial and foreign exchange markets, as he pointed to the potential negative ramifications from a possible United States interest hike.

"I call on you to closely monitor the market situation and respond to it in a timely and resolute manner," he said.

Hwang went on to urge the Cabinet ministers to make concerted efforts to protect the socially vulnerable, including children from low-income families and senior citizens, particularly during the winter season.

Later in the day, Hwang held a luncheon meeting with senior professors and journalists as part of his efforts to solicit their views on ways to bring the nation, gripped by the scandal, back on track.

Hwang renewed his pledge to focus on forestalling any government vacuum and restoring stability in state governance.

Meanwhile, Hwang stepped up efforts to tackle a series of pending issues that can affect the wellbeing of citizens, as he strives to project an image of a trustworthy -- albeit temporary -- leader.

On the day, he directed Agriculture Minister Kim Jae-soo to convene a meeting of senior government officials and civilian experts, dedicated to containing avian influenza (AI), on a daily basis to better tackle the highly contagious virus.

He also instructed top officials from provincial governments to hold their own daily meetings separately to help stem the spread of the bird flu that has ravaged chicken farms across the country since mid-November.

Visiting police stations in Seoul, he called on officers to tighten their crackdown on crimes targeting women and other vulnerable individuals, particularly in the nighttime. He also ordered the police to "root out" violent or drunk drivers, saying they could cause large-scale accidents involving many casualties.

Regarding the heavy snowfall expected for some parts of the country between Tuesday night and Wednesday afternoon, Hwang directed related ministers to take the necessary steps to minimize any possible damage or inconvenience to citizens.

Japan News
Attacks by Anonymous against Japan rising
Tuesday, 13 December 2016
Byline: Staff reporter

Cyber-attacks against Japan apparently carried out by international hacker group Anonymous have been increasing since September.
Last autumn, a number of government websites and other sites came under attack. However, the recent attacks are different from sophisticated cyber-attacks that aim to steal information. Experts call for people to respond calmly by taking necessary steps in advance without fearing them too much.

Late at night on Sept. 3, the website of the Hiroshima National Peace Memorial Hall for the Atomic Bomb Victims became inaccessible. Shortly after, a group saying it was Anonymous and opposed to dolphin hunting and other issues posted a statement online claiming responsiblity.

An official at the memorial hall said in bewilderment, "We have nothing to do with dolphin hunting."

It is believed a series of Anonymous attacks called Operation Killing Bay started around 2013 in protest against Japan's whale hunting and the annual dolphin hunts in Taiji, Wakayama Prefecture, in September.

Last year, to protest against the dolphin hunting in Taiji, distributed denial of service (DDoS) attacks were launched against government offices websites and infrastructure operators such as airports. DDoS attacks are aimed at rendering websites and other online services unavailable by sending a huge amount of data to the server.

According to police, the number of cyber-attacks Anonymous is believed to be involved in has grown since September. There were no cyber- attack-related website problems from May to August, but 29 incidents were confirmed in September, followed by 26 in October. From Nov. 1 to Nov. 27, there were 53 cases, bringing the total from September to Nov. 27 to 108.

In comparison, incidents ranged between the 10s and 20s each month from September to November last year, but rose to 56 in December.

"Their aim is not to make websites unavailable, but to promote their presence," said Nobuhiro Tsuji, senior security researcher at SoftBank Technology Corp.

This year, the targets of the attacks have conspicuously been small organizations and shops such as izakaya Japanese pubs, and groups totally unrelated to dolphin hunting. "The hackers could be different from last year, and their resources could be smaller," Tsuji said.

'Respond coolly'

When Anonymous started around 2006, it advocated the establishment of the freedom of the internet and made political appeals through legally permitted activities such as street demonstrations.

Currently, however, Anonymous tends to carry out cyber-attacks with the aid of unknown individuals who respond to invitations on Twitter and other websites. Participants are increasingly committing cyber-attacks for fun.

The website of the Kasumigaura river office of the Land, Infrastructure, Transport and Tourism Ministry came under attack in 2012. Anonymous is believed to have confused Kasumigaura with Tokyo's bureaucratic district of Kasumigaseki. The incident was indicative of the group's sloppy management.

Anonymous' main attack method, DDoS, can be committed without significant expertise. Basically, there is no way to defend against such attacks. It is a matter of waiting for an attack to cease, although measures have recently been developed to mitigate damage.

"Compared to cyber-attacks aimed at stealing information, DDoS attacks are not so sophisticated. In most cases, the websites attacked went down and that was it," said Masakatsu Morii, a professor at Kobe University specializing in information and telecommunications engineering.

Some observers point out that such cyber- attacks could increase ahead of the 2020 Tokyo Olympics and Paralympics. Morii said, "It is important that companies and organizations take necessary measures calmly. If they are attacked, they should respond coolly without overreacting."

The Australian Financial Review
Lone wolves and data dumps a problem (Canada)
Tuesday, 13 December 2016
Byline: Jonathan Porter

Sydney - Constant reconnaissance probes by nation states, attacks by computer network robber barons and lone wolves and data dumps from disgruntled workers - that is digital Australia's bleak picture painted for a cyber security forum in Sydney recently.
And without constant vigilance and fine-tuning of our cyber defences, the problem will only get worse.

"A lot of nation states and militaries are investing in capabilities that can be used to target utilities; power, water resource and energy providers," Major-General Stephen Day, former head of cyber at the

Department of Defence who was the inaugural head of the Australian Cyber Security Centre, told the Australian Computer Society Cyber Forum in Sydney.

"There is no question reconnaissance is going on right now."

The glimpse behind the curtain at Australia's cyber defenders came during the question and answer period at the end of the forum, attended by some of the world's leading experts in the field.

An attendee put to the panel that an emerging risk was not lone wolf attackers "but of a state-sponsored cyber-attack sometimes from friendly countries we consider allies" and asked what was being done to mitigate the risk.

Day agreed that state-sponsored attacks were a "significant risk", particularly if people looked down the track a few years.

He added that there was also a "significant challenge with organised crime".

"We looked at the sectors that mattered most to our nation either from an economic prosperity perspective or from a national security perspective and put them in a priority order and looked at those sectors that were likely to be targeted by organised crime or by nation states and then we directed our organisational energy to help those sectors.

"So if, for example, you are in the utilities sector or critical infrastructure sector you will have had more experience of government contacting and working with you than the retail sector or the banking sector where you are likely to meet the police more than the national security base."

Victorian minister for Small Business, Innovation and Trade Philip Dalidakis said that while Day's statements were "sexy" and would generate headlines "the one thing everyone in the room has to be extremely cognisant of is that the overwhelming majority of attacks occur from within".

"Yes, we need to be able to stop attacks from the outside of the firewall but the fact of the matter is the two greatest attacks we have seen of data theft from inside were from Bradley Manning and (Edward) Snowden," he told the forum.

"There are a range of companies that will swear black and blue that they have got algorithms that will help flag anomalies within the system - people accessing certain types of data that they haven't done for ages - (or) if you have got your networks categorised under different security levels - people trying to access levels [other] than their security classification. Ultimately it comes down to people and training, each organisation has to have people who are trained appropriately who can deal with it when - it's not a matter of if - it occurs."

Some of the greatest risks in organisations were the IT divisions themselves, he says.

"People who have the administrative access rights and passwords are sometimes the ones who are undertaking a whole range of activities that people on the rest of the network are banned from doing - including downloading huge amounts of illegal data. Which is, of course, one of the ways people get in.

"So don't go away from this thinking that if you focus on external you are protected because your internal [network] is 80 per cent of your risk."

On the intelligence side, he said he could speak more freely than other panel members because he was not a representative of the federal government.

Dalidakis said the nation was well served by the Five Eyes agreement on signals intelligence sharing with the US, Canada, New Zealand and the United Kingdom.

Fellow panel member Sandra Ragg, assistant secretary for cyber policy in the Department of the Prime Minister and Cabinet, said the nation did need to improve its cyber defences.

"The first thing we can do is improve our cyber defences.

"People focus on state- sponsored threats but cybercrime is a huge piece of the threat to our economy."

Politico
Is Trump's Twitter account a national security threat?
Tuesday, 13 December 2016
Byline: Nahal Toosi

Washington - Donald Trump has years of experience launching Twitter wars. But now, as he prepares to take the highest office in the country, there are growing fears that his tweets could spur a genuine national security crisis.
Intelligence and defense specialists believe the president-elect's use of the popular and powerful social media network is already being used by foreign agencies to analyze his personality, track his habits and detect clues about what to expect from a Trump-led American government.

And that's just based on what Trump writes on Twitter. It's not even counting the vulnerabilities that could arise if overseas hackers invade his phone and digital accounts.

"We've never had a president that's shared so much of themselves, not just what they're saying, but their psychological ticks in such an overt manner, and you can be sure that foreign actors are studying that, too," said P.W. Singer, a defense expert and co-author of "Cybersecurity and Cyberwar." "We're beginning to see what excites him, what angers him, what sets him off. We've never had this ability to read so much on what a president is thinking."

Trump, who prefers mobile phones to computers, is highly attached to his Twitter account (@realDonaldTrump), using the platform to share his thoughts deep into the night. Days after his stunning election victory, he was reportedly worried he would not be able to keep his Android phone upon reaching the Oval Office, suggesting he plans to keep tweeting even after he's sworn in. During his first sitdown interview as president-elect, he told "60 Minutes" that he would be "very restrained" in his Twitter use while in office, before using his account to rail against The New York Times the same day the interview aired.

Trump's following of 17.2 million is likely to expand as he takes office, and his disdain for the mainstream media may bolster his desire to keep up his direct outreach to the public through Twitter.

For the most part, the president-elect has used Twitter to comment on people and institutions on the domestic front, or to defend himself against their criticisms. His tweets are believed to have even influenced the stock market, including on Monday, when his criticism of Lockheed Martin's F-35 program was followed by a drop in the aerospace company's market value. On several occasions, however, Trump has ventured into the international realm.

In recent days, amid lingering Chinese anger over Trump's decision to break U.S. protocol and speak directly to the president of Taiwan, Trump, using two tweets, wrote: "Did China ask us if it was OK to devalue their currency (making it hard for our companies to compete), heavily tax our products going into.. their country (the U.S. doesn't tax them) or to build a massive military complex in the middle of the South China Sea? I don't think so!" On Monday, he used Twitter to sow doubts about claims he's not hard enough on Russia.

Granted, foreign intelligence agencies will likely look at all of Trump's public utterances -- his speeches, interviews, written press releases -- as well as those of his aides to try to understand one of the more unusual men ever to win the White House. (U.S. intelligence analysts do similar studies of foreign leaders, especially in countries such as Iran and North Korea, whose governments are considered hostile and with whom U.S. communication is limited.)

But so far, at least, Twitter has proven one of the purest distillations of Trump around -- a raw version of a businessman-turned-politician keen on ignoring the traditional conventions of the presidency.

Twitter's 140-character limit on tweets appears to appeal to Trump's short attention span and his preference for rapid-fire interactions. But 140 characters often don't leave space for much context, explanation or nuance. So what Trump writes may come across as more forthright and harsher than what foreign governments are accustomed to in the diplomatic arena. The risk for a misunderstanding is, therefore, higher.

Foreign analysts following Trump's Twitter may not be inclined to simply take everything he writes at face value, especially when it comes to highly sensitive subjects. But, using sophisticated data tools, they

may look for patterns that, over time, can help them better predict if Trump is being serious. In all likelihood, many intelligence specialists overseas have probably already done such analyses based on Trump's more than 34,000 tweets so far.

"If Trump's comments accurately reflect his intent, then we're giving the opponents a head start in dealing with the incoming presidential administration," a former U.S. intelligence officer said of Trump's Twitter habits. "If his comments are meant to conceal other intentions, then we're doing a pretty good job in misleading our adversaries."

A foreign government may check to see if Trump uses certain types of words before he takes certain types of actions. If Trump keeps tweeting during his presidency, a foreign entity may analyze what types of things he writes before making a policy announcement. (If Trump were to enable Twitter's geo-location services, that could also grab the attention of overseas actors, though it doesn't appear he uses that feature.) Even a lengthy silence from Trump could be a signal of some sort, sources connected to the intelligence community told POLITICO.

In August, David Robinson, a data scientist, published an analysis of Trump's tweets using digital tools.

It indicated that there were at least two people tweeting out under Trump's account. The tweets from an Android phone appeared to be coming from the Manhattan billionaire himself -- they were angrier and more negative. The ones from an iPhone were more quotidian, sharing announcements and photos; those were likely posted by one or more Trump campaign aides. (Some tweets may have been written by a staffer trying to sound like Trump.)

"A lot of 'emotionally charged' words, like 'badly', 'crazy', 'weak', and 'dumb', were overwhelmingly more common on Android," Robinson wrote, meaning it was Trump who was probably behind those particular tweets.

The U.S. has occasionally found itself in diplomatic dust-ups thanks to Twitter.

In September, during President Barack Obama's visit to China, the Defense Intelligence Agency tweeted "Classy as always China" after the American leader was deprived of a normal red-carpet arrival due to a dispute over which stairs he could use to leave his plane. The Pentagon-based agency later deleted the tweet and apologized.

Four years earlier in Egypt, during the brief presidency of Muslim Brotherhood leader Mohamed Morsi, the U.S. Embassy in Cairo slapped the Islamist organization's English-language Twitter account after it expressed concern for the safety of U.S. diplomats amid violent protests near their building.

"Thanks. By the way, have you checked out your own Arabic feeds? I hope you know we read those too," the embassy tweeted, implying the Brotherhood was using a very different tone in its non-English messages. The Americans later deleted the tweet.

Although Twitter has been around for most of Barack Obama's presidency, the outgoing president has been careful in using the medium. He was allowed to start using his own official account, @POTUS, only a couple of years ago: in May 2015, he sent out an inaugural tweet. The @POTUS account will be made available to Trump once he is sworn in.

The @BarackObama account is run by Organizing for Action, a liberal group that has long supported the president. It was not immediately clear if Obama would take over that account once he leaves office, but he's used it in the past, signing tweets he composed with a "-bo".

The White House Communications Agency, a military division that handles presidential communications security, referred questions about Trump's Twitter account and plans to safeguard his digital devices to the president-elect's transition team. The transition team did not respond to a request for comment. To date, it's not clear if Trump's phone conversations with foreign leaders are fully secured, though his team has said precautions have been taken.

Even as foreign capitals sift through Trump's tweets, there are questions about whether the social media company should take away his account for calling out individual Americans on Twitter. Trump's targets have included an Indianapolis union leader and a college student, who have faced death threats and harassment as a result.

When asked for comment about whether Trump should be booted off the platform, a spokesperson for the company replied: "The Twitter Rules apply to all accounts."

Reuters
Top U.S. spy agency has not embraced CIA assessment on Russia hacking - sources
Tuesday, 13 December 2016
Byline: Jonathan Landy, Mark Hosenball

Washington - The overseers of the U.S. intelligence community have not embraced a CIA assessment that Russian cyber attacks were aimed at helping Republican President-elect Donald Trump win the 2016 election, three American officials said on Monday.
While the Office of the Director of National Intelligence (ODNI) does not dispute the CIA's analysis of Russian hacking operations, it has not endorsed their assessment because of a lack of conclusive evidence that Moscow intended to boost Trump over Democratic opponent Hillary Clinton, said the officials, who declined to be named.

The position of the ODNI, which oversees the 17 agency-strong U.S. intelligence community, could give Trump fresh ammunition to dispute the CIA assessment, which he rejected as "ridiculous" in weekend remarks, and press his assertion that no evidence implicates Russia in the cyber attacks.

Trump's rejection of the CIA's judgment marks the latest in a string of disputes over Russia's international conduct that have erupted between the president- elect and the intelligence community he will soon command.

An ODNI spokesman declined to comment on the issue.

"ODNI is not arguing that the agency (CIA) is wrong, only that they can't prove intent," said one of the three U.S. officials. "Of course they can't, absent agents in on the decision-making in Moscow."

The Federal Bureau of Investigation, whose evidentiary standards require it to make cases that can stand up in court, declined to accept the CIA's analysis - a deductive assessment of the available intelligence - for the same reason, the three officials said.

The ODNI, headed by James Clapper, was established after the Sept. 11, 2001, attacks on the recommendation of the commission that investigated the attacks. The commission, which identified major intelligence failures, recommended the office's creation to improve coordination among U.S. intelligence agencies.

In October, the U.S. government formally accused Russia of a campaign of cyber attacks against American political organizations ahead of the Nov. 8 presidential election. Democratic President Barack Obama has said he warned Russian President Vladimir Putin about consequences for the attacks.

Reports of the assessment by the CIA, which has not publicly disclosed its findings, have prompted congressional leaders to call for an investigation.

Obama last week ordered intelligence agencies to review the cyber attacks and foreign intervention in the presidential election and to deliver a report before he turns power over to Trump on Jan. 20.

The CIA assessed after the election that the attacks on political organizations were aimed at swaying the vote for Trump because the targeting of Republican organizations diminished toward the end of the summer and focused on Democratic groups, a senior U.S. official told Reuters on Friday.

Moreover, only materials filched from Democratic groups - such as emails stolen from John Podesta, the Clinton campaign chairman - were made public via WikiLeaks, the anti-secrecy organization, and other outlets, U.S. officials said.

"THIN REED"

The CIA conclusion was a "judgment based on the fact that Russian entities hacked both Democrats and Republicans and only the Democratic information was leaked," one of the three officials said on Monday.

"(It was) a thin reed upon which to base an analytical judgment," the official added.

Republican Senator John McCain said on Monday there was "no information" that Russian hacking of American political organizations was aimed at swaying the outcome of the election.

"It's obvious that the Russians hacked into our campaigns," McCain said. "But there is no information that they were intending to affect the outcome of our election and that's why we need a congressional investigation," he told Reuters.

McCain questioned an assertion made on Sunday by Republican National Committee Chairman Reince Priebus, tapped by Trump to be his White House chief of staff, that there were no hacks of computers belonging to Republican organizations.

"Actually, because Mr. Priebus said that doesn't mean it's true," said McCain. "We need a thorough investigation of it, whether both (Democratic and Republican organizations) were hacked into, what the Russian intentions were. We cannot draw a conclusion yet. That's why we need a thorough investigation."

In an angry letter sent to ODNI chief Clapper on Monday, House Intelligence Committee Chairman Devin Nunes said he was "dismayed" that the top U.S. intelligence official had not informed the panel of the CIA's analysis and the difference between its judgment and the FBI's assessment.

Noting that Clapper in November testified that intelligence agencies lacked strong evidence linking Russian cyber attacks to the WikiLeaks disclosures, Nunes asked that Clapper, together with CIA and FBI counterparts, brief the panel by Friday on the latest intelligence assessment of Russian hacking during the election campaign.

Yahoo News
Suspected Russian cyberattack waged on Clinton campaign just days before vote
Monday, 12 December 2016
Byline: Michael Isikoff

Washington - In the closing days of the 2016 election campaign, hackers believed to be working for Russian intelligence launched a new wave of attacks on Hillary Clinton's campaign and the Democratic National Committee -- a previously unreported cyberoffensive that heightened concerns, now endorsed by the CIA, that the Russian government was seeking to influence the outcome of the election in favor of Donald Trump, according to sources familiar with the investigations into the attempted intrusions.
The attacks came in the form of so-called "phishing" emails sent to nearly a dozen campaign and committee staffers in a renewed effort at penetrating their networks, said Dmitri Alperovitch, the co-founder and chief technology officer of CrowdStrike, the cybersecurity firm hired by the DNC to repel

attacks on its network. Staffers at that point were alert enough to reject entreaties to click on the unsolicited email messages that would have allowed the hackers into their computers, he said.

But at least one top Clinton campaign staffer, communications director Jennifer Palmieri, told Yahoo News on Sunday that she received an alert from Google in mid- October informing her that her personal Gmail account had been targeted by a "foreign state" actor and that her password needed to be changed.

"They were targeting us throughout the election," said another former senior Clinton campaign staffer, who asked not to be identified. "They never stopped trying to get back in."

The disclosure of the late campaign attack could fuel a mounting controversy over U.S. intelligence findings that link Russian intelligence to the cyberattacks for the express purpose of throwing the election as part of a campaign, orchestrated in Moscow, to defeat Clinton.

The Washington Post reported Saturday that the CIA has briefed members of Congress on an assessment that the Russians targeted Democratic political organizations and campaign officials as part of a specific effort to defeat Clinton and elect Trump. This goes beyond an earlier public finding that U.S. intelligence officials were "confident" that the Russian government was behind the cyberattacks, but did not ascribe a motive for the Russians doing so.

One piece of damning evidence behind the new finding is that the CIA and the FBI have both identified specific individuals associated with or close to the Russian government who provided the DNC emails to WikiLeaks, which began publishing them in July, a senior law enforcement official told Yahoo News. Despite reports of a clash between the CIA and the FBI over the motive behind Russia's intelligence service in launching the operation, the differences are more a matter of "degree" and emphasis, with the FBI believing there may have been "mixed" motives for the Russian effort, the official said. Still, "we all agree they did these things," the official said.

But President-elect Trump doubled down on his rejection of the intelligence findings in an interview with Fox News anchor Chris Wallace that aired Sunday, dismissing any conclusion that points to Russian government involvement.

"I think it's ridiculous," Trump told Chris Wallace in interview that aired on "Fox News Sunday," his first Sunday show sit-down since winning the election. "I don't believe it."

"If you look at the story and you take a look at what they said, there's great confusion," Trump added. "Nobody really knows, and hacking is very interesting. Once they hack, if you don't catch them in the act you're not going to catch them. They have no idea if it's Russia or China or somebody. It could be somebody sitting in a bed someplace. I mean, they have no idea."

Alperovitch of CrowdStrike, the cybersecurity firm that first publicly linked the cyberattacks to Russian intelligence, said Sunday that he was "puzzled" by Trump's remarks and assumes he has not yet been fully briefed on the matter. (CrowdStrike, whose principals include Shawn Henry, the former chief of the FBI's cyber division, was initially hired by the DNC to investigate the cyberattacks and defend its network last May.)

"At this point, the matter of attribution on the intrusions has been settled,"Alperovitch said. "There is nobody that looks at the evidence who disputes this." Asked his level of confidence in his firm's findings, he responded "100 percent."

Much of the evidence, he said, revolves around the nature of the sophisticated tools used by the attackers on the DNC and forensic evidence showing strong similarities to Russian cyberattacks that have occurred in Ukraine and other Eastern European countries -- as well as to intrusions of the Joint Chiefs of Staff, the White House and the State Department and other U.S. government agencies. "The digital fingerprints are of the same origin," said Alperovitch.

CrowdStrike initially identified two sets of attackers on the DNC's servers: One, dubbed "Cozy Bear," was associated with the Russian FSB (the successor to the Soviet KGB) and which first breached the DNC's network in the summer of 2015. Another, dubbed "Fancy Bear," has been associated with Russia's military intelligence service, the GRU. The latter infiltrated the DNC's network in late April of this year in what turned into a far more devastating attack, resulting in the disclosure of 20,000 internal DNC emails to WikiLeaks -- an act, according to Alperovitch, of "information warfare." (He acknowledged that a third Russian intelligence service, the SVR, which has responsibility for foreign intelligence operations, may also have been involved.)

"When we look at this over 10 years -- literally hundreds of intrusions -- [and] you look at the tradecraft, you look at the victims, it all points to Russian intelligence services," Alperovitch said.

In addition, he said, there was another separate cyberattack discovered in late September from an undetermined party that penetrated DNC computers with software containing sensitive voter analytic data that was being provided in regular memos to Clinton campaign manager Robby Mook, the sources said.

The breach was detected by CrowdStrike, and the cyberinvaders were expelled from a cloud server housing the data; this server was distinct from the DNC's internal computer network that had been previously breached, he said. But the intruders were never identified, and it was never determined whether the data -- containing detailed reports on voter registration and estimates of likely voter participation in the November election -- was ever actually stolen.

Alperovitch said he doesn't know whether these hackers were associated with Russian intelligence; they used different methods and publicly available cybertools to pull it off -- also he said the DNC never authorized his firm to conduct a full investigation. But he said the late October "phishing" attacks on the

DNC and the Clinton campaign resembled the earlier Fancy Bear attacks, leading him to conclude they were likely the work of the GRU.

Moreover, attacks by the Cozy Bear intruders have continued throughout the fall, targeting multiple organizations, including think tanks and universities whose scholars work on Russian policy issues, he said.

And even more recently, he said, there was evidence that the separate "Fancy Bear" hackers are now also attacking political organizations in Germany and elsewhere in Europe in an apparent attempt to meddle in their elections as well. (The chief of German domestic intelligence said last week that there has been a recent increase in "aggressive cyberespionage" against German politicians and warned about "growing evidence for attempts to influence the [German] federal elections next year."

"These activities have not stopped," said Alperovitch. "Now that they were executed [in the United States] and they have a successful playbook, I fully expect they are going to continue."

Press TV
Iranian Army unveils new indigenous combat, reconnaissance drones
Tuesday, 13 December 2016

Tehran - The Iranian Army's Ground Forces has unveiled two domestically-designed and -manufactured drones on the final day of major military exercises code-named Mohammad Rasoulallah IV (Mohammad, the Messenger of God IV) in southeastern Iran.
One of the two aircraft, code- named Oghab (Eagle), is a combat drone capable of carrying air-to-surface missiles.

The other, code-named Shahin (Falcon) and developed and manufactured under a project code-named Shahid Mohsen Ghotaslou, can collect information on the positions and movements of enemy forces on reconnaissance missions. It boasts a flight endurance of 24 hours.

General Seyyed Kamal Peyambari, the spokesman for the military drills, said the jamming and combat techniques of drones were also fully tested at various altitudes on Tuesday, with the participation of military commanders and defense experts.

Peyambari noted that sophisticated and innovative weapons such as super- caliber 107mm rocket launchers, optimized versions of the 62.5mm PSG-1 and Dragunov semi-automatic sniper rifles, a jammer with an effective range of 800 meters, drone jammers, and cellular satellite phone jammers were put to practice on the last day of the drills as well.

Various and extensive psychological war techniques such as drills using 122mm flyer-carrying rockets, tactical radios and directional sound systems were also put to the test for the first time.

The senior Iranian military figure further noted that hand-launched drones as well as land minelayers were also tried out.

Peyambari added that electronic warfare, armored, infantry, mechanized infantry, commando, and intelligence units present at the Mohammad Rasoulallah IV military exercise, which covered an area of 220,000 square kilometers, successfully carried out their operations on the third day of the drills.

Iran has conducted major military drills in recent years to enhance the defense capabilities of its Armed Forces and to test modern military tactics and state-of-the-art equipment. Each year, the country inaugurates a host of new projects and hardware developed with reliance on domestic capabilities.

The Islamic Republic maintains that its defense power is driven by deterrence and poses no threat to any other country.

Hindustan Times
Legion: Meet the hackers who broke into Twitter accounts (Canada).
Tuesday, 13 December 2016

New Delhi - A hackers' group called Legion has repeatedly breached the Twitter accounts of some well-known Indians, including Congress vice- president Rahul Gandhi and prominent journalist Barkha Dutt. Legion has not posted any classified information on the hacked accounts but has threatened to expose email communications among Congress party leaders in the New Year. Earlier this month, they on his Twitter handle, vowing to bring to justice the fugitive industrialist who has defaulted on at least Rs 7,000 crore bank loans.

Here is some detail about the hackers' group: What is Legion? It is a coalition of like-minded hackers based out of five countries - the United States, Sweden, Canada, Thailand and Romania, according to the Delhi police's cybercrime cell. The group seeks to expand its activities, leaving its email id -- legion_group@sigaint.org - for more hackers to join their campaign.

Are they connected with Legion of Doom of the 1980s? The group does not appear to have any links with the hackers' group Legion of Doom (LoD) that targeted rich and famous people's email accounts in the mid-1980s. LoD remained active till early 2000s. However, the two groups appear to share ideological goals in targeting what they say are the rich and corrupt. LoD was founded by US-based hacker Lex Luthor after he broke away from the Knights of Shadow.

Why do they hack people's accounts? Legion fancies itself as cyber vigilantes working to expose the corrupt. But the group is yet to bolster their anti-corruption crusader credentials, given that it has so far offered very little valuable information.

How does Legion operate? Legion communicates through email servers and browsers that are shielded against surveillance. In other words, it does not use Google Chrome or Internet Explorer but a browser called The Onion Router (TOR), which is difficult to track (provides anonymity) and allows a user to communicate directly with another one. This is also called the darknet, a platform often used by activists and journalists seeking to avoid a surveillance dragnet.

Are there other such hackers' groups? Yes. Anonymous is another loosely associated international network of activist and hacktivists which started operating in 2003. The group's website describes it as "an Internet gathering" with "a very loose and decentralised command structure that operates on ideas rather than directives". The group became known for crashing websites of governments, corporates and religious groups. Anonymous members (known as "Anons") use the Guy Fawkes mask as their emblem.

Saudi Gazette
IoT continues to pose a key cyber security threat
Tuesday, 13 December 2016
Byline: Mohammed Al-Moneer

Riyadh - The cyber landscape changes dramatically year after year. If you blink, you may miss something; whether that's a noteworthy hack, a new attack vector or new solutions to protect your business. Sound cyber security means trying to stay one step ahead of threat actors.
In the spirit of looking toward the future, I wanted to grab my crystal ball and take my best guess at what will be the big story lines in cyber security in 2017.

1. IoT continues to pose a major threat. In late 2016, all eyes were on IoT-borne attacks. Threat actors were using Internet of Things devices to build botnets to launch massive distributed denial of service (DDoS) attacks. In two instances, these botnets collected unsecured "smart" cameras. As IoT devices proliferate, and everything has a Web connection -- refrigerators, medical devices, cameras, cars, tires, you name it -- this problem will continue to grow unless proper precautions like two-factor authentication, strong password protection and others are taken.

Device manufactures must also change behavior. They must scrap default passwords and either assign unique credentials to each device or apply modern password configuration techniques for the end user during setup.

2. DDoS attacks get even bigger. We recently saw some of the largest DDoS attacks on record, in some instances topping 1 Tbps. That's absolutely massive, and it shows no sign of slowing. Through 2015, the largest attacks on record were in the 65 Gbps range.

Going into 2017, we can expect to see DDoS attacks grow in size, further fueling the need for solutions tailored to protect against and mitigate these colossal attacks.

3. Predictive analytics gains ground. Math, machine learning and artificial intelligence will be baked more into security solutions. Security solutions will learn from the past, and essentially predict attack vectors and behavior based on that historical data. This means security solutions will be able to more accurately and intelligently identify and predict attacks by using event data and marrying it to real-world attacks.

4. Attack attempts on industrial control systems. Similar to the IoT attacks, it's only due time until we see major industrial control system (ICS) attacks. Attacks on ecommerce stores, social media platforms and others have become so commonplace that we've almost grown cold to them. Bad guys will move onto bigger targets: dams, water treatment facilities and other critical systems to gain recognition.

5. Upstream providers become targets. The DDoS attack launched against DNS provider Dyn, which resulted in knocking out many major sites that use Dyn for DNS services, made headlines because it highlighted what can happen when threat actors target a service provider as opposed to just the end customers.

These types of attacks on upstream providers causes a ripple effect that interrupts service not only for the provider, but all of their customers and users. The attack on Dyn set a dangerous precedent and will likely be emulated several times over in the coming year.

6. Physical security grows in importance. Cyber security is just one part of the puzzle. Strong physical security is also necessary. In 2017, companies will take notice, and will implement stronger physical security measures and policies to protect against internal threats and theft and unwanted devices coming in and infecting systems.

7. Automobiles become a target. With autonomous vehicles on the way and the massive success of sophisticated electric cars like Teslas, the automobile industry will become a much more attractive target for attackers. Taking control of an automobile isn't fantasy, and it could be a real threat next year.

8. Point solutions no longer do the job. The days of Frankensteining together a set of security solutions has to stop. Instead of buying a single solution for each issue, businesses must trust security solutions from best-of-breed vendors and partnerships that answer a number of security needs. Why have 12 solutions when you can have three? In 2017, your security footprint will get smaller, but will be much more powerful.

9. The threat of ransomware grows. Ransomware was one of the fastest growing online threats in 2016, and it will become more serious and more frequent in 2017. We've seen businesses and individuals pay thousands of dollars to free their data from the grip of threat actors. The growth of ransomware means we must be more diligent to protect against it by not clicking on anything suspicious. Remember: if it sounds too good to be true, it probably is.

10. Security teams are 24/7. The days of security teams working 9-to-5 are long gone. Now is the dawn of the 24/7 security team. As more security solutions become services-based, consumers and businesses will demand the security teams and their vendors be available around the clock. While monitoring tools do some of the work, threats don't stop just because it's midnight, and security teams need to be ready to do battle all day, every day. Those are 10 things we see happening in the cyber security space next year.

Fars News Agency
Iran's Ground Force Unveils New Drone during Massive Drills
Tuesday, 13 December 2016

Tehran - The Iranian Ground Force unveiled a new drone named 'Farpad' during the massive wargames codenamed 'Mohammad Rasoulallah (PBUH) 4' in the Southeastern parts of the country on Monday morning. The hand- launched drone is run by autopilot and can fly maximum 45 minutes to the range of 20km.
Also during the second day of the three-day drills, the Iranian Ground Force unveiled a jamming system which is capable of confronting Unmanned Aerial Vehicles (UAVs) in a range of 3km and can force it to land after taking its control. The system is also portable by individuals.

In another development in the wargames, the home-made Toufan missiles whose range and destruction and precision-striking power have been improved were fired by helicopters and hit simulated enemy's targets precisely.

Also, the latest sniper gun manufactured for the Iranian Ground Force, 'Taher', with a range of 1.2km was unveiled on Monday. The gun weighs 4.4kg (without scope and magazine) and is 1.28m in length.

Meantime, the 209 (Cobra) and 214 helicopters of the Iranian Ground Force's air force units fired several rockets at two floating targets in Makran region (in the Sea of Oman) and destroyed them.

Also, two Mirage fighter jets of the Iranian Air Force participated in the drills for the first time and used air-based weapons in operations against the simulated enemy.

The massive 'Mohammad Rasoulallah (PBUH) 4' wargames started in the Southeastern parts of the country on Sunday morning.

"On the first day of the drills, rapid reaction units from other geographical regions of the country were transferred to the operational regions via air and ground in the shortest possible time," Spokesman of the drills General Seyed Kamal Payambari told reporters yesterday.

He said that the drills are being held in the strategic Southeastern parts of the country in a range of over 220,000km with the participation of different units of Ground Force, logistic forces of the Air Force and Khatam ol-Anbia Air Defense Base.

According to General Payambari, assessment of the Iranian forces' preparedness in the tactical fields and decreasing the time for their rapid reaction against threats as well as using new defense systems are among the goals pursued in the wargames.

Meantime, Army Airborne Commander Brigadier-General Houshang Yari announced on Sunday that dozens of different types of helicopters are flying over the wargames zone.

"Tens of different types of 206, 214, 209 (Cobra) and Chinook helicopters are present in the drills zone," General Yari told reporters today.

"During the drills, the command, track, control and close fire support missions as well as numerous heliborne operations will be carried out by the Airborne helicopters," he added.

General Yari said that the drills will also be a touchstone to assess the agility and power to overhaul and maintain helicopters.

Fars News Agency
Civil Defense Official Warns of New US Cyber Attack against Iran
Tuesday, 13 December 2016

Tehran - A senior member of Iran's Civil Defense Organization warned that Washington has hatched plots to launch new cyber operations against the country's infrastructures.
"At present, the US has launched a project named Nitro Zeus with the aim of attacking Iran's defense and telecommunication infrastructures," Alireza Karimi said on Monday, addressing a conference in Tehran.

"Based on studies that we have carried out, the project is assessed to be much more dangerous than the Stuxnet project," he added.

His remarks came after Deputy Head of Iran's Civil Defense Organization Brigadier General Mohammad Hassan Mansourian underlined in October his organization's full preparedness to confront the cyberattack and cultural invasion threats.

"Iran's Civil Defense Organization can defuse cyberattacks and cultural invasions," Brigadier General Mansourian said. He underlined that the advanced countries are currently making huge investments in the field of civil defense.

Mansourian underscored that the cyberattack and cultural invasion should only be responded by the national civil defense system.

In May 2015, Head of Iran's Civil Defense Organization Brigadier General Gholamreza Jalali announced that the country has set up cyber defense workgroups to better coordinate measures for defending nuclear facilities against enemies' cyber attacks.

"The country's vital cyber infrastructures have been identified and separate cyber workgroups have been formed in all fields," Jalali told reporters in Tehran.

"For instance a cyber defense workgroup was set up in the nuclear field for Natanz nuclear installations and no serious incident has threatened this section in the past two years," he added.

In relevant remarks in October 2014, Jalali revealed that a US cyberattack on Iran's nuclear enrichment facility in Natanz failed due to his organization's tough defensive measures.

"The first cyberattack, codenamed Olympic Games, was carried out on Natanz and was declared by the US President, but it met our heavy (defensive) response," Jalali told reporters in a press conference in Tehran.

The senior commander said the US changed its cyber commander following the failure in the cyberattack on Natanz, adding that the US general was forced to retire several months ago "due to the wrong information and data that he had presented to President Obama". And this was the result of our direct confrontation with them, General Jalali added.

The US was the principal player in the most sophisticated cyber-attack ever known and has been orchestrating a campaign against Iran designed to undermine the country's nuclear program.

The New York Times came up with an in-depth report on June 1, 2012 saying that from the very first month Barack Obama took over as US President, he secretly ordered increasingly sophisticated attacks on Iran's computer systems that run the country's main nuclear enrichment facilities.

The disclosures about Obama's role in the cyberwar against Iran appear to show beyond doubt that the US, with the help of Israel, was behind the Stuxnet virus attack on Iran's centrifuge machines - used to enrich uranium. The revelation then indicated that Washington and Tel Aviv were also behind the Flamer and Duqu virus attacks discovered by experts in May 2012.

Codenamed Olympic Games, the attacks were spearheaded by the US government under the Bush administration. Stuxnet targeted Siemens industrial equipment to spin hundreds of centrifuges beyond their breaking points and eventually disable Iran's nuclear efforts.

According to the report, Obama decided to speed up the attacks, even after the worm escaped from Iran's Natanz plant in 2010 and later ended up on the Internet.

During a meeting following the worm's escape, Obama even considered that the worm should be stopped thinking that America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised. Should we shut this thing down? Obama asked members of the President's national security team.

However, he finally decided to go ahead with the cyberattacks. What followed thereafter was the Natanz plant being hit by several newer versions of the worm.

The report is said to be based on 18 months of interviews with current and former American, European and Israeli officials involved in the program as well as with outside experts, who provided contradictory assessments of how successful the attack was in slowing down Iran's progress of developing nuclear weapons.

While internal Obama administration estimates claim the effort was delayed by 18 months to two years, some other experts, both inside and outside the government, said that Iran's enrichment levels had steadily recovered. A year later, Iran enriched uranium to the 20-percent grade, way beyond the 5-percent purity level that was done in Natanz in 2012.

Le Télégramme
Cybersécurité. La Bretagne au coeur du combat
Tuesday, 13 December 2016
Byline: Journaliste maison

Bruz, France - Jean-Yves Le Drian, ministre de la Défense, a dévoilé au centre DGA Maîtrise de l'information à Bruz (35), près de Rennes, la doctrine des armées en matière de cybersécurité. « L'émergence d'un nouveau milieu, d'un champ de bataille cyber, doit nous amener à repenser profondément notre manière d'aborder l'art de la guerre (...), comme l'aviation au début du XXe siècle », a-t-il assuré, soulignant : « En temps de guerre, l'arme cyber pourra être la réponse, ou une partie de la réponse, à une agression armée, qu'elle soit de nature cyber ou non ». La doctrine présentée ce lundi, qui repose sur trois piliers - renseignement, protection/défense et lutte informatique offensive - est l'une des plus élaborées énoncées en Europe, avec celle du Royaume-Uni. Concrètement, la France pourra recourir au combat numérique comme à une arme classique de type missile pour riposter à une attaque, aussi bien cyber que conventionnelle. « Nos capacités cyber offensives doivent nous permettre de nous introduire dans les systèmes ou les réseaux de nos ennemis, afin d'y causer des dommages, des interruptions de service ou des neutralisations temporaires ou définitives », a relevé le ministre.

Un bataillon de 2.600 « combattants numériques »

Un commandement des opérations cyber, placé sous la responsabilité directe du chef d'État-Major des armées, va être créé, dès janvier 2017. Il disposera d'un état-major resserré qui supervisera 2.600 « combattants numériques » . Les armées pourront « neutraliser » des infrastructures utilisées pour attaquer des intérêts français mais aussi « riposter » plus largement à une attaque cyber, a expliqué Jean-Yves Le Drian.

« Si une attaque cyber s'apparente à un acte de guerre, une riposte adéquate s'imposera (...) dans une logique de conflit ouvert », a-t-il souligné. Si l'attaque transite par un État qui « n'aurait pas empêché une telle utilisation, la responsabilité de cet État pourrait être mise en jeu », a-t-il averti.

Le Monde
Un an après sa création, la commission chargée du contrôle du renseignement
Tuesday, 13 December 2016
Byline: Jacques Follorou

Paris - Un an après sa création, la commission chargée du contrôle du renseignement affirme son indépendance
L'avis de la Commission nationale de contrôle des techniques de renseignement, née en octobre 2015 pour faire contrepoids aux puissants moyens de surveillance accordés aux services secrets, n'est que consultatif mais le premier ministre l'a suivi dans la plupart des cas.

Pour son premier rapport annuel, présenté mardi 13décembre, la Commission nationale de contrôle des techniques de renseignement (CNCTR), née, le 3octobre 2015, pour faire contrepoids aux puissants moyens de surveillance accordés aux services secrets français dans la loi du 24juillet 2015 sur le renseignement, jouait une part de sa crédibilité.

Nommé président de cette nouvelle instance indépendante, Francis Delon, ex-secrétaire général de la défense nationale et l'un des pères fondateurs de la plateforme nationale du renseignement technique qui alimente depuis 2008 la communauté française du renseignement, devait prouver que les premiers soupçons de grande proximité avec l'Etat étaient infondés. Il devait, de plus, montrer que dans une période où l'émotion pèse sur les décisions politiques, il saurait résister aux pressions l'invitant à ne pas s'opposer aux libertés prises avec le droit.

La CNCTR est chargée de contrôler de l'utilisation d'une douzaine de moyens de surveillance par les services de renseignement français. L'avis de la CNCTR, composée de dix-sept membres, dont trois ingénieurs, n'est que consultatif. Le premier ministre, seule autorité décisionnaire en la matière, l'a néanmoins suivi dans la plupart des cas. La procédure dite d'urgence, qui permet de s'exonérer du point de vue de la CNCTR, n'a été déclenchée qu'à une reprise selon le rapport qui ne fournit aucun détail opérationnel.

8538 interceptions de sécurité validées

En un an, la CNCTR a visé 48208 demandes de collecte de données de connexion, qui portent parfois sur de simples recherches de numéros dans des annuaires. Elle a donné un avis favorable à 2127 demandes de géolocalisation et elle a validé 8538 interceptions de sécurité, des écoutes téléphoniques, alors que l'instance qui existait auparavant, la Commission nationale de contrôle des interceptions de sécurité (CNCIS), née de la loi de 1991, en avait contrôlé un peu plus de 7000 lors de sa dernière année.

La CNCTR reste très discrète sur les 7711 fois où «d'autres techniques» ont été déployées avec son aval. S'agissait-il de pose de balises, de sonorisation d'appartements, de recueil ou de collecte de données informatiques? On n'en saura rien. La CNCTR explique qu'elle est tenue par la loi qui lui interdit de révéler des capacités opérationnelles. Elle signale néanmoins que faute d'achèvement du chantier de «centralisation des données recueillies» par ces nouvelles techniques, elle n'a pas encore une vision sur leur utilisation sur tout le territoire.

6,9% des demandes renvoyées aux services

En matière d'avis défavorables, on note une augmentation par rapport au temps de la CNCIS qui ne donnait son avis que sur les interceptions de sécurité et les données de connexions. La CNCTR a renvoyé aux services 6,9% des demandes contre environ 1% à l'époque de la CNCIS. Avant la loi de juillet2015, les services de renseignement usaient d'un grand nombre de ces moyens intrusifs, balises, sonorisation de lieux, etc. sans demander l'autorisation à quiconque, en toute illégalité. Les avis défavorables de la CNCTR portent essentiellement sur ces outils, désormais légaux, mais particulièrement attentatoires à la vie privée.

Si la CNCTR s'est vue, de fait, reprocher par les services un surcroît de «paperasse», elle a surtout pu éprouver la réalité de son indépendance lors des tentatives du gouvernement de passer outre ses prérogatives. Ce fut ainsi le cas avec l'article851-2 sur le recueil de données de connexions en temps réel attachées à une personne sur l'ensemble de ses moyens de communication.

La loi sur le renseignement du 24juillet 2015 disposait que cette collecte ne pouvait être effectuée que «sur une personne préalablement identifiée comme présentant une menace» . Le gouvernement et le chef de l'Etat ont tenté, en janvier, d'utiliser ce moyen pour mettre sous surveillance des listes entières de suspects, notamment les fameux fichés «S» pour islam radical, soit près de 14000 personnes. M.Delon a bloqué cette requête considérant qu'elle n'est pas conforme à la loi qui impose que chaque demande doit être individualisée et justifiée.

Pour contourner ce refus de valider «des surveillances groupées et simplifiées», le gouvernement, soutenu par un législateur, davantage soucieux d'étendre la surveillance d'Etat que de jouer son rôle de contre-pouvoir, a, depuis, modifié à deux reprises le périmètre de cet article de loi. Dans le cadre des lois sur la prorogation de l'Etat d'urgence, le Parlement a d'abord élargi la surveillance aux personnes «pouvant constituer une menace» . Et fin juillet, il a étendu la collecte de données de connexion en temps réel à l'entourage de la personne surveillée dès lors qu'il existait simplement «des raisons

sérieuses de penser» qu'espionner ces gens au sein de cercles familiaux, amicaux, professionnels ou occasionnels puisse avoir un intérêt.

L'«exception hertzienne»

Si les parlementaires n'ont pas été d'une grande aide pour la CNCTR, elle a, en revanche, trouvé dans le Conseil constitutionnel un soutien inattendu pour tenter d'étendre son contrôle sur un pan entier des surveillances en France qui restaient jusque-là interdites, les communications hertziennes. Qualifiée d' «exception hertzienne» par la CNCTR, cette dérogation du droit consacrée par la loi de 1991 sur les interceptions puis prorogée dans la loi de juillet de 2015, a pris fin lors de sa censure, le 21octobre, par le Conseil constitutionnel.

Se félicitant de la décision du Conseil de vouloir faire entrer la surveillance par voie hertzienne dans le droit commun et d'avoir été chargée par lui de veiller à son application d'ici au vote d'une nouvelle loi, au plus tard le 31décembre 2017, la CNCTR a, au moins jusqu'à cette date, le pouvoir de viser chaque demande d'interceptions effectuée par cette technique. Souhaitant poursuivre son avantage, la CNCTR demande, dans son rapport, d'être «consultée sur l'éventuelle nouvelle législation» .

Le Temps (Suisse)
ID Quantique se déploie à l'international
Tuesday, 13 December 2016
Byline: Dejan Nikolic

Londres - Le numéro un mondial de la cryptographie quantique et de la génération de nombres aléatoires ouvre un bureau à Londres, signe un partenariat stratégique avec le géant coréen SK Telecom et s'attaque au marché chinois
ID Quantique (IDQ), pépite issue des laboratoires de physique appliquée de l'Université de Genève, s'offre un déploiement sans précédent. L'actuel numéro un mondial de la cryptographie quantique et de la génération de nombres aléatoires étend tout d'abord ses activités à la Grande-Bretagne. A travers notamment un contrat consistant à sécuriser les échanges d'informations entre l'un des sites de BT (anciennement British Telecommunications) et Cambridge.

IDQ ouvre également une officine britannique, afin de prendre part à une plateforme scientifique nationale de 384 millions de francs sur cinq ans. « Huit grandes universités du pays ainsi que le secteur privé et public participent à ce programme », précise Grégoire Ribordy, fondateur d'IDQ, qui imagine affecter cinq collaborateurs à Londres d'ici à un an.

Parallèlement à cette nouvelle tête de pont britannique, IDQ signe une alliance avec SK Telecom, le principal opérateur de Corée du Sud (29,45 millions de clients, soit environ 50% du marché local, pour près de 15 milliards de francs de chiffre d'affaires l'an passé). Ce rapprochement avec la major de l'un des pays les plus connectés de la planète est assorti d'une levée de fonds de plus de 4 millions de francs.

Soit la troisième injection de capital en quinze ans, les deux précédentes rondes ayant permis d'engranger respectivement un million (2004) et quatre millions (2014).

La fibre commerciale

L'entreprise carougeoise, lancée en 2001 et qui affiche une croissance moyenne de 30% par an, emploie aujourd'hui une cinquantaine de salariés, soit plus du double qu'en 2014. Son dernier tour de financement, auquel participent d'autres investisseurs stratégiques, est destiné à renforcer sa suprématie à l'échelle planétaire. Et d'asseoir son développement en Asie.

« L'une des filiales de SK Telecom fabrique des puces pour smartphones intégrant des nombres aléatoires, relève Grégoire Ribordy. Ce dispositif bon marché, qui permet de réduire la vulnérabilité des appareils, est en passe de révolutionner le monde de la téléphonie mobile. » Un boîtier traditionnel, de taille standard, coûte environ 1000 francs. Avec la technologie sud-coréenne embarquée, générer des clés ou des mots de passe exclusifs coûtera jusqu'à 100 fois moins cher.

Promesses quinquennales

Dans la foulée, IDQ inaugure son entrée sur le marché chinois. Via une coentreprise avec China Quantum Technologies (CQT), une société pionnière dans les technologies quantiques, à l'origine du plus important réseau commercial en la matière. Soit entre les villes de Shanghai et de Hangzhou, un tronçon de communication ultra-sécurisé d'environ 200 km. « Les contrats ont été signés il y a un mois », se félicite Grégoire Ribordy, sur le point d'ouvrir avec son partenaire chinois une usine dans la province du Zhejiang.

Le nouveau site de production, appelé à fonctionner avant fin 2017 avec un effectif de 50 collaborateurs, doit notamment permettre à CQT d'accéder au savoirfaire genevois en participant à la fabrication notamment de produits d'appel destinés aux casinos et aux paris en ligne. En échange de quoi, IDQ se voit offrir une porte d'entrée sur le potentiel commercial chinois.

La cryptographie quantique est l'un des cinq axes du 13e plan quinquennal de Pékin, définis comme étant d'importance stratégique cruciale pour la nation. Le prix d'un appareil de cryptage, qui c oûte actue llement 50 000 francs pièce, « sera divisé par dix grâce aux volumes du marché chinois », estime Grégoire Ribordy.

Toutefois, les spécialistes se heurtent pour l'heure à un obstacle technique de poids: par voie terrestre, le système ne fonctionne que de point à point, jusqu'à cent kilomètres au maximum. Au-delà, trop de photons sont perdus par diffusion en raison des imperfections de la fibre. Il faut alors aménager des noeuds intermédiaires pour que la particule qui compose la lumière, et qui sert à envoyer les clés de chiffrement nécessaires au décodage de l'information, soit impossible à intercepter. Le maillage Shanghai-Hangzhou, qui garantit que toute tentative d'espionnage provoque l'autodestruction du signal, en compte par exemple cinq.

Mais la Chine rêve d'inaugurer, d'ici à 2030, un système d'échange de données inviolable à l'échelle mondiale. Pékin a ainsi lancé le 15 août dernier le premier satellite de communication indéchiffrable à longue distance (près de 2500 km). Seul hic: l'instrument en orbite doit être orienté de manière extrêmement précise vers les stations au sol. « Ce sera comme lancer une pièce de monnaie d'un avion volant à 100 km d'altitude et espérer qu'elle vienne se ficher exactement dans la fente d'une tirelire cochon en rotation », avait alors expliqué Wang Jianyu, le responsable en chef de cette percée technologique de Pékin.

Le Télégramme
Lannion. Nouvelle Breizh cyber valley
Tuesday, 13 December 2016
Byline: Journaliste maison

Lannion, France - Marie-Hélène Clam et Riwan Marhic Après Rennes et Bruz (35), la journée cybersécurité du ministre de la Défense, Jean-Yves Le Drian, s'est achevée sur le site de Nokia, à Lannion (22). Il s'y est vu confirmer la création de 500 emplois d'ingénieur Recherche et Développement d'ici à la fin 2018, dont une grande partie à Lannion, ciblée pôle mondial pour ce secteur.
« Lannion sera le centre mondial pour Nokia concernant la recherche en cybersécurité », a lancé Marc Rouanne, le numéro deux du groupe Nokia. Devant un Jean-Yves Le Drian acquis à la cause puisque lanceur du Pact Cybersécurité dès 2012, le dirigeant a confirmé le recrutement de 500 ingénieurs Recherche et Développement dont 300 jeunes diplômés. À lui seul, le site de Lannion accueillera une centaine de ces ingénieurs amenés à travailler sur la 4G, la 5G, l'internet des objets et bien sûr la cybersécurité. « Nokia est aussi sponsor de la première formation informatique et cyberdéfense de l'École nationale supérieure d'ingénieurs de Bretagne-Sud (ENSIBS) à Vannes, aide au codéveloppement des start-up locales et des acteurs européens », a ajouté Arnaud Laforge, directeur du site.

Scanner le trafic pour détecter les espions

Une heure durant, le ministre a pu assister à des démonstrations : du chiffrement des données à la détection des espions, appliqués aux domaines militaire et civil. « Les pare-feu, qui servent à se protéger des intrusions extérieures par internet, sont inutiles car plus d'un million d'appareils sont déjà infectés, a expliqué Giuseppe Targia, directeur de la sécurité chez Nokia. Certains pirates peuvent déjà avoir accès à nos machines. Notre solution basée sur la reflectométrie permet de vérifier en continu s'il y a des irrégularités au sein de notre réseau, juste en observant le comportement de nos appareils ».Adopté par la Banque de France, ce système permet de scanner le trafic automatiquement et de détecter des pertes de données dues à un réseau vieillissant ou à une interception des données, donc à de l'espionnage. Espionnage rendu possible grâce à des dispositifs coûtant moins de 10 achetés sur internet, que les pirates placent dans les boîtiers de fibre optique. Pour s'en protéger, l'équipementier développe un nouveau type de boîtier sécurisé qui sera opérationnel, fin 2017. Autre innovation, le réseau ultra-compact. Ce gros sac à dos permet d'établir des communications fiables en quelques minutes, n'importe

où dans le monde. Déjà utilisé par les Marines américains, il peut être fixé à un drone ou à un ballon et bénéficie d'une couverture téléphonique et internet à 70 km à la ronde. En plus de son usage militaire, il sera mis à disposition des ONG ou des pompiers en cas de catastrophe naturelle.

« Comme des anticorps »

« La meilleure défense que nous connaissions, c'est le système immunitaire humain. Alors on s'en est inspiré pour notre cybersécurité : quand il y a un problème, le réseau réagit vite et apprend de ce problème pour s'en prémunir à l'avenir, comme des anticorps », résume Giuseppe Targia. Des innovations qui ont impressionné Jean-Yves Le Drian. « C'est quasiment une cyber armée qui se met en place en Bretagne. Dans le contexte de menace terroriste et avec 50 milliards d'objets connectés d'ici à 2025, il s'agit pour la France de garder de l'avance pour préserver son leadership sur ce domaine. Et Lannion en sera une Breizh cyber valley ».

Le Figaro
Le Conseil national du numérique hausse le ton face au fichier TES
Tuesday, 13 December 2016
Byline: Elisa Braun

Paris - Le fichage des Français au sein d'une base de données unique inquiète l'organe indépendant Non, c'est non. Le Conseil national du numérique (CNNum) reste intransigeant sur le fichier TES, qui permet au gouvernement de regrouper les données personnelles (sexe, couleur des yeux, taille, photo, empreintes digitales, filiation, nationalité...) de près de 60 millions de Français. Le CNNum en avait déjà demandé la suspension le 7 novembre dernier dans une lettre ouverte au gouvernement, où il déplorait les risques de dérives créées par un tel dispositif.

La nouvelle prise de position du CNNum publiée lundi et qui résulte des contributions recueillies par sa plateforme de consultation et d'auditions d'experts, est encore moins tendre avec le gouvernement. Outre la demande réitérée de suspension du fichier, le Conseil préconise dans son rapport l'instauration d'un débat public sur les sujets de l'identité administrative et l'identité en ligne. Il insiste également sur l'«urgence à instaurer une nouvelle gouvernance des choix technologiques au sein de l'État».

Un contre-exemple symptomatique

Au-delà de la polémique, le fichier TES apparaît selon le CNNum comme «le symptôme d'un processus décisionnel qui, en matière technologique, n'intègre pas suffisamment les exigences d'une vision politique de long terme». Au fil des pages du rapport, le Conseil mentionne les nombreux risques de dérives que constitue un tel fichier dans un contexte d'attaques cybersécuritaries accrues. Il recommande d'édicter un cadre général pour ce type de décision, et suggère notamment l'obligation de fournir des études d'impact approfondies et de tenir des débats publics.

L'organe consultatif recommande de renforcerle rôle d'instances spécialisées comme la Commission nationale informatique et libertés (Cnil), la direction interministérielle du numérique et du système d'information et de communication de l'État (Dinsic) et de l'agence nationale de la sécurité des systèmes d'information, l'Anssi.

Une querelle sans fin

Le fichage des Français a rouvert les fractures créées par le projet de loi sur le Renseignement, l'an dernier. Si le fichier TES est censé simplifier les formalités d'obtention et de renouvellement des titres d'identité, ainsi qu'éviter la fraude documentaire, certains opposants ont dénoncé son caractère attentatoire à la vie privée. Dans un contexte d'État d'urgence prolongé et de mesures prises contre le terrorisme, ce fichier TES a aussi été critiqué pour sa potentielle utilisation à des fins de renseignement.

Bernard Cazeneuve - alors ministre de l'Intérieur et à l'initiative du décret - a écarté cette possibilité devant la commission des Lois de l'Assemblée, le 9 novembre. Il n'a en revanche pas su lever les doutes de certains parlementaires, concernant les risques de sécurité liés à la concentration en un même fichier d'autant de données sensibles. Le ministère de l'Intérieur a consenti à rendre optionnel le versement des empreintes biométriques dans la base de données. Le ministère a également saisi la Dinsic (Direction interministérielle du numérique et du système d'information et de communication de l'État) et de l'Anssi (Agence nationale de la sécurité des systèmes d'information) afin d'évaluer le risque d'attaque informatique.

Lors d'une récente audition à la commission des lois du Sénat, les dirigeants de ces deux institutions n'ont pas fait mystère de leur intention d'amender le projet de l'Intérieur. Guillaume Poupard, directeur de l'ANSSI, s'est inquiété des risques géopolitiques: «Que se passerait-il si quelqu'un voulait déstabiliser la France non pas via une attaque très visible, mais en distillant des erreurs de-ci, de-là au sein du fichier?», rappelant que «ce genre d'armes est de plus en plus utilisé dans le cadre de conflits avoués ou pas entre grands États». «Je crois qu'il faut remettre à plat tout cela pour que le débat puisse reprendre sur des fondamentaux plus solides», a plaidé Henri Verdier, directeur du Dinsic. À la différence des deux instances, le CNNum, qui souhaite pour sa part repenser intégralement le fichier TES, reste pour sa part un organe purement consultatif.

La Tribune (France)
Surveillance spatiale : la France reste dans la cour des Etats- Unis et de la Russie
Tuesday, 13 December 2016
Byline: Michel Cabirol

Paris - La direction générale de l'armement a notifié le contrat de modernisation du système de surveillance de l'espace Graves à l'ONERA et à la PME Degreane Horizon. Un enjeu crucial pour la France qui peut ainsi suivre dans l'espace les satellites espions.

Le ministère de la Défense lance la modernisation du système de surveillance de l'espace Graves comme l'avait annoncé La Tribune (lien : http://www.latribune.fr/entreprises- finance/industrie/aeronautique-defense/surveillance-spatiale-la-france- modernise-le-systeme-graves-a-minima-602219.html). La direction générale de l'armement (DGA) a notifié un contrat pouvant s'élever jusqu'à 40 millions d'euros, qui comprend une tranche ferme et des tranches optionnelles, à deux cocontractants : le centre français de la recherche aéronautique spatiale et de défense l'ONERA et la PME électronique Degreane Horizon, spécialisée dans l'acquisition et l'émission de données sensibles. Cette filiale du groupe Vinci était depuis 2003 un des fournisseurs du centre de recherche français sur ce programme. La DGA a toutefois confié à l'ONERA la responsabilité du maintien des performances du système puis de son amélioration.

La tranche ferme de ce programme de rénovation court sur une période de cinq ans (huit ans si on rajoute toutes les tranches optionnelles). Elle représente plus de la moitié de la valeur du contrat, selon le chef de projet du système Graves au sein de l'ONERA, Florent Muller. Le système Graves est essentiellement installé sur trois sites, l'un à Dijon (le site d'émission avec les grande antennes), un autre sur le plateau d'Albion (site de réception) et, enfin, à Lyon Mont-Verdun, où le centre opérationnel de surveillance militaire des objets spatiaux (COSMOS), traite les données du système Graves (exploitation).

Graves, un système de renseignement stratégique

Mis en service depuis 2005 pour le compte de l'armée de l'air, le système Graves (pour Grand Réseau Adapté à VEille Spatiale) est un programme unique en Europe. Seuls les États-Unis et la Russie ont officiellement un programme équivalent alors qu'un cercle très restreint de pays, comme la Chine par exemple, pourraient en posséder un également. A ce jour, il est capable "de cataloguer des objets de la gamme du mini-satellite jusqu'à 1.000 km d'altitude", souligne Florent Muller. Soit un engin de la taille d'une machine à laver.

"Les données générées permettent de calculer à tout instant la position de l'ensemble des satellites suivis", précise-t-il. Actuellement, Graves détecte et catalogue tous les jours plus de 2.500 objets. C'est l'armée de l'air qui assure la mise à jour quotidienne du catalogue. Car pour rester catalogué, un objet doit être détecté tous les jours.

« La France a été le troisième pays au monde, après les Américains et les Russes, à se doter d'un tel système, avait expliqué en juin 2015 dans une interview accordée à la Tribune le PDG de l'ONERA, Bruno Sainjon. L'ONERA a conçu Graves, a piloté sa réalisation et l'a transféré à l'armée de l'air en 2005. Ce programme a notamment permis des échanges de données avec les États-Unis. Et, en avril 2015, cette coopération s'est renforcée, les deux ministères de la Défense voulant désormais échanger des informations classifiées". »

Ce système de renseignement militaire stratégique, un outil extrêmement précieux pour la France, peut notamment suivre à une altitude de moins de 1.000 kilomètres les satellites espions, qui survolent la France et observent les sites sensibles. Ce qui permet à l'armée de l'air de cataloguer pratiquement tous

les satellites espions alliés et ennemis ainsi que d'autres engins spatiaux. "Graves permet de détecter les menaces qui pèsent sur nos propres moyens spatiaux", confirme Florent Muller.

L'armée de l'air a d'ailleurs reconnu avoir identifié en 2012, puis 2013 et, enfin, en 2015, des engins spatiaux qui se sont approchés de satellites militaires français. Ces satellites sont d'ailleurs restés à leur contact pendant une période relativement longue. Très certainement pour les écouter. Il détecte également les vols en formation de satellites. En outre, Graves permet d'éviter d'éventuelles collisions entre des débris spatiaux et les satellites français en les déplaçant le cas échéant.

Enfin, le système concourt à la protection des populations face aux rentrées atmosphériques à risques (engins spatiaux, comètes...). Car plus de 12.000 satellites artificiels et objets divers, dont la taille est supérieure à dix centimètres, orbitent autour de la Terre.

Graves pourrait identifier des micro-satellites

Malgré sa robustesse et sa simplicité, le système Graves, un prototype qui était innovant en 2005, doit être aujourd'hui modernisé, les équipements ayant vieilli. Cette opération de rénovation permettra désormais d'assurer la pérennité de Graves "jusqu'en 2030", estime Florent Muller. Dans ce contexte, la tranche ferme du contrat confié à l'ONERA et à Degreane Horizon comprend en grande partie le traitement des obsolescences du système ainsi que quelques améliorations de ses performances, notamment du calculateur de traitement de signal.

« Certaines performances seront accrues grâce notamment à des interventions au niveau des antennes de réception et du traitement du signal, supportées par un nouveau calculateur", explique l'ONERA dans son communiqué. »

Plus précisément, l'ONERA sera en charge de la rénovation et des améliorations des sites de réception et d'exploitation. La filiale de Vinci modernisera pour sa part à l'identique les systèmes d'émissions en gérant les obsolescences.

Avec les tranches conditionnelles, de nouvelles améliorations du système sont prévues. En parallèle du lancement de la tranche ferme, l'ONERA effectuera des études techniques opérationnelles pour définir quelles pourraient être les options pour améliorer Graves. "A l'issue de ces études, un certain nombre d'options accessibles pourra être ainsi notifié en parallèle de la tranche ferme", confirme Florent Muller.

L'ONERA vise notamment l'amélioration de l'observation d'objets spatiaux plus petits. Et de passer "de façon progressive avec les options les plus complètes" de la détection de mini-satellites (inférieur à 500 kg) à celles de micro-satellites (inférieur à 150 kg). Dans sa nouvelle configuration, Graves détectera beaucoup plus d'objets spatiaux qu'actuellement si les tranches conditionnelles du contrat sont levées.

Un outil de souveraineté

Entre une modernisation a minima et une modernisation plus ambitieuse, le ministère de la Défense n'a pas encore tout à fait tranché en découpant le programme de modernisation de Graves en plusieurs tranches, dont des tranches optionnelles. Cet outil de souveraineté permet pourtant de discuter d'égal à égal - ou presque - avec les États-Unis. Ce qui n'est pas rien et confirme bien que la France est depuis 2005 dans le club très fermé des puissances dotées de capacités autonomes de surveillance de l'espace. Au ministère de la Défense de décider de l'ampleur de cette opération cruciale pour l'indépendance de la France en matière de surveillance spatiale une fois les recommandations de l'ONERA émises.

Développé sous contrat de la DGA, le système Graves est constitué d'un radar bistatique spécifique associé à un système de traitement automatisé qui permet la création et le maintien à jour d'une base de données des paramètres orbitaux des satellites qu'il détecte. Fruit de la collaboration des spécialistes des départements Électromagnétisme et radar (DEMR) et Conception et évaluation des performances des systèmes (DCPS) de l'ONERA, le radar du système Graves a été spécifiquement conçu pour la surveillance de l'espace.

Le Petit Bleu de Lot-et-Garonne
Cybersécurité : la France muscle son arsenal
Tuesday, 13 December 2016
Byline: Journaliste maison

Paris - Le combat numérique va devenir une arme à part entière des armées françaises, aussi bien offensive que défensive, face à une cybermenace qui vise de plus en plus les intérêts vitaux des États. «L'émergence d'un nouveau milieu, d'un champ de bataille cyber, doit nous amener à repenser profondément notre manière d'aborder l'art de la guerre», a déclaré hier le ministre de la Défense Jean-Yves Le Drian, en dévoilant la doctrine des armées françaises en matière de cybersécurité.

Dans un monde de plus en plus interconnecté, les cyberattaques venant d'États, hackers, groupes terroristes ou criminels se multiplient, a relevé le ministre.

Elles peuvent paralyser des infrastructures vitales (réseaux téléphoniques, centrales électriques, transport..) tout comme des cibles militaires en tentant de pénétrer les systèmes embarqués d'aéronefs, bâtiments de guerre ou blindés.

«L'arme cyber peut avoir des effets tout à fait comparables à l'armement plus conventionnel», a averti Jean-Yves Le Drian en inaugurant les nouveaux locaux de DGA Maîtrise de l'information, qui réunit les cyberexperts de la Défense à Bruz (Ile-et-Vilaine) près de Rennes.

Face à ces menaces, les armées verrouillent de plus en plus leurs systèmes d'information - ils sont protégés par des «murailles» et des «patrouilles» qui traquent les intrus - mais intègrent aussi désormais le cyber comme une arme offensive.

«En temps de guerre, l'arme cyber pourra être la réponse, ou une partie de la réponse, à une agression armée, qu'elle soit de nature cyber ou non», a énoncé M. Le Drian.

Concrètement, la France pourra recourir au combat numérique comme à une arme classique de type missile pour riposter à une attaque aussi bien cyber que conventionnelle.

Un commandement des opérations cyber, le CYBERCOM, placé sous la responsabilité directe du chef d'état-major des armées, va être pour cela créé en janvier 2017.

Il disposera d'un état- major resserré qui surpervisera 2.600 «combattants numériques» d'ici 2019.

Le Figaro
20.282 personnes espionnées en un an sur le territoire français
Tuesday, 13 December 2016
Byline: Christophe Cornevin

Paris - Dans son premier rapport d'activité dévoilé mardi matin, la Commission nationale de contrôle des techniques de renseignement (CNCTR) évalue que 47% des personnes surveillées l'ont été dans des dossiers terroristes et 29% au titre de la «lutte contre la criminalité organisée» ainsi que de la «prévention des violences collectives».
Entre le 3 octobre 2015 et le 2 octobre dernier, quelque 20.282 personnes ont été espionnées par les services français. En dévoilant mardi matin son premier rapport d'activité, la Commission nationale de contrôle des techniques de renseignement (CNCTR) a évalué le nombre d'hommes et de femmes qui ont fait l'objet d'une surveillance. Celle-ci passe par l'emploi de la technique la moins intrusive, à savoir l'obtention des «fadettes» (facturations détaillées) de la personne ciblée jusqu'à des moyens plus lourds, telles que la sonorisation ou l'installation de moyens vidéo dans les domiciles en passant par les interceptions de sécurité, la géolocalisation, l'accès en temps réel aux données de connexion» ou encore l'emploi - encore parcimonieux - des «Imsi catchers» permettant de siphonner à distance les données de connexion des téléphones mobiles.

Les algorithmes, c'est-à-dire la «boite noire», tant contestée censée assurer un recueil massif de données, ne devraient être mis en ouvre qu'au printemps prochain. «Pour l'heure, ils n'ont pas pu être mis en place pour des raisons de moyens techniques», précise-t-on à la CNCTR.

47% dans les radars de l'antiterrorisme

Au nombre de ceux ayant «fait l'objet d'une technique de renseignement au moins», le rapport de la CNCTR révèle que «9624 personnes, soit 47% du total, ont été surveillées au titre de la prévention du terrorisme» et que 5848 autres, soit 29% du total, ont été ciblées dans des dossiers de lutte contre la criminalité organisée ainsi que «la prévention de violences collectives de nature à porter gravement atteinte à la paix publique».

La CNCTR, qui se dit «particulièrement vigilante sur ce point», considère que «cette finalité ne saurait être interprétée comme permettant la pénétration d'un milieu syndical ou politique ou la limitation du droit constitutionnel de manifester ses opinions, y compris extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré.» Nombre d'observateurs y ont vu une disposition visant les zadistes mais aussi les no-borders, les blacks blocks ou encore les hooligans.

Les autres 24% de personnes placées dans les radars des services, qu'ils soient Français ou étrangers, ont été soupçonnés de porter atteinte à «l'indépendance nationale, l'intégrité du territoire et la défense nationale», d'espionnage industriel ou encore d'être liés à la «prolifération des armes de destructions massives».

8538 avis sur des demandes d'interceptions de sécurité

La démarche, tout à fait inédite dans le panorama feutré de l'espionnage, ne permet «aucun point de comparaison avec l'étranger», précise le conseiller d'État Francis Delon, président de la CNCTR qui, en aparté, ne se dit «pas particulièrement surpris» par le chiffre.

Cette instance indépendante, qui bénéficie d'un budget de 2,9 millions d'euros, vérifie la validité des techniques déployées de la DGSE, de la DGSI, de Tracfin ou encore de la Direction du renseignement militaire.

Depuis le 3 octobre 2015, la CNCTR a rendu 8538 avis sur des demandes d'interceptions de sécurité, contre 7703 l'année précédente. Le nombre des géolocalisations en temps réel a quant à lui bondi de 87% pour atteindre les 2127 demandes en 2016. Observant dans son rapport que «la prévention du terrorisme a, pour la première fois, été le fondement légal le plus fréquemment invoqué», la CNCTR ne constate cependant aucune explosion de la surveillance liée à la menace islamiste.

Composée de neuf «sages» - quatre hauts magistrats, quatre parlementaires et un expert en Télécoms - et d'une secrétaire de 17 personnes dont deux ingénieurs, elle s'est réunie de manière collégiale à 180 reprises à raison de trois fois par semaine pour examiner des cas individuels et mener des dossiers de fonds. Au terme des examens, la CNCTR a retoqué 6,9% des demandes.

New York Times
G.O.P. Feud Looms as Leaders Back Russia Inquiries
Tuesday, 13 December 2016
Byline: Jennifer Steinhauer

Washington - The top two Republicans in Congress said on Monday that they supported investigations into possible Russian cyberattacks to influence the American election, setting up a potential confrontation with President-elect Donald J. Trump in his first days in office.

"Any foreign breach of our cybersecurity measures is disturbing, and I strongly condemn any such efforts," said Senator Mitch McConnell, Republican of Kentucky and the majority leader, adding, "The Russians are not our friends."

Mr. McConnell's support for investigating American intelligence findings that Moscow intervened in the election on Mr. Trump's behalf could presage friction between the Republicans who control Congress, and who have long taken a hard line against Russia, and the president-elect, who has mocked the findings.

Mr. McConnell also went out of his way to address Mr. Trump's claim that the C.I.A. could not be trusted because of flawed intelligence before the Iraq war.

"Let me say that I have the highest confidence in the intelligence community," Mr. McConnell said, "and especially the Central Intelligence Agency. The C.I.A. is filled with selfless patriots, many of whom anonymously risk their lives for the American people."

The top Republican in the House, Speaker Paul D. Ryan of Wisconsin, said he supported a continuing investigation by Representative Devin Nunes of California, the chairman of the House Intelligence Committee. In a statement, Mr. Ryan said: "As I've said before, any foreign intervention in our elections is entirely unacceptable. And any intervention by Russia is especially problematic because, under President Putin, Russia has been an aggressor that consistently undermines American interests."

Congressional Republicans announced their support for inquiries after Mr. Trump railed for much of the weekend against the intelligence findings. But their remarks, especially Mr. Ryan's, were far from fiery, reflecting both a fear of offending Mr. Trump, who has taken many positions against traditional Republican orthodoxy, and the Republicans' belief that Democrats have selectively leaked intelligence information for political gain.

Critics from both parties are questioning Mr. Trump's apparent choice of Rex W. Tillerson, the chief executive of Exxon Mobil, as secretary of state, particularly because of his longstanding business connections with Russia and his close relationship with President Vladimir V. Putin, whom he has known for two decades. Mr. Trump said in a Twitter post on Monday night that he would make a formal announcement on the job on Tuesday morning.

Senators Lindsey Graham of South Carolina and Marco Rubio of Florida, both Republicans, have expressed concern about the reports of cyberattacks, as have numerous Democrats. But Mr. Rubio, in an apparent reference to Mr. Tillerson, went a step further on Monday, writing on Twitter, "Being a 'friend of Vladimir' is not an attribute I am hoping for from a #SecretaryOfState."

Mr. McConnell said the Senate investigation would be led by Senator Richard M. Burr, Republican of North Carolina, the chairman of the Intelligence Committee. Senator John McCain, Republican of

Arizona, the chairman of the Armed Services Committee, will add a subcommittee to look into cyberattacks, led by Mr. Graham.

"The first thing we want to establish is, 'Did the Russians hack into our political system?'" Mr. Graham said in an interview on Monday. "Then you work outward from there. I have a high degree of confidence Russia did this."

Mr. Nunes, a member of Mr. Trump's transition team, said in a statement that the Intelligence Committee had been "conducting vigorous oversight of the investigations into election-related cyberattacks."

Mr. Nunes also noted that his committee would be scrutinizing the review of the Russian effort to influence the election ordered last week by President Obama.

Democrats have used the latest intelligence findings to renew their calls for an urgent inquiry. John D. Podesta, Hillary Clinton's campaign chairman, demanded on Monday that all information about Russia's meddling be declassified, and that the Obama administration explain what it knows about the hacking and when it knew it.

"We now know that the C.I.A. has determined Russia's interference in our elections was for the purpose of electing Donald Trump," Mr. Podesta wrote in a statement. "This should distress every American. Never before in the history of our republic have we seen such an effort to undermine the bedrock of our democracy."

Three Senate Democrats -- Benjamin L. Cardin of Maryland, Dianne Feinstein of California and Patrick J. Leahy of Vermont -- called on Monday for the creation of an independent, nonpartisan commission to comprehensively investigate allegations of Russian interference in the 2016 election.

But Mr. McConnell stopped short of calling for a special select committee, saying that the Senate Intelligence Committee was "more than capable of conducting a complete review" of the matter.

While he stopped short of saying whether he agreed that Russia had interfered in the election in support of Mr. Trump, Mr. McConnell said, "We need to approach all these on the assumption the Russians do not wish us well."

Mr. McCain was less equivocal, saying Monday that there was "no doubt about the hacking" by Russian intelligence services. He called the hacking of the Democratic National Committee and related accounts "another form of warfare" in an appearance on "CBS This Morning" with Senator Chuck Schumer of New York, the incoming Democratic leader.

And one week before the Electoral College meets to ratify Mr. Trump's election victory, 10 electors have demanded their own intelligence briefing on Russian efforts to elect Mr. Trump.

For his part, Mr. Trump was dismissive of the intelligence findings and suggested that Democrats were simply stirring controversy. "Can you imagine if the election results were the opposite and WE tried to play the Russia/CIA card. It would be called conspiracy theory!" Mr. Trump said in a Twitter post on Monday.

The White House press secretary, Josh Earnest, said that the administration would support a congressional review. He also rejected the notion that the administration had failed to adequately highlight the Russian efforts before the election, saying it had extensively briefed Congress all year about Russian electoral meddling.

"There has been intensive cooperation between the intelligence community and other national security agencies, and members of Congress in both parties, both before and after the election," Mr. Earnest said. "The briefings have been provided in a variety of settings, both classified and unclassified."

Even beyond the conclusions of the intelligence community, Mr. Trump's campaign had widely known and extensive ties to the Russian government. A campaign manager, Paul Manafort, had worked for the Russian-backed government in Ukraine, and Mr. Trump's choice for national security adviser, Lt. Gen. Michael T. Flynn, had consulted for a Russian-backed media group, Mr. Earnest noted.

Mr. Earnest said that Congress had a "special responsibility" to investigate the ties between the Trump campaign and the Russian government, because those connections were widely known before the election. He added that, for Capitol Hill Republicans, how to "reconcile their political strategy and their patriotism is something they're going to have to explain."

Wired
Trump Ignoring US Intelligence Creates Risks Beyond Russian Hacking
Monday, 12 December 2016
Byline: Andy Greenberg

New York - Observers and alumni of America's intelligence community have already fretted over Donald Trump's impending control of the world's most powerful spy agencies. They've worried that he could abuse their heady surveillance capabilities, turn them on his personal enemies, revamp the NSA's mass surveillance programs, and strip away domestic privacy protections once in charge. But before Trump has even taken office, he's already found a less expected way to abuse the US intelligence community: Ignore, contradict, and insult it.
Trump's relationship--or lack thereof-- with US intelligence agencies isn't just a cause for political spectacle. According to national security experts and former intelligence agency staffers, it could have serious consequences that go well beyond the current dispute over Russian hacking.

The Russia Rift

On Friday, the Washington Post and New York Times reported that the CIA has confirmed that the Russian government repeatedly hacked and leaked Democratic Party documents throughout the presidential election season with the express intention of aiding Trump's campaign. That conclusion goes a significant step beyond earlier intelligence reports that had merely pinned the attacks on the Kremlin without naming its motive.

In response, the Trump transition team offered a brusque rejection of that finding: "These are the same people that said Saddam Hussein had weapons of mass destruction," read the Trump team's statement.

That abrupt dismissal of the intelligence community's findings follows months of Trump's assertions that no one can know the source of the last year's long series of political hacks--despite a publicly released report from the Office of the Director of National Intelligence and the Department of Homeland Security stating that Vladimir Putin's state- sponsored hackers were behind those breaches. "It could be some guy in his home in New Jersey," Trump maintained in a Time interview earlier last week.

The remarks build on what may be the most troubling recent revelation of all, that Trump has declined the traditional daily intelligence briefing given to presidents and presidents-elect. Instead, he receives the briefing only about once a week. "I get it when I need it," he told Fox News Sunday. "You know, I'm, like, a smart person."

That dismissal and disregard of the intelligence agencies' fact-finding represents a disturbing potential preview of the next four years, say former members of the US intelligence community who spoke with WIRED. They worry that it threatens to politicize the intelligence community's work, pushing it toward conclusions that will please the president rather than inform him. They say the growing rift demoralizes staffers, leading to a loss of valuable talent, and that it could leave the commander-in-chief himself dangerously ignorant of crucial world events.

Susan Hennessey, a former NSA lawyer who is now with the Brookings Institution, says that since Trump was elected, she's spoken with former colleagues who are still in the intelligence community who have been "stunned" to hear Trump's repeated rejections of their findings. "It's not outrage, although that might be under the surface," she says of her former colleagues' response. "It's real uncertainty and a sense of fear...shock, bewilderment, wondering what's going to happen next."

Playing Politics

Trump's kneejerk comparison of the Russian hacking report to the faulty intel on Saddam Hussein's weapons of mass destruction takes that dismay to another level, says one former CIA official who helped to write the president's daily briefing under both Obama and Bush. "We've never seen something like this before. It's pretty ballsy," says the former agency official, who requested anonymity because he's not authorized by his current employer to speak about political issues. "From dismissing

the briefings to dismissing the current assessment on the Russia stuff, it seems like he's still in campaign mode. He's politicizing the intel, and that's a problem."

"Every administration has problems with some intelligence," says Patrick Skinner, a former CIA official under Bush and Obama who now works for the security consulting firm the Soufan Group. "But it really shouldn't be public. The open disdain Trump has shown for the agencies is unprecedented."

Trump's transition team didn't respond to WIRED's request for comment.

To be fair, Trump isn't the only skeptic of the intelligence agencies' findings. Neither the leaked CIA assessment that Kremlin hackers were motivated to help Trump nor the intelligence community's October report attributing the attacks to Russia have been backed up with published evidence. That's led Democratic members of congress Elijah Cummings and Eric Swalwell to demand a commission to independently investigate the hacking incidents. President Obama has directed intelligence agencies to conduct a renewed investigation into the attacks. And Republican Senators John McCain and Lindsay Graham joined with Democrats Chuck Schumer and Jack Reed to call for a congressional investigation into the hacker intrusions, splitting with Trump and other Republican leaders who have ignored or dismissed the Russian hacking reports.

In an interview on the CBS show Face the Nation Sunday, Senator McCain clarified that he doesn't doubt Russia was the source of the breaches of targets like the Democratic National Committee and the Democratic Congressional Campaign Committee, but still wants to better understand the motive of those attacks, and whether they targeted Republicans, too. What he doesn't dispute is that Russia was the source. "Now whether they intended to interfere to the degree that they were trying to elect a certain candidate, I think that's the subject of investigation," McCain said. "But facts are stubborn things. They did hack into this campaign."

Trump's doubt of the intelligence agencies' findings isn't the first sign that the divisiveness of the last year's presidential campaign has led to new, partisan distrust of the intelligence community's work, argues Dave Aitel, a former NSA staffer who now runs the security firm Immunity. That doubt had already surfaced with FBI director James Comey's public statements about the bureau's investigation of Hillary Clinton's private email server. The Clinton campaign and Democratic leaders have criticized Comey's behavior, accusing him of influencing the electoral process by writing a letter to Congress about new emails that surfaced in that investigation just weeks ahead of election day. "Our intelligence community has become a political football, and that's something that should never occur," says Aitel. "You need to have trust, and we don't have trust."

Broader Threats

Aitel says that lack of confidence in intelligence agencies' findings and politicization of their work has left his former colleagues increasingly "jaded." And he says that problem of low morale, already sunken after public response to the revelations of NSA leaker Edward Snowden, could lead to a dangerous brain

drain from key agencies. "They don't complain, they don't whine to the press, they just leave," argues Aitel. "Then you get talent shortfalls, and then you get mission failures, which are bombs blowing up in American cities."

Compounding those issues are fears that Trump will continue to ignore his own intelligence apparatus, making uninformed decisions on the world stage, says ex-CIA officer Skinner. Some members of Trump's transition team have reportedly accepted daily intelligence briefings, including his pick for defense secretary, General James Mattis, and vice-president elect Mike Pence. But a president who wields ultimate executive power without that information could be dangerous, says Skinner. "If you close your eyes, the threat is still there: North Korea still exists, ISIS still exists," says Skinner. "These things are complex. You can't counter North Korea with gut feelings."

The rejection feeds back into the morale issue as well. "There's a firm belief in the intelligence community that the president having this information is a really important thing," says ex-NSA lawyer Hennessey. "When you have a boss essentially saying they don't believe or value your work--an outright rejection based on absolutely no evidence--there's a profound sense of uncertainty."

Beyond Trump's specific rejection of any inconvenient finding, Hennessey says it's that larger dismissal of the intelligence community that's most troubling. "If an intelligence agency produces a piece of evidence that's ignored, people can be killed," she says. "The consequences could be as dire as you can possibly imagine."

Radio Free Europe
Cyberattacks On Finance Ministry, Treasury
Monday, 12 December 2016
Byline: Christopher Miller

Kyiv - Ukrainian authorities are still looking for the culprits nearly a week after troublesome cyberattacks against official financial institutions that appeared to be designed to inflict maximum chaos on end- of-the-year payments.
But the head of staff of the Ukrainian Security Service (SBU) identified the so-called malware used in the December 6 attack as the same disruptive software employed in an unprecedented incident a year earlier, blamed on Russia, that cut off power to hundreds of thousands of homes in Ukraine.

Hundreds of thousands of hryvnyas' worth of remittances were delayed or stopped completely over the course of two days after hackers knocked the websites and payment systems of the Ministry of Finance, State Treasury, and pension fund offline, according to statements posted to those sites and local reports.

The National Police are leading the investigation and have discussed the case with the SBU, Oleksandr Tkachuk, chief of staff of the SBU, told RFE/RL on December 12.

The Finance Ministry, which described the incident as a "coordinated professional hacking attack," also claimed the attack had damaged its network equipment.

Tkachuk confirmed that "some data was destroyed and access to networks was blocked."

He said authorities were not prepared to discuss many details publicly because it would take time to fully assess them, adding that attribution in the cybersecurity sphere is a tricky business.

Tkachuk said the attack appeared to bear some similarity to a December 2015 attack against the Prykarpattyaoblenergo power company in Ukraine's western Ivano-Frankivsk region that cut power to hundreds of thousands of homes.

Critical Infrastructure

Ukrainian officials blamed that cyberattack on Russia and speculated that it might have been retaliation for Kyiv cutting off electricity one month earlier to Crimea, which Russia seized from Ukraine in early 2014.

But experts at the time warned that the greater message might be that hackers had the power to shut down critical infrastructure -- something that cybersecurity experts had long feared but never seen in practice.

Elizabeth Sherwood-Randall, a deputy secretary at the U.S. Department of Energy, also blamed Russia for the December 2015 cyberattack.

In that case, the hackers used malicious software called KillDisk, which deletes or overwrites data in system files, causing computers to crash.

KillDisk was also used in the December 6 attacks, the SBU's Tkachuk told RFE/RL.

Relations between Kyiv and Moscow soured after Russia forcibly annexed Crimea in March 2014, and Russia has been accused by Kyiv and Western powers of backing a separatist conflict in eastern in Ukraine that has killed more than 9,750 people.

Kyiv has on several occasions blamed Russia for cyberattacks -- including one on Ukraine's election system ahead of the presidential vote in May 2014 -- that it claims are part of Moscow's greater "hybrid war," a military strategy that combines conventional warfare, irregular warfare, and cyberwarfare.

CBC News
Federal government's Canada.ca project 'off the rails'
Tuesday, 13 December 2016
Byline: Staff reporter

The federal government's bid to merge 1,500 departmental and agency websites into a single site, Canada.ca, is a year behind schedule and almost 10 times over budget. And experts warn it is on track to be another failed government IT project, like the Phoenix pay system.
"It's gone off the rails. It's a disaster," said one government source with knowledge of the project who spoke on condition of anonymity.

CBC spoke with a number of government workers who are also familiar with the project in different departments and they all expressed similar evaluations.

The Canada.ca initiative was launched in 2013 with the goal of making it easier for people to find and use government information online. A $1.54-million contract for a new content management system, where all government websites would be moved, was awarded to Adobe in 2015.

The original deadline to have all active web content moved to the single portal was this month. But in June, it was pushed back to December 2017, which was the initial deadline for the migration of all archived content.

The contract with Adobe is now above $9.4 million, according to government figures.

The actual migration of the websites is up to the departments themselves and is to be done within existing budgets and staffing. Since 2015, eight of the largest departments have budgeted or spent more than $28 million on this project.

Those departments include: Employment and Social Development; Immigration, Refugees and Citizenship; Health; Environment; Canada Revenue Agency; National Defence; Fisheries and Oceans; and Global Affairs.

According to the government, only 10,000 web pages have been moved to date. There are more than 17 million Government of Canada web pages in total.

"If it's cost them already 10 times their existing budget to migrate only 0.05 per cent of the content for the Government of Canada, we're talking about it ultimately costing hundreds of millions of dollars. It's not a small price ticket," said Mike Gifford, CEO of Ottawa-based web development company Open Concept, who has written articles criticizing the government's approach to Canada.ca.

New deadline 'impossible'

Based on the current timeline, Gifford said he thinks the December 2017 deadline is unrealistic. He's not alone.

"Absolutely impossible to achieve," said Timothy Lethbridge, who teaches software engineering and computer science at the University of Ottawa. "And I'm sure many people inside the project know it."

There's also a good chance of the project failing altogether, Lethbridge said, because large IT projects are exponentially more complex. "As a project of this size gets bigger, the probability of failure goes up."

If the government spread the work out over a number of years and spent a billion dollars, it might be able to make the migration a success, Lethbridge said. But he questioned whether taxpayers would be getting value for money at that point.

This is not the first large government IT project to run into problems.

The government will spend at least $50 million this year to try to fix problems with the new Phoenix pay system, which has seen thousands of public servants underpaid, overpaid or not paid at all.

The initiative to transform the government's email system has been stalled for months because of problems with new software.

And Shared Services Canada, the agency created in 2011 to modernize IT-related services in government, has been slammed for its many missteps, particularly by the auditor general.

"There's a trend," said Robin Galipeau, managing partner of OpenPlus, a content architecture company. "There's definitely something going on there. Large renewal projects in IT are failing in government."

OpenPlus, along with Dell and Microsoft, submitted a bid to create the new CMS for Canada.ca.

Ministers refuse to comment

According to OpenPlus Chief Technology Officer Joel Brockbank, the federal government continues to erroneously believe there are one-size-fits-all software solutions for its IT goals.

"There never is," he said. "It's like your cross-trainer running shoes. It's not good for anything that you do."

The key to not having large IT projects fail, Brockbank said, is to simply not do them. Instead, such projects should be done in stages or "bite-size chunks."

None of the ministers whose departments are involved in the Canada.ca migration project were willing to comment when contacted by CBC News.

Treasury Board President Scott Brison, Social Development Minister Yves Duclos and Public Services and Procurement Minister Judy Foote all declined requests. As did Michel Laviolette, the director general of Service Canada, and John Messina, the federal government's chief information officer.

"That tells me they have something to hide," said Debi Daviau, president of the Professional Institute of the Public Service of Canada, the union representing many of the government's IT workers.

"If they're unwilling to be transparent about the decisions they make, that calls those decisions into question."

Yonhap News Agency
Military investigators raid cyber command in hacking probe
Tuesday, 13 December 2016
Byline: Staff reporter

Seoul - Military investigators have raided South Korea's cyber command as part of their investigation into the first hacking of the command's intranet that is being blamed on North Korea, military officials said Tuesday.
"The Defense Security Command is thoroughly looking into how the cyberattacks took place, what confidential information has been leaked and if there was any professional negligence," a military official told Yonhap News Agency.

He confirmed that military prosecutors were overseeing the raid while the Defense Security Command was collecting documents in a raid to the cyber command on Tuesday.

In September, the defense ministry recognized that a total of 3,200 computers, including 700 linked with the intranet, were contaminated with malware a month after the latest cyberattack took place.

The ministry found in October some military documents were hacked while refusing to provide details. The computer used by Defense Minister Han Min-koo also turned out to have been compromised.

Last week, the ministry said the IP addresses linked to the attack were traced to a location in China that has been used by North Korean hackers.

As one of the military's two integration servers was jointly linked to the internet and the intranet, it allowed the hackers to gain access to the intranet, it said.

The cyber command separated the affected server from the whole network to avoid the spread of viruses in October, two months after the initial hacking attempt was made in August.

It marked the first time that the data of South Korea's cyber command has been compromised. South Korea set up the command in January 2010 as part of its efforts to counter external hacking attempts on the country's military.

North Korea -- which has thousands of cyberwarfare personnel -- has a track record of waging cyberattacks on South Korea and the United States in recent years, though it has flatly denied any involvement.

Yonhap News Agency
Acting President Hwang redoubles calls for robust cyberdefense
Tuesday, 13 December 2016
Byline: Song Sang-ho

Seoul - South Korea's Acting President and Prime Minister Hwang Kyo- ahn on Tuesday redoubled calls for robust cyberdefense against North Korea, saying cyberwarfare with the provocative state has already begun.
Following a suspected hacking by Pyongyang of Seoul's cybercommand intranet, Hwang and South Korean security officials have repeatedly stressed the need to prepare against the North's surreptitious cyberattacks which could be as devastating as physical military strikes.

"As evidenced in the recent hack of the (South's) defense ministry, North Korea has attempted to mount cyberattacks on major government facilities, and (this shows) cyberwarfare has already begun," he said during the first regular Cabinet meeting since he took over as acting president last Friday after President Park Geun-hye was impeached over a corruption scandal.

"Related ministries, including the ministries of defense and future planning, must devise thorough measures to prevent any recurrence (of hacking incidents) and take special caution not to allow any minor mistakes to threaten our security," he added.

The defense ministry said last week that a total of 3,200 computers, including 700 linked with the intranet, were infected with malware in August. The computer used by Defense Minister Han Min-koo was also affected, officials said.

In recent years, Seoul has been pushing to bolster its cyberdefense capabilities as Pyongyang has launched a host of attacks on South Korean corporate and government websites by mobilizing its specially trained personnel, including those based in China and other foreign countries.

The reclusive regime has denied responsibility for its cyberattacks including the latest one, upbraiding Seoul for "fabricating" claims about online attacks.

Hwang, in particular, ordered the government to check the nation's financial, traffic, broadcasting and energy networks, and other major national facilities to verify if they are exposed to any cybersecurity threats.

On the economic front, Hwang said that the country's economic fundamentals remain strong as Seoul has striven to maintain a consistent policy despite political uncertainties sparked by the corruption scandal.

The acting president also urged economic officials to keep close tabs on the financial and foreign exchange markets, as he pointed to the potential negative ramifications from a possible United States interest hike.

"I call on you to closely monitor the market situation and respond to it in a timely and resolute manner," he said.

Hwang went on to urge the Cabinet ministers to make concerted efforts to protect the socially vulnerable, including children from low-income families and senior citizens, particularly during the winter season.

Later in the day, Hwang held a luncheon meeting with senior professors and journalists as part of his efforts to solicit their views on ways to bring the nation, gripped by the scandal, back on track.

Hwang renewed his pledge to focus on forestalling any government vacuum and restoring stability in state governance.

Meanwhile, Hwang stepped up efforts to tackle a series of pending issues that can affect the wellbeing of citizens, as he strives to project an image of a trustworthy -- albeit temporary -- leader.

On the day, he directed Agriculture Minister Kim Jae-soo to convene a meeting of senior government officials and civilian experts, dedicated to containing avian influenza (AI), on a daily basis to better tackle the highly contagious virus.

He also instructed top officials from provincial governments to hold their own daily meetings separately to help stem the spread of the bird flu that has ravaged chicken farms across the country since mid-November.

Visiting police stations in Seoul, he called on officers to tighten their crackdown on crimes targeting women and other vulnerable individuals, particularly in the nighttime. He also ordered the police to

"root out" violent or drunk drivers, saying they could cause large-scale accidents involving many casualties.

Regarding the heavy snowfall expected for some parts of the country between Tuesday night and Wednesday afternoon, Hwang directed related ministers to take the necessary steps to minimize any possible damage or inconvenience to citizens.

Japan News
Attacks by Anonymous against Japan rising
Tuesday, 13 December 2016
Byline: Staff reporter

Cyber-attacks against Japan apparently carried out by international hacker group Anonymous have been increasing since September.
Last autumn, a number of government websites and other sites came under attack. However, the recent attacks are different from sophisticated cyber-attacks that aim to steal information. Experts call for people to respond calmly by taking necessary steps in advance without fearing them too much.

Late at night on Sept. 3, the website of the Hiroshima National Peace Memorial Hall for the Atomic Bomb Victims became inaccessible. Shortly after, a group saying it was Anonymous and opposed to dolphin hunting and other issues posted a statement online claiming responsiblity.

An official at the memorial hall said in bewilderment, "We have nothing to do with dolphin hunting."

It is believed a series of Anonymous attacks called Operation Killing Bay started around 2013 in protest against Japan's whale hunting and the annual dolphin hunts in Taiji, Wakayama Prefecture, in September.

Last year, to protest against the dolphin hunting in Taiji, distributed denial of service (DDoS) attacks were launched against government offices websites and infrastructure operators such as airports. DDoS attacks are aimed at rendering websites and other online services unavailable by sending a huge amount of data to the server.

According to police, the number of cyber-attacks Anonymous is believed to be involved in has grown since September. There were no cyber- attack-related website problems from May to August, but 29 incidents were confirmed in September, followed by 26 in October. From Nov. 1 to Nov. 27, there were 53 cases, bringing the total from September to Nov. 27 to 108.

In comparison, incidents ranged between the 10s and 20s each month from September to November last year, but rose to 56 in December.

"Their aim is not to make websites unavailable, but to promote their presence," said Nobuhiro Tsuji, senior security researcher at SoftBank Technology Corp.

This year, the targets of the attacks have conspicuously been small organizations and shops such as izakaya Japanese pubs, and groups totally unrelated to dolphin hunting. "The hackers could be different from last year, and their resources could be smaller," Tsuji said.

'Respond coolly'

When Anonymous started around 2006, it advocated the establishment of the freedom of the internet and made political appeals through legally permitted activities such as street demonstrations.

Currently, however, Anonymous tends to carry out cyber-attacks with the aid of unknown individuals who respond to invitations on Twitter and other websites. Participants are increasingly committing cyber-attacks for fun.

The website of the Kasumigaura river office of the Land, Infrastructure, Transport and Tourism Ministry came under attack in 2012. Anonymous is believed to have confused Kasumigaura with Tokyo's bureaucratic district of Kasumigaseki. The incident was indicative of the group's sloppy management.

Anonymous' main attack method, DDoS, can be committed without significant expertise. Basically, there is no way to defend against such attacks. It is a matter of waiting for an attack to cease, although measures have recently been developed to mitigate damage.

"Compared to cyber-attacks aimed at stealing information, DDoS attacks are not so sophisticated. In most cases, the websites attacked went down and that was it," said Masakatsu Morii, a professor at Kobe University specializing in information and telecommunications engineering.

Some observers point out that such cyber- attacks could increase ahead of the 2020 Tokyo Olympics and Paralympics. Morii said, "It is important that companies and organizations take necessary measures calmly. If they are attacked, they should respond coolly without overreacting."

The Australian Financial Review
Lone wolves and data dumps a problem (Canada)
Tuesday, 13 December 2016
Byline: Jonathan Porter

Sydney - Constant reconnaissance probes by nation states, attacks by computer network robber barons and lone wolves and data dumps from disgruntled workers - that is digital Australia's bleak picture painted for a cyber security forum in Sydney recently.
And without constant vigilance and fine-tuning of our cyber defences, the problem will only get worse.

"A lot of nation states and militaries are investing in capabilities that can be used to target utilities; power, water resource and energy providers," Major-General Stephen Day, former head of cyber at the Department of Defence who was the inaugural head of the Australian Cyber Security Centre, told the Australian Computer Society Cyber Forum in Sydney.

"There is no question reconnaissance is going on right now."

The glimpse behind the curtain at Australia's cyber defenders came during the question and answer period at the end of the forum, attended by some of the world's leading experts in the field.

An attendee put to the panel that an emerging risk was not lone wolf attackers "but of a state-sponsored cyber-attack sometimes from friendly countries we consider allies" and asked what was being done to mitigate the risk.

Day agreed that state-sponsored attacks were a "significant risk", particularly if people looked down the track a few years.

He added that there was also a "significant challenge with organised crime".

"We looked at the sectors that mattered most to our nation either from an economic prosperity perspective or from a national security perspective and put them in a priority order and looked at those sectors that were likely to be targeted by organised crime or by nation states and then we directed our organisational energy to help those sectors.

"So if, for example, you are in the utilities sector or critical infrastructure sector you will have had more experience of government contacting and working with you than the retail sector or the banking sector where you are likely to meet the police more than the national security base."

Victorian minister for Small Business, Innovation and Trade Philip Dalidakis said that while Day's statements were "sexy" and would generate headlines "the one thing everyone in the room has to be extremely cognisant of is that the overwhelming majority of attacks occur from within".

"Yes, we need to be able to stop attacks from the outside of the firewall but the fact of the matter is the two greatest attacks we have seen of data theft from inside were from Bradley Manning and (Edward) Snowden," he told the forum.

"There are a range of companies that will swear black and blue that they have got algorithms that will help flag anomalies within the system - people accessing certain types of data that they haven't done for ages - (or) if you have got your networks categorised under different security levels - people trying to access levels [other] than their security classification. Ultimately it comes down to people and training,

each organisation has to have people who are trained appropriately who can deal with it when - it's not a matter of if - it occurs."

Some of the greatest risks in organisations were the IT divisions themselves, he says.

"People who have the administrative access rights and passwords are sometimes the ones who are undertaking a whole range of activities that people on the rest of the network are banned from doing - including downloading huge amounts of illegal data. Which is, of course, one of the ways people get in.

"So don't go away from this thinking that if you focus on external you are protected because your internal [network] is 80 per cent of your risk."

On the intelligence side, he said he could speak more freely than other panel members because he was not a representative of the federal government.

Dalidakis said the nation was well served by the Five Eyes agreement on signals intelligence sharing with the US, Canada, New Zealand and the United Kingdom.

Fellow panel member Sandra Ragg, assistant secretary for cyber policy in the Department of the Prime Minister and Cabinet, said the nation did need to improve its cyber defences.

"The first thing we can do is improve our cyber defences.

"People focus on state- sponsored threats but cybercrime is a huge piece of the threat to our economy."

Politico
Is Trump's Twitter account a national security threat?
Tuesday, 13 December 2016
Byline: Nahal Toosi

Washington - Donald Trump has years of experience launching Twitter wars. But now, as he prepares to take the highest office in the country, there are growing fears that his tweets could spur a genuine national security crisis.
Intelligence and defense specialists believe the president-elect's use of the popular and powerful social media network is already being used by foreign agencies to analyze his personality, track his habits and detect clues about what to expect from a Trump-led American government.

And that's just based on what Trump writes on Twitter. It's not even counting the vulnerabilities that could arise if overseas hackers invade his phone and digital accounts.

"We've never had a president that's shared so much of themselves, not just what they're saying, but their psychological ticks in such an overt manner, and you can be sure that foreign actors are studying that, too," said P.W. Singer, a defense expert and co-author of "Cybersecurity and Cyberwar." "We're beginning to see what excites him, what angers him, what sets him off. We've never had this ability to read so much on what a president is thinking."

Trump, who prefers mobile phones to computers, is highly attached to his Twitter account (@realDonaldTrump), using the platform to share his thoughts deep into the night. Days after his stunning election victory, he was reportedly worried he would not be able to keep his Android phone upon reaching the Oval Office, suggesting he plans to keep tweeting even after he's sworn in. During his first sitdown interview as president-elect, he told "60 Minutes" that he would be "very restrained" in his Twitter use while in office, before using his account to rail against The New York Times the same day the interview aired.

Trump's following of 17.2 million is likely to expand as he takes office, and his disdain for the mainstream media may bolster his desire to keep up his direct outreach to the public through Twitter.

For the most part, the president-elect has used Twitter to comment on people and institutions on the domestic front, or to defend himself against their criticisms. His tweets are believed to have even influenced the stock market, including on Monday, when his criticism of Lockheed Martin's F-35 program was followed by a drop in the aerospace company's market value. On several occasions, however, Trump has ventured into the international realm.

In recent days, amid lingering Chinese anger over Trump's decision to break U.S. protocol and speak directly to the president of Taiwan, Trump, using two tweets, wrote: "Did China ask us if it was OK to devalue their currency (making it hard for our companies to compete), heavily tax our products going into.. their country (the U.S. doesn't tax them) or to build a massive military complex in the middle of the South China Sea? I don't think so!" On Monday, he used Twitter to sow doubts about claims he's not hard enough on Russia.

Granted, foreign intelligence agencies will likely look at all of Trump's public utterances -- his speeches, interviews, written press releases -- as well as those of his aides to try to understand one of the more unusual men ever to win the White House. (U.S. intelligence analysts do similar studies of foreign leaders, especially in countries such as Iran and North Korea, whose governments are considered hostile and with whom U.S. communication is limited.)

But so far, at least, Twitter has proven one of the purest distillations of Trump around -- a raw version of a businessman-turned-politician keen on ignoring the traditional conventions of the presidency.

Twitter's 140-character limit on tweets appears to appeal to Trump's short attention span and his preference for rapid-fire interactions. But 140 characters often don't leave space for much context, explanation or nuance. So what Trump writes may come across as more forthright and harsher than

what foreign governments are accustomed to in the diplomatic arena. The risk for a misunderstanding is, therefore, higher.

Foreign analysts following Trump's Twitter may not be inclined to simply take everything he writes at face value, especially when it comes to highly sensitive subjects. But, using sophisticated data tools, they may look for patterns that, over time, can help them better predict if Trump is being serious. In all likelihood, many intelligence specialists overseas have probably already done such analyses based on Trump's more than 34,000 tweets so far.

"If Trump's comments accurately reflect his intent, then we're giving the opponents a head start in dealing with the incoming presidential administration," a former U.S. intelligence officer said of Trump's Twitter habits. "If his comments are meant to conceal other intentions, then we're doing a pretty good job in misleading our adversaries."

A foreign government may check to see if Trump uses certain types of words before he takes certain types of actions. If Trump keeps tweeting during his presidency, a foreign entity may analyze what types of things he writes before making a policy announcement. (If Trump were to enable Twitter's geo-location services, that could also grab the attention of overseas actors, though it doesn't appear he uses that feature.) Even a lengthy silence from Trump could be a signal of some sort, sources connected to the intelligence community told POLITICO.

In August, David Robinson, a data scientist, published an analysis of Trump's tweets using digital tools.

It indicated that there were at least two people tweeting out under Trump's account. The tweets from an Android phone appeared to be coming from the Manhattan billionaire himself -- they were angrier and more negative. The ones from an iPhone were more quotidian, sharing announcements and photos; those were likely posted by one or more Trump campaign aides. (Some tweets may have been written by a staffer trying to sound like Trump.)

"A lot of 'emotionally charged' words, like 'badly', 'crazy', 'weak', and 'dumb', were overwhelmingly more common on Android," Robinson wrote, meaning it was Trump who was probably behind those particular tweets.

The U.S. has occasionally found itself in diplomatic dust-ups thanks to Twitter.

In September, during President Barack Obama's visit to China, the Defense Intelligence Agency tweeted "Classy as always China" after the American leader was deprived of a normal red-carpet arrival due to a dispute over which stairs he could use to leave his plane. The Pentagon-based agency later deleted the tweet and apologized.

Four years earlier in Egypt, during the brief presidency of Muslim Brotherhood leader Mohamed Morsi, the U.S. Embassy in Cairo slapped the Islamist organization's English-language Twitter account after it expressed concern for the safety of U.S. diplomats amid violent protests near their building.

"Thanks. By the way, have you checked out your own Arabic feeds? I hope you know we read those too," the embassy tweeted, implying the Brotherhood was using a very different tone in its non-English messages. The Americans later deleted the tweet.

Although Twitter has been around for most of Barack Obama's presidency, the outgoing president has been careful in using the medium. He was allowed to start using his own official account, @POTUS, only a couple of years ago: in May 2015, he sent out an inaugural tweet. The @POTUS account will be made available to Trump once he is sworn in.

The @BarackObama account is run by Organizing for Action, a liberal group that has long supported the president. It was not immediately clear if Obama would take over that account once he leaves office, but he's used it in the past, signing tweets he composed with a "-bo".

The White House Communications Agency, a military division that handles presidential communications security, referred questions about Trump's Twitter account and plans to safeguard his digital devices to the president-elect's transition team. The transition team did not respond to a request for comment. To date, it's not clear if Trump's phone conversations with foreign leaders are fully secured, though his team has said precautions have been taken.

Even as foreign capitals sift through Trump's tweets, there are questions about whether the social media company should take away his account for calling out individual Americans on Twitter. Trump's targets have included an Indianapolis union leader and a college student, who have faced death threats and harassment as a result.

When asked for comment about whether Trump should be booted off the platform, a spokesperson for the company replied: "The Twitter Rules apply to all accounts."

Reuters
Top U.S. spy agency has not embraced CIA assessment on Russia hacking - sources
Tuesday, 13 December 2016
Byline: Jonathan Landy, Mark Hosenball

Washington - The overseers of the U.S. intelligence community have not embraced a CIA assessment that Russian cyber attacks were aimed at helping Republican President-elect Donald Trump win the 2016 election, three American officials said on Monday.
While the Office of the Director of National Intelligence (ODNI) does not dispute the CIA's analysis of Russian hacking operations, it has not endorsed their assessment because of a lack of conclusive

evidence that Moscow intended to boost Trump over Democratic opponent Hillary Clinton, said the officials, who declined to be named.

The position of the ODNI, which oversees the 17 agency-strong U.S. intelligence community, could give Trump fresh ammunition to dispute the CIA assessment, which he rejected as "ridiculous" in weekend remarks, and press his assertion that no evidence implicates Russia in the cyber attacks.

Trump's rejection of the CIA's judgment marks the latest in a string of disputes over Russia's international conduct that have erupted between the president- elect and the intelligence community he will soon command.

An ODNI spokesman declined to comment on the issue.

"ODNI is not arguing that the agency (CIA) is wrong, only that they can't prove intent," said one of the three U.S. officials. "Of course they can't, absent agents in on the decision-making in Moscow."

The Federal Bureau of Investigation, whose evidentiary standards require it to make cases that can stand up in court, declined to accept the CIA's analysis - a deductive assessment of the available intelligence - for the same reason, the three officials said.

The ODNI, headed by James Clapper, was established after the Sept. 11, 2001, attacks on the recommendation of the commission that investigated the attacks. The commission, which identified major intelligence failures, recommended the office's creation to improve coordination among U.S. intelligence agencies.

In October, the U.S. government formally accused Russia of a campaign of cyber attacks against American political organizations ahead of the Nov. 8 presidential election. Democratic President Barack Obama has said he warned Russian President Vladimir Putin about consequences for the attacks.

Reports of the assessment by the CIA, which has not publicly disclosed its findings, have prompted congressional leaders to call for an investigation.

Obama last week ordered intelligence agencies to review the cyber attacks and foreign intervention in the presidential election and to deliver a report before he turns power over to Trump on Jan. 20.

The CIA assessed after the election that the attacks on political organizations were aimed at swaying the vote for Trump because the targeting of Republican organizations diminished toward the end of the summer and focused on Democratic groups, a senior U.S. official told Reuters on Friday.

Moreover, only materials filched from Democratic groups - such as emails stolen from John Podesta, the Clinton campaign chairman - were made public via WikiLeaks, the anti-secrecy organization, and other outlets, U.S. officials said.

"THIN REED"

The CIA conclusion was a "judgment based on the fact that Russian entities hacked both Democrats and Republicans and only the Democratic information was leaked," one of the three officials said on Monday.

"(It was) a thin reed upon which to base an analytical judgment," the official added.

Republican Senator John McCain said on Monday there was "no information" that Russian hacking of American political organizations was aimed at swaying the outcome of the election.

"It's obvious that the Russians hacked into our campaigns," McCain said. "But there is no information that they were intending to affect the outcome of our election and that's why we need a congressional investigation," he told Reuters.

McCain questioned an assertion made on Sunday by Republican National Committee Chairman Reince Priebus, tapped by Trump to be his White House chief of staff, that there were no hacks of computers belonging to Republican organizations.

"Actually, because Mr. Priebus said that doesn't mean it's true," said McCain. "We need a thorough investigation of it, whether both (Democratic and Republican organizations) were hacked into, what the Russian intentions were. We cannot draw a conclusion yet. That's why we need a thorough investigation."

In an angry letter sent to ODNI chief Clapper on Monday, House Intelligence Committee Chairman Devin Nunes said he was "dismayed" that the top U.S. intelligence official had not informed the panel of the CIA's analysis and the difference between its judgment and the FBI's assessment.

Noting that Clapper in November testified that intelligence agencies lacked strong evidence linking Russian cyber attacks to the WikiLeaks disclosures, Nunes asked that Clapper, together with CIA and FBI counterparts, brief the panel by Friday on the latest intelligence assessment of Russian hacking during the election campaign.

Yahoo News
Suspected Russian cyberattack waged on Clinton campaign just days before vote
Monday, 12 December 2016
Byline: Michael Isikoff

Washington - In the closing days of the 2016 election campaign, hackers believed to be working for Russian intelligence launched a new wave of attacks on Hillary Clinton's campaign and the Democratic

National Committee -- a previously unreported cyberoffensive that heightened concerns, now endorsed by the CIA, that the Russian government was seeking to influence the outcome of the election in favor of Donald Trump, according to sources familiar with the investigations into the attempted intrusions. The attacks came in the form of so-called "phishing" emails sent to nearly a dozen campaign and committee staffers in a renewed effort at penetrating their networks, said Dmitri Alperovitch, the co-founder and chief technology officer of CrowdStrike, the cybersecurity firm hired by the DNC to repel attacks on its network. Staffers at that point were alert enough to reject entreaties to click on the unsolicited email messages that would have allowed the hackers into their computers, he said.

But at least one top Clinton campaign staffer, communications director Jennifer Palmieri, told Yahoo News on Sunday that she received an alert from Google in mid- October informing her that her personal Gmail account had been targeted by a "foreign state" actor and that her password needed to be changed.

"They were targeting us throughout the election," said another former senior Clinton campaign staffer, who asked not to be identified. "They never stopped trying to get back in."

The disclosure of the late campaign attack could fuel a mounting controversy over U.S. intelligence findings that link Russian intelligence to the cyberattacks for the express purpose of throwing the election as part of a campaign, orchestrated in Moscow, to defeat Clinton.

The Washington Post reported Saturday that the CIA has briefed members of Congress on an assessment that the Russians targeted Democratic political organizations and campaign officials as part of a specific effort to defeat Clinton and elect Trump. This goes beyond an earlier public finding that U.S. intelligence officials were "confident" that the Russian government was behind the cyberattacks, but did not ascribe a motive for the Russians doing so.

One piece of damning evidence behind the new finding is that the CIA and the FBI have both identified specific individuals associated with or close to the Russian government who provided the DNC emails to WikiLeaks, which began publishing them in July, a senior law enforcement official told Yahoo News. Despite reports of a clash between the CIA and the FBI over the motive behind Russia's intelligence service in launching the operation, the differences are more a matter of "degree" and emphasis, with the FBI believing there may have been "mixed" motives for the Russian effort, the official said. Still, "we all agree they did these things," the official said.

But President-elect Trump doubled down on his rejection of the intelligence findings in an interview with Fox News anchor Chris Wallace that aired Sunday, dismissing any conclusion that points to Russian government involvement.

"I think it's ridiculous," Trump told Chris Wallace in interview that aired on "Fox News Sunday," his first Sunday show sit-down since winning the election. "I don't believe it."

"If you look at the story and you take a look at what they said, there's great confusion," Trump added. "Nobody really knows, and hacking is very interesting. Once they hack, if you don't catch them in the act you're not going to catch them. They have no idea if it's Russia or China or somebody. It could be somebody sitting in a bed someplace. I mean, they have no idea."

Alperovitch of CrowdStrike, the cybersecurity firm that first publicly linked the cyberattacks to Russian intelligence, said Sunday that he was "puzzled" by Trump's remarks and assumes he has not yet been fully briefed on the matter. (CrowdStrike, whose principals include Shawn Henry, the former chief of the FBI's cyber division, was initially hired by the DNC to investigate the cyberattacks and defend its network last May.)

"At this point, the matter of attribution on the intrusions has been settled,"Alperovitch said. "There is nobody that looks at the evidence who disputes this." Asked his level of confidence in his firm's findings, he responded "100 percent."

Much of the evidence, he said, revolves around the nature of the sophisticated tools used by the attackers on the DNC and forensic evidence showing strong similarities to Russian cyberattacks that have occurred in Ukraine and other Eastern European countries -- as well as to intrusions of the Joint Chiefs of Staff, the White House and the State Department and other U.S. government agencies. "The digital fingerprints are of the same origin," said Alperovitch.

CrowdStrike initially identified two sets of attackers on the DNC's servers: One, dubbed "Cozy Bear," was associated with the Russian FSB (the successor to the Soviet KGB) and which first breached the DNC's network in the summer of 2015. Another, dubbed "Fancy Bear," has been associated with Russia's military intelligence service, the GRU. The latter infiltrated the DNC's network in late April of this year in what turned into a far more devastating attack, resulting in the disclosure of 20,000 internal DNC emails to WikiLeaks -- an act, according to Alperovitch, of "information warfare." (He acknowledged that a third Russian intelligence service, the SVR, which has responsibility for foreign intelligence operations, may also have been involved.)

"When we look at this over 10 years -- literally hundreds of intrusions -- [and] you look at the tradecraft, you look at the victims, it all points to Russian intelligence services," Alperovitch said.

In addition, he said, there was another separate cyberattack discovered in late September from an undetermined party that penetrated DNC computers with software containing sensitive voter analytic data that was being provided in regular memos to Clinton campaign manager Robby Mook, the sources said.

The breach was detected by CrowdStrike, and the cyberinvaders were expelled from a cloud server housing the data; this server was distinct from the DNC's internal computer network that had been previously breached, he said. But the intruders were never identified, and it was never determined

whether the data -- containing detailed reports on voter registration and estimates of likely voter participation in the November election -- was ever actually stolen.

Alperovitch said he doesn't know whether these hackers were associated with Russian intelligence; they used different methods and publicly available cybertools to pull it off -- also he said the DNC never authorized his firm to conduct a full investigation. But he said the late October "phishing" attacks on the DNC and the Clinton campaign resembled the earlier Fancy Bear attacks, leading him to conclude they were likely the work of the GRU.

Moreover, attacks by the Cozy Bear intruders have continued throughout the fall, targeting multiple organizations, including think tanks and universities whose scholars work on Russian policy issues, he said.

And even more recently, he said, there was evidence that the separate "Fancy Bear" hackers are now also attacking political organizations in Germany and elsewhere in Europe in an apparent attempt to meddle in their elections as well. (The chief of German domestic intelligence said last week that there has been a recent increase in "aggressive cyberespionage" against German politicians and warned about "growing evidence for attempts to influence the [German] federal elections next year."

"These activities have not stopped," said Alperovitch. "Now that they were executed [in the United States] and they have a successful playbook, I fully expect they are going to continue."

Press TV
Iranian Army unveils new indigenous combat, reconnaissance drones
Tuesday, 13 December 2016

Tehran - The Iranian Army's Ground Forces has unveiled two domestically-designed and -manufactured drones on the final day of major military exercises code-named Mohammad Rasoulallah IV (Mohammad, the Messenger of God IV) in southeastern Iran.
One of the two aircraft, code- named Oghab (Eagle), is a combat drone capable of carrying air-to-surface missiles.

The other, code-named Shahin (Falcon) and developed and manufactured under a project code-named Shahid Mohsen Ghotaslou, can collect information on the positions and movements of enemy forces on reconnaissance missions. It boasts a flight endurance of 24 hours.

General Seyyed Kamal Peyambari, the spokesman for the military drills, said the jamming and combat techniques of drones were also fully tested at various altitudes on Tuesday, with the participation of military commanders and defense experts.

Peyambari noted that sophisticated and innovative weapons such as super- caliber 107mm rocket launchers, optimized versions of the 62.5mm PSG-1 and Dragunov semi-automatic sniper rifles, a jammer with an effective range of 800 meters, drone jammers, and cellular satellite phone jammers were put to practice on the last day of the drills as well.

Various and extensive psychological war techniques such as drills using 122mm flyer-carrying rockets, tactical radios and directional sound systems were also put to the test for the first time.

The senior Iranian military figure further noted that hand-launched drones as well as land minelayers were also tried out.

Peyambari added that electronic warfare, armored, infantry, mechanized infantry, commando, and intelligence units present at the Mohammad Rasoulallah IV military exercise, which covered an area of 220,000 square kilometers, successfully carried out their operations on the third day of the drills.

Iran has conducted major military drills in recent years to enhance the defense capabilities of its Armed Forces and to test modern military tactics and state-of-the-art equipment. Each year, the country inaugurates a host of new projects and hardware developed with reliance on domestic capabilities.

The Islamic Republic maintains that its defense power is driven by deterrence and poses no threat to any other country.

Hindustan Times
Legion: Meet the hackers who broke into Twitter accounts (Canada).
Tuesday, 13 December 2016

New Delhi - A hackers' group called Legion has repeatedly breached the Twitter accounts of some well-known Indians, including Congress vice- president Rahul Gandhi and prominent journalist Barkha Dutt. Legion has not posted any classified information on the hacked accounts but has threatened to expose email communications among Congress party leaders in the New Year. Earlier this month, they on his Twitter handle, vowing to bring to justice the fugitive industrialist who has defaulted on at least Rs 7,000 crore bank loans.

Here is some detail about the hackers' group: What is Legion? It is a coalition of like-minded hackers based out of five countries - the United States, Sweden, Canada, Thailand and Romania, according to the Delhi police's cybercrime cell. The group seeks to expand its activities, leaving its email id -- legion_group@sigaint.org - for more hackers to join their campaign.

Are they connected with Legion of Doom of the 1980s? The group does not appear to have any links with the hackers' group Legion of Doom (LoD) that targeted rich and famous people's email accounts in the mid-1980s. LoD remained active till early 2000s. However, the two groups appear to share

ideological goals in targeting what they say are the rich and corrupt. LoD was founded by US-based hacker Lex Luthor after he broke away from the Knights of Shadow.

Why do they hack people's accounts? Legion fancies itself as cyber vigilantes working to expose the corrupt. But the group is yet to bolster their anti-corruption crusader credentials, given that it has so far offered very little valuable information.

How does Legion operate? Legion communicates through email servers and browsers that are shielded against surveillance. In other words, it does not use Google Chrome or Internet Explorer but a browser called The Onion Router (TOR), which is difficult to track (provides anonymity) and allows a user to communicate directly with another one. This is also called the darknet, a platform often used by activists and journalists seeking to avoid a surveillance dragnet.

Are there other such hackers' groups? Yes. Anonymous is another loosely associated international network of activist and hacktivists which started operating in 2003. The group's website describes it as "an Internet gathering" with "a very loose and decentralised command structure that operates on ideas rather than directives". The group became known for crashing websites of governments, corporates and religious groups. Anonymous members (known as "Anons") use the Guy Fawkes mask as their emblem.

Saudi Gazette
IoT continues to pose a key cyber security threat
Tuesday, 13 December 2016
Byline: Mohammed Al-Moneer

Riyadh - The cyber landscape changes dramatically year after year. If you blink, you may miss something; whether that's a noteworthy hack, a new attack vector or new solutions to protect your business. Sound cyber security means trying to stay one step ahead of threat actors.
In the spirit of looking toward the future, I wanted to grab my crystal ball and take my best guess at what will be the big story lines in cyber security in 2017.

1. IoT continues to pose a major threat. In late 2016, all eyes were on IoT-borne attacks. Threat actors were using Internet of Things devices to build botnets to launch massive distributed denial of service (DDoS) attacks. In two instances, these botnets collected unsecured "smart" cameras. As IoT devices proliferate, and everything has a Web connection -- refrigerators, medical devices, cameras, cars, tires, you name it -- this problem will continue to grow unless proper precautions like two-factor authentication, strong password protection and others are taken.

Device manufactures must also change behavior. They must scrap default passwords and either assign unique credentials to each device or apply modern password configuration techniques for the end user during setup.

2. DDoS attacks get even bigger. We recently saw some of the largest DDoS attacks on record, in some instances topping 1 Tbps. That's absolutely massive, and it shows no sign of slowing. Through 2015, the largest attacks on record were in the 65 Gbps range.

Going into 2017, we can expect to see DDoS attacks grow in size, further fueling the need for solutions tailored to protect against and mitigate these colossal attacks.

3. Predictive analytics gains ground. Math, machine learning and artificial intelligence will be baked more into security solutions. Security solutions will learn from the past, and essentially predict attack vectors and behavior based on that historical data. This means security solutions will be able to more accurately and intelligently identify and predict attacks by using event data and marrying it to real-world attacks.

4. Attack attempts on industrial control systems. Similar to the IoT attacks, it's only due time until we see major industrial control system (ICS) attacks. Attacks on ecommerce stores, social media platforms and others have become so commonplace that we've almost grown cold to them. Bad guys will move onto bigger targets: dams, water treatment facilities and other critical systems to gain recognition.

5. Upstream providers become targets. The DDoS attack launched against DNS provider Dyn, which resulted in knocking out many major sites that use Dyn for DNS services, made headlines because it highlighted what can happen when threat actors target a service provider as opposed to just the end customers.

These types of attacks on upstream providers causes a ripple effect that interrupts service not only for the provider, but all of their customers and users. The attack on Dyn set a dangerous precedent and will likely be emulated several times over in the coming year.

6. Physical security grows in importance. Cyber security is just one part of the puzzle. Strong physical security is also necessary. In 2017, companies will take notice, and will implement stronger physical security measures and policies to protect against internal threats and theft and unwanted devices coming in and infecting systems.

7. Automobiles become a target. With autonomous vehicles on the way and the massive success of sophisticated electric cars like Teslas, the automobile industry will become a much more attractive target for attackers. Taking control of an automobile isn't fantasy, and it could be a real threat next year.

8. Point solutions no longer do the job. The days of Frankensteining together a set of security solutions has to stop. Instead of buying a single solution for each issue, businesses must trust security solutions from best-of-breed vendors and partnerships that answer a number of security needs. Why have 12 solutions when you can have three? In 2017, your security footprint will get smaller, but will be much more powerful.

9. The threat of ransomware grows. Ransomware was one of the fastest growing online threats in 2016, and it will become more serious and more frequent in 2017. We've seen businesses and individuals pay thousands of dollars to free their data from the grip of threat actors. The growth of ransomware means we must be more diligent to protect against it by not clicking on anything suspicious. Remember: if it sounds too good to be true, it probably is.

10. Security teams are 24/7. The days of security teams working 9-to-5 are long gone. Now is the dawn of the 24/7 security team. As more security solutions become services-based, consumers and businesses will demand the security teams and their vendors be available around the clock. While monitoring tools do some of the work, threats don't stop just because it's midnight, and security teams need to be ready to do battle all day, every day. Those are 10 things we see happening in the cyber security space next year.

Fars News Agency
Iran's Ground Force Unveils New Drone during Massive Drills
Tuesday, 13 December 2016

Tehran - The Iranian Ground Force unveiled a new drone named 'Farpad' during the massive wargames codenamed 'Mohammad Rasoulallah (PBUH) 4' in the Southeastern parts of the country on Monday morning. The hand- launched drone is run by autopilot and can fly maximum 45 minutes to the range of 20km.
Also during the second day of the three-day drills, the Iranian Ground Force unveiled a jamming system which is capable of confronting Unmanned Aerial Vehicles (UAVs) in a range of 3km and can force it to land after taking its control. The system is also portable by individuals.

In another development in the wargames, the home-made Toufan missiles whose range and destruction and precision-striking power have been improved were fired by helicopters and hit simulated enemy's targets precisely.

Also, the latest sniper gun manufactured for the Iranian Ground Force, 'Taher', with a range of 1.2km was unveiled on Monday. The gun weighs 4.4kg (without scope and magazine) and is 1.28m in length.

Meantime, the 209 (Cobra) and 214 helicopters of the Iranian Ground Force's air force units fired several rockets at two floating targets in Makran region (in the Sea of Oman) and destroyed them.

Also, two Mirage fighter jets of the Iranian Air Force participated in the drills for the first time and used air-based weapons in operations against the simulated enemy.

The massive 'Mohammad Rasoulallah (PBUH) 4' wargames started in the Southeastern parts of the country on Sunday morning.

"On the first day of the drills, rapid reaction units from other geographical regions of the country were transferred to the operational regions via air and ground in the shortest possible time," Spokesman of the drills General Seyed Kamal Payambari told reporters yesterday.

He said that the drills are being held in the strategic Southeastern parts of the country in a range of over 220,000km with the participation of different units of Ground Force, logistic forces of the Air Force and Khatam ol-Anbia Air Defense Base.

According to General Payambari, assessment of the Iranian forces' preparedness in the tactical fields and decreasing the time for their rapid reaction against threats as well as using new defense systems are among the goals pursued in the wargames.

Meantime, Army Airborne Commander Brigadier-General Houshang Yari announced on Sunday that dozens of different types of helicopters are flying over the wargames zone.

"Tens of different types of 206, 214, 209 (Cobra) and Chinook helicopters are present in the drills zone," General Yari told reporters today.

"During the drills, the command, track, control and close fire support missions as well as numerous heliborne operations will be carried out by the Airborne helicopters," he added.

General Yari said that the drills will also be a touchstone to assess the agility and power to overhaul and maintain helicopters.

Fars News Agency
Civil Defense Official Warns of New US Cyber Attack against Iran
Tuesday, 13 December 2016

Tehran - A senior member of Iran's Civil Defense Organization warned that Washington has hatched plots to launch new cyber operations against the country's infrastructures.
"At present, the US has launched a project named Nitro Zeus with the aim of attacking Iran's defense and telecommunication infrastructures," Alireza Karimi said on Monday, addressing a conference in Tehran.

"Based on studies that we have carried out, the project is assessed to be much more dangerous than the Stuxnet project," he added.

His remarks came after Deputy Head of Iran's Civil Defense Organization Brigadier General Mohammad Hassan Mansourian underlined in October his organization's full preparedness to confront the cyberattack and cultural invasion threats.

"Iran's Civil Defense Organization can defuse cyberattacks and cultural invasions," Brigadier General Mansourian said. He underlined that the advanced countries are currently making huge investments in the field of civil defense.

Mansourian underscored that the cyberattack and cultural invasion should only be responded by the national civil defense system.

In May 2015, Head of Iran's Civil Defense Organization Brigadier General Gholamreza Jalali announced that the country has set up cyber defense workgroups to better coordinate measures for defending nuclear facilities against enemies' cyber attacks.

"The country's vital cyber infrastructures have been identified and separate cyber workgroups have been formed in all fields," Jalali told reporters in Tehran.

"For instance a cyber defense workgroup was set up in the nuclear field for Natanz nuclear installations and no serious incident has threatened this section in the past two years," he added.

In relevant remarks in October 2014, Jalali revealed that a US cyberattack on Iran's nuclear enrichment facility in Natanz failed due to his organization's tough defensive measures.

"The first cyberattack, codenamed Olympic Games, was carried out on Natanz and was declared by the US President, but it met our heavy (defensive) response," Jalali told reporters in a press conference in Tehran.

The senior commander said the US changed its cyber commander following the failure in the cyberattack on Natanz, adding that the US general was forced to retire several months ago "due to the wrong information and data that he had presented to President Obama". And this was the result of our direct confrontation with them, General Jalali added.

The US was the principal player in the most sophisticated cyber-attack ever known and has been orchestrating a campaign against Iran designed to undermine the country's nuclear program.

The New York Times came up with an in-depth report on June 1, 2012 saying that from the very first month Barack Obama took over as US President, he secretly ordered increasingly sophisticated attacks on Iran's computer systems that run the country's main nuclear enrichment facilities.

The disclosures about Obama's role in the cyberwar against Iran appear to show beyond doubt that the US, with the help of Israel, was behind the Stuxnet virus attack on Iran's centrifuge machines - used to enrich uranium. The revelation then indicated that Washington and Tel Aviv were also behind the Flamer and Duqu virus attacks discovered by experts in May 2012.

Codenamed Olympic Games, the attacks were spearheaded by the US government under the Bush administration. Stuxnet targeted Siemens industrial equipment to spin hundreds of centrifuges beyond their breaking points and eventually disable Iran's nuclear efforts.

According to the report, Obama decided to speed up the attacks, even after the worm escaped from Iran's Natanz plant in 2010 and later ended up on the Internet.

During a meeting following the worm's escape, Obama even considered that the worm should be stopped thinking that America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised. Should we shut this thing down? Obama asked members of the President's national security team.

However, he finally decided to go ahead with the cyberattacks. What followed thereafter was the Natanz plant being hit by several newer versions of the worm.

The report is said to be based on 18 months of interviews with current and former American, European and Israeli officials involved in the program as well as with outside experts, who provided contradictory assessments of how successful the attack was in slowing down Iran's progress of developing nuclear weapons.

While internal Obama administration estimates claim the effort was delayed by 18 months to two years, some other experts, both inside and outside the government, said that Iran's enrichment levels had steadily recovered. A year later, Iran enriched uranium to the 20-percent grade, way beyond the 5-percent purity level that was done in Natanz in 2012.

Le Télégramme
Cybersécurité. La Bretagne au coeur du combat
Tuesday, 13 December 2016
Byline: Journaliste maison

Bruz, France - Jean-Yves Le Drian, ministre de la Défense, a dévoilé au centre DGA Maîtrise de l'information à Bruz (35), près de Rennes, la doctrine des armées en matière de cybersécurité. « L'émergence d'un nouveau milieu, d'un champ de bataille cyber, doit nous amener à repenser profondément notre manière d'aborder l'art de la guerre (...), comme l'aviation au début du XXe siècle », a-t-il assuré, soulignant : « En temps de guerre, l'arme cyber pourra être la réponse, ou une partie de la réponse, à une agression armée, qu'elle soit de nature cyber ou non ». La doctrine présentée ce lundi, qui repose sur trois piliers - renseignement, protection/défense et lutte informatique offensive - est l'une des plus élaborées énoncées en Europe, avec celle du Royaume-Uni. Concrètement, la France pourra recourir au combat numérique comme à une arme classique de type missile pour riposter à une attaque, aussi bien cyber que conventionnelle. « Nos capacités cyber offensives doivent nous permettre

de nous introduire dans les systèmes ou les réseaux de nos ennemis, afin d'y causer des dommages, des interruptions de service ou des neutralisations temporaires ou définitives », a relevé le ministre.

Un bataillon de 2.600 « combattants numériques »

Un commandement des opérations cyber, placé sous la responsabilité directe du chef d'État-Major des armées, va être créé, dès janvier 2017. Il disposera d'un état-major resserré qui supervisera 2.600 « combattants numériques » . Les armées pourront « neutraliser » des infrastructures utilisées pour attaquer des intérêts français mais aussi « riposter » plus largement à une attaque cyber, a expliqué Jean-Yves Le Drian.

« Si une attaque cyber s'apparente à un acte de guerre, une riposte adéquate s'imposera (...) dans une logique de conflit ouvert », a-t-il souligné. Si l'attaque transite par un État qui « n'aurait pas empêché une telle utilisation, la responsabilité de cet État pourrait être mise en jeu », a-t-il averti.

Le Monde
Un an après sa création, la commission chargée du contrôle du renseignement
Tuesday, 13 December 2016
Byline: Jacques Follorou

Paris - Un an après sa création, la commission chargée du contrôle du renseignement affirme son indépendance
L'avis de la Commission nationale de contrôle des techniques de renseignement, née en octobre 2015 pour faire contrepoids aux puissants moyens de surveillance accordés aux services secrets, n'est que consultatif mais le premier ministre l'a suivi dans la plupart des cas.

Pour son premier rapport annuel, présenté mardi 13décembre, la Commission nationale de contrôle des techniques de renseignement (CNCTR), née, le 3octobre 2015, pour faire contrepoids aux puissants moyens de surveillance accordés aux services secrets français dans la loi du 24juillet 2015 sur le renseignement, jouait une part de sa crédibilité.

Nommé président de cette nouvelle instance indépendante, Francis Delon, ex-secrétaire général de la défense nationale et l'un des pères fondateurs de la plateforme nationale du renseignement technique qui alimente depuis 2008 la communauté française du renseignement, devait prouver que les premiers soupçons de grande proximité avec l'Etat étaient infondés. Il devait, de plus, montrer que dans une période où l'émotion pèse sur les décisions politiques, il saurait résister aux pressions l'invitant à ne pas s'opposer aux libertés prises avec le droit.

La CNCTR est chargée de contrôler de l'utilisation d'une douzaine de moyens de surveillance par les services de renseignement français. L'avis de la CNCTR, composée de dix-sept membres, dont trois ingénieurs, n'est que consultatif. Le premier ministre, seule autorité décisionnaire en la matière, l'a

néanmoins suivi dans la plupart des cas. La procédure dite d'urgence, qui permet de s'exonérer du point de vue de la CNCTR, n'a été déclenchée qu'à une reprise selon le rapport qui ne fournit aucun détail opérationnel.

8538 interceptions de sécurité validées

En un an, la CNCTR a visé 48208 demandes de collecte de données de connexion, qui portent parfois sur de simples recherches de numéros dans des annuaires. Elle a donné un avis favorable à 2127 demandes de géolocalisation et elle a validé 8538 interceptions de sécurité, des écoutes téléphoniques, alors que l'instance qui existait auparavant, la Commission nationale de contrôle des interceptions de sécurité (CNCIS), née de la loi de 1991, en avait contrôlé un peu plus de 7000 lors de sa dernière année.

La CNCTR reste très discrète sur les 7711 fois où «d'autres techniques» ont été déployées avec son aval. S'agissait-il de pose de balises, de sonorisation d'appartements, de recueil ou de collecte de données informatiques? On n'en saura rien. La CNCTR explique qu'elle est tenue par la loi qui lui interdit de révéler des capacités opérationnelles. Elle signale néanmoins que faute d'achèvement du chantier de «centralisation des données recueillies» par ces nouvelles techniques, elle n'a pas encore une vision sur leur utilisation sur tout le territoire.

6,9% des demandes renvoyées aux services

En matière d'avis défavorables, on note une augmentation par rapport au temps de la CNCIS qui ne donnait son avis que sur les interceptions de sécurité et les données de connexions. La CNCTR a renvoyé aux services 6,9% des demandes contre environ 1% à l'époque de la CNCIS. Avant la loi de juillet2015, les services de renseignement usaient d'un grand nombre de ces moyens intrusifs, balises, sonorisation de lieux, etc. sans demander l'autorisation à quiconque, en toute illégalité. Les avis défavorables de la CNCTR portent essentiellement sur ces outils, désormais légaux, mais particulièrement attentatoires à la vie privée.

Si la CNCTR s'est vue, de fait, reprocher par les services un surcroît de «paperasse», elle a surtout pu éprouver la réalité de son indépendance lors des tentatives du gouvernement de passer outre ses prérogatives. Ce fut ainsi le cas avec l'article851-2 sur le recueil de données de connexions en temps réel attachées à une personne sur l'ensemble de ses moyens de communication.

La loi sur le renseignement du 24juillet 2015 disposait que cette collecte ne pouvait être effectuée que «sur une personne préalablement identifiée comme présentant une menace» . Le gouvernement et le chef de l'Etat ont tenté, en janvier, d'utiliser ce moyen pour mettre sous surveillance des listes entières de suspects, notamment les fameux fichés «S» pour islam radical, soit près de 14000 personnes. M.Delon a bloqué cette requête considérant qu'elle n'est pas conforme à la loi qui impose que chaque demande doit être individualisée et justifiée.

Pour contourner ce refus de valider «des surveillances groupées et simplifiées», le gouvernement, soutenu par un législateur, davantage soucieux d'étendre la surveillance d'Etat que de jouer son rôle de contre-pouvoir, a, depuis, modifié à deux reprises le périmètre de cet article de loi. Dans le cadre des lois sur la prorogation de l'Etat d'urgence, le Parlement a d'abord élargi la surveillance aux personnes «pouvant constituer une menace» . Et fin juillet, il a étendu la collecte de données de connexion en temps réel à l'entourage de la personne surveillée dès lors qu'il existait simplement «des raisons sérieuses de penser» qu'espionner ces gens au sein de cercles familiaux, amicaux, professionnels ou occasionnels puisse avoir un intérêt.

L'«exception hertzienne»

Si les parlementaires n'ont pas été d'une grande aide pour la CNCTR, elle a, en revanche, trouvé dans le Conseil constitutionnel un soutien inattendu pour tenter d'étendre son contrôle sur un pan entier des surveillances en France qui restaient jusque-là interdites, les communications hertziennes. Qualifiée d' «exception hertzienne» par la CNCTR, cette dérogation du droit consacrée par la loi de 1991 sur les interceptions puis prorogée dans la loi de juillet de 2015, a pris fin lors de sa censure, le 21octobre, par le Conseil constitutionnel.

Se félicitant de la décision du Conseil de vouloir faire entrer la surveillance par voie hertzienne dans le droit commun et d'avoir été chargée par lui de veiller à son application d'ici au vote d'une nouvelle loi, au plus tard le 31décembre 2017, la CNCTR a, au moins jusqu'à cette date, le pouvoir de viser chaque demande d'interceptions effectuée par cette technique. Souhaitant poursuivre son avantage, la CNCTR demande, dans son rapport, d'être «consultée sur l'éventuelle nouvelle législation» .

Le Temps (Suisse)
ID Quantique se déploie à l'international
Tuesday, 13 December 2016
Byline: Dejan Nikolic

Londres - Le numéro un mondial de la cryptographie quantique et de la génération de nombres aléatoires ouvre un bureau à Londres, signe un partenariat stratégique avec le géant coréen SK Telecom et s'attaque au marché chinois
ID Quantique (IDQ), pépite issue des laboratoires de physique appliquée de l'Université de Genève, s'offre un déploiement sans précédent. L'actuel numéro un mondial de la cryptographie quantique et de la génération de nombres aléatoires étend tout d'abord ses activités à la Grande-Bretagne. A travers notamment un contrat consistant à sécuriser les échanges d'informations entre l'un des sites de BT (anciennement British Telecommunications) et Cambridge.

IDQ ouvre également une officine britannique, afin de prendre part à une plateforme scientifique nationale de 384 millions de francs sur cinq ans. « Huit grandes universités du pays ainsi que le secteur

privé et public participent à ce programme », précise Grégoire Ribordy, fondateur d'IDQ, qui imagine affecter cinq collaborateurs à Londres d'ici à un an.

Parallèlement à cette nouvelle tête de pont britannique, IDQ signe une alliance avec SK Telecom, le principal opérateur de Corée du Sud (29,45 millions de clients, soit environ 50% du marché local, pour près de 15 milliards de francs de chiffre d'affaires l'an passé). Ce rapprochement avec la major de l'un des pays les plus connectés de la planète est assorti d'une levée de fonds de plus de 4 millions de francs. Soit la troisième injection de capital en quinze ans, les deux précédentes rondes ayant permis d'engranger respectivement un million (2004) et quatre millions (2014).

La fibre commerciale

L'entreprise carougeoise, lancée en 2001 et qui affiche une croissance moyenne de 30% par an, emploie aujourd'hui une cinquantaine de salariés, soit plus du double qu'en 2014. Son dernier tour de financement, auquel participent d'autres investisseurs stratégiques, est destiné à renforcer sa suprématie à l'échelle planétaire. Et d'asseoir son développement en Asie.

« L'une des filiales de SK Telecom fabrique des puces pour smartphones intégrant des nombres aléatoires, relève Grégoire Ribordy. Ce dispositif bon marché, qui permet de réduire la vulnérabilité des appareils, est en passe de révolutionner le monde de la téléphonie mobile. » Un boîtier traditionnel, de taille standard, coûte environ 1000 francs. Avec la technologie sud-coréenne embarquée, générer des clés ou des mots de passe exclusifs coûtera jusqu'à 100 fois moins cher.

Promesses quinquennales

Dans la foulée, IDQ inaugure son entrée sur le marché chinois. Via une coentreprise avec China Quantum Technologies (CQT), une société pionnière dans les technologies quantiques, à l'origine du plus important réseau commercial en la matière. Soit entre les villes de Shanghai et de Hangzhou, un tronçon de communication ultra-sécurisé d'environ 200 km. « Les contrats ont été signés il y a un mois », se félicite Grégoire Ribordy, sur le point d'ouvrir avec son partenaire chinois une usine dans la province du Zhejiang.

Le nouveau site de production, appelé à fonctionner avant fin 2017 avec un effectif de 50 collaborateurs, doit notamment permettre à CQT d'accéder au savoirfaire genevois en participant à la fabrication notamment de produits d'appel destinés aux casinos et aux paris en ligne. En échange de quoi, IDQ se voit offrir une porte d'entrée sur le potentiel commercial chinois.

La cryptographie quantique est l'un des cinq axes du 13e plan quinquennal de Pékin, définis comme étant d'importance stratégique cruciale pour la nation. Le prix d'un appareil de cryptage, qui c oûte actue llement 50 000 francs pièce, « sera divisé par dix grâce aux volumes du marché chinois », estime Grégoire Ribordy.

Toutefois, les spécialistes se heurtent pour l'heure à un obstacle technique de poids: par voie terrestre, le système ne fonctionne que de point à point, jusqu'à cent kilomètres au maximum. Au-delà, trop de photons sont perdus par diffusion en raison des imperfections de la fibre. Il faut alors aménager des noeuds intermédiaires pour que la particule qui compose la lumière, et qui sert à envoyer les clés de chiffrement nécessaires au décodage de l'information, soit impossible à intercepter. Le maillage Shanghai-Hangzhou, qui garantit que toute tentative d'espionnage provoque l'autodestruction du signal, en compte par exemple cinq.

Mais la Chine rêve d'inaugurer, d'ici à 2030, un système d'échange de données inviolable à l'échelle mondiale. Pékin a ainsi lancé le 15 août dernier le premier satellite de communication indéchiffrable à longue distance (près de 2500 km). Seul hic: l'instrument en orbite doit être orienté de manière extrêmement précise vers les stations au sol. « Ce sera comme lancer une pièce de monnaie d'un avion volant à 100 km d'altitude et espérer qu'elle vienne se ficher exactement dans la fente d'une tirelire cochon en rotation », avait alors expliqué Wang Jianyu, le responsable en chef de cette percée technologique de Pékin.

Le Télégramme
Lannion. Nouvelle Breizh cyber valley
Tuesday, 13 December 2016
Byline: Journaliste maison

Lannion, France - Marie-Hélène Clam et Riwan Marhic Après Rennes et Bruz (35), la journée cybersécurité du ministre de la Défense, Jean-Yves Le Drian, s'est achevée sur le site de Nokia, à Lannion (22). Il s'y est vu confirmer la création de 500 emplois d'ingénieur Recherche et Développement d'ici à la fin 2018, dont une grande partie à Lannion, ciblée pôle mondial pour ce secteur.
« Lannion sera le centre mondial pour Nokia concernant la recherche en cybersécurité », a lancé Marc Rouanne, le numéro deux du groupe Nokia. Devant un Jean-Yves Le Drian acquis à la cause puisque lanceur du Pact Cybersécurité dès 2012, le dirigeant a confirmé le recrutement de 500 ingénieurs Recherche et Développement dont 300 jeunes diplômés. À lui seul, le site de Lannion accueillera une centaine de ces ingénieurs amenés à travailler sur la 4G, la 5G, l'internet des objets et bien sûr la cybersécurité. « Nokia est aussi sponsor de la première formation informatique et cyberdéfense de l'École nationale supérieure d'ingénieurs de Bretagne-Sud (ENSIBS) à Vannes, aide au codéveloppement des start-up locales et des acteurs européens », a ajouté Arnaud Laforge, directeur du site.

Scanner le trafic pour détecter les espions

Une heure durant, le ministre a pu assister à des démonstrations : du chiffrement des données à la détection des espions, appliqués aux domaines militaire et civil. « Les pare-feu, qui servent à se protéger des intrusions extérieures par internet, sont inutiles car plus d'un million d'appareils sont déjà infectés, a expliqué Giuseppe Targia, directeur de la sécurité chez Nokia. Certains pirates peuvent déjà avoir accès à nos machines. Notre solution basée sur la reflectométrie permet de vérifier en continu s'il y a des

irrégularités au sein de notre réseau, juste en observant le comportement de nos appareils ».Adopté par la Banque de France, ce système permet de scanner le trafic automatiquement et de détecter des pertes de données dues à un réseau vieillissant ou à une interception des données, donc à de l'espionnage. Espionnage rendu possible grâce à des dispositifs coûtant moins de 10 achetés sur internet, que les pirates placent dans les boîtiers de fibre optique. Pour s'en protéger, l'équipementier développe un nouveau type de boîtier sécurisé qui sera opérationnel, fin 2017. Autre innovation, le réseau ultra-compact. Ce gros sac à dos permet d'établir des communications fiables en quelques minutes, n'importe où dans le monde. Déjà utilisé par les Marines américains, il peut être fixé à un drone ou à un ballon et bénéficie d'une couverture téléphonique et internet à 70 km à la ronde. En plus de son usage militaire, il sera mis à disposition des ONG ou des pompiers en cas de catastrophe naturelle.

« Comme des anticorps »

« La meilleure défense que nous connaissions, c'est le système immunitaire humain. Alors on s'en est inspiré pour notre cybersécurité : quand il y a un problème, le réseau réagit vite et apprend de ce problème pour s'en prémunir à l'avenir, comme des anticorps », résume Giuseppe Targia. Des innovations qui ont impressionné Jean-Yves Le Drian. « C'est quasiment une cyber armée qui se met en place en Bretagne. Dans le contexte de menace terroriste et avec 50 milliards d'objets connectés d'ici à 2025, il s'agit pour la France de garder de l'avance pour préserver son leadership sur ce domaine. Et Lannion en sera une Breizh cyber valley ».

Le Figaro
Le Conseil national du numérique hausse le ton face au fichier TES
Tuesday, 13 December 2016
Byline: Elisa Braun

Paris - Le fichage des Français au sein d'une base de données unique inquiète l'organe indépendant Non, c'est non. Le Conseil national du numérique (CNNum) reste intransigeant sur le fichier TES, qui permet au gouvernement de regrouper les données personnelles (sexe, couleur des yeux, taille, photo, empreintes digitales, filiation, nationalité...) de près de 60 millions de Français. Le CNNum en avait déjà demandé la suspension le 7 novembre dernier dans une lettre ouverte au gouvernement, où il déplorait les risques de dérives créées par un tel dispositif.

La nouvelle prise de position du CNNum publiée lundi et qui résulte des contributions recueillies par sa plateforme de consultation et d'auditions d'experts, est encore moins tendre avec le gouvernement. Outre la demande réitérée de suspension du fichier, le Conseil préconise dans son rapport l'instauration d'un débat public sur les sujets de l'identité administrative et l'identité en ligne. Il insiste également sur l'«urgence à instaurer une nouvelle gouvernance des choix technologiques au sein de l'État».

Un contre-exemple symptomatique

Au-delà de la polémique, le fichier TES apparaît selon le CNNum comme «le symptôme d'un processus décisionnel qui, en matière technologique, n'intègre pas suffisamment les exigences d'une vision politique de long terme». Au fil des pages du rapport, le Conseil mentionne les nombreux risques de dérives que constitue un tel fichier dans un contexte d'attaques cybersécuritaries accrues. Il recommande d'édicter un cadre général pour ce type de décision, et suggère notamment l'obligation de fournir des études d'impact approfondies et de tenir des débats publics.

L'organe consultatif recommande de renforcerle rôle d'instances spécialisées comme la Commission nationale informatique et libertés (Cnil), la direction interministérielle du numérique et du système d'information et de communication de l'État (Dinsic) et de l'agence nationale de la sécurité des systèmes d'information, l'Anssi.

Une querelle sans fin

Le fichage des Français a rouvert les fractures créées par le projet de loi sur le Renseignement, l'an dernier. Si le fichier TES est censé simplifier les formalités d'obtention et de renouvellement des titres d'identité, ainsi qu'éviter la fraude documentaire, certains opposants ont dénoncé son caractère attentatoire à la vie privée. Dans un contexte d'État d'urgence prolongé et de mesures prises contre le terrorisme, ce fichier TES a aussi été critiqué pour sa potentielle utilisation à des fins de renseignement.

Bernard Cazeneuve - alors ministre de l'Intérieur et à l'initiative du décret - a écarté cette possibilité devant la commission des Lois de l'Assemblée, le 9 novembre. Il n'a en revanche pas su lever les doutes de certains parlementaires, concernant les risques de sécurité liés à la concentration en un même fichier d'autant de données sensibles. Le ministère de l'Intérieur a consenti à rendre optionnel le versement des empreintes biométriques dans la base de données. Le ministère a également saisi la Dinsic (Direction interministérielle du numérique et du système d'information et de communication de l'État) et de l'Anssi (Agence nationale de la sécurité des systèmes d'information) afin d'évaluer le risque d'attaque informatique.

Lors d'une récente audition à la commission des lois du Sénat, les dirigeants de ces deux institutions n'ont pas fait mystère de leur intention d'amender le projet de l'Intérieur. Guillaume Poupard, directeur de l'ANSSI, s'est inquiété des risques géopolitiques: «Que se passerait-il si quelqu'un voulait déstabiliser la France non pas via une attaque très visible, mais en distillant des erreurs de-ci, de-là au sein du fichier?», rappelant que «ce genre d'armes est de plus en plus utilisé dans le cadre de conflits avoués ou pas entre grands États». «Je crois qu'il faut remettre à plat tout cela pour que le débat puisse reprendre sur des fondamentaux plus solides», a plaidé Henri Verdier, directeur du Dinsic. À la différence des deux instances, le CNNum, qui souhaite pour sa part repenser intégralement le fichier TES, reste pour sa part un organe purement consultatif.

La Tribune (France)
Surveillance spatiale : la France reste dans la cour des Etats- Unis et de la Russie

Tuesday, 13 December 2016
Byline: Michel Cabirol

Paris - La direction générale de l'armement a notifié le contrat de modernisation du système de surveillance de l'espace Graves à l'ONERA et à la PME Degreane Horizon. Un enjeu crucial pour la France qui peut ainsi suivre dans l'espace les satellites espions.
Le ministère de la Défense lance la modernisation du système de surveillance de l'espace Graves comme l'avait annoncé La Tribune (lien : http://www.latribune.fr/entreprises- finance/industrie/aeronautique-defense/surveillance-spatiale-la-france- modernise-le-systeme-graves-a-minima-602219.html). La direction générale de l'armement (DGA) a notifié un contrat pouvant s'élever jusqu'à 40 millions d'euros, qui comprend une tranche ferme et des tranches optionnelles, à deux cocontractants : le centre français de la recherche aéronautique spatiale et de défense l'ONERA et la PME électronique Degreane Horizon, spécialisée dans l'acquisition et l'émission de données sensibles. Cette filiale du groupe Vinci était depuis 2003 un des fournisseurs du centre de recherche français sur ce programme. La DGA a toutefois confié à l'ONERA la responsabilité du maintien des performances du système puis de son amélioration.

La tranche ferme de ce programme de rénovation court sur une période de cinq ans (huit ans si on rajoute toutes les tranches optionnelles). Elle représente plus de la moitié de la valeur du contrat, selon le chef de projet du système Graves au sein de l'ONERA, Florent Muller. Le système Graves est essentiellement installé sur trois sites, l'un à Dijon (le site d'émission avec les grande antennes), un autre sur le plateau d'Albion (site de réception) et, enfin, à Lyon Mont-Verdun, où le centre opérationnel de surveillance militaire des objets spatiaux (COSMOS), traite les données du système Graves (exploitation).

Graves, un système de renseignement stratégique

Mis en service depuis 2005 pour le compte de l'armée de l'air, le système Graves (pour Grand Réseau Adapté à VEille Spatiale) est un programme unique en Europe. Seuls les États-Unis et la Russie ont officiellement un programme équivalent alors qu'un cercle très restreint de pays, comme la Chine par exemple, pourraient en posséder un également. A ce jour, il est capable "de cataloguer des objets de la gamme du mini-satellite jusqu'à 1.000 km d'altitude", souligne Florent Muller. Soit un engin de la taille d'une machine à laver.

"Les données générées permettent de calculer à tout instant la position de l'ensemble des satellites suivis", précise-t-il. Actuellement, Graves détecte et catalogue tous les jours plus de 2.500 objets. C'est l'armée de l'air qui assure la mise à jour quotidienne du catalogue. Car pour rester catalogué, un objet doit être détecté tous les jours.

« La France a été le troisième pays au monde, après les Américains et les Russes, à se doter d'un tel système, avait expliqué en juin 2015 dans une interview accordée à la Tribune le PDG de l'ONERA, Bruno Sainjon. L'ONERA a conçu Graves, a piloté sa réalisation et l'a transféré à l'armée de l'air en 2005. Ce programme a notamment permis des échanges de données avec les États-Unis. Et, en avril 2015, cette

coopération s'est renforcée, les deux ministères de la Défense voulant désormais échanger des informations classifiées". »

Ce système de renseignement militaire stratégique, un outil extrêmement précieux pour la France, peut notamment suivre à une altitude de moins de 1.000 kilomètres les satellites espions, qui survolent la France et observent les sites sensibles. Ce qui permet à l'armée de l'air de cataloguer pratiquement tous les satellites espions alliés et ennemis ainsi que d'autres engins spatiaux. "Graves permet de détecter les menaces qui pèsent sur nos propres moyens spatiaux", confirme Florent Muller.

L'armée de l'air a d'ailleurs reconnu avoir identifié en 2012, puis 2013 et, enfin, en 2015, des engins spatiaux qui se sont approchés de satellites militaires français. Ces satellites sont d'ailleurs restés à leur contact pendant une période relativement longue. Très certainement pour les écouter. Il détecte également les vols en formation de satellites. En outre, Graves permet d'éviter d'éventuelles collisions entre des débris spatiaux et les satellites français en les déplaçant le cas échéant.

Enfin, le système concourt à la protection des populations face aux rentrées atmosphériques à risques (engins spatiaux, comètes...). Car plus de 12.000 satellites artificiels et objets divers, dont la taille est supérieure à dix centimètres, orbitent autour de la Terre.

Graves pourrait identifier des micro-satellites

Malgré sa robustesse et sa simplicité, le système Graves, un prototype qui était innovant en 2005, doit être aujourd'hui modernisé, les équipements ayant vieilli. Cette opération de rénovation permettra désormais d'assurer la pérennité de Graves "jusqu'en 2030", estime Florent Muller. Dans ce contexte, la tranche ferme du contrat confié à l'ONERA et à Degreane Horizon comprend en grande partie le traitement des obsolescences du système ainsi que quelques améliorations de ses performances, notamment du calculateur de traitement de signal.

« Certaines performances seront accrues grâce notamment à des interventions au niveau des antennes de réception et du traitement du signal, supportées par un nouveau calculateur", explique l'ONERA dans son communiqué. »

Plus précisément, l'ONERA sera en charge de la rénovation et des améliorations des sites de réception et d'exploitation. La filiale de Vinci modernisera pour sa part à l'identique les systèmes d'émissions en gérant les obsolescences.

Avec les tranches conditionnelles, de nouvelles améliorations du système sont prévues. En parallèle du lancement de la tranche ferme, l'ONERA effectuera des études techniques opérationnelles pour définir quelles pourraient être les options pour améliorer Graves. "A l'issue de ces études, un certain nombre d'options accessibles pourra être ainsi notifié en parallèle de la tranche ferme", confirme Florent Muller.

L'ONERA vise notamment l'amélioration de l'observation d'objets spatiaux plus petits. Et de passer "de façon progressive avec les options les plus complètes" de la détection de mini-satellites (inférieur à 500 kg) à celles de micro-satellites (inférieur à 150 kg). Dans sa nouvelle configuration, Graves détectera beaucoup plus d'objets spatiaux qu'actuellement si les tranches conditionnelles du contrat sont levées.

Un outil de souveraineté

Entre une modernisation a minima et une modernisation plus ambitieuse, le ministère de la Défense n'a pas encore tout à fait tranché en découpant le programme de modernisation de Graves en plusieurs tranches, dont des tranches optionnelles. Cet outil de souveraineté permet pourtant de discuter d'égal à égal - ou presque - avec les États-Unis. Ce qui n'est pas rien et confirme bien que la France est depuis 2005 dans le club très fermé des puissances dotées de capacités autonomes de surveillance de l'espace. Au ministère de la Défense de décider de l'ampleur de cette opération cruciale pour l'indépendance de la France en matière de surveillance spatiale une fois les recommandations de l'ONERA émises.

Développé sous contrat de la DGA, le système Graves est constitué d'un radar bistatique spécifique associé à un système de traitement automatisé qui permet la création et le maintien à jour d'une base de données des paramètres orbitaux des satellites qu'il détecte. Fruit de la collaboration des spécialistes des départements Électromagnétisme et radar (DEMR) et Conception et évaluation des performances des systèmes (DCPS) de l'ONERA, le radar du système Graves a été spécifiquement conçu pour la surveillance de l'espace.

Le Petit Bleu de Lot-et-Garonne
Cybersécurité : la France muscle son arsenal
Tuesday, 13 December 2016
Byline: Journaliste maison

Paris - Le combat numérique va devenir une arme à part entière des armées françaises, aussi bien offensive que défensive, face à une cybermenace qui vise de plus en plus les intérêts vitaux des États. «L'émergence d'un nouveau milieu, d'un champ de bataille cyber, doit nous amener à repenser profondément notre manière d'aborder l'art de la guerre», a déclaré hier le ministre de la Défense Jean-Yves Le Drian, en dévoilant la doctrine des armées françaises en matière de cybersécurité.

Dans un monde de plus en plus interconnecté, les cyberattaques venant d'États, hackers, groupes terroristes ou criminels se multiplient, a relevé le ministre.

Elles peuvent paralyser des infrastructures vitales (réseaux téléphoniques, centrales électriques, transport..) tout comme des cibles militaires en tentant de pénétrer les systèmes embarqués d'aéronefs, bâtiments de guerre ou blindés.

«L'arme cyber peut avoir des effets tout à fait comparables à l'armement plus conventionnel», a averti Jean-Yves Le Drian en inaugurant les nouveaux locaux de DGA Maîtrise de l'information, qui réunit les cyberexperts de la Défense à Bruz (Ile-et-Vilaine) près de Rennes.

Face à ces menaces, les armées verrouillent de plus en plus leurs systèmes d'information - ils sont protégés par des «murailles» et des «patrouilles» qui traquent les intrus - mais intègrent aussi désormais le cyber comme une arme offensive.

«En temps de guerre, l'arme cyber pourra être la réponse, ou une partie de la réponse, à une agression armée, qu'elle soit de nature cyber ou non», a énoncé M. Le Drian.

Concrètement, la France pourra recourir au combat numérique comme à une arme classique de type missile pour riposter à une attaque aussi bien cyber que conventionnelle.

Un commandement des opérations cyber, le CYBERCOM, placé sous la responsabilité directe du chef d'état-major des armées, va être pour cela créé en janvier 2017.

Il disposera d'un état- major resserré qui surpervisera 2.600 «combattants numériques» d'ici 2019.

Le Figaro
20.282 personnes espionnées en un an sur le territoire français
Tuesday, 13 December 2016
Byline: Christophe Cornevin

Paris - Dans son premier rapport d'activité dévoilé mardi matin, la Commission nationale de contrôle des techniques de renseignement (CNCTR) évalue que 47% des personnes surveillées l'ont été dans des dossiers terroristes et 29% au titre de la «lutte contre la criminalité organisée» ainsi que de la «prévention des violences collectives».
Entre le 3 octobre 2015 et le 2 octobre dernier, quelque 20.282 personnes ont été espionnées par les services français. En dévoilant mardi matin son premier rapport d'activité, la Commission nationale de contrôle des techniques de renseignement (CNCTR) a évalué le nombre d'hommes et de femmes qui ont fait l'objet d'une surveillance. Celle-ci passe par l'emploi de la technique la moins intrusive, à savoir l'obtention des «fadettes» (facturations détaillées) de la personne ciblée jusqu'à des moyens plus lourds, telles que la sonorisation ou l'installation de moyens vidéo dans les domiciles en passant par les interceptions de sécurité, la géolocalisation, l'accès en temps réel aux données de connexion» ou encore l'emploi - encore parcimonieux - des «Imsi catchers» permettant de siphonner à distance les données de connexion des téléphones mobiles.

Les algorithmes, c'est-à-dire la «boite noire», tant contestée censée assurer un recueil massif de données, ne devraient être mis en ouvre qu'au printemps prochain. «Pour l'heure, ils n'ont pas pu être mis en place pour des raisons de moyens techniques», précise-t-on à la CNCTR.

47% dans les radars de l'antiterrorisme

Au nombre de ceux ayant «fait l'objet d'une technique de renseignement au moins», le rapport de la CNCTR révèle que «9624 personnes, soit 47% du total, ont été surveillées au titre de la prévention du terrorisme» et que 5848 autres, soit 29% du total, ont été ciblées dans des dossiers de lutte contre la criminalité organisée ainsi que «la prévention de violences collectives de nature à porter gravement atteinte à la paix publique».

La CNCTR, qui se dit «particulièrement vigilante sur ce point», considère que «cette finalité ne saurait être interprétée comme permettant la pénétration d'un milieu syndical ou politique ou la limitation du droit constitutionnel de manifester ses opinions, y compris extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré.» Nombre d'observateurs y ont vu une disposition visant les zadistes mais aussi les no-borders, les blacks blocks ou encore les hooligans.

Les autres 24% de personnes placées dans les radars des services, qu'ils soient Français ou étrangers, ont été soupçonnés de porter atteinte à «l'indépendance nationale, l'intégrité du territoire et la défense nationale», d'espionnage industriel ou encore d'être liés à la «prolifération des armes de destructions massives».

8538 avis sur des demandes d'interceptions de sécurité

La démarche, tout à fait inédite dans le panorama feutré de l'espionnage, ne permet «aucun point de comparaison avec l'étranger», précise le conseiller d'État Francis Delon, président de la CNCTR qui, en aparté, ne se dit «pas particulièrement surpris» par le chiffre.

Cette instance indépendante, qui bénéficie d'un budget de 2,9 millions d'euros, vérifie la validité des techniques déployées de la DGSE, de la DGSI, de Tracfin ou encore de la Direction du renseignement militaire.

Depuis le 3 octobre 2015, la CNCTR a rendu 8538 avis sur des demandes d'interceptions de sécurité, contre 7703 l'année précédente. Le nombre des géolocalisations en temps réel a quant à lui bondi de 87% pour atteindre les 2127 demandes en 2016. Observant dans son rapport que «la prévention du terrorisme a, pour la première fois, été le fondement légal le plus fréquemment invoqué», la CNCTR ne constate cependant aucune explosion de la surveillance liée à la menace islamiste.

Composée de neuf «sages» - quatre hauts magistrats, quatre parlementaires et un expert en Télécoms - et d'une secrétaire de 17 personnes dont deux ingénieurs, elle s'est réunie de manière collégiale à 180 reprises à raison de trois fois par semaine pour examiner des cas individuels et mener des dossiers de fonds. Au terme des examens, la CNCTR a retoqué 6,9% des demandes.

New York Times
G.O.P. Feud Looms as Leaders Back Russia Inquiries
Tuesday, 13 December 2016
Byline: Jennifer Steinhauer

Washington - The top two Republicans in Congress said on Monday that they supported investigations into possible Russian cyberattacks to influence the American election, setting up a potential confrontation with President-elect Donald J. Trump in his first days in office.
"Any foreign breach of our cybersecurity measures is disturbing, and I strongly condemn any such efforts," said Senator Mitch McConnell, Republican of Kentucky and the majority leader, adding, "The Russians are not our friends."

Mr. McConnell's support for investigating American intelligence findings that Moscow intervened in the election on Mr. Trump's behalf could presage friction between the Republicans who control Congress, and who have long taken a hard line against Russia, and the president-elect, who has mocked the findings.

Mr. McConnell also went out of his way to address Mr. Trump's claim that the C.I.A. could not be trusted because of flawed intelligence before the Iraq war.

"Let me say that I have the highest confidence in the intelligence community," Mr. McConnell said, "and especially the Central Intelligence Agency. The C.I.A. is filled with selfless patriots, many of whom anonymously risk their lives for the American people."

The top Republican in the House, Speaker Paul D. Ryan of Wisconsin, said he supported a continuing investigation by Representative Devin Nunes of California, the chairman of the House Intelligence Committee. In a statement, Mr. Ryan said: "As I've said before, any foreign intervention in our elections is entirely unacceptable. And any intervention by Russia is especially problematic because, under President Putin, Russia has been an aggressor that consistently undermines American interests."

Congressional Republicans announced their support for inquiries after Mr. Trump railed for much of the weekend against the intelligence findings. But their remarks, especially Mr. Ryan's, were far from fiery, reflecting both a fear of offending Mr. Trump, who has taken many positions against traditional Republican orthodoxy, and the Republicans' belief that Democrats have selectively leaked intelligence information for political gain.

Critics from both parties are questioning Mr. Trump's apparent choice of Rex W. Tillerson, the chief executive of Exxon Mobil, as secretary of state, particularly because of his longstanding business connections with Russia and his close relationship with President Vladimir V. Putin, whom he has known for two decades. Mr. Trump said in a Twitter post on Monday night that he would make a formal announcement on the job on Tuesday morning.

Senators Lindsey Graham of South Carolina and Marco Rubio of Florida, both Republicans, have expressed concern about the reports of cyberattacks, as have numerous Democrats. But Mr. Rubio, in an apparent reference to Mr. Tillerson, went a step further on Monday, writing on Twitter, "Being a 'friend of Vladimir' is not an attribute I am hoping for from a #SecretaryOfState."

Mr. McConnell said the Senate investigation would be led by Senator Richard M. Burr, Republican of North Carolina, the chairman of the Intelligence Committee. Senator John McCain, Republican of Arizona, the chairman of the Armed Services Committee, will add a subcommittee to look into cyberattacks, led by Mr. Graham.

"The first thing we want to establish is, 'Did the Russians hack into our political system?'" Mr. Graham said in an interview on Monday. "Then you work outward from there. I have a high degree of confidence Russia did this."

Mr. Nunes, a member of Mr. Trump's transition team, said in a statement that the Intelligence Committee had been "conducting vigorous oversight of the investigations into election-related cyberattacks."

Mr. Nunes also noted that his committee would be scrutinizing the review of the Russian effort to influence the election ordered last week by President Obama.

Democrats have used the latest intelligence findings to renew their calls for an urgent inquiry. John D. Podesta, Hillary Clinton's campaign chairman, demanded on Monday that all information about Russia's meddling be declassified, and that the Obama administration explain what it knows about the hacking and when it knew it.

"We now know that the C.I.A. has determined Russia's interference in our elections was for the purpose of electing Donald Trump," Mr. Podesta wrote in a statement. "This should distress every American. Never before in the history of our republic have we seen such an effort to undermine the bedrock of our democracy."

Three Senate Democrats -- Benjamin L. Cardin of Maryland, Dianne Feinstein of California and Patrick J. Leahy of Vermont -- called on Monday for the creation of an independent, nonpartisan commission to comprehensively investigate allegations of Russian interference in the 2016 election.

But Mr. McConnell stopped short of calling for a special select committee, saying that the Senate Intelligence Committee was "more than capable of conducting a complete review" of the matter.

While he stopped short of saying whether he agreed that Russia had interfered in the election in support of Mr. Trump, Mr. McConnell said, "We need to approach all these on the assumption the Russians do not wish us well."

Mr. McCain was less equivocal, saying Monday that there was "no doubt about the hacking" by Russian intelligence services. He called the hacking of the Democratic National Committee and related accounts "another form of warfare" in an appearance on "CBS This Morning" with Senator Chuck Schumer of New York, the incoming Democratic leader.

And one week before the Electoral College meets to ratify Mr. Trump's election victory, 10 electors have demanded their own intelligence briefing on Russian efforts to elect Mr. Trump.

For his part, Mr. Trump was dismissive of the intelligence findings and suggested that Democrats were simply stirring controversy. "Can you imagine if the election results were the opposite and WE tried to play the Russia/CIA card. It would be called conspiracy theory!" Mr. Trump said in a Twitter post on Monday.

The White House press secretary, Josh Earnest, said that the administration would support a congressional review. He also rejected the notion that the administration had failed to adequately highlight the Russian efforts before the election, saying it had extensively briefed Congress all year about Russian electoral meddling.

"There has been intensive cooperation between the intelligence community and other national security agencies, and members of Congress in both parties, both before and after the election," Mr. Earnest said. "The briefings have been provided in a variety of settings, both classified and unclassified."

Even beyond the conclusions of the intelligence community, Mr. Trump's campaign had widely known and extensive ties to the Russian government. A campaign manager, Paul Manafort, had worked for the Russian-backed government in Ukraine, and Mr. Trump's choice for national security adviser, Lt. Gen. Michael T. Flynn, had consulted for a Russian-backed media group, Mr. Earnest noted.

Mr. Earnest said that Congress had a "special responsibility" to investigate the ties between the Trump campaign and the Russian government, because those connections were widely known before the election. He added that, for Capitol Hill Republicans, how to "reconcile their political strategy and their patriotism is something they're going to have to explain."

Wired
Trump Ignoring US Intelligence Creates Risks Beyond Russian Hacking
Monday, 12 December 2016
Byline: Andy Greenberg

New York - Observers and alumni of America's intelligence community have already fretted over Donald Trump's impending control of the world's most powerful spy agencies. They've worried that he could abuse their heady surveillance capabilities, turn them on his personal enemies, revamp the NSA's mass surveillance programs, and strip away domestic privacy protections once in charge. But before Trump

has even taken office, he's already found a less expected way to abuse the US intelligence community: Ignore, contradict, and insult it.
Trump's relationship--or lack thereof-- with US intelligence agencies isn't just a cause for political spectacle. According to national security experts and former intelligence agency staffers, it could have serious consequences that go well beyond the current dispute over Russian hacking.

The Russia Rift

On Friday, the Washington Post and New York Times reported that the CIA has confirmed that the Russian government repeatedly hacked and leaked Democratic Party documents throughout the presidential election season with the express intention of aiding Trump's campaign. That conclusion goes a significant step beyond earlier intelligence reports that had merely pinned the attacks on the Kremlin without naming its motive.

In response, the Trump transition team offered a brusque rejection of that finding: "These are the same people that said Saddam Hussein had weapons of mass destruction," read the Trump team's statement.

That abrupt dismissal of the intelligence community's findings follows months of Trump's assertions that no one can know the source of the last year's long series of political hacks--despite a publicly released report from the Office of the Director of National Intelligence and the Department of Homeland Security stating that Vladimir Putin's state- sponsored hackers were behind those breaches. "It could be some guy in his home in New Jersey," Trump maintained in a Time interview earlier last week.

The remarks build on what may be the most troubling recent revelation of all, that Trump has declined the traditional daily intelligence briefing given to presidents and presidents-elect. Instead, he receives the briefing only about once a week. "I get it when I need it," he told Fox News Sunday. "You know, I'm, like, a smart person."

That dismissal and disregard of the intelligence agencies' fact-finding represents a disturbing potential preview of the next four years, say former members of the US intelligence community who spoke with WIRED. They worry that it threatens to politicize the intelligence community's work, pushing it toward conclusions that will please the president rather than inform him. They say the growing rift demoralizes staffers, leading to a loss of valuable talent, and that it could leave the commander-in-chief himself dangerously ignorant of crucial world events.

Susan Hennessey, a former NSA lawyer who is now with the Brookings Institution, says that since Trump was elected, she's spoken with former colleagues who are still in the intelligence community who have been "stunned" to hear Trump's repeated rejections of their findings. "It's not outrage, although that might be under the surface," she says of her former colleagues' response. "It's real uncertainty and a sense of fear...shock, bewilderment, wondering what's going to happen next."

Playing Politics

Trump's kneejerk comparison of the Russian hacking report to the faulty intel on Saddam Hussein's weapons of mass destruction takes that dismay to another level, says one former CIA official who helped to write the president's daily briefing under both Obama and Bush. "We've never seen something like this before. It's pretty ballsy," says the former agency official, who requested anonymity because he's not authorized by his current employer to speak about political issues. "From dismissing the briefings to dismissing the current assessment on the Russia stuff, it seems like he's still in campaign mode. He's politicizing the intel, and that's a problem."

"Every administration has problems with some intelligence," says Patrick Skinner, a former CIA official under Bush and Obama who now works for the security consulting firm the Soufan Group. "But it really shouldn't be public. The open disdain Trump has shown for the agencies is unprecedented."

Trump's transition team didn't respond to WIRED's request for comment.

To be fair, Trump isn't the only skeptic of the intelligence agencies' findings. Neither the leaked CIA assessment that Kremlin hackers were motivated to help Trump nor the intelligence community's October report attributing the attacks to Russia have been backed up with published evidence. That's led Democratic members of congress Elijah Cummings and Eric Swalwell to demand a commission to independently investigate the hacking incidents. President Obama has directed intelligence agencies to conduct a renewed investigation into the attacks. And Republican Senators John McCain and Lindsay Graham joined with Democrats Chuck Schumer and Jack Reed to call for a congressional investigation into the hacker intrusions, splitting with Trump and other Republican leaders who have ignored or dismissed the Russian hacking reports.

In an interview on the CBS show Face the Nation Sunday, Senator McCain clarified that he doesn't doubt Russia was the source of the breaches of targets like the Democratic National Committee and the Democratic Congressional Campaign Committee, but still wants to better understand the motive of those attacks, and whether they targeted Republicans, too. What he doesn't dispute is that Russia was the source. "Now whether they intended to interfere to the degree that they were trying to elect a certain candidate, I think that's the subject of investigation," McCain said. "But facts are stubborn things. They did hack into this campaign."

Trump's doubt of the intelligence agencies' findings isn't the first sign that the divisiveness of the last year's presidential campaign has led to new, partisan distrust of the intelligence community's work, argues Dave Aitel, a former NSA staffer who now runs the security firm Immunity. That doubt had already surfaced with FBI director James Comey's public statements about the bureau's investigation of Hillary Clinton's private email server. The Clinton campaign and Democratic leaders have criticized Comey's behavior, accusing him of influencing the electoral process by writing a letter to Congress about new emails that surfaced in that investigation just weeks ahead of election day. "Our intelligence community has become a political football, and that's something that should never occur," says Aitel. "You need to have trust, and we don't have trust."

Broader Threats

Aitel says that lack of confidence in intelligence agencies' findings and politicization of their work has left his former colleagues increasingly "jaded." And he says that problem of low morale, already sunken after public response to the revelations of NSA leaker Edward Snowden, could lead to a dangerous brain drain from key agencies. "They don't complain, they don't whine to the press, they just leave," argues Aitel. "Then you get talent shortfalls, and then you get mission failures, which are bombs blowing up in American cities."

Compounding those issues are fears that Trump will continue to ignore his own intelligence apparatus, making uninformed decisions on the world stage, says ex-CIA officer Skinner. Some members of Trump's transition team have reportedly accepted daily intelligence briefings, including his pick for defense secretary, General James Mattis, and vice-president elect Mike Pence. But a president who wields ultimate executive power without that information could be dangerous, says Skinner. "If you close your eyes, the threat is still there: North Korea still exists, ISIS still exists," says Skinner. "These things are complex. You can't counter North Korea with gut feelings."

The rejection feeds back into the morale issue as well. "There's a firm belief in the intelligence community that the president having this information is a really important thing," says ex-NSA lawyer Hennessey. "When you have a boss essentially saying they don't believe or value your work--an outright rejection based on absolutely no evidence--there's a profound sense of uncertainty."

Beyond Trump's specific rejection of any inconvenient finding, Hennessey says it's that larger dismissal of the intelligence community that's most troubling. "If an intelligence agency produces a piece of evidence that's ignored, people can be killed," she says. "The consequences could be as dire as you can possibly imagine."

Radio Free Europe
Cyberattacks On Finance Ministry, Treasury
Monday, 12 December 2016
Byline: Christopher Miller

Kyiv - Ukrainian authorities are still looking for the culprits nearly a week after troublesome cyberattacks against official financial institutions that appeared to be designed to inflict maximum chaos on end- of-the-year payments.
But the head of staff of the Ukrainian Security Service (SBU) identified the so-called malware used in the December 6 attack as the same disruptive software employed in an unprecedented incident a year earlier, blamed on Russia, that cut off power to hundreds of thousands of homes in Ukraine.

Hundreds of thousands of hryvnyas' worth of remittances were delayed or stopped completely over the course of two days after hackers knocked the websites and payment systems of the Ministry of Finance, State Treasury, and pension fund offline, according to statements posted to those sites and local reports.

The National Police are leading the investigation and have discussed the case with the SBU, Oleksandr Tkachuk, chief of staff of the SBU, told RFE/RL on December 12.

The Finance Ministry, which described the incident as a "coordinated professional hacking attack," also claimed the attack had damaged its network equipment.

Tkachuk confirmed that "some data was destroyed and access to networks was blocked."

He said authorities were not prepared to discuss many details publicly because it would take time to fully assess them, adding that attribution in the cybersecurity sphere is a tricky business.

Tkachuk said the attack appeared to bear some similarity to a December 2015 attack against the Prykarpattyaoblenergo power company in Ukraine's western Ivano-Frankivsk region that cut power to hundreds of thousands of homes.

Critical Infrastructure

Ukrainian officials blamed that cyberattack on Russia and speculated that it might have been retaliation for Kyiv cutting off electricity one month earlier to Crimea, which Russia seized from Ukraine in early 2014.

But experts at the time warned that the greater message might be that hackers had the power to shut down critical infrastructure -- something that cybersecurity experts had long feared but never seen in practice.

Elizabeth Sherwood-Randall, a deputy secretary at the U.S. Department of Energy, also blamed Russia for the December 2015 cyberattack.

In that case, the hackers used malicious software called KillDisk, which deletes or overwrites data in system files, causing computers to crash.

KillDisk was also used in the December 6 attacks, the SBU's Tkachuk told RFE/RL.

Relations between Kyiv and Moscow soured after Russia forcibly annexed Crimea in March 2014, and Russia has been accused by Kyiv and Western powers of backing a separatist conflict in eastern in Ukraine that has killed more than 9,750 people.

Kyiv has on several occasions blamed Russia for cyberattacks -- including one on Ukraine's election system ahead of the presidential vote in May 2014 -- that it claims are part of Moscow's greater "hybrid war," a military strategy that combines conventional warfare, irregular warfare, and cyberwarfare.

CBC News
Federal government's Canada.ca project 'off the rails'
Tuesday, 13 December 2016
Byline: Staff reporter

The federal government's bid to merge 1,500 departmental and agency websites into a single site, Canada.ca, is a year behind schedule and almost 10 times over budget. And experts warn it is on track to be another failed government IT project, like the Phoenix pay system.
"It's gone off the rails. It's a disaster," said one government source with knowledge of the project who spoke on condition of anonymity.

CBC spoke with a number of government workers who are also familiar with the project in different departments and they all expressed similar evaluations.

The Canada.ca initiative was launched in 2013 with the goal of making it easier for people to find and use government information online. A $1.54-million contract for a new content management system, where all government websites would be moved, was awarded to Adobe in 2015.

The original deadline to have all active web content moved to the single portal was this month. But in June, it was pushed back to December 2017, which was the initial deadline for the migration of all archived content.

The contract with Adobe is now above $9.4 million, according to government figures.

The actual migration of the websites is up to the departments themselves and is to be done within existing budgets and staffing. Since 2015, eight of the largest departments have budgeted or spent more than $28 million on this project.

Those departments include: Employment and Social Development; Immigration, Refugees and Citizenship; Health; Environment; Canada Revenue Agency; National Defence; Fisheries and Oceans; and Global Affairs.

According to the government, only 10,000 web pages have been moved to date. There are more than 17 million Government of Canada web pages in total.

"If it's cost them already 10 times their existing budget to migrate only 0.05 per cent of the content for the Government of Canada, we're talking about it ultimately costing hundreds of millions of dollars. It's not a small price ticket," said Mike Gifford, CEO of Ottawa-based web development company Open Concept, who has written articles criticizing the government's approach to Canada.ca.

New deadline 'impossible'

Based on the current timeline, Gifford said he thinks the December 2017 deadline is unrealistic. He's not alone.

"Absolutely impossible to achieve," said Timothy Lethbridge, who teaches software engineering and computer science at the University of Ottawa. "And I'm sure many people inside the project know it."

There's also a good chance of the project failing altogether, Lethbridge said, because large IT projects are exponentially more complex. "As a project of this size gets bigger, the probability of failure goes up."

If the government spread the work out over a number of years and spent a billion dollars, it might be able to make the migration a success, Lethbridge said. But he questioned whether taxpayers would be getting value for money at that point.

This is not the first large government IT project to run into problems.

The government will spend at least $50 million this year to try to fix problems with the new Phoenix pay system, which has seen thousands of public servants underpaid, overpaid or not paid at all.

The initiative to transform the government's email system has been stalled for months because of problems with new software.

And Shared Services Canada, the agency created in 2011 to modernize IT-related services in government, has been slammed for its many missteps, particularly by the auditor general.

"There's a trend," said Robin Galipeau, managing partner of OpenPlus, a content architecture company. "There's definitely something going on there. Large renewal projects in IT are failing in government."

OpenPlus, along with Dell and Microsoft, submitted a bid to create the new CMS for Canada.ca.

Ministers refuse to comment

According to OpenPlus Chief Technology Officer Joel Brockbank, the federal government continues to erroneously believe there are one-size-fits-all software solutions for its IT goals.

"There never is," he said. "It's like your cross-trainer running shoes. It's not good for anything that you do."

The key to not having large IT projects fail, Brockbank said, is to simply not do them. Instead, such projects should be done in stages or "bite-size chunks."

None of the ministers whose departments are involved in the Canada.ca migration project were willing to comment when contacted by CBC News.

Treasury Board President Scott Brison, Social Development Minister Yves Duclos and Public Services and Procurement Minister Judy Foote all declined requests. As did Michel Laviolette, the director general of Service Canada, and John Messina, the federal government's chief information officer.

"That tells me they have something to hide," said Debi Daviau, president of the Professional Institute of the Public Service of Canada, the union representing many of the government's IT workers.

"If they're unwilling to be transparent about the decisions they make, that calls those decisions into question."

Yonhap News Agency
Military investigators raid cyber command in hacking probe
Tuesday, 13 December 2016
Byline: Staff reporter

Seoul - Military investigators have raided South Korea's cyber command as part of their investigation into the first hacking of the command's intranet that is being blamed on North Korea, military officials said Tuesday.
"The Defense Security Command is thoroughly looking into how the cyberattacks took place, what confidential information has been leaked and if there was any professional negligence," a military official told Yonhap News Agency.

He confirmed that military prosecutors were overseeing the raid while the Defense Security Command was collecting documents in a raid to the cyber command on Tuesday.

In September, the defense ministry recognized that a total of 3,200 computers, including 700 linked with the intranet, were contaminated with malware a month after the latest cyberattack took place.

The ministry found in October some military documents were hacked while refusing to provide details. The computer used by Defense Minister Han Min-koo also turned out to have been compromised.

Last week, the ministry said the IP addresses linked to the attack were traced to a location in China that has been used by North Korean hackers.

As one of the military's two integration servers was jointly linked to the internet and the intranet, it allowed the hackers to gain access to the intranet, it said.

The cyber command separated the affected server from the whole network to avoid the spread of viruses in October, two months after the initial hacking attempt was made in August.

It marked the first time that the data of South Korea's cyber command has been compromised. South Korea set up the command in January 2010 as part of its efforts to counter external hacking attempts on the country's military.

North Korea -- which has thousands of cyberwarfare personnel -- has a track record of waging cyberattacks on South Korea and the United States in recent years, though it has flatly denied any involvement.

Yonhap News Agency
Acting President Hwang redoubles calls for robust cyberdefense
Tuesday, 13 December 2016
Byline: Song Sang-ho

Seoul - South Korea's Acting President and Prime Minister Hwang Kyo- ahn on Tuesday redoubled calls for robust cyberdefense against North Korea, saying cyberwarfare with the provocative state has already begun.
Following a suspected hacking by Pyongyang of Seoul's cybercommand intranet, Hwang and South Korean security officials have repeatedly stressed the need to prepare against the North's surreptitious cyberattacks which could be as devastating as physical military strikes.

"As evidenced in the recent hack of the (South's) defense ministry, North Korea has attempted to mount cyberattacks on major government facilities, and (this shows) cyberwarfare has already begun," he said during the first regular Cabinet meeting since he took over as acting president last Friday after President Park Geun-hye was impeached over a corruption scandal.

"Related ministries, including the ministries of defense and future planning, must devise thorough measures to prevent any recurrence (of hacking incidents) and take special caution not to allow any minor mistakes to threaten our security," he added.

The defense ministry said last week that a total of 3,200 computers, including 700 linked with the intranet, were infected with malware in August. The computer used by Defense Minister Han Min-koo was also affected, officials said.

In recent years, Seoul has been pushing to bolster its cyberdefense capabilities as Pyongyang has launched a host of attacks on South Korean corporate and government websites by mobilizing its specially trained personnel, including those based in China and other foreign countries.

The reclusive regime has denied responsibility for its cyberattacks including the latest one, upbraiding Seoul for "fabricating" claims about online attacks.

Hwang, in particular, ordered the government to check the nation's financial, traffic, broadcasting and energy networks, and other major national facilities to verify if they are exposed to any cybersecurity threats.

On the economic front, Hwang said that the country's economic fundamentals remain strong as Seoul has striven to maintain a consistent policy despite political uncertainties sparked by the corruption scandal.

The acting president also urged economic officials to keep close tabs on the financial and foreign exchange markets, as he pointed to the potential negative ramifications from a possible United States interest hike.

"I call on you to closely monitor the market situation and respond to it in a timely and resolute manner," he said.

Hwang went on to urge the Cabinet ministers to make concerted efforts to protect the socially vulnerable, including children from low-income families and senior citizens, particularly during the winter season.

Later in the day, Hwang held a luncheon meeting with senior professors and journalists as part of his efforts to solicit their views on ways to bring the nation, gripped by the scandal, back on track.

Hwang renewed his pledge to focus on forestalling any government vacuum and restoring stability in state governance.

Meanwhile, Hwang stepped up efforts to tackle a series of pending issues that can affect the wellbeing of citizens, as he strives to project an image of a trustworthy -- albeit temporary -- leader.

On the day, he directed Agriculture Minister Kim Jae-soo to convene a meeting of senior government officials and civilian experts, dedicated to containing avian influenza (AI), on a daily basis to better tackle the highly contagious virus.

He also instructed top officials from provincial governments to hold their own daily meetings separately to help stem the spread of the bird flu that has ravaged chicken farms across the country since mid-November.

Visiting police stations in Seoul, he called on officers to tighten their crackdown on crimes targeting women and other vulnerable individuals, particularly in the nighttime. He also ordered the police to

"root out" violent or drunk drivers, saying they could cause large-scale accidents involving many casualties.

Regarding the heavy snowfall expected for some parts of the country between Tuesday night and Wednesday afternoon, Hwang directed related ministers to take the necessary steps to minimize any possible damage or inconvenience to citizens.

Japan News
Attacks by Anonymous against Japan rising
Tuesday, 13 December 2016
Byline: Staff reporter

Cyber-attacks against Japan apparently carried out by international hacker group Anonymous have been increasing since September.
Last autumn, a number of government websites and other sites came under attack. However, the recent attacks are different from sophisticated cyber-attacks that aim to steal information. Experts call for people to respond calmly by taking necessary steps in advance without fearing them too much.

Late at night on Sept. 3, the website of the Hiroshima National Peace Memorial Hall for the Atomic Bomb Victims became inaccessible. Shortly after, a group saying it was Anonymous and opposed to dolphin hunting and other issues posted a statement online claiming responsiblity.

An official at the memorial hall said in bewilderment, "We have nothing to do with dolphin hunting."

It is believed a series of Anonymous attacks called Operation Killing Bay started around 2013 in protest against Japan's whale hunting and the annual dolphin hunts in Taiji, Wakayama Prefecture, in September.

Last year, to protest against the dolphin hunting in Taiji, distributed denial of service (DDoS) attacks were launched against government offices websites and infrastructure operators such as airports. DDoS attacks are aimed at rendering websites and other online services unavailable by sending a huge amount of data to the server.

According to police, the number of cyber-attacks Anonymous is believed to be involved in has grown since September. There were no cyber- attack-related website problems from May to August, but 29 incidents were confirmed in September, followed by 26 in October. From Nov. 1 to Nov. 27, there were 53 cases, bringing the total from September to Nov. 27 to 108.

In comparison, incidents ranged between the 10s and 20s each month from September to November last year, but rose to 56 in December.

"Their aim is not to make websites unavailable, but to promote their presence," said Nobuhiro Tsuji, senior security researcher at SoftBank Technology Corp.

This year, the targets of the attacks have conspicuously been small organizations and shops such as izakaya Japanese pubs, and groups totally unrelated to dolphin hunting. "The hackers could be different from last year, and their resources could be smaller," Tsuji said.

'Respond coolly'

When Anonymous started around 2006, it advocated the establishment of the freedom of the internet and made political appeals through legally permitted activities such as street demonstrations.

Currently, however, Anonymous tends to carry out cyber-attacks with the aid of unknown individuals who respond to invitations on Twitter and other websites. Participants are increasingly committing cyber-attacks for fun.

The website of the Kasumigaura river office of the Land, Infrastructure, Transport and Tourism Ministry came under attack in 2012. Anonymous is believed to have confused Kasumigaura with Tokyo's bureaucratic district of Kasumigaseki. The incident was indicative of the group's sloppy management.

Anonymous' main attack method, DDoS, can be committed without significant expertise. Basically, there is no way to defend against such attacks. It is a matter of waiting for an attack to cease, although measures have recently been developed to mitigate damage.

"Compared to cyber-attacks aimed at stealing information, DDoS attacks are not so sophisticated. In most cases, the websites attacked went down and that was it," said Masakatsu Morii, a professor at Kobe University specializing in information and telecommunications engineering.

Some observers point out that such cyber- attacks could increase ahead of the 2020 Tokyo Olympics and Paralympics. Morii said, "It is important that companies and organizations take necessary measures calmly. If they are attacked, they should respond coolly without overreacting."

The Australian Financial Review
Lone wolves and data dumps a problem (Canada)
Tuesday, 13 December 2016
Byline: Jonathan Porter

Sydney - Constant reconnaissance probes by nation states, attacks by computer network robber barons and lone wolves and data dumps from disgruntled workers - that is digital Australia's bleak picture painted for a cyber security forum in Sydney recently.
And without constant vigilance and fine-tuning of our cyber defences, the problem will only get worse.

"A lot of nation states and militaries are investing in capabilities that can be used to target utilities; power, water resource and energy providers," Major-General Stephen Day, former head of cyber at the Department of Defence who was the inaugural head of the Australian Cyber Security Centre, told the Australian Computer Society Cyber Forum in Sydney.

"There is no question reconnaissance is going on right now."

The glimpse behind the curtain at Australia's cyber defenders came during the question and answer period at the end of the forum, attended by some of the world's leading experts in the field.

An attendee put to the panel that an emerging risk was not lone wolf attackers "but of a state-sponsored cyber-attack sometimes from friendly countries we consider allies" and asked what was being done to mitigate the risk.

Day agreed that state-sponsored attacks were a "significant risk", particularly if people looked down the track a few years.

He added that there was also a "significant challenge with organised crime".

"We looked at the sectors that mattered most to our nation either from an economic prosperity perspective or from a national security perspective and put them in a priority order and looked at those sectors that were likely to be targeted by organised crime or by nation states and then we directed our organisational energy to help those sectors.

"So if, for example, you are in the utilities sector or critical infrastructure sector you will have had more experience of government contacting and working with you than the retail sector or the banking sector where you are likely to meet the police more than the national security base."

Victorian minister for Small Business, Innovation and Trade Philip Dalidakis said that while Day's statements were "sexy" and would generate headlines "the one thing everyone in the room has to be extremely cognisant of is that the overwhelming majority of attacks occur from within".

"Yes, we need to be able to stop attacks from the outside of the firewall but the fact of the matter is the two greatest attacks we have seen of data theft from inside were from Bradley Manning and (Edward) Snowden," he told the forum.

"There are a range of companies that will swear black and blue that they have got algorithms that will help flag anomalies within the system - people accessing certain types of data that they haven't done for ages - (or) if you have got your networks categorised under different security levels - people trying to access levels [other] than their security classification. Ultimately it comes down to people and training,

each organisation has to have people who are trained appropriately who can deal with it when - it's not a matter of if - it occurs."

Some of the greatest risks in organisations were the IT divisions themselves, he says.

"People who have the administrative access rights and passwords are sometimes the ones who are undertaking a whole range of activities that people on the rest of the network are banned from doing - including downloading huge amounts of illegal data. Which is, of course, one of the ways people get in.

"So don't go away from this thinking that if you focus on external you are protected because your internal [network] is 80 per cent of your risk."

On the intelligence side, he said he could speak more freely than other panel members because he was not a representative of the federal government.

Dalidakis said the nation was well served by the Five Eyes agreement on signals intelligence sharing with the US, Canada, New Zealand and the United Kingdom.

Fellow panel member Sandra Ragg, assistant secretary for cyber policy in the Department of the Prime Minister and Cabinet, said the nation did need to improve its cyber defences.

"The first thing we can do is improve our cyber defences.

"People focus on state- sponsored threats but cybercrime is a huge piece of the threat to our economy."

Politico
Is Trump's Twitter account a national security threat?
Tuesday, 13 December 2016
Byline: Nahal Toosi

Washington - Donald Trump has years of experience launching Twitter wars. But now, as he prepares to take the highest office in the country, there are growing fears that his tweets could spur a genuine national security crisis.
Intelligence and defense specialists believe the president-elect's use of the popular and powerful social media network is already being used by foreign agencies to analyze his personality, track his habits and detect clues about what to expect from a Trump-led American government.

And that's just based on what Trump writes on Twitter. It's not even counting the vulnerabilities that could arise if overseas hackers invade his phone and digital accounts.

"We've never had a president that's shared so much of themselves, not just what they're saying, but their psychological ticks in such an overt manner, and you can be sure that foreign actors are studying that, too," said P.W. Singer, a defense expert and co-author of "Cybersecurity and Cyberwar." "We're beginning to see what excites him, what angers him, what sets him off. We've never had this ability to read so much on what a president is thinking."

Trump, who prefers mobile phones to computers, is highly attached to his Twitter account (@realDonaldTrump), using the platform to share his thoughts deep into the night. Days after his stunning election victory, he was reportedly worried he would not be able to keep his Android phone upon reaching the Oval Office, suggesting he plans to keep tweeting even after he's sworn in. During his first sitdown interview as president-elect, he told "60 Minutes" that he would be "very restrained" in his Twitter use while in office, before using his account to rail against The New York Times the same day the interview aired.

Trump's following of 17.2 million is likely to expand as he takes office, and his disdain for the mainstream media may bolster his desire to keep up his direct outreach to the public through Twitter.

For the most part, the president-elect has used Twitter to comment on people and institutions on the domestic front, or to defend himself against their criticisms. His tweets are believed to have even influenced the stock market, including on Monday, when his criticism of Lockheed Martin's F-35 program was followed by a drop in the aerospace company's market value. On several occasions, however, Trump has ventured into the international realm.

In recent days, amid lingering Chinese anger over Trump's decision to break U.S. protocol and speak directly to the president of Taiwan, Trump, using two tweets, wrote: "Did China ask us if it was OK to devalue their currency (making it hard for our companies to compete), heavily tax our products going into.. their country (the U.S. doesn't tax them) or to build a massive military complex in the middle of the South China Sea? I don't think so!" On Monday, he used Twitter to sow doubts about claims he's not hard enough on Russia.

Granted, foreign intelligence agencies will likely look at all of Trump's public utterances -- his speeches, interviews, written press releases -- as well as those of his aides to try to understand one of the more unusual men ever to win the White House. (U.S. intelligence analysts do similar studies of foreign leaders, especially in countries such as Iran and North Korea, whose governments are considered hostile and with whom U.S. communication is limited.)

But so far, at least, Twitter has proven one of the purest distillations of Trump around -- a raw version of a businessman-turned-politician keen on ignoring the traditional conventions of the presidency.

Twitter's 140-character limit on tweets appears to appeal to Trump's short attention span and his preference for rapid-fire interactions. But 140 characters often don't leave space for much context, explanation or nuance. So what Trump writes may come across as more forthright and harsher than

what foreign governments are accustomed to in the diplomatic arena. The risk for a misunderstanding is, therefore, higher.

Foreign analysts following Trump's Twitter may not be inclined to simply take everything he writes at face value, especially when it comes to highly sensitive subjects. But, using sophisticated data tools, they may look for patterns that, over time, can help them better predict if Trump is being serious. In all likelihood, many intelligence specialists overseas have probably already done such analyses based on Trump's more than 34,000 tweets so far.

"If Trump's comments accurately reflect his intent, then we're giving the opponents a head start in dealing with the incoming presidential administration," a former U.S. intelligence officer said of Trump's Twitter habits. "If his comments are meant to conceal other intentions, then we're doing a pretty good job in misleading our adversaries."

A foreign government may check to see if Trump uses certain types of words before he takes certain types of actions. If Trump keeps tweeting during his presidency, a foreign entity may analyze what types of things he writes before making a policy announcement. (If Trump were to enable Twitter's geo-location services, that could also grab the attention of overseas actors, though it doesn't appear he uses that feature.) Even a lengthy silence from Trump could be a signal of some sort, sources connected to the intelligence community told POLITICO.

In August, David Robinson, a data scientist, published an analysis of Trump's tweets using digital tools.

It indicated that there were at least two people tweeting out under Trump's account. The tweets from an Android phone appeared to be coming from the Manhattan billionaire himself -- they were angrier and more negative. The ones from an iPhone were more quotidian, sharing announcements and photos; those were likely posted by one or more Trump campaign aides. (Some tweets may have been written by a staffer trying to sound like Trump.)

"A lot of 'emotionally charged' words, like 'badly', 'crazy', 'weak', and 'dumb', were overwhelmingly more common on Android," Robinson wrote, meaning it was Trump who was probably behind those particular tweets.

The U.S. has occasionally found itself in diplomatic dust-ups thanks to Twitter.

In September, during President Barack Obama's visit to China, the Defense Intelligence Agency tweeted "Classy as always China" after the American leader was deprived of a normal red-carpet arrival due to a dispute over which stairs he could use to leave his plane. The Pentagon-based agency later deleted the tweet and apologized.

Four years earlier in Egypt, during the brief presidency of Muslim Brotherhood leader Mohamed Morsi, the U.S. Embassy in Cairo slapped the Islamist organization's English-language Twitter account after it expressed concern for the safety of U.S. diplomats amid violent protests near their building.

"Thanks. By the way, have you checked out your own Arabic feeds? I hope you know we read those too," the embassy tweeted, implying the Brotherhood was using a very different tone in its non-English messages. The Americans later deleted the tweet.

Although Twitter has been around for most of Barack Obama's presidency, the outgoing president has been careful in using the medium. He was allowed to start using his own official account, @POTUS, only a couple of years ago: in May 2015, he sent out an inaugural tweet. The @POTUS account will be made available to Trump once he is sworn in.

The @BarackObama account is run by Organizing for Action, a liberal group that has long supported the president. It was not immediately clear if Obama would take over that account once he leaves office, but he's used it in the past, signing tweets he composed with a "-bo".

The White House Communications Agency, a military division that handles presidential communications security, referred questions about Trump's Twitter account and plans to safeguard his digital devices to the president-elect's transition team. The transition team did not respond to a request for comment. To date, it's not clear if Trump's phone conversations with foreign leaders are fully secured, though his team has said precautions have been taken.

Even as foreign capitals sift through Trump's tweets, there are questions about whether the social media company should take away his account for calling out individual Americans on Twitter. Trump's targets have included an Indianapolis union leader and a college student, who have faced death threats and harassment as a result.

When asked for comment about whether Trump should be booted off the platform, a spokesperson for the company replied: "The Twitter Rules apply to all accounts."

Reuters
Top U.S. spy agency has not embraced CIA assessment on Russia hacking - sources
Tuesday, 13 December 2016
Byline: Jonathan Landy, Mark Hosenball

Washington - The overseers of the U.S. intelligence community have not embraced a CIA assessment that Russian cyber attacks were aimed at helping Republican President-elect Donald Trump win the 2016 election, three American officials said on Monday.
While the Office of the Director of National Intelligence (ODNI) does not dispute the CIA's analysis of Russian hacking operations, it has not endorsed their assessment because of a lack of conclusive

evidence that Moscow intended to boost Trump over Democratic opponent Hillary Clinton, said the officials, who declined to be named.

The position of the ODNI, which oversees the 17 agency-strong U.S. intelligence community, could give Trump fresh ammunition to dispute the CIA assessment, which he rejected as "ridiculous" in weekend remarks, and press his assertion that no evidence implicates Russia in the cyber attacks.

Trump's rejection of the CIA's judgment marks the latest in a string of disputes over Russia's international conduct that have erupted between the president- elect and the intelligence community he will soon command.

An ODNI spokesman declined to comment on the issue.

"ODNI is not arguing that the agency (CIA) is wrong, only that they can't prove intent," said one of the three U.S. officials. "Of course they can't, absent agents in on the decision-making in Moscow."

The Federal Bureau of Investigation, whose evidentiary standards require it to make cases that can stand up in court, declined to accept the CIA's analysis - a deductive assessment of the available intelligence - for the same reason, the three officials said.

The ODNI, headed by James Clapper, was established after the Sept. 11, 2001, attacks on the recommendation of the commission that investigated the attacks. The commission, which identified major intelligence failures, recommended the office's creation to improve coordination among U.S. intelligence agencies.

In October, the U.S. government formally accused Russia of a campaign of cyber attacks against American political organizations ahead of the Nov. 8 presidential election. Democratic President Barack Obama has said he warned Russian President Vladimir Putin about consequences for the attacks.

Reports of the assessment by the CIA, which has not publicly disclosed its findings, have prompted congressional leaders to call for an investigation.

Obama last week ordered intelligence agencies to review the cyber attacks and foreign intervention in the presidential election and to deliver a report before he turns power over to Trump on Jan. 20.

The CIA assessed after the election that the attacks on political organizations were aimed at swaying the vote for Trump because the targeting of Republican organizations diminished toward the end of the summer and focused on Democratic groups, a senior U.S. official told Reuters on Friday.

Moreover, only materials filched from Democratic groups - such as emails stolen from John Podesta, the Clinton campaign chairman - were made public via WikiLeaks, the anti-secrecy organization, and other outlets, U.S. officials said.

"THIN REED"

The CIA conclusion was a "judgment based on the fact that Russian entities hacked both Democrats and Republicans and only the Democratic information was leaked," one of the three officials said on Monday.

"(It was) a thin reed upon which to base an analytical judgment," the official added.

Republican Senator John McCain said on Monday there was "no information" that Russian hacking of American political organizations was aimed at swaying the outcome of the election.

"It's obvious that the Russians hacked into our campaigns," McCain said. "But there is no information that they were intending to affect the outcome of our election and that's why we need a congressional investigation," he told Reuters.

McCain questioned an assertion made on Sunday by Republican National Committee Chairman Reince Priebus, tapped by Trump to be his White House chief of staff, that there were no hacks of computers belonging to Republican organizations.

"Actually, because Mr. Priebus said that doesn't mean it's true," said McCain. "We need a thorough investigation of it, whether both (Democratic and Republican organizations) were hacked into, what the Russian intentions were. We cannot draw a conclusion yet. That's why we need a thorough investigation."

In an angry letter sent to ODNI chief Clapper on Monday, House Intelligence Committee Chairman Devin Nunes said he was "dismayed" that the top U.S. intelligence official had not informed the panel of the CIA's analysis and the difference between its judgment and the FBI's assessment.

Noting that Clapper in November testified that intelligence agencies lacked strong evidence linking Russian cyber attacks to the WikiLeaks disclosures, Nunes asked that Clapper, together with CIA and FBI counterparts, brief the panel by Friday on the latest intelligence assessment of Russian hacking during the election campaign.

Yahoo News
Suspected Russian cyberattack waged on Clinton campaign just days before vote
Monday, 12 December 2016
Byline: Michael Isikoff

Washington - In the closing days of the 2016 election campaign, hackers believed to be working for Russian intelligence launched a new wave of attacks on Hillary Clinton's campaign and the Democratic

National Committee -- a previously unreported cyberoffensive that heightened concerns, now endorsed by the CIA, that the Russian government was seeking to influence the outcome of the election in favor of Donald Trump, according to sources familiar with the investigations into the attempted intrusions. The attacks came in the form of so-called "phishing" emails sent to nearly a dozen campaign and committee staffers in a renewed effort at penetrating their networks, said Dmitri Alperovitch, the co-founder and chief technology officer of CrowdStrike, the cybersecurity firm hired by the DNC to repel attacks on its network. Staffers at that point were alert enough to reject entreaties to click on the unsolicited email messages that would have allowed the hackers into their computers, he said.

But at least one top Clinton campaign staffer, communications director Jennifer Palmieri, told Yahoo News on Sunday that she received an alert from Google in mid- October informing her that her personal Gmail account had been targeted by a "foreign state" actor and that her password needed to be changed.

"They were targeting us throughout the election," said another former senior Clinton campaign staffer, who asked not to be identified. "They never stopped trying to get back in."

The disclosure of the late campaign attack could fuel a mounting controversy over U.S. intelligence findings that link Russian intelligence to the cyberattacks for the express purpose of throwing the election as part of a campaign, orchestrated in Moscow, to defeat Clinton.

The Washington Post reported Saturday that the CIA has briefed members of Congress on an assessment that the Russians targeted Democratic political organizations and campaign officials as part of a specific effort to defeat Clinton and elect Trump. This goes beyond an earlier public finding that U.S. intelligence officials were "confident" that the Russian government was behind the cyberattacks, but did not ascribe a motive for the Russians doing so.

One piece of damning evidence behind the new finding is that the CIA and the FBI have both identified specific individuals associated with or close to the Russian government who provided the DNC emails to WikiLeaks, which began publishing them in July, a senior law enforcement official told Yahoo News. Despite reports of a clash between the CIA and the FBI over the motive behind Russia's intelligence service in launching the operation, the differences are more a matter of "degree" and emphasis, with the FBI believing there may have been "mixed" motives for the Russian effort, the official said. Still, "we all agree they did these things," the official said.

But President-elect Trump doubled down on his rejection of the intelligence findings in an interview with Fox News anchor Chris Wallace that aired Sunday, dismissing any conclusion that points to Russian government involvement.

"I think it's ridiculous," Trump told Chris Wallace in interview that aired on "Fox News Sunday," his first Sunday show sit-down since winning the election. "I don't believe it."

"If you look at the story and you take a look at what they said, there's great confusion," Trump added. "Nobody really knows, and hacking is very interesting. Once they hack, if you don't catch them in the act you're not going to catch them. They have no idea if it's Russia or China or somebody. It could be somebody sitting in a bed someplace. I mean, they have no idea."

Alperovitch of CrowdStrike, the cybersecurity firm that first publicly linked the cyberattacks to Russian intelligence, said Sunday that he was "puzzled" by Trump's remarks and assumes he has not yet been fully briefed on the matter. (CrowdStrike, whose principals include Shawn Henry, the former chief of the FBI's cyber division, was initially hired by the DNC to investigate the cyberattacks and defend its network last May.)

"At this point, the matter of attribution on the intrusions has been settled,"Alperovitch said. "There is nobody that looks at the evidence who disputes this." Asked his level of confidence in his firm's findings, he responded "100 percent."

Much of the evidence, he said, revolves around the nature of the sophisticated tools used by the attackers on the DNC and forensic evidence showing strong similarities to Russian cyberattacks that have occurred in Ukraine and other Eastern European countries -- as well as to intrusions of the Joint Chiefs of Staff, the White House and the State Department and other U.S. government agencies. "The digital fingerprints are of the same origin," said Alperovitch.

CrowdStrike initially identified two sets of attackers on the DNC's servers: One, dubbed "Cozy Bear," was associated with the Russian FSB (the successor to the Soviet KGB) and which first breached the DNC's network in the summer of 2015. Another, dubbed "Fancy Bear," has been associated with Russia's military intelligence service, the GRU. The latter infiltrated the DNC's network in late April of this year in what turned into a far more devastating attack, resulting in the disclosure of 20,000 internal DNC emails to WikiLeaks -- an act, according to Alperovitch, of "information warfare." (He acknowledged that a third Russian intelligence service, the SVR, which has responsibility for foreign intelligence operations, may also have been involved.)

"When we look at this over 10 years -- literally hundreds of intrusions -- [and] you look at the tradecraft, you look at the victims, it all points to Russian intelligence services," Alperovitch said.

In addition, he said, there was another separate cyberattack discovered in late September from an undetermined party that penetrated DNC computers with software containing sensitive voter analytic data that was being provided in regular memos to Clinton campaign manager Robby Mook, the sources said.

The breach was detected by CrowdStrike, and the cyberinvaders were expelled from a cloud server housing the data; this server was distinct from the DNC's internal computer network that had been previously breached, he said. But the intruders were never identified, and it was never determined

whether the data -- containing detailed reports on voter registration and estimates of likely voter participation in the November election -- was ever actually stolen.

Alperovitch said he doesn't know whether these hackers were associated with Russian intelligence; they used different methods and publicly available cybertools to pull it off -- also he said the DNC never authorized his firm to conduct a full investigation. But he said the late October "phishing" attacks on the DNC and the Clinton campaign resembled the earlier Fancy Bear attacks, leading him to conclude they were likely the work of the GRU.

Moreover, attacks by the Cozy Bear intruders have continued throughout the fall, targeting multiple organizations, including think tanks and universities whose scholars work on Russian policy issues, he said.

And even more recently, he said, there was evidence that the separate "Fancy Bear" hackers are now also attacking political organizations in Germany and elsewhere in Europe in an apparent attempt to meddle in their elections as well. (The chief of German domestic intelligence said last week that there has been a recent increase in "aggressive cyberespionage" against German politicians and warned about "growing evidence for attempts to influence the [German] federal elections next year."

"These activities have not stopped," said Alperovitch. "Now that they were executed [in the United States] and they have a successful playbook, I fully expect they are going to continue."

Press TV
Iranian Army unveils new indigenous combat, reconnaissance drones
Tuesday, 13 December 2016

Tehran - The Iranian Army's Ground Forces has unveiled two domestically-designed and -manufactured drones on the final day of major military exercises code-named Mohammad Rasoulallah IV (Mohammad, the Messenger of God IV) in southeastern Iran.
One of the two aircraft, code- named Oghab (Eagle), is a combat drone capable of carrying air-to-surface missiles.

The other, code-named Shahin (Falcon) and developed and manufactured under a project code-named Shahid Mohsen Ghotaslou, can collect information on the positions and movements of enemy forces on reconnaissance missions. It boasts a flight endurance of 24 hours.

General Seyyed Kamal Peyambari, the spokesman for the military drills, said the jamming and combat techniques of drones were also fully tested at various altitudes on Tuesday, with the participation of military commanders and defense experts.

Peyambari noted that sophisticated and innovative weapons such as super- caliber 107mm rocket launchers, optimized versions of the 62.5mm PSG-1 and Dragunov semi-automatic sniper rifles, a jammer with an effective range of 800 meters, drone jammers, and cellular satellite phone jammers were put to practice on the last day of the drills as well.

Various and extensive psychological war techniques such as drills using 122mm flyer-carrying rockets, tactical radios and directional sound systems were also put to the test for the first time.

The senior Iranian military figure further noted that hand-launched drones as well as land minelayers were also tried out.

Peyambari added that electronic warfare, armored, infantry, mechanized infantry, commando, and intelligence units present at the Mohammad Rasoulallah IV military exercise, which covered an area of 220,000 square kilometers, successfully carried out their operations on the third day of the drills.

Iran has conducted major military drills in recent years to enhance the defense capabilities of its Armed Forces and to test modern military tactics and state-of-the-art equipment. Each year, the country inaugurates a host of new projects and hardware developed with reliance on domestic capabilities.

The Islamic Republic maintains that its defense power is driven by deterrence and poses no threat to any other country.

Hindustan Times
Legion: Meet the hackers who broke into Twitter accounts (Canada).
Tuesday, 13 December 2016

New Delhi - A hackers' group called Legion has repeatedly breached the Twitter accounts of some well-known Indians, including Congress vice- president Rahul Gandhi and prominent journalist Barkha Dutt. Legion has not posted any classified information on the hacked accounts but has threatened to expose email communications among Congress party leaders in the New Year. Earlier this month, they on his Twitter handle, vowing to bring to justice the fugitive industrialist who has defaulted on at least Rs 7,000 crore bank loans.

Here is some detail about the hackers' group: What is Legion? It is a coalition of like-minded hackers based out of five countries - the United States, Sweden, Canada, Thailand and Romania, according to the Delhi police's cybercrime cell. The group seeks to expand its activities, leaving its email id -- legion_group@sigaint.org - for more hackers to join their campaign.

Are they connected with Legion of Doom of the 1980s? The group does not appear to have any links with the hackers' group Legion of Doom (LoD) that targeted rich and famous people's email accounts in the mid-1980s. LoD remained active till early 2000s. However, the two groups appear to share

ideological goals in targeting what they say are the rich and corrupt. LoD was founded by US-based hacker Lex Luthor after he broke away from the Knights of Shadow.

Why do they hack people's accounts? Legion fancies itself as cyber vigilantes working to expose the corrupt. But the group is yet to bolster their anti-corruption crusader credentials, given that it has so far offered very little valuable information.

How does Legion operate? Legion communicates through email servers and browsers that are shielded against surveillance. In other words, it does not use Google Chrome or Internet Explorer but a browser called The Onion Router (TOR), which is difficult to track (provides anonymity) and allows a user to communicate directly with another one. This is also called the darknet, a platform often used by activists and journalists seeking to avoid a surveillance dragnet.

Are there other such hackers' groups? Yes. Anonymous is another loosely associated international network of activist and hacktivists which started operating in 2003. The group's website describes it as "an Internet gathering" with "a very loose and decentralised command structure that operates on ideas rather than directives". The group became known for crashing websites of governments, corporates and religious groups. Anonymous members (known as "Anons") use the Guy Fawkes mask as their emblem.

Saudi Gazette
IoT continues to pose a key cyber security threat
Tuesday, 13 December 2016
Byline: Mohammed Al-Moneer

Riyadh - The cyber landscape changes dramatically year after year. If you blink, you may miss something; whether that's a noteworthy hack, a new attack vector or new solutions to protect your business. Sound cyber security means trying to stay one step ahead of threat actors.
In the spirit of looking toward the future, I wanted to grab my crystal ball and take my best guess at what will be the big story lines in cyber security in 2017.

1. IoT continues to pose a major threat. In late 2016, all eyes were on IoT-borne attacks. Threat actors were using Internet of Things devices to build botnets to launch massive distributed denial of service (DDoS) attacks. In two instances, these botnets collected unsecured "smart" cameras. As IoT devices proliferate, and everything has a Web connection -- refrigerators, medical devices, cameras, cars, tires, you name it -- this problem will continue to grow unless proper precautions like two-factor authentication, strong password protection and others are taken.

Device manufactures must also change behavior. They must scrap default passwords and either assign unique credentials to each device or apply modern password configuration techniques for the end user during setup.

2. DDoS attacks get even bigger. We recently saw some of the largest DDoS attacks on record, in some instances topping 1 Tbps. That's absolutely massive, and it shows no sign of slowing. Through 2015, the largest attacks on record were in the 65 Gbps range.

Going into 2017, we can expect to see DDoS attacks grow in size, further fueling the need for solutions tailored to protect against and mitigate these colossal attacks.

3. Predictive analytics gains ground. Math, machine learning and artificial intelligence will be baked more into security solutions. Security solutions will learn from the past, and essentially predict attack vectors and behavior based on that historical data. This means security solutions will be able to more accurately and intelligently identify and predict attacks by using event data and marrying it to real-world attacks.

4. Attack attempts on industrial control systems. Similar to the IoT attacks, it's only due time until we see major industrial control system (ICS) attacks. Attacks on ecommerce stores, social media platforms and others have become so commonplace that we've almost grown cold to them. Bad guys will move onto bigger targets: dams, water treatment facilities and other critical systems to gain recognition.

5. Upstream providers become targets. The DDoS attack launched against DNS provider Dyn, which resulted in knocking out many major sites that use Dyn for DNS services, made headlines because it highlighted what can happen when threat actors target a service provider as opposed to just the end customers.

These types of attacks on upstream providers causes a ripple effect that interrupts service not only for the provider, but all of their customers and users. The attack on Dyn set a dangerous precedent and will likely be emulated several times over in the coming year.

6. Physical security grows in importance. Cyber security is just one part of the puzzle. Strong physical security is also necessary. In 2017, companies will take notice, and will implement stronger physical security measures and policies to protect against internal threats and theft and unwanted devices coming in and infecting systems.

7. Automobiles become a target. With autonomous vehicles on the way and the massive success of sophisticated electric cars like Teslas, the automobile industry will become a much more attractive target for attackers. Taking control of an automobile isn't fantasy, and it could be a real threat next year.

8. Point solutions no longer do the job. The days of Frankensteining together a set of security solutions has to stop. Instead of buying a single solution for each issue, businesses must trust security solutions from best-of-breed vendors and partnerships that answer a number of security needs. Why have 12 solutions when you can have three? In 2017, your security footprint will get smaller, but will be much more powerful.

9. The threat of ransomware grows. Ransomware was one of the fastest growing online threats in 2016, and it will become more serious and more frequent in 2017. We've seen businesses and individuals pay thousands of dollars to free their data from the grip of threat actors. The growth of ransomware means we must be more diligent to protect against it by not clicking on anything suspicious. Remember: if it sounds too good to be true, it probably is.

10. Security teams are 24/7. The days of security teams working 9-to-5 are long gone. Now is the dawn of the 24/7 security team. As more security solutions become services-based, consumers and businesses will demand the security teams and their vendors be available around the clock. While monitoring tools do some of the work, threats don't stop just because it's midnight, and security teams need to be ready to do battle all day, every day. Those are 10 things we see happening in the cyber security space next year.

Fars News Agency
Iran's Ground Force Unveils New Drone during Massive Drills
Tuesday, 13 December 2016

Tehran - The Iranian Ground Force unveiled a new drone named 'Farpad' during the massive wargames codenamed 'Mohammad Rasoulallah (PBUH) 4' in the Southeastern parts of the country on Monday morning. The hand- launched drone is run by autopilot and can fly maximum 45 minutes to the range of 20km.
Also during the second day of the three-day drills, the Iranian Ground Force unveiled a jamming system which is capable of confronting Unmanned Aerial Vehicles (UAVs) in a range of 3km and can force it to land after taking its control. The system is also portable by individuals.

In another development in the wargames, the home-made Toufan missiles whose range and destruction and precision-striking power have been improved were fired by helicopters and hit simulated enemy's targets precisely.

Also, the latest sniper gun manufactured for the Iranian Ground Force, 'Taher', with a range of 1.2km was unveiled on Monday. The gun weighs 4.4kg (without scope and magazine) and is 1.28m in length.

Meantime, the 209 (Cobra) and 214 helicopters of the Iranian Ground Force's air force units fired several rockets at two floating targets in Makran region (in the Sea of Oman) and destroyed them.

Also, two Mirage fighter jets of the Iranian Air Force participated in the drills for the first time and used air-based weapons in operations against the simulated enemy.

The massive 'Mohammad Rasoulallah (PBUH) 4' wargames started in the Southeastern parts of the country on Sunday morning.

"On the first day of the drills, rapid reaction units from other geographical regions of the country were transferred to the operational regions via air and ground in the shortest possible time," Spokesman of the drills General Seyed Kamal Payambari told reporters yesterday.

He said that the drills are being held in the strategic Southeastern parts of the country in a range of over 220,000km with the participation of different units of Ground Force, logistic forces of the Air Force and Khatam ol-Anbia Air Defense Base.

According to General Payambari, assessment of the Iranian forces' preparedness in the tactical fields and decreasing the time for their rapid reaction against threats as well as using new defense systems are among the goals pursued in the wargames.

Meantime, Army Airborne Commander Brigadier-General Houshang Yari announced on Sunday that dozens of different types of helicopters are flying over the wargames zone.

"Tens of different types of 206, 214, 209 (Cobra) and Chinook helicopters are present in the drills zone," General Yari told reporters today.

"During the drills, the command, track, control and close fire support missions as well as numerous heliborne operations will be carried out by the Airborne helicopters," he added.

General Yari said that the drills will also be a touchstone to assess the agility and power to overhaul and maintain helicopters.

Fars News Agency
Civil Defense Official Warns of New US Cyber Attack against Iran
Tuesday, 13 December 2016

Tehran - A senior member of Iran's Civil Defense Organization warned that Washington has hatched plots to launch new cyber operations against the country's infrastructures.
"At present, the US has launched a project named Nitro Zeus with the aim of attacking Iran's defense and telecommunication infrastructures," Alireza Karimi said on Monday, addressing a conference in Tehran.

"Based on studies that we have carried out, the project is assessed to be much more dangerous than the Stuxnet project," he added.

His remarks came after Deputy Head of Iran's Civil Defense Organization Brigadier General Mohammad Hassan Mansourian underlined in October his organization's full preparedness to confront the cyberattack and cultural invasion threats.

"Iran's Civil Defense Organization can defuse cyberattacks and cultural invasions," Brigadier General Mansourian said. He underlined that the advanced countries are currently making huge investments in the field of civil defense.

Mansourian underscored that the cyberattack and cultural invasion should only be responded by the national civil defense system.

In May 2015, Head of Iran's Civil Defense Organization Brigadier General Gholamreza Jalali announced that the country has set up cyber defense workgroups to better coordinate measures for defending nuclear facilities against enemies' cyber attacks.

"The country's vital cyber infrastructures have been identified and separate cyber workgroups have been formed in all fields," Jalali told reporters in Tehran.

"For instance a cyber defense workgroup was set up in the nuclear field for Natanz nuclear installations and no serious incident has threatened this section in the past two years," he added.

In relevant remarks in October 2014, Jalali revealed that a US cyberattack on Iran's nuclear enrichment facility in Natanz failed due to his organization's tough defensive measures.

"The first cyberattack, codenamed Olympic Games, was carried out on Natanz and was declared by the US President, but it met our heavy (defensive) response," Jalali told reporters in a press conference in Tehran.

The senior commander said the US changed its cyber commander following the failure in the cyberattack on Natanz, adding that the US general was forced to retire several months ago "due to the wrong information and data that he had presented to President Obama". And this was the result of our direct confrontation with them, General Jalali added.

The US was the principal player in the most sophisticated cyber-attack ever known and has been orchestrating a campaign against Iran designed to undermine the country's nuclear program.

The New York Times came up with an in-depth report on June 1, 2012 saying that from the very first month Barack Obama took over as US President, he secretly ordered increasingly sophisticated attacks on Iran's computer systems that run the country's main nuclear enrichment facilities.

The disclosures about Obama's role in the cyberwar against Iran appear to show beyond doubt that the US, with the help of Israel, was behind the Stuxnet virus attack on Iran's centrifuge machines - used to enrich uranium. The revelation then indicated that Washington and Tel Aviv were also behind the Flamer and Duqu virus attacks discovered by experts in May 2012.

Codenamed Olympic Games, the attacks were spearheaded by the US government under the Bush administration. Stuxnet targeted Siemens industrial equipment to spin hundreds of centrifuges beyond their breaking points and eventually disable Iran's nuclear efforts.

According to the report, Obama decided to speed up the attacks, even after the worm escaped from Iran's Natanz plant in 2010 and later ended up on the Internet.

During a meeting following the worm's escape, Obama even considered that the worm should be stopped thinking that America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised. Should we shut this thing down? Obama asked members of the President's national security team.

However, he finally decided to go ahead with the cyberattacks. What followed thereafter was the Natanz plant being hit by several newer versions of the worm.

The report is said to be based on 18 months of interviews with current and former American, European and Israeli officials involved in the program as well as with outside experts, who provided contradictory assessments of how successful the attack was in slowing down Iran's progress of developing nuclear weapons.

While internal Obama administration estimates claim the effort was delayed by 18 months to two years, some other experts, both inside and outside the government, said that Iran's enrichment levels had steadily recovered. A year later, Iran enriched uranium to the 20-percent grade, way beyond the 5-percent purity level that was done in Natanz in 2012.

Le Télégramme
Cybersécurité. La Bretagne au coeur du combat
Tuesday, 13 December 2016
Byline: Journaliste maison

Bruz, France - Jean-Yves Le Drian, ministre de la Défense, a dévoilé au centre DGA Maîtrise de l'information à Bruz (35), près de Rennes, la doctrine des armées en matière de cybersécurité. « L'émergence d'un nouveau milieu, d'un champ de bataille cyber, doit nous amener à repenser profondément notre manière d'aborder l'art de la guerre (...), comme l'aviation au début du XXe siècle », a-t-il assuré, soulignant : « En temps de guerre, l'arme cyber pourra être la réponse, ou une partie de la réponse, à une agression armée, qu'elle soit de nature cyber ou non ». La doctrine présentée ce lundi, qui repose sur trois piliers - renseignement, protection/défense et lutte informatique offensive - est l'une des plus élaborées énoncées en Europe, avec celle du Royaume-Uni. Concrètement, la France pourra recourir au combat numérique comme à une arme classique de type missile pour riposter à une attaque, aussi bien cyber que conventionnelle. « Nos capacités cyber offensives doivent nous permettre

de nous introduire dans les systèmes ou les réseaux de nos ennemis, afin d'y causer des dommages, des interruptions de service ou des neutralisations temporaires ou définitives », a relevé le ministre.

Un bataillon de 2.600 « combattants numériques »

Un commandement des opérations cyber, placé sous la responsabilité directe du chef d'État-Major des armées, va être créé, dès janvier 2017. Il disposera d'un état-major resserré qui supervisera 2.600 « combattants numériques » . Les armées pourront « neutraliser » des infrastructures utilisées pour attaquer des intérêts français mais aussi « riposter » plus largement à une attaque cyber, a expliqué Jean-Yves Le Drian.

« Si une attaque cyber s'apparente à un acte de guerre, une riposte adéquate s'imposera (...) dans une logique de conflit ouvert », a-t-il souligné. Si l'attaque transite par un État qui « n'aurait pas empêché une telle utilisation, la responsabilité de cet État pourrait être mise en jeu », a-t-il averti.

Le Monde
Un an après sa création, la commission chargée du contrôle du renseignement
Tuesday, 13 December 2016
Byline: Jacques Follorou

Paris - Un an après sa création, la commission chargée du contrôle du renseignement affirme son indépendance
L'avis de la Commission nationale de contrôle des techniques de renseignement, née en octobre 2015 pour faire contrepoids aux puissants moyens de surveillance accordés aux services secrets, n'est que consultatif mais le premier ministre l'a suivi dans la plupart des cas.

Pour son premier rapport annuel, présenté mardi 13décembre, la Commission nationale de contrôle des techniques de renseignement (CNCTR), née, le 3octobre 2015, pour faire contrepoids aux puissants moyens de surveillance accordés aux services secrets français dans la loi du 24juillet 2015 sur le renseignement, jouait une part de sa crédibilité.

Nommé président de cette nouvelle instance indépendante, Francis Delon, ex-secrétaire général de la défense nationale et l'un des pères fondateurs de la plateforme nationale du renseignement technique qui alimente depuis 2008 la communauté française du renseignement, devait prouver que les premiers soupçons de grande proximité avec l'Etat étaient infondés. Il devait, de plus, montrer que dans une période où l'émotion pèse sur les décisions politiques, il saurait résister aux pressions l'invitant à ne pas s'opposer aux libertés prises avec le droit.

La CNCTR est chargée de contrôler de l'utilisation d'une douzaine de moyens de surveillance par les services de renseignement français. L'avis de la CNCTR, composée de dix-sept membres, dont trois ingénieurs, n'est que consultatif. Le premier ministre, seule autorité décisionnaire en la matière, l'a

néanmoins suivi dans la plupart des cas. La procédure dite d'urgence, qui permet de s'exonérer du point de vue de la CNCTR, n'a été déclenchée qu'à une reprise selon le rapport qui ne fournit aucun détail opérationnel.

8538 interceptions de sécurité validées

En un an, la CNCTR a visé 48208 demandes de collecte de données de connexion, qui portent parfois sur de simples recherches de numéros dans des annuaires. Elle a donné un avis favorable à 2127 demandes de géolocalisation et elle a validé 8538 interceptions de sécurité, des écoutes téléphoniques, alors que l'instance qui existait auparavant, la Commission nationale de contrôle des interceptions de sécurité (CNCIS), née de la loi de 1991, en avait contrôlé un peu plus de 7000 lors de sa dernière année.

La CNCTR reste très discrète sur les 7711 fois où «d'autres techniques» ont été déployées avec son aval. S'agissait-il de pose de balises, de sonorisation d'appartements, de recueil ou de collecte de données informatiques? On n'en saura rien. La CNCTR explique qu'elle est tenue par la loi qui lui interdit de révéler des capacités opérationnelles. Elle signale néanmoins que faute d'achèvement du chantier de «centralisation des données recueillies» par ces nouvelles techniques, elle n'a pas encore une vision sur leur utilisation sur tout le territoire.

6,9% des demandes renvoyées aux services

En matière d'avis défavorables, on note une augmentation par rapport au temps de la CNCIS qui ne donnait son avis que sur les interceptions de sécurité et les données de connexions. La CNCTR a renvoyé aux services 6,9% des demandes contre environ 1% à l'époque de la CNCIS. Avant la loi de juillet2015, les services de renseignement usaient d'un grand nombre de ces moyens intrusifs, balises, sonorisation de lieux, etc. sans demander l'autorisation à quiconque, en toute illégalité. Les avis défavorables de la CNCTR portent essentiellement sur ces outils, désormais légaux, mais particulièrement attentatoires à la vie privée.

Si la CNCTR s'est vue, de fait, reprocher par les services un surcroît de «paperasse», elle a surtout pu éprouver la réalité de son indépendance lors des tentatives du gouvernement de passer outre ses prérogatives. Ce fut ainsi le cas avec l'article851-2 sur le recueil de données de connexions en temps réel attachées à une personne sur l'ensemble de ses moyens de communication.

La loi sur le renseignement du 24juillet 2015 disposait que cette collecte ne pouvait être effectuée que «sur une personne préalablement identifiée comme présentant une menace» . Le gouvernement et le chef de l'Etat ont tenté, en janvier, d'utiliser ce moyen pour mettre sous surveillance des listes entières de suspects, notamment les fameux fichés «S» pour islam radical, soit près de 14000 personnes. M.Delon a bloqué cette requête considérant qu'elle n'est pas conforme à la loi qui impose que chaque demande doit être individualisée et justifiée.

Pour contourner ce refus de valider «des surveillances groupées et simplifiées», le gouvernement, soutenu par un législateur, davantage soucieux d'étendre la surveillance d'Etat que de jouer son rôle de contre-pouvoir, a, depuis, modifié à deux reprises le périmètre de cet article de loi. Dans le cadre des lois sur la prorogation de l'Etat d'urgence, le Parlement a d'abord élargi la surveillance aux personnes «pouvant constituer une menace» . Et fin juillet, il a étendu la collecte de données de connexion en temps réel à l'entourage de la personne surveillée dès lors qu'il existait simplement «des raisons sérieuses de penser» qu'espionner ces gens au sein de cercles familiaux, amicaux, professionnels ou occasionnels puisse avoir un intérêt.

L'«exception hertzienne»

Si les parlementaires n'ont pas été d'une grande aide pour la CNCTR, elle a, en revanche, trouvé dans le Conseil constitutionnel un soutien inattendu pour tenter d'étendre son contrôle sur un pan entier des surveillances en France qui restaient jusque-là interdites, les communications hertziennes. Qualifiée d' «exception hertzienne» par la CNCTR, cette dérogation du droit consacrée par la loi de 1991 sur les interceptions puis prorogée dans la loi de juillet de 2015, a pris fin lors de sa censure, le 21octobre, par le Conseil constitutionnel.

Se félicitant de la décision du Conseil de vouloir faire entrer la surveillance par voie hertzienne dans le droit commun et d'avoir été chargée par lui de veiller à son application d'ici au vote d'une nouvelle loi, au plus tard le 31décembre 2017, la CNCTR a, au moins jusqu'à cette date, le pouvoir de viser chaque demande d'interceptions effectuée par cette technique. Souhaitant poursuivre son avantage, la CNCTR demande, dans son rapport, d'être «consultée sur l'éventuelle nouvelle législation» .

Le Temps (Suisse)
ID Quantique se déploie à l'international
Tuesday, 13 December 2016
Byline: Dejan Nikolic

Londres - Le numéro un mondial de la cryptographie quantique et de la génération de nombres aléatoires ouvre un bureau à Londres, signe un partenariat stratégique avec le géant coréen SK Telecom et s'attaque au marché chinois
ID Quantique (IDQ), pépite issue des laboratoires de physique appliquée de l'Université de Genève, s'offre un déploiement sans précédent. L'actuel numéro un mondial de la cryptographie quantique et de la génération de nombres aléatoires étend tout d'abord ses activités à la Grande-Bretagne. A travers notamment un contrat consistant à sécuriser les échanges d'informations entre l'un des sites de BT (anciennement British Telecommunications) et Cambridge.

IDQ ouvre également une officine britannique, afin de prendre part à une plateforme scientifique nationale de 384 millions de francs sur cinq ans. « Huit grandes universités du pays ainsi que le secteur

privé et public participent à ce programme », précise Grégoire Ribordy, fondateur d'IDQ, qui imagine affecter cinq collaborateurs à Londres d'ici à un an.

Parallèlement à cette nouvelle tête de pont britannique, IDQ signe une alliance avec SK Telecom, le principal opérateur de Corée du Sud (29,45 millions de clients, soit environ 50% du marché local, pour près de 15 milliards de francs de chiffre d'affaires l'an passé). Ce rapprochement avec la major de l'un des pays les plus connectés de la planète est assorti d'une levée de fonds de plus de 4 millions de francs. Soit la troisième injection de capital en quinze ans, les deux précédentes rondes ayant permis d'engranger respectivement un million (2004) et quatre millions (2014).

La fibre commerciale

L'entreprise carougeoise, lancée en 2001 et qui affiche une croissance moyenne de 30% par an, emploie aujourd'hui une cinquantaine de salariés, soit plus du double qu'en 2014. Son dernier tour de financement, auquel participent d'autres investisseurs stratégiques, est destiné à renforcer sa suprématie à l'échelle planétaire. Et d'asseoir son développement en Asie.

« L'une des filiales de SK Telecom fabrique des puces pour smartphones intégrant des nombres aléatoires, relève Grégoire Ribordy. Ce dispositif bon marché, qui permet de réduire la vulnérabilité des appareils, est en passe de révolutionner le monde de la téléphonie mobile. » Un boîtier traditionnel, de taille standard, coûte environ 1000 francs. Avec la technologie sud-coréenne embarquée, générer des clés ou des mots de passe exclusifs coûtera jusqu'à 100 fois moins cher.

Promesses quinquennales

Dans la foulée, IDQ inaugure son entrée sur le marché chinois. Via une coentreprise avec China Quantum Technologies (CQT), une société pionnière dans les technologies quantiques, à l'origine du plus important réseau commercial en la matière. Soit entre les villes de Shanghai et de Hangzhou, un tronçon de communication ultra-sécurisé d'environ 200 km. « Les contrats ont été signés il y a un mois », se félicite Grégoire Ribordy, sur le point d'ouvrir avec son partenaire chinois une usine dans la province du Zhejiang.

Le nouveau site de production, appelé à fonctionner avant fin 2017 avec un effectif de 50 collaborateurs, doit notamment permettre à CQT d'accéder au savoirfaire genevois en participant à la fabrication notamment de produits d'appel destinés aux casinos et aux paris en ligne. En échange de quoi, IDQ se voit offrir une porte d'entrée sur le potentiel commercial chinois.

La cryptographie quantique est l'un des cinq axes du 13e plan quinquennal de Pékin, définis comme étant d'importance stratégique cruciale pour la nation. Le prix d'un appareil de cryptage, qui c oûte actue llement 50 000 francs pièce, « sera divisé par dix grâce aux volumes du marché chinois », estime Grégoire Ribordy.

Toutefois, les spécialistes se heurtent pour l'heure à un obstacle technique de poids: par voie terrestre, le système ne fonctionne que de point à point, jusqu'à cent kilomètres au maximum. Au-delà, trop de photons sont perdus par diffusion en raison des imperfections de la fibre. Il faut alors aménager des noeuds intermédiaires pour que la particule qui compose la lumière, et qui sert à envoyer les clés de chiffrement nécessaires au décodage de l'information, soit impossible à intercepter. Le maillage Shanghai-Hangzhou, qui garantit que toute tentative d'espionnage provoque l'autodestruction du signal, en compte par exemple cinq.

Mais la Chine rêve d'inaugurer, d'ici à 2030, un système d'échange de données inviolable à l'échelle mondiale. Pékin a ainsi lancé le 15 août dernier le premier satellite de communication indéchiffrable à longue distance (près de 2500 km). Seul hic: l'instrument en orbite doit être orienté de manière extrêmement précise vers les stations au sol. « Ce sera comme lancer une pièce de monnaie d'un avion volant à 100 km d'altitude et espérer qu'elle vienne se ficher exactement dans la fente d'une tirelire cochon en rotation », avait alors expliqué Wang Jianyu, le responsable en chef de cette percée technologique de Pékin.

Le Télégramme
Lannion. Nouvelle Breizh cyber valley
Tuesday, 13 December 2016
Byline: Journaliste maison

Lannion, France - Marie-Hélène Clam et Riwan Marhic Après Rennes et Bruz (35), la journée cybersécurité du ministre de la Défense, Jean-Yves Le Drian, s'est achevée sur le site de Nokia, à Lannion (22). Il s'y est vu confirmer la création de 500 emplois d'ingénieur Recherche et Développement d'ici à la fin 2018, dont une grande partie à Lannion, ciblée pôle mondial pour ce secteur.
« Lannion sera le centre mondial pour Nokia concernant la recherche en cybersécurité », a lancé Marc Rouanne, le numéro deux du groupe Nokia. Devant un Jean-Yves Le Drian acquis à la cause puisque lanceur du Pact Cybersécurité dès 2012, le dirigeant a confirmé le recrutement de 500 ingénieurs Recherche et Développement dont 300 jeunes diplômés. À lui seul, le site de Lannion accueillera une centaine de ces ingénieurs amenés à travailler sur la 4G, la 5G, l'internet des objets et bien sûr la cybersécurité. « Nokia est aussi sponsor de la première formation informatique et cyberdéfense de l'École nationale supérieure d'ingénieurs de Bretagne-Sud (ENSIBS) à Vannes, aide au codéveloppement des start-up locales et des acteurs européens », a ajouté Arnaud Laforge, directeur du site.

Scanner le trafic pour détecter les espions

Une heure durant, le ministre a pu assister à des démonstrations : du chiffrement des données à la détection des espions, appliqués aux domaines militaire et civil. « Les pare-feu, qui servent à se protéger des intrusions extérieures par internet, sont inutiles car plus d'un million d'appareils sont déjà infectés, a expliqué Giuseppe Targia, directeur de la sécurité chez Nokia. Certains pirates peuvent déjà avoir accès à nos machines. Notre solution basée sur la reflectométrie permet de vérifier en continu s'il y a des

irrégularités au sein de notre réseau, juste en observant le comportement de nos appareils ».Adopté par la Banque de France, ce système permet de scanner le trafic automatiquement et de détecter des pertes de données dues à un réseau vieillissant ou à une interception des données, donc à de l'espionnage. Espionnage rendu possible grâce à des dispositifs coûtant moins de 10 achetés sur internet, que les pirates placent dans les boîtiers de fibre optique. Pour s'en protéger, l'équipementier développe un nouveau type de boîtier sécurisé qui sera opérationnel, fin 2017. Autre innovation, le réseau ultra-compact. Ce gros sac à dos permet d'établir des communications fiables en quelques minutes, n'importe où dans le monde. Déjà utilisé par les Marines américains, il peut être fixé à un drone ou à un ballon et bénéficie d'une couverture téléphonique et internet à 70 km à la ronde. En plus de son usage militaire, il sera mis à disposition des ONG ou des pompiers en cas de catastrophe naturelle.

« Comme des anticorps »

« La meilleure défense que nous connaissions, c'est le système immunitaire humain. Alors on s'en est inspiré pour notre cybersécurité : quand il y a un problème, le réseau réagit vite et apprend de ce problème pour s'en prémunir à l'avenir, comme des anticorps », résume Giuseppe Targia. Des innovations qui ont impressionné Jean-Yves Le Drian. « C'est quasiment une cyber armée qui se met en place en Bretagne. Dans le contexte de menace terroriste et avec 50 milliards d'objets connectés d'ici à 2025, il s'agit pour la France de garder de l'avance pour préserver son leadership sur ce domaine. Et Lannion en sera une Breizh cyber valley ».

Le Figaro
Le Conseil national du numérique hausse le ton face au fichier TES
Tuesday, 13 December 2016
Byline: Elisa Braun

Paris - Le fichage des Français au sein d'une base de données unique inquiète l'organe indépendant Non, c'est non. Le Conseil national du numérique (CNNum) reste intransigeant sur le fichier TES, qui permet au gouvernement de regrouper les données personnelles (sexe, couleur des yeux, taille, photo, empreintes digitales, filiation, nationalité...) de près de 60 millions de Français. Le CNNum en avait déjà demandé la suspension le 7 novembre dernier dans une lettre ouverte au gouvernement, où il déplorait les risques de dérives créées par un tel dispositif.

La nouvelle prise de position du CNNum publiée lundi et qui résulte des contributions recueillies par sa plateforme de consultation et d'auditions d'experts, est encore moins tendre avec le gouvernement. Outre la demande réitérée de suspension du fichier, le Conseil préconise dans son rapport l'instauration d'un débat public sur les sujets de l'identité administrative et l'identité en ligne. Il insiste également sur l'«urgence à instaurer une nouvelle gouvernance des choix technologiques au sein de l'État».

Un contre-exemple symptomatique

Au-delà de la polémique, le fichier TES apparaît selon le CNNum comme «le symptôme d'un processus décisionnel qui, en matière technologique, n'intègre pas suffisamment les exigences d'une vision politique de long terme». Au fil des pages du rapport, le Conseil mentionne les nombreux risques de dérives que constitue un tel fichier dans un contexte d'attaques cybersécuritaries accrues. Il recommande d'édicter un cadre général pour ce type de décision, et suggère notamment l'obligation de fournir des études d'impact approfondies et de tenir des débats publics.

L'organe consultatif recommande de renforcerle rôle d'instances spécialisées comme la Commission nationale informatique et libertés (Cnil), la direction interministérielle du numérique et du système d'information et de communication de l'État (Dinsic) et de l'agence nationale de la sécurité des systèmes d'information, l'Anssi.

Une querelle sans fin

Le fichage des Français a rouvert les fractures créées par le projet de loi sur le Renseignement, l'an dernier. Si le fichier TES est censé simplifier les formalités d'obtention et de renouvellement des titres d'identité, ainsi qu'éviter la fraude documentaire, certains opposants ont dénoncé son caractère attentatoire à la vie privée. Dans un contexte d'État d'urgence prolongé et de mesures prises contre le terrorisme, ce fichier TES a aussi été critiqué pour sa potentielle utilisation à des fins de renseignement.

Bernard Cazeneuve - alors ministre de l'Intérieur et à l'initiative du décret - a écarté cette possibilité devant la commission des Lois de l'Assemblée, le 9 novembre. Il n'a en revanche pas su lever les doutes de certains parlementaires, concernant les risques de sécurité liés à la concentration en un même fichier d'autant de données sensibles. Le ministère de l'Intérieur a consenti à rendre optionnel le versement des empreintes biométriques dans la base de données. Le ministère a également saisi la Dinsic (Direction interministérielle du numérique et du système d'information et de communication de l'État) et de l'Anssi (Agence nationale de la sécurité des systèmes d'information) afin d'évaluer le risque d'attaque informatique.

Lors d'une récente audition à la commission des lois du Sénat, les dirigeants de ces deux institutions n'ont pas fait mystère de leur intention d'amender le projet de l'Intérieur. Guillaume Poupard, directeur de l'ANSSI, s'est inquiété des risques géopolitiques: «Que se passerait-il si quelqu'un voulait déstabiliser la France non pas via une attaque très visible, mais en distillant des erreurs de-ci, de-là au sein du fichier?», rappelant que «ce genre d'armes est de plus en plus utilisé dans le cadre de conflits avoués ou pas entre grands États». «Je crois qu'il faut remettre à plat tout cela pour que le débat puisse reprendre sur des fondamentaux plus solides», a plaidé Henri Verdier, directeur du Dinsic. À la différence des deux instances, le CNNum, qui souhaite pour sa part repenser intégralement le fichier TES, reste pour sa part un organe purement consultatif.

La Tribune (France)
Surveillance spatiale : la France reste dans la cour des Etats- Unis et de la Russie

Tuesday, 13 December 2016
Byline: Michel Cabirol

Paris - La direction générale de l'armement a notifié le contrat de modernisation du système de surveillance de l'espace Graves à l'ONERA et à la PME Degreane Horizon. Un enjeu crucial pour la France qui peut ainsi suivre dans l'espace les satellites espions.
Le ministère de la Défense lance la modernisation du système de surveillance de l'espace Graves comme l'avait annoncé La Tribune (lien : http://www.latribune.fr/entreprises- finance/industrie/aeronautique-defense/surveillance-spatiale-la-france- modernise-le-systeme-graves-a-minima-602219.html). La direction générale de l'armement (DGA) a notifié un contrat pouvant s'élever jusqu'à 40 millions d'euros, qui comprend une tranche ferme et des tranches optionnelles, à deux cocontractants : le centre français de la recherche aéronautique spatiale et de défense l'ONERA et la PME électronique Degreane Horizon, spécialisée dans l'acquisition et l'émission de données sensibles. Cette filiale du groupe Vinci était depuis 2003 un des fournisseurs du centre de recherche français sur ce programme. La DGA a toutefois confié à l'ONERA la responsabilité du maintien des performances du système puis de son amélioration.

La tranche ferme de ce programme de rénovation court sur une période de cinq ans (huit ans si on rajoute toutes les tranches optionnelles). Elle représente plus de la moitié de la valeur du contrat, selon le chef de projet du système Graves au sein de l'ONERA, Florent Muller. Le système Graves est essentiellement installé sur trois sites, l'un à Dijon (le site d'émission avec les grande antennes), un autre sur le plateau d'Albion (site de réception) et, enfin, à Lyon Mont-Verdun, où le centre opérationnel de surveillance militaire des objets spatiaux (COSMOS), traite les données du système Graves (exploitation).

Graves, un système de renseignement stratégique

Mis en service depuis 2005 pour le compte de l'armée de l'air, le système Graves (pour Grand Réseau Adapté à VEille Spatiale) est un programme unique en Europe. Seuls les États-Unis et la Russie ont officiellement un programme équivalent alors qu'un cercle très restreint de pays, comme la Chine par exemple, pourraient en posséder un également. A ce jour, il est capable "de cataloguer des objets de la gamme du mini-satellite jusqu'à 1.000 km d'altitude", souligne Florent Muller. Soit un engin de la taille d'une machine à laver.

"Les données générées permettent de calculer à tout instant la position de l'ensemble des satellites suivis", précise-t-il. Actuellement, Graves détecte et catalogue tous les jours plus de 2.500 objets. C'est l'armée de l'air qui assure la mise à jour quotidienne du catalogue. Car pour rester catalogué, un objet doit être détecté tous les jours.

« La France a été le troisième pays au monde, après les Américains et les Russes, à se doter d'un tel système, avait expliqué en juin 2015 dans une interview accordée à la Tribune le PDG de l'ONERA, Bruno Sainjon. L'ONERA a conçu Graves, a piloté sa réalisation et l'a transféré à l'armée de l'air en 2005. Ce programme a notamment permis des échanges de données avec les États-Unis. Et, en avril 2015, cette

coopération s'est renforcée, les deux ministères de la Défense voulant désormais échanger des informations classifiées". »

Ce système de renseignement militaire stratégique, un outil extrêmement précieux pour la France, peut notamment suivre à une altitude de moins de 1.000 kilomètres les satellites espions, qui survolent la France et observent les sites sensibles. Ce qui permet à l'armée de l'air de cataloguer pratiquement tous les satellites espions alliés et ennemis ainsi que d'autres engins spatiaux. "Graves permet de détecter les menaces qui pèsent sur nos propres moyens spatiaux", confirme Florent Muller.

L'armée de l'air a d'ailleurs reconnu avoir identifié en 2012, puis 2013 et, enfin, en 2015, des engins spatiaux qui se sont approchés de satellites militaires français. Ces satellites sont d'ailleurs restés à leur contact pendant une période relativement longue. Très certainement pour les écouter. Il détecte également les vols en formation de satellites. En outre, Graves permet d'éviter d'éventuelles collisions entre des débris spatiaux et les satellites français en les déplaçant le cas échéant.

Enfin, le système concourt à la protection des populations face aux rentrées atmosphériques à risques (engins spatiaux, comètes...). Car plus de 12.000 satellites artificiels et objets divers, dont la taille est supérieure à dix centimètres, orbitent autour de la Terre.

Graves pourrait identifier des micro-satellites

Malgré sa robustesse et sa simplicité, le système Graves, un prototype qui était innovant en 2005, doit être aujourd'hui modernisé, les équipements ayant vieilli. Cette opération de rénovation permettra désormais d'assurer la pérennité de Graves "jusqu'en 2030", estime Florent Muller. Dans ce contexte, la tranche ferme du contrat confié à l'ONERA et à Degreane Horizon comprend en grande partie le traitement des obsolescences du système ainsi que quelques améliorations de ses performances, notamment du calculateur de traitement de signal.

« Certaines performances seront accrues grâce notamment à des interventions au niveau des antennes de réception et du traitement du signal, supportées par un nouveau calculateur", explique l'ONERA dans son communiqué. »

Plus précisément, l'ONERA sera en charge de la rénovation et des améliorations des sites de réception et d'exploitation. La filiale de Vinci modernisera pour sa part à l'identique les systèmes d'émissions en gérant les obsolescences.

Avec les tranches conditionnelles, de nouvelles améliorations du système sont prévues. En parallèle du lancement de la tranche ferme, l'ONERA effectuera des études techniques opérationnelles pour définir quelles pourraient être les options pour améliorer Graves. "A l'issue de ces études, un certain nombre d'options accessibles pourra être ainsi notifié en parallèle de la tranche ferme", confirme Florent Muller.

L'ONERA vise notamment l'amélioration de l'observation d'objets spatiaux plus petits. Et de passer "de façon progressive avec les options les plus complètes" de la détection de mini-satellites (inférieur à 500 kg) à celles de micro-satellites (inférieur à 150 kg). Dans sa nouvelle configuration, Graves détectera beaucoup plus d'objets spatiaux qu'actuellement si les tranches conditionnelles du contrat sont levées.

Un outil de souveraineté

Entre une modernisation a minima et une modernisation plus ambitieuse, le ministère de la Défense n'a pas encore tout à fait tranché en découpant le programme de modernisation de Graves en plusieurs tranches, dont des tranches optionnelles. Cet outil de souveraineté permet pourtant de discuter d'égal à égal - ou presque - avec les États-Unis. Ce qui n'est pas rien et confirme bien que la France est depuis 2005 dans le club très fermé des puissances dotées de capacités autonomes de surveillance de l'espace. Au ministère de la Défense de décider de l'ampleur de cette opération cruciale pour l'indépendance de la France en matière de surveillance spatiale une fois les recommandations de l'ONERA émises.

Développé sous contrat de la DGA, le système Graves est constitué d'un radar bistatique spécifique associé à un système de traitement automatisé qui permet la création et le maintien à jour d'une base de données des paramètres orbitaux des satellites qu'il détecte. Fruit de la collaboration des spécialistes des départements Électromagnétisme et radar (DEMR) et Conception et évaluation des performances des systèmes (DCPS) de l'ONERA, le radar du système Graves a été spécifiquement conçu pour la surveillance de l'espace.

Le Petit Bleu de Lot-et-Garonne
Cybersécurité : la France muscle son arsenal
Tuesday, 13 December 2016
Byline: Journaliste maison

Paris - Le combat numérique va devenir une arme à part entière des armées françaises, aussi bien offensive que défensive, face à une cybermenace qui vise de plus en plus les intérêts vitaux des États. «L'émergence d'un nouveau milieu, d'un champ de bataille cyber, doit nous amener à repenser profondément notre manière d'aborder l'art de la guerre», a déclaré hier le ministre de la Défense Jean-Yves Le Drian, en dévoilant la doctrine des armées françaises en matière de cybersécurité.

Dans un monde de plus en plus interconnecté, les cyberattaques venant d'États, hackers, groupes terroristes ou criminels se multiplient, a relevé le ministre.

Elles peuvent paralyser des infrastructures vitales (réseaux téléphoniques, centrales électriques, transport..) tout comme des cibles militaires en tentant de pénétrer les systèmes embarqués d'aéronefs, bâtiments de guerre ou blindés.

«L'arme cyber peut avoir des effets tout à fait comparables à l'armement plus conventionnel», a averti Jean-Yves Le Drian en inaugurant les nouveaux locaux de DGA Maîtrise de l'information, qui réunit les cyberexperts de la Défense à Bruz (Ile-et-Vilaine) près de Rennes.

Face à ces menaces, les armées verrouillent de plus en plus leurs systèmes d'information - ils sont protégés par des «murailles» et des «patrouilles» qui traquent les intrus - mais intègrent aussi désormais le cyber comme une arme offensive.

«En temps de guerre, l'arme cyber pourra être la réponse, ou une partie de la réponse, à une agression armée, qu'elle soit de nature cyber ou non», a énoncé M. Le Drian.

Concrètement, la France pourra recourir au combat numérique comme à une arme classique de type missile pour riposter à une attaque aussi bien cyber que conventionnelle.

Un commandement des opérations cyber, le CYBERCOM, placé sous la responsabilité directe du chef d'état-major des armées, va être pour cela créé en janvier 2017.

Il disposera d'un état- major resserré qui surpervisera 2.600 «combattants numériques» d'ici 2019.

Le Figaro
20.282 personnes espionnées en un an sur le territoire français
Tuesday, 13 December 2016
Byline: Christophe Cornevin

Paris - Dans son premier rapport d'activité dévoilé mardi matin, la Commission nationale de contrôle des techniques de renseignement (CNCTR) évalue que 47% des personnes surveillées l'ont été dans des dossiers terroristes et 29% au titre de la «lutte contre la criminalité organisée» ainsi que de la «prévention des violences collectives».
Entre le 3 octobre 2015 et le 2 octobre dernier, quelque 20.282 personnes ont été espionnées par les services français. En dévoilant mardi matin son premier rapport d'activité, la Commission nationale de contrôle des techniques de renseignement (CNCTR) a évalué le nombre d'hommes et de femmes qui ont fait l'objet d'une surveillance. Celle-ci passe par l'emploi de la technique la moins intrusive, à savoir l'obtention des «fadettes» (facturations détaillées) de la personne ciblée jusqu'à des moyens plus lourds, telles que la sonorisation ou l'installation de moyens vidéo dans les domiciles en passant par les interceptions de sécurité, la géolocalisation, l'accès en temps réel aux données de connexion» ou encore l'emploi - encore parcimonieux - des «Imsi catchers» permettant de siphonner à distance les données de connexion des téléphones mobiles.

Les algorithmes, c'est-à-dire la «boite noire», tant contestée censée assurer un recueil massif de données, ne devraient être mis en ouvre qu'au printemps prochain. «Pour l'heure, ils n'ont pas pu être mis en place pour des raisons de moyens techniques», précise-t-on à la CNCTR.

47% dans les radars de l'antiterrorisme

Au nombre de ceux ayant «fait l'objet d'une technique de renseignement au moins», le rapport de la CNCTR révèle que «9624 personnes, soit 47% du total, ont été surveillées au titre de la prévention du terrorisme» et que 5848 autres, soit 29% du total, ont été ciblées dans des dossiers de lutte contre la criminalité organisée ainsi que «la prévention de violences collectives de nature à porter gravement atteinte à la paix publique».

La CNCTR, qui se dit «particulièrement vigilante sur ce point», considère que «cette finalité ne saurait être interprétée comme permettant la pénétration d'un milieu syndical ou politique ou la limitation du droit constitutionnel de manifester ses opinions, y compris extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré.» Nombre d'observateurs y ont vu une disposition visant les zadistes mais aussi les no-borders, les blacks blocks ou encore les hooligans.

Les autres 24% de personnes placées dans les radars des services, qu'ils soient Français ou étrangers, ont été soupçonnés de porter atteinte à «l'indépendance nationale, l'intégrité du territoire et la défense nationale», d'espionnage industriel ou encore d'être liés à la «prolifération des armes de destructions massives».

8538 avis sur des demandes d'interceptions de sécurité

La démarche, tout à fait inédite dans le panorama feutré de l'espionnage, ne permet «aucun point de comparaison avec l'étranger», précise le conseiller d'État Francis Delon, président de la CNCTR qui, en aparté, ne se dit «pas particulièrement surpris» par le chiffre.

Cette instance indépendante, qui bénéficie d'un budget de 2,9 millions d'euros, vérifie la validité des techniques déployées de la DGSE, de la DGSI, de Tracfin ou encore de la Direction du renseignement militaire.

Depuis le 3 octobre 2015, la CNCTR a rendu 8538 avis sur des demandes d'interceptions de sécurité, contre 7703 l'année précédente. Le nombre des géolocalisations en temps réel a quant à lui bondi de 87% pour atteindre les 2127 demandes en 2016. Observant dans son rapport que «la prévention du terrorisme a, pour la première fois, été le fondement légal le plus fréquemment invoqué», la CNCTR ne constate cependant aucune explosion de la surveillance liée à la menace islamiste.

Composée de neuf «sages» - quatre hauts magistrats, quatre parlementaires et un expert en Télécoms - et d'une secrétaire de 17 personnes dont deux ingénieurs, elle s'est réunie de manière collégiale à 180 reprises à raison de trois fois par semaine pour examiner des cas individuels et mener des dossiers de fonds. Au terme des examens, la CNCTR a retoqué 6,9% des demandes.

New York Times
G.O.P. Feud Looms as Leaders Back Russia Inquiries
Tuesday, 13 December 2016
Byline: Jennifer Steinhauer

Washington - The top two Republicans in Congress said on Monday that they supported investigations into possible Russian cyberattacks to influence the American election, setting up a potential confrontation with President-elect Donald J. Trump in his first days in office.
"Any foreign breach of our cybersecurity measures is disturbing, and I strongly condemn any such efforts," said Senator Mitch McConnell, Republican of Kentucky and the majority leader, adding, "The Russians are not our friends."

Mr. McConnell's support for investigating American intelligence findings that Moscow intervened in the election on Mr. Trump's behalf could presage friction between the Republicans who control Congress, and who have long taken a hard line against Russia, and the president-elect, who has mocked the findings.

Mr. McConnell also went out of his way to address Mr. Trump's claim that the C.I.A. could not be trusted because of flawed intelligence before the Iraq war.

"Let me say that I have the highest confidence in the intelligence community," Mr. McConnell said, "and especially the Central Intelligence Agency. The C.I.A. is filled with selfless patriots, many of whom anonymously risk their lives for the American people."

The top Republican in the House, Speaker Paul D. Ryan of Wisconsin, said he supported a continuing investigation by Representative Devin Nunes of California, the chairman of the House Intelligence Committee. In a statement, Mr. Ryan said: "As I've said before, any foreign intervention in our elections is entirely unacceptable. And any intervention by Russia is especially problematic because, under President Putin, Russia has been an aggressor that consistently undermines American interests."

Congressional Republicans announced their support for inquiries after Mr. Trump railed for much of the weekend against the intelligence findings. But their remarks, especially Mr. Ryan's, were far from fiery, reflecting both a fear of offending Mr. Trump, who has taken many positions against traditional Republican orthodoxy, and the Republicans' belief that Democrats have selectively leaked intelligence information for political gain.

Critics from both parties are questioning Mr. Trump's apparent choice of Rex W. Tillerson, the chief executive of Exxon Mobil, as secretary of state, particularly because of his longstanding business connections with Russia and his close relationship with President Vladimir V. Putin, whom he has known for two decades. Mr. Trump said in a Twitter post on Monday night that he would make a formal announcement on the job on Tuesday morning.

Senators Lindsey Graham of South Carolina and Marco Rubio of Florida, both Republicans, have expressed concern about the reports of cyberattacks, as have numerous Democrats. But Mr. Rubio, in an apparent reference to Mr. Tillerson, went a step further on Monday, writing on Twitter, "Being a 'friend of Vladimir' is not an attribute I am hoping for from a #SecretaryOfState."

Mr. McConnell said the Senate investigation would be led by Senator Richard M. Burr, Republican of North Carolina, the chairman of the Intelligence Committee. Senator John McCain, Republican of Arizona, the chairman of the Armed Services Committee, will add a subcommittee to look into cyberattacks, led by Mr. Graham.

"The first thing we want to establish is, 'Did the Russians hack into our political system?'" Mr. Graham said in an interview on Monday. "Then you work outward from there. I have a high degree of confidence Russia did this."

Mr. Nunes, a member of Mr. Trump's transition team, said in a statement that the Intelligence Committee had been "conducting vigorous oversight of the investigations into election-related cyberattacks."

Mr. Nunes also noted that his committee would be scrutinizing the review of the Russian effort to influence the election ordered last week by President Obama.

Democrats have used the latest intelligence findings to renew their calls for an urgent inquiry. John D. Podesta, Hillary Clinton's campaign chairman, demanded on Monday that all information about Russia's meddling be declassified, and that the Obama administration explain what it knows about the hacking and when it knew it.

"We now know that the C.I.A. has determined Russia's interference in our elections was for the purpose of electing Donald Trump," Mr. Podesta wrote in a statement. "This should distress every American. Never before in the history of our republic have we seen such an effort to undermine the bedrock of our democracy."

Three Senate Democrats -- Benjamin L. Cardin of Maryland, Dianne Feinstein of California and Patrick J. Leahy of Vermont -- called on Monday for the creation of an independent, nonpartisan commission to comprehensively investigate allegations of Russian interference in the 2016 election.

But Mr. McConnell stopped short of calling for a special select committee, saying that the Senate Intelligence Committee was "more than capable of conducting a complete review" of the matter.

While he stopped short of saying whether he agreed that Russia had interfered in the election in support of Mr. Trump, Mr. McConnell said, "We need to approach all these on the assumption the Russians do not wish us well."

Mr. McCain was less equivocal, saying Monday that there was "no doubt about the hacking" by Russian intelligence services. He called the hacking of the Democratic National Committee and related accounts "another form of warfare" in an appearance on "CBS This Morning" with Senator Chuck Schumer of New York, the incoming Democratic leader.

And one week before the Electoral College meets to ratify Mr. Trump's election victory, 10 electors have demanded their own intelligence briefing on Russian efforts to elect Mr. Trump.

For his part, Mr. Trump was dismissive of the intelligence findings and suggested that Democrats were simply stirring controversy. "Can you imagine if the election results were the opposite and WE tried to play the Russia/CIA card. It would be called conspiracy theory!" Mr. Trump said in a Twitter post on Monday.

The White House press secretary, Josh Earnest, said that the administration would support a congressional review. He also rejected the notion that the administration had failed to adequately highlight the Russian efforts before the election, saying it had extensively briefed Congress all year about Russian electoral meddling.

"There has been intensive cooperation between the intelligence community and other national security agencies, and members of Congress in both parties, both before and after the election," Mr. Earnest said. "The briefings have been provided in a variety of settings, both classified and unclassified."

Even beyond the conclusions of the intelligence community, Mr. Trump's campaign had widely known and extensive ties to the Russian government. A campaign manager, Paul Manafort, had worked for the Russian-backed government in Ukraine, and Mr. Trump's choice for national security adviser, Lt. Gen. Michael T. Flynn, had consulted for a Russian-backed media group, Mr. Earnest noted.

Mr. Earnest said that Congress had a "special responsibility" to investigate the ties between the Trump campaign and the Russian government, because those connections were widely known before the election. He added that, for Capitol Hill Republicans, how to "reconcile their political strategy and their patriotism is something they're going to have to explain."

Wired
Trump Ignoring US Intelligence Creates Risks Beyond Russian Hacking
Monday, 12 December 2016
Byline: Andy Greenberg

New York - Observers and alumni of America's intelligence community have already fretted over Donald Trump's impending control of the world's most powerful spy agencies. They've worried that he could abuse their heady surveillance capabilities, turn them on his personal enemies, revamp the NSA's mass surveillance programs, and strip away domestic privacy protections once in charge. But before Trump

has even taken office, he's already found a less expected way to abuse the US intelligence community: Ignore, contradict, and insult it.
Trump's relationship--or lack thereof-- with US intelligence agencies isn't just a cause for political spectacle. According to national security experts and former intelligence agency staffers, it could have serious consequences that go well beyond the current dispute over Russian hacking.

The Russia Rift

On Friday, the Washington Post and New York Times reported that the CIA has confirmed that the Russian government repeatedly hacked and leaked Democratic Party documents throughout the presidential election season with the express intention of aiding Trump's campaign. That conclusion goes a significant step beyond earlier intelligence reports that had merely pinned the attacks on the Kremlin without naming its motive.

In response, the Trump transition team offered a brusque rejection of that finding: "These are the same people that said Saddam Hussein had weapons of mass destruction," read the Trump team's statement.

That abrupt dismissal of the intelligence community's findings follows months of Trump's assertions that no one can know the source of the last year's long series of political hacks--despite a publicly released report from the Office of the Director of National Intelligence and the Department of Homeland Security stating that Vladimir Putin's state- sponsored hackers were behind those breaches. "It could be some guy in his home in New Jersey," Trump maintained in a Time interview earlier last week.

The remarks build on what may be the most troubling recent revelation of all, that Trump has declined the traditional daily intelligence briefing given to presidents and presidents-elect. Instead, he receives the briefing only about once a week. "I get it when I need it," he told Fox News Sunday. "You know, I'm, like, a smart person."

That dismissal and disregard of the intelligence agencies' fact-finding represents a disturbing potential preview of the next four years, say former members of the US intelligence community who spoke with WIRED. They worry that it threatens to politicize the intelligence community's work, pushing it toward conclusions that will please the president rather than inform him. They say the growing rift demoralizes staffers, leading to a loss of valuable talent, and that it could leave the commander-in-chief himself dangerously ignorant of crucial world events.

Susan Hennessey, a former NSA lawyer who is now with the Brookings Institution, says that since Trump was elected, she's spoken with former colleagues who are still in the intelligence community who have been "stunned" to hear Trump's repeated rejections of their findings. "It's not outrage, although that might be under the surface," she says of her former colleagues' response. "It's real uncertainty and a sense of fear...shock, bewilderment, wondering what's going to happen next."

Playing Politics

Trump's kneejerk comparison of the Russian hacking report to the faulty intel on Saddam Hussein's weapons of mass destruction takes that dismay to another level, says one former CIA official who helped to write the president's daily briefing under both Obama and Bush. "We've never seen something like this before. It's pretty ballsy," says the former agency official, who requested anonymity because he's not authorized by his current employer to speak about political issues. "From dismissing the briefings to dismissing the current assessment on the Russia stuff, it seems like he's still in campaign mode. He's politicizing the intel, and that's a problem."

"Every administration has problems with some intelligence," says Patrick Skinner, a former CIA official under Bush and Obama who now works for the security consulting firm the Soufan Group. "But it really shouldn't be public. The open disdain Trump has shown for the agencies is unprecedented."

Trump's transition team didn't respond to WIRED's request for comment.

To be fair, Trump isn't the only skeptic of the intelligence agencies' findings. Neither the leaked CIA assessment that Kremlin hackers were motivated to help Trump nor the intelligence community's October report attributing the attacks to Russia have been backed up with published evidence. That's led Democratic members of congress Elijah Cummings and Eric Swalwell to demand a commission to independently investigate the hacking incidents. President Obama has directed intelligence agencies to conduct a renewed investigation into the attacks. And Republican Senators John McCain and Lindsay Graham joined with Democrats Chuck Schumer and Jack Reed to call for a congressional investigation into the hacker intrusions, splitting with Trump and other Republican leaders who have ignored or dismissed the Russian hacking reports.

In an interview on the CBS show Face the Nation Sunday, Senator McCain clarified that he doesn't doubt Russia was the source of the breaches of targets like the Democratic National Committee and the Democratic Congressional Campaign Committee, but still wants to better understand the motive of those attacks, and whether they targeted Republicans, too. What he doesn't dispute is that Russia was the source. "Now whether they intended to interfere to the degree that they were trying to elect a certain candidate, I think that's the subject of investigation," McCain said. "But facts are stubborn things. They did hack into this campaign."

Trump's doubt of the intelligence agencies' findings isn't the first sign that the divisiveness of the last year's presidential campaign has led to new, partisan distrust of the intelligence community's work, argues Dave Aitel, a former NSA staffer who now runs the security firm Immunity. That doubt had already surfaced with FBI director James Comey's public statements about the bureau's investigation of Hillary Clinton's private email server. The Clinton campaign and Democratic leaders have criticized Comey's behavior, accusing him of influencing the electoral process by writing a letter to Congress about new emails that surfaced in that investigation just weeks ahead of election day. "Our intelligence community has become a political football, and that's something that should never occur," says Aitel. "You need to have trust, and we don't have trust."

Broader Threats

Aitel says that lack of confidence in intelligence agencies' findings and politicization of their work has left his former colleagues increasingly "jaded." And he says that problem of low morale, already sunken after public response to the revelations of NSA leaker Edward Snowden, could lead to a dangerous brain drain from key agencies. "They don't complain, they don't whine to the press, they just leave," argues Aitel. "Then you get talent shortfalls, and then you get mission failures, which are bombs blowing up in American cities."

Compounding those issues are fears that Trump will continue to ignore his own intelligence apparatus, making uninformed decisions on the world stage, says ex-CIA officer Skinner. Some members of Trump's transition team have reportedly accepted daily intelligence briefings, including his pick for defense secretary, General James Mattis, and vice-president elect Mike Pence. But a president who wields ultimate executive power without that information could be dangerous, says Skinner. "If you close your eyes, the threat is still there: North Korea still exists, ISIS still exists," says Skinner. "These things are complex. You can't counter North Korea with gut feelings."

The rejection feeds back into the morale issue as well. "There's a firm belief in the intelligence community that the president having this information is a really important thing," says ex-NSA lawyer Hennessey. "When you have a boss essentially saying they don't believe or value your work--an outright rejection based on absolutely no evidence--there's a profound sense of uncertainty."

Beyond Trump's specific rejection of any inconvenient finding, Hennessey says it's that larger dismissal of the intelligence community that's most troubling. "If an intelligence agency produces a piece of evidence that's ignored, people can be killed," she says. "The consequences could be as dire as you can possibly imagine."

Radio Free Europe
Cyberattacks On Finance Ministry, Treasury
Monday, 12 December 2016
Byline: Christopher Miller

Kyiv - Ukrainian authorities are still looking for the culprits nearly a week after troublesome cyberattacks against official financial institutions that appeared to be designed to inflict maximum chaos on end- of-the-year payments.
But the head of staff of the Ukrainian Security Service (SBU) identified the so-called malware used in the December 6 attack as the same disruptive software employed in an unprecedented incident a year earlier, blamed on Russia, that cut off power to hundreds of thousands of homes in Ukraine.

Hundreds of thousands of hryvnyas' worth of remittances were delayed or stopped completely over the course of two days after hackers knocked the websites and payment systems of the Ministry of Finance, State Treasury, and pension fund offline, according to statements posted to those sites and local reports.

The National Police are leading the investigation and have discussed the case with the SBU, Oleksandr Tkachuk, chief of staff of the SBU, told RFE/RL on December 12.

The Finance Ministry, which described the incident as a "coordinated professional hacking attack," also claimed the attack had damaged its network equipment.

Tkachuk confirmed that "some data was destroyed and access to networks was blocked."

He said authorities were not prepared to discuss many details publicly because it would take time to fully assess them, adding that attribution in the cybersecurity sphere is a tricky business.

Tkachuk said the attack appeared to bear some similarity to a December 2015 attack against the Prykarpattyaoblenergo power company in Ukraine's western Ivano-Frankivsk region that cut power to hundreds of thousands of homes.

Critical Infrastructure

Ukrainian officials blamed that cyberattack on Russia and speculated that it might have been retaliation for Kyiv cutting off electricity one month earlier to Crimea, which Russia seized from Ukraine in early 2014.

But experts at the time warned that the greater message might be that hackers had the power to shut down critical infrastructure -- something that cybersecurity experts had long feared but never seen in practice.

Elizabeth Sherwood-Randall, a deputy secretary at the U.S. Department of Energy, also blamed Russia for the December 2015 cyberattack.

In that case, the hackers used malicious software called KillDisk, which deletes or overwrites data in system files, causing computers to crash.

KillDisk was also used in the December 6 attacks, the SBU's Tkachuk told RFE/RL.

Relations between Kyiv and Moscow soured after Russia forcibly annexed Crimea in March 2014, and Russia has been accused by Kyiv and Western powers of backing a separatist conflict in eastern in Ukraine that has killed more than 9,750 people.

Kyiv has on several occasions blamed Russia for cyberattacks -- including one on Ukraine's election system ahead of the presidential vote in May 2014 -- that it claims are part of Moscow's greater "hybrid war," a military strategy that combines conventional warfare, irregular warfare, and cyberwarfare.

Canadian Press
Trudeau must meet public's digital demands for inclusion, transparency: memos
Tuesday, 05 January 2016
Byline: Jim Bronskill

OTTAWA _ Justin Trudeau's advisers are warning that the federal government needs to do a better job of connecting with Canadians _ especially online _ in order to keep pace with ever-evolving public expectations.
The new landscape is being shaped by policy complexity, rapid technological change, limited finances and increasing demands for citizen involvement, say internal briefing memos prepared for the prime minister.

More and more, people expect the government to include them early and often in the design of policy and programming choices that affect them, say the notes, obtained by The Canadian Press under the Access to Information Act.

"There is a gap in Canada between how citizens communicate with each other and with private sector service providers (e.g. banks) and their experience with the federal government," says one memo.

In order to remain relevant to Canadians, the government needs to focus on delivering high-quality, factual digital content.

However, government is often bogged down by red tape, the need for signoffs from various layers of management and barriers to effectively spending money and assigning people to tasks, the notes say.

The memos point out other problems and hurdles:

_ the access-to-information system that allows people to make formal requests for government files is "time-consuming and expensive to administer";

_ Canadians are "broadly concerned and uncertain" of how the government uses their personal information, whether it be for law enforcement, national security or other purposes;

_ the government is grappling with cyberthreats to its information holdings from so-called 'hacktivists,' criminals and others.

The notes suggest updating the outmoded 2006 federal communications policy to reflect the "voracious demand" from Canadians for online information and the rising use of mobile devices.

Information published on the prime minister's website and social media accounts must be factually accurate and non-partisan _ tenets that should be enshrined in a new communications policy, the advisers say.

Government advertising is seen to be "partisan in nature" at times, another shortcoming that must be addressed in the revised policy, the notes stress.

The Conservative government was pilloried by critics for lavish multimillion-dollar ad campaigns that seemed to convey little useful information.

The Privy Council Office is already working with Treasury Board officials to ensure potential amendments to the policy include "clear accountabilities for non- partisanship" when it comes to ads.

These days, many policy problems _ from climate change to terrorism and security _ develop and shift rapidly and unexpectedly, with little time for government to analyze and respond effectively, the notes say.

The federal public service is responding by trying to support innovation across government and highlighting successful pilot projects and new approaches.

For example, Heath Canada is using number-crunching tools to assess and predict whether imported consumer goods are likely to comply with health standards before they enter Canada.

The Trudeau government "could consider making a high-level, public commitment" to encourage departments to take such new paths, the notes say.

However, other challenges lie in attracting young, skilled workers to the public service and ensuring federal agencies are free of harassment and discrimination.

iPolitics.ca
Feds must work with partners to limit threats to safety: Transport Canada
Tuesday, 05 January 2016
Byline: Amanda Connolly

Emerging safety threats in the transportation sector will require greater cooperation between the federal government and its provincial, municipal, international and private sector partners, newly released Transport Canada documents say.
The transition briefing documents -- notes prepared by senior bureaucrats for an incoming minister after a change in government -- were published online Monday by Transport Canada, among other departments.

The Transport Canada briefings outline several key concerns for Liberal Transportation Minister Marc Garneau as he adjusts to his new portfolio, among them the need to move away from "rigid regulatory

structures" to better respond to attacks on airlines and the formulation of new laws and regulations to ensure safe use of new technologies like drones and driverless cars.

According to the document, transportation remains a target despite the shift from global terror attacks to lone-wolf style attacks, and that it is bringing new costs and privacy concerns for transportation providers and travellers.

"Mitigating the risks from such random, decentralized sources generates new costs for industry and government, and new inconveniences and personal privacy concerns for travellers," it says.

The notes also say risks are becoming more difficult to predict and that "modern, effective and efficient oversight systems" will be key to mitigating the risks posed to transportation from attackers and other dangers.

In particular, it suggests that there needs to be less focus on "rigid regulatory structures" and more focus on identifying flexible alternatives that will let regulators respond to rapidly changing threat environments, noting that being able to access and manage data will be "critical" to facilitating that process.

As well, Canada needs to get better at regulating new "disruptive technologies" like drones and driverless cars -- or risk being left behind as the emerging technological sector grows.

"Oversight of unmanned aerial vehicles (UAVs) and driverless cars in particular may require new regulation and legislation to ensure commercial and private use is safe and secure," the document says. "Need faster development of policies and regulatory frameworks to support growth potential of these sectors or risk being left behind."

One of the challenges for the government in regulating the sector is the speed at which new technologies are being developed, the briefing notes say.

As well, the need to work with other countries to harmonize regulations has been challenging for regulators.

Overall, the document argues that government needs to take a proactive role in communicating risks and working with partners to create regulations to address emerging threats and comes on the heels of heated debate throughout the election about what steps the government should take to keep Canadians safe from attacks by extremists.

It also follows an initiative by transportation officials to step up regulation of drones: as iPolitics reported last summer, Transport Canada said that it intends to introduce new regulations in 2016 for drones weighing less than 25 kilograms that are operated within sight of the controller.

Those rules will likely see small drones treated more like cars: it's expected users will need to obtain a pilot permit and be at least 16 years of age to operate the drones -- or 14 years old if they have adult supervision.

Operators of the smaller model drones would also be required to obtain training as part of the permitting process and pass a Transport Canada written exam, which would be created specifically for UAVs, and the drones would have to be registered and marked.

Canadian Press/Presse Canadienne
Military investigating alleged security breach at intelligence centre
Tuesday, 05 January 2016

HALIFAX - Military police in Halifax are investigating an alleged security breach at one of the Royal Canadian Navy's most sensitive security operations.

According to court documents, military investigators allege that between 2004 and 2009 a web designer working at HMCS Trinity -- the military's principal East Coast intelligence centre -- used Defence Department networks to improperly store secret files.

A search warrant filed in provincial court alleges the actions of a man identified only as "Mr. Zawidski" violated a section of the federal Security Information Act that deals with wrongful communication of information.

None of the allegations has been proven in court and a military spokesman couldn't confirm whether charges have been laid.

The warrant says military police seized four hard drives, a laptop computer, some CDs and floppy disks from Zawidski's Halifax office at HMCS Dockyard in September following a complaint about a possible security breach.

The document says Zawidski's personal network drive contained 1,086 secret documents, dated between 2004 and 2009.

The Cipher Brief
Cyber Espionage
Monday, 04 January 2016
Byline: John Sipher

Comment - For years, I slept fitfully after a "friend" told me that it wasn't the noisy mosquitos buzzing in my ears at night that were a problem. Instead, it was the female mosquitos that made no noise at all but

laid eggs in your ears at night. That image wrecked my sleep until the Internet helped me to dispel the myth years later.
The cyber threat is a little like the silent mosquito. The biggest dangers are the ones that you will never know about.

However, if you follow the public discourse on the nature of the cyber threat to the U.S., it seems that the bulk of the dialogue has to do with the issue of hackers and the thousands of daily thwarted attacks against government and private computer systems. It is almost as if the danger is easily detected, and a better password and up-to- date antivirus software can solve the problem.

However, the far bigger threat is from foreign intelligence and terrorist groups, who have the talent, resources, and wherewithal to do serious damage to U.S. interests - damage we may never realize until it is too late. While we publically frame the problem by citing how many attacks are observed every day, the far bigger problem is hidden. An intelligence organization's job is to pick your pocket without you ever knowing anything is amiss. You won't make it very far as an intelligence officer if your adversary becomes aware of your activities.

Of the capable organizations that are determined to do us harm, perhaps the most competent, dedicated, and focused is Russia's Special Communications Service, the Russian equivalent of the U.S. National Security Agency (NSA).

Russia doesn't do many things well (dancing bears, perhaps). Spying, however, is a Russian specialty honed by decades of experience controlling its population and stealing from the West. The U.S. has been their main enemy since WWII and remains so today. Indeed, while we more often hear about Chinese cyber activities, the Russian cyber espionage enterprise is far more sophisticated and capable than its Chinese counterpart, according to statements by U.S. intelligence officials.

Unlike in the U.S., the Russian espionage effort is central to its foreign policy, and its offensive cyber capability is a particularly powerful weapon that is used to challenge the U.S. across the board. Indeed, the Russian NSA equivalent is used for - among other things - cyber warfare, espionage, counterintelligence, internal control of its citizens, disinformation, and propaganda. Russia's cyber attacks - both blatant and stealthy - are used to achieve geopolitical ends and to maintain an asymmetric ability to damage the U.S.

The Russians have shown a willingness to use the cyber weapons at their disposal, and have done so effectively. In 2007, the Russians swamped Estonian computer systems to express their anger at perceived Estonian disrespect of Russian symbols. A year later, they combined sophisticated cyber intrusions with their military attack against Georgian forces. More recently, they used offensive cyber tools to support their aggressive annexation of Crimea and eastern Ukraine. We even witnessed Russian cyber probing of top U.S. financial institutions in 2013.

Internally, the Russians use cyber weapons to maintain control over their population. By law, all private encryption equipment in Russia is required to be licensed by Russian Intelligence. Likewise, all internet providers in Russia have to install hardware/equipment provided by the Russian NSA equivalent (and pay for it themselves). There is no such thing as privacy in Russia.

While the U.S. Government is probably the biggest target of Russian cyber spying, you can be confident that they go after anyone and anything that can help them get what they need. They surely steal directly from Yahoo, Google, Facebook, and social media platforms. If they want to collect compromising information on a person in a bank, military unit, national laboratory, or nuclear power plant, you can be sure that they are swimming in e-mail and personal data that can help them craft an approach to that individual.

At the same time, the Russians are collecting the capability to understand and possibly disrupt our power grid, air traffic control, oil and gas infrastructure, and transit networks. Additionally, recent reports cite a significant increase in Russian submarine surveillance activity in the vicinity of the strategic underwater fiber cables that facilitate commercial and classified communications. This aggressive effort has intensified fears of Russian efforts to tap or cut these critical deep sea communication conduits that carry trillions of dollars a day in global business.

The only real way to protect ourselves from this kind of sophisticated cyber warfare is a robust public-private partnership between our intelligence and law enforcement services, and those companies that provide the backbone of our computer networks. In this sense, perhaps the most damaging of Edward Snowden's many traitorous acts was to destroy the trust between the private sector and our security professionals. We are now talking past each other, and the Russians, Chinese, Iranians, and others are having a field day. Until those key relationships and trust is restored, we will remain in a vulnerable state.

So, the next time you hear a story about hackers attacking various computer networks, think of the buzzing mosquito, and remember that there is probably something much more dangerous happening away from public notice.

Note: John Sipher is a senior project leader at the McChrystal Group. John retired in 2014 after a 28-year career in the Central Intelligence Agency's National Clandestine Service.

NL Times
Dutch will not force "backdoors" on businesses: no limits to encryption
Monday, 04 January 2016
Byline: Zack Newmark

The Hague - The Dutch cabinet has no plans to force businesses to build in "backdoors" for investigative agencies to snoop on data, Security and Justice Minister Ard van der Steur told parliament on Monday.

The ruling coalition sees the privacy and security provided by encryption methods as being more important than making it easier for authorities to access information.
Van der Steur noted that more businesses and individuals are making use of encryption. "That is important for the confidence people have in digital products and services, and for the Dutch economy from the perspective of the fast developing digital society," the minister said in a letter.

Simultaneously, he said that encryption often hinders investigations, particularly into child pornography, cyber attacks, support of foreign military operations and terrorism. "[Encryption] makes it difficult, slow or impossible to gain timely insight into communications for the purpose of safeguarding national security and the investigation into criminal offenses," he stated.

"The above-mentioned legitimate access to data and communications through investigation, intelligence and security services, however, constitutes an infringement on the confidential communications of citizens."

The minister also said that forcing firms to install a backdoor creates an opening for criminals and terrorists to access data that can then be used in an illicit act.

Gulf News
Social media campaign highlights Taiz plight
Tuesday, 05 January 2016
Byline: Saeed Al Batati

Al Mukalla - Yemeni activists have turned to social media networks to draw the world's attention to the plight of tens of thousands of people who live under Al Houthis siege in the city of Taiz and pressure the militants to allow international organisations to enter aid to the city.
Activists who initiated #endtaizsiege hashtag on Saturday say that the online campaign have reached over a thousand of people online.

Latifa Ali, a Yemeni journalist based in the United States, told Gulf News that she and many other activists decided to turn to social media after diplomatic and military efforts failed to end months of crippling blockade on the city. "Due to the disregard of the international community, we turned to other alternatives."

The activists widely shared photos of people from the city climbing rough and mountainous roads carrying vital food and medical supplies. "We want to put pressure on Al Houthis to open a corridor for humanitarian aid so that it can reach residents in the besieged city."

Despite the calls for mercy, Iran-backed Al Houthis have tightened their siege and intensified their shelling of Taiz.

Mohammad Al Qubati, a medic and the head of the Supreme Medical Committee, told Gulf News that nothing has changed on the ground and the city is still experiencing a devastating humanitarian crisis.

"Injured people die in hospital emergency rooms because there is neither medical oxygen cylinders or medicine. We were forced into sending an appeal to residents who might use oxygen cylinders to treat relatives to send them to local hospital."

Al Qubati said that they carry the dead and injured people on donkeys because ambulances cannot move due to shortage of fuel and the intensity of the shelling.

"We have recently managed to collect 20 oxygen cylinders from locals. But each hospital in the city needs between 170 to 200 cylinders. Drugs that are carried on the donkeys and camels spoil before arriving in hospitals because of the sun heat." At least five civilians are killed every day from shelling and fighting, he said.

The densely populated city has been on the frontline of the continuing civil war between government forces and Al Houthi militants and their allied forces since March.

Resistance fighters loyal to president Abd Rabbo Mansour Hadi are in control of the city's main districts but Al Houthis control the suburbs.

Meanwhile, on the ground, army commanders battling Al Houthi militants in the southern Al Shourejah region said they foiled an assault by Al Houthi militants to recapture the region in the province of Taiz.

"The warplanes targeted Al Houthis gatherings in many places in Al Shourejah an destroyed Katyusha rockets and mortar shells launchers." a senior army officer who preferred to anonymous because he was not authorised by his seniors to brief reporters told Gulf News from the battlefield. Across the country, warplanes from a Saudi-led coalition escalated air raids on military sites controlled by Al Houthis and their allied forces after the ceasefire was officially ended on Saturday.

Residents in the capital reported huge explosions on Sunday and Monday in the Special Security camp, Al Daylami air base and many other areas.

The warplanes also attacked an air defence camp in the western city of Hodeida. According to local media reports, the coalition jet hit Sanhan, a Saleh stronghold and his hometown in the Sana'a province. Saudi Arabia formed a coalition with some allied Arab countries early last year and began in March bombing Al Houthis militants who were quickly advancing in many provinces. The coalition blunted their expansion and helped the exiled government to return to the port city of Aden.

London Times
Hackers thwart online efforts to trap Jihadists
Tuesday, 05 January 2016
Byline: Fiona Hamilton

London - Teams of hackers who are taking down online jihadist accounts may be harming counter-terrorism efforts, one of Europe's most senior law enforcement chiefs has warned.
Rob Wainwright, the director of Europol, told The Times that the hackers, who are disabling thousands of pro-Islamic State accounts, may be thwarting the work of police and intelligence agencies.

British and European security services regularly monitor jihadist websites and may allow them to continue operating online if they are providing useful information about the whereabouts of Islamists and their plans. Hacking collectives such as Anonymous have declared war on the jihadists after the terrorist attack in Paris and have threatened to take down thousands of their internet accounts. Law enforcement agencies now fear that the hackers could be doing more harm than good. Mr Wainwright said that Europol and Scotland Yard already had teams dedicated to assessing jihadist online activity and disabling their social media accounts when appropriate. They were best placed to make such decisions, he said.

"Sometimes the timings of the social media account takedowns [by the authorities] will be deliberate, and part of wider concerted action," he said. "The point is that where it is done in an independent way, clearly unconnected with what we are doing, we lose control of it. We can't therefore ensure that the intended effect is the right one."

Mr Wainwright said that Europol did not want to encourage hackers, whose crimes were often investigated.

Security experts agreed that interference by hackers could cause problems, but said that their knowledge should be used by the intelligence services. Will Geddes, managing director of International Corporate Protection, said that Anonymous had a fantastic pool of capability. "They could be massively helpful in fighting against terrorism and radicalisation," he said.

Ukraine Utility Cyber Attack Wider Than Reported: Experts
Tuesday, 05 January 2016
Byline: Staff report

Frankfurt - A central European security software firm said on Monday that a cyber attack last month in Ukraine was broader than initially reported last week when the nation's secret police blamed a power outage on Russia.

Western Ukraine power company Prykarpattyaoblenergo reported an outage on Dec. 23, saying the area affected included regional capital Ivano- Frankivsk. Ukraine's SBU state security service responded by blaming Russia and the energy ministry in Kiev set up a commission to investigate the matter.

While Prykarpattyaoblenergo was the only Ukraine electric firm that reported an outage, similar malware was found in the networks of at least two other utilities, said Robert Lipovsky, senior malware researcher at Bratislava-based security company ESET. He said they were ESET customers, but declined to name them or elaborate.

"The reported case was not an isolated incident," he said.

Prykarpattyaoblenergo publicly blamed its outage on "interference" in the working of its system. The Kremlin did not respond to a request for comment.

Researchers with computer security firms Trend Micro and iSight Partners said ESET's assessment that the attackers sought to infect other utilities appeared credible, shedding new light on evidence that this is the first power outage proven to have been caused by a cyber attack. Experts have warned for years, with growing urgency, that electric utilities are vulnerable to cyber attacks that could cut power.

"This is the first time we have proof and can tie malware to a particular outage," said Trend Micro senior researcher Kyle Wilhoit. "It is pretty scary."

Cyber firm iSight Partners said that ESET's report of multiple attacks is consistent with its own analysis.

"There is pretty strong consensus that there was a blackout caused by a computer network attack," said iSight's director of cyber espionage analysis, John Hultquist.

Experts with ESET, iSight and Trend Micro told Reuters the attackers used a malicious software platform known as "BlackEnergy" to access utility networks, planting a related piece of malware, "KillDisk," on targeted systems.

KillDisk can delete or overwrite data files.

Researchers say they have yet to determine whether KillDisk's job was to knock out power or simply conceal the attack.

Cyber criminals have been using versions of BlackEnergy since 2007. Over the past two years, there has been widespread reports that a Moscow-backed group, Sandworm, was using it for targeted attacks.

The Hindustan Times
Hackers Eye Spies

Tuesday, 05 January 2016

New Delhi - Community to monitor officers leaking info to international spies gearing up to keep a close eye on serving and retired defence personnel to ensure they are not passing information to international spies on the virtual world.
The move by hacking community is to ensure that no information is being leaked via social networking websites, which can be used against the nation. The step was taken after reports of defence personnel's involvement in the ISI spy racket surfaced.

The Crime Branch of Delhi Police on Monday arrested IAF airman Ranjith KK, who was honey trapped by ISI agency by creating a fake profile on Facebook. He had been talking to " pretty woman" Damini McNaught for the last several months on Facebook and was passing sensitive details related to the Air Force.

Recently, security agencies arrested serving and retired defence personnel from various locations who were leaking information to Pakistani security agency ISI. " We will follow the modus operandi used by international agents. We will track Indian officers and will try to get information from them.

The moment they pass any information, we will alert the security agency giving proof against them," said a hacker who claims to be a part of ethical hacking community Anonymous- India.

There are close to 2,000 retired and serving officers who are under the scanner of security agencies for suspectedly passing information for money or through honey trap.

Admitting the process of tracking is illegal, hackers said the move is in national interest. " It is an illegal and a time taking process but the underground community is ready for surveillance to shield the country from outsiders," said a hacker on the condition of anonymity.

Cyber experts claim that international spies from countries like Pakistan, US and China have maximum interest in gathering information from India.

The international spying agencies, in order to make their spying activities seamless, untraceable and invisible, also carry out high- tech attacks which compromise the computer and network, but they carry out targeted attack on social media so that they get insider classified information.

"Spies have created many fake profiles on social media. These profiles are of different nature which includes different sex, age, cast and nationality with distinct interests.

They use it according to their targets. A dedicate team of spies is working to track vulnerable people on social media," said cyber crime expert Kislay Choudhary, who works closely with Delhi and Noida police.

"As a person discloses that he works for Army, Navy or the Air Force, he/ she comes on the radar of international spies who start following them on the virtual world.

By some means, which includes honey trap, they start interacting with the user. Spies also keep a track of their interest or hobbies to make a conversation and get friendly," Choudhary explained.

Experts claim spies from countries like Pak, US and China have maximum interest in gathering info from India Community to monitor officers leaking info to international spies.

Fars News Agency
Saudi Defense Ministry's Website Hacked in Protest at Sheikh Nimr's Execution
Tuesday, 05 January 2016

Tehran - A group of young Saudi hackers took down the website of Saudi Arabia's Defense Ministry to show their protest at the execution of prominent Shiite cleric Sheikh Nimr Baqir al-Nimr by the kingdom. The Saudi defense ministry's website was hacked on Sunday night by a group of Young Saudis called 'Brave Youth Fighting Religious Taboos' and it was inaccessible for several hours.

The hackers said their cyberattack on the defense ministry's website was meant as a retribution for the execution of Sheikh Nimr by the Riyadh government.

"We will continue defending the religious sanctities and also targeting the enemies and oppressors involved in the killing of the freedom-seekers and revolutionaries," the hackers said in a statement issued after hacking the website.

Saudi Arabia announced on Saturday that it had executed the prominent Shiite Muslim cleric. Hours later, Sunni and Shiite Muslims from across the world rushed to condemn his execution, vowing revenge.

In a relevant development in May, the internal Internet network belonging to the Saudi Foreign Ministry had come under a cyber-attack.

The cyber-attack disclosed over 1 million secret and classified documents of the Saudi government which showed the kingdom's hostile and devilish policies against other countries of the world, including their support for the terrorists in Syria and Iraq.

The National (UAE)
When hacking got personal in 2015 (Canada).
Tuesday, 05 January 2016
Byline: Peter Nowak

Abu Dhabi - If there is any lesson that using the internet in 2015 taught us, it's that it's getting increasingly difficult to avoid having our personal data stolen by hackers.
From children's toys and hotels to mobile phone companies and insurance brokerages, virtually no one was safe from malicious breaches. And, if anything, hacking became a little more personal - and a little meaner - in 2015.

In June, hackers stole the records of at least 22 million United States government workers stored with the Office of Personnel Management. The full repercussions of the breach - considered the most damaging in US national security so far - aren't yet known, but analysts are worried about the potential for blackmail of government employees by enemy powers armed with the sensitive information.

The US-based healthcare providers Anthem and Excellus BlueCross BlueShield had 80 million and 10 million customer records leaked, respectively, in September and February. Birth dates, addresses and social security numbers were included, exposing millions to potential identity theft and fraud. Law-enforcement officials failed to identify the perpetrators.

The records of 2.4 million customers, including up to 900,000 credit card numbers, were stolen from the UK electronics retailer Carphone Warehouse in August. Even LastPass, an online tool that helps users manage their many different passwords, was hit in June. The breached data was encrypted and the company said damage was minimal, but users were, nevertheless, urged to change their passwords. The list goes on and on

Many of the victims in the disparate breaches were forced to deal with identity theft and financial turmoil, and the only thing that kept the breaches from wreaking a sort of collective mass havoc was - seemingly - the hackers' own good graces. But even those, if they exist at all, appear to be running out.

In July, hackers calling themselves The Impact Team announced they had stolen data from adultery-enabling website Ashley Madison. The group threatened to release the information, which included the names and home addresses of the site's 39 million members, unless it shut down immediately.

When the Toronto-based parent company, Avid Life Media, did not comply, the hackers dumped gigabytes worth of usernames and credit card transactions, plus sensitive emails from executives.

Among the revelations in those correspondences was the fact that company founder, Noel Biderman, a married man, had multiple affairs despite previous denials about infidelity. Examination of the data also revealed that most of the site's female users were fake and that the company failed to delete user accounts even after charging fees to do so.

The fallout for users was more pronounced. Heads rolled as judges, politicians and teachers were outed as members. Families split up and fears of blackmail spread fast. A New Orleans pastor and Ashley Madison user, fearing he too would lose his job, committed suicide.

Adultery is an ethical issue, but regardless of where one stands on it, at the heart of the breach lies the fact that the Ashley Madison hackers appointed themselves moral arbiters of the site and - by extension - its users. Avid Life Media is facing a US$567 million class-action lawsuit and will probably never recover the trust of its users, even if it is claiming to have added four million new members since the breach. But the social ramifications for its users, imparted by self-appointed judges, marked it as a different kind of hack.

Ethically motivated breaches against wrongdoing companies, governments or institutions have been happening for years but in 2015, their perpetrators seemed to care less about the everyday people caught in their wake, and not just in the Ashley Madison case.

Bombastic and divisive US presidential candidate Donald Trump was also targeted last year, with his hotel chain announcing in October that it had been the victim of a year-long breach. Hackers may have gained access to thousands of customer credit card numbers during that period, the chain said.

While Mr Trump may have suffered a personal knock to his brand and reputation, as the hackers desired, the true victims - the ones who likely had to deal with the financial fallout of having their data stolen - were guilty of no crime other than staying in hotels bearing his name.

Hackers in September also went after Patreon, a Kickstarter-like crowdfunding site used by independent artists and creators to support their small-scale initiatives. The perpetrators and motives are unknown, but Patreon is the veritable opposite of the corporations normally targeted by hacktivists. Why they would want to harm independent creators trying to eke out a living through online donations is a disturbing question.

Closing out the year, hackers in November stole 4.8 million records from Hong Kong-based toy maker VTech, leaking the names, genders and birthdays of more than 200,000 children. One of the individuals who claimed responsibility later said he just wanted the company made aware of security failings that allowed the hack to be fixed. Whether the hacker was aware that thousands of children had been exposed to potential miscreants is unknown.

There's little doubt that data breaches were one of the biggest stories of 2015 and, unfortunately, they will not be going away.

But with hackers increasingly appointing themselves arbiters of the moral behaviour of institutions and individuals, and the effects of their actions having more profound social effects than just simple financial damages, authorities are heading into this year facing more pressure to take action against what is a growing epidemic.

Canadian Press
Top courts threaten federal government with legal action over new IT rules
Thursday, 07 January 2016
Byline: Jordan Press
Section: general

OTTAWA _ Newly released documents show the country's highest court is ready to launch a legal battle with the federal government over new IT rules which the Supreme Court of Canada fears would threaten its independence.
The Supreme Court is not alone in these concerns: the Federal Court, Federal Court of Appeal, Court Martial Appeal Court and Tax Court are all prepared to launch a constitutional challenge against having the government's super-IT department involved in their digital affairs.

The federal Liberals are now left to decide how to handle an issue created by a decision of the previous Conservative government that came into effect during the federal election.

That decision forced the courts to go through Shared Services Canada for all IT purchases, such as servers, routers and software, rather than letting them make the procurements on their own. The courts had that power until Sept. 1, when the new rules kicked in and made them a "mandatory client" of Shared Services Canada, which oversees purchases and digital services for 43 of the heaviest IT users in the federal government.

The move approved by the Conservative cabinet in May 2015 was supposed to save money, since Shared Services Canada buys in bulk for the federal government, and improve digital security, because Shared Services Canada buys from safe suppliers.

Briefing material provided to Prime Minister Justin Trudeau shortly after he took office shows the courts were worried that having a government department involved in their IT services "and the perceived implications for control of their data" infringed on judicial independence.

"They must maintain control of their data, not only because of concerns about confidentiality, but also because an independent judiciary cannot tolerate having its sensitive information controlled by a separate branch of government," reads part of Trudeau's briefing on urgent issues facing the new government.

In an August letter to the government's top bureaucrat, officials for the courts argued that they shouldn't be subject to Shared Services Canada's oversight and should be exempt like agents of Parliament, including the auditor general, privacy commissioner and information commissioner.

If the government doesn't backtrack on the cabinet decision, the country's top judges "are prepared to take legal action," Trudeau was warned.

The advice Trudeau received in the secret briefing material has been blacked out from the documents obtained by The Canadian Press under the Access to Information Act.

A spokeswoman for Public Services Minister Judy Foote, who oversees Shared Services Canada, has yet to respond to questions about what the Liberals plan to do with the courts' complaint.

Shared Services Canada, in an email, would only say that everything the agency does is "aligned with all legislative and legal requirements," including "the need to maintain judicial independence." The department didn't say how exactly that works.

The Guardian (London)
Web services firm CloudFlare accused by Anonymous of helping Isis
Thursday, 07 January 2016
Byline: Alex Hern
Section: general

London - Anonymous has attacked web services startup CloudFlare for providing protection against cyberattacks to pro-Isis websites.
The company protects customers against the distributed denial of service (DDoS) attacks popular amongst groups like Anonymous by routing connections through its own content delivery network. By weeding out malicious connections, it prevents DDoS attacks from succeeding in their goal of overwhelming a website with traffic so that it collapses.

But according to members of Anonymous, which has reaffirmed its yearlong "war" against Isis following the Paris attacks, that technology is also being used by pro-Isis websites to protect themselves against the hacktivist collective's attempts to bring down their servers.

The week before the Paris attacks, Ghost Security, an Anonymous- affiliated "counter-terrorism network", counted almost 40 websites that use CloudFlare's services to protect their content. According to GhostSec, 34 were propaganda websites, four were discussion forums, and two offered technical services.

Such accusations are nothing new to CloudFlare, which has long argued that it is not its job to police content on its network. In August 2013, in response to similar allegations from James Cook, a reporter at the Kernel magazine, the company's chief executive Matthew Princepublished a blogpost laying out its view on free speech on its network.

Prince wrote: "A website is speech. It is not a bomb. There is no imminent danger it creates and no provider has an affirmative obligation to monitor and make determinations about the theoretically harmful nature of speech a site may contain ...

"If we were to receive a valid court order that compelled us to not provide service to a customer then we would comply with that court order. We have never received a request to terminate the site in question from any law enforcement authority, let alone a valid order from a court."

In response to the latest criticism from Anonymous, Prince has redoubled his stance. "I did see a Twitter handle said that they were mad at us," he told The Register. "I'd suggest this was armchair analysis by kids - it's hard to take seriously. Anonymous uses us for some of its sites, despite pressure from some quarters for us to take Anonymous sites offline."

"Even if we were hosting sites for Isis, it wouldn't be of any use to us ... I should imagine those kinds of people pay with stolen credit cards and so that's a negative for us."

Those statements are now prompting a further call amongst Anonymous members to boycott the company altogether.

The Guardian has not received a response to a request for comment from Cloudflare.

Wall Street Journal
NSA Safeguards to be considered
Thursday, 07 January 2016
Byline: Adam Entous
Section: general

Washington - The U.S. House Intelligence Committee will consider whether new safeguards are needed for handling communications intercepted by the NationalSecurity Agency that involve U.S. lawmakers or other Americans, the top Democrat on the panel said on Wednesday.
The move follows a report in The Wall Street Journal about how the NSA targeted Israeli communications during the 2015 congressional debate over a nuclear accord with Iran. The Journal said the NSA targeted the communications of Israeli Prime Minister Benjamin Netanyahu and other senior Israeli officials, and, in so doing, swept up the contents of some of their private conversations with lawmakers and Jewish-American groups.

At the request of the committee's chairman, Rep. Devin Nunes (R., Calif.), members of the panel on Wednesday received a classified briefing from intelligence agencies about how they handled intercepted Israeli communications "to, from or about" lawmakers, officials said.

Current and former U.S. officials declined to say whether the communications in question were between Israeli officials and U.S. lawmakers directly, or whether they were Israeli officials discussing their contacts with members of Congress after the fact, or both.

CNN.com
Top intel officials say NSA didn't spy on members of Congress
Thursday, 07 January 2016
Byline: Dierdre Walsh
Section: general

Washington - Top U.S. intelligence officials told the House Intelligence Committee Wednesday that the National Security Agency did not spy on any members of Congress during last year's contentious Iran nuclear debate.
The testimony came in response to concerns raised by the panel about a Wall Street Journal report last month that said the U.S., while surveilling U.S. allies, also snooped on some members of Congress, according to members of the House Intelligence Committee who attended a classified briefing on the matter.

"They were not listening to or monitoring representatives or members of Congress," Utah Republican Rep. Chris Stewart, who serves on the panel, told CNN.

The Journal reported that the NSA conducted surveillance of Israeli Prime Minister Benjamin Netanyahu and inadvertently picked up conversations with members of Congress about the controversial nuclear agreement with Iran that Congress debated over the summer and fall. Netanyahu was a strong critic of the deal, and he and his administration communicated with members on Capitol Hill regularly during the negotiations and around the vote on legislation to allow the deal's implementation.

The Journal detailed how the NSA's surveillance of Netanyahu and other top foreign leaders who are close allies of the U.S. continued, even after President Barack Obama insisted more than two years ago that he would end the practice.

On Wednesday, James Clapper, the director of the National Intelligence Committee, and NSA Director Adm. Mike Rogers told members of the House Intelligence Committee that no conversations including members were monitored.

The top Democrat on the Intelligence Committee, Rep. Adam Schiff, D-California, told CNN in a written statement that "There is no evidence that the intelligence community was spying on members, or that the laws and procedures governing any incidental collection on members of Congress were violated in any way."

Citing the classified nature of the briefing, members declined to discuss any issues surrounding any reported monitoring of Netanyahu.

After the Journal's report, House Intelligence Committee Chairman Devin Nunes announced his committee would investigate after the holiday recess, and Wednesday's classified briefing was the first opportunity to press Clapper and Rogers about the details of the report.

Stewart told CNN that officials admitted they didn't know the source of the Journal story, but were doing their own formal investigation to determine the source.

Another Democrat on the committee declined to get into specifics, but said he was satisfied after the session.

"I've been briefed on the matter. I asked tough questions of the panelists and am satisfied that all procedures were followed by the Intelligence Community," California Democratic Rep. Eric Swalwell told CNN after the closed door briefing, adding, "I will continue to be vigilant in making sure that all citizens and their constitutional rights are protected."

A source close to the House intelligence panel said the committee received a lot of the information it requested from the intelligence community about the allegations in the Journal story, and it has not decided what further steps it will take on the matter.

Reuters
U.S. power companies told to review defenses after Ukraine cyber attack
Thursday, 07 January 2016
Byline: Jim Finkle
Section: general

Boston - A quasi-governmental U.S. electric industry group last week advised members to review network defenses following reports that 80,000 customers of a Western Ukraine utility lost power for six hours following a cyber attack.
The Electricity Information Sharing and Analysis Center, or E-ISAC, urged members to "do a better job" at implementing multiple layers of defense against potential cyber attacks, saying the incident at Ukraine's Prykarpattyaoblenergo electricity provider appeared to be the result of a "coordinated effort by a malicious actor."

The nine-page confidential document, reviewed by Reuters, did not identify deficiencies in the U.S. grid that could lead to similar attacks.

Security experts said businesses in many sectors were closely following the Ukraine incident because it was a watershed event: the first known cyber attack to take down an electric grid. It was also one of just a handful of known cyber attacks that have damaged any kind of physical infrastructure.

Kimberly Mielcarek, a spokeswoman for E-ISAC, said that the organization would continue to provide more data as it pursued an investigation with help of the federal government.

"There is no credible evidence that the incident could affect North American grid operations and no plans to modify existing regulations or guidance based on this incident," she said in an emailed statement.

Prykarpattyaoblenergo reported an outage on Dec. 23. Ukraine's SBU state security service blamed Russia and the energy ministry set up a commission to investigate. A ministry spokesman said on Wednesday that the results will not be released until after Jan. 18.

The Kremlin has not responded to requests for comment.

The U.S. Central Intelligence Agency, Department of Homeland Security, Federal Bureau of Investigation and White House National Security Council all declined to comment on efforts to probe the incident.

The E- ISAC report identified systems integrator Galician Computer Co as having worked for Prykarpattyaoblenergo and two other utilities that were reported to have been targeted in the attack but did not experience outages: Chernivtsioblenergo and Kyivoblenergo.

"The integrator is the single point of connection between various regional electrical entities in the Ukraine that were exposed to this attack," the report said.

Galician Computer Co told Reuters via email that it had provided software to only one of the three firms and was not involved in running any of the plants.

"According to reports from employees at that regional power firm, attacks were definitely carried out and led to blackouts," the statement said. "We do not have any other information regarding this incident."

Fox News
Clinton's private email account exploits FOIA loophole, report says
Thursday, 07 January 2016
Byline: Catherine Herridge, Pamela Browne
Section: general

Washington - Hillary Clinton's unorthodox use of a private email account and personal server for government business exploited a loophole in the State Department's FOIA, or Freedom of Information Act, process, according to the findings of the first Inspector General report to stem from her email scandal.
Congress asked the Office of Inspector General, the State Department's independent watchdog, to investigate the issue following the revelation that Mrs. Clinton did not use a government email account while secretary of state.

Fox News reviewed the 25-page report and its findings before they were made publicly available.

The report reads in part:

"FOIA neither authorizes nor requires agencies to search for Federal records in personal email accounts maintained on private servers or through commercial providers (for example Gmail, Yahoo, and Hotmail.) Furthermore, the FOIA Analyst has no way to independently locate Federal records from such accounts unless employees take steps to preserve official emails in Department record keeping systems."

The report strongly suggests that it relies on employees at all levels to follow the regulations, and when personal email is used, to forward copies to a State Department account so that it can be captured.

"Under current law and Department policy, employees who use personal email to conduct official business are required to forward or copy email from a personal account to their respective Department accounts within 20 Days."

Clinton did not have a State Department email address to which she could forward message traffic from her personal account, and it remains unclear whether she provided all her State Department business emails to the State Department or federal courts, where FOIA lawsuits have been filed.

The report also found that the State Department wait time for Freedom of Information Act Requests far exceeds that of other departments. For example, FOIA requires agencies to respond to requests within 20 working days, and "some requests involving the Office of the Secretary have taken more than 500 days to process."

The State Department is also criticized for practices that "do not consistently meet statutory and regulatory requirements for completeness and rarely meet requirements for timeliness."

Given Clinton's use of a private account, where more than 1,000 classified emails have been identified, including at least two at the Top Secret level, it appeared ironic that the report states employees had not been reminded of their FOIA responsibilities "...since March 2009, when former Secretary Clinton sent a message commemorating Freedom of Information Day."

The OIG report makes four recommendations, including that the Office of the Secretary should fully comply with FOIA requirements. The department said it agreed with the recommendations and changes had been made.

State Department spokesperson John Kirby said in response late Wednesday, ?"The Department is committed to transparency, and the issues addressed in this report have the full attention of Secretary Kerry and the Department's senior staff. While the volume of State Freedom of Information Act requests has tripled since 2008, our resources to respond have not kept pace.

"That said, we know we must continue to improve our FOIA responsiveness and are taking additional steps to do so. That's why Secretary Kerry asked the State Inspector General to undertake this review in March, and it's why he appointed a Transparency Coordinator this Fall."

Le Soleil
L'armée garde un oeil sur La Meute
Thursday, 07 January 2016
Byline: Jean-Michel Genois Gagnon
Section: general

Québec - L'armée surveille de près les membres des Forces armées canadiennes (FAC) inscrits dans le groupe Facebook La Meute.
Dévoilé par Le Soleil à la fin du mois de décembre, le regroupement «secret» compte aujourd'hui plus de 16 000 invités (membres et observateurs). Son fondateur, Eric Corvus, un vétéran des Forces armées canadiennes, avait souligné lors de son entrevue que le groupe avait été créé pour «protéger nos terres, nos valeurs, nos fondements, notre liberté, notre sécurité ainsi que l'avenir de nos enfants contre l'envahisseur islamique».

Pour l'heure, aucune enquête n'a été ouverte par la police militaire concernant certains membres des FAC inscrits sur la page Web. «On [la police militaire] s'intéresse aux cas les plus graves qui peuvent mener à des accusations de nature criminelle», stipule le major Mercier. Cela ne signifie toutefois pas que les militaires inscrits ne s'exposent pas à des sanctions. «On est au courant de la situation. On connaît le site et on l'observe. Il n'y a pas d'enquête comme telle de la police militaire, mais il peut y avoir plusieurs autres types d'enquêtes. Ça peut être des enquêtes disciplinaires, des enquêtes sommaires ou des enquêtes administratives», précise-t-il. «Cela relève davantage de la chaîne de commandement de l'individu.»

Les Forces armées canadiennes ne sont pas en mesure de chiffrer le nombre de militaires inscrits sur le groupe et ne possèdent aucune politique particulière qui restreindrait un membre des FAC à participer à un forum dans les médias sociaux. Néanmoins, «les militaires des FAC sont tenus de respecter les normes les plus élevées en matière de conduite professionnelle et personnelle. Le ministère de la Défense nationale et les FAC ne tolèrent pas la discrimination», a écrit l'armée dans un échange de courriels.

«Si la participation ou les activités d'un membre des FAC sur un site Web ou une page de Facebook remettent en question la pertinence du maintien en service d'un militaire, ce dernier peut faire l'objet de mesures administratives ou de mesures disciplinaires. Chaque incident sera évalué au cas par cas. Les résultats de mesures administratives sont confidentiels, en vertu de la Loi sur la protection des renseignements personnels», ajoute le FAC.

Deux plaintes

Inquiète de voir que le groupe La Meute prend de l'expansion, une personne avec qui Le Soleil a discuté a déposé deux plaintes au cours des dernières semaines contre le regroupement, l'une à la Gendarmerie royale du Canada (GRC) et l'autre à la Sûreté du Québec. «Ce que je dénonce, c'est le fait que c'est un groupe qui devient lui-même des extrémistes. Ils dénoncent les musulmans qui sont extrémistes, qui veulent radicaliser le peuple. Mais ils le deviennent eux-mêmes en ayant des propos haineux sur leur page. Ce n'est pas tous les musulmans qui sont pareils.»

La GRC n'a pas voulu confirmer si une enquête a été ouverte.

Afin de clarifier la position du groupe, Eric Corvus a tenu à publier un message le 2 janvier sur la page Facebook La Meute. «À tous ceux qui croient et désirent que La Meute ait été créée afin de nous conduire vers l'anarchie, briser des vitres, mettre le feu, prendre les armes, je vous prierais de prendre le temps d'analyser votre perception, car il n'en est rien. Nous ne sommes pas un berceau de la haine.»

La page Facebook La Meute a été créée à l'automne par un ancien militaire qui a été déployé en Afghanistan en 2004 et en 2007. Il souffre depuis d'un trouble de stress post-traumatique, pour lequel il est suivi. La Meute souhaite éventuellement obtenir son statut d'organisation à but non lucratif.

Jerusalem Post
Will Iran win the technology war?
Thursday, 07 January 2016
Byline: Shlomo Maital
Section: general

Jerusalem - Military Intelligence chief Maj.- Gen. Herzl Halevi bears a heavy burden. This "philosopher general," as a New York Times journalist once called him, is responsible for tracking the deeds, words and even thoughts of Israel's foes, alerting political and military leaders to potential threats. Halevi's undergraduate degree is in philosophy.
He told the The Times, "Through the years, I used philosophy much in a practical manner... philosophers spoke about how to balance, how to prioritize...this is something I find very helpful."

In an unusual closed lecture he gave on October 29 for Tel Aviv's College of Management, the usually reticent and understated general, formerly head of the elite Sayeret Matkal commando unit and tabbed as a leading candidate to become the next chief of staff, said, "If you ask me whether we'll have a war with Iran over the next 10 years, I'll give you a surprising answer. We are already at war with Iran. We're having a technological war with Iran. Our engineers are fighting Iranian engineers today and it's becoming increasingly significant."

He told the daily Haaretz that he was pessimistic. "Today, we have the advantage. Iran is closing in on it. Since the 1979 Iranian revolution, the number of universities and university students in Iran has

increased 20-fold, compared with three and a half times for Israel." Enrollment in science, technology, engineering and math in Iran is skyrocketing, he said.

In other words - in this technology war, Israel is losing. I read about Halevi's speech just after reading two reports prepared by my S. Neaman Institute colleagues at the Technion in Haifa comparing human capital in science and technology in Israel, Iran and Turkey. These reports update an earlier study done in 2011.

New data show that for Israel, in the past decade, science and technology university students per 1,000 persons remained constant at 14, while in Iran, that figure is 25, having doubled in 10 years. Between 2007 and 2014, the number of Israeli universities ranked (in the widely used "Shanghai" list) in the top 100 in the world in science fell from four to three, while Iran managed to place a university in the top 100 for the first time.

Iran has a staggering number of science and engineering college students - over two million, an increase of 161 percent since 2004. For the same period, the comparable number for Israel rose only 20 percent, to 107,000.

According to data of Thomson-Reuters, a global information company based in New York and Toronto, Iran has the world's fastest- growing scientific output, measured by peer- reviewed articles in international journals. In December 2013, Iran put a monkey named Fargam ("auspicious" in Farsi) into orbit and returned him safely to earth. Rockets capable of launching satellites can also carry military payloads great distances.

Ironically, the economic sanctions imposed on Iran by the West appear to have been a major factor in Iran's burgeoning science. According to the just issued UNESCO science report "Towards 2030," "The sanctions... have accelerated the shift from a resource-based economy to a knowledge economy by challenging policymakers to look beyond extractive industries to the country's human capital for wealth creation... between 2006 and 2011 the number of firms declaring R&D activities more than doubled." The UNESCO report notes that Iran ranked seventh worldwide for the volume of scientific papers related to nanotechnology.

I spoke to Dr. Daphne Getz, senior research fellow at Technion's S. Neaman Institute, who led the preparation of all the 2011 and 2015 studies, and asked her about Iran's rapid progress.

The Jerusalem Report: Four years ago, you and your team analyzed the Thomson- Reuters Web of Science database and showed how Turkey and Iran are closing the science and technology gap with Israel. The press reported this study widely. Now, four years later, you and your team have issued two new reports on the same topic, providing detailed statistical evidence. Was there any official reaction to your 2011 report? Are our political leaders asleep, or are they aware of the threat posed by Israel's losing its technological advantage?

Getz: "The report was circulated to all the relevant government ministries. I received responses from two ministries, Education and Defense. Education - from the Chief Scientist, who asked to meet with me, to discuss the possibility of requesting a study of readiness of high school grads for university science and technology studies, and how we can prepare them for such studies, in math, physics and computer science. In the end, owing to bureaucratic obstacles, no such study was ordered.

"I also heard from the Defense Ministry. I met with two senior officials of the ministry, who came to interview me regarding our findings. They told me that, in their unit, our report was compulsory reading. I was impressed that the data in it was taken very seriously, but they did not share with me the actions undertaken (or not undertaken) in response to the trends that we described."

In the West, Iran's Shi'ite Ayatollahs are widely mocked and scorned. Top of the list is the leader of the Islamic Republic of Iran, Ayatollah Sayyid Ali Khamenei. But Khamenei has decreed that Iran will turn into a major scientific power in the future and his book "The Bliss of Knowledge" (now out in English) is a road map showing how this will be achieved.

Can one imagine Rabbi Aharon Leib Shteinman, head of the Council of Torah Sages, playing a similar role, when ultra- Orthodox schools do not even teach math and science?

The Jerusalem Report: "In Israel, we tend to see our ultra- religious as anti-science. Their schools, for instance, teach math and science poorly or not at all. And we assume that Iran is the same. But Iran's Supreme Council of the Cultural Revolution, led by clerics and ayatollahs, has announced: "The revival of the great Islamic civilization is contingent upon allout progress in science." The ayatollahs, led by Khamenei, have actually been the driving force behind Iran's progress in science. Do your data support the Supreme Council's statement that Iran is indeed massively backing its science, technology and math programs with huge resources?"

Getz: "In Iran, there is no contradiction between science and technology and religion - the opposite is the case. The religious leaders say that Islam is in favor of science and Khamenei, the supreme ayatollah, claims in his speeches that true Islam walks hand in hand with science and technology.

Ayatollah Mohammad Khatami, when he ruled, published in 2005 his vision for 20 years in the future - a road map for economic, political, cultural, and social development whose goal was to transform Iran into a nation with an economy based on knowledge rather than on petroleum. The investment in education and in universities is part of this plan, as are the goals for increasing gross expenditure on R&D as a percentage of GDP and the increase in national investment in R&D per capita.

These investments and supporting policies have led to an increase in the number of students in science and engineering; have stimulated scientific research, and have increased R&D output that finds expression in the steep rise in the number of scientific publications and in the improvement in their quality. In high schools, students are directed to learn scientific disciplines, and this results in achievements in examinations and impressive showings in international competitions in science. Our

findings show that the strengthening of achievements in science that we identified in 2011 have continued to this day. Iranian universities not included in the top 500 universities in the world, according to the Shanghai rankings, today appear among the top 100-200 universities in the world in science and engineering."

The Jerusalem Report: "One of the most interesting indicators your studies provide is that of the Science Olympiads [The International Science Olympiads are a group of worldwide annual competitions in various areas of science designed for the four to six best high-school students from each participating country selected through internal National Science Olympiads.] Iran attaches huge importance to these Olympiads; Khamenei himself met with Iran's student contestants. You show that Israel's performance index in this contest for youths is far inferior to that of Iran and Turkey. What is this measure and is it really significant? Does it tell us something about how Iran prioritizes science? Is Israel truly trying its best to identify scientific talent very early and develop it?"

Getz: "The International Olympiads in science compare the achievements of teams of four to six outstanding high-school students from various countries, who compete in math, physics, chemistry, and biology. If we take, for instance, the achievements of Israel, Iran and Turkey in the math Olympiad in 2015, the six contestants from Iran reached 7th place out of 104 countries, winning three gold medals, two silver medals and one bronze. Six contestants from Turkey came 20th, with five gold medals, and Israel's team placed only 40th, with one gold medal, no silver medals and one bronze."

Getz drew my attention to Prof. Maryam Mirzakhani, a math professor at Stanford University born and raised in Iran, who last year became the first woman in the prize's 80-year history to win the coveted Fields Medal, described as the Nobel Prize for mathematics. Mirzakhani won gold medals for Iran in the Math Olympiads in 1994 and 1995, and later studied at Iran's Sharif University of Technology There is another key area in which Iran has overtaken Israel - science policy leadership.

In his two years in office, Iran's President Hassan Rouhani has built a cabinet full of PhD technocrats. One of his youngest cabinet ministers is Sorena Sattari, 43, a mechanical engineer, vice president for science and technology. Sattari says he seeks to link science more tightly to the economy and claims he will imbue Iran with "entrepreneurial spirit. He doles out $600 million yearly in low- interest loans to 1,650 start-ups, perhaps imitating Israel's Chief Scientist grants.

Sattari's counterpart in Israel is Minister of Science, Technology and Space Ophir Akunis, 42, whose degree is in Political Science. Akunis is young, ambitious, energetic ? a rising star in the Likud party. But he lacks academic knowledge of the subject his ministry administers.

Contrast that background with Israel's first minister of science, Prof. Yuval Ne'eman, whose work on the classification of the basic particle known as the hadron should have won him a Nobel Prize, together with Caltech Prof. Murray Gell-Mann.

The "Towards 2030" UNESCO report notes that in Israel "there is a visible ageing of scientists and engineers in some fields, including physical sciences and engineering. The shortage of professional staff will be a major handicap for the national innovation system, as the growing demand for engineers and technical professionals begins to outpace supply."

Getz tells me what she believes should be done. We need an urgent coordinated strategic plan, she says, linking the Economics, Education, Defense and Science Ministries to strengthen Israel's science and technology capabilities and to maintain the technological advantage over nations dedicated to wiping us out.

In Arthur Miller's play "Death of a Salesman," salesman Willy Loman's wife Linda pleads for more respect for her husband, "attention, attention must be finally paid..." Those ringing words apply strongly to the efforts of Iran, Turkey, Saudi Arabia, and other neighboring Islamic countries to close the science and technology gap with Israel.

Israel has many excellent think tanks, like the one at which I work. They alert Israel's leaders to areas of deep concern.

But are their data, words and reports falling on deaf ears, like the words of Linda Loman? Is attention being paid, even when the Military Intelligence chief himself forcefully sounds the alarm?

Le Monde
Le gouvernement néerlandais défend le chiffrement des données
Thursday, 07 January 2016
Byline: Journaliste maison
Section: general

La Haye - C'est une position à contre-courant de celle de la plupart des gouvernements européens que défend désormais le gouvernement néerlandais. Après les attentats ces dernières semaines à Paris et à San Bernardino, le débat sur le chiffrement des données et des communications a été relancé, et plusieurs pays, comme la Grande-Bretagne ou la Chine, ont annoncé leur volonté de légiférer sur la question. Objectif: que les entreprises technologiques permettent aux autorités d'accéder, sans décision de justice, aux données chiffrées de leurs utilisateurs -par exemple en contraignant les services Web à installer des «portes dérobées» dans leurs logiciels.
C'est tout l'inverse que viennent de défendre, dans un texte publié lundi 4janvier , le ministre de la sécurité et de la justice néerlandais, Ard van der Steur, et le ministre des affaires économiques, Henk Camp. Dans cette déclaration, ils soulignent «l'importance d'un chiffrement robuste (...) pour la protection des données des citoyens, des entreprises, du gouvernement et de l'économie néerlandaise tout entière.»

Le texte affirme aussi que le chiffrement est «important pour l'exercice de la liberté d'expression» , celle des citoyens, précise-t-il, mais aussi des journalistes, «en permettant des communications confidentielles» . Les deux ministres vont plus loin, assurant même que l'affaiblissement du chiffrement représente un danger, puisqu'il « expose le trafic Internet à l'espionnage des criminels, des terroristes et d'agences de renseignement étrangères ».

Quelques «entorses» possibles

Malgré ces affirmations, le gouvernement se réserve le droit à quelques «entorses» à ces principes, pour une « cause légitime» . Une formulation très vague, ouverte à tout type d'interprétation.

Cette déclaration a été applaudie par les défenseurs des libertés numériques, comme Rejo Zenger, un des représentants de l'organisation néerlandaise Bits of Freedom, interrogé par Le Monde : «Le gouvernement a conclu, à raison, qu'une telle vulnérabilité pouvait être utilisée par n'importe qui. Il est techniquement impossible de créer une vulnérabilité que seuls les enquêteurs de la police et les services secrets d'un seul pays puissent utiliser.» Pour lui, la position néerlandaise s'explique par l'importance accordée au numérique par les citoyens et le gouvernement:

«Aux Pays-Bas, nous avons une importante infrastructure numérique. La plupart des gens disposent d'une connexion à haut débit et beaucoup font leurs courses en ligne, achètent des livres et des machines à laver sur des sites d'e-commerce. Le gouvernement a ses propres besoins: les citoyens déclarent leurs impôts en ligne, le renseignement chiffre les secrets d'Etat, l'armée sécurise l'information. Tout cela ne peut fonctionner que si nous avons confiance dans la sécurité de l'infrastructure numérique.»

Depuis les révélations d'Edward Snowden en2013 sur la surveillance massive de la NSA , les géants du Web ont renforcé le chiffrement des données de leurs utilisateurs. Au grand dam de nombreux gouvernements, qui considèrent que cela complique le travail des agences de renseignement, notamment pour repérer de potentiels terroristes. Un débat relancé ces dernières semaines, même si rien n'indique dans l'état actuel des enquêtes que les terroristes impliqués dans les attentats de Paris et San Bernardino aient eu recours à des techniques de chiffrement.

La position des Pays-Bas fait donc office d'exception. Ce n'est d'ailleurs pas la première fois que le pays s'intéresse au sujet du chiffrement: le mois dernier, le Parlement a décidé de financer à hauteur de 500000 euros le développent d'OpenSSL, une série d'outils de chiffrement libres et gratuits.

Wall Street Journal
Bugs in Wi-Fi Hookups Cripple Web Security
Tuesday, 19 January 2016
Byline: Jennifer Valentino-DeVries

New York - In late 2014, a small Massachusetts software company got an ominous email: A computer-security researcher said a flaw in one of its programs put millions world-wide at risk of being hacked. Engineers at the company, Allegro Software Development Corp., analyzed the flaw in the program, which can help users access the controls of home Internet routers. They quickly realized something strange: They had fixed this bug nearly 10 years earlier. But it lived on, even in new devices.

The reason: A component maker had included the 2002 version of Allegro's software with its chipset and hadn't updated it. Router makers used those chips in more than 10 million devices. The router makers said they didn't know a later version of Allegro's software fixed the bug.

The router flaw highlights an enduring problem in computer security: Fixing bugs once they have been released into the world is sometimes difficult and often overlooked. The flaw's creator must develop a fix, or "patch." Then it often must alert millions of technically unsophisticated users, who have to install the patch.

The chain can break at many points: Patches aren't distributed. Users aren't alerted or neglect to apply the patch. Hackers exploit any weak link.

In the case of the routers, Allegro said it couldn't apply the patch, because it doesn't have access to the devices. The company urges manufacturers to use the latest version of its software but can't require them to do so. "Nobody does that," said Loren Shade, vice president of marketing. "We've thought about it, but it's kind of hard to enforce."

To shed light on the problem, The Wall Street Journal commissioned a security researcher to test 20 popular Internet routers purchased new in the second half of 2015.

Ten arrived with known, documented security weaknesses. Tod Beardsley, a researcher at security company Rapid7 Inc. who conducted the tests, said the vulnerable routers had outdated "firmware," the programs that run a device. Four others had old firmware that had subsequent updates that Mr. Beardsley said could contain undocumented security problems.

Half of the group of 20 didn't let users easily check for new software during the standard setup process. Instead, users had to search on the Web or run optional programs. In addition, two routers incorrectly told users that updated software wasn't available, when in fact it was, and one directed users to download software that had a severe, documented security flaw.

The Journal's findings dovetail with those of Shahar Tal, a researcher formerly at Check Point Software Technologies Ltd. who helped find the Allegro bug, dubbed "Misfortune Cookie" because it allows hackers to attack the router using malicious Web cookies.

In scans over the Internet this spring, Mr. Tal found that 79% of the routers that initially contained Misfortune Cookie were still vulnerable, five months after the problem had been disclosed in public announcements and to the device makers.

Router makers are cutting corners by not checking the security of their products and failing to make efforts to keep customers informed of updates, he said. They "aren't paying the price for bad security," Mr. Tal said. "They're trying to cut prices by a dollar and win that contract from service provider X. Security isn't on their mind."

Router makers contacted by the Journal said security was important to them, and most said they had plans to improve how users are notified of new software-- which often depends on a user noticing an update on the router's website. But several also said routers more than a couple of years old are less likely to get fixed.

Home routers are an easy target because manufacturers compete largely on price, for devices that typically sell for less than $100. Customers acquire the routers either from retailers or from Internet-service providers. Once routers are sold, manufacturers have little incentive to update them to improve security. Routers can remain in use for years after what manufacturers term their "end of life," meaning they no longer issue updates.

The same problem is evident in smartphones and the growing market for Internet-connected computers in everything from printers to television sets.

Security researchers recently showed how they could hijack an email account through a refrigerator by attacking the link it used to display the owner's Google calendar on the door's touch screen. Other researchers have demonstrated they can change the settings on Internet-connected medical devices, managed remotely by nurses and doctors, that infuse medicines into patients.

The Federal Trade Commission last year warned that companies entering these markets "may not have experience" with security. For users, the commission said, "It may be difficult or impossible to update the software or apply a patch."

Alphabet Inc.'s Google regularly updates its Android mobile-operating system, which runs roughly three-fourths of the world's smartphones, to patch security holes. But it generally relies on device makers and telecom carriers to distribute the new software. Device makers don't always distribute it, particularly for cheaper phones or those more than a year old.

University of Cambridge researchers in October said more than 85% of 20,000 Android devices they studied had at least one of 11 known critical vulnerabilities, largely because of "inaction by some manufacturers and network operators." That could allow a hacker to take control of a phone, usually through a malicious app.

A Google spokeswoman said the company is working with manufacturers and carriers to distribute updates more quickly. Google also said it has made efforts to keep harmful apps, which hackers typically use to exploit a weakness in a device, off its Play Store. It said fewer than 1% of Android devices have installed a potentially harmful app.

Software on Apple Inc. devices is more commonly up-to-date, because Apple manufactures iPhones and iPads and controls more of the update process.

Automatic updates

Microsoft Corp. in late 2004 activated automatic updates by default on Windows machines. Some software, such as Google's Chrome Web browser, updates itself every few weeks.

Such efforts help more-secure software spread faster. Mozilla Corp. said more than 70% of users of its Firefox Web browser are on the latest version within 20 days of its release; since 2013, Firefox has updated on its own when the user restarts. Before that, when the browser prompted users to upgrade every few months, it took more than a year to get that many users on the newest software.

As security improves on personal computers, hackers seek other ways into networks. Routers make an inviting target.

Once in control of a router, hackers can access almost anything a user sends over the Internet, sometimes even if it is encrypted. In one incident reported in 2014, hackers hijacked routers to siphon off bank-account details from Polish consumers. Researchers in Spain last year tested 22 routers and found that each had at least one security vulnerability.

Researchers at Internet- technology company Akamai Technologies Inc. said criminals also increasingly offer to infiltrate routers and use them to overwhelm targeted websites for a fee. Attack instigators may want to gain an advantage in online games, punish companies for bad service, camouflage another attack or extort money, said Eric Kobrin, Akamai's director of information security. Such router- type attacks were rare a year ago but in 2015 accounted for 10% to 20% of denial-of-service attacks, he said.

Mr. Kobrin said a group called Lizard Squad used routers and other home devices to direct malicious traffic that knocked gaming networks for Microsoft's Xbox and Sony Corp.'s PlayStation offline for hours on Christmas Day 2014.

None of the routers tested by the Journal was vulnerable to these types of attacks out of the box, with default settings in place. The Journal's tests found at least one flaw that has been used by hackers. "The Moon" worm was documented spreading among Linksys routers in 2014. A new Linksys E1200 N300 router purchased in July 2015 and tested by the Journal shipped with software from 2013 that still had the vulnerability the worm exploited.

Belkin International Inc., which owns the Linksys brand, initially said the 2013 software wasn't vulnerable to the bug, but after discussions with the Journal it acknowledged that users should update to newer software to protect from the hack. The company said all new routers are now shipping to stores with the later software.

Users can update device software to address such vulnerabilities, but most of the devices tested by the Journal didn't notify owners that new software was available. Two routers-- one made by Belkin and one by Netgear Inc.-- incorrectly told users there was no update.

In a statement, Netgear said new routers might arrive with old versions of firmware because it can take months for a router to get from a factory to a consumer. The router that incorrectly said an update wasn't available didn't work "as expected," Netgear said. Follow-up tests after the Journal contacted Netgear showed the router correctly indicated an update was available.

Belkin said its router couldn't find the update because the updated software hadn't been properly loaded on its computers. The company made the software available after being contacted by the Journal.

Another router, made by D-Link Systems Inc., directed U.S. users to download a version of the software that still contained a bug with the highest severity level in the National Institute of Standards and Technology's National Vulnerability Database. The bug had been fixed by D-Link in May, but the patch was made available only on international D-Link sites and an obscure Internet forum.

After being contacted by the Journal, D-Link said in December that the company hadn't put the fixed firmware on its U.S. site because it had been conducting a "validation test" to confirm "that the firmware is succeeding." The update was put on the U.S. site in early January.

"I was surprised at the level of problems users would have just updating" the software, said Mr. Beardsley, the Rapid7 researcher who conducted the Journal's tests.

The tests found other security weaknesses. All but two of the 20 routers tested used insecure, widely known passwords by default and didn't require users to change them. All 20 used network settings that security researchers say can be easily guessed by hackers.

The routers tested by Mr. Beardsley had fixed two problems regularly cited by security researchers in the past: None had remote administration settings enabled by default, and none was easily accessible over the Internet by openings that hackers regularly probe.

The Journal's tests didn't look for new vulnerabilities. Instead, they focused on known problems, to highlight weaknesses in the security chain. The Misfortune Cookie flaw was more prevalent in routers sold abroad than in the U.S., researchers said.

Mr. Tal, the researcher who found the bug, said he became interested in studying Allegro's software when he realized how widely it was used -- and that the most-common version was from 2002. He and fellow researchers saw it on more than 200 models from dozens of router manufacturers but didn't understand why it was so prevalent.

They eventually linked the software to MediaTek Inc., which had supplied chips for the vulnerable routers. MediaTek said the faulty software had been incorporated into the chip by a company it acquired and that maintenance fell through the cracks until 2014, when MediaTek learned about the Misfortune Cookie flaw.

"Once we were alerted, we acted quickly to minimize impact and remedy the issue for customers," by working with router makers to update the firmware, a MediaTek spokesman said.

Huawei Technologies Co., for example, published a fix for its two routers affected by Misfortune Cookie in December 2014, soon after being contacted by the researchers. In a statement, Huawei said it "expresses appreciation" to the researchers for disclosing the bug and urged people to download the latest firmware from the company's website.

TP-Link Technologies Co. initially had 23 affected models, according to the researchers. More than a year after the bug was publicized, the company's support site showed that three of the models had updates to address the vulnerability. TP-Link said seven additional models were scheduled to be updated before early February, but that other models were considered "end of life" and wouldn't be updated. The company is "prioritizing support for newer products, of which a larger portion are likely to still be in service," a company spokesman said.

But security pros say people often use these types of devices for a long time. Routers "are things you just set up and don't think about," said Mr. Tal, the researcher. "They stay out there for years and years until they break."

Ottawa Citizen
Burkina Faso attack shows need to boost information-gathering: Sajjan
Tuesday, 19 January 2016
Byline: Lee Berthiaume

ST. ANDREWS, N.B. - Defence Minister Harjit Sajjan says better intelligence capabilities, as well as co-operation with Canada's allies, are essential for preventing the types of terror attacks that have struck Burkina Faso and other parts of the world.
Six Canadians were killed over the weekend when militants linked to al-Qaida stormed a hotel in Ouagadougou, the capital of Burkina Faso in West Africa. Days earlier, a Canadian was killed during an attack by Islamic State-inspired terrorists in Indonesia.

Speaking on the sidelines of a three-day retreat between Prime Minister Justin Trudeau and his cabinet ministers, Sajjan said Canada has "to get better at our intelligence capabilities in other parts of the world so that we have a better chance of preventing attacks like this from happening.

"This only happens if we start working in greater co-operation with our intelligence partners," he added. "Which means not just the military, but also the police forces as well."

Intelligence co-operation between Canada and its allies has been the subject of massive controversy in recent years, particularly after U.S. whistleblower Edward Snowden revealed that American and Canadian spy agencies have been running massive intelligence-gathering operations.

The previous Conservative government also enacted controversial anti-terror legislation, Bill C-51, that increased the scope and powers of Canada's intelligence operations. The Liberals promised during the election to amend the law, but haven't said how. Instead, they have promised broad consultations first.

Sajjan, who is responsible for the ultra-secret Communications Security Establishment, which is Canada's electronic spy agency, said "the safety of Canadians will always be paramount," but also that there "has to be a balance."

"There can be a fine balance with security, and when it comes to preventing these types of attacks and co-operation between agencies, it does not have to infringe on Canadian rights," Sajjan said. "We can actually do this better. It's just a matter of being better co-ordinated."

Canadian Press
'Troubling' Conservative torture policy up for review, Goodale says
Tuesday, 19 January 2016
Byline: Jim Bronskill

OTTAWA _ The Trudeau Liberals will review controversial directives enacted by the Harper government that allow for the sharing of information even when it might lead to torture, says the public safety minister.

The ``troubling set of issues'' raised by the foreign information-sharing policy ``will be raised in the course of our consultations'' on the overall national security direction of the new government, Ralph Goodale said in a recent interview with The Canadian Press.

The news follows pressure from human-rights and privacy advocates to conduct a wide-ranging examination of security policies introduced by the Conservatives, whisked from office in the October election.

The federal policy on foreign information-sharing has been roundly criticized for effectively condoning the torture of people in overseas prisons, contrary to international law and Canada's United Nations commitments.

A four-page 2010 framework document, released under the Access to Information Act, says when there is a ``substantial risk'' that sending information to, or soliciting information from, a foreign agency would result in torture _ and it is unclear whether the risk can be managed through assurances or other means _ the matter should be referred to the responsible deputy minister or agency head.

In deciding what to do, the agency head will consider factors including the threat to Canada's national security and the nature and imminence of the threat; the status of Canada's relationship with _ and the human rights record of _ the foreign agency; and the rationale for believing that sharing the information would lead to torture.

Critics say when there is a serious risk of torture, there should be no sharing _ period.

The Canadian Security Intelligence Service, the RCMP, the Canada Border Services Agency, National Defence and the Communications Security Establishment, Canada's electronic spy agency, are bound by the federal policy on sharing information with foreign agencies.

``That's a very troubling set of issues,'' Goodale said, adding the government intends to develop a response ``that reflects what Canadians want.''

``We'll be listening very carefully for the messages from Canadians on that subject.''

Goodale said the Liberal government is open to a general rethinking of national security legislation, not just a few changes the party has promised to the omnibus bill known as C-51.

The government plans to give Canadians their say before deciding what changes to make.

Globe and Mail
Chinese soldiers implicated in U.S. military hacking case
Tuesday, 19 January 2016

Byline: Colin Freeze

Two Chinese government soldiers were part of a hacking conspiracy allegedly carried out by a Chinese resident of Canada to steal secrets relating to components of F-35s and other American warplanes, according to court-filed documents.
Prosecution "books of record," recently released by a Vancouver court following a request from The Globe and Mail, make explicit Chinese military ties that were not publicly alleged when this rare cyberespionage prosecution was launched in 2014.

The case centres on Su Bin, a 50-year-old Chinese aviation industry entrepreneur residing in Vancouver, and the two unnamed "co-conspirators" revealed to be Chinese soldiers.

Despite their military connection, it remains unclear whether the alleged scheme was statesponsored, or whether the conspirators were essentially soldiers moonlighting to enrich themselves.

Prime Minister Justin Trudeau is considering a visit to China this spring to talk about free trade. In recent years, both U.S.

President Barack Obama and former prime minister Stephen Harper have gone public with concerns about Chinese cyberespionage.

While most countries spy, China is feared to be in a class of its own when it comes to using hackers to steal military and commercial secrets. Four years ago, now-retired American spymaster Keith Alexander claimed that cybercrime costs the United States hundreds of billions of dollars each year.

In June, 2014, such fears were given a human face. That's when Canadian police arrested Mr. Su on a U.S. warrant that charged him with being part of an illegal hacking conspiracy. The ongoing extradition case against him relies on intercepted e-mail exchanges, in which Mr. Su allegedly helped to focus the hacking efforts of the two Chinese co-conspirators.

The allegation is that the conspirators worked together to identify and raid secure databases belonging to U.S. military contractors who make jets for the Pentagon.

Mr. Su allegedly directed the two hackers toward the e-mail accounts of American aviation engineers whose accounts he felt to be worth breaking into; from there, the China-based hackers mined corporate networks for engineering manuals related to F-35, C- 17 and F-22 military jets, documents show. During such breaches, the co- conspirators allegedly circled back to Mr. Su with long lists of files, to ask him what documents they should try to take.

The original U.S. charging documents released in 2014 mention the two "unindicted co-conspirators," but only as people "affiliated with multiple organizations and entities." No mention was then made of potential ties to China's People's Liberation Army (PLA).

Yet materials recently released to The Globe explicitly describe them as "two Chinese military officers." And U.S. authorities say they know this because they intercepted an e-mail attachment bearing a digital image of one coconspirator's "Chinese military identification showing his photograph, name, rank, military unit, and year and month of birth." He is also said to have used certain "monikers or nicknames" within the Chinese military.

Other intercepted photos allegedly show the other conspirator's "Hong Kong identification" and a picture of him wearing a Chinese military uniform.

No names are revealed in the documents. It is not clear why U.S. prosecutors minimized the military connection at first, nor why they declined to lay charges against the two co-conspirators if their identities are known. "I'm going to decline to comment on the matter at this time, as the extradition proceeding is ongoing in Canada," said Thom Mrozek, a U.S. Justice Department spokesman.

Mr. Su's extradition hearing took place in Vancouver last July.

According to news reports, Canadian Crown lawyers did refer in passing to the two co-conspirators as Chinese military officers, but gave no additional information. In September, a Canadian judge ordered Mr. Su extradited, but he remains in Vancouver pending an appeal to be heard later this year.

Most of the e-mails intercepted in the case were sent between 2009 and 2012. Some speak of bids to sell stolen data; at one point, Mr. Su allegedly tells his coconspirators that it is hard to collect "big money." At another, he tells them a certain Chinese aviation company is likely "too stingy" to pay them much.

This illustrates how both profit and patriotism motivate spying done on China's behalf. Observers have long pointed out that Beijing leverages two types of hackers: squads of PLA soldiers whose full-time jobs are to hack away at the West's secrets, and also unaffiliated, arms-length hackers who sell their wares to Chinese firms. What the Su Bin prosecution suggests is that the soldiers and freelancers are, at times, the same people.

"The problem has always been the hackers seem to do the same work from 9 to 5, and then 5 to midnight when they got home," says Adam Segal, a New Yorkbased scholar who is releasing a book next month called The Hacked World Order. "So it's very hard to very clearly say this guy is a freelancer, this guy is a PLA hacker. Sometimes they are doing it under the direction of the PLA, sometimes they are doing it as freelancers to make money."

Chinese hacking "is going to continue to be a big issue" in coming years, Mr. Segal says, despite a recent détente. In September, Chinese President Xi Jinping met with Mr. Obama, and the two nations publicly pledged to curtail cyber activities aimed at stealing commercial trade secrets. No mention was made,

however, of the kinds of spying that aim to secure a military edge - or to blunt that of a potential adversary.

Mr. Su is not accused of being a hacker himself. But, according to the documents, engineers and executives with Boeing, Lockheed Martin and Airbus are preparing to testify that his e-mail trails show that he helped the Chinese hackers take bona fide engineering documents off secure servers; this work, they will say, essentially gave China a free ride on aspects of jet projects that cost the U.S. military billions to develop.

While the China-based hackers allegedly used a network of Internet "hop points" to hide the trail of the stolen data, Mr. Su himself appears to have violated some rudimentary Internet-secrecy principles.

For example, he allegedly talked to his co-conspirators using Gmail and Hotmail services based in the United States, services which U.S. federal agents readily searched once they got the warrants to do so. At one point, he allegedly e- mailed his conspirators a password for an encrypted document - saying that the password was his phone number, then going the extra step of typing out that phone number.

Mr. Su appears to have moved to Vancouver from Beijing only a short while before his arrest.

In 2012, The Wall Street Journal profiled Mr. Su as a resident of Beijing, describing him as an army officer's son who had become a multimillionaire Chinese aerospace entrepreneur. Mr. Su was quoted as saying that he and his family were heading to Canada because he didn't like living under Chinese rule.

The newly released documents say Mr. Su carried a Canadian permanent resident card and also a business card saying he had worked as a project manager for a "test flight academy in Africa."

Most of his other personal documentation described him as the founder of Lode Tech, a Chinabased company that bought and sold harness cables used in the aviation industry.

Motherboard (Vice)
'Teens' Who Hacked CIA Director Also Hit White House Official
Tuesday, 19 January 2016
Byline: Lorenzo Franceschi-Bicchierai

New York - The hacking group that has been targeting government officials since October, when it broke into the AOL email account of CIA Director John Brennan, has claimed yet another victim.
This time, the victim is President Barack Obama's senior advisor on science and technology John Holdren, Motherboard has learned. One of the cybercriminals linked to the group that hacked Brennan broke into Holdren's home telephone and email account and set it so that all the calls would get forwarded to the Free Palestine Movement. This is exactly what happened to US Director of National Intelligence James Clapper last week.

On Monday, one of the members of the hacking group, which is known as Crackas With Attitude, or CWA, sent me an email to tell me about his latest feat.

"If you don't believe me you can call the home phone," he said, before sending me a phone number that belongs to Holdren, according to public records.

When I called the number, the founder of the Free Palestine Movement Paul Larudee picked up the phone. Larudee said that the same person who called him last week to tell him that he would receive calls directed at Clapper called him again on Monday morning.

"I did it again," said the hacker, according to Larudee, who told me he recognized the voice of the hacker.

One of the CWA hackers, known as Cubed, told me that the person who broke into Holdren's account was somebody called Fearz, or @fearhax, who identifies himself as an ex-member of CWA on his bio. Cracka, another CWA hacker, also told me that it was Fearz who was able to get into Holdren's account with a spear phishing (a term for getting information by deceiving via a targeted attack) his wife. (Cracka also said CWA has disbanded, but it appears its members are still in touch with each other and share information.)

"[Fearz] sent [Holdren's wife] Cheryl an email claiming to be John LOL," Cracka told me in an online chat, adding that the phishing emails said "something like 'Hey honey, do you have the password for our joint Xfinity account? I lost it.'"

Then Cheryl sent the password to the hacker, according to Cracka, allowing him to get into their Comcast Xfinity account.

The White House declined to comment, but confirmed that Holdren, who's the Director of the Office of Science and Technology Policy (OSTP), was targeted. "We are aware of this issue and have reported it to law enforcement," a spokesperson for the White House OSTP told Motherboard.

The FBI did not respond to Motherboard's request for comment.

The hackers also provided what they claimed was Holdren's cellphone number. When I called it, a person claiming to be John Holdren picked it up. However, he declined to comment until I proved who I was, and asked me to send him an email to his personal Gmail account. But he didn't respond to my email, nor another subsequent call.

Holdren is just the last in a long series of victims.

Cracka and his associates first became notorious when they hacked Brennan's email. But since then, they have targeted several government officials, including FBI's Deputy Director Mark Giuliano, James Clapper, and the former intelligence execute Vonna Weir Heaton.

Cracka told me on Monday that the group hacked several other government officials, including some the group never publicly bragged about. He mentioned Amy Hess, the FBI's executive assistant director for science and technology, White House Communications Director Jen Psaki, White House Chief of Staff Denis McDonough, the Deputy Secretary of State Tony Blinken, and the White House Deputy National Security Advisor Avril Haines.

Their month-long hacking spree prompted the FBI to issue an alert last year, warning politicians and police officers of the risk of getting "doxed" by a "hacktivist" group.

The hackers also appeared to have gained access to a slew of law enforcement tools and databases. In November, the hackers published more than 2,000 names belonging mostly to US law enforcement agents. Cracka told me that they found Holdren's wife's email address in one of the databases they were able to download in November.

"That was the best breach everrr [sic]," Cracka said.

The hackers have always claimed to be doing this to protest against the US government, and to support the cause of a free Palestine. In fact, Cracka asked me to include a statement in this article.

"Fuck zionist fucks and bomb Israel leaders," he said.

ABC (Australia)
Australia not prepared for cyber war
Tuesday, 19 January 2016
Byline: Francis Keany

A new report warns Australia is not adequately prepared for cyber war, with the nation "badly lagging" behind overseas counterparts and the Defence Force also at risk.
Research by the Australian Centre for Cyber Security (ACCS) said Australian government and civilian organisations were well behind China and the United States, which have gone to great lengths to prepare themselves.

The report released by Professor Greg Austin called for a "rapid catch-up in Australian capabilities for military security in the information age", warning Australia's response to the threats that have emerged in cyberspace has been "slow and fragmented".

Another report by the ACCS has also warned the Australian Defence Force (ADF) has not done enough to test its ability to ward off cyber attacks against weapons systems.

While Australia has relied on the United States for its security needs for the past 60 years, the report warned that support would be limited when it came to cyber warfare.

This is despite Australia's involvement in the Five Eyes intelligence alliance.

"The reliance by middle powers such as Australia on the United States for extended deterrence may not have as much impact in cyber space as for kinetic operations," Professor Austin said.

He said while there was public debate about the future of Australia's naval, air and ground capabilities, there has been "no effort in public by the government to benchmark Australian national security needs in cyber space in the same way".

"The country has had a high-profile national debate about whether we need a national capability to build naval combat ships and submarines, but we have been silent on the type of national cyber innovation system we need for future warfare."

The report said Australia at this stage was not prepared for a "medium-intensity war" that would include a sophisticated attack in cyber space.

"We need first of all an open and public debate on our military, security and civil needs in cyber space and how well our emerging capabilities match those needs," it said.

"We would have to admit, as so many specialists have argued, that we are badly lagging."

ADF weapons systems 'vulnerable'

A separate study, also released by the ACCS, has warned the ADF needs to do more to ensure its current weapons systems can withstand a cyber attack.

The report, by retired Group Captain Keith Joiner from the RAAF, said Australia's preparedness was about "six years" behind the United States.

"Consequently, the ADF is likely to be blind to the operational vulnerabilities of their major complex systems and platforms to cyber attack," Dr Joiner said.

The paper called for increased funding to enable the ADF to conduct cyber-survivability trials.

"The ADF needs to give the same attention to testing and evaluating the vulnerability to cyber attacks of its legacy systems as it affords to testing and evaluating vulnerabilities to conventional threats," it said.

The comments come as the Federal Government prepares to release its defence white paper, which is expected in coming months.

China likely to be 'far ahead' within 20 years

Professor Austin's study warned Australia risks being overtaken by China in relation to its defences against cyber attacks; and that it might already be too late to prevent it from happening.

"On current indications, within 20 years, China's civil, economic and military capabilities in cyber space will likely be very far ahead of Australia's, whereas today both countries might be judged to be both laggard countries," it said.

"Australia must now prepare to respond to the likely impact over the longer term of Beijing's higher commitment in the past 15 years to transformation through military cyber S&T (Science and Technology) compared with the Australian Government's lack of commitment in key areas of policy over the same period."

Professor Austin suggested Australia follow the path of China and provide its reservists with training on cyber warfare.

"China is exceptionally well placed to develop the most powerful and best-organised cyber militias in the world. It does not now have such a strong capability but it has taken steps along this path."

Innovation the key to 'cyber survivability'

Professor Austin called for a national innovation strategy, as well as a blueprint for "cyber survivability" if there is a direct military confrontation with a major power.

He also recommended increased investment in IT and education, to encourage more graduates into the field.

"Cyberspace governs all economic, social, scientific, business and medical activity dependent on any sort of computerised record keeping or more complex analysis," he said.

"Cyberspace unifies all domains of warfare, especially its political control and its political impacts."

Prime Minister Malcolm Turnbull has vowed to make innovation a cornerstone of his leadership.

Straits Times
Security agencies outline plans to tackle threats

Tuesday, 19 January 2016

Singapore is boosting the capabilities of its security agencies to deal with a range of threats, from terrorism to cyber crime.
The Singapore Armed Forces is developing know-how such as unmanned systems and robotics, and the police are installing cameras at HDB estates and public areas to deter criminal and terror activity.

These broad plans to keep Singapore safe and secure were outlined by the Defence, Foreign Affairs and Home Affairs ministries yesterday, in addenda to President Tony Tan Keng Yam's address to Parliament.

Speaking at the opening of Parliament last Friday, Dr Tan said Singapore can remain sovereign only if its people are able to determine their own fate.

Deputy Prime Minister and Coordinating Minister for National Security Teo Chee Hean, who oversees the National Security Coordination Secretariat, said yesterday that strengthening social resilience is also crucial.

"In the event of a crisis, it is not just the security agencies that will be called to respond. Our society as a whole will also be tested," he said. "We must ensure that we can bounce back from any incident, and emerge stronger and more united."

Several other ministries will release their plans this week. MPs will then debate these policies when Parliament sits for a week from next Monday.

Saudi Gazette
GCC warned to be on high alert against rising cyber security threat
Tuesday, 19 January 2016

Jeddah - Businesses need to be on high alert in the GCC to combat the growing threat from computer hackers, an IT transformation management expert warned Monday.
Morten Meltinis, IT expert at PA Consulting Group, said a number of recent scares have underlined why security must be high on the business agenda in the GCC to counter the increasing risk of cyber breaches.

PA said organizations need to understand their own weaknesses and increase their combined security knowledge, in the process making employees guardians of digital assets, rather than the potential source of risks.

"The UAE, for instance, is rising on the global list of countries with a high risk of having your computer infected and thereby vulnerable to being hacked," said Meltinis. "According to Kaspersky Labs, the UAE is in the second highest risk group of five."

Earlier this year, PA Consulting Group issued a three-point cyber security strategy for healthcare providers in the GCC from its Abu Dhabi regional headquarters. Another PA report in the UK said police analysts forecast the time spent on dealing with cybercrime will treble.

"One of the biggest problems is that many organizations do not know where they are vulnerable - they take the standard precautions without really knowing what is needed and what the threats are they are trying to protect themselves against," said Meltinis.

"It's crucial that employees know how to avoid the most common mistakes, and raising the lower bar of a company's combined security knowledge will eliminate many risks."

"If employees are given an understanding of where the organization is vulnerable they can act as custodians rather than be security risks themselves. Instead of applying very strict rules upon employees, companies should educate them so they understand what the threat is and the behaviors expected of them."

PA Consulting Group highlights the common use of a single password / email combination for multiple purposes as a major security risk. "Passwords should not be so complicated that the user has to write them down, but we also recommend educating employees about using unique username and password combinations for their personal and professional digital assets that they really care about," said Meltinis.

National Post
Beefing Up our cyber defences
Wednesday, 20 January 2016
Byline: Imran Ahmad, Marlon Hylton And Bernice Karn
Section: oped

With cyber attacks steadily increasing in sophistication, frequency and magnitude, we must ask ourselves whether Canada is ready to meet the challenge these threats pose to our economy, national security and the overall wellbeing of Canadians. Unfortunately, when compared to the United States, the United Kingdom or Germany, Canada is clearly lagging in terms of cyber readiness.
This is in part due to a lack of Canada-specific data on the types of cyber attacks affecting the public and private sectors in this country. While the pending mandatory data breach notification provisions under the Personal Information Protection and Electronic Documents Act will likely help in this regard, the notification requirement will be limited to personal information and won't cover cyber attacks involving the theft of intellectual property, trade secrets or other types of critical business information.

Within this environment, it's understandable that the public and private sectors have struggled to develop an effective and comprehensive cyber strategy.

Nevertheless, last month alone, several positive developments within the public and private sectors signalled a real effort to move the yardsticks on Canada's cyber preparedness. The first was Prime Minister Justin Trudeau's mandate to his minister of public safety to lead a review of existing measures to protect critical infrastructure - utilities, transportation, financial sector, telecommunications, etc. - from cyber threats. Shortly thereafter, the Canadian Council of Chief Executives announced that it was establishing the Canadian Cyber Threat Exchange, a member-funded, not-for-profit organization focused on helping Canadian businesses and consumers protect themselves against cyber attacks.

Another private-sector initiative was the Canadian Advanced Technology Alliance survey on how Canadian businesses are responding to cyber threats. The survey results will provide a useful benchmark for businesses to critically assess their cybersecurity readiness. Finally, the Investment Industry Regulatory Organization of Canada just published a best practices guide to help the investment industry adopt a voluntary, risk-based cybersecurity framework that emphasizes the need for preparing effective cyber threat response plans.

These developments are clearly all positive steps in the right direction, but they need to fall within a broader national framework.

In the meantime, Canadian organizations remain highly vulnerable to cyber attacks and the legal implications that follow. That is why corporate directors and officers must ensure their organization's cyber defences are up and that the organization is ready to effectively respond, should a cyber attack occur. Neglecting these oversight responsibilities can very easily expose directors to litigation for breach of their fiduciary duties. This is particularly true now, as many new class action lawsuits are being

launched in Canada over data breaches resulting from cyber attacks - a trend we anticipate will continue to grow in the coming years.

In an effort to ensure they meet their legal obligations to protect the data and information entrusted to them, organizations can and should take concrete steps to improve their cyber defences. Recognizing that a successful cyber attack can have a serious impact on an organization's reputation, result in years of litigation and affect business continuity, including loss of revenue, the following steps can be quickwins that any organization can implement:

Know Where You Stand Map the organization's networks and IT systems, including gaining a clear understanding of what the key business functions are, as well as where the organization's critical data (i.e., the "Crown Jewels") resides and how it is protected.

Deploy Cyber Monitoring Build a cyber-monitoring team tasked with meeting regularly to assess threat levels, discuss how to address gaps and make recommendations to management and the board of directors. The team should include key legal, business and c-suite executive stakeholders. Audit and Test Cybersecurity measures should be audited and tested on a regular basis and results should be regularly reported to management and the board. This will ensure that the leadership team is aware of any potential cyber threats, that they understand the organization's cyberrisk profile and can assess the effectiveness of current defences and are able to call for necessary remedial steps. Train Employees Many cyber attacks are successful because employees did not receive appropriate cyber-security training. Employees need to understand the importance of protecting customer and business information and have solid grounding on how to make good judgments when faced with a potential cyber threat.

Have a Cyber Attack Response Plan Organizations have to expect that they will at some point be the victim of a successful cyber attack, with their network and data being compromised. The key to an effective response plan is to map out the key legal and business issues that will need to be addressed, how the organization will respond to each issue and who should lead and be accountable for each stage within the response plan.

As Canadians recognize that cyber threats within our connected society are the new norm, they can take some solace in the fact that the public and private sectors are taking steps to confront the problem.

That said, the key question remains whether we will be able to develop an effective national cyber-security framework before the next attack compromises the personal information of Canadians, cripples our critical infrastructure or otherwise negatively impacts our economy.

Toronto-based lawyers Imran Ahmad, Marlon Hylton and Bernice Karn are members of Cassels Brock Blackwell LLP's cyber- security practice.

The Guardian (London)
Alan Turing, James Bond and London Spy: how MI5 became Britain's most inclusive employer
Tuesday, 19 January 2016
Byline: Richard Norton-Taylor

Column - If you had walked past MI5's headquarters in central London earlier today, you might have noticed the rainbow flag flying above the building. It is not the first time - it flew there on the day of London's Pride festival last summer. But this time it was raised to mark the accolade of Stonewall's employer of the year: Britain's Security Service came top in the annual Stonewall Workplace Equality Index. The index measures an organisation's work in tackling discrimination and creating an inclusive workplace for lesbian, gay, bi and trans people.
MI5 in particular, it might be argued, needs to be inclusive. Much of its work, as it director general Andrew Parker, said, "goes on by necessity out of view". Its employees cannot talk about their work with outsiders. They need a workplace that is tolerant and welcoming, and an esprit de corps that encourages diversity.

Historically, when homosexuality was illegal, spying might have been a particularly attractive career for people used to hiding their personal - as well as political - proclivities. They could keep secrets, and tell lies. Perhaps the most notorious gay spies were Guy Burgess and Anthony Blunt, two members of the Cambridge ring whose circle was imbued with sexual liberation, of all kinds. (There was one exception. The ascetic John Cairncross told me years after he was exposed as the "Fifth Man" that he did not take to the fellow members of the spy ring because of their class - which protected them from exposure - and lifestyle.)

Now even James Bond, the most highly charged heterosexual of all spies, is confronted in Skyfall with a flirtatious gay scene when villain Raoul Silva, played by Javier Bardem, undoes Bond's shirt and strokes his chest while Bond is tied to a chair. "First time for everything?" he asks. Daniel Craig's Bond, replies: "What makes you think this is my first time?"

In 1954, Alan Turing, the codebreaking genius of wartime Bletchley Park, the forerunner of GCHQ, died in an apparent suicide after battling with his sexuality and being sentenced to chemical castration. More than 50 years later, Gareth Williams, the GCHQ maths genius, was found dead in his London flat while seconded to MI6. His death , unsurprisingly, is often thought to have been an inspiration for the recent BBC2 series, London Spy. The similarities between Williams and Alex, played by Edward Holcroft, are pretty clear - although writer Tom Rob Smith has said his character is a work of fiction. Nevertheless, these are cases - one fact, the other fiction - when their employers did not face up to a duty of care in a profession which can be uniquely lonely.

MI5 now has a LGBT "champion" to promote diversity, an 80-plus-strong LGBT network, and a "reverse mentoring" scheme for staff who want to develop their understanding of diversity. Staff are offered

"unconscious bias training". Meanwhile MI6, Bond's employer, uses Stonewall's logo on recruitment ads appealing for people who are "able to get on with diverse groups".

Until the early 90s, MI5 - like the Secret Intelligence Service, MI6 - prevented gay people from security-sensitive posts on the grounds they were vulnerable to blackmail. MI5 heading Stonewall's table will be leaving many of Britain's former security chiefs aghast - and be a lesson to any of them still in post, trying to hold fast to their service's old and damaging ethos.

The Register (UK)
For fsck's SAKKE: GCHQ-built phone voice encryption has massive backdoor - researcher
Wednesday, 20 January 2016
Byline: Kieren McCarthy

London - The UK government's official voice encryption protocol, around which it is hoping to build an ecosystem of products, has a massive backdoor that would enable the security services to intercept and listen to all past and present calls, a researcher has discovered.
Dr Steven Murdoch of University College London has posted an extensive blog post digging into the MIKEY-SAKKE spec in which he concludes that it has been specifically designed to "allow undetectable and unauditable mass surveillance."

He notes that in the "vast majority of cases" the protocol would be "actively harmful for security."

Murdoch uses the EFF's scorecard as a way of measuring the security of MIKEY-SAKKE, and concludes that it only manages to meet one of the four key elements for protocol design, namely that it provides end-to-end encryption.

However, due to the way that the system creates and shares encryption keys, the design would enable a telecom provider to insert themselves as a man-in-the-middle without users at either end being aware. The system would also allow a third party to unencrypt past and future conversations. And it does not allow for people to be anonymous or to verify the identity of the person they are talking to.

In other words, it would be the perfect model for the security services, who can apply pressure to a telecom company and then carry out complete surveillance on an unidentified individual.

While it is surprising that the official UK government system would have such a significant backdoor, it is perhaps less surprising when you consider who developed the spec: the information security arm of the UK listening post GCHQ, the Communications-Electronics Security Group (CESG).

The CESG - and the UK's civil service - started pushing the approach late last year and has incorporated it into a product spec called Secure Chorus. It has also set itself up as an evaluator of other products and is

trying to market its approach commercially by pushing it as "government-grade security." One example of a product already going through this evaluation is Cryptify Call, available for iOS and Android.

There is increasing demand for voicecall encryption. Unlike instant messaging, which effectively allowed companies to start from scratch and so has resulted in a number of highly secure products, phonecalls run over older infrastructure and almost always pass through telecom companies, usually in an unencrypted form (although the information may be encrypted while in transit).

MIKEY-SAKKE is unusual in that unlike most secure messaging and phone systems, it makes no effort at all to protect the identity of the people communicating with one another, providing easy-to- access maps of metadata.

That metadata can be used to specifically identify individuals and then, using the backdoor, access all their calls past and present. In other words, it is the perfect spying system.

Murdoch highlights in his post a number of occasions in which the UK security services have successfully compromised mobile phone networks - instances that were revealed by Edward Snowden - and notes that this is likely only the tip of the iceberg.

If at first you don't succeed

He also notes that GCHQ tried 20 years ago to introduce a similar protocol but that a "notable difference" exists between that effort and this MIKEY-SAKKE approach: "While the GCHQ protocol was explicitly stated to support key escrow to facilitate law enforcement and intelligence agency access, this controversial aspect has not been included in the description of MIKEY-SAKKE and instead the efficiency over EDH is emphasised."

Or in other words, the UK government doesn't want you to know that it can spy on everything you say.

Murdoch notes that things don't have to be this way - there are other products and protocols that provide a much higher level of security. Some, for example, protect past messages from being unencrypted, so even if someone does gain access to your encryption keys, they are limited to current calls. Others make it much harder for telcos to access unencrypted data as it flows through their system.

The hardest aspect, however, is ensuring that when initial contact is made with someone in order to exchange key encryption information, there isn't a person in the middle. One system to do this is to have people physically read out two words that appear on a device and have the other person hear and verify them before starting an encrypted conversation. However, Murdoch notes that even this approach is not foolproof; an attacker could simply impersonate the other caller.

In short then, unless you want to give telcos and government agencies unrestricted access to your phonecalls, it's best not to buy into the MIKEY-SAKKE / Secure Chorus claims of security.

Fox News
Inspector General: Clinton emails had intel from most secretive, classified programs
Tuesday, 19 January 2016
Byline: Catherine Herridge, Pamela Browne

Washington - Hillary Clinton's emails on her unsecured, homebrew server contained intelligence from the U.S. government's most secretive and highly classified programs, according to an unclassified letter from a top inspector general to senior lawmakers.
Fox News exclusively obtained the unclassified letter, sent Jan. 14 from Intelligence Community Inspector General I. Charles McCullough III. It laid out the findings of a recent comprehensive review by intelligence agencies that identified "several dozen" additional classified emails -- including specific intelligence known as "special access programs" (SAP).

That indicates a level of classification beyond even "top secret," the label previously given to two emails found on her server, and brings even more scrutiny to the presidential candidate's handling of the government's closely held secrets.

"To date, I have received two sworn declarations from one [intelligence community] element. These declarations cover several dozen emails containing classified information determined by the IC element to be at the confidential, secret, and top secret/sap levels," said the IG letter to lawmakers with oversight of the intelligence community and State Department. "According to the declarant, these documents contain information derived from classified IC element sources."

Intelligence from a "special access program," or SAP, is even more sensitive than that designated as "top secret" - as were two emails identified last summer in a random sample pulled from Clinton's private server she used as secretary of state. Access to a SAP is restricted to those with a "need-to-know" because exposure of the intelligence would likely reveal the source, putting a method of intelligence collection -- or a human asset -- at risk. Currently, some 1,340 emails designated "classified" have been found on Clinton's server, though the Democratic presidential candidate insists the information was not classified at the time.

"There is absolutely no way that one could not recognize SAP material," a former senior law enforcement with decades of experience investigating violations of SAP procedures told Fox News. "It is the most sensitive of the sensitive."

Executive Order 13526 -- called "Classified National Security Information" and signed Dec. 29, 2009 -- sets out the legal framework for establishing special access programs. The order says the programs can only be authorized by the president, "the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each."

The programs are created when "the vulnerability of, or threat to, specific information is exceptional," and "the number of persons who ordinarily will have access will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved," it states.

According to court documents, former CIA Director David Petraeus was prosecuted for sharing intelligence from special access programs with his biographer and mistress Paula Broadwell. At the heart of his prosecution was a non-disclosure agreement where Petraeus agreed to protect these closely held government programs, with the understanding "unauthorized disclosure, unauthorized retention or negligent handling ... could cause irreparable injury to the United States or be used to advantage by a foreign nation." Clinton signed an identical non-disclosure agreement Jan. 22, 2009.

Fox News is told that the recent IG letter was sent to the leadership of the House and Senate intelligence committees and leaders of the Senate Foreign Relations Committee, as well as the Office of the Director of National Intelligence (ODNI) and State Department inspector general.

Representatives for the ODNI and intelligence community inspector general had no comment.

In a statement, State Department spokesman John Kirby said, "The State Department is focused on and committed to releasing former Secretary Clinton's emails in a manner that protects sensitive information. No one takes this more seriously than we do."

The intelligence community IG was responding in his message to a November letter from the Republican chairmen of the Senate intelligence and foreign relations committees that questioned the State Department email review process after it was wrongly reported the intelligence community was retreating from the "top secret" designation.

As Fox News first reported, those two emails were "top secret" when they hit the server, and it is now considered a settled matter.

The intelligence agencies now have their own reviewers embedded at the State Department as part of the Freedom of Information Act (FOIA) process. The reviewers are identifying intelligence of a potentially classified nature, and referring it to the relevant intelligence agency for further review.

There is no formal appeals process for classification, and the agency that generates the intelligence has final say. The State Department only has control over the fraction of emails that pertain to their own intelligence.

While the State Department and Clinton campaign have said the emails in questions were "retroactively classified" or "upgraded" - to justify the more than 1,300 classified emails on her server - those terms are meaningless under federal law.

The former federal law enforcement official said the finding in the January IG letter represents a potential violation of USC 18 Section 793, "gross negligence" in the handling of secure information under the Espionage Act.

Ottawa Citizen
Canada hard-pressed to deliver on offer to aid intelligence in Iraq
Wednesday, 20 January 2016
Byline: David Pugliese

Defence Minister Harjit Sajjan has been touting the potential for Canada's military to help gather intelligence in Iraq in the battle against Islamic extremists.
But with no recent history of meaningful involvement in Iraq or Syria, a scarcity of Arabic speakers, and a lack of intelligence- gathering equipment such as drones, how much of a contribution can Canada's military make?

In late December, Sajjan told journalists that the Liberal government is considering contributing an intelligence capability to the war against the Islamic State, including helping improve the abilities of Iraqi security forces to target extremists. He suggested the Canadian Forces have technology to play this role, but didn't specify whether that would be equipment on the ground or in the air.

In other interviews, the minister has said that Canada's intelligence capabilities are second to none and the government was looking at how to increase that in the Iraq war.

Sajjan, a former officer who dealt with military intelligence during the Afghan war, has emphasized understanding the political and tribal dynamics of ongoing wars.

But the Canadian Forces don't have extensive background in Iraq, having concentrated most of their efforts for more than a decade on Afghanistan.

The Canadian military only has a handful of linguists who speak Arabic. Its intelligence organization acknowledges it has no idea of how many serving in its ranks speak languages used in Iraq or Syria.

"While the Canadian Armed Forces does maintain rosters of members with ability in languages other than English and French, we do not specifically track the number of Arabic speakers within the Intelligence Branch," Defence Department spokesman Evan Koronewski said in an email.

But he added, "all intelligence officers and operators are highly trained and provide commanders with valuable support to decisionmaking, planning and operations." The federal government's electronic spy agency, the Communications Security Establishment, could play more of a role, but it is already monitoring phone calls and emails of Islamic extremists.

The Canadian military doesn't have any long-range drones, such as those used by the U.S. and Britain to gather intelligence or target and kill ISIL leaders.

Shortly before entering the war in the fall of 2014, the RCAF put out feelers to Canada's aerospace industry on whether it could provide drones or intelligence-gathering aircraft on short notice.

Companies told the military it could be done but the RCAF never progressed further on that issue.

It wasn't the first time, however, the RCAF has conducted a lastminute search for intelligence equipment to support a war effort. During the Libyan conflict in 2011, senior Canadian military leaders pitched the idea of spending up to $600 million for armed drones to take part in the war but the Conservatives decided against that.

Although Public Services and Procurement Canada asked aerospace companies on Friday for information about drones they could provide, the RCAF has pointed out that is a capability for the longer term, and such aircraft, if purchased, wouldn't be available until after 2019.

One intelligence-related capability the Liberal government could provide is the RCAF's CP-140 surveillance aircraft.

Prime Minister Justin Trudeau has said his government will follow through with its plan to withdraw the six CF-18 fighter jets. Canada has been asked by the U.S. to leave the two CP-140s that are now flying surveillance missions over Iraq. The RCAF has at least four more of those aircraft, which have been modified with advanced surveillance equipment. The Liberals could boost that contribution, sources say.

Meanwhile, Sajjan wouldn't say why Canada won't be at a meeting in Paris this week in which counterparts from seven countries will discuss the fight against the Islamic State. The Washington Post cited an unnamed U.S. official saying the meeting would involve countries with "the most skin in the game."

But Sajjan minimized the importance of the meeting, saying he is regularly updated on the situation.

"Meetings happen all the time.

There's a number of other meetings that happen that you may not actually be aware of," he said. "I have a couple of meetings that are going to be coming up in the next few weeks to talk about ISIL."

The Courier-Mail
Turnbull calls for cyber war
Wednesday, 20 January 2016
Byline: Simon Benson

Washington - Malcolm Turnbull will ask US President Barack Obama to broaden the war against Islamic terrorists from the battlefield into cyberspace, when they meet at the White House today.
While the military campaign against ISIS was making gains, the Prime Minister yesterday warned the Western world was losing the social media propaganda war.

It is expected that Mr Turnbull will seek to promote Australia as taking a lead global role in cyber warfare.

"(ISIS) may have an archaic and barbaric ideology, but its use of technology and social media in particular is very sophisticated and agile," he said in a speech yesterday to the Washington- based Centre for Strategic and Independent Studies.

"(ISIS's) threat to sweep across continents like the armies of Mohammed, to stable their horses in the Vatican, are crazed delusions.

"We should not amplify them."Mr Turnbull has dramatically sharpened his language on terrorism since arriving in Washington on his first official visit to the US, which follows criticism that he has not been hawkish enough on terrorism since refusing extra troops.

Al Jazeera
Opinion: Sponsor Syrian Refugee - Canada's top Google search
Wednesday, 20 January 2016
Byline: Antonia Zerbisias
Section: Opinion

Last September, after the photograph of three-year-old Alan Kurdi's body on that Turkish beach hit the world's front pages, the top Google search term in Canada was, "How to sponsor a Syrian?"
The news media here, in the midst of covering a federal election campaign, jumped all over the Kurdi story. Not just because it was tragic, nor because of the Kurdi family's Canadian connection through the toddler's Vancouver-based aunt, but because the country, bitterly divided over the former Conservative government's attitudes towards Muslims, suddenly didn't recognise itself as the welcoming, multicultural nation it had long believed itself to be.

And so, on TV, online and in print, there were stories on how many refugees were expected, how few the Stephen Harper regime had approved, and how Canadians, individually, in groups and as part of community organisations, could sponsor Syrian refugee families.

Then, on October 19, 2015, the Harper Conservatives were defeated and the Liberal government under Justin Trudeau swept to power.

Immigration organisations such as Lifeline Syria were flooded with phone calls. Settlement services scrambled to produce handbooks and hold seminars on sponsorship. Children began competing in a "1,000 Schools Challenge" to each bring in a family.

People banded together in "Groups of Five" to raise the estimated $30,000 it takes to privately sponsor families of four. Churches, mosques and synagogues partnered to bring in refugees. Business stepped up, with funding, free mobile phones and furniture.

Property companies reserved hundreds of apartments. One entrepreneur pledged more than $1m to sponsor 50 families.

During the election campaign, Trudeau had promised to settle 25,000 refugees by the end of the year. That would prove to be impossible. Refugees can't row in crowded dinghies or stream over borders here as they do in Europe. They must come in by plane. It takes logistics. Which is why, despite the enthusiasm of many Canadians, the goal of 25,000 was trimmed to 10,000 by December 31, with the remainder due to land by March 2016.

True, many Canadians were resistant, split especially following the November bombings in Paris. So, while the media were running feel-good stories about the sponsor application rush, anybody scanning the comments sections would find very different attitudes indeed.

In early December, however, when Trudeau turned up at Toronto's Pearson International Airport to greet the first arrivals and help them into warm coats, the country's collective heart melted, its national pride burst.

Sure there were bumps. A sponsorship group in Oakville, Ontario found doors slammed shut when it sought housing for its refugee family.

In Vancouver, in what has been deemed a "hate crime", 15 men, women and children were pepper-sprayed at a welcome ceremony. The New Year's Eve sexual assault rampage allegedly committed by recent arrivals in Cologne triggered a wave of fear and loathing. But the planes kept landing.

According to Canada Immigration and Citizenship, as of January 14, 10,790 refugees have arrived, about half of them Christian, approximately half privately sponsored. Private groups are still submitting some 200 sponsorship applications a week.

Last Wednesday, Joe Jacobs' Syrian family landed. The Muslim couple and their eight children, who range in age from weeks-old to 17 years, had fled Daraa in southwestern Syria where the father was a baker. They arrived to shiver in sub-zero weather but to bask in a warm welcome.

"Our group was supposed to get 24 to 48 hours' notice that they were coming but we got a phone call saying that they were waiting at the hotel; we had to be there within the hour," Jacobs tells Al Jazeera. "Luckily we had made preparations ahead of time."

The Toronto teacher is part of a "Group of Five" that connected through their children's school. They raised money from others and contributed their own funds to bring in the family whose identity they are protecting. They are committed for one year to aid the newcomers with everything from finding housing, schools, jobs and language lessons to introducing them to the city and culture.

Jacobs is realistic about the challenges ahead: "You have to provide the support part but you can't be too paternalistic about it. You don't want to treat them as the wretched people of the earth. It is such a difficult position to be placed in where you're dependent on people where you really shouldn't have needed to be and you're expected to be so grateful. And I think that a danger with the whole programme a bit is that Canadians are trying to be very generous but need to be careful that these people are not treated as playthings; that these people should have what they need."

As for what he calls the "euphoria" and media frenzy over Canada's apparent acceptance of refugees, Jacobs is wary.

"It seems to be all about us," he observes. "There seems to be a lot of focus on how wonderful we are to be doing this sort of thing when, for example, part of the discussion for our [refugee] family is, 'How are we going to help these people to rise out of a certain level of poverty here in Canada?' These families have a really tough row to hoe ahead and I'm not sure how much Canada and the Canadians who are sponsoring are understanding of that."

What worries Jacobs is not so much that the refugees adjust to Canada - although that's critical - but that Canada adjusts to them.

"Last week, when we all were getting on a bus, the driver was like 'Holy ****!' and was just looking at them; it was such a negative reaction," he recalls. "The family didn't understand but we certainly saw that a negative view is out there. I don't know how predominant it is, but it has the potential to grow when the euphoria dies down."

Jane Philpott, the health minister, seemed unconcerned last week when she declared: "The integration phase is ultimately the most important phase, to make sure that these Syrian refugees become well integrated into Canadian culture, that they understand our cultural values and practices.

"The question to me is more can the people of Montreal and Toronto handle this?" Jacobs says. "It's not so much whether the system can. It's whether Canada allows these people to live in poverty or will support them to become economically integrated members of society. "And if they don't, the question then becomes why did we say we're going to accept them?"

Antonia Zerbisias is an award-winning Canadian journalist.

The Australian
Cyber world the new frontline in terror war
Wednesday, 20 January 2016
Byline: David Crowe

Washington - Australia and the US are preparing a wider front in the fight against terrorism as they negotiate ways to implement "cyber warfare" campaigns to disrupt -Islamic State's propaganda -machine and stymie its efforts to recruit jihadists.
Malcolm Turnbull will discuss the tactics with counter-terrorism experts in Washington DC amid growing concern the US and its -allies are not doing enough to -defeat the terrorist group on the battlefield and online.

The talks will follow the Prime Minister's meeting with President Barack Obama to map out the next phase of the military campaign, including the prospect of retaking Mosul from the terrorists who overran Iraq's second-largest city last May.

"The discussion on cyber goes to how can we take the fight back to them," the US ambassador to Australia, John Berry, said in Washington DC.

"How can we isolate them? Why are we giving them access to this institution called the internet that we created?" Amid a domestic political -dispute over whether Australia is doing enough in the military fight against Islamic State, Mr Turnbull gained clear support from the US on the criticism levelled against him.

In Iraq, the spokesman for the joint Coalition operations, Colonel Steve Warren, said the US was looking to all countries to contribute more to the campaign but that Australia already made a larger contribution than others countries.

"On the list of people who need to step up, the Australians are at the very bottom of that," Colonel Warren said in Iraq. "They've stepped up already. But it's time to see others." In the US, Mr Berry dismissed claims that Australia had rejected a request for more troops. "Some of the reporting on what was -requested is mistaken," he said.

"The request was for all of our 60 nation partners to identify areas where each of them, in their sovereign capacity, believed they could best contribute to the ongoing fight against ISIL.

"It misreports to say the United States requested additional troops. We did not. There was no such request." Mr Turnbull yesterday met Defence Secretary Ashton Carter during talks at the Pentagon about military strategy, including the hope of retaking Mosul.

Mr Turnbull backed the idea of a formal partition of parts of Iraq and Syria. "The border between Syria and Iraq is just a line on the map. -Neither country can be secured without a settlement in the other," Mr Turnbull said at the Centre for Strategic and International Studies in Washington DC.

"Unless the Sunni populations in Syria and Iraq can be reconciled with a new and inclusive order, then ISIL or a successor extremist group will have a ready recruiting ground.

"The enmities are so deep, the wrongs so shocking, that every -option should be on the table -- from an institutionalised power sharing to some form of partition."

Le Devoir
L'enveloppe brune, version XXIe siècle
Wednesday, 20 January 2016
Byline: Stéphane Baillargeon

Montréal - Radio-Canada lance une plateforme sécurisée pour lanceurs d'alerte
L'idée est tellement bonne et tellement simple qu'on se demande pourquoi aucun média québécois ne l'a eue auparavant : Radio-Canada (RC) annoncera officiellement aujourd'hui, mercredi, le lancement d'une plateforme numérique consacrée au transfert sécurisé de données. Le moyen de communication sécurisé, premier du genre pour un média québécois, est librement mis à la disposition des lanceurs d'alerte pour transmettre des informations sensibles aux médias.

L'idée est tellement bonne et tellement simple qu'on se demande pourquoi aucun média québécois ne l'a eue auparavant : Radio-Canada (RC) annoncera officiellement aujourd'hui, mercredi, le lancement d'une plateforme numérique consacrée au transfert sécurisé de données. Le moyen de communication sécurisé, premier du genre pour un média québécois, est librement mis à la disposition des lanceurs d'alerte pour transmettre des informations sensibles aux médias.

" C'est un outil de plus pour les journalistes qui s'ajoute aux bonnes vieilles enveloppes brunes, aux clés USB, aux disques durs externes, aux courriels envoyés d'adresses anonymes ", dit Marie-Maude Denis, journaliste et coanimatrice de l'émission Enquêtes d'ICI Radio-Canada Télé. " D'abord, il y a une très forte préoccupation pour la protection des sources, une valeur suprême pour nous, les journalistes d'enquête. Ensuite, pour un informateur qui désire rester anonyme, le choix d'un média peut parfois se faire en fonction de la confiance envers une organisation de presse. "

La plateforme baptisée Source anonyme est le résultat de l'Accélérateur d'idées. Avec ce concours interne intermittent, RC propose à ses employés de soumettre des plans pour bonifier leurs pratiques. Deux projets ont terminé la course l'an dernier, un sur les nouvelles formes de narration et celui-là sur les sources.

" Du point de vue des rapports entre sources et journalistes, nous faisons vraiment passer Radio-Canada au XXIe siècle, dit Xavier Kronström Richard, cofondateur avec Thomas Le Jouan du RC Lab et de l'Accélérateur d'idées. C'est un moyen dans l'air du temps, lié à la cybersurveillance par exemple. "

L'étincelle est venue de là. " J'ai soumis ce projet pour informateurs dans la foulée des événements qui ont entouré les révélations d'Edward Snowden ", explique l'idéatrice Catherine Mathys, chroniqueuse à l'émission de radio La sphère et blogueuse sur Triplex. L'informaticien américain a révélé l'ampleur des programmes de surveillance de masse américano- britanniques. " Quand j'ai soumis l'idée, aucun média au Canada n'avait une telle plateforme. Le temps que je devienne une des cinq finalistes du concours, le Globe and Mail avait lancé sa plateforme. Il en existe ailleurs dans le monde. Mais bon, moi, je proposais juste que RC se dote de cet outil pour nos équipes d'enquête. "

En quoi cet outil numérique s'avère-t-il particulièrement intéressant ? Marie-Maude Denis répond avec l'exemple d'un envoi massif de données. Pas vraiment un cas fictif comme le prouvent les Offshore Leaks qui ont coulé vers un consortium de 36 médias (dont RC), des masses d'infos sur les paradis fiscaux depuis 2013.

" Notre plateforme peut peut-être inciter des informateurs à nous transmettre ce genre de données extrêmement volumineuses, dit la reporter et animatrice. C'est donc une offre supplémentaire pour communiquer avec nous en utilisant un processus très, très sérieux d'homologation de la sécurité. "

Comment ça marche

Le fonctionnement semble simple. Un bouton placé sur le site de l'émission Enquêtes mène à sourceanonyme.radio-canada.ca. La page d'accueil explique l'utilisation de la messagerie SecureDrop, " technologie en code ouvert développée par Aaron Swartz et gérée par la fondation Freedom of the Press ". Pour l'instant, la mécanique est en anglais, mais RC développe une version en français avec la Fondation basée en Californie.

L'utilisateur doit télécharger gratuitement le navigateur Tor, l'ouvrir et suivre les instructions pour finalement recevoir un code unique pour la transmission des informations sensibles. Les instructions recommandent de le mémoriser et ne l'écrire " nulle part ". Une station informatique sert à décrypter les messages et " seul un nombre restreint de responsables " y a accès.

" Sur notre site, nous aidons les gens à transmettre des informations de manière anonyme et nous, de notre côté, nous avons une station qui reçoit les messages cryptés sans identifier l'émetteur, résume Xavier K. Richard. C'est un peu une boîte de courriels mais où tout est crypté de part et d'autre. "

Cela établi, rien n'assure la sécurité pleine et entière, blindée et étanche. " Il n'y a aucun moyen de communication, aussi sécuritaire soit-il, qui est confidentiel à 100 %, et nous le disons sur notre plateforme, dit Mme Mathys. Une brèche est toujours possible, ne serait-ce qu'à partir de l'ordinateur

de l'informateur. On n'a pas de pouvoir là-dessus. Mais la plateforme est très, très sécuritaire. Elle est utilisée par une vingtaine de médias dans le monde et c'est une des ressources les plus fiables. "

Ce qui rappelle finalement l'importance de protéger socialement les lanceurs d'alerte. Le récent rapport de la commission Charbonneau sur la collusion dans l'industrie de la construction au Québec en faisait une recommandation.

" Les mesures pour protéger les sources journalistiques sont essentielles et pourtant insuffisantes en ce moment, dit Mme Denis. Le gouvernement [du Québec] a commencé à discuter d'un projet pour protéger les sources, mais il est très, très limité. Les journalistes sont unanimes pour reconnaître qu'on manque de protection vis-à-vis des personnes qui prennent parfois énormément de risques pour dénoncer certaines situations. Nous, comme journalistes, on accompagne ces gens parfois pendant des années, en prenant de très grands risques, souvent par altruisme, pour aider la société à voir plus clair. Alors tout mécanisme de protection supplémentaire des lanceurs d'alerte sera applaudi. "

Faut-il finalement voir dans la création de Source anonyme un effet pervers de l'assèchement d'une grande talle des enquêtes avec le dépôt du rapport de la commission Charbonneau ? " La talle n'est pas sèche : je peux vous dire que c'est encore bien irrigué par en dessous ", répond Marie- Claude Denis en rigolant. Catherine Mathys ajoute que son projet date d'avant la fin des travaux de la Commission.

The National (UAE)
Cyber attacks will get violent in the future, UAE security expert warns
Wednesday, 20 January 2016
Byline: Caline Malek

Dubai - The next wave of -cyber attacks will attempt to take human lives, according to a senior officer at the telecommunications operator du.
Although the country was taking steps to establish better protection against attacks on critical national infrastructure, Tamer El Bahey, who is the senior director of security monitoring and operations at du, said more investment was needed for detecting and responding to incidents.

"In the evolution of cyber attacks, we started from those that caused annoyance to people. Then we moved to those that would disrupt network and services on organisations," he said.

"Now, we are in the era of attacks where most information is exposed. Credit card information is being stolen and we should anticipate the worst."

Mr El Bahey, who addressed an audience at Intersec in Dubai on Tuesday, said such new attacks would involve hacking remote devices.

"For example, you can disable a car's brakes or engine while it is moving or a pacemaker in hospitals, which would play with configuration and cause death to patients," he said.

"There are lots of attacks against critical national infrastructure like one that happened in Australia where they hacked into the water system and started to release untreated water into the water stream.

"So imagine if someone released poisonous chemicals into the water stream of people and they got seriously sick and died."

Matthew Cochran, chairman of Defence Marketing Services Council in Abu Dhabi, said the threat level was growing.

"There is a lack of cyber security awareness and many of the things that people must be aware of are things like access control," he said.

"It's not about physical access control any more. It's about your mobile device and anything that's connected to the internet. The internet brings great possibilities but also, if unchecked, could bring new threats that we haven't seen; and that will start with the telecommunications and network security."

The UAE's National Electronic Security Authority is taking strict measures to counter such threats.

"In the UAE, we use a lot of technology," Mr El Bahey said. "The UAE is now establishing these kinds of controls, telling people they need to make sure their critical national infrastructure [must] be protected, resilient and can absorb these kinds of attacks. It is leading in the Middle East and the Gulf."

Simon Williams, global business continuity manager at National Bank of Abu Dhabi, said the UAE was well prepared for any attack but there was no room for complacency.

"We need to identify critical infrastructure and it should be the focus of our investment," Mr El Bahey said.

"We need to better invest in detection and incident--response capabilities. Prevention isn't working or helping any more. We need to balance the investment because 85 per cent is invested by the industry in preventive controls while just 15 per cent on detective and incident response. We need to have a fair share between the two."

Chosun Ilbo
Latest Cyber Attack Traced to N.Korea
Wednesday, 20 January 2016

A recent cyber attack on South Korean government agencies has been traced to North Korea as expected.Police said the IP addresses of the senders of spam e-mails on Jan. 13-14, right after the North's latest nuclear test, were the same as those used in a cyber attack against Korea Hydro and Nuclear Power in 2014.The e-mails containing malicious code purported to come from Cheong Wa Dae and targeted thousands of government employees here. Police said the IP addresses have been traced to the northeastern Chinese province of Liaoning that borders North Korea and match those used in the cyber attack against the nuclear agency in 2014.In 2014, the hackers threatened to paralyze nuclear power plants and leaked some reactor blueprints to the public.Police said the latest attack was something known as "two-track phishing e-mails" where hackers hide malware in second e-mails that are sent after recipients respond to the uncompromised first e- mails.

Times of India
IB intercept hints at terror strike on Jan 23
Wednesday, 20 January 2016
Byline: Rohan Dua

Chandigarh - Three weeks after the Pathankot terror attack, an Intelligence Bureau (IB) intercept of a Bangladeshi mobile number has sent security agencies into a tizzy. The coded phrase -- "doctor medicine lekar jayega" -- was intercepted on January 15 twice by IB sleuths on a telecom gateway. Gateway alerts Indian authorities of all incoming calls from Pakistan and Bangladesh based on a specific area or series of numbers.
The alert, sent to all state police chiefs on Monday, says that Bangladesh-based Islamist group Hizb ut-Tahrir (HuT) is planning to carry out terror strikes at 23 locations across India, including Gurdaspur and Pathankot. "The group is planning bomb and suicide attacks on January 23," it reads. "In view of this, the field staff must be sensitized to take all necessary preventive and precautionary measures including review and strengthening of security of Army, Air Force, BSF and other vital installations."

It adds that this time malls, bazaars and educational institutes could be on the group's radar. According to the alert, HuT, which has a significant presence in Pakistan and Bangladesh, is planning these strikes with assistance from Jaish-e-Muhammed (JeM) and Lashkar-e-Taiba (LeT).

The alert hints at growing strength of HuT's armed wing called Harakat ul-Muhojirinfi Britaniya that trains its cadres in chemical, bacteriological, and biological warfare.

Punjab Police officers are taking this alert seriously for multiple reasons. For starters, it gives specific details. Also officials had recently found a GPS device outside the barracks of the Railway Police Force (RPF) office in Ferozepur -- another district of Punjab that shares a border with Pakistan -- which had Bangladesh time pre-fed in it. Bangladesh time is half an hour ahead of India. The device has sent to Forensic Science Laboratory, Chandigarh.

"This may me just coincidental but our men were surprised to find an abandoned device with Bangladesh time," said a senior Punjab Police cop. This is the second high alert after the December 27 IB note that warned of a "spectacular" attack by at least 15 terrorists of JeM and LeT just ahead of the Pathankot strike.

Bloomberg View
Clinton Takes On Top Intelligence Watchdog
Thursday, 21 January 2016
Byline: Josh Rogin

Column - Hillary Clinton's presidential campaign Wednesday accused the intelligence community's top oversight official of conspiring with Republicans in the Senate to leak sensitive information about her personal e-mail server. That's a risky move, considering that it has produced no hard evidence of a conspiracy and the accused parties are denying it.
The public dispute between the former Secretary of State and the Inspector General of the Intelligence Community reached new heights following Tuesday's report by Fox News on a letter sent by inspector general I. Charles McCullough to Senate Intelligence Committee Chairman Richard Burr and Senate Foreign Relations Committee Chairman Bob Corker. In the letter, McCullough stated that he had received sworn declarations from two separate intelligence agencies that cover "several dozen e-mails" on Clinton's private server. These e-mails were determined by these agencies to contain information that should have been treated as secret, top secret, and "SAP," an abbreviation that refers to "special access programs," which are among the most sensitive in the government.

Clinton campaign spokesman Brian Fallon told me in an interview Wednesday that the campaign believes that McCullough and the Republican senators worked behind the scenes to orchestrate a series of events that would lead to the disclosure of those declarations.

"It is suspect from the beginning that the intelligence community inspector general is continuing to reveal materials and surface allegations while the Justice Department review is going on," Fallon said. "It's completely fair to suspect that the intelligence community inspector general is not operating in good faith." He provided no hard evidence to support these assumptions, however.

Now that the FBI is investigating the handling of information found on Clinton's server, Fallon said, the intelligence community inspector general should stay out of it and let the Justice Department do its work. But McCullough's letter shows he intends to keep trying to influence the outcome.

According to the Clinton campaign, the inspector general and the Republican senators have separate agendas in wanting to influence the public debate over whether or not Clinton's e-mail server contained highly classified information. The Republicans simply want to hurt Clinton's political aspirations, Fallon said. But the inspector general's move, Fallon said, is part of a campaign to influence a bureaucratic battle between the intelligence community and the State Department.

The State Department and intelligence agencies disagreed last August over whether two e-mails found on Clinton's server should have been treated as "top secret." The State Department said the information that the e-mails contained was not classified when the messages were sent, but the intelligence agencies said the information was always classified and should have been treated as such. The State Department asked James Clapper, the director of national intelligence, to adjudicate that dispute.

In November, a Politico report stated that intelligence officials reviewing those two e-mails were leaning toward the State Department's opinion. Following that report, Burr and Corker wrote to McCullough to ask for an update and McCullough responded. Fallon alleges that the timing of the letters is evidence enough of a conspiracy to leak the information.

"It looks like Clapper's office will undercut McCullough," Fallon said. "McCullough is trying to litigate this with Clapper and have his own view of these two e-mails upheld."

Burr told me in a short interview Wednesday that his committee was just following up with the intelligence community inspector general about his progress in getting information from the intelligence agencies. He denied leaking McCullough's letter or working with McCullough behind the scenes in any way.

"I can tell you there's no conspiracy or collusion between Bob Corker and I and the inspector general," Burr said. "The Clinton campaign would be wrong."

Deb Chapman, spokesperson for the intelligence community inspector general's office, declined to comment on the Clinton campaign's allegations, but said that McCullough stands by the information contained in his letter to Burr and Corker, a copy of which Fox News obtained.

"Catherine Herridge's article was spot on," she said, referring to Fox News's intelligence correspondent. "It's all accurate."

For a major political candidate and former cabinet official to publicly accuse an inspector general of the intelligence community of intentional leaking and collusion with their political opponents is remarkable, if not unprecedented. McCullough, an attorney and former FBI agent, was unanimously confirmed for his position in 2011 and received praise from senators on both sides of the aisle.

"No one should make such an accusation without evidence," Steven Aftergood, who directs the project on government secrecy at the Federation of American Scientists, told me. "If there is evidence of collusion or partisanship, it should be presented. If there is no such evidence, the accusation should not be made."

Whether or not the information in the e- mails is really top secret is unknowable because the e-mails are not public, Aftergood said. Several reports Wednesday quoted anonymous officials saying the information in question was not particularly sensitive because it referred to public news reports about the U.S. drone program. That program is highly classified but often discussed in the press.

"CIA considers everything about the targeted killing program to be highly classified covert action," Aftergood said. "But the State Department can consider information in the press to be unclassified."

Even passing on news clippings about a classified program can be considered mishandling of classified information, but it's a case-by-case evaluation and the lines are murky, said Aftergood. Usually, deference is given to the agency that originated the information, in this case the CIA and another as yet unnamed agency.

For Fallon and the Clinton team, their inability to publicly discuss the content of the e-mails is key to their grievance: How can Clinton defend herself from leaks without talking about what was on her server? The intelligence community inspector general's office has a corresponding problem: It can't fend off Clinton's accusations of partisanship and collusion because it is enjoined from commenting on political matters.

Clinton's calculation seems clear: By framing the controversy over the private e-mail server as a good-faith dispute between two government bureaucracies, she can divert attention from her own culpability in placing so much sensitive information in her own house. But that strategy depends on the State Department standing by her.

That may be changing, at least in public. Whereas in August, department officials said they were confident their own review of the e- mails revealed no information marked classified at the time it was sent, their public line is now less definitive.

"Our FOIA review process is still ongoing. Once that process is complete, if it is determined that information should be classified as Top Secret we will do so," State Department spokesman John Kirby told me in a statement.

Intelligence officials, even inspectors general, are not immune from politics, both internal and partisan. But Clinton's team simply cannot prove that McCullough is leaking against them. Her campaign can only muddy the waters and delay until the FBI finishes its work. If the Clinton campaign decides then to go after the FBI, it will be picking a fight with an even more formidable opponent.

The Intercept
The White House Asked Social Media Companies to Look for Terrorists. Here's Why They'd #Fail.
Thursday, 21 January 2016
Byline: Jenna McLaughlin

Column - The White House asked internet companies during a counterterrorism summit earlier this month to consider using their technology to help "detect and measure radicalization."
"Should we explore ways to more quickly and comprehensively identify terrorist content online so that online service providers can remove it if it violates their terms of service?" asked a White House briefing document that outlined the main topics of conversation for the meeting. The document, which was obtained by The Intercept, is now posted online.

The briefing suggested that the algorithm Facebook uses to spot and prevent possible suicides might be a helpful model for a technology to locate terrorists, asking: "Are there other areas where online providers have used technology to identify harmful content and remove it? ... Something like Facebook's suicide process flow?"

Government officials also want to use such an algorithm for law enforcement purposes. "Are there technologies that could make it harder for terrorists to use the internet ... or easier for us to find them when they do?" read the briefing.

"We are interested in all options to better identify terrorist networks, or indications of impending plots. ... Are there ways to glean from changes in patterns of use of these platforms involvement in preparations for violence?"

An increasingly large proportion of terrorism investigations these days start with tweets or posts, generally flagged by family members or informants. Civil libertarians worry that the FBI is using protected speech to identify potential subjects of entrapment. But the FBI's concern is that it's not seeing everything it needs to see.

And at the same time, there's increased pressure for social media companies to deny radical groups an open platform for speech.

No wonder the government wants an algorithm.

But there are some major problems with trying to use computer code to find "terrorists" or "terrorist" content.

First of all, it doesn't work. Many experts, including people with law enforcement, academic, and scientific backgrounds, agree that it's practically impossible to boil down the essential predictive markers that make up a terrorist who is willing and capable of carrying out an attack and then successfully pick him out of a crowd.

"Many believe that data mining is the crystal ball that will enable us to uncover future terrorist plots. But even in the most wildly optimistic projections, data mining isn't tenable for that purpose," wrote Bruce Schneier, prominent cryptologist and fellow at Harvard's Berkman Center for Internet and Society, in 2006.

Despite hyped-up cable news coverage and fearmongering messages from government officials, terrorism is an incredibly rare event in the United States. According to the New America Foundation's attack tracker, there have been a total of nine "violent jihadist attacks" on U.S. soil since September 11, 2001, resulting in 45 deaths.

Algorithms are good at some things -- like correctly concluding that your credit card has been stolen. But that's because it happens so commonly, there are not many variables, and incidents follow a predictable pattern.

"Something as unique and rare as terrorism -- that's what makes this different from credit card fraud," Schneier told The Intercept.

Consider medical testing, Schneier said. "When a disease is very rare, if your test tests positive, it's almost always wrong, because your chances of having that disease are one in a million."

Think about that for a minute: Imagine you're trying to determine who has that incredibly rare disease, and it can be spotted by genetic testing.

Say your test is 90 percent accurate in determining whether someone suffers from that disease. That means it is also wrong 10 percent of the time. One out of 10 of your patients will test positive, even though chances are that none of them have the disease.

Out of a million people, 10,000 would test positive -- but chances are only one would really have the disease. And you wouldn't know which one.

Now imagine the odds are one in 100 million, amid many hundreds of millions of social media postings. Imagine how many posts would be deleted or referred to law enforcement in error.

And keep in mind there's no real way to come up with a test for terrorism that's even 90 percent accurate. There's not even a good statistical database of people charged for terrorism-related crimes, just for starters.

False positives when using algorithms to spot suspected credit card fraud have little cost. "A call to the customer from a credit issuer will reassure the customer whether he or she is correctly targeted or not," said Jim Harper, a senior fellow at the Cato Institute, during a Senate Judiciary Committee hearing on data mining in 2007.

But "identifying" terrorists is a different matter. "Because of the statistical impossibility of catching terrorists through data mining, and because of its high costs in investigator time, taxpayer dollars, lost privacy, and threatened liberty, I conclude that data mining does not work in the area of terrorism," Harper said.

"Of course there's no way for software to identify and remove terrorists or terrorist content from online media," Phil Rogaway, a computer science professor at UC Davis, wrote in an email to The Intercept. "A group of humans would routinely disagree if a given email or post constitutes terrorist content, so how on earth is a program to make such a determination?"

A 2008 government study also concluded that counterterrorism data-mining programs seeking patterns in personal information, like travel records, phone records, and website browsing history, were ineffective and should be evaluated for privacy impacts.

Local "fusion centers" designed to share intelligence and data on terrorism and report back to the Department of Homeland Security were described by Senate investigators in 2012 as "oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism."

And what if such an algorithm is put into action, and starts automatically deleting posts?

In the briefing document, the administration asks whether "technologies used for the prevention of spam" might be useful in locating and removing terrorist content.

But a filter like that could easily snatch up First Amendment protected speech.

"Censorship has never been an effective method of achieving security, and shuttering websites and suppressing online content will be as unhelpful as smashing printing presses," said former FBI agent Michael German, a fellow at the Brennan Center for Justice.

I shared some passages from the White House briefing with him. "These passages make clear that the government continues to cling to long-disproven, simplistic theories of terrorist radicalization, which suggest that the exposure to extreme ideas leads to terrorist violence," he wrote in an email to The Intercept. "If ideas are identified as the problem, the only solution can be the suppression of those expressing such sentiments."

Algorithms that filter content are "a really powerful tool for a more authoritarian government," said Schneier.

"Electronic monitoring and censorship can be effective for chilling political dissent, removing much content that authority frowns upon, and making people fearful of discussing political subjects online," UC Davis' Rogaway wrote in an email. "China already does this quite effectively."

The government briefing does acknowledge that "respecting U.S. First Amendment commitments to human rights such as freedom of expression" would be important in any sort of system of identifying and reporting radical online posts.

But overall, the briefing document "reveals a troubling amount of magical thinking on the part of government officials," German wrote. "It seems they are going to continue ignoring the vast amount of research that describes terrorism as a complex behavior that can only be understood in the context of

the political situation in which it arises, and continue investing in snake-oil salesmen who promise a simple solution that identifies the 'bad guys' right before they strike."

The Local (Sweden)
Ecuador: Sweden to question Assange 'soon'
Thursday, 21 January 2016

Stockholm - WikiLeaks founder Julian Assange could face questions from Swedish prosecutors "in the coming days" at his hideout at the Ecuadoran embassy in London, the President of Ecuador has said. Rafael Correa did not give a date for the interrogation over a 2010 rape allegation in Sweden, which Assange denies, but said it would happen "very soon".

"We hope in the coming days Mr Julian Assange will be interrogated by Ecuadoran authorities on the basis of questions and requests from Swedish prosecutors," the president told a press conference on Wednesday.

Assange fled to the embassy in 2012 to escape extradition proceedings.

The 44-year- old Australian refuses to travel to Sweden to answer the allegation, saying he fears he would then face extradition to the United States and trial over the leaking of hundreds of thousands of classified US military and diplomatic documents in 2010.

After a three-year stalemate, Ecuador and Sweden signed a legal cooperation deal last month that clears the way for Assange to be interrogated at the embassy.

FCW.com (US)
U.S. discloses zero-day exploitation practices
Thursday, 21 January 2016
Byline: Chase Gunter

Washington - The federal government has confirmed that it uses undisclosed software bugs not only in espionage and intelligence gathering, but also in the course of law enforcement activities.
In November 2015, the government released a redacted version of the Vulnerabilities Equities Process, the policy that lets agencies such as the National Security Agency and FBI decide whether to announce the flaws to vendors for patching. Just weeks ago, the government argued that acknowledging its exploitation of the software flaws, known as zero-day vulnerabilities, would damage national security.

Now the government has rescinded some of those redactions in its first official acknowledgment of "defensive, offensive and/or law enforcement-related [and] prosecutorial" uses of the vulnerabilities beyond counterterrorism efforts. The disclosure comes in response to a Freedom of Information Act

lawsuit filed by the Electronic Frontier Foundation seeking the release of documents on the U.S. government's use of such flaws for intelligence gathering.

"This is the first confirmation that [the Vulnerabilities Equities Process] is used for law enforcement, which was an open secret," said EFF staff attorney Andrew Crocker. The surveillance isn't used for "just national security or intelligence gathering."

The government has long been suspected of discovering and stockpiling flaws in commercial code to gather information for potential use in cyber warfare, although the government has denied doing so.

If alerted to the existence of the vulnerabilities, software companies could quickly create a security patch. However, by not alerting developers, government agencies leave the vulnerabilities open for their own covert access -- and potentially for any malefactors capable of exploiting the flaws. That means the government must choose between protecting its surveillance access and protecting U.S. software against hacking, which can have "far-reaching consequences for both information security and user privacy," according to EFF's FOIA request.

The less-redacted document also discloses the government's policy for deciding what to do when a vulnerability is discovered. NSA is supposed to report the vulnerability to the company unless there is "a clear national security or law enforcement" reason not to. The decision about whether and what to publicize is solely at the agencies' discretion.

Furthermore, although the process was finalized in 2010, it was not effectively implemented, which led to a 2013 presidential review board's recommendation "to prioritize disclosure over offensive hacking."

The remaining redacted information likely includes which agencies have been involved in discussions about zero-day disclosures, according to EFF. The government is still withholding that information in the name of national security. EFF has a February court date to contest that claim.

Wall Street Journal
U.S. Tech Firms Take Fight Over Encryption to Davos
Thursday, 21 January 2016
Byline: Sam Schechner

Davos - Tensions are rising between governments and big U.S. technology companies over widening surveillance demands, part of a broader debate over how to reconcile online privacy with the fight against terrorism.
The battle will surface this week at the World Economic Forum, after a year in which terrorist groups including Islamic State killed hundreds in attacks around the world -- in some cases, officials say, using popular online tools to recruit followers and communicate.

Governments, particularly in Europe, want U.S. tech firms to turn over more information to them directly. Law-enforcement and intelligence officials say firms should build ways to turn over conversations into encrypted chat programs like Facebook Inc.'s WhatsApp.

Tech firms respond that weakening encryption could damage security on the Internet, and say new laws demanding access would put them in an impossible position.

"You could be placed in a situation where you have to decide what law to break," said Brad Smith, Microsoft Corp.'s chief legal officer, who is among the executives debating surveillance at Davos. "It isn't a comfortable place to be."

Countries usually can demand information about people only within their borders. But many of the biggest online services are based -- and store their data -- in the U.S., raising questions of jurisdiction.

Since 2013, when former U.S. NationalSecurity Agency contractor Edward Snowden leaked documents alleging widespread government snooping by the U.S. and allied countries, American tech companies have become vocal opponents of surveillance policies that could scare away privacy-conscious users.

Some firms have started encrypting mobile phones by default, often in ways that mean the firms don't have keys to decrypt them.

Now, amid evidence that plotters in the Nov. 13 attacks in Paris had at least downloaded encrypted chat applications, law- enforcement authorities have renewed calls for firms to re-engineer those programs to allow them to be decrypted. They contend investigations are being thwarted because of encryption.

Telecommunications executives, which have had to contend with surveillance requests for some time, say the decision should be left to governments. "I don't think it is Silicon Valley's decision to make about whether encryption is the right thing to do," AT&T Chief Executive Randall Stephenson said Wednesday.

Silicon Valley companies are lobbying officials in Davos. They contend that changing their architecture to thwart encryption would open their systems to hackers -- and not stop criminals from building their own end-to-end encryption systems anyway.

"You can do what you want from a policy perspective, but you can't stop mathematics," said Javier Aguera, chief scientist of Silent Circle, which offers encrypted communication apps and phones.

American tech firms say they already cooperate with authorities outside the U.S., but that their hands are tied by U.S. law.

In general, they will turn over only limited personal information about users to certain U.S.-allied countries, executives say. They direct European authorities to channel more-detailed requests to the U.S. government through bilateral treaties in a process that can take months.

Some other requests, like requests for information about devices, can go directly through local authorities because they are often about device thefts or taxes, Apple says.

In Davos, several executives said they are pushing for governments to adopt a new system to expedite cross- border requests. Such a system, which would require new treaties and eventually could entail a new multilateral data-sharing accord, would aim to avoid legal conflicts like that posed by a proposed U.K. law that would require tech firms to turn over data directly to U.K. authorities.

"The answer is an interlocking legal system between countries," said one tech executive. "There are legitimate surveillance needs here."

CBC.CA
Crimes involving technology are on the rise like never before: police
Friday, 22 January 2016

Sudbury - Sudbury police say they're struggling to keep up with cybercrime in the city -- something the chief says all police forces in the world are having difficulty with.
Cybercrime isn't just computer hacking anymore, Paul Pedersen said. The majority of the cybercrime police see now are things like trafficking, theft, and harassment -- all done with the use of technology.

Just a few years ago they were seizing desktop computers, but they're now having to solve crimes through people's online profiles and smart phones.

"We've got stalking -- which everybody can understand. But we now have harassment coming in the form of texts, in the form of email messages," Pedersen said.

"And where that complicates things for us is the ability to pull that information off of computers, store that data, and then disclose that data."

Police report that one-to-two per cent of all cybercrime in Canada is being reported -- and that means it's harder for them to know what they're up against.

"We keep talking about cybercrime as an emerging crime," Pedersen continued.

"But the reality is it's alive and well in all of our communities and certainly here in Sudbury."

Greater Sudbury Police Detective Sergeant Blair Ramsay told CBC News the growth of cybercrime is "the same as everywhere else ... it's growing. It's involved in a lot of crimes."

"We've increased our forensic analysts from two to three," he continued. The team involves two investigators and a victim identification officer.

How is an unknown victim identified from a photo?

"We dig into the image. Work with Adobe. Look at the background of the image, look for clues," Ramsay said.

"You'd be surprised by what you can find."

Common cyber crimes involve identity theft, criminal harassment, threats, child exploitation and drug dealing.

And scammers.

"We have had some cases of people reporting they have been extorted for money," Ramsay said, noting that people on dating websites are being asked to send "compromising" photos of themselves, only to be later blackmailed.

What can people do to protect themselves?

Ramsay said the Canadian Anti-Fraud Centre has a lot of good safety tips, which can be found here.

"If you think you're being targeted for an online scam, search it [online]," he said.

"If you think you're targeted, generally somebody else has too, and you'll see a lot of results."

Ramsay said tips to keep children safe online can be found at cybertip.ca.

People can also contact local police for more information.

The Hill
Security researcher: Ukraine power grid facing new wave of cyberattacks
Friday, 22 January 2016
Byline: Katie Bo Williams

Washington - Ukrainian power plants are still facing an onslaught of cyberattacks in the wake of a malware-caused blackout in December, according to a U.S. security firm.
"[On January 19th], we discovered a new wave of these attacks, where a number of electricity distribution companies in Ukraine were targeted again following the power outages in December," malware researcher Robert Lipovsky wrote in a post on the blog We Live Security.

But the kind of malware used in this latest wave of attacks is not the same code that left 80,000 people in the western regions of Ukraine without power last month, Lipovsky notes.

"What's particularly interesting is that the malware that was used this time is not BlackEnergy, which poses further questions about the perpetrators behind the ongoing operation," he wrote.

"The malware is based on a freely-available open-source backdoor -- something no one would expect from an alleged state-sponsored malware operator."

The incident in December, believed to be the first time a blackout was caused by a cyberattack, has been widely attributed to Russia.

The Ukrainian security service, SBU, was swift to blame Russia for planting malware to cause the blackout. Relations between the two nations have been in a steep decline since Russia annexed Crimea last year and began supporting pro-Russian separatists in Ukraine.

"We found that the [malware] came from Russia," SBU said. "It was an attempt to interfere in the system. But it was discovered and prevented."

The U.S.'s Industrial Control Systems Cyber Emergency Response Team is assisting Ukraine in investigating the blackout, but it has neither confirmed that the malware was the principle culprit behind the blackout nor attributed the attack to Russia.

The team "can confirm that a BlackEnergy 3 variant was present in the system," but "based on the technical artifacts, we cannot confirm a causal link between the power outage with the presence of the malware," the agency said earlier this month.

Lipovsky warns that the latest wave of attacks, far from confirming Russia as the culprit, "suggests that the possibility of false flag operations should also be considered.

"We currently have no evidence that would indicate who is behind these cyberattacks and to attempt attribution by simple deduction based on the current political situation might bring us to the correct answer, or it might not," Lipovsky wrote.

The Economist
Of warrants and watchers
Friday, 22 January 2016

London - Spies need secrecy and the public wants privacy. So finding the right legal framework in which the intelligence and security agencies can do their work, including--when necessary--intruding into people's private lives, is inherently tricky.
Britain's laws on bugging and snooping are out of date. Written in a pre-internet era, they give sweeping powers to the home secretary to authorise the interception and collection of electronic information, and the planting of bugs (in spookspeak, "equipment interference"). Without a stronger legal basis, these powers could fall foul of European judges on human-rights and data-protection grounds.

Moreover, until the revelations by Edward Snowden, a fugitive American intelligence contractor now living in Moscow, most people had no idea of the reach of Britain's digital spy agency, the Government Communications Headquarters (GCHQ), and how close its ties are with America's National Security Agency. The Snowden revelations infuriated digital-privacy advocates and also alarmed the technology industry, which feels squeezed between government demands and its customers' expectations.

The draft bill on investigatory powers going through Parliament attempts to sort out this mess. It follows the failure two years ago of a previous bill, dubbed the "snoopers' charter", and the hurried passage of a stopgap bill that expires this summer. The bill is under scrutiny by a joint committee of peers and MPs, which will report on February 11th.

Arguments rage over both form and content. Critics say the consultation is too hurried for one of the most important pieces of legislation in recent years. They object to the vagueness of some of the language (including new bits of jargon such as "internet connection records", which could mean the complete history of somebody's activity on the internet). The definition of these terms, and of such words as "urgent", "necessary" and "proportionate", will be contained in codes of practice, yet to be published.

For some, the fact that GCHQ has long had the capabilities it now avows is no reason to accept them. The bulk collection of information, they say, breaches privacy. Overly zealous spooks might link databases, and trawl them looking for patterns, drawing conclusions purely on the basis of inference, with no redress for those concerned. The data could be passed to (or pinched by) other countries, notably America, which could then decide, say, to put innocent people on no- fly lists. British Muslims already complain of costly, humiliating and unexplained last-minute blocks on trips to America, apparently based on their behaviour on the internet. Warehouses of sensitive data are magnets for criminals and other malefactors.

Critics of the bill also worry about a conflict of laws, under which Britain might oblige them to hand over data about their clients even when another country expressly prohibits this. Big technology companies such as Google, Facebook and Apple have written to the parliamentary committee to highlight this danger, though they declined to send their bosses to give evidence in person.

Some of this is posturing. The bill does not mandate the creation of a central database of everybody's internet history. Nor, contrary to some claims, will it force technology companies to install back doors in their encryption software to meet requests from GCHQ. Most supposedly encrypted products are already transparent to their providers: it is only by analysing its users' e-mails and browsing activity, for example, that Google is able to sell advertisements tailored to their tastes.

The law authorises GCHQ to ask for help. But when it comes across genuinely uncrackable encryption ("end-to- end", in industry jargon), it has other options, such as planting software on the device concerned. The tech companies, say cynics, are pretending to show how fiercely they resist government requests, while remaining happy to co-operate in private.

The purported conflict of laws is somewhat overblown as well. GCHQ will not force a company to break other countries' laws (risking an embarrassing public spat). The bigger worry for the government is how to protect the agency's intelligence capabilities from judges in Luxembourg and Strasbourg, whose view of espionage is rooted not in the British tradition of royal prerogative and empire, but in continental memories of totalitarianism.

For this reason the bill introduces a new idea. The home secretary's warrants will be reviewed by judges, who will check them for lawfulness and reasonableness. The creation of these commissioners was recommended in a report last year by David Anderson, a lawyer who is the independent scrutineer of Britain's anti-terrorist legislation. The spooks have no objection. Their activities are already scrutinised retrospectively by commissioners. They would also like their warrants to have more legal force in foreign eyes.

The committee is now debating the commissioners' hiring, firing and remit. It is also mulling evidence from lawyers and media-freedom campaigners. Communications between lawyers and their clients enjoy almost bulletproof legal protection: spies too should be told explicitly to steer clear of them. Journalists fret that sources (especially whistle-blowers) may have insufficient protection.

Another issue is a provision in the bill requiring "communication service providers" (ie, internet and telecoms firms) to store customers' internet records. It is unclear what this will mean in practice, how intrusive it will be, what it will cost and whether, since people get on the internet in many different ways, it can even work.

The biggest divide is not over the technicalities of intelligence oversight, but in attitudes to what spies do. Some believe the agencies to be overmighty, beguiling politicians with tales of derring-do and lobbying zealously for their cause in the media. Such worries are not groundless. Parliament's intelligence and security committee was surprised and annoyed by a drooling series of articles that resulted after GCHQ gave the Times unprecedented access to its headquarters in Cheltenham.

Yet nobody has evidence that GCHQ acts unlawfully or menacingly under the existing system. Most Britons--and most politicians--think the spooks do a good job and, beset by fears of terrorism, crime, child abuse and foreign spies, want a legal structure that lets them keep at it.

The Register (UK)
GCHQ spies quashed this phone encryption because it was too good against snoopers
Friday, 22 January 2016
Byline: Kieren McCarthy

London - The researcher who discovered that the UK government's phone encryption standard has a huge backdoor installed has made another discovery: GCHQ's rejection of a better encryption standard because it didn't allow for undetectable spying.
Dr Steven Murdoch has updated his original post on the MIKEY-SAKKE standard, developed by UK listening post GCHQ, to include a document from the 3GPP standardization group that was responsible for the 3G mobile phone standard and which also developed the 4G and LTE standards (i.e., what your phone currently uses).

That document stems from a meeting back in 2010 and outlines how a representative from the National Technical Assistance Centre (NTAC) - GCHQ's decryption and data analysis arm - worked to reject the MIKEY-IBAKE standard because it could produce a slight delay in people's phone calls when they were being intercepted.

"Due to the timing and interaction required to perform the man-in-the-middle attack during call setup, there will be additional latency in call setup," it reads. "This will be especially pronounced when large numbers of surveillance subjects are active in one region or one switch."

It goes on to note that the IBAKE standard would mean if an individual's connection was tapped, it could interfere with other authentication efforts, i.e., someone might notice they were under surveillance. And it noted that the standard would make it difficult to go back retroactively and listen to past conversations.

Jigsaw pieces

Although the document is not new - it was published on the whistleblower Cryptome website back in 2014 - its relevance has only just come to light thanks to the UK government's efforts to push the MIKEY-SAKKE standard for the latest end-to-end phone encryption products.

That effort is not limited to government departments: it is also being marketed to the broader commercial world through a product spec it has called Secure Chorus by highlighting its "government-grade security." It has also set itself up as an evaluator of other products, one example being Cryptify Call, available for iOS and Android.

MIKEY-SAKKE is mentioned possibly for the first time in the 2010 rejection of the IBAKE approach. The document notes: "In light of these requirements, UK government has developed a similar scheme, MIKEY-SAKKE, which supports 3GPP SA3 LI requirements and has additional benefits such as low latency."

That standard that the UK government specifically developed to allow for full and unnoticeable surveillance is the same one that six years later it is now trying to push into the expanding commercial market for more secure phone calls. It is notable that it makes no mention of the ability to invisibly intercept calls in its description of the protocol.

In short: the security services are trying to get people to hardwire the same standards that make it possible to intercept existing phone calls into products that are specifically designed to avoid that exact scenario.

Well, you can't blame them for trying.

Fox News
Clinton emails so secret some lawmakers can't read them
Thursday, 21 January 2016
Byline: Catherine Herridge

Washington - Some of Hillary Clinton's emails on her private server contained information so secret that senior lawmakers who oversee the State Department cannot read them without fulfilling additional security requirements, Fox News has learned.
The emails in question, as Fox News first reported earlier this week, contained intelligence classified at a level beyond "top secret." Because of this designation, not all the lawmakers on key committees reviewing the case have high enough clearances.

A source with knowledge of the intelligence review told Fox News that senior members of the Senate Foreign Relations Committee, despite having high-level clearances, are among those not authorized to read the intelligence from so-called "special access programs" without taking additional security steps -- like signing new non-disclosure agreements.

These programs are highly restricted to protect intelligence community sources and methods.

As Fox News previously reported, a Jan. 14 letter from Intelligence Community Inspector General I. Charles McCullough III to senior lawmakers said an intelligence review identified "several dozen" additional classified emails -- including specific intelligence from "special access programs" (SAP).

That indicates a level of classification beyond even "top secret," the label previously given to two emails found on her server, and brings even more scrutiny to the Democratic presidential candidate's handling of the government's closely held secrets.

Fox News is told that the reviewers who handled the SAP intelligence identified in Clinton's emails had to sign additional non-disclosure agreements even though they already have the highest level of clearance -- known as TS/SCI or Top Secret/Sensitive Compartmented information. This detail was first reported by NBC News.

This alone seems to undercut the former secretary of state's and other officials' claims that the material is "innocuous."

In an interview with NPR, Clinton claimed the latest IG finding doesn't change anything and suggested it was politically motivated.

"This seems to me to be, you know, another effort to inject this into the campaign, it's another leak," she said. "I'm just going to leave it up to the professionals at the Justice Department because nothing that this says changes the fact that I never sent or received material marked classified."

Despite Clinton's claims, it is the content that is classified; the markings on the documents do not affect that.

A former Justice Department official said there is another problem -- warnings from State Department IT employees and others that she should be using a government account.

"If you have a situation where someone was knowingly violating the law and that they knew that what they were doing was prohibited by federal law because other people were saying, you're violating the law, knock it off, and they disregarded that advice and they went ahead, that's a very difficult case to defend," Thomas Dupree said.

Times of Israel
Defense against Cyber Pirates
Friday, 22 January 2016

Jerusalem - Sabotage by cyber-attack is the latest threat to governments and industries all over the world, and the shipping industry is no exception. Andrew Ginter, VP of Industrial Security at Waterfall Security Solutions, in a conversation about the increasing threat of cyber attacks at sea, and how ship-owners can protect their vessels
Picture the scene. The ship has run aground in shallow water. It shouldn't have been anywhere near the sandbank it's resting on, but the crew were unable to control it. It's now listing badly and valuable cargo is falling overboard. The mystified captain is muttering something. The camera zooms in on him and we listen. "We must have been hacked," he's saying. "We must have been hacked." If this were the opening scene of the next James Bond film, most of us would think it a perfectly credible incident - and we'd be right, because it is.

Sabotage by cyber-attack is the latest threat to governments and industries all over the world, and the shipping industry is no exception. We all have enemies, be they political, economic or simply plain criminal, and the more equipment we connect to one network or another, the more vulnerable we become.

Ships today are completely computerized. In our continued attempts to reduce costs by increasing efficiency, more and more functions are being automated or remotely controlled, and gigabytes of data are collected every day to help us monitor the performance of our equipment. Navigation is heavily automated. Equipment usage is monitored to reduce costs through predictive maintenance. Everything from vessel position, speed and heading to fuel usage, hull stress and engine condition are monitored automatically for use in advanced optimization and prediction algorithms. Everything is connected to the network, so we can see what's going on and adjust it for optimum performance. Even the containers can be equipped with communications technology now, to give us 24/7 feedback on their comfort levels, from temperature to humidity to good vibrations. Systems can be fitted which remotely control and adjust the temperature of refrigerated containers.

The problem is, once we introduce connectivity into our operations to make it possible to interact remotely with a motion sensor in a container or, more importantly, a navigation device in a ship's control network, we make it possible for someone else to interact with our equipment, too.

"The trade off between increased efficiency and increased vulnerability is one that businesses in many industries are failing to take into account," says Andrew Ginter, VP industrial security, Waterfall Security Solutions. "We see the benefits more clearly than we see the risks."

One barrier to understanding is visibility. The most visible attacks are common viruses, malware and attacks by insiders. There's a new generation of attackers out there now, though, who work hard at invisibility. Most victims have no idea they have been compromised until months after the fact, if ever.

A more subtle barrier is the difference between espionage and sabotage. Over the last five years most of the high- profile cyber attacks were espionage attacks - stealing information. The big risk to shipping is not espionage, however, but cyber sabotage.

"Most security practitioners are much more aware of espionage risks than sabotage risks," says Ginter. "As a result we install security systems that are reasonably good at preventing the theft of data, but do little to prevent equipment damage, or worse. The prevention of cyber sabotage needs a different approach," he stresses.

"Common wisdom has it that a control system can be secured with a firewall and a bit of encryption," continues Ginter. Unfortunately, there is more wishful thinking than wisdom here. "Firewalls forward messages between networks, and they do what they can to identify and eliminate attack messages, but no firewall is or can ever be perfect. All firewalls forward some attack messages into protected networks."

In practice, all software can be hacked, Ginter explains, because all software has bugs, and many bugs are security vulnerabilities. "I wrote software for 25 years," he says. "I did not deliberately put bugs into every piece of software I wrote, but every piece of software I wrote still had bugs."

This is why intrusion detection is fundamental to defending against cyber espionage. If every message through the firewall could contain an attack, and all software can be hacked, then intrusion detection is critical. We need to assume we will be compromised, we need to search out those compromised computers, and we need to erase those computers and restore them from clean backups.

This approach fails us in the world of cyber sabotage, however. We cannot take a grounded ship and "restore it from backup." Fundamentally, intrusion detection takes time; recent studies show that it takes months to find the average intrusion. For all of that time, an invisible intruder has remote control of our vessel: falsifying data and mis-operating equipment. This is unacceptable.

While reports of stolen bank details and credit card numbers are becoming commonplace on our TV news, we don't hear so much about cyber attacks on infrastructure or industrial assets, but this doesn't mean they're not happening. If we were a multinational industry giant with customers all over the world, how likely would we be to admit that our security had been breached if we were not legally bound to disclose breaches?

Worse, attackers with no desire to be discovered are likely to disguise their interventions to look like random system failures, so their victims never know they were attacked. "This is why we don't hear about attacks," confirms Ginter, "but if you look at surveys, 70 to 80 per cent of people say they have been compromised in the last 12 months and an even greater number expect to be compromised next year."

Where have these threats come from? Why are attackers now starting to target infrastructure rather than data? There is an element of 'because they can' in there, because our headlong rush towards connectivity has made it possible for them to attack us, but the big question is about motive. What do they have to gain? There will always be terrorists with political motives and pirates with ransom demands, but the new breed of cyber attacker is more likely to be looking for an economic advantage over a rival, or to make a killing on the stock market. There has to be a profit motive.

It is generally accepted today that organised crime is behind the most visible attacks on home computers and corporate systems, because they have proven paths to profit from such attacks. "The average credit card number is worth 25 cents on the black market," says Ginter. "The average bank account number and password is worth between a dollar and a hundred dollars, depending on how much money is in the account. There's a whole industry for laundering the money, and more recently, a whole industry has been developed around stealing corporate secrets. The question that people are asking now is, how soon will an industry be developed around simulating random failures on ships or at other industrial sites to manipulate markets, or for other profit motives? Many are also asking, is this happening already, silently?"

Ginter has an example from close to home that illustrates the potential threat very well. "I live in Alberta in Canada," he says. "A pipeline that used to send gasoline from east to west across the country was recently reversed and now sends crude oil back east for refining. Alberta now has local refiners that can provide us with gasoline. But in the middle of last summer, at the time of peak gasoline consumption, the biggest refinery in the region mysteriously went down. In spite of the worldwide collapse in oil prices, we were paying through the nose for gasoline.

"The refinery didn't tell us why it went down," he continues. "It didn't have to. News reports talked about some kind of equipment failure. But think about it - if someone broke into the refinery's network and caused some equipment to fail without leaving obvious traces of cyber attack behind, and then went long on gasoline futures in our geography and made a killing on the commodities market, would anybody notice? These guys are very good at what they do. This kind of opportunity is something that if

organised crime isn't doing it today, we're certainly worried about it happening in the future. These guys are professionals. They're going to cover their tracks.

"So the question is, who profits when a ship is delayed by mechanical problems or computer problems with its navigational systems? Everything on the ship is delayed, so what's on the vessel? Is it something that somebody can profit by? Can they go short on the shipping company or can they go short on the company that owns the goods? If goods are delayed it may affect someone's profits for the quarter. This is the kind of thing that people are worried about. Where there's opportunity, somebody is going to take advantage."

Somebody took advantage in 2013 in an attack on the US retailer, Target, which resulted in costly court proceedings over the insurance claim, and incalculable damage to the company's reputation. How did they do that? "This was a data theft attack, but the attackers used the same kind vulnerability that we see with control systems on ships and in every industry," says Ginter. "They got into Target through a vendor. The attackers did not come after Target. They were just poking around, systematically breaking into one business after another to see what profit they could make. Then they broke into a vendor that provided Target with refrigeration and HVAC hardware and services. They stole remote access credentials from the refrigeration vendor and used them to log into Target. They didn't have to break through the Target firewall - they just logged in like any other user. How many vendors have remote access to our ships?"

Security awareness and preparedness vary greatly according to geography, says Ginter. "In North America there are regulations in the power sector. If the bad guys want to target the North American power sector they're going to come up against NERC CIP [the North American Electric Reliability Corporation's Critical Infrastructure Protection standards]. Now, NERC CIP is far from perfect, but it is much better than nothing. In much of the rest of the world, there is nothing."

If you get your regulations right in the first place, compliance will bring best practices into play. The question though, is how can best practices become standard practices for industries that are not regulated? "I don't see any rules emerging for the shipping industry," says Ginter. "There's no body that can enforce rules like that."

There have already been attempted attacks on the US power grid by the terrorist organisation ISIS, though these initial attacks were described by authorities as "low capability" attacks. Attack capabilities can be purchased, however, and ISIS has money. "These simple attacks are going to become more sophisticated," says Ginter. "All it takes is a little money for ISIS to buy world class attack capabilities to come after the grid, and they have plenty of money."

While the next target depends on the specific motivation of the next cyber attacker, it would be a mistake to base our security defence on the likelihood of an attack. What's unlikely today may be more likely tomorrow, but tomorrow may be too late to prevent the attack.

"Prudent security practitioners defend against well-known attack capabilities," says Ginter. "They do not defend against the motive of the moment. They do not look around and say 'how many ships were stranded last year in the middle of the ocean like this?' Motives can change in a heartbeat. Somebody can suddenly get a bee in their bonnet and decide to come after us. Capabilities evolve much more slowly. So industrial sites today are looking at the capabilities in the threat environment and defending against them before someone develops a motive to use those capabilities against their sites."

If our organization is lucky enough not to have been targeted by a cyber attacker yet, what approach to security are we going to take? Are we going to look at the statistics of ships being attacked in this way and respond according to our perception of likelihood, or are we going to put protections in place before serious harm is done?

For those looking for credible sabotage- oriented protection, there are solutions available. Waterfall Security Solutions is a cyber security specialist that produces hardware-enforced security products, focused on preventing the cyber sabotage of ICS (industrial control system) networks. The hardware part of the solution is called a unidirectional gateway.

"We have a family of products but our flagship product is the unidirectional gateway," says Ginter. "The gateways enable safe network integration. The gateways let businesses monitor their control system equipment, but make it physically impossible to send any attack back in to those critical networks.

"We claim 100 per cent protection against network attacks coming from external networks," he continues. "While there is no technology that can prevent absolutely all attacks, these silent, online, network-based attacks are the workhorse of cyber sabotage, and are the specific risk that comes with increased network connectivity. Our gateways eliminate that specific threat vector entirely."

When a unidirectional gateway becomes the only connection between a more trusted network and a less trusted network, he explains, data travels only one way, so nothing gets back in to the ICS network. Waterfall makes the data available for anyone who needs it, by replicating industrial databases and devices. "Anyone who wants the real-time data can ask the replicas and get the same answer they would have had by asking the live systems," Ginter explains. "They get the same answer from the replica as the control system equipment would have given them, without ever sending a message to the control system and putting that equipment at risk."

Waterfall Security Solutions produces a family of products that are based on or complement its unidirectional gateways. The Waterfall FLIP is a kind of gateway that can reverse orientation on a schedule, to provide continuous monitoring and occasional batch updates of shipboard systems, such as security updates or weather forecasts. Inbound/outbound gateways can provide continuous updates of onboard systems through separate, independent replications, without ever introducing the kinds of attack paths that always come with firewalls. Application data control add-ons apply fine-grained policy-based controls to data in motion between networks. All of these products frustrate modern, silent, remote-control cyber sabotage attack capabilities, as well as a host of older, more mundane attacks.

The 2015 "Safety and Shipping Review" by Allianz identified cyber sabotage attacks on shipping as "a major concern." Cyber sabotage attack capabilities have become much more sophisticated in the course of the last decade. Attackers use powerful software tools, and like all software, attack tools become more and more capable as new versions are released. Basic security hygiene, such as firewalls, anti-virus systems, security updates, encryption and long passwords, provide little protection against modern attacks by criminals or 'hacktivists'.

"In the shipping industry, we need to take inspiration from control system cyber security standards and regulations in other industries," says Ginter. The French ANSSI standards for critical infrastructure protection prohibit firewalls at the boundaries of the most important control system networks, permitting only unidirectional gateways. The North American NERC CIP standards provide relief from one third of the security regulations when unidirectional gateways are used instead of firewalls at large power plants. The ISA, IEC, NIST and many other standards all position unidirectional gateways as stronger than firewall protections for control system security programs.

"We have a window of opportunity now, to protect the control systems and navigation systems on our vessels, before we start suffering very serious losses," concludes Ginter. "Increased automation and connectivity brings increased opportunities and profits, but only if we address the risks."

The Economist
Snoopers and scrutiny
Thursday, 21 January 2016
Byline: Editorial Board

Editorial - Few balances are harder to strike than those involved in running a spy agency. After a terrorist attack, voters demand action and politicians respond by granting their spies greater powers to bug and snoop, as with America's Patriot Act in 2001 and the wide-ranging surveillance law passed after the attacks in France last year. Yet these very powers can, if abused, distort the political system, chill freedom of expression and tilt the scales of justice. When the full extent of clandestine activities come to light, as with Edward Snowden's revelations about America's National Security Agency, many feel queasy and demand that the spooks are reined in again.
So a lot is riding on Britain's attempt to update the law governing the domestic activities of its spy agencies. The draft bill will make explicit how the electronic-intelligence agency, GCHQ, may (with a warrant) plant bugs on computers and other devices, collect and analyse bulk information (such as mobile-phone activity and web-browsing records) and read private messages. Get the details right, and Britain can provide a model of how to balance security and freedom; get them wrong, and centuries of freedom might shrivel.

The bill's biggest success is its self-restraint. It does not require firms to weaken the encryption they sell to customers, as politicians in several countries, including Britain, would like. If people want security on

the internet, they have no alternative to strong encryption. The agencies have other means of collecting data, including bugging phones and computers.

The draft bill is also right to require companies to retain, at least for a time, data about mobile-phone and internet activity that may, subject to a warrant, be of use to future investigations. Intelligence agencies need to be able to look back at the history of a suspected terrorist's contacts and movements.

Elsewhere, however, the bill could be better. It rightly strengthens GCHQ's powers to pursue terrorists, gangsters and foreign spies. And it offers extra safeguards: new judicial commissioners will review warrants which, as now, will be issued by the home secretary. Politicians should have ultimate responsibility; if things go wrong, they carry the can. But the bill will work best if it is backed by a consensus. For that reason it needs to reassure those who fear that politicians may abuse their powers. Instead of holding their posts at the prime minister's behest, the commissioners should be appointed as judges are and their dismissal should require a vote in Parliament. To avoid "capture", they should serve a single fixed term.

In addition, the proposed system merely requires the commissioners to check that a warrant has been issued lawfully and reasonably--broadly the same standard applicable to judicial review of other government decisions. But the extra secrecy with which intelligence agencies operate means that is not enough. The commissioners need a reserve power to weigh warrants on their merits. Also missing is explicit protection for lawyers' communications with their clients.

Just as important as the nuts and bolts of the new law is its implementation. GCHQ's demands may be legal, but if they are too costly or intrusive, companies dealing with technology and data will simply move abroad. For all these reasons, other countries should watch Britain closely.

Wall Street Journal
NSA Chief Says U.S. at 'Tipping Point' on Cyberweapons
Thursday, 21 January 2016
Byline: Damian Paletta

Washington - The U.S. military has spent five years developing advanced cyberweapon and digital capabilities and is likely to deploy them more publicly soon, the head of the Pentagon's U.S. Cyber Command said Thursday.
Adm. Mike Rogers, who is also director of the National Security Agency, said U.S. policy makers have largely agreed on rules of engagement for when cyberweapons can be used for defense.

There is still an open discussion, however, about when cyberweapons should be used for "offense," such as carrying out attacks against a group or foreign country.

"You can tell we are at the tipping point now," Adm. Rogers said. "The capacity and the capability are starting to come online [and] really starting to pay off in some really tangible capabilities that you will start to see us apply in a broader and broader way."

Still, Adm. Rogers stopped short of specifying how exactly these cyberpowers could be deployed in coming months.

Despite a series of high-profile cyberattacks in the past two years, including a large-scale breach at Sony Pictures Entertainment Inc. in late 2014 and the theft of millions of records from the U.S. Office of Personnel Management in 2015, Adm. Rogers suggested many Americans have become complacent, since they don't see the rise of cyber armies and cybercriminals affecting their daily lives.

That could change fast, he said, if a cyberattack achieves large-scale destruction, particularly in a fashion resembling a more traditional weapon. Analysts have said these sorts of acts could including attacking a country's electrical grid or knocking a nation's financial system offline.

"I'm watching capability when I go, 'Wow, if the intent were to change, we'd have some real challenges here,' and intent can change really quickly," he said. "I would urge us not to draw the conclusion that there is nothing here we really need to worry about. I would argue it's going to get worse before it gets better."

Adm. Rogers, who has led the NSA and Cyber Command for two years, was brought in to stabilize the agency after a furor over the far-reaching surveillance program disclosed by former contractor Edward Snowden. The NSA has seen some of its powers clipped, most notably when Congress last year banned bulk collection of telephone records.

Adm. Rogers has said the agency needs to do more to restore public confidence, and he has been adamant that the government needs to develop specific rules about the emerging digital battlefield.

Following the OPM breach, which some U.S. officials attributed to Chinese hackers, many lawmakers have said the White House and Pentagon need to clarify rules of engagement and make them public. These could include specific punishments and retaliatory actions, as a way to deter future attacks.

Adm. Rogers said policy makers have been working to develop "the same kind of standards" for responding to cyberattacks that they use for other warfare.

The NSA director also said the agency will launch a reorganization this year to better mesh its two tasks--digital spying and data collection on the one hand and protecting information on the other.

"We have got to integrate much more," he said. "This traditional approach we had...built walls of granite between them."

The Intercept
NSA Chief Stakes Out Pro-Encryption Position, in Contrast to FBI
Thursday, 21 January 2016
Byline: Jenna McLaughlin

Washington - National Security Agency Director Adm. Mike Rogers said Thursday that "encryption is foundational to the future," and arguing about it is a waste of time.
Speaking to the Atlantic Council, a Washington, D.C., think tank, Rogers stressed that the cybersecurity battles the U.S. is destined to fight call for more widespread use of encryption, not less. "What you saw at OPM, you're going to see a whole lot more of," he said, referring to the massive hack of the Office of Personnel Management involving the personal data about 20 million people who have gotten background checks.

"So spending time arguing about 'hey, encryption is bad and we ought to do away with it' ... that's a waste of time to me," he said, shaking his head.

"So what we've got to ask ourselves is, with that foundation, what's the best way for us to deal with it? And how do we meet those very legitimate concerns from multiple perspectives?"

Other government officials -- most notably FBI Director James Comey -- have been crusading for a way that law enforcement can get access to encrypted data.

But technologists pretty much universally agree that creating some sort of special third-party access would weaken encryption to the point that it would threaten every internet transaction we make, from online banking to filling out our health records to emailing our friends and significant others. A hole in encryption for special FBI access would be a hole that criminals could sneak through, too.

While there's been a lot of talk about giving up some privacy for security, Rogers said both are paramount.

"Concerns about privacy have never been higher. Trying to get all those things right, to realize that -- it isn't about one or the other," he said. He does not think that "security is the imperative and that ought to drive everything." Nor should privacy, he continued. "We've got to meet these two imperatives. We've got some challenging times ahead of us, folks."

Comey, who formerly advocated for a way to get law enforcement access without weakening encryption, recently switched tactics. Now he is pressuring companies to change their business models and simply not offer true end-to-end encryption to their customers.

The White House has decided not to pursue legislation to outlaw unbreakable end-to-end encryption, following pressure from privacy advocates and scientists. But the intelligence community's top lawyer,

Bob Litt, privately advised the administration that a major terrorist attack could be an opportune moment to do so.

And the White House has not issued a statement in defense of encryption, to the frustration of Apple CEO Tim Cook, among others.

Meanwhile, Sens. Richard Burr, R-N.C., and Dianne Feinstein, D- Calif., are reportedly planning their own proposed legislation to require law enforcement access.

Rogers' comments could indicate a split on this issue between the intelligence community and domestic law enforcement.

The previous NSA director, Michael Hayden, said in January that he thinks Comey is on the wrong side of this debate. "I disagree with Jim Comey. I actually think end-to-end encryption is good for America," he said.

Hayden has also spoken about how U.S. intelligence agencies have figured out how to get the information they need without weakening encryption -- such as using metadata, which shows who is contacting whom. Another former NSA boss, Mike McConnell, has also spoken out against trying to install backdoors in encryption.

Left unsaid is the fact that the FBI and NSA have the ability to circumvent encryption and get to the content too -- by hacking. Hacking allows law enforcement to plant malicious code on someone's computer in order to gain access to the photos, messages, and text before they were ever encrypted in the first place, and after they've been decrypted. The NSA has an entire team of advanced hackers, possibly as many as 600, camped out at Fort Meade.

CBC.CA
Crimes involving technology are on the rise like never before: police
Friday, 22 January 2016

Sudbury - Sudbury police say they're struggling to keep up with cybercrime in the city -- something the chief says all police forces in the world are having difficulty with.
Cybercrime isn't just computer hacking anymore, Paul Pedersen said. The majority of the cybercrime police see now are things like trafficking, theft, and harassment -- all done with the use of technology.

Just a few years ago they were seizing desktop computers, but they're now having to solve crimes through people's online profiles and smart phones.

"We've got stalking -- which everybody can understand. But we now have harassment coming in the form of texts, in the form of email messages," Pedersen said.

"And where that complicates things for us is the ability to pull that information off of computers, store that data, and then disclose that data."

Police report that one-to-two per cent of all cybercrime in Canada is being reported -- and that means it's harder for them to know what they're up against.

"We keep talking about cybercrime as an emerging crime," Pedersen continued.

"But the reality is it's alive and well in all of our communities and certainly here in Sudbury."

Greater Sudbury Police Detective Sergeant Blair Ramsay told CBC News the growth of cybercrime is "the same as everywhere else ... it's growing. It's involved in a lot of crimes."

"We've increased our forensic analysts from two to three," he continued. The team involves two investigators and a victim identification officer.

How is an unknown victim identified from a photo?

"We dig into the image. Work with Adobe. Look at the background of the image, look for clues," Ramsay said.

"You'd be surprised by what you can find."

Common cyber crimes involve identity theft, criminal harassment, threats, child exploitation and drug dealing.

And scammers.

"We have had some cases of people reporting they have been extorted for money," Ramsay said, noting that people on dating websites are being asked to send "compromising" photos of themselves, only to be later blackmailed.

What can people do to protect themselves?

Ramsay said the Canadian Anti-Fraud Centre has a lot of good safety tips, which can be found here.

"If you think you're being targeted for an online scam, search it [online]," he said.

"If you think you're targeted, generally somebody else has too, and you'll see a lot of results."

Ramsay said tips to keep children safe online can be found at cybertip.ca.

People can also contact local police for more information.

The Hill
Security researcher: Ukraine power grid facing new wave of cyberattacks
Friday, 22 January 2016
Byline: Katie Bo Williams

Washington - Ukrainian power plants are still facing an onslaught of cyberattacks in the wake of a malware-caused blackout in December, according to a U.S. security firm.
"[On January 19th], we discovered a new wave of these attacks, where a number of electricity distribution companies in Ukraine were targeted again following the power outages in December," malware researcher Robert Lipovsky wrote in a post on the blog We Live Security.

But the kind of malware used in this latest wave of attacks is not the same code that left 80,000 people in the western regions of Ukraine without power last month, Lipovsky notes.

"What's particularly interesting is that the malware that was used this time is not BlackEnergy, which poses further questions about the perpetrators behind the ongoing operation," he wrote.

"The malware is based on a freely-available open-source backdoor -- something no one would expect from an alleged state-sponsored malware operator."

The incident in December, believed to be the first time a blackout was caused by a cyberattack, has been widely attributed to Russia.

The Ukrainian security service, SBU, was swift to blame Russia for planting malware to cause the blackout. Relations between the two nations have been in a steep decline since Russia annexed Crimea last year and began supporting pro-Russian separatists in Ukraine.

"We found that the [malware] came from Russia," SBU said. "It was an attempt to interfere in the system. But it was discovered and prevented."

The U.S.'s Industrial Control Systems Cyber Emergency Response Team is assisting Ukraine in investigating the blackout, but it has neither confirmed that the malware was the principle culprit behind the blackout nor attributed the attack to Russia.

The team "can confirm that a BlackEnergy 3 variant was present in the system," but "based on the technical artifacts, we cannot confirm a causal link between the power outage with the presence of the malware," the agency said earlier this month.

Lipovsky warns that the latest wave of attacks, far from confirming Russia as the culprit, "suggests that the possibility of false flag operations should also be considered.

"We currently have no evidence that would indicate who is behind these cyberattacks and to attempt attribution by simple deduction based on the current political situation might bring us to the correct answer, or it might not," Lipovsky wrote.

The Economist
Of warrants and watchers
Friday, 22 January 2016

London - Spies need secrecy and the public wants privacy. So finding the right legal framework in which the intelligence and security agencies can do their work, including--when necessary--intruding into people's private lives, is inherently tricky.
Britain's laws on bugging and snooping are out of date. Written in a pre-internet era, they give sweeping powers to the home secretary to authorise the interception and collection of electronic information, and the planting of bugs (in spookspeak, "equipment interference"). Without a stronger legal basis, these powers could fall foul of European judges on human-rights and data-protection grounds.

Moreover, until the revelations by Edward Snowden, a fugitive American intelligence contractor now living in Moscow, most people had no idea of the reach of Britain's digital spy agency, the Government Communications Headquarters (GCHQ), and how close its ties are with America's National Security Agency. The Snowden revelations infuriated digital-privacy advocates and also alarmed the technology industry, which feels squeezed between government demands and its customers' expectations.

The draft bill on investigatory powers going through Parliament attempts to sort out this mess. It follows the failure two years ago of a previous bill, dubbed the "snoopers' charter", and the hurried passage of a stopgap bill that expires this summer. The bill is under scrutiny by a joint committee of peers and MPs, which will report on February 11th.

Arguments rage over both form and content. Critics say the consultation is too hurried for one of the most important pieces of legislation in recent years. They object to the vagueness of some of the language (including new bits of jargon such as "internet connection records", which could mean the complete history of somebody's activity on the internet). The definition of these terms, and of such words as "urgent", "necessary" and "proportionate", will be contained in codes of practice, yet to be published.

For some, the fact that GCHQ has long had the capabilities it now avows is no reason to accept them. The bulk collection of information, they say, breaches privacy. Overly zealous spooks might link databases, and trawl them looking for patterns, drawing conclusions purely on the basis of inference, with no redress for those concerned. The data could be passed to (or pinched by) other countries, notably America, which could then decide, say, to put innocent people on no- fly lists. British Muslims already complain of costly, humiliating and unexplained last-minute blocks on trips to America, apparently based on their behaviour on the internet. Warehouses of sensitive data are magnets for criminals and other malefactors.

Critics of the bill also worry about a conflict of laws, under which Britain might oblige them to hand over data about their clients even when another country expressly prohibits this. Big technology companies such as Google, Facebook and Apple have written to the parliamentary committee to highlight this danger, though they declined to send their bosses to give evidence in person.

Some of this is posturing. The bill does not mandate the creation of a central database of everybody's internet history. Nor, contrary to some claims, will it force technology companies to install back doors in their encryption software to meet requests from GCHQ. Most supposedly encrypted products are already transparent to their providers: it is only by analysing its users' e-mails and browsing activity, for example, that Google is able to sell advertisements tailored to their tastes.

The law authorises GCHQ to ask for help. But when it comes across genuinely uncrackable encryption ("end-to- end", in industry jargon), it has other options, such as planting software on the device concerned. The tech companies, say cynics, are pretending to show how fiercely they resist government requests, while remaining happy to co-operate in private.

The purported conflict of laws is somewhat overblown as well. GCHQ will not force a company to break other countries' laws (risking an embarrassing public spat). The bigger worry for the government is how to protect the agency's intelligence capabilities from judges in Luxembourg and Strasbourg, whose view of espionage is rooted not in the British tradition of royal prerogative and empire, but in continental memories of totalitarianism.

For this reason the bill introduces a new idea. The home secretary's warrants will be reviewed by judges, who will check them for lawfulness and reasonableness. The creation of these commissioners was recommended in a report last year by David Anderson, a lawyer who is the independent scrutineer of Britain's anti-terrorist legislation. The spooks have no objection. Their activities are already scrutinised retrospectively by commissioners. They would also like their warrants to have more legal force in foreign eyes.

The committee is now debating the commissioners' hiring, firing and remit. It is also mulling evidence from lawyers and media-freedom campaigners. Communications between lawyers and their clients enjoy almost bulletproof legal protection: spies too should be told explicitly to steer clear of them. Journalists fret that sources (especially whistle-blowers) may have insufficient protection.

Another issue is a provision in the bill requiring "communication service providers" (ie, internet and telecoms firms) to store customers' internet records. It is unclear what this will mean in practice, how intrusive it will be, what it will cost and whether, since people get on the internet in many different ways, it can even work.

The biggest divide is not over the technicalities of intelligence oversight, but in attitudes to what spies do. Some believe the agencies to be overmighty, beguiling politicians with tales of derring-do and lobbying zealously for their cause in the media. Such worries are not groundless. Parliament's intelligence and security committee was surprised and annoyed by a drooling series of articles that resulted after GCHQ gave the Times unprecedented access to its headquarters in Cheltenham.

Yet nobody has evidence that GCHQ acts unlawfully or menacingly under the existing system. Most Britons--and most politicians--think the spooks do a good job and, beset by fears of terrorism, crime, child abuse and foreign spies, want a legal structure that lets them keep at it.

The Register (UK)
GCHQ spies quashed this phone encryption because it was too good against snoopers
Friday, 22 January 2016
Byline: Kieren McCarthy

London - The researcher who discovered that the UK government's phone encryption standard has a huge backdoor installed has made another discovery: GCHQ's rejection of a better encryption standard because it didn't allow for undetectable spying.
Dr Steven Murdoch has updated his original post on the MIKEY-SAKKE standard, developed by UK listening post GCHQ, to include a document from the 3GPP standardization group that was responsible for the 3G mobile phone standard and which also developed the 4G and LTE standards (i.e., what your phone currently uses).

That document stems from a meeting back in 2010 and outlines how a representative from the National Technical Assistance Centre (NTAC) - GCHQ's decryption and data analysis arm - worked to reject the MIKEY-IBAKE standard because it could produce a slight delay in people's phone calls when they were being intercepted.

"Due to the timing and interaction required to perform the man-in-the-middle attack during call setup, there will be additional latency in call setup," it reads. "This will be especially pronounced when large numbers of surveillance subjects are active in one region or one switch."

It goes on to note that the IBAKE standard would mean if an individual's connection was tapped, it could interfere with other authentication efforts, i.e., someone might notice they were under surveillance. And it noted that the standard would make it difficult to go back retroactively and listen to past conversations.

Jigsaw pieces

Although the document is not new - it was published on the whistleblower Cryptome website back in 2014 - its relevance has only just come to light thanks to the UK government's efforts to push the MIKEY-SAKKE standard for the latest end-to-end phone encryption products.

That effort is not limited to government departments: it is also being marketed to the broader commercial world through a product spec it has called Secure Chorus by highlighting its "government-grade security." It has also set itself up as an evaluator of other products, one example being Cryptify Call, available for iOS and Android.

MIKEY-SAKKE is mentioned possibly for the first time in the 2010 rejection of the IBAKE approach. The document notes: "In light of these requirements, UK government has developed a similar scheme, MIKEY-SAKKE, which supports 3GPP SA3 LI requirements and has additional benefits such as low latency."

That standard that the UK government specifically developed to allow for full and unnoticeable surveillance is the same one that six years later it is now trying to push into the expanding commercial market for more secure phone calls. It is notable that it makes no mention of the ability to invisibly intercept calls in its description of the protocol.

In short: the security services are trying to get people to hardwire the same standards that make it possible to intercept existing phone calls into products that are specifically designed to avoid that exact scenario.

Well, you can't blame them for trying.

Fox News
Clinton emails so secret some lawmakers can't read them
Thursday, 21 January 2016
Byline: Catherine Herridge

Washington - Some of Hillary Clinton's emails on her private server contained information so secret that senior lawmakers who oversee the State Department cannot read them without fulfilling additional security requirements, Fox News has learned.
The emails in question, as Fox News first reported earlier this week, contained intelligence classified at a level beyond "top secret." Because of this designation, not all the lawmakers on key committees reviewing the case have high enough clearances.

A source with knowledge of the intelligence review told Fox News that senior members of the Senate Foreign Relations Committee, despite having high-level clearances, are among those not authorized to read the intelligence from so-called "special access programs" without taking additional security steps -- like signing new non-disclosure agreements.

These programs are highly restricted to protect intelligence community sources and methods.

As Fox News previously reported, a Jan. 14 letter from Intelligence Community Inspector General I. Charles McCullough III to senior lawmakers said an intelligence review identified "several dozen" additional classified emails -- including specific intelligence from "special access programs" (SAP).

That indicates a level of classification beyond even "top secret," the label previously given to two emails found on her server, and brings even more scrutiny to the Democratic presidential candidate's handling of the government's closely held secrets.

Fox News is told that the reviewers who handled the SAP intelligence identified in Clinton's emails had to sign additional non-disclosure agreements even though they already have the highest level of clearance -- known as TS/SCI or Top Secret/Sensitive Compartmented information. This detail was first reported by NBC News.

This alone seems to undercut the former secretary of state's and other officials' claims that the material is "innocuous."

In an interview with NPR, Clinton claimed the latest IG finding doesn't change anything and suggested it was politically motivated.

"This seems to me to be, you know, another effort to inject this into the campaign, it's another leak," she said. "I'm just going to leave it up to the professionals at the Justice Department because nothing that this says changes the fact that I never sent or received material marked classified."

Despite Clinton's claims, it is the content that is classified; the markings on the documents do not affect that.

A former Justice Department official said there is another problem -- warnings from State Department IT employees and others that she should be using a government account.

"If you have a situation where someone was knowingly violating the law and that they knew that what they were doing was prohibited by federal law because other people were saying, you're violating the law, knock it off, and they disregarded that advice and they went ahead, that's a very difficult case to defend," Thomas Dupree said.

Times of Israel
Defense against Cyber Pirates
Friday, 22 January 2016

Jerusalem - Sabotage by cyber-attack is the latest threat to governments and industries all over the world, and the shipping industry is no exception. Andrew Ginter, VP of Industrial Security at Waterfall Security Solutions, in a conversation about the increasing threat of cyber attacks at sea, and how ship-owners can protect their vessels
Picture the scene. The ship has run aground in shallow water. It shouldn't have been anywhere near the sandbank it's resting on, but the crew were unable to control it. It's now listing badly and valuable cargo is falling overboard. The mystified captain is muttering something. The camera zooms in on him and we listen. "We must have been hacked," he's saying. "We must have been hacked." If this were the opening scene of the next James Bond film, most of us would think it a perfectly credible incident - and we'd be right, because it is.

Sabotage by cyber-attack is the latest threat to governments and industries all over the world, and the shipping industry is no exception. We all have enemies, be they political, economic or simply plain criminal, and the more equipment we connect to one network or another, the more vulnerable we become.

Ships today are completely computerized. In our continued attempts to reduce costs by increasing efficiency, more and more functions are being automated or remotely controlled, and gigabytes of data are collected every day to help us monitor the performance of our equipment. Navigation is heavily automated. Equipment usage is monitored to reduce costs through predictive maintenance. Everything from vessel position, speed and heading to fuel usage, hull stress and engine condition are monitored automatically for use in advanced optimization and prediction algorithms. Everything is connected to the network, so we can see what's going on and adjust it for optimum performance. Even the containers can be equipped with communications technology now, to give us 24/7 feedback on their comfort levels, from temperature to humidity to good vibrations. Systems can be fitted which remotely control and adjust the temperature of refrigerated containers.

The problem is, once we introduce connectivity into our operations to make it possible to interact remotely with a motion sensor in a container or, more importantly, a navigation device in a ship's control network, we make it possible for someone else to interact with our equipment, too.

"The trade off between increased efficiency and increased vulnerability is one that businesses in many industries are failing to take into account," says Andrew Ginter, VP industrial security, Waterfall Security Solutions. "We see the benefits more clearly than we see the risks."

One barrier to understanding is visibility. The most visible attacks are common viruses, malware and attacks by insiders. There's a new generation of attackers out there now, though, who work hard at invisibility. Most victims have no idea they have been compromised until months after the fact, if ever.

A more subtle barrier is the difference between espionage and sabotage. Over the last five years most of the high- profile cyber attacks were espionage attacks - stealing information. The big risk to shipping is not espionage, however, but cyber sabotage.

"Most security practitioners are much more aware of espionage risks than sabotage risks," says Ginter. "As a result we install security systems that are reasonably good at preventing the theft of data, but do little to prevent equipment damage, or worse. The prevention of cyber sabotage needs a different approach," he stresses.

"Common wisdom has it that a control system can be secured with a firewall and a bit of encryption," continues Ginter. Unfortunately, there is more wishful thinking than wisdom here. "Firewalls forward messages between networks, and they do what they can to identify and eliminate attack messages, but no firewall is or can ever be perfect. All firewalls forward some attack messages into protected networks."

In practice, all software can be hacked, Ginter explains, because all software has bugs, and many bugs are security vulnerabilities. "I wrote software for 25 years," he says. "I did not deliberately put bugs into every piece of software I wrote, but every piece of software I wrote still had bugs."

This is why intrusion detection is fundamental to defending against cyber espionage. If every message through the firewall could contain an attack, and all software can be hacked, then intrusion detection is critical. We need to assume we will be compromised, we need to search out those compromised computers, and we need to erase those computers and restore them from clean backups.

This approach fails us in the world of cyber sabotage, however. We cannot take a grounded ship and "restore it from backup." Fundamentally, intrusion detection takes time; recent studies show that it takes months to find the average intrusion. For all of that time, an invisible intruder has remote control of our vessel: falsifying data and mis-operating equipment. This is unacceptable.

While reports of stolen bank details and credit card numbers are becoming commonplace on our TV news, we don't hear so much about cyber attacks on infrastructure or industrial assets, but this doesn't mean they're not happening. If we were a multinational industry giant with customers all over the world, how likely would we be to admit that our security had been breached if we were not legally bound to disclose breaches?

Worse, attackers with no desire to be discovered are likely to disguise their interventions to look like random system failures, so their victims never know they were attacked. "This is why we don't hear about attacks," confirms Ginter, "but if you look at surveys, 70 to 80 per cent of people say they have been compromised in the last 12 months and an even greater number expect to be compromised next year."

Where have these threats come from? Why are attackers now starting to target infrastructure rather than data? There is an element of 'because they can' in there, because our headlong rush towards connectivity has made it possible for them to attack us, but the big question is about motive. What do they have to gain? There will always be terrorists with political motives and pirates with ransom demands, but the new breed of cyber attacker is more likely to be looking for an economic advantage over a rival, or to make a killing on the stock market. There has to be a profit motive.

It is generally accepted today that organised crime is behind the most visible attacks on home computers and corporate systems, because they have proven paths to profit from such attacks. "The average credit card number is worth 25 cents on the black market," says Ginter. "The average bank account number and password is worth between a dollar and a hundred dollars, depending on how much money is in the account. There's a whole industry for laundering the money, and more recently, a whole industry has been developed around stealing corporate secrets. The question that people are asking now is, how soon will an industry be developed around simulating random failures on ships or at other industrial sites to manipulate markets, or for other profit motives? Many are also asking, is this happening already, silently?"

Ginter has an example from close to home that illustrates the potential threat very well. "I live in Alberta in Canada," he says. "A pipeline that used to send gasoline from east to west across the country was recently reversed and now sends crude oil back east for refining. Alberta now has local refiners that can provide us with gasoline. But in the middle of last summer, at the time of peak gasoline consumption, the biggest refinery in the region mysteriously went down. In spite of the worldwide collapse in oil prices, we were paying through the nose for gasoline.

"The refinery didn't tell us why it went down," he continues. "It didn't have to. News reports talked about some kind of equipment failure. But think about it - if someone broke into the refinery's network and caused some equipment to fail without leaving obvious traces of cyber attack behind, and then went long on gasoline futures in our geography and made a killing on the commodities market, would anybody notice? These guys are very good at what they do. This kind of opportunity is something that if

organised crime isn't doing it today, we're certainly worried about it happening in the future. These guys are professionals. They're going to cover their tracks.

"So the question is, who profits when a ship is delayed by mechanical problems or computer problems with its navigational systems? Everything on the ship is delayed, so what's on the vessel? Is it something that somebody can profit by? Can they go short on the shipping company or can they go short on the company that owns the goods? If goods are delayed it may affect someone's profits for the quarter. This is the kind of thing that people are worried about. Where there's opportunity, somebody is going to take advantage."

Somebody took advantage in 2013 in an attack on the US retailer, Target, which resulted in costly court proceedings over the insurance claim, and incalculable damage to the company's reputation. How did they do that? "This was a data theft attack, but the attackers used the same kind vulnerability that we see with control systems on ships and in every industry," says Ginter. "They got into Target through a vendor. The attackers did not come after Target. They were just poking around, systematically breaking into one business after another to see what profit they could make. Then they broke into a vendor that provided Target with refrigeration and HVAC hardware and services. They stole remote access credentials from the refrigeration vendor and used them to log into Target. They didn't have to break through the Target firewall - they just logged in like any other user. How many vendors have remote access to our ships?"

Security awareness and preparedness vary greatly according to geography, says Ginter. "In North America there are regulations in the power sector. If the bad guys want to target the North American power sector they're going to come up against NERC CIP [the North American Electric Reliability Corporation's Critical Infrastructure Protection standards]. Now, NERC CIP is far from perfect, but it is much better than nothing. In much of the rest of the world, there is nothing."

If you get your regulations right in the first place, compliance will bring best practices into play. The question though, is how can best practices become standard practices for industries that are not regulated? "I don't see any rules emerging for the shipping industry," says Ginter. "There's no body that can enforce rules like that."

There have already been attempted attacks on the US power grid by the terrorist organisation ISIS, though these initial attacks were described by authorities as "low capability" attacks. Attack capabilities can be purchased, however, and ISIS has money. "These simple attacks are going to become more sophisticated," says Ginter. "All it takes is a little money for ISIS to buy world class attack capabilities to come after the grid, and they have plenty of money."

While the next target depends on the specific motivation of the next cyber attacker, it would be a mistake to base our security defence on the likelihood of an attack. What's unlikely today may be more likely tomorrow, but tomorrow may be too late to prevent the attack.

"Prudent security practitioners defend against well-known attack capabilities," says Ginter. "They do not defend against the motive of the moment. They do not look around and say 'how many ships were stranded last year in the middle of the ocean like this?' Motives can change in a heartbeat. Somebody can suddenly get a bee in their bonnet and decide to come after us. Capabilities evolve much more slowly. So industrial sites today are looking at the capabilities in the threat environment and defending against them before someone develops a motive to use those capabilities against their sites."

If our organization is lucky enough not to have been targeted by a cyber attacker yet, what approach to security are we going to take? Are we going to look at the statistics of ships being attacked in this way and respond according to our perception of likelihood, or are we going to put protections in place before serious harm is done?

For those looking for credible sabotage- oriented protection, there are solutions available. Waterfall Security Solutions is a cyber security specialist that produces hardware-enforced security products, focused on preventing the cyber sabotage of ICS (industrial control system) networks. The hardware part of the solution is called a unidirectional gateway.

"We have a family of products but our flagship product is the unidirectional gateway," says Ginter. "The gateways enable safe network integration. The gateways let businesses monitor their control system equipment, but make it physically impossible to send any attack back in to those critical networks.

"We claim 100 per cent protection against network attacks coming from external networks," he continues. "While there is no technology that can prevent absolutely all attacks, these silent, online, network-based attacks are the workhorse of cyber sabotage, and are the specific risk that comes with increased network connectivity. Our gateways eliminate that specific threat vector entirely."

When a unidirectional gateway becomes the only connection between a more trusted network and a less trusted network, he explains, data travels only one way, so nothing gets back in to the ICS network. Waterfall makes the data available for anyone who needs it, by replicating industrial databases and devices. "Anyone who wants the real-time data can ask the replicas and get the same answer they would have had by asking the live systems," Ginter explains. "They get the same answer from the replica as the control system equipment would have given them, without ever sending a message to the control system and putting that equipment at risk."

Waterfall Security Solutions produces a family of products that are based on or complement its unidirectional gateways. The Waterfall FLIP is a kind of gateway that can reverse orientation on a schedule, to provide continuous monitoring and occasional batch updates of shipboard systems, such as security updates or weather forecasts. Inbound/outbound gateways can provide continuous updates of onboard systems through separate, independent replications, without ever introducing the kinds of attack paths that always come with firewalls. Application data control add-ons apply fine-grained policy-based controls to data in motion between networks. All of these products frustrate modern, silent, remote-control cyber sabotage attack capabilities, as well as a host of older, more mundane attacks.

The 2015 "Safety and Shipping Review" by Allianz identified cyber sabotage attacks on shipping as "a major concern." Cyber sabotage attack capabilities have become much more sophisticated in the course of the last decade. Attackers use powerful software tools, and like all software, attack tools become more and more capable as new versions are released. Basic security hygiene, such as firewalls, anti-virus systems, security updates, encryption and long passwords, provide little protection against modern attacks by criminals or 'hacktivists'.

"In the shipping industry, we need to take inspiration from control system cyber security standards and regulations in other industries," says Ginter. The French ANSSI standards for critical infrastructure protection prohibit firewalls at the boundaries of the most important control system networks, permitting only unidirectional gateways. The North American NERC CIP standards provide relief from one third of the security regulations when unidirectional gateways are used instead of firewalls at large power plants. The ISA, IEC, NIST and many other standards all position unidirectional gateways as stronger than firewall protections for control system security programs.

"We have a window of opportunity now, to protect the control systems and navigation systems on our vessels, before we start suffering very serious losses," concludes Ginter. "Increased automation and connectivity brings increased opportunities and profits, but only if we address the risks."

The Economist
Snoopers and scrutiny
Thursday, 21 January 2016
Byline: Editorial Board

Editorial - Few balances are harder to strike than those involved in running a spy agency. After a terrorist attack, voters demand action and politicians respond by granting their spies greater powers to bug and snoop, as with America's Patriot Act in 2001 and the wide-ranging surveillance law passed after the attacks in France last year. Yet these very powers can, if abused, distort the political system, chill freedom of expression and tilt the scales of justice. When the full extent of clandestine activities come to light, as with Edward Snowden's revelations about America's National Security Agency, many feel queasy and demand that the spooks are reined in again.
So a lot is riding on Britain's attempt to update the law governing the domestic activities of its spy agencies. The draft bill will make explicit how the electronic-intelligence agency, GCHQ, may (with a warrant) plant bugs on computers and other devices, collect and analyse bulk information (such as mobile-phone activity and web-browsing records) and read private messages. Get the details right, and Britain can provide a model of how to balance security and freedom; get them wrong, and centuries of freedom might shrivel.

The bill's biggest success is its self-restraint. It does not require firms to weaken the encryption they sell to customers, as politicians in several countries, including Britain, would like. If people want security on

the internet, they have no alternative to strong encryption. The agencies have other means of collecting data, including bugging phones and computers.

The draft bill is also right to require companies to retain, at least for a time, data about mobile-phone and internet activity that may, subject to a warrant, be of use to future investigations. Intelligence agencies need to be able to look back at the history of a suspected terrorist's contacts and movements.

Elsewhere, however, the bill could be better. It rightly strengthens GCHQ's powers to pursue terrorists, gangsters and foreign spies. And it offers extra safeguards: new judicial commissioners will review warrants which, as now, will be issued by the home secretary. Politicians should have ultimate responsibility; if things go wrong, they carry the can. But the bill will work best if it is backed by a consensus. For that reason it needs to reassure those who fear that politicians may abuse their powers. Instead of holding their posts at the prime minister's behest, the commissioners should be appointed as judges are and their dismissal should require a vote in Parliament. To avoid "capture", they should serve a single fixed term.

In addition, the proposed system merely requires the commissioners to check that a warrant has been issued lawfully and reasonably--broadly the same standard applicable to judicial review of other government decisions. But the extra secrecy with which intelligence agencies operate means that is not enough. The commissioners need a reserve power to weigh warrants on their merits. Also missing is explicit protection for lawyers' communications with their clients.

Just as important as the nuts and bolts of the new law is its implementation. GCHQ's demands may be legal, but if they are too costly or intrusive, companies dealing with technology and data will simply move abroad. For all these reasons, other countries should watch Britain closely.

Wall Street Journal
NSA Chief Says U.S. at 'Tipping Point' on Cyberweapons
Thursday, 21 January 2016
Byline: Damian Paletta

Washington - The U.S. military has spent five years developing advanced cyberweapon and digital capabilities and is likely to deploy them more publicly soon, the head of the Pentagon's U.S. Cyber Command said Thursday.
Adm. Mike Rogers, who is also director of the National Security Agency, said U.S. policy makers have largely agreed on rules of engagement for when cyberweapons can be used for defense.

There is still an open discussion, however, about when cyberweapons should be used for "offense," such as carrying out attacks against a group or foreign country.

"You can tell we are at the tipping point now," Adm. Rogers said. "The capacity and the capability are starting to come online [and] really starting to pay off in some really tangible capabilities that you will start to see us apply in a broader and broader way."

Still, Adm. Rogers stopped short of specifying how exactly these cyberpowers could be deployed in coming months.

Despite a series of high-profile cyberattacks in the past two years, including a large-scale breach at Sony Pictures Entertainment Inc. in late 2014 and the theft of millions of records from the U.S. Office of Personnel Management in 2015, Adm. Rogers suggested many Americans have become complacent, since they don't see the rise of cyber armies and cybercriminals affecting their daily lives.

That could change fast, he said, if a cyberattack achieves large-scale destruction, particularly in a fashion resembling a more traditional weapon. Analysts have said these sorts of acts could including attacking a country's electrical grid or knocking a nation's financial system offline.

"I'm watching capability when I go, 'Wow, if the intent were to change, we'd have some real challenges here,' and intent can change really quickly," he said. "I would urge us not to draw the conclusion that there is nothing here we really need to worry about. I would argue it's going to get worse before it gets better."

Adm. Rogers, who has led the NSA and Cyber Command for two years, was brought in to stabilize the agency after a furor over the far-reaching surveillance program disclosed by former contractor Edward Snowden. The NSA has seen some of its powers clipped, most notably when Congress last year banned bulk collection of telephone records.

Adm. Rogers has said the agency needs to do more to restore public confidence, and he has been adamant that the government needs to develop specific rules about the emerging digital battlefield.

Following the OPM breach, which some U.S. officials attributed to Chinese hackers, many lawmakers have said the White House and Pentagon need to clarify rules of engagement and make them public. These could include specific punishments and retaliatory actions, as a way to deter future attacks.

Adm. Rogers said policy makers have been working to develop "the same kind of standards" for responding to cyberattacks that they use for other warfare.

The NSA director also said the agency will launch a reorganization this year to better mesh its two tasks--digital spying and data collection on the one hand and protecting information on the other.

"We have got to integrate much more," he said. "This traditional approach we had...built walls of granite between them."

The Intercept
NSA Chief Stakes Out Pro-Encryption Position, in Contrast to FBI
Thursday, 21 January 2016
Byline: Jenna McLaughlin

Washington - National Security Agency Director Adm. Mike Rogers said Thursday that "encryption is foundational to the future," and arguing about it is a waste of time.
Speaking to the Atlantic Council, a Washington, D.C., think tank, Rogers stressed that the cybersecurity battles the U.S. is destined to fight call for more widespread use of encryption, not less. "What you saw at OPM, you're going to see a whole lot more of," he said, referring to the massive hack of the Office of Personnel Management involving the personal data about 20 million people who have gotten background checks.

"So spending time arguing about 'hey, encryption is bad and we ought to do away with it' ... that's a waste of time to me," he said, shaking his head.

"So what we've got to ask ourselves is, with that foundation, what's the best way for us to deal with it? And how do we meet those very legitimate concerns from multiple perspectives?"

Other government officials -- most notably FBI Director James Comey -- have been crusading for a way that law enforcement can get access to encrypted data.

But technologists pretty much universally agree that creating some sort of special third-party access would weaken encryption to the point that it would threaten every internet transaction we make, from online banking to filling out our health records to emailing our friends and significant others. A hole in encryption for special FBI access would be a hole that criminals could sneak through, too.

While there's been a lot of talk about giving up some privacy for security, Rogers said both are paramount.

"Concerns about privacy have never been higher. Trying to get all those things right, to realize that -- it isn't about one or the other," he said. He does not think that "security is the imperative and that ought to drive everything." Nor should privacy, he continued. "We've got to meet these two imperatives. We've got some challenging times ahead of us, folks."

Comey, who formerly advocated for a way to get law enforcement access without weakening encryption, recently switched tactics. Now he is pressuring companies to change their business models and simply not offer true end-to-end encryption to their customers.

The White House has decided not to pursue legislation to outlaw unbreakable end-to-end encryption, following pressure from privacy advocates and scientists. But the intelligence community's top lawyer,

Bob Litt, privately advised the administration that a major terrorist attack could be an opportune moment to do so.

And the White House has not issued a statement in defense of encryption, to the frustration of Apple CEO Tim Cook, among others.

Meanwhile, Sens. Richard Burr, R-N.C., and Dianne Feinstein, D- Calif., are reportedly planning their own proposed legislation to require law enforcement access.

Rogers' comments could indicate a split on this issue between the intelligence community and domestic law enforcement.

The previous NSA director, Michael Hayden, said in January that he thinks Comey is on the wrong side of this debate. "I disagree with Jim Comey. I actually think end-to-end encryption is good for America," he said.

Hayden has also spoken about how U.S. intelligence agencies have figured out how to get the information they need without weakening encryption -- such as using metadata, which shows who is contacting whom. Another former NSA boss, Mike McConnell, has also spoken out against trying to install backdoors in encryption.

Left unsaid is the fact that the FBI and NSA have the ability to circumvent encryption and get to the content too -- by hacking. Hacking allows law enforcement to plant malicious code on someone's computer in order to gain access to the photos, messages, and text before they were ever encrypted in the first place, and after they've been decrypted. The NSA has an entire team of advanced hackers, possibly as many as 600, camped out at Fort Meade.

Ottawa Citizen
Get smarter about foreign intelligence
Wednesday, 27 January 2016
Byline: Alistair Hensler

Re: Canada is increasing its intelligence efforts, Jan. 20.
In his opinion piece, Wesley Wark has proposed various ways that Canada could increase its intelligence efforts to support our allies in the fight against ISIL. In so doing, Wark has identified the numerous disparate government departments and agencies that are engaged in collecting foreign intelligence.

Therein lies the principal problem with Canada's foreign intelligence efforts: there is no central organization to manage and correlate the government's foreign intelligence operations. Canada is the only G7 country without a centralized foreign intelligence collection capability. If the government is serious about becoming a "smart power," as Wark states, it must address this deficiency. The task is onerous but not impossible. The first step is to define foreign intelligence and identify all those government resources, financial and personnel, currently engaged in analyses, collation and distribution. There will be surprises. For example, Foreign Affairs, which has historically blocked the creation of a centralized foreign intelligence capability, maintains resources for that purpose; others include Canadian Security Intelligence Service and National Defence.

The second step is to transfer those resources into a new centralized agency which would have the Communications Security Establishment, the primary foreign intelligence collector, as its cornerstone. This new agency would become the sole collector of foreign intelligence on behalf of the government. Having one agency has the added benefit of facilitating government oversight of foreign intelligence operations, which does not occur under the current diverse organizational structure.

The time is right for a major shift in the Canadian foreign intelligence community so we can contribute in a meaningful way to the fight against ISIL and other terrorist organizations.

Alistair Hensler

Ottawa, former assistant director, CSIS

Canadian Press
Five things to take away from government's National Defence performance report
Wednesday, 27 January 2016
Byline: Staff reporter

OTTAWA _ The federal government released departmental performance reports this week, including one for National Defence, which spent $18.4 billion in the budget year that ended last March. Here are five interesting and unusual facts from the annual disclosure tabled in Parliament.

_ The House of Commons voted to appropriate $20.4 billion for the military, but as in past years, a substantial amount _ $1.9 billion _ was not spent. Of that, $1.3 billion was for purchases of new planes, ships and vehicles that had been budgeted but was either unavailable _ or delayed by the former Conservative government _ until future years. Not all of the surplus funds have to go back to the federal treasury.

_ A significant number of full- time military members were unable to be deployed on operations _ both at home and abroad _ because of dental issues. The report says 5.4 per cent of those deemed ineligible required ongoing dental care, while 15.4 per cent did not show up for their annual dental fitness exams. National Defence says it will have to proactively remind personnel of their obligations.

_ A lot of public attention is paid to the Canadian Security Intelligence Service spy agency (CSIS) and the Communications Security Establishment (CSE), Canada's electronic spy agency, but not many people realize the Canadian military maintains a large defence intelligence system. Last year, it produced more than 5,000 reports, which it shared not only with the top brass but with government departments. The branch also spent $202.4 million in hopes of providing "credible, timely, and integrated analysis of defence intelligence issues."

_ The army may have service problems with its trucks, but the Royal Canadian Air Force managed an overall fleet serviceability rate of 93 per cent for its jets, fixed-wing planes and helicopters. That's despite having some aircraft that are more than 50 years old. The department report notes, however, that spare parts "remain a concern for certain fleets," and they've only be able to maintain serviceability rates by robbing "parts from other aircraft, which increases maintenance requirements."

_ National Defence spent $113 million less than expected on international combat operations last year. It's not because the air force was being stingy with the bombs. Rather, the former Conservative government built the cost of winding down the bombing campaign against the Islamic State of Iraq and the Levant into its budget projections. National Defence says the incremental cost of the war against ISIL _ the cost over and above buying and maintaining the military equipment _ was $70 million between April 2014 and March 2015.

Globe and Mail
U.S. takeover of network carrying sensitive federal data raises security concerns
Wednesday, 27 January 2016
Byline: Steven Chase

A U.S. takeover of a national fibre optic network in Canada that carries sensitive federal government telecommunications traffic is raising security concerns that the United States will find it easier to gain access to confidential Canadian data.
In a transaction that closed this month, Manitoba Telecom Services Inc.'s Allstream unit has been bought by U.S.- based Zayo Group.

Allstream, with its coast-to-coast Internet backbone network, is under contract to carry data for 43 Canadian departments and agencies, including the Department of National Defence, the RCMP and Canada Revenue Agency.

In 2013, the Harper government blocked a deal to sell Allstream to Egypt's Accelero Capital Holdings on the grounds of national security. Ottawa said it kept Allstream out of foreign hands because it "provides critical telecommunications services to businesses and governments, including the government of Canada."

Manitoba Telecom and Zayo announced the deal in November, and the Trudeau government declined to conduct an official national security review.

"The 45-day period during which the government could raise national security concerns has passed," said Stéfanie Power, a spokeswoman for the Department of Innovation, Science and Economic Development, which screens foreign takeovers through its investment review division.

Critics say the net result of the deal is that a foreign entity now owns and controls a network carrying extremely confidential Internet traffic for Ottawa. No other major domestic network supplier to the federal government is foreign owned and controlled.

The Allstream takeover was announced weeks after Prime Minister Justin Trudeau took office. The period for review by Ottawa ended in early January.

Michael Geist, an expert in Internet law at the University of Ottawa, says U.S. ownership of a Canadian Internet backbone makes it easier for Washington to obtain access to the data it carries, either through the courts or covertly.

"Any time you have a U.S.based entity that owns a Canadian network, it increases the risk that U.S. authorities will have easier access to the information that runs on that network," Prof. Geist said.

Legislation such as the U.S. Patriot Act gives the United States power to compel a U.S. company to produce information, including communication possessed by a foreign subsidiary.

"It's not limited to the U.S Patriot Act. U.S. authorities have a number of legal mechanisms that allow them to try to gain access and [this] is unquestionably made easier when the entity that they are dealing with is U.S. based," Prof. Geist said.

Manitoba Telecom's chief corporate and strategy officer, Paul Beauregard, said his company worked long and hard to provide sufficient information to satisfy the government that "Zayo would be an appropriate purchaser from a security perspective."

Innovation Minister Navdeep Bains defended Ottawa's conduct in this case, saying every foreign investment is "subject to a due diligence process."

He declined to explain why the Liberals decided against a formal national security review, saying these are ordered only when the government feels "investment could be injurious to national security."

Washington has made it clear it considers data held by U.S. companies abroad part of its purview.

Microsoft is appealing an order by a U.S. court in 2014 to turn over e-mails on company servers in Ireland. Last fall, U.S. government lawyer Justin Anderson told Reuters News that U.S. law enforcement believes it can obtain electronic information held by U.S. companies with a valid warrant, regardless of where the data are stored. "It's not a question of ownership," Mr. Anderson said, likening it to seizing account records from a bank. "It's about custody and control."

Conservative foreign affairs critic Tony Clement slammed the Liberals for skipping a national security review and said he wants to know what protections Canada has obliged Zayo to enact to prevent interception of crucial data.

"The Trudeau cabinet declined to do even the very least to examine whether Canada's national interests are being affected by this transaction. This is a very bad precedent," he said. "Canadians deserve to know what safeguards the government of Canada is putting into place to ensure the protection of sensitive and proprietary information."

An executive with Zayo Group said the company also provides telecommunication and data services elsewhere outside the United States, including for customers in northern Europe.

"They all take their data security very seriously ... so we are used to operating in that environment," said Dave Jones, executive vice-president of security and IT. "Security is very important to Zayo."

Asked to gauge the risk that the U.S. government could demand access to data on Zayo's new Canadian network, Mr. Jones said "it's not something we can comment on specifically."

Ray Boisvert, a former assistant director of intelligence at the Canadian Security Intelligence Service, said Ottawa appears to be betting a major ally will not take advantage.

"Generally speaking, friends don't spy on friends," Mr. Boisvert said.

Andrew Clement, a professor in University of Toronto's faculty of information, said spying revelations from whistleblower Edward Snowden should breed skepticism among Canadian decision-makers about what kind of surveillance spying the United States might undertake. "A significant part of the Canadian Internet backbone has just transferred to U.S. ownership.

This is critical infrastructure from a Canadian sovereignty point of view," Prof. Clement said.

The Courier-Mail
Social media deal to cut terror hype
Wednesday, 27 January 2016
Byline: Staff reporter

Federal Government agencies are expanding their ties with Facebook, Google and Twitter in a bid to stop terrorist propaganda infiltrating Australian youths.
The Government is also continuing to review programs that provide teachers with information to spot teens who are at risk of being radicalised.

Multiple school-aged children are undergoing government deradicalisation programs after they were found to be considering going to the Middle East as jihadists.

The preventive measures, launched by former prime minister Tony Abbott and continued under Malcolm Turnbull, are now a critical part of Australia's national security policy.

The Courier-Mail understands that government min-isters and agency heads have held multiple meetings with the -online media giants, which are deactivating profiles and accounts that spread propaganda.

Counter-Terrorism Minister Michael Keenan confirmed the Government was in regular contact with the giants."We work with social media companies, including Google, Twitter and Facebook, and with operational agencies to tear down violent extremist material," he said.

The Australian
Terror documents 'on teen's phone'
Wednesday, 27 January 2016
Byline: Mark Schliebs

Sameh Bayda last used the -encrypted messaging service Telegram at 5.12am on Wednesday, January 13. A few hours later, counter--terrorism police raided his house.
Seizing the teenager's phone, which he had used to access that encrypted app, they found three documents allegedly containing written instructions, including from terrorist group al-Qa'ida, "connected with the preparation for a terrorist act".

One of these, written in Arabic, provided "instruction on how to carry out a successful stabbing attack", a court was told yesterday. Another, also in Arabic, -detailed "how to make an improvised explosive device".

The 18-year-old former Granville Boys High School student faces the prospect of up to 15 years in prison.

Mr Bayda's neighbours in Guildford in western Sydney said they feared the damage he might have done to himself and his "beautiful" family.

While Mr Bayda's use of -Telegram did not spark the police raid -- investigators had become increasingly concerned about his activities over recent weeks -- sources said it marked a shift in the tactics alleged extremists used.

Communications sent using encrypted services such as Telegram cannot easily be read by police.

The company's website says it is more secure than its "mass--market" competitors, using "end-to-end encryption (that) leave no trace on our servers, support self-destructing messages and don't allow forwarding".

Two days after Mr Bayda's brick duplex house was raided, Telegram founder Pavel Durov tweeted that his company was -removing up to 10 accounts linked to Islamic State every day.

At this point, it is not clear what the documents on Mr Bayda's phone contained, although the authorities say such material is being widely circulated between -extremists online.

What court documents tendered yesterday describe as "a PDF document in English published by the proscribed terrorist organisation al-Qa'ida in the Arabian Peninsula" is thought to be a copy of the group's online propaganda magazine Inspire.

At least one senior Islamic State member, Junaid Hussain, who is also known to have used Telegram, last year sent out -instructions on how to build -improvised explosives similar to those used in the 2013 Boston Marathon attack.

Hussain was reportedly killed in a drone strike in Raqqa in Syria in August. On the evidence before the court, the case against Mr Bayda rests largely on the material found on his mobile phone. Police do not allege he was planning a specific attack, but have charged him with "knowingly collect/make documents connected with terrorism".

Court documents say he was "reckless" as to the connection of the images in the documents to terrorism.

He is not thought to be directly connected to any known extremist group in Sydney, although the links between these individuals can often be indirect or unclear. Despite this, the police were worried.

Neighbours said the house had been visited by detectives last year, around the time of a co-ordinated series of counter-terrorism raids across the city codenamed Operation Appleby.

During the January 13 raid, Mr Bayda was served with a firearms prohibition order, allowing police to search him and his home without first obtaining a court warrant.

Then, on Monday afternoon, the 18-year-old was arrested. Taken into custody just before 3pm, he was refused bail.

He declined to appear in court yesterday and is due to face court again next week.

A photograph of Mr Bayda, one of four children, posted online shows a bearded, soft-faced teenager wearing fluorescent work gear. In October, he registered himself as the sole director of Westside Painting and Decorating Pty, and began advertising himself online as a "licensed and insured painter" with "over five years of experience".

Although he deleted his Facebook account last year, a YouTube channel established in the name of "Sameh Bayda" includes tributes to Osama bin Laden and a Kuwaiti suicide bomber who targeted -Syrian troops and Hezbollah members in Syria last year.

Two weeks ago, the same YouTube channel shared a video featuring Islamic preacher Junaid Thorne. "Look right, left and centre, what do you see? All you see is our ummah (community) suffering from multiple and several wounds to its body," Mr Thorne says in the film.

Appealing to Muslim youth, Mr Thorne says: "If you don't get up and make a change to better the situation of our ummah, nothing will change." No one answered the door at Mr Bayda's Guildford duplex yesterday, although one neighbour, Arthur Solo, described the family as "one of the most beautiful" he had met.

"From what I've seen of the boy, it's all just bravado," Mr Solo said. "The boy must realise the gravity of it. That's what I fear, the disservice he's done to himself, his family and the other Middle Eastern people around here."

London Times
Russian hoaxers behind bomb threats to pupils
Wednesday, 27 January 2016
Byline: Nicola Woolcock

London - A Russian group using Twitter has reportedly claimed responsibility for a series of bomb hoaxes that led to thousands of children being evacuated from schools in Britain and France yesterday.

Schools in London, the West Midlands, Cornwall and Paris were targeted but it is not known if the incidents were linked. Three of the six schools evacuated in the Midlands had suffered similar hoaxes last week.

Police said that there was no credible threat behind the calls, but they caused widespread disruption. The Russian group is said to have invited pupils to get in touch if they wanted to "get out of school".

The account, Evacuators 2K16, has since been deleted but has been blamed for instigating another bomb hoax in America.

The profile for @Ev4cuati0nSquad, which has been suspended, apparently said: "We are six individuals based internationally. For bomb threat requests please email us."

The group reportedly said it hated authority and loved to cause mayhem, according to the Daily Mail. It said people could send in requests for their school, work or business to be sent a bomb threat, and asked for payments in Bitcoin, the virtual payment.

Prices varied from $5 for a school to $50 for a major sports event.

An American news website said that the group was responsible for string of bomb threats at a police station, supermarket, hospital and shop yesterday, a week after similar pre-recorded threats at schools. They were all in the small town of Weymouth in Massachusetts.

Four schools were targeted in London, according to the Metropolitan police, in separate threats made yesterday morning. They all claimed that a suspicious device had been left at the premises, and pupils were evacuated. The calls are being treated as malicious communications by detectives.

West Midlands police said the calls were made in quick succession at about 9am to four schools in Sandwell, one in Dudley and one in south Birmingham.

It comes after similar phone threats to four schools in the Black Country last week after which hundreds of pupils were evacuated before police confirmed that the calls were hoaxes. Six schools in central Paris were evacuated yesterday after they received anonymous calls that bombs had been hidden in the buildings, police and the school authorities said.

Gulf Times
Kaspersky warns of regional threat from cyber criminals and terrorists
Wednesday, 27 January 2016
Byline: Dean Carroll

Undisclosed placeline - The Russian, who claimed his mission was to "save the world" from cyber criminals and terrorists, has warned the region's leaders to take the threat very seriously in the run up to major events such as Expo 2020 in Dubai and the 2022 football world cup in Qatar. Speaking exclusively to Gulf Business, Kaspersky Labs chief executive officer Eugene Kaspersky claimed that malware was becoming evermore sophisticated as traditional crime gangs and terrorists started to employ hackers.
"There are both global threats and regional threats," he said. "Globally, it is really about energy in the form of power plants and grids. If there is no power, then nothing else works in whatever country you are in - it's a problem for any nation. Then of course, you have major critical areas that could be attacked such as financial services and transportation.

"In this region, there is a dependence on the oil and gas sector. You also produce aluminium here through local systems and there are desalination plants to provide fresh water. Attacks on these systems would be very painful for the economy and damaging for national security."

Asked to describe the worst-case scenario in terms of potential attacks on critical infrastructure, he insisted that there had already been major incidents that could almost be classied as cyber-terrorism or cyber-war. The attack on Saudi Aramco "being an example". Kaspersky said: "For two weeks, the company was paralyzed.

"We are very vulnerable. We depend on technology; you cannot now get back to the time when humans were solely responsible for managing everything. Computers are faster than us humans and they consume less power. They don't sleep, they have no vacations and no holidays - and they are less expensive.

"The computers made the world faster and better but at the same time they are vulnerable. We fixed many of the old problems through computers but now we have a new set of problems. The worst-case scenario is if the bad guys attack these vulnerabilities or there are mistakes leading to serious problems with our critical infrastructure."

Touching upon the need to regulate the digital world in order to better control the threat from rogue actors, the CEO said total freedom on the internet was "dangerous".

Haaretz
Islamic Terrorists Increasingly Embracing Cyberwarfare
Wednesday, 27 January 2016
Byline: Danna Harman

Jerusalem - The forces of militant Islam today may be medieval in their philosophies, Prime Minister Benjamin Netanyahu warned Tuesday - but they are increasingly modern in their methods.

"These militants are using the technologies that we use," he said, addressing the crowd of international cyber technology experts gathered at the Tel Aviv Trade Fair and Convention Center for the Cybertech 2016 conference.

The two-day annual event drew some 3,000 participants, organizers say, including representatives of leading multinational and Israeli corporations and startups, investors and entrepreneurs from the various fields of cybersecurity, as well as government and military officials from around the world. Among those present were U.S. Deputy Secretary of Homeland Security Alejandro Mayorkas and Colonel Andre Lourenco Eiras, head of Brazil's Cyber Defense Program, who is charged with cyber protection for the upcoming Olympics in that country.

"We are facing... a force that challenges modernity, and that force is a savage... primitive medievalism that seeks to take our world back to the dark ages of humanity, over a thousand years ago," said Netanyahu.

"This is one of those few times in history in which the forces that seem to take humanity back are using some of the forces that take humanity forward. And this presents a greater challenge to us," continued the prime minister, echoing a similar warning he made last week at the World Economic Forum in Davos.

Netanyahu boasted that Israel was on the forefront of that fight, as one of the top five major cyber powers in the world, and accounting for about 10 percent of global sales in the cyber- security business. But, still, he admitted, in the cyber war against the "the forces of medievalism," Israel could not stand alone. "There is a critical need for like-minded governments to have serious discussions about cooperation in the broader international realm," he said.

This theme of cooperation was repeated during sessions on the first day of the conference: "In cybersecurity there are no borders," stressed Zionist Union MK Erel Margalit, who heads Israel's Cyber-Security Lobby in the Knesset. "If you want to be secure and open and private, you need to cooperate," he reiterated, chairing a panel discussion on the need for a task force "among friends."

On the question of what such cooperation might look like, Netanyahu, and others, were less detailed: "I do not seek to have a universal code, because it will work for cyber peacekeeping just like the UN works for international peacekeeping - it doesn't," said Netanyahu.

"What we need is a meeting of international leaders to discuss what could be done among countries that want to maintain freedom and safety in their societies," said Netanyahu, suggesting the establishment of "international standards" to increase cybersecurity. "This is something that has yet to be done, but I've been speaking about this with world leaders," he said.

Gustav Lindstorm, head of the emerging security challenges program at the Geneva Center for Security Policy, added that it was quite clear to all that the only way to fight cyber threats - be they in arenas of finance, national defense or any other - was for countries to cooperate.

"The multi- stakeholder model is indispensable," he stressed, speaking on a panel about international cooperation and shared responsibility. "Cybersecurity cannot be achieved by a single stakeholder, structure or organization. There is simply no way."

Speaking after Netanyahu at the opening plenary session, Gil Shwed, the founder and CEO of Check Point Software Technologies, said that while advances in cybersecurity have been great, cyber threats are growing at an even more alarming rate.

"We tend to think about cybersecurity threats in the way we think of conventional threats. But it's different," he said, explaining that in cyberspace it's often unclear who are the enemies, what their motives are or what weapons they have in their arsenals. If, said Shwed, in conventional warfare, one could rely on intelligence, deterrence and retaliation - in cyberspace, these were both harder to get right, and also not enough. "By the time the malware is inside - damage is already done," he said. "We need to be one more step ahead."

Washington Free Beacon
Chinese Military Revamps Cyber Warfare, Intelligence Forces
Wednesday, 27 January 2016
Byline: Bill Gertz

Washington - A recent Chinese military reorganization is increasing the danger posed by People's Liberation Army cyber warfare and intelligence units that recently were consolidated into a new Strategic Support Force.
The announcement of the military reorganization made on Dec. 31 by the Chinese government provided few details of what has changed for three military intelligence units formerly under the now-defunct General Staff Department.

However, U.S. officials and China analysts say the major cyber warfare and intelligence-gathering groups were elevated into the new Strategic Support Force, a military service-level force equal in standing to China's army, navy, air force and missile services.

They include the 3rd Department, or 3PLA, that is believed to have as many as 100,000 cyber warfare hackers and signals intelligence troops under its control. The group includes highly-trained personnel who specialize in network attacks, information technology, code-breaking, and foreign languages.

Five members of a 3PLA hacking group were indicted by the Justice Department for commercial cyber attacks against American companies in 2014.

The 4th Department, China's separate military electronic intelligence and electronic warfare service, is also part of the new support force. Additionally, the traditional military spy service devoted to human spying known as 2PLA was combined into the new support force.

"From a strategic perspective, the PLA will now be able to move forward with the concept of integrated network electronic warfare and better manage the use of satellites for [intelligence, surveillance, and reconnaissance]," said former military intelligence officer Larry Wortzel.

James Lewis, a cyber specialist with the Center for Strategic and International Studies, said the new force will enhance the capacity of the PLA.

"They have a ways to go, but this is their effort to compete with the U.S. in the information domain," Lewis said. "It fits with their improved [anti-satellite] and cyber attack capabilities."

The 3PLA was identified by the National Security Agency as one of China's most aggressive cyber spying agencies.

Classified documents made public last year revealed that the NSA estimates 3PLA hackers conducted more than 30,000 cyber attacks aimed at gathering defense industrial secrets. More than 500 of the cyber attacks were gauged to involve "significant intrusions" of defense networks.

Compromises included the theft of secrets regarding the F-35 and F-22 jets, the B-2 bomber, and space-based laser systems.

The NSA learned details of the operations by conducting its own cyber penetration in 2009 of a network connected to 3PLA computers.

Adm. Mike Rogers, commander of the U.S. Cyber Command, said large-scale hacking has numbed many Americans to a threat that is growing.

"If you look at the trends, if you look at the activity, for example, that we see within critical infrastructure in the United States, power and other things, you see nation states, individuals, and actors within those systems," Rogers said last week.

"To date we have not seen on any significant scale a desire to take that access and employ it as a way to bring the system down," he said.

"But what happens when that changes? Because as military, I've always thought about threat as a combination of capability and intent. I'm watching capability where I go, wow. If the intent were to change we have some real challenges here. And intent can change very quickly."

Chinese military expert Yin Zhuo told the state-run People's Daily newspaper that foreign forces continue to conduct cyber attacks on Chinese government, military and civilian facilities and the new Strategic Support Force will focus on the threat.

"It is imperative that we possess a corresponding defense force," he said. "The Strategic Support Force will play an important role in safeguarding our nation's financial security and protecting our people's safety in daily lives."

The overall functions of the Strategic Support Force are targeting detection and reconnaissance, satellite and space operations, electronic warfare and cyber warfare. "All these are new domains that will determine whether our military can win victories on future battlefields," Yin said.

The force will be integrated within other military groups and will provide "potent battlefield support for joint operation actions of multiple services and arms so as to achieve the goal of winning local wars under informatized conditions," Yin said.

U.S. intelligence officials disclosed to the Washington Free Beacon last year that China has sharply increased funding for cyber warfare capabilities.

The funding increase--an estimated 30 percent more devoted to cyber warfare and cyber spying--follows Beijing's assessments that its capabilities lag behind those of the United States.

The buildup of cyber warfare capabilities was described by officials as a long term, strategic buildup of digital warfare capabilities.

By contrast with China, the U.S. Cyber Command currently has around 6,000 people engaged in both cyber defense and cyber attack preparations. The NSA, which conducts the bulk of cyber intelligence-gathering, employs a force of at least 40,000 people.

Wortzel, the former military intelligence officer, said the new force combines the electronic warfare and countermeasures capabilities of 4PLA with the signals intelligence capabilities of 3PLA, along with control of satellites and space-based intelligence, surveillance, and reconnaissance.

The cyber warfare, collection and defense responsibilities had been divided between 3PLA and 4PLA. "Now they apparently will be consolidated in the Strategic Support Force," Wortzel said, noting that the civilian Ministry of State Security will probably keep its separate cyber and intelligence gathering capabilities.

Lewis, the CSIS cyber expert, said the PLA reorganization is "probably good news on the cyber espionage front."

"It gives Xi the control to tamp down PLA spying--he seems to want to do this after calculating that the gain now isn't worth the friction," Lewis said. "But it's bad news for warfighting as they are reorganizing with one opponent in mind."

In September, Chinese leader Xi Jinping announced that China's military needed "a new strategy for information warfare amid a global military revolution."

The 3PLA headquarters is located in Beijing's Haidian district and its branch offices are located in Shanghai, Qingdao, Sanya, Chengdu, and Guangzhou. The Shanghai office is said to be focused exclusively on targeting the United States.

The five PLA hackers indicted by the Justice Department, who remain wanted by the FBI, were part of a 3PLA agency called Unit 61398, which has been identified as a major cyber attack unit behind the theft of large amounts of U.S. government and private sector data, ranging from secrets related to the F-35 jet to corporate secrets about nuclear power generation.

Peter Mattis, a China analyst with the Jamestown Foundation, said the new military reorganization is the most significant change since the PLA was reorganized in the 1950s and likely will integrate the resources of the 2PLA, 3PLA and 4PLA into various regional and functional military headquarters.

"Although no specific announcements have thus far been made about the intelligence apparatus, it seems unreasonable to think the PLA's intelligence system will go untouched," Mattis stated in an article published in War on the Rocks.

China's most senior intelligence officer in the past has been the deputy chief of the General Staff Department, who played a key role in the ruling Communist Party decision-making on domestic and foreign affairs. That position will likely now be taken by the chief of the Strategic Support Force. China has not identified the new leader.

China's government relies heavily on the use of strategic intelligence, based on the precepts of the ancient strategist Sun Tzu who said the acme of skill was defeating your enemy without shooting.

"The biggest question about the reorganization of intelligence is how the PLA will do within the intelligence apparatus to increase jointness--one of the stated goals of the reforms," Mattis stated.

"Plenty of evidence suggests the Chinese military wants intelligence more connected to operational decision-making."

Times of Israel
Israel's Electric Authority hit by 'severe' cyber-attack
Wednesday, 27 January 2016

Byline: Tamar Pileggi

Jerusalem - Israel's Electric Authority is currently being targeted by a "severe cyber-attack," Energy Minister Yuval Steinitz said Tuesday, adding that steps are being taken to counter the assault. Addressing the Cybertech Conference in Tel Aviv, Steinitz said the attack was discovered on Monday, and that his ministry was "already handling it," along with the Israel National Cyber Bureau.

"The virus was already identified and the right software was already prepared to neutralize it," he said. "We had to paralyze many of the computers of the Israeli Electricity Authority. We are handling the situation and I hope that soon, this very serious event will be over ... but as of now, computer systems are still not working as they should."

"This is a fresh example of the sensitivity of infrastructure to cyberattacks, and the importance of preparing ourselves in order to defend ourselves against such attacks," he said. Steinitz did not say whether Israel has identified any suspects behind the attack.

The Electricity Authority is a department in the Ministry of Energy, and is a separate entity to the Israel Electric Corporation, the country's state-owned utility company.

In mid-July, the Israel's National Cyber Authority warned that the country would be targeted by a massive cyberattack.

Government ministries and security agencies were alerted to look for any changes in their computer systems, and security officials were instructed to prepare for "any possible scenario," the Israeli daily Haaretz reported.

The warning went into effect immediately and included computer systems and cellular phones, according to the report.

Over the last two years, Israel has been targeted by a number of cyberattacks. Officials estimated hackers affiliated with Hezbollah and the Iranian government were behind the infiltration attempts.

In April, members of the Anonymous hacking group defaced dozens of Israeli websites in what it warned would be an "electronic holocaust." Dubbed OpIsrael, the anti-Israel hackers targeted websites of the Israeli government and organizations, Facebook pages and gained access to personal emails. The annual attacks have thus far not caused disruption of Internet services in Israel, and failed to bring down any major governmental websites.

In response, Israel has invested resources to streamline its offensive and defensive cyber capabilities, and announced last month the establishment of a new IDF corps responsible for all such cyber activity.

Israel has also become a center of cybersecurity research and development, with multinationals from the US, Europe and Asia setting up R&D labs to develop better and more effective cyberdefense strategies and technologies.

Israeli cybersecurity firms are said to export $3 billion in knowledge, services and solutions each year, developing many of the technologies the world will need in the coming years to protect banks, infrastructure and government servers.

Jerusalem Post
Israel's electrical grid attacked in massive cyber attack (Canada).
Wednesday, 27 January 2016

Jerusalem - As Israelis cranked up their heaters during the current cold snap, the Public Utility Authority was attacked by one of the largest cyber assaults that the country has experienced, Minister of Infrastructure, Energy and Water Yuval Steinitz said on Tuesday.
"Yesterday we identified one of the largest cyber attacks that we have experienced," Steinitz said at the CyberTech 2016 conference at the Tel Aviv Trade Fair and Convention Center.

Steinitz said that attack was dealt with by his ministry and the National Cyber Bureau and that it was under control.

The incident occurred during two consecutive days of record-breaking winter electricity consumption, with the Israel Electric Corporation reporting a demand of 12,610 megawatts on Tuesday evening as temperatures dipped to below-freezing levels.

"I can tell you that the virus was identified and software was activated to neutralize it," Steinitz said. "This is a fresh example of what we need to be prepared to face at any time," he added.

Hundreds of international delegations were attending the CyberTech 2016 Conference. The third annual event drew state leaders, representatives of leading multinational and Israeli corporations and startups, investors and entrepreneurs in the field of cyber security.

A US delegation led by Homeland Security Deputy Secretary Alejandro Mayorkas, a large Japanese representation, a group of Canadian banking executives and a delegation organized by the International Monetary Fund from developing countries were among those expected to attend what is referred to as the largest exhibition of cyber technologies outside the United States.

Fox News
FBI going 'right to the source' in Clinton email probe, interviewing intel agencies
Tuesday, 26 January 2016

Byline: Catherine Herridge, Pamela Browne

Washington - The FBI is going straight to the source in its investigation of classified emails that crossed Hillary Clinton's personal server, speaking with the intelligence agencies - and in some cases, the individuals - that generated the information, two intelligence sources familiar with the probe told Fox News.

Investigators are meeting with the agencies and individuals to determine the classification level in the emails. The step speaks to the diligence with which the bureau is handling the investigation, despite the former secretary of state's claims that the matter boils down to a mere interagency dispute.

"This is not merely a difference of opinion between the State Department and the Department of Justice," one intelligence source, who is not authorized to speak on the record, told Fox News, referring to comments on the Sunday talk shows and by the Clinton campaign downplaying the FBI's investigation. "The bureau will go directly to depose specific individuals in agencies who generated the highly classified materials."

The source added, "At the end of the day it will be a paper case. Emails never disappear because computers never forget."

A former senior FBI intelligence officer, while not directly involved in the Clinton email investigation, previously told Fox News it was standard practice for the bureau to go directly to the originating source because it is cleaner and maintains the integrity of the investigation.

"You want to go right to the source," Timothy Gill Sr., a former senior FBI intelligence officer, said. "Investigative protocol would demand that."

Fox News first reported that intelligence beyond "Top Secret" known as "SAP," or "Special Access Programs," was identified in the Clinton emails on her unsecured private server. Access to SAP is restricted to only those with a "need to know" because exposure of the intelligence would likely reveal a human asset or method of collection. The findings were shared with the Senate Intelligence and Foreign Affairs committees in a Jan. 14 letter from the intelligence community inspector general.

Fox News also confirmed that at least one email contained intelligence from human spying, known as "HCS-0," which is code for highly sensitive human intelligence operations.

The FBI investigation is centered around Clinton and members of her staff to determine if they deliberatively trafficked and shared information from highly classified sources onto an unsecure private email system.

"The bureau does not waive its primacy in espionage cases," the intelligence source said, referring to USC 18 793 and 794. "The security investigation is now part and parcel with the criminal [public

corruption] investigation." The source said both tracks are being pursued "vigorously" and there is a sense of "incredulity as to what is being discovered."

Violations of US 18 Section 793 fall under "gross mishandling" of national defense information. Potential violations under Section 794, "gathering or delivering defense information to aid" a foreign government, are more serious and challenging to prove.

Howard Krongard, former inspector general of the State Department, told Fox News, "I continue to believe the question of how [and from whom] material actually got from the classified network to Hillary Clinton's server is the key to the puzzle."

It is not possible to "cut and paste" from a classified network to an unclassified system, like Clinton's personal email account, to perform what is known in intelligence circles as "jumping the gap."

Paul Sperry, a media fellow at the Hoover Institution, reported Saturday in the New York Post that Clinton and her top aides "had access to a Pentagon-run classified network that goes up to the Secret level as well as a separate system used for Top Secret communications."

Former intelligence and law enforcement officers say one of the most likely scenarios is that an individual who had access to classified information summarized it in their own words or provided details during exchanges via email, which is a criminal violation and goes against non-disclosure agreements.

"The spillage could occur by somebody basically ignoring those guidelines it would have to be that way. There's no possible way she could transfer media off of an SCI high system ... onto an unclassified server," said Dan Maguire, a special operations veteran who spent 46 years handling highly classified information and being deeply engaged on special access programs.

"I think it reflects, probably two things -- perhaps an ignorance on the part of the individuals involved who've been doing this who are trying to please their boss and don't recognize the sensitivity and how that impacts on national security, and then an element of arrogance to even think or consider that you would pass information on an unclassified file server," Maguire said.

A review of the Clinton emails has found at least 1,340 containing classified information. A State Department challenge to two emails, classified at the "Top Secret" level failed, as Fox News first reported in December. The agency that gets the information in effect owns the information, and has final say over its classification.

In its most recent statement on classified information found on Clinton's server, the Clinton campaign described the issue as an "interagency dispute."

Spokesman Brian Fallon said, "It does not change the fact that these emails were not classified at the time they were sent or received. It is alarming that the intelligence community IG, working with

Republicans in Congress, continues to selectively leak materials in order to resurface the same allegations and try to hurt Hillary Clinton's presidential campaign. The Justice Department's inquiry should be allowed to proceed without any further interference."

Wall Street Journal
The Data Breach You Haven't Heard About
Wednesday, 27 January 2016
Byline: Rep. Will Hurd
Section: oped

Op-ed - A security breach recently discovered at software developer Juniper Networks has U.S. officials worried that foreign hackers have been reading the encrypted communications of U.S. government agencies for the past three years. Yet compared with the uproar over the Office of Personnel Management breach, first disclosed last June, this recent breach has gone largely unnoticed.
On Dec. 17 the California-based Juniper Networks announced that an unauthorized backdoor had been placed in its ScreenOS software, and a breach was possible since 2013. This allowed an outside actor to monitor network traffic, potentially decrypt information, and even take control of firewalls. Days later the company provided its clients -- which include various U.S. intelligence entities -- with an "emergency security patch" to close the backdoor.

The federal government has yet to determine which agencies are using the affected software or if any agencies have used the patch to close the backdoor. Without a complete inventory of compromised systems, lawmakers are unable to determine what adversaries stole or could have stolen.

If government systems have yet to be fixed then adversaries could still be stealing sensitive information crucial to national security. The Department of Homeland Security is furiously working to determine the extent to which the federal government used ScreenOS. But Congress still doesn't know the basic details of the breach.

Yet this vital information should not be difficult to obtain. After all, U.S. banks that use this software for encryption were forced to share the extent of their use to the Securities and Exchange Commission only hours after the compromise was disclosed. It is government agencies that are dragging their feet.

This is why I and my colleagues on the House Committee on Oversight and Government Reform recently wrote a letter to the heads of 24 federal agencies demanding an inventory of their systems running the affected software, and whether or not they have installed the patch. If they fail to respond they will be called before Congress to explain why they couldn't produce this basic information -- even though the 2002 Federal Information Security Management Act requires government bodies to monitor and protect the data they possess.

Once we learn which agencies were using the faulty software, finish patching all the systems and conduct a damage assessment, we need to examine why this older version of ScreenOS, last updated in 2011, was being used in the first place. This product is considered a legacy system that many users have replaced with better technology, yet the U.S. government hadn't bothered to update to a newer, more-secure system.

Sadly, this isn't surprising. Last year, according to the U.S. Government Accountability Office, the federal government spent over $80 billion on IT procurement and 80% of those funds were for legacy systems -- outdated technology or software similar to ScreenOS. This practice of not keeping up with the times renders our nation's IT infrastructure less efficient and exponentially more vulnerable.

Finally, this incident shows that backdoors to bypass encryption -- even those requested by law enforcement or mandated by lawmakers -- are extremely dangerous. There is no way to create a backdoor that is not vulnerable to this kind of breach. Encryption is essential to our national security and economy; we should be focused on strengthening it not weakening it.

Note: Rep. Hurd, a Republican from Texas, sits on the House Homeland Security Committee and is chairman of the IT Subcommittee on Oversight and Government Reform.

US News and World Report
NSA Water, Electricity Supply Safe as 'Off Now' Push Ends in Failure
Tuesday, 26 January 2016
Byline: Steven Nelson

Washington - An effort in state legislatures across the country to pull the plug - literally - on the National Security Agency has ended in failure, with mass surveillance opponents lamenting over spineless colleagues and the national group behind the push looking to support more bite-size reforms.
The almost completely abandoned effort aimed to deny water and electricity to the spy agency following Edward Snowden's 2013 disclosures about the NSA's bulk collection of U.S. phone records and Internet surveillance programs.

Through legislation, state politicians sought to ban state and local governments from providing "material support" to the NSA, including services from public utilities. Bills in Maryland, home to the agency's Fort Meade headquarters, and Utah, location of a massive NSA data storage facility, threatened water deals with local governments that are essential to agency operations.

The ambitious legislative campaign attracted wide media coverage, but failed to achieve victory.

Former Maryland Del. Michael Smigiel, the Republican sponsor of his state's legislation, recalls five of his seven cosponsors promptly jumping ship in 2014. "I just found out the NSA is in my district," he recalls one of the men telling him.

In Utah, Rep. Marc Roberts, also a Republican sponsor, says he won't reintroduce the bill this year, concluding its failure "means people would rather give up their liberty for a little bit of security" and that there's broad skepticism about states' power to curb NSA operations.

Bills in other states - including Alaska, Arizona, Indiana, Iowa, Mississippi, Missouri, Oklahoma, South Carolina, Texas, Tennessee and Washington - also have failed. A bill in California passed, but after being made toothless.

The bills generally said states and their political subdivisions cannot supply material support to federal agencies that collect citizens' metadata without individualized warrants, and often included a ban on using evidence gathered in such a way in state courts.

Mike Maharrey, a spokesman for the Tenth Amendment Center, which crafted the model legislation used by state legislators, says the center has turned its focus toward enlisting support for privacy reforms that "aren't quite as aggressive" but still can have a "big impact up the chain."

Last year, there were more than a dozen material support-banning bills, he says. Now, he knows of just one, in Michigan, and he isn't particularly optimistic about its chances.

"There's a great deal of willingness and openness and eagerness about taking action at the state level," Maharrey says. "There obviously is an appetite for this, but we have come to realize just how powerful the law enforcement and, in the case of the NSA, the military lobby is."

Maharrey's group now is promoting draft legislation from the American Civil Liberties Union that would restrict the use of phone location-tracking Stingray devices, limit warrantless access to communications and establish state rules for drones and license plate readers. The ACLU announced last week its privacy legislation already had been introduced in 16 states.

"We're still working to figure out how to bring enough pressure from the bottom on these institutions to make them bend," Maharrey says. "We've definitely created a foundation for something we will continue into the future. We're just looking at other ways to move the ball forward."

Some sponsors of the more ambitious legislation, meanwhile, have looked to higher office. Ted Lieu, a Democrat, sponsored California's successful yet weakened bill, and was elected to Congress shortly afterward. Smigiel, who lost a low-vote legislative primary, now is seeking to knock off U.S. Rep. Andy Harris, R-Md., by running on a libertarian platform against the famously anti-marijuana lawmaker ahead of an April primary.

Smigiel says he's getting support from pot reformers and supporters of autonomy for the District of Columbia, which a Harris budget amendment barred from regulating recreational marijuana sales

despite 70 percent of district voters casting ballots for legalization. A poll Smigiel commissioned found him crushing Harris, though it also presented respondents with questions about Harris' record.

If elected to Congress, Smigiel sees himself working with fellow libertarians such as Reps. Thomas Massie, R-Ky., and Justin Amash, R-Mich., and likeminded Democrats to tackle NSA surveillance.

Though Congress passed and President Barack Obama last year signed the USA Freedom Act, ending the government's automatic bulk collection and storage of domestic U.S. call records, deeper reform, such as a ban on "backdoor" searches of Internet communications of Americans, remains stuck despite such an effort passing the House of Representatives twice.

Smigiel says he's alarmed at the lack of action from elected officials, particularly given recent revelations that members of Congress were affected by the executive branch's monitoring of Israel's campaign against the recent Iran nuclear deal.

"The result has been exactly what you see: an emboldening of the agency to continue its spying on Americans and on Congress," he says.

Reuters
South Korea says suspects North Korea may have attempted cyber attacks
Wednesday, 27 January 2016

South Korea said on Wednesday it suspected North Korea of attempting cyber attacks against targets in the South, following a nuclear test by the North this month that defied United Nations sanctions. South Korea has been on heightened military and cyber alert since the Jan. 6 test, which Pyongyang called a successful hydrogen bomb test, although U.S. officials and experts doubt that it managed such a technological advance.

"At this point, we suspect it is an act by North Korea," Jeong Joon-hee, a spokesman of the South's Unification Ministry, told a news briefing, when asked about reports that the North might have attempted cyber attacks.

Authorities were investigating, Jeong said, but did not provide further details.

Last week, South Korean President Park Geun-hye said the scope of threats from North Korea was expanding to include cyber warfare and the use of drones to infiltrate the South.

North Korea has been using balloons to drop propaganda leaflets in the South, amid heightened tension on the Korean peninsula since the nuclear test.

Since the test, there have been unconfirmed news reports that the computer systems of some South Korean government agencies and companies had been infected with malicious codes that might have been sent by the North.

Defectors from the North have previously said the country's spy agency, run by the military, operates a sophisticated cyber-warfare unit that attempts to hack, and sabotage, enemy targets.

South Korea and the United States blamed North Korea for a 2014 cyber attack on Sony Pictures that crippled its systems and led to the leaks of unreleased films and employee data.

At the time, the company was set to release the film, "The Interview", featuring a fictional plot to assassinate North Korean leader Kim Jong Un.

North Korea has denied the allegation.

In 2013, cybersecurity researchers said they believed North Korea was behind a series of attacks against computers at South Korean banks and broadcasting companies.

Times of India
Chinese investors bet big on India, internet giants pour funds into digital startups
Wednesday, 27 January 2016
Byline: Samidha Sharma & Boby Kurian

New Delhi - The drought is turning into a deluge. For years, Chinese investment in India remained a trickle -- $1.2 billion between 2000 and September 2015, which was only 0.47% of the total foreign direct investment inflow. While China became India's largest trading partner in 2008, investment flow from the country remained hostage to national security concerns.
That looks set to change significantly given the spate of announcements in the last few weeks. Wanda, China's largest commercial real estate developer, announced investment worth $10 billion in Haryana. SAIC Motor, China's largest carmaker, proposes to buy GM's Gujarat facility. About 100 small and medium Chinese enterprises have promised investments worth $1 billion.

In the startup space, Chinese companies are no more restricted to proposals, but have been making aggressive and widespread investments. The new year began with China's online travel company Ctrip picking up a strategic stake in Makemytrip and Baidu unveiling discussions with multiple Indian internet startups for investments. This comes in the backdrop of Alibaba's high profile investments in Snapdeal and Paytm last year. Another Chinese internet giant Tencent Holdings started investing when it took a wager on Bangalore-based healthcare startup Practo last year.

"Chinese internet companies have recognized the big potential in India's digital startups where there are similarities in learning curves and experiences," Frank Hancock, managing director, advisory, Barclays

said. He pointed out that the broader FDI investments have pivoted towards the east with Japan competing with the US and the UK among the top three sources of capital. "In that context, the incremental Chinese private investments are important from a signaling perspective," Hancock said.

A recent Credit Suisse report highlighted that India's internet and e-commerce journey bears close similarity with that of China, with a lag of 8-10 years. "The presence of such investors on the boards of investee companies enables access to insightful market advice and winning business models," said Anup Vikal, CFO, Snapdeal, which has attracted investments from Alibaba, Taiwan's Foxconn and Japanese telecoms & internet giant Softbank.

Besides the strategic investors, Hillhouse Capital, one of the largest China-based investment funds, picked up a stake in online classifieds player Cardekho last year, and took positions in the domestic public markets. More significant, though little known, are the investments by State Administration of Foreign Exchange (SAFE), a fully-owned subsidiary of People's Bank of China, in some of India's pedigree large cap stocks. SAFE, entrusted with managing China's estimated $3.5 trillion foreign reserves, started taking positions in Indian public equities at least two quarters back, several top bankers in Mumbai said in recent conversations.

Between January 1, 2015 and January 22 this year, investors from Asia chose 48 Indian startups to provide financial backing. The 22 companies, from countries including Japan, China, South Korea, Taiwan, Singapore and Malaysia, participated in funding rounds worth $3.4 billion in this period. Chinese companies Alibaba, Tencent, Ctrip, Didi Kuaidi, Hillhouse Capital and Tybourne (Hong Kong) were significant investors.

Most of China's cash reserves are said to be invested in dollar and euro denominated assets though it has started taking risk exposures in other geographies as well. While Chinese investor interest around Indian internet startups has gathered momentum, it is yet to translate into other sectors which the dragon has eyed for some years now.

Take, for instance, Fosun, arguably, the largest Chinese private conglomerate and the most active overseas acquirer. Fosun -- with interests spanning from pharma to real estate to internet -- started scouting for investments in India more than two years ago but hasn't struck any deals yet.

This is where some bankers forsee "the mutual dislike" between Indian and Chinese businesses, which are rooted in cultural differences and historical prejudices. "Private businesses in the two countries vary vastly, and love to look down upon each other," a senior banker said on condition of anonymity. Then there are whispers about India preferring neutral money from Japan and Canada to build its infrastructure.

Still, there isn't much doubt that China, and broadly the east, is becoming a large source of capital for new-age Indian entrepreneurs. "So far the US internet companies have had a lock on the India market. However, about a year ago, the Chinese internet conglomerates started to stitch things together in India

with strategic bets. Their approach is very long-term which bodes well for Indian startups who were dependent on very few deep-pocketed funds for writing the larger cheques," says Avnish Bajaj, MD at Matrix Partners India, an active investor in early stage tech companies like Quikr, Practo and Ola among others.

Hancock of Barclays said he would expect Chinese investors to top up their US counterparts. "I would see large Chinese private investments in the country's internet leaders which are already vetted by US venture capital and private equity funds," he explained, suggesting a slightly cautious Chinese action in a sector where Japan's SoftBank has become a prolific investor.

Outside the digital economy, bankers said, Japan has clearly signaled its intent for aggressive investments in infrastructure as it wants India to be a geopolitical counterweight to China. They, however, are counting on Chinese investments into Indian healthcare and real estate gathering steam. Mainland China's biggest property developer Wanda's fresh proposal of $10 billion investment in Haryana follows earlier announced joint ventures with Anil Ambani's Reliance Group to develop integrated townships in Navi Mumbai and Hyderabad.

As China joins Japan, Taiwan and South Korea to pump FDI into India, much depends on how its private businesses muscle up in the face of a slump after an extended economic miracle.

Globe and Mail
Scientists raise alarm over inadequate supercomputers
Wednesday, 03 February 2016
Byline: Ivan Semeniuk
Section: general

Canada's national computer capacity needs expensive and ongoing upgrades from Ottawa to provide country with the digital muscle required to operate in the world's top tier, scientists say
Scientists across Canada who need access to fast and powerful supercomputers to conduct their federally funded research say they are falling behind their international competitors, or having to switch to less ambitious projects because the country's digital research infrastructure is insufficient to meet their needs.

The problem is so acute, those affected say, that fixing it will require Ottawa to pour tens of millions more into Canada's national computer capacity each year, and rethink how the system is supported in the long term.

What's needed is not simply more data storage but also computational capacity - the ability to crunch through reams of calculations to do things like analyze genetic variants across an entire population or simulate the Earth's climate. The challenge is exacerbated by the rapid turnover of digital technology, and by growing demand from researchers anxious to leverage the power of big data and highperformance computing to make breakthroughs.

Compute Canada, the organization tasked with supporting university-based researchers with their digital needs, says that the growing reliance on computation in many areas of science means that it is no longer able to provide its biggest users with the digital muscle they need to operate in the world's top tier.

The organization projects that more modest users of its services could be running into similar barriers in the next couple of years.

Since only researchers with federal funding can apply to Compute Canada, the digital bottleneck means the government is, in some cases, paying for science that it can't support.

Meanwhile, the nation's digital infrastructure faces a coming tsunami of demand through a range of large-scale research projects that the government has already committed to.

"We're alarmed," said Compute Canada's president, Mark Dietrich.

"Important big science initiatives threaten to overwhelm our already stretched capabilities." For Peter Tieleman, a University of Calgary chemist who draws on Compute Canada's resources more than any other individual scientist to model the behaviour of cell membranes and their interactions with

molecules including candidate drugs, the limitations mean that he has to divide his projects across different computer systems and forgo investigations that simply cannot be done in Canada.

"Personalized medicine is only going to be personalized if we're able to analyze data at the level of the individual," said Dr. Tieleman, referring to a trend in medical research to tailor potential treatments for disease to a patient's unique genetic characteristics.

In recent weeks, Compute Canada has faced ire and distress from researchers over its allocation of computer resources for 2016. Many applicants received far less than expected, while others have been cut off entirely.

"It's the hardest year we've had - and last year was already bad," said Dugan O'Neil, chief science officer for the organization.

Among those whose allocation was reduced to zero is Scott Ormiston, a professor of mechanical engineering at the University of Manitoba. As a consequence, one of Dr. Ormiston's graduate students, who is developing software to reveal fluid and gas interactions in pipes - a topic that is relevant for averting nuclear accidents - may be unable to complete his PhD, already overdue because of diminished computer resources.

"I don't know what to do. All my plans are in jeopardy," said the student, Foad Hassaninejadfarahani, whose funding has now run out.

Although there is widespread agreement that Canada's research-computing and datamanagement tools need an upgrade, opinions vary about whether advanced computing is a pressing problem.

"It's not something that, today, is keeping me awake at night," said Feridun Hamdullahpur, who chairs the Leadership Council for Digital Infrastructure, a university-led group that reports to the federal government.

Dr. Hamdullahpur, who is president of the University of Waterloo, said he is not aware of any researchers on his campus who have been hampered by a lack of access to computational capacity, though he added that the future might bring such constraints.

The council, which meets Thursday in Ottawa, is scheduled to hear from Compute Canada about the organization's concerns.

Others say the problem is long standing and has already cost Canada its ability to attract top researchers in some fields.

"It's a pretty terrible situation," said Robert Thacker, a cosmologist at St. Mary's University in Halifax who uses supercomputers to study the formation of galaxies and the large-scale structure of the universe.

Dr. Thacker said the last time his group was able to publish computationally based work on par with that going on in the United States and Europe was in 2008. He added that his department recently lost its bid to attract a rising star in the field to a faculty position in part because of Canada's limited computational resources. Instead, the researcher, a Canadian scientist who was working abroad, accepted an offer in the United States.

Sabrina Foran, a spokesperson for the federal Department of Innovation, Science and Economic Development, said the government is working to develop a new digital research infrastructure strategy. A funding boost to Compute Canada was announced last year by the Conservative government in the lead-up to the federal election, but scientists say this will merely replace aging systems without adding more capacity.

Toronto Star
Shared IT agency yet to show its worth
Wednesday, 03 February 2016
Byline: Alex Boutilier
Section: general

OTTAWA -- The federal government's $1.9-billion IT department is having trouble showing if it's saving Ottawa any money and is beset with delays, according to the auditor general's report.
Shared Services Canada was created in 2012 to centralize and improve the federal government's scattered IT landscape, while cutting costs by delivering tech support centrally.

Trouble is, the department doesn't have a way of actually measuring if they're improving services or cutting costs.

"They don't really have a baseline that documents whose going to do what, what levels of services should the departments expect to have, what type of information should they expect to receive, to give them an indication of how their systems are being managed," said Auditor General Michael Ferguson.

"I think the task that they set for themselves from the beginning was ambitious and complex, so really I think it's up to them to demonstrate how they're going to meet that goal.

. . . They have a big job ahead of themselves."

Ferguson's audit found that SSC had no process to determine costs or measure progress and savings, and the agency's senior management were briefed with unclear or inaccurate reports about progress.

The auditor general's office tabled its fall 2014-15 reports to Parliament Tuesday, dealing with issues from dangerous and illegal exports slipping by border guards, the lack of progress on government considering gender-based analysis, and a series of concerning issues with the First Nations Health Authority in British Columbia.

But the issue most likely to dog the new Liberal government is the costly problems in modernizing Ottawa's technology.

SSC was created in 2012 under the previous Conservative government with a mandate to consolidate the government's IT services under one roof.

Tony Clement, the former minister responsible for Treasury Board who announced SSC's creation in 2011, declined a request for comment.

Globe and Mail
Challenges plague Ottawa's push to centralize IT services, Auditor says
Wednesday, 03 February 2016
Byline: Michelle Zilio
Section: general

OTTAWA - The federal department in charge of centralizing the government's information-technology systems has made limited progress in doing so, knocking out communications for emergency workers in Saskatchewan on one occasion, and is having trouble proving that its efforts are actually saving money, a new report by Canada's Auditor-General says.
In the report tabled in Parliament on Tuesday, Auditor-General Michael Ferguson found that Shared Services Canada, which became a department in 2012, has encountered challenges in its mandate to modernize, standardize and consolidate the e- mail, data centre and network services for 43 federal departments by 2020.

Shared Services Canada "did not set clear and concrete expectations of what departments would receive in terms of ongoing service, support and information," Mr. Ferguson said in a prepared statement. "It is also unable to accurately demonstrate cost savings achieved through the transformation of government IT services."

The report also found that Shared Services did not outline "clear and concrete expectations" for how it would deliver services and "rarely" provided enough information to departments to help them meet government IT security policies, guidelines and standards.

The department's problems were made clear in a case study from March 24, 2014, when all first responders - police, fire and emergency medical services - in Saskatchewan lost radio voice communications for 40 minutes. First responders were forced to use their personal cellphones to

communicate with each other, but reception was spotty or non-existent in some areas. The outage linked back to Shared Services, which managed the emergency radio services, and accidentally rendered a crucial feature of the radio network unavailable while making changes to the network.

Mr. Ferguson said Shared Services' problems originated with its implementation, and the department continues to struggle with ambitious and complex goals.

"They didn't put in place things like service-level agreements with the 43 departments and organizations that they provide services to," he told reporters. "So that starts them out in a situation where they don't really have a baseline that documents who's going to do what, what level of services should the departments expect to have, what type of information should they expect to receive to give them an in indication of how their systems are being managed."

New Democratic MP David Christopherson said the big question is whether the current effort to create government-wide technology can be fixed or should be scrapped.

"I would think that, given the mess that it is right now, that it may very well make more sense for them to start all over," he said.

But Public Services Minister Judy Foote said the government is committed to completing the IT transformation process by 2020.

The audit also found the department did not have consistent financial practices to prove that savings were being generated. For instance, Shared Services did not take individual departmental implementation cost estimates, ranging from $500,000 to $5-million each, into account when determining savings that would be achieved by moving to a new e-mail system.

As a part of its e-mail transformation initiative, Shared Services Canada had planned to migrate 500,000 e-mail mailboxes to the new service by the end of March, 2015. But, according to the audit, the department reported to its senior management that it had migrated only 3,000 by that date.

Speaking to reporters on Tuesday, Ms. Foote said "the cost is not the issue for us right now," as "the delivery of services is what's really important for Canadians."

Wait for disability benefits too long

Canadians with terminal illnesses and grave medical conditions are waiting too long to be approved for federal disability benefits, and a tribunal that was created to speed appeals when disability claims are denied has made the system even slower, the Auditor- General says.

Although Employment and Social Development Canada usually approves or rejects claims for Canada Pension Plan (CPP) disability benefits within an acceptable amount of time, an audit released on

Tuesday found the department's promise to take no more than 48 hours to process claims for people with terminal illnesses was being met in just 7 per cent of cases.

And just 59 per cent of people who have grave illnesses such as liver cancer, Alzheimer's disease or paranoid schizophrenia are getting their applications for benefits approved within the department's standard of 30 days, said the audit, which examined the claims-approvals process over five years ending in 2014-15.

"These are people who have worked in the Canadian work force and they've made their contributions to the CPP and this is one of the benefits that they expect to be there when they need it," Auditor-General Michael Ferguson said of those applying for disability benefits. "So the department needs to treat this as a service for people and make that whole system better."

The audit found that the application process for CPP disability benefits is extremely cumbersome - the application kit contains eight documents totalling 42 pages.

In addition, the audit said the Social Security Tribunal, which was established in 2014 to increase the speed and efficiency of the existing process for hearing appeals of rejected claims, was actually bogging things down. From 2011-12 to 2014-15, the average time an appellant waited for a decision increased from 402 days to 884 days.

When the department took a second look at 5,414 appeals that were in a backlog as of December, 2014, it overturned one-third of the original decisions. A random sample of those reversed decisions examined by the auditors found many were overturned without any substantial new evidence. The claim of one applicant was denied six times before it was approved.

The auditors said this suggests the department needs to do more to ensure its original decisions are consistent and appropriate.

Treasury Board President Scott Brison told reporters the problems unearthed by the Auditor-General apply to the actions of the previous Conservative government.

"It would be very easy for us as ministers of the current government, the new government, to simply lay blame. We're not doing that," Mr. Brison said. "We're actually taking action and are actually going to move forward, working with Canadians."

Power & Influence (a Hill Times publications)
The Public Servants: The non-partisan advisers
Wednesday, 03 February 2016
Byline: Ally Foster
Section: general

Implementing Prime Minister Justin Trudeau's grand to-do list is a hive of civil servants who will play an influential role in shaping Canadian policy, priorities, values, and history.
Newly elected Prime Minister Justin Trudeau has a grand policy to-do list. Some call it lofty, while many call it 'ambitious.' Regardless, it's going to take a lot of work to see to fruition and the bulk of the weight will fall on the public service. They're the ones providing the expertise necessary to make informed, strategic and wise policy decisions. They have the spirited and innovative thinking required for Canada to stay competitive in an increasingly fast-paced and globalized world; and are a dedicated and steadfast force to loyally implement decisions and deliver services in a timely and reliable fashion.

Here are the ones to watch in 2016, the most influential civil servants, and how they'll wield power in this new political environment.

The Deputies

A deputy minister carries a great deal of responsibility as the senior civil servant in a government department. The DM takes political direction from the appointed minister, but responsibility for the day-to- day operations, program development, budget, and employee management of the department lie with the deputy minister.

In the newly- named Department of Global Affairs, the foreign affairs file is managed by deputy minister Daniel Jean, who has held the position since late 2013 after an extensive international career in the foreign service. Working in immigration, he was posted to the U.S., Hong Kong, and Port-au-Prince twice (including during the coup that unseated Jean-Bertrand Aristide).

Mr. Jean will likely make good use of that international experience, as he faces a challenging policy agenda. The Liberal government must make tough international decisions regarding how to contribute to the fight against the Islamic State, how to properly integrate 25,000 Syrian refugees within Canada's border, deciding what kind of role Canada should have as international peacekeepers, as well as how to navigate ongoing tensions with Russia.

Mr. Jean will be working closely with Malcolm Brown, who was named special adviser to the Clerk of the Privy Council on the Syrian Refugee Initiative by Mr. Trudeau in early November, after serving as the DM of International Development.

Also within the Global Affairs department is International Trade deputy minister Christine Hogan. Ms. Hogan has been a public servant since 1988, and is valuable in that she's negotiated and led policy reforms in areas ranging from the environment and energy to international development and defence. In terms of international trade policy, Ms. Hogan will be advising the Trudeau team on issues like the Trans-Pacific Partnership, locking down the Canada-European Union trade agreement, China's ongoing push for a free trade deal, and Canada and Mexico's trade sanctions against the United States for foreign beef and pork labelling requirements.

Perhaps the DM who will face the most change under the new government, and will be given a great deal of responsibility, is Michael Martin, deputy minister at Environment and Climate Change Canada. In contrast to the previous government's lacklustre approach to sustainable environment priorities, Mr. Trudeau campaigned strongly on making Canada a steward for climate change awareness and environmental protection. Mr. Martin will be busy this year stewarding Canada's response to the recent UN climate change agreement signed in Paris.

Another filet hat will be implementing a very different policy agenda is the one managed by Colleen Swords, DM of Indigenous and Northern Affairs Canada. The Oct. 19 election was considered a landmark for Canada's Indigenous communities; a record 10 aboriginal MPs were elected, and First Nations communities experienced the highest voter turnout in history.

Mr. Trudeau promised to call a national inquiry into missing and murdered Indigenous women and girls within 100 days of being elected, improve education and clean drinking water in First Nations communities, implement all of the recommendations made by the Truth and Reconciliation Commission and a review on all Indigenous-related legislation passed by the Harper government. Ms. Swords will be front and centre of all it, helping her minister, Carolyn Bennett, on the file.

Perhaps one of the most tenured of the current crowd of deputy ministers is John Knubley, deputy minister of Industry, who has held his position in Industry Canada since September 2012. But Mr. Knubley's portfolio is about to be shaken up.

The Science, Technology and Innovation Council (STIC) released a report in 2015 stating that Canada has fallen behind its allies in recent years in terms of investing into research and development-- dropping almost $1-billion between 2006-2013. After the release of the report, Mr. Knubley told the press that there wasn't a whole lot of evidence that billions of dollars spent by the Canadian government on research tax credits and more than 70 industrial support programs have had much of an impact on industrial innovation. But going forward, he may have a government that takes a new, innovating and collaborative approach to finding creative solutions to boost industrial development in Canada.

Other deputy ministers to keep an eye on are Bill Pentney, Justice DM, who has risen through the bureaucratic ranks over the past 25 years. The former University of Ottawa professor served as the general counsel and director of legal services at the Canadian Human Rights Commission, which will be an asset considering the Liberal government's rehabilitative approach to crime. He will also be working closely with Ms. Swords on the missing and murdered Indigenous women inquiry, and will have a slew of legislative initiatives to shepherd as the Trudeau government moves ahead with the legalization of marijuana, repealing Bill C-51, the controversial Anti-terrorism Act, addressing hand gun laws and responding to the Supreme Court's decision on physician-assisted suicide.

Jean-François Tremblay, Infrastructure and Communities deputy minister since July 2015, brings experience from a previous role as deputy secretary to the Cabinet (operations) in the Privy Council

Office. Mr. Tremblay will be crucial in helping the Liberal government consult with provinces, territories, and municipalities in order to create what they call an "integrated, intermodal national transportation strategy, that serves large and small communities,"--a promise they committed to fulfilling within two years of taking office. Mr. Trudeau also said his government will develop a predictable and reliable transportation funding commitment for at least 10 years, which Mr. Tremblay will be helping to lead.

Paul Rochon, DM Finance, was appointed by Stephen Harper in April 2014--a surprise to some, as he was a veteran within the finance department and an experienced economist, but was still a newbie to the upper echelons of the bureaucracy. He had only been a deputy minister at international development for less than a year when he was shuffled into the role. Mr. Rochon, who made his mark as Canada's lead negotiator at Group of 20 finance ministers' meetings, will be tasked with implementing the new economic policies of the Liberal government, including dropping the middle income-tax bracket from 22 to 20.5 per cent as well as creating a new tax bracket: 33 per cent on income over $200,000.

On the defence file, DM John Forster will face some complex work, including what kind of military role Canada will play in the global fight against ISIS, how to fi x a procurement system that many consider broken, and how engaged Canada should be in peacekeeping efforts going forward. Mr. Forster, appointed DM of Defence in February 2015, has experience working on intricate, internationally-focused files with serious, life-and-death ramifications. Mr. Forster was shuffled from his position as the head of Canada electronic spy agency, the Communications Security Establishment.

Janice Charette was only Canada's top bureaucrat for about 15 months before the prime minister appointed Michael Wernick to the top job. It's no suprise the new government did so, as is usually the case with new incoming political masters, but she will remain a senior adviser because she's proven to indispensable as the Liberals found their feet. With a frantic post-election schedule of international travel, hiring political staffers took a backseat to the urgent matters of the day, and the Liberals leaned heavily on public servants in the early weeks. Ms. Charette accompanied Prime Minister Justin Trudeau on his first trip abroad, to the G20 in Turkey and the Asia Pacific Economic Cooperation Summit in the Philippines, and she met with him and his top advisers every day and will likely remain in a senior role.

The Security

Replacing Mr. Forster at the notoriously secret spy agency is Greta Bossenmaier, who shoulders a great deal of responsibility at a time when public scrutiny on the security of Canadians and the boundaries of surveillance are both high.

The agency monitors global data, including cyber and airwaves, for intelligence from outside Canada's border. Ms. Bossenmaier certainly has international experience, having worked as deputy minister of the Afghanistan Task Force in the Privy Council Office, and associate deputy minister of foreign affairs.

Her counterpart at the Canadian Security Intelligence Service (CSIS), Michel Coulombe, has been the director since October 2013, and was a significant appointment considering it was the first time a

director was assigned from within the service. Mr. Coulombe, a veteran who has worked as an intelligence office since 1986--just two years after CSIS was formed--has international experience, having overseen CSIS's operations abroad as assistant director of foreign collection.

Together, their plates will be loaded with high-pressure work this year. With the Liberal government committing to resettling 25,000 Syrian refugees in Canada by the end of February 2016, and in the shadow of the Paris attacks in November 2015, many Canadians have concerns about domestic security. Mr. Coulombe and Ms. Bossenmaier will be working closely with both RCMP Commissioner Bob Paulson and Richard Fadden, National Security Adviser to the Prime Minister, in their efforts to keep Canadians both at home and abroad safe.

The Diplomats

Perhaps one of Canada's best diplomats is the one we keep posted right in Ottawa: Governor General David Johnston. The former lawyer and president of the University of Waterloo is known to be well-liked and highly-respected (both by government and Canadians), and has earned a reputation for being genuine, down to earth and approachable. The GG makes himself available through Twitter interaction and Skype sessions--recently Skyping with aboriginal students from Atlantic Canada.

One of the most influential foreign dignitaries in Ottawa's diplomatic circle is the representative from Canada's closest ally, the United States. Bruce Heyman has been U.S. President Barack Obama's man in Ottawa since March 2014, but was known to have an unusually cool relationship with the former prime minister, mostly due--pundits say--to the U.S.'s refusal to approve the Keystone XL pipeline.

While Prime Minister Trudeau has voiced disappointment over President Obama's decision to reject the oil pipeline project, he also stressed that it would not hurt relations with Canada's neighbour. Meanwhile, Mr. Heyman has showed signs of excitement and optimism when asked about working with the new prime minister, singing his praise to The Canadian Press, saying: Mr. Trudeau is "a good man. He's smart, he's affable, he's caring. ... He's going to be a great representative for your country." The northern neighbours currently have a lot of mutual bilateral policies to attend to, including climate change targets, combating the threats posed by ISIL, border crossing facilitation, and regulatory harmonization.

Another major influential diplomat going forward will be Chinese Ambassador to Canada Luo Zhaohui, who is actively promoting China's economic growth and encouraging the Canadian government to boost bilateral trade and lock in a free trade agreement as soon as possible.

Keepers of the Money

Aside from the title of Auditor General of Canada, Michael Ferguson also has an unofficial and rather comical designation: the angriest man in Canada. Most photos of the man who keeps the government spending inline shows him scowling at the camera, his eyes showing skepticism and mistrust; really, a

good person to hold Parliament accountable for the spending of public funds. Auditor General since November 2011, Mr. Ferguson was appointed after working as the deputy minister of Finance of New Brunswick.

Canada's other main monetary adviser is Stephen Poloz, Governor of the Bank of Canada. Mr. Poloz provides the Canadian government analysis of the national and global economy, and makes recommendations about how to strengthen Canada's economic activity. Many observers say he will have more freedom to give transparent and honest advice under the Trudeau government. After not ruling out negative interest rates last December, Mr. Poloz will be an influential player in navigating the uncertain economic climate. One sector that was previously a major booster of the Canadian economy was energy, but with the so-called oil crash, there have been changes in that area as well.

Peter Watson, chair of the National Energy Board, will be forced to adjust to those new realities, as well as navigate a potentially tense relationship with Mr. Trudeau, who campaigned on a promise to conduct a full review of Canada's environmental assessment practices, including a reform of the arms-length regulating board.

Ottawa Citizen
Shared Services a costly failure
Wednesday, 03 February 2016
Byline: James Bagnall
Section: column

It's little wonder that so many federal government departments dislike or distrust Shared Services Canada, the computer services agency established in 2011.The portrait offered Tuesday by Auditor General Michael Ferguson in his biannual audit suggests the agency conducts its operations with a sloppy disregard for both the quality and quantity of services it provides to 43 departments.
This is all the more astonishing given Shared Services' sweeping mandate - which is to develop a single email system for the entire federal government, consolidate nearly 500 data centres to seven, and streamline the government's telecommunications services.

Although the agency has a generous annual budget in excess of $1.4 billion and more than 6,100 employees, Ferguson noted it fell well short of the standards expected by the departments it serves. Indeed, were this a private sector firm, it would have lost its customers years ago.

Among the major shortcomings:

Shared Services is running late on the implementation of its major projects, particularly the one involving email services. Ferguson noted that as of March 31, 2015 - when the email project was originally meant to be finished - only 3,000 out of more than 500,000 mailboxes had migrated to the new Canada.ca form. And just 100 out of 15,600 applications to new data centres had been upgraded.

¦¦ Shared Services has claimed that consolidating information technology will produce significant savings but failed to note the significant implementation costs borne by the various federal departments it works with. Of the departments surveyed by Ferguson, the unaccounted costs ranged from $500,000 to $5 million per department - and this was related just to the common email project. ¦¦Although Shared Services was launched nearly five years ago, only now has it committed to let its 43 "partner" departments know how it will actually deliver computer infrastructure services. Its selfimposed deadline is Dec. 31, 2016. ¦¦The auditor general sampled 50 out of 3,000 business arrangements signed with departments about what services Shared Service will provide and discovered "none

SHARED SERVICES FROM A1 BY THE of the agreements contained commitments to fulfil and report on security expectations."

The latter point is especially revealing. Over the next few years, Shared Services is meant to help departments migrate more than 15,000 applications - ranging from human resources to accounting - to the proposed new data centres. From the departments' point of view, this is an opportunity to upgrade software and run things more efficiently.

However, Ferguson's auditors discovered the service level agreements did not actually spell out the responsibilities for Shared Services or its partners. Not only that, they concluded, the agreements "were used mainly to recover costs for services that were deemed new or optional and therefore not covered by funds already appropriated from partners for information technology services." In short, Shared Services was looking after its own priorities.

Shockingly, Shared Services provided reports to partner departments for just 10 per cent of the agreements and even these did not cover all the services committed to by the agency.

Indeed, the profile that emerges from Ferguson's audit is of a relatively young federal agency whose raison d'être is customer service - but which doesn't appear to have a clue what that means.

The Liberal government, asked Tuesday about the agency's failure, said simply that Shared Services, created under the Conservatives, was "not set up to succeed." Public Services and Procurement Minister Judy Foote pledged, without detail, stronger leadership. jbagnall@postmedia.com

NUMBERS

2012 Year Shared Services Canada was established with a mandate to consolidate the federal government's sprawling IT assets.

43 Number of partner agencies and departments for SSC.

$209M Yearly savings SSC claims to be responsible for.

$1.9B Amount Shared Services Canada spends each year.

485 Number of data centres SSC is supposed to consolidate (to just seven) by 2020.

Globe and Mail
Where privacy and security intersect, will police and intelligence (finally) work together?
Wednesday, 03 February 2016
Byline: David Omand
Section: oped

Concerns that two of Canada's intelligence agencies, the Canadian Security Establishment (CSE) and the Canadian Security Intelligence Services (CSIS), broke the rules by sharing intercepted data with Canada's allies, will further spur public debate about how to strengthen public oversight and accountability mechanisms for Canada's intelligence gathering agencies. Since the revelations of Edward Snowden that authorities can access personal communications from mobile devices and computers, the public the world over has become sensitized to issues of online privacy.
At the same time, terrorist atrocities have continued. The murder in Burkino Faso of six Quebeckers along with many others follows the 2015 Paris attack on journalists working for Charlie Hebdo, on a Jewish synagogue, on British and other European tourists murdered on a Tunisian beach, the downing of a Russian airliner, the Bataclan theatre massacre in Paris, and the San Bernardino killings. The Internet is filled with ultra-violent jihadi images from Syria. Criminal activities of human traffickers result in refugees being drowned trying to reach Europe. Every week brings new cyber attacks on our financial system and infrastructure. Presidents Assad and Putin remind us of the dangers that authoritarian regimes can pose.

The year 2016 must be one of reconciliation in which democracies work out a social compact to allow their authorities lawfully to obtain the digital intelligence needed to keep us safe and secure, but under strong safeguarding norms of proper behaviour towards information on the Internet that ensure respect for our rights to privacy and free speech. One norm should be to have independent judicial and parliamentary oversight of intelligence activity towards which Canada seems to be moving under the leadership of Ralph Goodale, Minister of Public Safety. Another norm should be commitment by nations to do nothing that might weaken the security of the systems upon which the Internet relies and might reduce our confidence in it as a secure medium to do business.

An interesting early test case is the United Kingdom. The U.K. Parliament has now embarked on scrutiny of a comprehensive Investigative Powers Bill placing all forms of digital intelligence gathering by the British authorities, inside and outside the country, under the rule of law, providing for judicially approved warrants after examination of the necessity and proportionality of the case for the activity, and strengthening oversight. It does not include "back-door" provisions to weaken encryption, which the intelligence agencies did not ask for, but powers are sought to have Internet communications records retained for a year by the companies. A question still to be answered is how far the Internet

companies (many of course giant American corporations) will co- operate with governments like the U.K. to provide the police and intelligence agencies with information on the communications of their suspects. Not all companies may for commercial and technical reasons feel able to retain the data that long, but most I suspect want to help the fight against terrorism and serious crime, such as child abuse, but only with a clear legal route as provided for in the U.K. Bill.

The U.K. government seems to have taken to heart the judgments of the British Courts and other independent reviews that GCHQ (the British partner of CSE) does conduct all its activities within U.K. law, but the way the law was being applied in the past was, to put it mildly, obscure to the public. A U.K. court therefore ruled the British government had not met the proper standard of the rule of law, under which citizens must be able to understand how the law bears on them. The comprehensive bill now under parliamentary scrutiny is the result, a gold standard in terms of transparency.

We will need to wait to see whether police and intelligence agencies working under such strict conditions, and with both parliamentary and judicial oversight, can actually acquire the pre-emptive intelligence needed to keep the public safe and secure. Previous generations of intelligence officers might have doubted this was possible. I know that the present generation of intelligence leadership is determined to make it work. For all our sakes, we must hope they succeed.

Sir David Omand is a former director of GCHQ, the UK signals intelligence and cyber security agency.

Australian Associated Press
Hackers could be behind phone threats
Wednesday, 03 February 2016
Byline: Jacqueline Le
Section: general

Melbourne - Threatening phone calls to schools across Australia could be the work of teenage hackers using online programs to make untraceable calls and create computer-generated voice messages. They could also be the work of criminals, but authorities remain tight-lipped about their investigations, even as schools across Australia on Wednesday received threatening phone calls for the fourth time in a week.

Schools in Queensland and NSW also received threatening phone calls again on Wednesday.

Victoria Police are investigating whether some may have originated from a selective Melbourne school, but a technology researcher says someone could have falsified the call origin to make it look like it had come from Nossal High School.

Not much is publicly known about the calls other than they are automated, and threatening.

"We don't know who is behind it, or what tools they are using," University of Melbournehacking researcher Suelette Dreyfus told AAP on Wednesday.

"We don't know anything about them, if they're in Australia or overseas."

It's possible an account on an online phone service may have been hacked and used to make the calls.

A hoax of this nature and scale suggests whoever is behind it has good technology skills, Dr Dreyfus says.

"I'm surprised at how rapid-fire these calls are - to so many different places, and in such a short amount of time - and how it's affecting so many children," she said.

But each time a hoax call is made, the perpetrator risks exposing information about themselves or their location.

"If the hackers or hoaxers have been bad about their operational security, then I think it might be a relatively short time before police are knocking on their doors," Dr Dreyfus said.

"But if they've been very good about it, it could be quite some time."

Since Friday, an undisclosed number of schools in Australia and overseas have received threatening phone calls, which have prompted emergency evacuations.

"The question is, are these guys real criminals, are they teenage hackers who are hoaxing people?," Dr Dreyfus said.

"Either way, they're causing a lot of stress to parents who are probably very worried about the safety of their children."

Last Friday an automated message warned schools a bomb was on their premises, and on Tuesday the threats were either about a bomb, or that shooting would occur.

The principal of Berwick Lodge Primary in Melbourne - which received a threatening phone call on Friday - said if disruption is the aim, it is working.

"We come to work wondering whether the next call is going to be one of these threats," Henry Grossek said.

"We're mentally exhausted."

New York Times
Deal Struck to Balance U.S.-Europe Data Fears

Wednesday, 03 February 2016
Byline: Mark Scott
Section: general

New York - European officials on Tuesday agreed to a deal with the United States that would let Google, Amazon and thousands of other businesses continue moving people's digital data, including social media posts and financial information, back and forth across the Atlantic.
With billions of dollars of business potentially at stake, the data-transfer deal was the result of more than three months of often tense negotiations between United States and European Union policy makers, who have clashed over what level of privacy individuals can expect when companies and government agencies follow ever-expanding digital footprints.

Part of the challenge is balancing individuals' privacy concerns with national security obligations, particularly in light of mounting fears about international terrorism.

The agreement announced on Tuesday aims to address those privacy concerns and strike that balance by including written guarantees by the United States -- to be reviewed annually -- that American intelligence agencies would not have indiscriminate access to Europeans' digital data when it is sent across the Atlantic. Whether that provision will reassure privacy-rights groups remains to be seen.

Many obstacles still await the deal, which must be officially approved by the European Union's 28 member states. National data protection regulators have yet to give their support to the pact, and European privacy-rights advocates are preparing to file legal challenges seeking to overturn it.

The data-transfer agreement, replacing a 15-year- old pact that Europe's highest court struck down in October, is intended to let the free flow of digital data -- the lifeblood of many global businesses -- continue as usual.

In seeking to ensure the continued free flow of data, the deal announced on Tuesday could especially benefit big American companies like Google, Facebook and Amazon that tend to dominate Internet searches, social media and digital commerce in Europe. But it is also meant to let nontech companies like the drug maker Pfizer and the industrial conglomerate General Electric continue to send customer and employee data between the United States and Europe.

Europe's privacy watchdogs had demanded that European and American officials agree to a new deal by Jan. 31. Although negotiators missed that deadline, they had been meeting almost continuously in Brussels since Sunday to reach an agreement. They were driven by a sense of urgency, as industry executives and trade bodies on both sides of the Atlantic worried that the means for transferring data between two of the world's largest economies remained in jeopardy.

Most sensitive, perhaps, were provisions demanded by the European Commission, the executive arm of the European Union, aimed at limiting how American intelligence agencies collect data on Europeans when companies send their personal information to the United States.

The American negotiators, in response, agreed to provide the annual written assurances.

These guarantees, European officials said, will be reviewed each year, with American and European policy makers meeting to ensure that the strict privacy rights of Europe's more than 500 million citizens are respected by United States agencies.

"We will hold the U.S. accountable on the commitments that they have made," Vera Jourova, the European Union's justice commissioner who has led the negotiating team, said on Tuesday.

The new deal "is a major achievement for privacy and for businesses on both sides of the Atlantic," Penny Pritzker, the United States Commerce secretary, said in a statement on Tuesday. "It provides certainty that will help grow the digital economy."

Both sides will now spend the next two weeks completing the details of the new pact, which is to be called the E.U.-U.S. Privacy Shield. If formally approved, it would go into effect by early April.

But the deal's first hurdle comes on Wednesday, when Europe's increasingly powerful national privacy agencies plan to pass their own judgment on how data can be safely transferred outside the European Union.

Many of these agencies, which can investigate and issue fines to companies that they suspect of misusing people's digital information, remain skeptical that rules protecting Europeans' data will be upheld in the United States. And some of these monitors have said that they will support further restrictions on how companies can move the data if they suspect it may be misused.

"We are part of the game," Isabelle Falque-Pierrotin, France's privacy chief, said in an interview last month in Paris. "If you provide these services, then you have to protect people's privacy rights."

Ms. Falque-Pierrotin is the chairwoman of the Pan-European body that will announce its assessment on Wednesday.

The agreement drew praise on Tuesday from DigitalEurope, a group representing trade associations and multinational tech companies doing business in Europe, including Apple, Google and Microsoft.

John Higgins, the group's director general, called in a statement for national privacy agencies "to view this signal from the European Commission as a sign of good faith and to hold off with any potential enforcement action until the new agreement has been fully implemented."

Privacy groups, though, expressed concern that the data- transfer deal does not comply with European law, which views an individual's right to privacy almost on par with freedom of expression.

Several consumer groups have said that they will file complaints with European privacy agencies to challenge the new agreement, while others have called on the United States to improve its own privacy laws to match those currently available in Europe.

"The problem is that the U.S. remains unchanged," said Marc Rotenberg, president of the Electronic Privacy Information Center in Washington.

Despite these expected challenges, some European officials on Tuesday defended the new safe harbor agreement.

In particular, the European Commission highlighted how the United States had proposed greater oversight on the access American intelligence agencies have to Europeans' data.

The United States also agreed to establish an ombudsman in the State Department to act as a first point of contact for Europeans if they believed American government agencies had misused their data.

Access granted to American intelligence agencies had become a sticking point in light of revelations by Edward J. Snowden, the former NationalSecurity Agency contractor, about that agency's surveillance of foreign citizens.

During the most recent talks in Brussels, which involved officials from the United States Commerce Department and the Federal Trade Commission, among others, American negotiators had argued that United States law provided greater oversight and supervision of American intelligence agencies' use of personal data than rules now in place across the European Union, according to several officials who spoke on the condition of anonymity because they were not authorized to speak publicly.

National security arguments had become more vehement following the terrorist attacks in Paris last November, those officials said. United States ambassadors had defended the integrity of oversight of American intelligence agencies in discussions with senior politicians in countries like France, Germany and Britain in recent weeks, according to the officials who asked to remain anonymous.

But European Commission, which does not have the power to rule on its member states' national security practices, had demanded written guarantees.

"This isn't going to be a one-off decision by the commission," said Ms. Jourova, the European justice commissioner. "We have achieved effective protection of Europeans' rights."

London Times

Drones will spy from the stratosphere
Wednesday, 03 February 2016
Byline: Deborah Haynes
Section: general

London - Britain will buy the world's first highaltitude drone to spy from the stratosphere for months at a time.
The solar-powered Zephyr aircraft will be used by special forces and regular soldiers as part of a £2 billion boost to intelligence-gathering capabilities, defence sources said. The Ministry of Defence is to spend £10.6 million on two prototypes to be built in the UK. Test flights are expected next year.

"They will be able to fly higher and for longer to gather constant, reliable information over vast areas," Michael Fallon, the defence secretary, said The aircraft flies at 70,000ft, twice the height of a commercial airliner, but weighs only 30kg (66lb). The Zephyr, which travels at about 30mph (48km/h), is called a high altitude pseudo-satellite because it is a cross between a drone and a satellite.

It holds the record for the longest flight -- 14 days -- for an unrefuelled aircraft and could remain airborne for months thanks to its solar batteries.

It carries communications equipment that will enable soldiers standing 400 miles apart to talk via radio. Cameras will provide unprecedented continuous coverage of terrain.

The programme has been developed by Airbus Group in Farnborough. Its design is so commercially sensitive that even the blueprint for the two propellers on its front is top secret.

Press Trust of India
Password-stealing 'dorkbot' prowling in Indian cyberspace
Wednesday, 03 February 2016
Section: general

New Delhi - Cyber security sleuths have alerted Indian internet users against the malicious activity of an online virus called 'dorkbot' which perpetrates itself through social networking sites and steals sensitive personal data and passwords of a user.
The malware, a variant of online virus and worm, has been specifically seen affecting operating systems running on Windows in the recent past. "It has been observed that the variants of malware named as 'dorkbot' targeting windows operating systems, are spreading.

"The malware belongs to the family of worms having backdoor functionality and spreads through various vectors including drive-by-download attacks, social networking sites and compromised websites with browser exploits via removable drives in the form of auto-run exploits or by means of malicious

links in instant messaging chats or internet relay chats," a latest advisory issued by the Computer Emergency Response Team of India (CERT-In) said.

The CERT-In is the nodal agency to combat hacking, phishing and to fortify security-related defences of the Indian Internet domain.

The deadly virus, with almost a dozen aliases, is capable of stealing sensitive information from infected machine including stored passwords, browser data, cookies and has a smart and lethal potential to take complete control of the affected system, it said.

Christian Science Monitor
Hard lessons emerge from cyberattack on Ukraine's power grid
Wednesday, 03 February 2016
Byline: Jack Detsch
Section: general

Boston - A cyberattack linked to a December blackout in Ukraine signals new dangers for critical infrastructure operators such as power suppliers and other utilities, experts said Monday.
The fact is that many supervisory control and data acquisition (SCADA) systems - the type compromised in the Ukrainian attacks and utilized at countless other power facilities - aren't designed to be secure against digital attacks, said security researcher Peiter Zatko, also known by his hacker nom de gare Mudge.

"They were designed to be in isolated environments that don't talk with the outside world," said Mr. Zatko. "You didn't want these to be connected to the Internet."

Zatko spoke at an event Monday cosponsored by Passcode and Harvard University's Belfer Center for Science and International Affairs to further explore the Ukraine cyberattack that many experts believe led to power outages for some 80,000 customers in the western region of Ivano-Frankivsk for nearly six hours.

The incident has sent shockwaves throughout the critical infrastructure sector in the US and beyond, and follows recent reports of hackers linked to Iran breaching networks at a dam outside Rye, N.Y., and at the major power supplier Calpine Corp. Renewed concerns about digital threats to the power grid have also led the Pentagon's Defense Advanced Research Projects Agency (DARPA) to devote $77 million to helping utilities defend against and recover from future cyberattacks.

A former security researcher at DARPA, Zatko said that many critical infrastructure companies have simply ignored security patches for industrial networks and that often companies making software for these facilities aren't security conscious enough. "The developers writing the code aren't thinking about security."

It also appears that Ukrainian facilities involved in the attack weren't following industry guidelines that could prevent hackers from gaining access to essential systems. Reuters recently reported that power utilities in Ukraine ignored their own rules regarding "air gaps" - separating critical control systems from the Internet - before December's attack.

Analysts still aren't certain of the exact timeline of the Ukraine attack. But according to research from SANS Institute, a nonprofit that specializes in cybersecurity training, attackers breached SCADA systems at the facilities, deployed malware to infect and damage servers, and attacked call centers at the utilities with a distributed denial of service attack.

Oleh Sych, a consultant to Ukrainian government officials investigating the attack, told Reuters that hackers probably used phishing e-mails designed to trick power operators into clicking on malicious documents, thus allowing them access to the network.

The cybersecurity intelligence firm iSightPartners said the group behind the attack could be connected to the Russia-linked Sandworm Team, which conducts cyberespionage operations. While many experts agree that the cyberattack led to the power outage, there's still no consensus about how the hackers actually shut down parts of the power grid.

"We've never had to deal with a cyberattack against the grid that took the power down," said Robert M. Lee, chief executive officer of Dragos Security and an instructor for the SANS Institute, who participated in the Monday event. "If [the US power grid] was ever impacted in more than one region, we couldn't recover that easily."

In a survey of 500 security leaders at critical infrastructure firms conducted by TrendMicro and the Organization of American States in 2015, 53 percent of responses indicated that attacks had increased over the past year. But despite the uptick in reports of breaches into utilities, experts said on Monday that cyber threat intelligence in the critical infrastructure sector has not improved much - as has been the case with companies in other industries.

"The thing that bothers me is that we're not looking into those environments," said Lee. "It's not trivial to take down the power grid."

Minnesota Public Radio (MPR)
Group sues feds for documents on Minnesota counterterrorism program
Wednesday, 03 February 2016
Byline: Mukhtar Ibrahim
Section: general

Minneapolis - A New York-based advocacy group is suing two federal agencies over a controversial counterterrorism program focused on Muslim communities in several states, including Minnesota. The Brennan Center for Justice at New York University School of Law said it went to court to challenge the United States Justice Department and Department of Homeland Security after exhausting other efforts to get records on the Countering Violent Extremism program, or CVE.

The Justice Department in 2014 launched CVE pilots in Minneapolis, Los Angeles and Boston, calling it a way to bring religious and community leaders and law enforcement officials together to counter efforts by ISIS and other terror groups to recruit fighters in the U.S.

Some Minnesota Muslims have questioned the pilot's intent and raised concerns that it's simply a way to gather intelligence. U.S. Attorney for Minnesota Andrew Luger, who leads the CVE program in Minnesota, has told his Somali community task force he would not use the program that way.

Brennan Center officials say they began asking federal authorities more than a year ago for documents on the CVE program detailing its policies, procedures, funding and constitutional safeguards. They said they received some documents related to the Los Angeles and Boston programs, but none about Minnesota.

The group is particularly troubled about efforts in the Twin Cities "to use CVE to monitor Somali-American children in school," said Brennan Center attorney Michael Price.

"Our concern here is that the current iteration of CVE will have some negative impacts on Muslim communities including stigmatization, reinforcing Islamophobic stereotypes, facilitating covert intelligence gathering and suppressing decent," Price said.

Luger's office declined comment on the lawsuit.

It's unclear if there are rules prohibiting law enforcement agencies from gathering intelligence from Muslim communities, Price said. With the lawsuit, he added, the center is trying to determine the rules governing the government's participation in the CVE program and how the program operates.

In a report to lawmakers released Monday, the Department of Public Safety outlined several strategies that it said will guide a "successful approach in Minnesota to counter radicalization and terrorist recruitment."

The agency recommended collaboration with schools and establishing programs that would identify individuals who are "on the path to violent extremism."

"These programs may identify reliable and consistent sources to make referrals such as schools, places of worship, social workers, or doctors; divert those who have begun the process of radicalization and

may be on the path to violent extremism; and provide an opportunity for such individuals to transition back into mainstream society within their community," the report said.

DPS also calls on training community members to identify youth who may be at risk for recruitment.

In St. Paul, the police department has its own CVE effort focused on Minnesota's East African community. It recently received a $100,000 grant from the State Homeland Security Program, which funds state programs focused on terrorism prevention.

Many efforts in countering violent extremism have largely relied on the idea that it's possible to identify people on the verge of becoming radicals, but there's no "typical trajectory that a person follows to become a terrorist," Price said.

"What teenager isn't a little disaffected or exhibits signs of alienation?" he added. "I think that describes most teenagers."

Times of Israel
In cyber car hacks, loose lips can kill, says expert
Wednesday, 03 February 2016
Byline: David Shamah
Section: general

Jerusalem - With a crowded playing field in the cyber-security business, companies and experts seek ways to stand out. For cyber experts, that often means being the first to discover a new virus, security breach, or other hole that needs to be plugged up.
That's the way the business is supposed to work, said Yoni Heilbronn of Israeli Internet of Things security firm Argus; but there are rules.

"You can't go public with a vulnerability without informing the company that has the security breach, so they can repair it," he said on the sidelines of last week's CyberTech 2016 event in Tel Aviv. "If you do reveal the weaknesses of a device or system without giving the team responsible a chance to mitigate it, you could be putting the money or even lives of people at risk. It's not just unethical - it's dangerous."

Especially in the business Argus deals with - the connected car business. With more vehicles than ever connected to the Internet - either through an in-vehicle communications system or via a connection to a driver's smartphone - the opportunities for hackers to mess with cars is greater than ever.

Argus has developed a solution that analyzes communication packets (the segments of data) that come into and go out of the vehicle, determining if the packets are associated with the kind of behavior expected (e.g., signals from specific IP addresses, commands that make sense given the current activity

of the vehicle, etc.). Suspect connections can be blocked or traced, preventing hackers from remotely grabbing control of a vehicle's steering or braking system.

Argus supplies car manufacturers, their Tier 1 suppliers and aftermarket connectivity providers with ready-to-embed technology that can be seamlessly integrated into any vehicle product line for any connected vehicle anywhere in the world without changes to the vehicle's architecture, said Heilbronn. Among the company's customers are some of the top Tier 1 auto part and component suppliers, like Lear Electronics, Delphi, Bosch, and others.

That such remote vehicle hacking is possible was proven beyond a shadow of a doubt last July, when white-hat hackers Charlie Miller and Chris Valasek took control of a Chrysler Jeep vehicle being driven at top speed by Wired journalist Andy Greenberg. Miller and Valasek turned the radio on full- blast, ran the air-conditioner, and even took control of the accelerator - scaring Greenberg to the point where he was forced to "drop any semblance of bravery, grab my iPhone with a clammy fist, and beg the hackers to make it stop."

Heilbronn doesn't know if Miller and Vaselek informed Chrysler in advance of what they were going to do or how they were planning to do it. But one person who did not reveal his intentions to a targeted company was Corey Thuen of Digital Bond Labs, who Progressive Insurance said did not inform it of a security flaw in a dongle it distributed to insured drivers to report on their on-road driving habits and behavior, qualifying them for a safe driving discount. After finding a security flaw in the dongle, he went public.

Contacted by business magazine Forbes for comment, Progressive said that "if an individual has credible evidence of a potential vulnerability related to our device, we would prefer that the person would first disclose that potential vulnerability to us so that we could evaluate it and, if necessary, correct it before the vulnerability could be exploited. While it's unfortunate that Mr. Thuen didn't share his findings with us privately in advance, we would welcome his confidential and detailed input so that we can properly evaluate his claims." Forbes noted that Thuen told them that he tried to reach the dongle's manufacturer Xirgo in advance, but received no response.

In any event, there's a right way and a wrong way to reveal cyber-safety problems, and Argus "would never reveal things in that manner, out of concern for the safety of the public," said Heilbronn. And Argus has a great deal of opportunity to do the right cyber-thing. "There are only a handful of companies in the world doing cyber-security for connected cars, and we are the biggest one," he said.

The company has been in touch with any number of manufacturers and Tier-1 suppliers about security issues; in 2014, for example, it revealed a problem with a connected-car solution made by Zubie, which, upon hearing of the problem, immediately dealt with it - and it was only then that Argus told the story.

"Once we detected Zubie's security gap we duly notified Zubie with full details of our findings as required by our responsible disclosure policy," said Heilbronn. It's not about reputation or profits, but about keeping hackers from pushing the envelope too far.

"Very often we will hear about hackers who tried to duplicate exploits that were tried and succeeded," said Heilbronn. "When it comes to money or identity theft, as painful as that is, it usually does not put the lives of people at risk; with all the hassle involved, banks and other institutions are insured, so the public, while inconvenienced, usually gets compensated. In hacking of connected vehicles, things are different - and any exploit that succeeds could end up endangering the lives of drivers and others who are on the road with them.

"Who knows if any of the many car accidents that take place each year are the result not of failed brakes and the like, but of hacking?" added Heilbronn. "There are a lot of dangerous people out there - hackers, hacktivists, criminals, and terrorists - who are potentially capable of doing this. By 2020, there will be as many as 400 million connected vehicles on the road - meaning that there will a lot more hacking opportunities. We should not be giving these people material to work with."

Bloomberg View
Europe's New 'Privacy Shield' Looks Leaky
Wednesday, 03 February 2016
Byline: Noah Feldman
Section: column

Column - The European Union and the United States reached a new deal Tuesday on privacy protections for Europeans' data that gets sent to U.S. servers. The agreement, to be called Privacy Shield, replaces an agreement repudiated by the European Court of Justice in October. That's good news for major corporations like Facebook and Google that want continued access to their European users' data. But the new agreement requires scrutiny itself, which European regulators and probably the ECJ are going to give it. Notwithstanding the powerful business interests at stake, there's reason to think that the agreement may have loopholes that make it difficult for those bodies to uphold.

The arrangement from 2000, called Safe Harbor, was struck down by the ECJ essentially on the ground that American companies were giving the National Security Agency access to Europeans' data. The question before the European court was whether data transferred to the U.S. receives an "adequate level of protection" under the EU's Data Protection Directive.

The answer was no -- and for complicated reasons. The court acknowledged that under U.S. law, statutory and constitutional requirements trumped the Safe Harbor agreement. It went on to say that, based on the revelations of former NSA contractor Edward Snowden, the level of privacy protection provided in practice by the U.S. wasn't high enough to satisfy European standards. The agreement was therefore rejected.

It's crucial to realize that the ECJ judgment included the recognition that, under EU law, it's all right for a government to peek at consumers' private data under some circumstances. What the court was saying, was that U.S. law wasn't protective enough to satisfy European standards. It looked to a judgment by the High Court of Ireland, holding said that "the revelations made by Edward Snowden had demonstrated a 'significant over-reach' on the part of the NSA and other federal agencies."

In particular, the Irish court was concerned that European citizens "have no effective right to be heard" by U.S. courts if the privacy of their data is breached by security agencies because the breach takes place in secret.

The ECJ had to admit that EU law doesn't contain "a definition of the concept of an adequate level of protection." But it concluded that adequacy must mean "a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union."

In other words, if U.S. privacy protection was weaker than EU protection, the agreement must be invalidated. The new agreement must be assessed against this background to see if it will pass legal muster.

The highlight of the deal, emphasized by the European Commission in its announcement, is what's supposed to be "written assurance" from the U.S. that Europeans' data will be protected. Under the agreement, the U.S. director of national intelligence will certify that Europeans' data won't be subject to "mass surveillance." That sounds better than the old agreement, which didn't include an explicit promise from the intelligence community.

But the DNI will almost surely be able to make this promise in very general terms. And, in practice, even targeted American surveillance might still be much broader and less privacy-protecting than anything European countries typically allow. The U.S. says it will review data proportionately, which means something specific in Europe but could well mean something different in the U.S.

What's more, under U.S. law, there's ordinarily little or no protection for data belonging to foreigners so long as it's outside the U.S. That law hasn't changed. It seems at least possible that the NSA might simply try to target Europeans' data before it gets transferred to the U.S. If it's doing so covertly, no one will know about it to complain.

Another provision of the new agreement creates an ombudsman for Europeans to raise data privacy concerns. This is presumably intended as a means of recourse and to satisfy the Irish court's worry about secrecy. But he or she probably won't have access to the U.S.'s secret interpretations of law or secret surveillance.

A further provision says that U.S. companies must agree to robust privacy protections before transferring data. That should probably keep them from voluntarily transferring data to the NSA in violation of privacy regulations. But if U.S. law requires the transfer, they'll still have to comply.

All this means is that there's plenty of room for the ECJ to find that Privacy Shield is inadequate like its predecessor. But will it?

That depends in part on how strongly the EU rates its negotiating position. No one in the European political elite really wants to give up on Facebook or Amazon. And no EU bureaucrat really thinks the U.S. will change its national security laws to please the EU.

The new agreement is a pragmatic compromise meant to preserve legal formality and the fig leaf of data privacy without upsetting national security either for the U.S. or for European intelligence services that might like a chance to see their own citizens' data.

The ECJ may not want to upset this delicate balance. In that case, it can assess the new agreement generously. That would solve the practical problem. Bu the disparity between European and American conceptions of privacy will remain.

The Guardian (London)
Google to divert extremist searches to anti-radicalisation websites
Wednesday, 03 February 2016
Byline: Ben Quinn
Section: general

London - Users of Google who put extremist-related entries into the search engine are to be directed towards anti-radicalisation links under a pilot programme, MPs have been told by an executive for the company. The initiative, aimed at countering the online influence of groups such as Islamic State, is running alongside another pilot scheme designed to make videos posted by extremists easier to identify. The schemes were mentioned by Anthony House, senior manager for public policy and communications at Google, who was appearing alongside counterparts from Twitter and Facebook at a home affairs select committee hearing on countering extremism. "We should get the bad stuff down, but but it's also extremely important that people are able to find good information, that when people are feeling isolated, that when they go online, they find a community of hope, not a community of harm," he said.

All three were challenged by MPs about the extent of their companies' roles in combating the use of social media by groups such as Isis for propaganda and recruitment purposes.

Committee chairman Keith Vaz asked how many people are in the sites' "hit squads" that monitor content. He was told Twitter, which has 320 million users worldwide, has "more than 100" staff. The Facebook and Google executives did not give a number.

Simon Milner, Facebook's policy director for UK and Ireland, Middle East, Africa and Turkey, said that the site has become a "hostile place" for Isis: "Keeping people safe is our number one priority. Isis is part of that, but it's absolutely not the only extremist organisation or behaviour that we care about." He added that Facebook recognised from research that people did not typically get radicalised exclusively online - rather, it was a combination of real-world and online contact - and was working as a result with groups in society such as Imams.

The three were also questioned about the thresholds they apply on notifying authorities about terrorist material identified by staff or users. Labour MP Chuka Umunna asked: "What is the threshold beyond which you decide ... that you must proactively notify the law enforcement agencies?"

House and Milner said their threshold was "threat to life", while Nick Pickles, UK public policy manager at Twitter, told the MPs: "We don't proactively notify. Because Twitter's public, that content is available, so often it's been seen already."

Pickles also stressed that decisions on whether to notify account holders that they were under investigation were "context specific" and insisted that Twitter worked with authorities to ensure that they do not disrupt investigations.

London Daily Telegraph
Google to deliver wrong search results to would-be jihadis
Wednesday, 03 February 2016
Byline: David Barrett
Section: general

London - Jihadi sympathisers who type extremism-related words into Google will be shown anti-radicalisation links instead, under a pilot scheme announced by the internet giant.
The new technology means people at risk of radicalisation will be presented with internet links which are the exact opposite of what they were searching for.

Dr Anthony House, a senior Google executive, revealed the pilot scheme in evidence to MPs scrutinising the role of internet companies in combating extremism.

"We are working on counter-narratives around the world. This year one of the things we're looking at is we are running two pilot programmes," said Dr House.

"One is to make sure these types of views are more discoverable. The other is to make sure when people put potentially damaging search terms into our search engine they also find these counter narratives."

Governments and other agencies have recognised the importance of "counter-narratives" in combating extremism online - such as propaganda videos by Islamic State of Iraq and the Levant, also known as Isis- by encouraging moderate Muslims or other groups to challenge terrorist ideologies.

Dr House told the Commons' home affairs select committee that Google removed 14 million videos from its YouTube site in 2014 for a range of reasons including terrorist content and for breaking other rules.

The company received 100,000 "flags" from members of the public about content they consider inappropriate.

Nick Pickles, from Twitter, said the micro-blogging site has taken down tens of thousands of violent extremist accounts in the last 12 months.

Twitter, which has 320 million users, employs "more than 100" people working in teams to deal with inappropriate use of the site, he said.

Keith Vaz MP, the committee chairman, asked Dr House and Simon Milner, of Facebook, how many people they employed in "hit squads" to remove terrorist and extremist material.

However, both companies declined to reveal figures publicly.

A Google spokeswoman said the pilot project referred to by Dr House would bring up counter-narrative messages in "AdWords" - the sponsored links which are returned at the top of a Google search - and not the search results themselves.

Dr House said later: "We offer Google AdWords Grants to NGOs so that meaningful counter-speech ads can be surfaced in response to search queries like 'join Isis'."

USA Today
Congress shouldn't force encryption 'backdoors,' says key House Democrat
Tuesday, 02 February 2016
Byline: Erin Kelly
Section: general

Washington - Congress is unlikely to pass legislation to force U.S. tech companies to build "backdoors" into encrypted devices to allow the government to gather information on suspected terrorists, the senior Democrat on the House Intelligence Committee said Tuesday.
"I don't think a legislative solution at this point is feasible or even desirable," Rep. Adam Schiff, D-Calif., told reporters at a breakfast hosted by the Christian Science Monitor.

Schiff said he would prefer that lawmakers work with the tech industry to try to come up with solutions. He said it makes little sense to force American companies to let the government break the encryption that keeps their customers' data private when terrorists and criminals can just turn to products made by foreign companies.

"I think the encryption issue is really a global challenge," he said.

Congress is struggling with how to handle the complex issue in the wake of last November's attacks in Paris, where investigators believe that some of the terrorists used encrypted phone apps to communicate via the "Dark Web."

Senate Intelligence Committee Chairman Richard Burr, R-N.C., and Vice Chair Dianne Feinstein, D- Calif., have indicated that they will introduce legislation that would require tech companies to provide a backdoor into encrypted communication when law enforcement officials obtain a court order to investigate a specific person.

Companies such as Apple and Google -- responding to consumer demands for privacy -- have developed smart phones and other devices with encryption that is so strong that even the companies can't break it. Silicon Valley opposes any effort by Congress to mandate backdoors into encryption, warning that it would have the unintended result of making Americans more vulnerable to hackers and identity thieves.

"I think that's going to be very tough to move forward with," Schiff said of the proposed Senate bill. "At present, we really lack a consensus (in Congress)."

House Homeland Security Committee Chairman Michael McCaul, R-Texas, and Sen. Mark Warner, D-Va., are offering an alternative bill that would create a commission made up of tech industry executives, law enforcement and intelligence officials, college professors and other experts to try to come up with recommendations.

"I think a commission is fine, but it may be a bit redundant," Schiff said.

Schiff and House Intelligence Committee Chairman Devin Nunes, R-Calif., have already asked the National Academy of Sciences to issue a report on whether it is technologically possible to come up with ways for law enforcement and intelligence agencies to conduct legitimate investigations without sacrificing privacy or opening the door to hackers.

As terrorist groups such as the Islamic State increasingly use social media to recruit new members, the U.S. government needs to turn to outside groups to help fight back on Twitter and other sites, Schiff said.

"The area where we have really fallen down is in the area of countering the message (from terrorists)," he said. "The government is the wrong messenger."

Instead, the government should turn to "more credible sources" within the Muslim community who can talk to people about what Islam really stands for and how the terrorists have perverted the religion's message, Schiff said.

"The government can't respond to 20,000 tweets from ISIS," he said. "We need the help of millions of Muslims."

Schiff also said he doesn't believe Congress will repeal a controversial provision of the Patriot Act anti-terrorism law that is set to expire next year.

Lawmakers are considering whether to change or repeal Section 702 of the law, which allows the National Security Agency to target the communications of people in other nations and capture the content of e-mails, instant messages, Facebook messages, web browsing history, and more without a warrant. Although it targets foreigners, it also sweeps up the data of Americans with whom they communicate even if the Americans aren't suspected of any wrongdoing.

Last year, Congress voted to approve the USA Freedom Act, which ended the NSA's mass surveillance of Americans' phone records under Section 215 of the Patriot Act. But Schiff said Section 702 is seen as much more effective at catching terrorists than the phone metadata program ever was.

"Section 702...has been very consequential," Schiff said. "The case for it is much stronger."

The House Judiciary Committee on Tuesday was scheduled to hold a closed session on the issue.

Les Echos
Une cybercriminalité de plus en plus professionnelle
Wednesday, 03 February 2016
Byline: Julie Le Bolzer
Section: general

Non identifié - L'année a été marquée par la professionnalisation de la cybercriminalité.
Avec la montée en puissance d'un djihad 2.0, le développement d'un marché de la vulnérabilité informatique et l'émergence d'une cyberdiplomatie.

Il innove, se diversifie, se globalise... Bref, le cybercrime se porte bien. Que ce soit dans le secteur bancaire (détournement de transactions), dans le Web (piratage d'applications), dans l'environnement matériel (prise de contrôle à distance d'une voiture ou encore d'un fusil) et même dans l'espace (interceptions de données émises par un satellite), l'année passée a eu son lot d'attaques astucieuses, toujours plus créatives...

Des équipes de spécialistes

« Les attaques n'émanent plus d'individus isolés, il s'agit d'équipes de spécialistes. Nous sommes face à des cybercriminels de plus en plus performants et de plus en plus connectés entre eux : ils multiplient les interactions et partagent leurs expertises », précise Alain Juillet qui fut directeur du renseignement de la DGSE puis responsable de la cellule Intelligence économique à Matignon, aujourd'hui président du Club des directeurs de sécurité des entreprises (voir l'interview sur lesechos.fr).

Un business très rentable

Par ailleurs, les cyberattaques semblent toujours plus rentables pour les hackers. Illustration que les criminels n'oeuvrent pas seulement pour la beauté du geste mais aussi et surtout à des fins mercantiles, « leurs gains ont atteint des sommets en 2015 : jusqu'à plusieurs dizaines de millions d'euros » , pointe Fabien Cozic, directeur d'enquêtes chez Red Team. « Les entreprises doivent prendre conscience que le risque cyber est celui qui peut leur coûter le plus cher : plus cher qu'un incendie, qu'un échec de lancement de produit, qu'une erreur comptable... » insiste Alain Juillet.

Le cyber-risque est désormais intégré par une majorité d'organisations et les conséquences d'une attaque sont scrutées avec attention... et sur le long terme. « L'attaque qui a frappé l'entreprise américaine Target remonte à décembre 2013, pourtant les conséquences les plus importantes ne se font jour que maintenant, constate le colonel Eric Freyssinet, chef de la division de Lutte contre la cybercriminalité au pôle judiciaire de la Gendarmerie nationale. D'où la nécessité de prévenir, c'est-à-dire être conscient des risques, de mettre en oeuvre les moyens de s'en prémunir, de se préparer à gérer l'incident et à en maîtriser les conséquences. » Une autre grande tendance s'est dégagée l'an passé : le développement d'un véritable marché des « zero-day » (voir encadré) et, plus globalement, du commerce de l'exploitation de la vulnérabilité informatique, comme l'a souligné le Clusif dans son « Panorama 2015 de la cybercriminalité » .

100.000 tweets quotidiens

La tragique actualité a fait apparaître un autre phénomène : le rôle fondamental d'Internet et des réseaux sociaux dans les diverses attaques qui ont notamment touché la France. « A des attaques ter

roristes djihadistes terrestres, des vagues de cyberattaques font quasiment toujours échos », observe-t-on à la Direction centrale de la police judiciaire (DCPJ). Ce fait n'est pas nouveau : dans son panorama daté de 2004, le Clusif alertait déjà sur le fait que la Toile était utilisée par les terroristes. « Là où la donne change, c'est que Daech s'est entouré de spécialistes de la communication, des médias, de la vidéo et des réseaux sociaux : plus de 100.000 tweets émaneraient actuellement chaque jour de djihadistes », souligne François Paget, secrétaire général du Clusif. La cybercriminalité est aussi géopolitique. Un exemple avec le cas récent de piratage de l'Office de gestion du personnel américain (OPM), qui concernait les données personnelles de plus de 20 millions d'agents du gouvernement américain. Rendue publique en juillet 2015, cette attaque a été attribuée à la Chine par les Etats-Unis. « Les deux pays se sont alors retrouvés autour d'une table pour ne´gocier et trouver un terrain d'entente :

arrestations d'hackers en Chine, de´finition de lignes de bonne conduite sur le commerce... Cela en termes tre`s diplomatiques », souligne Loïc Guézo, cybersecurity strategist chez Trend Micro Inc.

Enfin, 2015 a vu se confirmer le risque lié aux objets connectés (lire l'interview ci-dessous). Mais dans ce domaine, le pire pourrait être à venir : le volume d'objets connectés ne va cesser de croître. Surtout, ils devraient être rejoints très bientôt par les objets autonomes qui pourraient, à leur tour, nous surprendre avec de nouveaux risques et de nouvelles formes d'attaques.

Washington Post
National Security Agency plans major reorganization
Tuesday, 02 February 2016
Byline: Ellen Nakashima
Section: general

Washington - The National Security Agency, the largest electronic spy agency in the world, is undertaking a major reorganization, merging its offensive and defensive organizations in the hope of making them more adept at facing the digital threats of the 21st century, according to current and former officials.
In place of the Signals Intelligence and Information Assurance directorates, the organizations that historically have spied on foreign targets and defended classified networks against spying, the NSA is creating a Directorate of Operations that combines the operational elements of each.

"This traditional approach we have where we created these two cylinders of excellence and then built walls of granite between them really is not the way for us to do business," said agency Director Michael S. Rogers, hinting at the reorganization -- dubbed NSA21 -- that is expected to be publicly rolled out this week.

"We've gotta be flat," he told an audience at the Atlantic Council last month. "We've gotta be agile."

Some lawmakers who have been briefed on the broad parameters consider restructuring a smart thing to do because an increasing amount of intelligence and threat activity is coursing through global computer networks.

"When it comes to cyber in particular, the line between collection capabilities and our own vulnerabilities -- between the acquisition of signals intelligence and the assurance of our own information -- is virtually nonexistent," said Rep. Adam B. Schiff (Calif.), the ranking Democrat on the House Intelligence Committee. "What is a vulnerability to be patched at home is often a potential collection opportunity abroad and vice versa."

But there have been rumblings of discontent within the NSA, which is based at Fort Meade, Md., as some fear a loss of influence or stature.

Some advocates for the comparatively small Information Assurance Directorate, which has about 3,000 people, fear that its ability to work with industry on cybersecurity issues will be undermined if it is viewed as part of the much larger "sigint" collection arm, which has about eight times as many personnel. The latter spies on overseas targets by hacking into computer networks, collecting satellite signals and capturing radio waves.

"The NSA21 initiative will ensure the National Security Agency continues to be the preeminent signals intelligence and information assurance organization in the world," said Jonathan Freed, director of strategic communications at the NSA. "These core missions are critical as we position NSA to face complex and evolving threats to the nation. Out of respect for our workforce, we cannot comment on any details or speculation before the plan is announced."

The change comes about a year after the CIA did its own revamping, ending divisions that have been in place for decades and creating new centers that team analysts with operators. The NSA's new directorate of operations also will place analysts with operators.

Rogers in a speech in December characterized the change as "among the most comprehensive" at the NSA since the late 1990s. He began the effort about a year ago, giving a team of employees from across the agency what he called the "director's charge." Among the major questions they were asked were: How can the agency better innovate?

And how "do we inculcate collaboration and integration" in operations?

For instance, said one former U.S. official familiar with the plan, both information assurance and foreign intelligence gathering rely on similar processes for data analysis and depend on each other. "But the challenge is they are very much two different cultures," the official said. "Unless you've worked on both sides of the house, you don't inherently trust each other."

The Information Assurance Directorate (IAD) seeks to build relationships with private-sector companies and help find vulnerabilities in software -- most of which officials say wind up being disclosed. It issues software guidance and tests the security of systems to help strengthen their defenses.

But the other side of the house at NSA, which looks for vulnerabilities that can be exploited to hack a foreign network, is much more secretive.

"You have this kind of clash between the closed environment of the sigint mission and the need of the information assurance team to be out there in the public and be seen as part of the solution," said a second former official. "I think that's going to be a hard trick to pull off."

Richard George, a former technical director for the IAD, said he saw how techniques that the defense side developed have helped the offense and vice versa. "It's got to be really useful to have those groups

closer together where they'll be sharing ideas and techniques more frequently," said George, now a senior cyber adviser at Johns Hopkins University's Applied Physics Lab.

Former NSA director Michael V. Hayden undertook one of the other major reorganizations, creating the Signals Intelligence Directorate (SID) in 2000 by merging two directorates -- Operations and Technology. He said he opted not to fold in the IAD,. "From the outside perspective," he said, "I needed an organization that was, and was seen to be, committed to defense."

At the time, he added, IAD needed to be strengthened and adapted to the cyber age. "Keeping it separate allowed me more direct visibility into that," he said. "That said, as the cyber mission matured, the operational and technological aspects of the SID and IAD missions merged more and more."

By 2005, as cyber threats were growing, Hayden decided to create a new organization that would enable the agency to leverage the intelligence it was getting from spying on overseas networks to help it defend against intrusions into the government's classified networks. The National Threat Operations Center (NTOC) was an experiment in combining offense and defense. "It was wildly successful," the first former official said.

NTOC dispelled the myth, the official said, that one person cannot operate under two sets of legal authorities -- offensive and defensive. "I can actually sit at my desk and one minute be using sigint data and authorities .?.?. and the next minute I could be using IA data and authorities and my mission is not changing," the official said. "You need checks and balances. You need to know what authority you're using at any given time, but it's possible."

Still, some congressional aides briefed on the broad outlines of the plan have expressed concern about mixing funding for intelligence activities and funding for cybersecurity activities.

One area where the sigint side is ahead of information assurance is in using big data analytic tools to manipulate large volumes of information quickly. "What we want to do is take advantage of that knowledge, to apply it as needed to the IA analysis," the first former official said.

Under the reorganization plan, there also will be separate directorates of Capabilities and of Research.

"One of the fundamental tenets you'll see us outline as we try to position NSA for .?.?. the environment I think we're going to see five, 10 years from now is a much more integrated approach to doing business," Rogers said at the Atlantic Council. "I don't like these stovepipes of SID and IAD. I love the expertise. And I love when we work together. But I want the integration to be at a much lower level, and much more foundational."

Le Droit
Services partagés Canada Loin de remplir ses objectifs, selon le Vérificateur général
Wednesday, 03 February 2016
Byline: Paul Gaboury
Section: general

Ottawa - Services partagés Canada a fait peu de progrès à l'égard de son plan visant la transformation des services informatiques de 43 ministères fédéraux. De plus, il a mal géré la sécurité des systèmes et est incapable de prouver les économies que ses initiatives doivent générer.
Dans un rapport déposé mardi, le vérificateur général du Canada, Michael Ferguson, soutient que le ministère, qui a un budget annuel de près de 2 milliards$, a fourni peu d'information sur le rendement des services et la sécurité de l'infrastructure.

«Tous les partenaires consultés ont souligné que le manque de rapports sur la sécurité les préoccupait parce qu'ils restent responsables de la sécurité globale de leurs programmes et de leurs services», écrit le vérificateur général.

Le ministère a aussi de la difficulté à calculer le total exact des économies, puisqu'il n'a pas pris en compte les coûts assumés par les autres ministères pendant la transition vers les nouveaux services. «Par conséquent, le total des économies financières réalisées par le gouvernement reste en grande partie inconnu», note M. Ferguson.

Peu de progrès

L'audit a révélé que peu de progrès ont été réalisés dans la transformation des services de courriels. À la fin mars 2015, environ 3000 boîtes de courriels avaient été transférées au nouveau service, alors qu'il avait été prévu qu'à cette date, plus de 500000 boîtes devaient l'être.

De plus, 436 des 485 centres de données étaient toujours en activité, alors que la cible était de réduire le nombre à sept d'ici 2020. Enfin, 100 des quelque 15600 applications avaient été transférées aux nouveaux centres de données, et seulement 300 des 23400 serveurs avaient été éliminés.

Illustration(s) :

La Presse Canadienne

All Africa
Anonymous s'attaque aux sites de Daech
Tuesday, 02 February 2016
Byline: Journaliste maison

Section: general

Madrid - Les hackers entravent l'enquête de la police espagnole sur un jihadiste marocain
Le collectif Anonymous a entravé une enquête de la Guardia civil espagnole sur un présumé jihadiste marocain par ses attaques lancées contre les sites web de l'organisation terroriste « Daech » .

Selon les médias espagnols, les attaques de ces hakers contre les sites web à caractère jihadiste après les attentats de Paris en novembre dernier, ont compliqué l'enquête des forces de sécurité espagnoles sur un Marocain suspecté d'être en relation avec l'Etat islamique.

Mais en dépit de tout cela, a précisé Europa Press, ces dernières ont pu appréhender Salim (A) en décembre dernier.

Selon la même source, ce natif au Maroc, âgé de 32 ans et qui dirige une sandwicherie à Pampelune (commune de la communauté de Navarre en Espagne), était le jour des attentats terroristes de Paris en train de suivre avec d'autres personnes un match de foot entre l'Espagne et l'Angleterre quand son téléphone portable a commencé à recevoir des informations sur ce qui se passait en France. Il a donc changé de canal « rapidement » mais il n'a pu s'empêcher de manifester sa joie à propos de ce qui advenait.

En trois ans seulement, il est passé du partage de la musique rap via les réseaux sociaux à leur utilisation pour diffuser sa vision du terrorisme et en faire l'apologie. La même source a indiqué que le changement a été également physique, car Salim porte depuis sa radicalisation une barbe version jihadiste.

Il partageait avec d'autres personnes des vidéos contenant des discours des jihadistes, des exécutions, des attentats et entraînements militaires. Mais la goutte qui a fait déborder le vase, a consisté en le fait qu'une personne non identifiée utilisait l'ADSL du local dirigé par Salim pour chercher des informations sur l'aéroport de Bruxelles et des hôtels à Antalya en Turquie.

Ce qui a incité les experts de la Guardia civil à renforcer leur surveillance et à acquérir l'intime conviction que Salim avait pour tâche d'embrigader et de recruter des jihadistes.

Par ailleurs, le journal espagnol El Pais a affirmé il y a quelques jours que 16 jihadistes marocains ayant résidé dans la péninsule ibérique sont morts en Syrie.

Il s'agit d'Ismael Afalah, Hakim Benajiba, Redouane Ben Sbih, Abdelaziz Chamout, Nourredine El Metoubi, Bilal El Helka, Abdelaziz El Morabet, Abdellah Mustapha El Sharif, Mustapha Ennassar, Mohamed Katoubi, Mustapha Oulguor, Ayoub Tribak, Jawad Taufik, Haj Tabbai, Mouhsine Mechihdan et Youssef Monbriktob.

La même source a également indiqué que 9 Espagnols d'origine marocaine ont trouvé la mort dans des combats en Syrie, affirmant que 139 combattants ont quitté l'Espagne pour rallier les groupes terroristes

en Syrie et en Libye dont 26 d'entre eux sont retournés au pays alors que 15 autres ont été emprisonnés.

Yonhap News Agency
S. Korea holds National Security Council meeting
Wednesday, 03 February 2016
Section: general

South Korea held a National Security Council meeting Wednesday to deal with North Korea's planned rocket launch, an official said.
Cheong Wa Dae, South Korea's presidential office, plans to announce South Korea's position at 8:30 a.m., presidential spokesman Jeong Yeon-guk told reporters.

Jeong said Tuesday that South Korea is taking necessary measures over the North's planned launch of a long-range rocket.

The North has notified U.N. agencies that it will launch an Earth observation satellite sometime between Feb. 8-25, confirming concerns that the communist nation is readying for a banned long-range rocket launch just a few weeks after its fourth nuclear test.

Yonhap News Agency
S. Korea taking necessary measures over N.K. rocket launch plan: Cheong Wa Dae
Wednesday, 03 February 2016
Section: general

South Korea is taking measures necessary to cope with North Korea's planned launch of a long-range rocket, Cheong Wa Dae said Tuesday.
Presidential spokesman Jeong Yeon-guk made the remark to Yonhap News Agency, saying the country is "keeping a close eye on moves related to North Korea's long-range missile launch."

The North has notified U.N. agencies that it will launch an earth observation satellite Feb. 8-25. That confirmed the concern that the communist nation is readying for a banned long-range rocket launch just a few weeks after its fourth nuclear test.

Yonhap News Agency
Two Aegis destroyers to monitor N. Korea's missile launch
Wednesday, 03 February 2016
Section: general

South Korea's military has put two of its three Aegis destroyers on a mission to detect and track North Korea's missile as the communist country appears to be gearing up for a long-range missile launch, a military source said Wednesday.
The North has informed international maritime, aviation and telecommunication agencies that it will launch a rocket to put satellite 'Kwangmyongsong' into orbit, taking a preparatory step to launch a long-range missile.

The outside world denounces the satellite launch as a pretext for testing a ballistic missile, which the North is developing in defiance of the United Nations Security Council.

"The military has increased the number of Aegis destroyers from one to two in preparation against the possibility of North Korea's long-range missile," the military official said.

Now, one is standing by in the Yellow Sea and the other is waiting in the waters south of Jeju Island, the official said.

Special features of the Navy's destroyers equipped with the U.S.-developed Aegis Combat System include a multi-function radar system that can detect ballistic missiles coming from some 1 kilometer away.

It took 54 seconds for the Sejong the Great Aegis destroyer to catch North Korea's long-range missile launched in December 2012.

The locations of the two deployed warships are meant to track the first and second stages of North Korea's multi-stage missile when it is launched.

Along with the destroyers, South Korea has also given a mission to the early warning and control aircraft 'Peace Eye' and the anti-ballistic radar 'Green Pine' as the country is bracing for the missile launch, according to other officials.

Reuters
North Korea tells UN agencies it plans satellite launch
Wednesday, 03 February 2016
Section: general

North Korea told U.N. agencies on Tuesday it plans to launch a satellite as early as next week, a move that could advance the country's long-range missile technology after its fourth nuclear test on Jan. 6. News of the planned launch between Feb. 8 and Feb. 25 drew fresh U.S. calls for tougher U.N. sanctions already under discussion in response to North Korea's nuclear test. State Department spokesman John Kirby said the United Nations needed to "send the North Koreans a swift, firm message."

Pyongyang has said it has a sovereign right to pursue a space programme by launching rockets, although the United States and other governments worry that such launches are missile tests in disguise.

"We have received information from DPRK regarding the launch of earth observation satellite 'Kwangmyongsong' between 8-25 February," a spokeswoman for the International Maritime Organization, a U.N. agency, told Reuters by email.

The International Telecommunication Union, another U.N. agency, told Reuters North Korea had informed it on Tuesday of plans to launch a satellite with a functional duration of four years, in a non-geostationary orbit.

It said the information provided by North Korea, whose official name is the Democratic People's Republic of Korea, was incomplete, and that it was seeking more details.

U.S. officials said last week that North Korea was believed to be making preparations for a test launch of a long-range rocket, after activity at its test site was observed by satellite.

The White House said on Tuesday that any satellite launch by North Korea would be viewed as "another destabilizing provocation." U.S. Assistant Secretary of State Daniel Russel, the senior U.S. diplomat for East Asia, told reporters it "argues even more strongly" for tougher U.N. sanctions.

Russel said a launch, "using ballistic missile technology," would be an "egregious violation" of North Korea's international obligations.

He said it showed the need "to raise the cost to the leaders through the imposition of tough additional sanctions and of course by ensuring the thorough and rigorous enforcement of the existing sanctions."

Russel said negotiations were "active" at the United Nations and that the United States and North Korea's main ally China "share the view that there needs to be consequences to North Korea for its defiance and for its threatening behaviours."

"Our diplomats are in deep discussion in New York about how to tighten sanctions, how to respond to violations," he said.

Asked about China's cautious response to U.S. calls for stronger and more effective sanctions on Pyongyang and Beijing's stress on the need for dialogue, Russel said:

"Yet another violation by the DPRK of the U.N. Security Council resolution, coming on the heels of its nuclear test, would be an unmistakable slap in the face to those who argue that you just need to show patience and dialogue with the North Koreans, but not sanctions."

White House spokesman Josh Earnest said China had "unique influence over the North Korean regime" and added: "we ... certainly are pleased to be able to work cooperatively and effectively with the Chinese to counter this threat."

Earlier on Tuesday, China's envoy for the North Korean nuclear issue arrived in the capital Pyongyang, the North's KCNA news agency reported.

North Korea last launched a long-range rocket in December 2012, sending an object it described as a communications satellite into orbit.

Western and Asian experts have said that launch was part of an effort to build an intercontinental ballistic missile.

North Korea has shown off two versions of a ballistic missile resembling a type that could reach the U.S. West Coast, but there is no evidence the missiles have been tested.

Pyongyang is also seen to be working to miniaturise a nuclear warhead to mount on a missile, but many experts say it is some time away from perfecting such technology.

North Korea said it successfully tested a hydrogen bomb last month but this was met with scepticism by U.S. and South Korean officials and nuclear experts. They said the blast was too small for it to have been a full-fledged hydrogen bomb.

Jakarta Post
Police to probe terrorist propaganda videos
Wednesday, 03 February 2016
Section: general

Police have said they will investigate several propaganda videos allegedly circulated by the Islamic State (IS) group via the internet.
Several videos had been brought to the attention of the police, National Counterterrorism Agency (BNPT) chief Comr. Gen. Saud Usman Nasution said on Tuesday, adding that the force would study them to gauge their authenticity and provenance.

Saud said the police's cybercrime division would handle the investigation, as it was not under the BNPT's jurisdiction. "They have a special team. It's not under our remit, but the remit of the police," Saud said on Tuesday as quoted by kompas.com.

The videos in question appear to contain threats, in Indonesian, against police and government officials. The security officers believe that the videos were released by IS.

The extremist group also recently released a threatening video to the Malaysian government, which is currently stepping up operations to detect and detain suspected IS-affiliated individuals.

As previously reported by The Straits Times, in a video in the Malay language, the Malaysia-Indonesia IS unit -the Katibah Nusantara - said it would take revenge for the capture of its members.

Entitled "Mesej Awam Kepada Malaysia" (A Public Message for Malaysia), the video warns: "If you catch us, we will only increase in number, but if you let us be, we will draw closer to our goal of bringing back the rule of the caliphs."

Washington Post
The British want to come to America -- with wiretap orders and search warrants
Friday, 05 February 2016
Byline: Ellen Nakashima, Andrea Peterson

Washington - If U.S. and British negotiators have their way, MI5, the British domestic security service, could one day go directly to American companies like Facebook or Google with a wiretap order for the online chats of British suspects in a counter-terrorism investigation.
The transatlantic allies have quietly begun negotiations this month on an agreement that would enable the British government to serve wiretap orders directly on U.S. communication firms for live intercepts in criminal and national security investigations involving its own citizens. Britain would also be able to serve orders to obtain stored data, such as emails.

The previously undisclosed talks are driven by what the two sides and tech firms say is an untenable situation in which foreign governments such as Britain cannot quickly obtain data for domestic probes because it happens to be held by companies in the United States. The two countries recently concluded a draft negotiating document, which will serve as the basis for the talks. The text has not been made public, but a copy was reviewed by The Washington Post.

The British government would not be able to directly obtain the records of Americans, if a U.S. citizen or resident surfaced in an investigation. And it would still have to follow the country's legal rules to obtain warrants.

Any final agreement will need congressional action, through amendments to surveillance laws such as the Wiretap Act and the Stored Communications Act.

Senior administration officials say they have concluded that British rules for data requests have "robust protections" for privacy and that they will not seek to amend them. But British and U.S. privacy advocates argue that civil liberties safeguards in Britain are inadequate.

The negotiating text was silent on the legal standard the British government must meet to obtain a wiretap order or a search warrant for stored data. Its system does not require a judge to approve search and wiretap warrants for surveillance based on probable cause, as is done in the United States. Instead, the home secretary, who oversees police and internal affairs, approves the warrant if that cabinet member finds that it is "necessary" for national security or to prevent serious crime and that it is "proportionate" to the intrusion.

If U.S. officials or Congress do not seek changes in the British standards, "what it means is they're going to allow a country that doesn't require independent judicial authorization before getting a wiretap to continue that practice, which seems to be a pretty fundamental constitutional protection in the United States," said Eric King, a privacy advocate and visiting lecturer in surveillance law at Queen Mary University of London. "That's being traded away."

Senior administration officials said that they are seeking to relieve the pressure on U.S. companies caught in a "conflict of laws." The United States bars American firms from providing intercepts to anyone but its government after U.S. law enforcement has obtained a court order. Britain wants to directly compel the production of the data and has already passed legislation to make that happen.

To obtain stored emails, a foreign government must rely on a mutual legal assistance treaty (MLAT) by which the country makes a formal diplomatic request for the data and the Justice Department then seeks a court order on its behalf -- a process that is said to take an average of 10 months.

"This has been an issue with the U.K. and other countries for a number of years," said one senior administration official, who like several others spoke on the condition of anonymity to discuss the negotiations. "Because of technological changes, the U.K. can no longer access data in the U.K. like they used to be able to, and more and more, U.K. nationals -- including criminals in their country -- are using providers like Google, Facebook, Hotmail. The more they are having challenges getting access to the data, the more our U.S. providers are facing a conflict of laws."

Administration officials and officials from several tech firms said the stakes are high if no agreement is reached.

They fear that if the trend continues, more foreign governments will force U.S. firms to host their data in those countries -- a practice known as "data localization." They also fear passage of laws, like the one in Britain that has not yet been enforced, requiring foreign firms doing business in their country to comply with their surveillance orders, even if the orders conflict with U.S. law.

"We're reaching a moment where the status quo is no longer workable," said an official at a major tech firm. "We're concerned about the mounting frustration and the inability of foreign governments, including the U.K., to receive responsive data in law enforcement investigations in a timely manner."

Up to now, he said, U.S. firms have "held their ground" when pressured to turn over data or conduct wiretaps in conflict with U.S. law. "Increasingly, that's not something we'll be able to do," he said.

Last week, the White House gave the State Department the green light to begin the formal negotiations. Officials stressed that they were in the very early stages of the talks, which probably will go on for months. They said they will seek to ensure that any agreement protects civil liberties.

But Gregory Nojeim, senior counsel at the Center for Democracy & Technology, a Washington-based privacy group, said: "I'm very concerned that this agreement could represent a dumbing down of surveillance standards that have always pertained in the United States. Enabling foreign governments to conduct wiretapping in the United States would be a sea change in current law. I don't see Congress going down that road."

Senior administration officials said that the goal is to help a close ally investigate serious crimes -- something that the United States has a shared interest in.

One potential example: London police are investigating a murder-for-hire plot, and the suspects are using Hotmail to communicate, and there's no connection to the United States other than the fact that the suspects' emails are on a Microsoft server in Redmond, Wash. Today, the police would have to use the MLAT process and wait months.

"Why should they have to do that?" said the administration official. "Why can't they investigate crimes in the U.K., involving U.K. nationals under their own laws, regardless of the fact that the data happens to be on a server overseas?"

Jennifer Daskal, a national security law professor at American University and a former Justice Department official, said before U.S. firms are asked to turn over data, they should be assured that the legal standard for the request is sufficiently high. It need not mimic precise U.S. standards, she said, but should at least require that requests be targeted, subject to independent review and privacy protections that weed out irrelevant information. If not in the agreement, Congress should mandate requirements, said Daskal, who is part of a coalition of privacy groups, companies and academics working on the issue.

A second administration official said that U.S. officials have concluded that Britain "already [has] strong substantive and procedural protections for privacy." He added: "They may not be word for word exactly what ours are, but they are equivalent in the sense of being robust protections."

As a result, he said, Britain's legal standards are not at issue in the talks. "We are not weighing into legal process standards in the U.K., no more than we would want the U.K. to weigh in on what our orders look like," he said.

British Home Office officials declined to comment directly on the talks. "We are clear about the need for law enforcement and the security and intelligence agencies to have the powers they need in the digital age, subject to strict safeguards and world-leading oversight arrangements," a representative said in a statement to The Post.

The agreement is intended to be reciprocal, so that the U.S. government could directly request wiretaps or stored data of a British provider as long as the target is American and not a British citizen.

The Independent (UK)
British government to fight UN ruling that it 'arbitrarily detained' WikiLeaks founder
Friday, 05 February 2016
Byline: Lizzie Dearden

London - The British Government is fighting a United Nations ruling that accused it of "arbitrarily detaining" Julian Assange in violation of his fundamental human rights.
The UN Working Group on Arbitrary Detention called on the UK and Sweden to immediately end the WikiLeaks founder's "deprivation of liberty" and compensate him.

But a spokesperson for the British Government said it would "formally contest" the findings and denied that Mr Assange's stay at the Ecuadorian Embassy in London constituted arbitrary detention.

"This changes nothing. We completely reject any claim that Julian Assange is a victim of arbitrary detention," he added.

"The opinion of the UN Working Group ignores the facts and the well-recognised protections of the British legal system.

"He is, in fact, voluntarily avoiding lawful arrest by choosing to remain in the Ecuadorean embassy."

The spokesperson said that as a rape allegation against Mr Assange is still being investigated in Sweden and subject to a European arrest warrant, the UK has a legal obligation to extradite him.

Britain is also not subject to the 1954 Caracas Convention, meaning it does not have to recognise diplomatic asylum.

"We are deeply frustrated that this unacceptable situation is still being allowed to continue," the Government spokesperson added.

"Ecuador must engage with Sweden in good faith to bring it to an end.

"Americas Minister Hugo Swire made this clear to the Ecuadorean Ambassador in November, and we continue to raise the matter in Quito."

When the findings were leaked on Thursday, Mr Assange said he would leave the Embassy if the panel ruled against him and accept arrest by British police.

"However, should I prevail and the state parties be found to have acted unlawfully, I expect the immediate return of my passport and the termination of further attempts to arrest me," he said in a statement.

Swedish prosecutors want to question him over allegations of rape stemming from a working visit he made to the country in 2010, when revelations made by WikiLeaks on the Iraq and Afghanistan wars were reverberating around the world.

But Mr Assange fears Sweden will extradite him to authorities in the US where he could be put on trial over the publication of thousands of classified military and diplomatic documents.

He has consistently denied the rape allegations but refused to return to Sweden and eventually sought refuge in the Ecuadorean embassy in London, where he has lived since June 2012.

Bloomberg View
Silicon Valley Should Join the War on Terrorism
Friday, 05 February 2016
Byline: Senator John McCain

Comment - Islamic State and other terrorist groups espouse a primitive ideology and rely on medieval tactics, but they use distinctly modern tools: social media and communications platforms designed to evade our most advanced efforts to fight terrorism.
By taking advantage of widely available encryption technologies, terrorists and common criminals alike can carry out their agendas in cyber safe havens beyond the reach of our intelligence agency tools and law enforcement capabilities. This is unacceptable. Americans of course need access to technology that keeps our personal and business communications private, but this must be balanced with concerns over national security.

Some technologists and Silicon Valley executives argue that any efforts by the government to ensure law- enforcement access to encrypted information will undermine users' privacy and make them less secure. This position is ideologically motivated and profit-driven, though not without merit. But, by speaking in absolute terms about privacy rights, they bring the discussion to a halt, while the security threat evolves. Top cryptologists have reasonably cautioned that "new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws," but this is not the end of the analysis. We recognize there may be risks to requiring such access, but we know there are risks to doing nothing.

To be clear, encryption is often a very good thing. It increases the security of our online activities, provides the confidence necessary for economic growth through the Internet, and protects our privacy by securing some of our most important personal information, such as financial data and health records. Yet as with many technological tools, terrorist organizations are using encryption with alarming success.

For example, "end-to-end" encryption -- which allows communications and data shared across devices and platforms to be seen only by the individual holding the receiving device -- protects information even from a lawful court order backed by probable cause. Apple, Google and other companies have recently made this level of encryption the default setting on many phones and operating systems. The result will be digital crime scenes to which law enforcement has no access.

Encryption technology is easy to get hold of and doesn't require much sophistication to use. Islamic State knows this, and keeps close tabs on which technologies to direct its followers to in order to evade government surveillance. A recent article in the journal Foreign Affairs called it "the first terrorist group to hold both physical and digital territory: in addition to the swaths of land it controls in Iraq and Syria, it dominates pockets of the internet with relative impunity."

This isn't just a problem in Iraq and Syria. The jihadists' followers and adherents use encryption to hide their communications within the U.S. FBI Director James Comey recently testified that the attackers in last year's Garland, Texas, shootings exchanged more than 100 text messages with an overseas terrorist, but law enforcement is still blinded to the content of those texts because they were encrypted.

In October, President Barack Obama announced that he would not seek legislation requiring government access to such data -- a capability that would have been routine for law enforcement before the age of advanced encryption. The administration is instead asking for the industry's voluntary assistance in modifying technology to meet our security needs. Progress in this outreach to industry has been made, Comey said in November, and "venom has been drained out of the conversation."

But this is not enough. Efforts to eliminate cyber safe havens must not be marked by the same half-measures that have defined this administration's military fight against Islamic State. The president needs to define a coherent strategy to address the increasing use of encrypted communications by those who wish America and its allies ill.

This would mean building coalitions, domestically and internationally, to update laws and international conventions that allow law enforcement agencies across the world lawful access to digital criminal evidence.

As part of this effort, Congress should consider legislation that would require U.S. telecommunications companies to adopt technological alternatives that allow them to comply with lawful requests for access to content, but that would not prescribe what those systems should look like. This would allow companies to retain flexibility to design their technologies to meet both their business needs and our national security interests. Such a proposal would be similar to legislation enacted in the 1990s that ensured law enforcement agencies are able to lawfully wiretap without mandating how those systems ought to be designed.

We have to encourage companies and individuals who rely on encryption to recognize that our security is threatened, not encouraged, by technologies that place vital information outside the reach of law enforcement. Developing technologies that aid terrorists like Islamic State is not only harmful to our security, but it is ultimately an unwise business model.

The threat posed by the status quo is unacceptable. The use of technology by terrorist groups to recruit members, spread hateful ideology and plot attacks will only expand. But, just as Islamic State's growth

through the establishment of safe havens in Iraq and Syria was not inevitable, the group's ability to use technology to the same end does not need to be either.

The Advertiser
Overseas hackers linked to threats
Friday, 05 February 2016
Byline: Steve Rice

Canberra - Bomb threats that have shaken schools in South Australia and around the nation may have emanated from overseas or from the so-called dark web.
Authorities are understood to believe sophisticated hackers are behind the attacks, which have now hit much of the country since last Friday and appear to be designed to cause unnecessary disruption and inconvenience.

NSW Police have previously said the threats appeared to have come from overseas, with no credible evidence they could be carried out in Australia.

There is also no indication that terror groups are responsible and counter-terrorism officers are not involved in investigations. Other intelligence suggests the attacks are believed to have emerged from the dark web - a vast layer of the worldwide web favoured by criminals because it is not easily accessible to ordinary internet users - with someone accepting money for sending automated recorded messages to school phones.

Dozens of schools in Victoria, Queensland, NSW and the ACT have been targeted in the past week. Schools across Britain, US, France, Netherlands, Sweden, Norway, Japan and Guam have received similar threats but authorities have not confirmed any links. They also have not been able to establish whether an international group of hackers called Evacuation Squad, which claimed responsibility for attacks on Twitter, was responsible.

An Australian Federal Police spokeswoman said investigators were aware of threats made to schools in several states and territories, adding: "The AFP takes all threats such as this seriously and can assure the community its cybercrime operations area is working with partner law enforcement agencies in Australia and overseas to actively pursue those who make threats.

"State and territory police are working in partnership with education departments and other key stakeholders on responding to such threats.

"This is a timely reminder to the Australian public that authorities take these incidents very seriously.

"Making such threats is a serious criminal offence and every effort will be made to identify the person or persons responsible."South Australia Police warned yesterday those responsible for making such threats

faced serious charges Anyone with information about the hoaxes should contact Crime Stoppers on 1800 333 000.

The Advertiser
Radical shift for Google searches
Friday, 05 February 2016
Byline: Rob Harris

Canberra - Google will attempt to divert Australian online searches for extremist material towards warnings about radicalisation.
Search engine and social media companies, including Facebook and Twitter, will join a Federal Government-led campaign pushing potential extremists towards a "counter-narrative".

Online firms are facing increased pressure tackle the propaganda put online by Islamic State militants and supporters who try to radicalise young people.

In the US this week, Google revealed it is undertaking a pilot program to divert searches for IS-related material towards sites to debunk the propaganda.

More than 50,000 IS-related accounts exist on Twitter alone. Facebook said it had also become a "hostile place" for IS and that keeping people safe was its "number one priority".

Minister Assisting the Prime Minister for Counter Terrorism, Michael Keenan, will hold discussions with the online giants later this month.

He urged parents, community leaders, teachers and friends to watch for warning signs that someone they know might be radicalising, and to be particularly wary about their online activities. "The online environment is being exploited by violent extremists to spread their propaganda and recruit others and their targets are getting younger and younger," Mr Keenan said.

"Just as parents and families have gained greater understanding of the dangers posed by online sexual predators, there needs to be increased awareness that extremists are using similar tactics to recruit and motivate susceptible individuals, particularly young people." The Commonwealth has committed $21 million to countering violent extremism online.

It has expanded relationships with companies such as Google and Facebook in a bid to eradicate terrorist propaganda targeting Australian youths.

Twitter is understood to have removed "tens of thousands" of extremist accounts in the past year and has more than 100 staff monitoring content around the world.

The Federal Government is also reviewing programs that provide teachers with information to spot teens at risk of being radicalised.A number of school-aged children in Melbourne are also -undergoing deradicalisation programs after they were found to be considering going to the Middle East as jihadists.

Haaretz
Israel's Military Censor Takes on Dozens of Bloggers, Facebook Pages
Friday, 05 February 2016
Byline: Gili Cohen

Jerusalem - Chief Military Censor Col. Ariella Ben-Avraham recently officially contacted some 30 bloggers and administrators of Facebook pages requesting that they submit items for review by the censor ahead of publication, provided they concern areas requiring review, according to the emergency regulations in force since the state's founding.
There are several dozen subjects on this list - mainly having to do with the military or security, or information about the enemy - that media outlets are required to submit to the censor for review. Failure to submit such items to the censor constitutes an offense and defense regulations enable the censor to file a complaint with law enforcement.

Up to now, the censor has examined the sensitivity of information prior to publication mainly with the major media outlets, but also with rescue organizations, cities near the front lines and more. Now the military censor is asking dozens of operators of Internet sites that have a relatively large following to proceed similarly. These pages are mainly ones that give news flashes online, forums dealing with the army and security, blogs that describe themselves as dealing with the news, and certain popular Facebook pages.

Yossi Gurevitch who runs the "George's Friends" page, which calls itself a "blog for social, political and media criticism," wrote on his Twitter account Wednesday that the military censor informed him that it "must see posts and status updates" that he writes about the Israel Defense Forces and the security establishment ahead of time. Gurevitch said he did not intend to heed this demand and was also going to see whether there were any legal steps he could take against it.

Ben-Avraham also contacted dozens of operators of popular public Facebook pages that have at least several thousand followers. The censor wanted to obtain information on how to contact the people who manage these Web pages.

In recent years, the censor has tried to adapt to the developments in the world of communications, and began monitoring social networks such as Facebook and Twitter, as well as blogs. In the past the former chief censor, Brig. Gen. Sima Vaknin-Gil, said, "I have no intention of entering into the personal diary of every citizen, and I want to make it clear that we are not looking at the Facebook pages of private individuals."

Up to now, the censor only took retroactive action against publications of material considered harmful to national security. The censor's computerized monitoring systems were used to examine online publications by established media outlets and others. But now the censor is asking independent publishers to submit their reports on matters concerning the military and security for prior review, before publication. This is a policy change that the censor says is required for adapting to the Internet age. The censor's office stressed that they are not monitoring private pages, but only ones that are defined as public (and appear as "media" in the social networks).

The censor in Israel operates in accordance with the 1945 Emergency Regulations, which require media outlets to submit to it, prior to publication, any material requested by the censor. Data from the censor's office shows that on average, 70 percent of the information requested is submitted in accordance with the aforementioned list of topics. Of all the reports that were not submitted to the censor, said Vaknin-Gil, only a very few would potentially have harmed national security.

In an article she published in the Military Advocate General's journal "Law and Military" about six months ago, Vaknin-Gil proposed changing the model for applying censorship since it is no longer in keeping with the changes wrought by the Internet, and also advocated that new legislation be enacted regarding the censor's activity, which would include a curtailing of the censor's authority.

Dr. Tehilla Shwartz Altshuler, head of the media reform program at the Israel Democracy Institute, called the censor's directive "extremely borderline, in terms of the law based on the Emergency Regulations."

"On the face of it, it looks like adding insult to injury: Not only do the defense regulations constitute an anti- democratic arrangement that does not recognize the right to free expression, the censor is now asking to expand these bad arrangements to the digital world, instead of fixing them. It is unreasonable that the system chooses to expand [the censor's] authority instead of using it in proper measure, under the perception that the world of 2016 can continue to operate in the reality of the beginning of the 20th century."

The military censor responded: "The fundamental value of freedom of expression, its importance and the need to correctly balance it with safeguarding national security, is always at the forefront of the censor's mind, and this applies to Internet publications too. The authorities of the censor, which are defined in the law and subject to the oversight of the Supreme Court, apply to every type of publication regarding national security, whether it be through traditional media outlets or another type of publication.

"The censor does not block the publication of all security-related information, but only of material that it is deemed will almost certainly harm national security. From time to time, the censor contacts relevant parties in order to underline the obligation to submit items concerning security for review prior to publication. In the past week, a number of Facebook pages that define themselves as news or breaking news pages were contacted in this way. No requests were made to remove any material.

"Let it be made very clear that these are not private profiles. They are all public profiles that define themselves as 'media' and are open to public scrutiny."

Times of Israel
Hack attacks on electricity, water systems already here, says expert
Friday, 05 February 2016
Byline: David Shamah

Jerusalem - You don't have to be paranoid to imagine that one day soon hackers will gain control of an important infrastructure system, like a water distribution system or a power plant - as apparently happened in Ukraine in December, where what are suspected to be Russian hackers used malware to cause a blackout in the country's Ivano-Frankivsk and other regions.
But what many people should be fearful of is the apparently blasé attitude of many government officials and even industry workers to protecting those infrastructure systems, said Irit Potter, CEO of Israeli security consulting group IP-Sec.

"Governments in the developing world are spending a lot of money to upgrade their communications infrastructure, developing connected smart cities and systems to improve the lives of residents - but security is barely a second thought for many of them," said Potter on the sidelines of the CyberTech 2016 event in Tel Aviv last week. "We work in many places in Latin America, and we see first-hand how a lax attitude leads to lax security."

Thousands of people from Israel and around the world converged at Cybertech 2016 to check out the latest in Israeli cyber-defense and detection technology - but that tech can only protect if it is implemented. For various reasons, the need for serious cyber-security has not yet been absorbed in many places in the developing world, said Potter. "In some countries there is more awareness but it is localized, perhaps on a specific server or department. There is no overall awareness and policy-setting in many of these places."

Certainly not for SCADA (supervisory control and data acquisition) systems, the systems that are usually part of closed networks that traditionally are used to control infrastructure. When an electric company needs to reroute power to different substations, it will use its closed SCADA network to make that change. Unconnected to any other networks - much less the Internet - and accessible only from specific computers, the SCADA systems were considered safe from hackers.

That traditional perception is part of the problem, said Potter. "In many cases, the only way to invade a SCADA network is to physically tap into communications equipment at the site of a substation or other facility, or to take over the power plant itself. But with the innovations involved in smart city technology, it hasn't yet sunk in for many administrators that their SCADA networks are now just as vulnerable as the Internet - and maybe more at risk."

The Ukraine hack, reported first by computer security specialist ESET, is a perfect example of how this works, said IP-Sec vice- president Moshe Raz.

"Part of the new trend in connected SCADA networks is a conversion from the traditional UNIX systems, which are hard to learn and difficult for hackers to gain control of, to the new user-friendly Windows systems."

According to ESET, that is apparently what happened in Ukraine; hackers used social engineering to get power plant workers to open infected Microsoft Office documents, which deliver malware that make their way to control systems.

That, the group said, appears to be what caused the December 23, 2015 blackouts. Security officials were able to find the virus and stop it from spreading.

"Although in Ukraine, Christmas is traditionally not celebrated on December 24th and 25th, a group of cyber- criminals has chosen this time of year to deliver a dark 'present' to a few hundred thousand people and many more might have also been this 'lucky', had the malware not been detected," ESET said, adding that it was likely Ukraine, and other places, would have to wrestle with this threat in the future as well.

That, finally, may wake up officials to the importance of security - and especially training personnel at infrastructure and other important facilities to deal with security issues, said Potter.

IP-Sec, which has been in business since 2004, does just that, and is considered one of the top security consulting firms in the world on SCADA defense. "We train personnel to identify threats, and help them learn what to do about those threats," said Potter. Among it customers in Israel are the large majority of large enterprises and government offices - "one of our smaller customers in Israel is the Tel Aviv Stock Exchange," said Potter - and the group works with governments around the world, and especially in Latin America, to train workers to deal with cyber-attacks.

"We work with organizations for about a year, setting up scenarios that they will have to face in real life, and help them learn how to deal with them on their own," said Potter. "In addition, we monitor their systems, alerting them on when there is a problem, and advising them on what action to take." Eventually, it's expected that the team will be able to handle things on their own. "Each security scenario is custom-designed for customers, so they can get a good sense of what they are up against."

Even with this intensive training, teams don't always get it - so one of IP-Sec's important activities is showing those in charge the bottom line costs of ignoring cyber-security. "Hackers cost companies money - even lives, if systems in places like hospitals are harmed - and for various reasons, not all public officials make the connection between cyber-security and financial security. We make sure they understand that. Once they do, you can believe they are a lot more amenable about ensuring the safety of their systems."

Khaleej Times
Baghdad in bid to silence Daesh's online propaganda machine
Friday, 05 February 2016

Dubai - Iraq is trying to persuade satellite firms to halt Internet services in areas under Daesh's rule, seeking to deal a major blow to the group's potent propaganda ma-chine which relies heavily on social media to inspire its followers to wage war. Social media apps like Twitter and Telegram are scrambling to limit Daesh's cyber-activities. So far that has proven to be a cat-and-mouse-game, with the group re-emerging through other accounts with videos showing beheadings and extolling the virtues of living in a caliphate. For Iraq then, the key is to stop the militant group from accessing the web at all - a feat, which if achieved, could sever a significant part of a propaganda campaign that has inspired deadly attacks in the West. Mobile networks are largely in-operable in the Daesh-held swathes of Iraq, areas which also have little fixed-line broadband infrastructure.
Militants instead use satellite dishes to connect to the web, or illicit microwave dishes that hook them into broadband networks in government-held areas, three telecoms industry sources said. There are many challenges for the Iraqi authorities: within the satellite Internet industry, no one assumes responsibility for identifying and vetting end users, the territory under Daesh's often shifts, and a complex web of middlemen makes it tough to pinpoint who is selling militants Internet capacity. The group has control over or operates in parts of western Iraq and northern and central Syria which have a population of up to 5 million people, according to the International Institute for Strategic Studies, most of them in Iraq.

To connect to the web via a satellite, all that is required is a V-sat terminal - a small dish receiver and a modem - and an Internet subscription. Daesh uses "the V-sat system to access the Internet in areas it controls," an Iraqi communications ministry official said. "What's still difficult for us is controlling V-sat receivers which connect directly to satellites providing Internet services that cover Iraq." In the Daesh-held northern city of Mosul, V-sat units can be bought for about $2,000-$3,000 at a sprawling electronics market near the university. The official said Iraq was in talks with satellite companies covering Iraq to halt Internet services to Daesh-controlled areas, adding that he had received "positive sig-nals" from them, but "the process is complicated and needs more time and procedures.

"Even if Iraq cuts off Daesh from satellite Internet, the group can re-main online through illegal networks set up by businessmen in towns such as Kirkuk, Arbil and Duhok. These entrepreneurs buy data capacity from fixed broadband providers, passing through many middle-men first. They connect this to microwave dishes, which have a range of about 40 kilometres to eventually reach end users in Daesh-controlled areas, said the three industry sources. "It's two hops via microwave dishes to Mosul," said the third industry source." Their activities have very little chance of being detected. If you can buy a certain amount of capacity for $100 in Arbil and sell it on for $500, it's good business."

Christian Science Monitor
How NSA reorganization could squander remaining trust
Friday, 05 February 2016
Byline: Jason Healey

Column - The coming reorganization of the National Security Agency may be a smart move for the agency but it'll hurt America's long-term national security interests.
At a recent talk at the Washington think tank Atlantic Council, NSA director Adm. Michael Rogers said he wanted to better integrate the agency's Information Assurance Directorate - its defensive arm that protects US systems and information - and the Signals Intelligence Directorate - the offensive branch that carries out spying operations.

The reorganization is needed, he said, because with these two separate divisions "we created these two amazing cylinders of excellence and then we built walls of granite between them."

As a veteran of the NSA, I suspect this reorganization will be good for the agency. But it is unlikely to create an agency that is more open, more trusted, or more able to work with America's true cyber defenders in the private sector.

There are significant reasons to believe that what may help the NSA will be bad for the US - or actually anyone who uses the Internet.

The NSA's cyberdefense team, widely seen the best in the US government (and maybe the world), needs to work publicly, openly, and internationally. But if further integrated with NSA's spies, it will be forever compromised.

The Information Assurance Directorate is respected for its technical skills, but many critics and observers see it as tainted because of what Edward Snowden - a former NSA contractor who turned government leaker - revealed about the agency's signals division.

The clearest example of that tarnish is evidence that the NSA intentionally weakening a cryptographic standard, handicapping all of our security for a better chance to breach adversaries. That meant that the needs of the spies were prioritized over those meant to defend the rest of us. And that's something that will likely continue in the reorganized agency.

Who in Silicon Valley or Europe will be able to trust that kind of organization?

Even with a separate information division, many companies and privacy advocates were convinced the newly passed information sharing act was simply another vector for passing along data to NSA's digital spies. With the two parts of the agency more integrated, such concerns will be even harder to dismiss.

Likewise, if a multinational company calls NSA now for technical help, as Google and Sony have done in the past, can executives really assure their boardrooms that their corporate data won't end up in a spy's database?

Gen. Michael Hayden, one of Rogers's predecessors, specifically kept the Information Assurance Directorate separate, as he "needed an organization that was, and was seen to be, committed to defense."

The separation within the agency, from this perspective, isn't about creating stovepipes but building a firewall to protect our privacy and the information division's independence.

In fact, the technologists and cyberdefenders in Information Assurance have long needed to be integrated less with secretive the agency's spies, and more with other parts of the government and the private sector. A better option would have been splitting off Information Assurance as the core of a truly independent and robust cyber department or agency.

That option is now closed. Once the cards are shuffled into the deck, they will be all but impossible to separate.

Note: Jason Healey is senior research scholar at Columbia University's School of International and Public Affairs and senior fellow at the Atlantic Council. He began his career as a US Air Force signals intelligence officer in Alaska, NSA, and the Pentagon.

The National (UAE)
The cutting edge of technology on show at Drones for Good competition
Friday, 05 February 2016
Byline: Nadeem Hanif

Dubai - Drones that can fly and travel under water, as well as support rescue efforts, are among the finalists of this year's UAE Drones for Good competition.
In the national category of the semi-finals at the Dubai Internet City on Thursday, Buildrone's construction and repair aerial robot drone, ReefRover's drone for studying underwater ecosystems, and FlyLab's drone for the education sector advanced into the finals.

The creators of FlyLab's drone are Ibrahim and Mohammed El Badawi. The siblings built the machine with off-the-shelf parts to help students gain knowledge about the environment and support classroom learning.

"During our display, we used the drone to measure the atmosphere by taking various readings," said Ibrahim. "But the great thing is that this technology can be used in a whole range of subjects like physics, art and other sciences."

The ReefRover team's drone was designed to aid marine research, while Buildrone impressed the judges with their machine that can detect damage to pipelines and conduct repairs. The eventual winner will take home Dh1 million.

Saif Al Aleeli, the competition's coordinator general, said innovation was key to building the future and using technology in the service of humanity.

"The drones sector is certainly in its early stages but we are confident it will evolve as a major contributor to the world economy." said Mr Al Aleeli, who is also the chief executive of the Dubai Museum of the Future Foundation.

In the international category, which carries a top prize of US$1 million (Dh3.67m), 19 teams from around the world on Thursday competed amid the buzz of rotor blades in the air.

Loon Copter's multi-rotor drone from America, 4Front Robotics' USAR Robot drone from Canada, and SenseLab's SaveME drone from Greece advanced into the finals.

Oakland University's Loon Copter drone was the most unique of its rivals, thanks to its ability to fly and travel under water like a submarine.

"We believe it's the world's first flying and swimming drone and we've already had interest from law enforcement about the concept," said Osamah Rawashdeh, the team leader and an associate professor of electrical and computer engineering at the university.

Besides surveying pipelines, the drone can also assist in search-and-rescue missions.

SenseLab's project transforms a smartphone into a little drone to support people in emergency situations, particularly those who are trapped, lost or wounded.

Its rival, 4Front Robotics's drone, is able to fly and navigate in highly confined spaces, and provide high resolution data in a matter of hours. The finals will take place on Saturday.

Wall Street Journal

A Cyberwar Update: Gen. Michael Hayden says recent government moves to protect cyberspace are too little, too late

Wednesday, 10 February 2016

Byline: John Bussey

Section: general

Interview - We're in a global cyberwar in which our corporate secrets are our chief prize. Are we up for the fight?
To get a clearer answer, The Wall Street Journal's John Bussey spoke with Gen. Michael Hayden, principal of Chertoff Group and former director of the Central Intelligence Agency and NationalSecurity Agency. Here are edited excerpts of the discussion.

MR. BUSSEY: We got some news last month. There's some legislation meant to increase cooperation between the government and business. Tell us about the bill and whether or not it helps CIOs protect corporate secrets.

GEN. HAYDEN: We're talking about CISA, the Cybersecurity Information Sharing Act. Good news, a step in the right direction. But it's too long in coming, it's too small a step. And it reveals that within any realistic planning horizon, you are largely responsible for your own defense in the cyber domain.

The government, our government will be permanently late for your cybersecurity. Look, your armed forces view cyber as a domain. Land, sea, air, space, cyber. It's a new domain. You and I have decided that this domain is so wonderful, empowering, we're going to take things we used to keep down here in a safe, in a drawer, in a wallet, and put it up here where it's largely undefended. This is the largest ungoverned space in recorded human history. There is no rule of law up here.

As taxpayers, you and I are going to want our government to defend us up here the way we have become accustomed to relying on the government for defending us down here. But there's the general sclerosis of government, and the technology is going to move much faster than any government can move. Then we have not yet decided what it is we want or what it is we will allow the government to keep us safe. You're going to have to be responsible for your safety [in the cyber domain] in a way in which you have not been required to be responsible for your safety [in the physical domain] since the closing of the American frontier in 1890.

MR. BUSSEY: It does seem that before the war on cybersecurity can be fought as a nation, we have to resolve the civil war internally over privacy.

GEN. HAYDEN: Yeah. And that's a multigenerational thing. We haven't arrived at a national consensus. In the American system, when the government doesn't show up, we generally pick up the burden ourselves. So, the good news is there's a lot of private-sector activity designed to keep us safe.

Let me explain this another way. When I think about a national-security problem, generally my instincts are the government is the prime mover. If you're into Civil War history, Gen. Grant or Gen. Lee says, "You, sir, your corps is the main body. And you, gentlemen, you will conform your movements to the movements of the main body." In government, I assumed that in cyberdefense, the main body was the government, and you shall conform your movements with the movements of the main body. In the cyber domain, you are the main body. What our government has to teach itself is that the government needs, in all but a few exceptional cases, to conform its movements to the movements of the main body, you.

MR. BUSSEY: One of the things that the private sector is doing is to look again at encryption.

GEN. HAYDEN: The issue here is end-to-end unbreakable encryption, should American firms be allowed to create such a thing. You've got Jim Comey, the director of the FBI, saying, "I am really going to suffer if I can't read Tony Soprano's email or if I've got to ask Tony for the PIN number before I get to read Tony's emails." I get it. There is an unarguable downside to unbreakable encryption. On the other side is the question: On balance, is America more or less secure with unbreakable end-to-end encryption, regardless of whether Jim can read Tony's emails?

I think Jim Comey's wrong. Jim's logic is based on the belief that he remains the main body and you should accommodate your movements to the movements of him, which is the main body. And I'm telling you, with regard to the cyber domain, he's not. You are.

MR. BUSSEY: Tell us how the landscape of threat is evolving or changing.

GEN. HAYDEN: The stealing-your-data stuff is there, and it's getting worse. Beyond that, [people are trying] not just to steal data, but to create effects. So you've got Stuxnet, which is the destruction of a thousand centrifuges at Natanz in Iran. I view it as an unalloyed good, but it was done using a weapon comprised of ones and zeros to create physical destruction.

Leon Panetta spent a lot of time in his last year or two in government talking about cyber Pearl Harbor, digital 9/11, catastrophic attack. I don't think that's what we have to worry about. I'm not frightened about the Chinese turning out all the lights east of the Mississippi. I'm not worried about that superpower, catastrophic attack.

I'm worried about the isolated, nothing to lose, "Ah, what the hell? Let's go see what happens," nation state who goes after a North American enterprise to create physical destruction to show that they can. The Sony attack is the poster child for that.

Times of Israel

Iran said to hack former Israeli army chief-of-staff, access his entire computer

Wednesday, 10 February 2016

Byline: Staff Report

Section: general

Jerusalem - A cyber-hacker working for Iran hacked the computer of a former IDF chief-of-staff, an Israeli television report said Tuesday, and gained access to the unnamed army chief's entire computer database.
The hacker was named by Channel 10 as Yaser Balaghi. He was said to have subsequently bragged about the hack, but he also inadvertently left behind a means to trace his identity. That error prompted Iran to halt the hacking operation, which targeted 1,800 people worldwide, including Israeli army generals, human rights activists in the Persian Gulf and scientists.

The Times of Israel reported on the Iranian hacking operation two weeks ago, after an Israeli cyber-security firm, Check Point, revealed its existence. Tuesday's Channel 10 report also cited information from Check Point.

Gil Shwed, CEO of Check Point Software Technologies, told Israel Radio in late January that the attack began two months earlier and that its targets received email messages aimed at sending spyware into their computers.

More than a quarter of the recipients opened the emails and thus unknowingly downloaded spyware, allowing the hackers to steal information from their hard drives.

Over the last two years, Israel has been targeted by a number of cyber-attacks. Officials say hackers affiliated with Hezbollah and the Iranian government were behind some of the infiltration attempts.

Also in late January, Energy Minister Yuval Steinitz revealed that Israel's Electric Authority was being targeted by a "severe cyber- attack," although he did not say where it was coming from.

In June, the Israeli ClearSky cyber-security company said it had discovered an ongoing wave of cyber attacks originating from Iran on targets in Israel and the Middle East, with Israeli generals again among the targets. The goal is "espionage or other nation-state interests," the firm said.

The hackers use techniques such as targeted phishing -- in which hackers gather user identification data using false web pages that look like real and reputable ones -- to hack into 40 targets in Israel and 500 worldwide, said ClearSky. In Israel the targets have included retired generals, employees of security consulting firms and researchers in academia.

Shwed warned that the pace of cyber-attacks is accelerating faster than the pace of investment in cyber safety.

Israel is second only to the United States in cyber-security technology, according to Gadi Tirosh, managing partner at Jerusalem Venture Partners, which has been one of the country's most active investors in the field.

There are currently 173 companies in Israel big enough to be backed by venture capital companies and other major investors. That does not include the hundreds of others that are bootstrapped or relying on other sources of funds; altogether, there are 430 cyber companies currently operating in Israel, according to a report released earlier this month by the Israel Venture Capital (IVC) Research Center, with an average of 52 new cyber startups established annually since 2000.

Wall Street Journal

Hackers Breach IRS Computer Systems

Wednesday, 10 February 2016

Byline: Laura Saunders, Richard Rubin

Section: general

Washington - The Internal Revenue Service said Tuesday it identified an automated attack on its computer systems aimed at gaining information that could be used to steal tax refunds.
The news came the same day the administration announced a proposal to boost cybersecurity in the federal government, though the plan's request for extra funds has an uncertain future in Congress.

The IRS said identity thieves last month used personal data of taxpayers that was stolen elsewhere in an attempt to generate e-file PIN numbers that could be used to file fraudulent returns and claim refunds.

E-file PIN numbers are used by some individuals to file their tax returns. The numbers are different from Identity Protection PIN numbers, which the IRS gives victims of tax-identification theft to protect them from future issues.

The agency said it identified unauthorized attempts to obtain e-file PINs for 464,000 Social Security numbers, of which 101,000 successfully accessed an e-file PIN.

No personal taxpayer data was disclosed by IRS systems, the agency said. It is notifying affected taxpayers by mail that their personal information was used by criminals. The IRS said it is protecting their accounts against tax ID theft.

An agency spokesman said identity thieves would typically need much more data than an e-file PIN to file a fraudulent return. The agency also said the incident isn't related to last week's outage of IRS tax processing systems.

Over the past year, the IRS, state tax officials and tax-preparation firms have conducted a campaign to combat the growing problem of tax-refund fraud, a crime in which thieves use stolen personal information to file a return claiming a fraudulent refund.

In 2015, hackers stole the personal information of more than 330,000 taxpayers from the IRS's "Get Transcript" database, which provided data from prior returns.

Meantime, White House officials said they plan to enact a range of initiatives this year they believe will strengthen federal computer networks against cyberattacks.

Obama administration officials are instituting what they call a cybersecurity national action plan, which would create a federal chief information security officer, establish a new commission that looks for ways to protect computer networks, and increase coordination among federal officials who focus on privacy issues.

The officials also will look to overhaul outdated government computer systems they believe are too easy for hackers to penetrate.

The plan would include an expansion of training and recruiting for federal jobs that focus on cybersecurity, as well as an education-loan forgiveness program for people who remain in certain posts.

"The federal government -- which is obligated to protect the information provided to it by the American people -- has a unique responsibility to lead," President Barack Obama wrote in an op-ed article in Tuesday's Wall Street Journal. "But the fact is we still don't have in place all the tools we need, including ones many businesses rely on every day."

Some parts of the plan can be implemented unilaterally, but the White House is seeking a 35% increase in the cybersecurity budget to secure $19 billion in funding for many of the programs next fiscal year.

Times of Israel

Pro-Palestinian hacker dumps data of thousands of Fed workers

Wednesday, 10 February 2016

Byline: Staff Report

Section: general

Jerusalem - An anonymous pro-Palestinian hacker released the employee information of thousands of people who work at the U.S. Justice Department and the Department of Homeland Security.
On Sunday and Monday, the hacker dumped data including employees' email addresses, phone numbers and job titles. The data was released via a Twitter account; the Twitter message included the hashtag #FreePalestine.

Government officials told The New York Times that the information appeared to be culled from internal government directories.

On Sunday, the hacker first made his intentions known to the technology news website Motherboard, which received a copy of the encrypted list before it was publicly released. Motherboard called some of those phone numbers at random and reached the people who were listed or their voicemail boxes, as well as the operations center of the FBI.

Among the job titles on the list were contractors, biologists, special agents, task force officers, technicians, intelligence analysts and language specialists.

The hacker told Motherboard that he first compromised the account of a Department of Justice employee and eventually hacked into the department's entire intranet.

In October, pro-Palestinian hackers hacked into the email account of CIA director John Brennan and hackers forwarded the calls of the director of national intelligence, James Clapper, to the Free Palestine Movement.

Saudi Gazette

WhatsApp voice call ban decision not ours: CITC

Wednesday, 10 February 2016

Byline: Staff Report

Section: general

Riyadh - The decision to ban WhatsApp voice call in the Kingdom was taken by the WhatsApp Company itself, according to the Communications and Information Technology Commission (CITC).
The Kingdom's telecom regulator clarified in a statement on Tuesday that the voice call service is not available in many countries, including some Gulf Cooperation Council (GCC) states, and this was because of the failure of the company in complying with the regulations prevailing in these states, the Saudi Press Agency reported.

The CITC's statement came in reaction to the reports being circulated in some media outlets about halting the WhatsApp voice call service in the Kingdom.

The commission also underscored its keenness in making available of the latest communications and IT services to the users, strictly in line with the rules and regulations prevailing in the Kingdom.

The call facility on WhatsApp, which was blocked earlier was suddenly resumed on Saturday. The service was blocked on March 15 last year in the Kingdom after pressure by telecom companies claiming it was creating big losses to them.

Fars News Agency

New Generation of Air-Based Cruise Missiles Delivered to Iranian Air Force

Wednesday, 10 February 2016

Section: general

Tehran - The Iranian defense ministry delivered its home-made and high-precision air-launched cruise missile, 'Nasr', to the Air Force on Tuesday.

"The missile is designed to attack and destroy specific targets," Defense Minister Brigadier General Hossein Dehqan said, addressing a ceremony to deliver the missiles to the Air Force today.

Noting that Nasr will increase the operational and tactical capabilities of the Air Force, he said the air-lauched missile can be mounted and fired from fighter jets in midair.

In relevant remarks in August, the defense minister had outlined plans to equip Iran-made drones with Nasr cruise missiles.

Dehqan made the remarks in Tehran, addressing the inauguration ceremony of the Nasr missile production line.

"Using the air-based Nasr missile by the Army and the Islamic Revolution Guards Corps (IRGC)'s Air Forces will remarkably increase their operational and tactical power," he said.

Dehqan said that the Nasr missile is equipped with a high-precision radar which enables it to trace and intercept targets, adding that after being fired from fighter jets, Nasr doesn't need any backup and the fighter jet can leave the danger zone immediately.

Noting that the Nasr missile can be mounted on different types of fighter jets, he announced Iran's future plan to equip its home-made drones with the air-based missile.

In recent years, Iran has made great achievements in the defense sector and gained self-sufficiency in essential military hardware and defense systems.

The country has repeatedly made it clear that its military might is merely based on the state's defense doctrine of deterrence and that it poses no threat to other countries.

In March, the Iranian defense ministry started the mass- delivery of different ballistic missiles, including Qadr, Qiam, Fateh 110 and Khalij-e Fars missiles, as well as Mersad air defense system to the IRGC and Khatam ol-Anbia Air Defense Base.

"The honorable specialists of the Defense Ministry's Aerospace Organization displayed the defense industry' power and capability in providing the Armed Forces' needs to the most advanced missile equipment by supplying them with Qadr, Qiam, Fateh 110 and Khalij-e Fars (Persian Gulf) ballistic missiles and Mersad air defense system and showed that the different and comprehensive sanctions of the enemies imposed strictly and specially on our defense sector have totally failed to undermine their resolve and determination," Dehqan said at the time, addressing a ceremony held to mark the delivery of the new missile systems to the IRGC and Khatam Ol-Anbia Air Defense Base.

"These missiles can strike and destroy enemy targets with a high precision capability and provide for a wide range of the Armed Forces' needs to missiles with different ranges," he added.

Dehqan underlined that all these missiles have been built by Iranian specialists, and said, "Today the Armed Forces enjoy such a high degree of defensive capabilities that they can counter back any kind of threat posed from beyond the borders of the Islamic Republic of Iran."

He also described enemies' threats of military action against Iran as media hype for internal use.

Qadr is a 2000km-range, liquid-fuel and ballistic missile which can reach territories as far as Israel. Qiam is also a new type of surface to surface and cruise missile.

The Fateh-110 is a short-range, road-mobile, solid-propellant, high- precision ballistic missile with advanced navigation and control systems.

The Fateh-110 has been designed and developed by the Iranian experts in the Defense Ministry's Aerospace Organization and has not been modeled on any foreign product.

The supersonic Khalij-e Fars (Persian Gulf) missile, which carries a 650-kilogram payload, is smart and immune to interception, and features high-precision systems.

The supersonic ballistic missile is the most advanced and most important missile of the IRGC Navy.

The distinctive feature of the missile lies in its supersonic speed and trajectory. While other missiles mostly traverse at subsonic speeds and in cruise style, Khalij-e Fars moves vertically after launch, traverses at supersonic speeds, finds the target through a smart program, locks on the target and hit it.

The range of the solid-fuel missile is 300km and it can be fired from triple launchers.

The missile could successfully hit a mobile target one-tenth of an aircraft carrier in its early tests.

Also, Mersad Air Defense Missile System is a completely indigenized system developed by the Iranian experts and technicians to promote the country's combat power.

The system has already passed field tests and is used as part of the country's integrated air defense network.

The Mersad system equipped with Shahin missiles is capable of tracing and targeting any enemy aircraft at 70 to 150km altitude and is considered as a mid-altitude system among the country's missile shields.

The National (UAE)

Full effect of digital currencies such as Bitcoin yet to be seen, Dubai summit hears

Wednesday, 10 February 2016

Byline: Staff Report

Section: general

Dubai - Cryptocurrencies, such as Bitcoin, are set to revolutionise how people pay for goods and services and move money around the world, according to the co-founder and president of Blockchain, a digital wallet and software company.
Cryptocurrencies are digital currencies exchanged over the internet and mainly used outside existing banking and government institutions.

Nicolas Carey, speaking on the second day of the World Government Summit, said the way we pay for items over the internet was changing, reported the state news agency, Wam.

"There is a great deal of talk about financial inclusion, but there are 2.5 billion people on Earth who do not have access to a bank account," Mr Carey said. "Even in the United States, one of the wealthiest countries in the world, 20.1 per cent of households are underbanked and 33 per cent of millennials do not expect to have a bank account in the next five years.

"If you combine all these people, with everyone who has access to the internet over smartphones, you can see the potential for cryptocurrencies.

"Digital is part of everyone's DNA. Digital money is a natural extension to the digital world. It offers frictionless and borderless transactions that are more open and more equal," Mr Carey said. More than US$1 billion (Dh3.67bn) has been invested in Bitcoin technology, he said.

In 2010 the first Bitcoin transaction took place when 10,000 Bitcoins were used to buy two pizzas. At today's exchange rate, Mr Carey said, the two pizzas would be worth $5 million.

Le Monde

Le directeur du renseignement américain reconnaît s'intéresser aux objets connectés

Wednesday, 10 February 2016

Byline: Journaliste maison

Section: general

Washington - « L'Internet des objets » représente un trésor de données pour les agences de surveillance et d'espionnage.
« A l'avenir, les services de renseignement pourraient tirer parti de l'Internet des objets pour identifier, surveiller ou localiser des suspects, découvrir des indicateurs potentiels, ou obtenir des mots de passe. »
Lors de son audition par le Sénat américain, mardi 9 février, le directeur national du renseignement, James Clapper, a eu un rare moment de franchise concernant la manière dont les services de renseignement états-uniens envisagent d'utiliser le développement des objets connectés - ce que l'on appelle aussi «l'Internet des objets».

Aux Etats-Unis, les objets connectés ont connu ces dernières années un fort développement. Les thermostats intelligents Nest (rachetés par Alphabet) proposent ainsi de contrôler son chauffage à distance, ou de manière automatisée - et de nombreuses marques de réfrigérateur proposent des fonctions allant de la gestion automatique de la température à... l'établissement d'une liste de courses en ligne en fonction de vos habitudes alimentaires et du degré de remplissage du congélateur.

Grande quantité de données collectées

Ces objets collectent une très grande quantité d'informations, potentiellement utilisables par des services de renseignement. Un rapport publié le 1er février par le centre de recherche Berkman de l'université Harvard estime même que la quantité de données rassemblées par ces objets en font l'une des pistes privilégiées pour que les agences de renseignement puissent contourner les protections mises en place sur de plus en plus de moyens de communication «classiques».

Ces dernières années, des failles de sécurité concernant plusieurs fabriquants d'objets connectés ont été révélées, le plus souvent après la publication en ligne d'informations personnelles de leurs utilisateurs. A la fin de 2015, par exemple, le fabriquant de jouets connectés Vtech avait reconnu avoir été la cible d'un important piratage, qui avait abouti au vol de données personnelles de nombreux utilisateurs de ses produits.

Agence France-Presse

Appels menaçants à des lycées: le suspect va être présenté à un juge

Wednesday, 10 February 2016

Byline: Journaliste maison

Section: general

Paris - Un lycéen dijonnais de 18 ans, féru d'informatique, qui avait été interpellé dans l'enquête sur des appels anonymes menaçants à des lycées parisiens, va être présenté mercredi à un juge d'instruction, a-t-on appris de source judiciaire.
Selon une source proche du dossier, en garde à vue, ce jeune homme qui s'est présenté comme un sympathisant de la démarche des Anonymous, s'est désolidarisé de ces alertes infondées à la bombe et a nié toute implication.

Il a créé un serveur qui permet d'anonymiser les envois et de brouiller les pistes sur internet, susceptible d'être utilisé par des "pirates" de la toile.

Les enquêteurs de l'Office central de lutte contre la cybercriminalité (OCLCTIC) de la PJ ont trouvé sa trace à partir d'un tweet revendiquant ces appels.

Ce message avait été envoyés par un expéditeur, nommé "Evacuation Squad", pseudo qui cacherait en fait un groupe de "hackers".

Ce tweet a permis de remonter à l'adresse IP (numéro d'identification de la connexion internet, ndlr) du lycéen dijonnais.

Mais il "ne cautionne pas les alertes à la bombe", infondées, qui se sont multipliées contre des lycées parisiens, selon une source proche du dossier.

"Il refuse de collaborer avec les services techniques de police concernant l'exploitation de son matériel informatique", a ajouté une source policière.

Il aurait été prévenu, par un moyen qu'il n'avait pas divulgué peu avant la fin de sa garde à vue, que son serveur avait pu être utilisé pour revendiquer ces appels malveillants.

Interrogé par l'AFP, le père du suspect a expliqué que son fils était en relation avec "des centaines" de personnes dans le monde et affirmé qu'il n'était "pas du genre à s'attaquer à des lycées avec des alertes à la bombe".

"Ce n'est pas un hacker, un hacker vient pour casser ou pirater, lui c'est un joueur expérimental qui entre dans un système, met un drapeau pour montrer qu'il était là comme un astronaute met un drapeau sur la Lune et il s'en va", a expliqué son père. Il a décrit son fils comme "un virtuose de l'informatique".

Les appels contre des établissements scolaires se sont multipliés ces dernières semaines dans un contexte de menace terroriste très élevée, après les attentats du 13 novembre.

Lundi 1er février et pour la troisième fois en quelques jours, des lycées et collèges français avaient reçu des menaces anonymes par téléphone, entraînant la mise à l'abri des élèves, voire leur évacuation.

D'autres établissements en province avaient également reçu des messages menaçants. A chaque fois, la police n'avait rien trouvé et les lycées avaient repris leur fonctionnement habituel.

Un scénario similaire s'était produit la semaine dernière au Royaume-Uni. Mais l'enquête française ne porte pas sur ces faits.

Illustration(s) :

LOIC VENANCE

Le lycée Henri IV, visé par des appels menaçants, le 16 février 2016 à Paris

Le Monde

Pékin victime des bravades de Kim Jong-un

Wednesday, 10 February 2016

Byline: Philippe Mesmer et Harold Thibault

Section: general

Pyongyang - Face à son voisin du Nord, la Corée du Sud veut déployer un système antimissile fourni par Washington
Pyongyang est en passe de réussir à dégrader un peu plus les relations déjà difficiles entre Washington et Pékin. A la suite du lancement par la Corée du Nord, dimanche 7 février, d'une fusée, ce que tous ses voisins interprètent comme un test déguisé de missile balistique, la Corée du Sud est désormais prête à déployer sur son territoire un système de radars et de missiles américain, capable d'intercepter un vecteur balistique nord-coréen en phase de descente.

Le président américain, Barack Obama, a confirmé, lundi, sur la chaîne CBS, que des consultations sont en cours " pour la première fois " . " Nous aimerions que cela se fasse vite " , a précisé Peter Cook, le porte- parole du Pentagone, au sujet du système antimissile baptisé " THAAD ", pour Terminal High Altitude Area Defense.

Pékin juge qu'une telle infrastructure d'interception pourrait également affaiblir sa propre dissuasion nucléaire. Rien n'empêche de tourner à terme le système THAAD contre l'arsenal nucléaire chinois. " La Chine ne voit pas le système THAAD comme une question de radar ou de missile, juge Kim Heung-kyu, spécialiste de la Chine à l'université sud-coréenne Ajou , mais comme une alliance -régionale entre les Etats-Unis, le- -Japon et la Corée du Sud. "

" Sentiment d'échec "Les autorités chinoises ont -convoqué dès dimanche l'ambassadeur sud-coréen à Pékin. La porte-parole du ministère des affaires étrangères chinois, Hua Chunying, a déclaré : " En quête de sa propre sécurité, un pays ne devrait pas altérer les intérêts sécuritaires de l'autre. " En cela, la Chine ne sort pas vainqueur de l'essai nucléaire et du tir nord-coréens. " Le sentiment d'échec est grand, car elle n'a pas réussi à convaincre le Nord d'y renoncer et souffre de voir le Sud se rapprocher en conséquence des Etats-Unis ", constate Shi Yinhong, professeur de relations internationales à l'Université du peuple, à Pékin.

La Chine avait pourtant déployé d'importants efforts pour tenter de convaincre son allié nord-coréen de renoncer à ce tir. " S'il y a une chose que la Chine ne veut pas voir, ce sont des essais , juge Mathieu Duchâtel, sous-directeur du programme Asie du European Council on Foreign Relations . Cela pousse la Corée du Sud à demander davantage aux Etats-Unis pour sa défense. Le Japon aussi est plus - actif, le tout dans un contexte stratégique qui se détériore. "

Le représentant spécial chinois pour les affaires coréennes, Wu Dawei, s'était rendu à Pyongyang le 2 février; un " effort diplomatique très sérieux " au cours duquel M. Wu avait indiqué avoir " dit ce qu'il y avait à dire et fait ce qu'il y avait à faire " . Visiblement sans effet puisque, le même jour, Pyongyang, témoignant de son peu de considération pour la démarche chinoise, avait informé l'Organisation maritime internationale de l'imminence de son tir. " La priorité de la Corée du Nord est sécuritaire, face au Sud et aux Etats-Unis. Sur ce terrain, elle ne se sent pas protégée par la Chine et ne l'écoute donc pas " , relève Cai Jian, directeur du centre d'études coréennes de l'université Fudan, à Shanghaï.

L'impuissance chinoise à peser sur les décisions nord-coréennes et sa réticence à se prononcer pour des sanctions après l'essai nucléaire du 6 janvier alimentent par ailleurs les frustrations de Séoul. En janvier, quand le ministre sud-coréen de la défense a tenté de joindre son homologue chinois pour discuter de l'essai nucléaire nord-coréen, il n'a eu aucune réponse. " Les meilleurs partenaires sont ceux qui vous tiennent la main dans les moments difficiles " , a souligné, une semaine plus tard, la présidente sud-coréenne, Park Geun-hye.

Auparavant, Mme Park avait accepté de ne pas pousser plus avant les discussions sur le THAAD, la Chine ayant averti que cela affecterait les relations bilatérales. Depuis sa prise de fonctions en 2013, elle a rencontré à six reprises son homologue chinois, Xi Jinping. Séoul a ainsi tenté de maintenir l'équilibre entre priorité économique et nécessité sécuritaire. La Chine est son premier partenaire commercial et devrait, selon les estimations de Séoul, lui envoyer huit millions de visiteurs en 2016.

Mais, pour ce qui est de se protéger, elle mise sur les 28 500 militaires américains stationnés sur son territoire. " Il serait ridicule, pour un pays souverain comme la Corée du Sud, de ne pas renforcer sa défense face à une menace grandissante comme celle des missiles nucléaires nord- coréens " ,estime Park Chang-kwon, de l'Institut coréen des analyses de défense, un organisme public sud-coréen. La presse sud-coréenne, pourtant généralement proche du pouvoir, n'hésite plus à parler d'une " décomposition " du lien avec Pékin, voire d'une véritable " claque " pour la présidente Park.

Le déploiement du système THAAD intéresse aussi le Japon. En novembre 2015, le ministre de la défense, Gen Nakatani, avait évoqué cette option. Et le 8 février, l'agence de presse japonaise Kyodo a évoqué la relance de discussions sur la coopération nippo-sud-coréenne dans le domaine du renseignement militaire. Séoul a toutefois démenti, affirmant qu'il fallait d'abord avoir l'appui de la population pour un tel accord, tout en admettant que cette option était envisagée.

Les Etats-Unis peuvent désormais retourner contre eux l'argumentaire des Chinois : leur politique de modération et d'incitation aux réformes économiques n'a pas convaincu Pyongyang d'abandonner sa quête de l'arme nucléaire. Selon cette vision, Pékin ne peut donc s'en prendre qu'à lui-même si ses voisins, Sud-Coréens ou Japonais, se tournent encore davantage vers Washington.

Washington Times

Islamic State supporters share Snowden video to explain need for encryption

Wednesday, 10 February 2016

Byline: Andrew Blake

Section: general

Washington - Islamic State supporters are using Edward Snowden and his revelations about the U.S. government's surveillance capabilities to urge followers of the terror group to adopt digital security practices, including the use of strong encryption.
Proponents of the Islamic State, also known as ISIS, started circulating a propaganda video across the Internet in recent days which contains several clips from Citizenfour, the 2014 film about Mr. Snowden and the U.S. National Security Agency, along with advice for evading the NSA's eavesdropping abilities.

Among the scenes from the Academy Award-winning documentary included in the 13-minute upload are clips in which the former government contractor describes the NSA's ability to gather digital communications anywhere on Earth; retired intelligence expert Bill Binney is also shown discussing mass

data analysis, and Jacob Appelbaum, a journalist and activist, describes how the NSA uses that information to make determinations about individuals based off of their interactions.

"This is just a drop in the ocean," reads an English-language translation of a title card that appears at the end of the video, as reported first by Vocativ on Monday. "Our enemies are monitoring us day and night, collecting our information and targeting us. This is very dangerous. Carelessness and negligence in digital security cannot be tolerated."

The video, "The Electronic War And The Negligence Of The Supporters Of Mujahedeen," concludes by directing viewers to a website, written in Arabic, which links to several articles and pages containing tutorials and information about digital security, encryption and the Islamic State. It's credited to "Technical Islamic State" and appears to have been created last July, but likely could see a resurgence in readers with the recent boost online from pro-Islamic State groups.

Vocativ reported that the video is the product of the Afaq Agency, "an ISIS-affiliated group focused on issues related to hacking and cyber security," and was discovered using the website's "deep web technology." Isdarat, a site that hosts Islamic State propaganda on both the deep web and the more widely accessed "surface" web, began hosting the video on Saturday. The Vocativ article makes no mention of Isdarat, but claims the video was shared this week by the Afaq Agency's account on Telegram, a social networking application popular among Islamic State supporters, and has since spread across social media.

Regardless of its origin, the video is making waves in the midst of a heated debate between lawmakers in Washington and the Silicon Valley tech sector with respect to regulating encryption. A national security discussion has intensified in recent weeks over whether or not Internet companies should be forced to decrypt digital communications for investigators that are otherwise protected by strong end-to-end encryption, and was among the main topics at a Senate Intelligence Committee hearing on Capitol Hill on Tuesday.

"I'm not sure we've exhausted all the possibilities here technologically," Director of National Intelligence James Clapper testified while discussing solutions to the government's so-called "going dark" debacle. "I would hope that we have not yet exhausted what can be done voluntarily."

Several members of the Obama administration have blamed Mr. Snowden in the past for allegedly having aided terrorists as a result of his unauthorized disclosures, including Chris Inglis, NSA's deputy director at the time the leaks were first reported.

"Having disclosed all of those methods, or at least some degree of those methods, it would be impossible to imagine that, as intelligent as they are in the use of technology, in the employment of communications for their own purposes, it's impossible to imagine that they wouldn't understand how they might be at risk to intelligence services around the world, not the least of which is the U.S. And

they necessarily do what they think is in their best interest to defend themselves," Mr. Inglis previously told The Washington Times.

The Guardian (London)

US intelligence chief: we might use the internet of things to spy on you

Wednesday, 10 February 2016

Byline: Spencer Ackerman, Sam Thielman

Section: general

New York - The US intelligence chief has acknowledged for the first time that agencies might use a new generation of smart household devices to increase their surveillance capabilities.
As increasing numbers of devices connect to the internet and to one another, the so-called internet of things promises consumers increased convenience - the remotely operated thermostat from Google-owned Nest is a leading example. But as home computing migrates away from the laptop, the tablet and the smartphone, experts warn that the security features on the coming wave of automobiles, dishwashers and alarm systems lag far behind.

In an appearance at a Washington thinktank last month, the director of the National Security Agency, Adm Michael Rogers, said that it was time to consider making the home devices "more defensible", but did not address the opportunities that increased numbers and even categories of connected devices provide to his surveillance agency.

However, James Clapper, the US director of national intelligence, was more direct in testimony submitted to the Senate on Tuesday as part of an assessment of threats facing the United States.

"In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials," Clapper said.

Clapper did not specifically name any intelligence agency as involved in household- device surveillance. But security experts examining the internet of things take as a given that the US and other surveillance services will intercept the signals the newly networked devices emit, much as they do with those from cellphones. Amateurs are already interested in easily compromised hardware; computer programmer John Matherly's search engine Shodan indexes thousands of completely unsecured web-connected devices.

Online threats again topped the intelligence chief's list of "worldwide threats" the US faces, with the mutating threat of low-intensity terrorism quickly following. While Clapper has for years used the equivocal term "evolving" when asked about the scope of the threat, he said Tuesday that Sunni violent extremism "has more groups, members, and safe havens than at any other point in history".

The Islamic State topped the threat index, but Clapper also warned that the US-backed Saudi war in Yemen was redounding to the benefit of al-Qaida's local affiliate.

Domestically, "homegrown extremists" are the greatest terrorist threat, rather than Islamic State or al-Qaida attacks planned from overseas. Clapper cited the San Bernardino and Chattanooga shootings as examples of lethal operations emanating from self-starting extremists "without direct guidance from [Isis] leadership".

US intelligence officials did not foresee Isis suffering significant setbacks in 2016 despite a war in Syria and Iraq that the Pentagon has pledged to escalate. The chief of defense intelligence, Marine Lt Gen Vincent Stewart, said the jihadist army would "probably retain Sunni Arab urban centers" in 2016, even as military leaders pledged to wrest the key cities of Raqqa and Mosul from it.

Contradicting the US defense secretary, Ashton Carter, Stewart said he was "less optimistic in the near term about Mosul", saying the US and Iraqi government would "certainly not" retake it in 2016.

The negative outlook comes as Carter traveled on Tuesday to meet with his fellow defense chiefs in Brussels for a discussion on increasing their contributions against Isis.

On the Iran nuclear deal, Clapper said intelligence agencies were in a "distrust and verify mode", but added: "We have no evidence thus far that they're moving toward violation."

Clapper's admission about the surveillance potential for networked home devices is rare for a US official. But in an overlooked 2012 speech, the then CIA director David Petraeus called the surveillance implications of the internet of things "transformational ... particularly to their effect on clandestine tradecraft".

During testimony to both the Senate armed services committee and the intelligence panel, Clapper cited Russia, China, Iran, North Korea and the Islamic State as bolstering their online espionage, disinformation, theft, propaganda and data-destruction capabilities. He warned that the US's ability to correctly attribute the culprits of those actions would probably diminish with "improving offensive tradecraft, the use of proxies, and the creation of cover organizations".

Clapper suggested that US adversaries had overtaken its online capabilities: "Russia and China continue to have the most sophisticated cyber programs."

The White House's new cybersecurity initiative, unveiled on Tuesday, pledged increased security for nontraditional networked home devices. It tasked the Department of Homeland Security to "test and certify networked devices within the 'Internet of Things'." It did not discuss any tension between the US's twin cybersecurity and surveillance priorities.

Connected household devices are a potential treasure trove to intelligence agencies seeking unobtrusive ways to listen and watch a target, according to a study that Harvard's Berkman Center for Internet and Society released last week. The study found that the signals explosion represented by the internet of things would overwhelm any privacy benefits by users of commercial encryption - even as Clapper in his testimony again alleged that the growth of encryption was having a "negative effect on intelligence gathering".

The report's authors cited a 2001 case in which the FBI had sought to compel a company that makes emergency communications hardware for automobiles - similar by description to OnStar, though the company was not named - to assist agents in Nevada in listening in on conversations in a client's car.

In February 2015, news reports revealed that microphones on Samsung "smart" televisions were "always on" so as to receive any audio that it could interpret as an instruction.

"Law enforcement or intelligence agencies may start to seek orders compelling Samsung, Google, Mattel, Nest or vendors of other networked devices to push an update or flip a digital switch to intercept the ambient communications of a target," the authors wrote.

L'Express

L'oeil caché du contre-terrorisme

Wednesday, 10 February 2016

Byline: E.P.

Section: general

Paris - La très secrète société américaine Palantir ne réserve pas son système d'analyse des données à la CIA. Elle tente de le vendre à la France comme arme anti-attentats.
L'oeil de Palantir Technologies se tourne vers le royaume de France. Pour les fans du Seigneur des anneaux, le nom de Palantir évoque aussitôt l'orbe sombre destiné à voir l'avenir dans ce roman d'heroic fantasy. Cofondée en 2004 par Alex Karp et Peter Thiel, la société, parmi les plus secrètes de la Silicon Valley, a reçu le soutien de la CIA via son fonds In-Q-Tel, afin notamment d'épauler les services de

renseignement dans la lutte contre le terrorisme. Sa technologie d'analyse massive des données aurait même aidé à retrouver Ben Laden. Une information jamais démentie... ni confirmée. Pas étonnant que l'entreprise tente aujour - d'hui de pénétrer en France, pays touché à deux reprises par des attentats en 2015. « Nous les avons rencontrés et avons évalué leur logiciel. Mais utiliser une solution américaine, de surcroît financée par la CIA, pose des problèmes de souveraineté nationale », indique-t-on au ministère de l'Intérieur.

La société met pourtant les bouchées doubles pour se développer en dehors des Etats-Unis. Un bureau a été ouvert à Londres à la fin de 2009 et une filiale a vu le jour à Paris au printemps dernier, implantée sur les Champs- Elysées. Selon des documents déposés au Royaume- Uni, Palantir a réalisé en 2014 un chiffre d'affaires de 33,4 millions d'euros, en croissance de 43 %. Mais convaincre la Direction générale de la sécurité intérieure (DGSI) est chose malaisée. Les Américains assurent que leur technologie est capable d'aider les analystes humains dans leur enquête, grâce à des outils informatiques et à une intelligence artificielle d'une puissance inédite. Le logiciel peut ainsi fouiller dans des bottes d'informations issues de multiples sources, afin d'y trouver les épingles du contre-terrorisme. Il permet de visualiser les contacts d'un suspect, ses transferts d'argent ou ses appels téléphoniques et de les comparer avec des schémas antérieurs d'attaques.

« Nous espérons que les données de santé ne sont pas concernées »

« Je n'ai pas rencontré M. Cazeneuve, indique Peter Thiel, président de Palantir Technologies. Mais nous avons des discussions avec tous les gouvernements d'Europe de l'Ouest qui souhaitent lutter contre le terrorisme. Tous ont besoin d'agir rapidement car, s'ils ne font rien, d'autres attaques surviendront et les partis populistes prospéreront. »

Pour s'implanter en France, Palantir s'appuie, selon nos informations, sur un premier client de renom, le n° 1 mondial de l'assurance, Axa. Le groupe présidé par Henri de Castries a créé en 2013 Data Innovation Lab, un laboratoire consacré à l'exploitation des données en vue d'évaluer le risque dans l'assurance automobile ou celle de l'habi - tation. Cette récente collaboration inquiète les pouvoirs publics : « Nous ne savons pas à quoi ont accès les Américains, glisse un conseiller gouverne - mental. Nous espérons que les données de santé ne sont pas concernées. »

La start-up opaque, valorisée 20 milliards de dollars, avait déjà suscité quelques remous. Elle aurait, selon La Lettre A, répondu à deux appels d'offres de l'Etat français à la fin de l'année dernière. Le premier concerne le Secrétariat général pour la modernisation de l'action publique (SGMAP) et le second la Direction générale des finances publiques (DGFIP) afin de traiter les données fiscales et de lutter contre la fraude. « Je ne suis pas au courant, a indiqué le ministre des Finances, Michel Sapin. Nous avons déjà des technologies similaires. » Pas facile de se faire une place en France.

Illustration(s) :

PHOTO TIRÉE DU FILM ZERO DARK THIRTY, ANNAPURNAPICTURES/ THE PICTURE DESK/ AFP

TRAQUE La technologie de Palantir aurait aidé à localiser Ben Laden, au Pakistan, en 2011.

Motherboard (Vice)

Sen. Feinstein Says Terrorists Only Need The Internet and Encryption To Attack

Tuesday, 09 February 2016

Byline: Lorenzo Franceschi-Bicchierai

Section: general

New York - The ongoing and seemingly endless debate over encryption technologies appears to have reached its most ridiculous apex.
On Tuesday, Sen. Dianne Feinstein (D-CA), said that all ISIS needs to carry out a terrorist attack in a Western country is an internet connection and an encrypted chat app. And no, she wasn't talking about a cyberattack.

Feinstein's comment came during a Senate hearing on national security threats in Washington D.C., while she was talking about the dangers of ISIS, or ISIL, and its supposed use of encryption to communicate and organize.

"While the coalition's air campaign is helping to deny ISIL some territorial safe havens and financial resources, how do we degrade it and destroy it if all they need to carry out an attack in the West is an internet connection and an encrypted message application?" Feinstein said during her opening remarks.

Feinstein's comment is perhaps the most grotesque attack on encryption since that of a Massachusetts prosecutor, who said last year that encryption would help perverts take inappropriate pictures of women wearing skirts, and get away with it. But ridiculous comments aside, her words highlight once more that numerous US politicians, as well as US government officials, are not giving up on their tirade against the rise of encryption.

Ever since Apple and Google announced that their new mobile operating systems would use encryption by default (Google later backed out of its promise) in September of 2014, a growing group of critics led by the FBI warned that these measures would make it hard, if not impossible, for cops and feds to do their job. The FBI Director James Comey, perhaps the most visible face in this ongoing crypto war, famously said that widespread use of encryption would "lead us all to a very dark place" where child molesters and terrorists get away with their crimes.

Yet, just as it's been happening in the last 17 months, nobody seemed willing, or capable, to propose an actual feasible solution. Comey said, once again, that he doesn't want a backdoor (nor a "golden key"), but didn't say what he wants other that tech companies to comply with court orders. US spy chief James Clapper said he "would hope" that tech companies and law enforcement haven't "exhausted" what can be done "voluntarily," but didn't specify what he'd like tech companies to do voluntarily.

The solution to the encryption debate remains fleeting, but what's clear is that the crypto war is not going to end any time soon.

Le Huffington Post (France)

Une cyberguerre enclenchée par Daech causerait beaucoup de dégâts

Wednesday, 10 February 2016

Byline: Antoine Böhm

Section: general

Non identifié - On a beaucoup écrit sur les capacités de Daech à mener une guerre numérique. L'essentiel des commentaires se focalise sur l'usage, peu créatif, des réseaux sociaux et d'internet comme d'un pur véhicule de propagande: Daech ne faisait que transmettre des communiqués, mettre en ligne des vidéos particulièrement macabres, et recruter de nouveaux membres. Il n'y avait qu'une légère différence, une différence de degré dans la technique, entre Al-Qaida et Daech: le deuxième utilisait Internet comme un véritable moyen de communication, quand le premier se cantonnait à en faire une vitrine de ses actions.
Peu de personnes, sinon les états-majors de renseignement et les forces de cyberguerre, ont évalué à sa juste mesure la menace qui planait: celle d'une véritable guerre portée contre un État par les canaux numériques. Il est possible de faire autant de dommages par la cyberguerre qu'en une guerre avec pourtant bien moins d'effectifs et de moyens. Ce manque de perspective vient d'une méconnaissance du fonctionnement d'internet : beaucoup pensent encore qu'un virus ne fait qu'envoyer des mails frauduleux, et que ces mails ne servent qu'à obtenir les codes de votre carte de crédit. Il est aujourd'hui possible d'éteindre pour quelques jours un service ou une entreprise, de mener un État à la faillite, de paralyser les systèmes bancaires, les réseaux d'électricité, les moyens de communication, les transports ou les services d'urgence par des techniques encore assez rudimentaires, avec très peu d'hommes -de hackers- aux commandes, et pour un coût dérisoire.

Il y eut des précédents. En 2007, entre le 27 avril et l'automne suivant, une série d'attaques a été menée par les Nashi, un groupe de hackers ultranationalistes russes proches du Kremlin, sur les sites

gouvernementaux d'Estonie. Elle fut lancée au prétexte d'une défense des communautés russophones face au gouvernement estonien qui avait fait déplacer un monument aux morts de l'Armée rouge près d'un cimetière militaire, à la périphérie de Tallinn. Début mai, il devient impossible d'obtenir des documents depuis les serveurs informatiques des sites nationaux, mais aussi à l'administration de travailler et de communiquer. Les banques sont à leur tour ciblées, privant les Estoniens des opérations bancaires courantes, de régler leurs factures ou d'acheter des billets de train ou d'avion. Les pompes à essence s'assèchent, puisqu'il est impossible de gérer les stocks, d'acheter et d'acheminer du carburant. Les Estoniens ne peuvent plus entrer ni sortir du pays, pendant quelques jours, pas plus qu'ils ne peuvent aller d'une ville à l'autre.

D'autres attaques prennent pour cibles les compagnies d'électricité: les ascenseurs cessent de fonctionner, ce d'autant plus qu'ils sont gérés à distance par des serveurs informatiques. De manière sporadique l'éclairage public est coupé, ainsi que les centrales alimentant Tallinn. Les chaînes de télévision et de radio ont cessé d'émettre, les ordinateurs sont éteints, la capitale est plongée dans une nuit noire. Pendant une très longue heure, le 2 mai, les urgences sont déconnectées. Dans le même temps, des militants pro-russes sont descendus dans les rues, tandis que les habitants de Tallinn se demandent ce qu'il se passe: est-ce une manifestation? une émeute? une nouvelle invasion de l'Estonie par l'armée russe? Menée plus avant, avec de véritables factions séditieuses, l'attaque aurait été meurtrière, sanglante, et aurait pu conduire au coup d'État.

Cette attaque fut conduite de manière extrêmement simple par les Nashi, par un moyen à la portée de n'importe quel groupe insurrectionnel : elle procède par déni de service (DoS), c'est-à-dire par une multiplication des requêtes informatiques sur un serveur jusqu'à ce qu'il sature. Les Nashi infectent un ordinateur à distance, par le biais d'un virus d'abord inactif. Au 27 avril, ils font réveiller l'ensemble des machines, et leur ordonnent de toutes se connecter au même site en même temps, de le réactualiser sans cesse, jusqu'à ce que le serveur visé rejette toute tentative de connexion. Si vous aviez un ordinateur branché à internet en 2007, il est tout à fait probable que vous y ayez participé à votre insu. Cette technique, appelée Botnet, est largement employée par Anonymous, et pourrait tout à fait être récupérée par un groupe tel que Daech. Cela est d'autant plus probable que, comme vient de le révéler Jean-Paul Rouiller, ancien des services secrets suisses et fondateur du Geneva Centre for Training and Analysis of Terrorism (GCTAT), un des membres d'Anonymous, "un ingénieur informaticien suisse récemment converti à l'islam" aurait rejoint Daech pour y monter un groupe de hackers.

L'on se trompe en croyant que Daech ne possède pas la technologie nécessaire pour mener des attaques internet de grande ampleur en Occident et, plus encore, de penser qu'elles puissent être moins virulentes que les attentats : en 2008, la Russie a cloué l'aviation géorgienne de Tbilissi au sol et engagé une véritable guerre de l'information par ce biais; en février 2011, les États-Unis ont réussi à stopper le programme nucléaire iranien en introduisant le virus Stuxnet dans les centrifugeuses de Natanz, les faisant exploser par d'infinies variations de température. Il est possible de faire exploser une centrale nucléaire avec un virus. En 2013, Barack Obama avait fait valoir que la principale menace pesant sur la défense des États-Unis était précisément un virus se concentrant sur les centres névralgiques du pays:

les serveurs contrôlant la distribution d'électricité et les centrales, et les serveurs ultra-protégés de Wall Street.

Dans la majeure partie des cas, une attaque DoS ou de type Stuxnet requiert très peu d'hommes sur le terrain, et des moyens financiers extrêmement réduits pour une grande efficacité. Cinq ingénieurs mercenaires parmi les meilleurs, n'ayant d'autre appât que le gain, et sans même d'accointance avec Daech, peuvent conduire un État à la faillite, comme une quarantaine de hackers activistes, dans une opération planifiée et bien réglée peuvent mettre à sac une capitale européenne.

Toronto Star

Gmail not immune to FOI requests

Wednesday, 10 February 2016

Byline: David Rider

Section: general

Ottawa - Ontario's Information and Privacy watchdog will soon remind politicians and civil servants that using Gmail, Hotmail or BlackBerry Messenger will not hide official communications from freedom-of-information requests.
"I would acknowledge that there may be information that should have been disclosed but hasn't been because of a lack of knowledge of what the rules are," commissioner Brian Beamish said in an interview Tuesday.

"If the email is dealing with government or agency or municipal business, it is subject to the legislation. It doesn't matter what device or account it is sent from."

The Star reported last week that Beamish's office ordered an Oshawa city councillor to disclose a 2013 email, involving a $5.9-million land deal, written on her personal account.

The issue exploded into U.S. headlines with revelations that Democratic nominee hopeful Hillary Clinton not only used private email for State Department business but had her own unsecured home server.

It is well known in Ontario political circles that some elected officials and their staff members use personal email, BBM and other online tools, including Google Calendar, for some official business.

Beamish said that, in the wake of discussions generated by the Oshawa story, his office is preparing guidelines to reinforce past assertions that work emails, regardless of how they're sent, are subject to Ontario's Freedom of Information and Protection of Privacy Act and a similar act covering municipal governments.

"I have no doubt that there is still a lack of knowledge of that out there," Beamish said. "We could probably do a better job at getting that message out."

The commissioner, who succeeded Ann Cavoukian in 2014, said he senses information and privacy officers in government offices understand the rules, but that some officials asked to turn over their relevant correspondence do not.

Just because an email is subject to the act doesn't mean the public will learn its contents.

Transparency advocates say Canada is behind some other countries in this respect. Politicians and bureaucrats routinely invoke exemptions that can see pages of released information blacked out in whole or part.

The Oshawa case was also notable because it was a city councillor, not a mayor or civil servant, forced to disclose an official communication.

Beamish acknowledged that most requests for councillors' communications are denied.

Generally, emails, letters and the like are not subject to the act when they are "political" - including communications with constituents and lobbyists.

Communications about official business, when they are acting as cabinet ministers, as parliamentary secretary or, at city hall, a committee chair, are fair game.

Beamish last year repeated Cavoukian's three-year-old call for Ontario Premier Kathleen Wynne's government to amend freedom-of-information laws to improve public access to communications generated by the municipal councillors they elect.

Mark Cripps, a spokesman for Municipal Affairs Minister Ted McMeekin, told the Star the minister recently met with Beamish about his suggested reforms. However, the government, including the Government and Consumer Services Ministry that oversees the acts, is still determining "the best path forward."

The Australian

Sub crew data 'too secret to reveal'

Wednesday, 10 February 2016

Byline: Cameron Stewart

Section: general

Canberra - The navy has slapped the first secret classification on the number of Australian submarine commanders and crew, claiming that revealing the figure would give foreign intelligence services too much information about the nat-ion's defence during growing strategic tension in the region.
The move comes as the navy faces a critical shortage of qualified submarine commanders, raising claims it is aimed at hiding bad news rather than for genuine security concerns.

The Australian understands the navy has failed to boost its ranks of qualified submarine commanders in the past five years, with a number of them failing the highly demanding "Perisher" command training course that qualifies them to captain a submarine.

As a result, the current Collins-class submarine commanding officers are a "Dad's Army". Four of the five commanders gained their Perisher qualifications between 15 and 24 years ago, two were lured back after retiring from the navy and another was recruited from the British Royal Navy.

The navy admitted in 2013 that it was concerned it had only 16 Perisher-qualified submarine officers, only a small handful of whom were actually available to command a submarine because others were too senior. Since then, only one extra officer has passed the course, meaning the navy has barely enough commanders available for its Collins-class fleet.

When independent senator Nick Xenophon recently asked the navy how many qualified submarine commanders it had, he was told the figure was classified despite it having been revealed at defence estimates hearings previously in 2013, 2011 and 2009.

Defence says it has changed its policy on national security grounds because of the growing number of foreign submarines in the region. China has recently embarked on an aggressive push to increase the size and capabilities of its submarine fleet.

A Defence spokesman said: "Regional nations continue to grow and develop their own submarine capabilities. This competitive environment reinforces the imperative to protect the capabilities and vulnerabilities of the Australian Submarine Force from foreign intelligence exploitation.

"Submarine workforce numbers, including the number of command qualified officers have been deemed sensitive as this data would assist intelligence agencies to assess the strength of the Australian

submarine force (and) in identifying the number of submarines that Australia could support and operate." Senator Xenophon said it was outrageous that Defence would suddenly classify these figures. "Defence can't use the cloak of nat-ional security to hide their failings in planning for our future defence needs," he said. "They need to fix the problem rather than try to submerge the truth from coming out. They can't make secret something that has been out in the open previously." The decision to classify the number of qualified submarine commanders is not particularly effective, given they are all listed by name on an honour board at the HMAS Stirling naval base in Perth. Their names and graduation dates are also listed in a recent book, A History of Australian Submarines, by Michael White.

The lack of qualified submarine commanders reflects the navy's inability to attract and promote enough prospective candidates. It also reflects the high failure rate -- often 50 per cent -- of the Dutch-run Perisher commander course in which candidates learn to command a submarine in sophisticated simulated war games involving surface ships, submarines and warplanes.

As well as commanders, the navy has struggled to train and attract enough submarine crews to man its four active submarines.

Navy chief Tim Barrett said in October there was still a sizeable shortfall of qualified submariners. The navy is taking steps to improve its recruitment of submariners, including substantial extra cash payments and a submarine workforce growth strategy to improve recruitment and retention.

Defence says a new employment package to begin this year includes seven enhanced conditions including extra payments "to assist with improving retention and to re-attract personnel back to the submarine workforce".

Senator Xenophon said it was a concern for the navy that its submarine commanders were such veterans and this showed there were too few new commanders coming through the system. "With no new blood in the system, our defence capability with become anaemic," he said.

Of the five current Collins-class commanders, HMAS Farncomb commander Ian Bray achieved Perisher qualifications in 1992, while HMAS Waller commander Richard Lindsey passed the course in 1998. HMAS Rankin commander Douglas Theobald qualified in 2000 while HMAS Sheean commander Jason Cuples passed Perisher in 2001. The most recently graduated Collins-class commander is HMAS Dechaineux's Robin Dainty in 2007.

Yonhap News Agency

Russia expresses concern to S. Korean envoy over THAAD decision

Wednesday, 10 February 2016

Section: general

Russia's Foreign Ministry on Tuesday expressed concerns to South Korea's ambassador over Seoul's decision to begin formal consultations on bringing in the U.S. THAAD missile defense system to the country to defend against North Korean threats.
Russian Deputy Foreign Minister Igor Morgulov conveyed the concern during a meeting with Amb. Park Ro-byug, the ministry said.

Shortly after North Korea's missile launch on Sunday, South Korea and the U.S. jointly announced they would begin official discussions on the possible placement of the U.S. Terminal High Altitude Area Defense (THAAD) missile defense system in South Korea.

Like China, Russia has opposed the possible deployment of THAAD, seeing it as a threat to their security interests.

The U.S. has repeatedly said that the system is aimed only at deterring North Korean threats.

Yonhap News Agency

National Assembly adopts resolution denouncing N.K. missile launch

Wednesday, 10 February 2016

Section: general

The National Assembly Wednesday endorsed a resolution censuring North Korea's recent rocket launch, demanding additional retaliation measures from the Seoul government.
The resolution, which was put to a vote during an extra session, was passed 241-0, with seven abstentions, three days after the North fired off a long-range rocket and placed a satellite into orbit.

The resolution urges Pyongyang to stop weapons development and become a responsible member of the international community, stressing repeated provocations will only deepen the impoverished regime's isolation.

"North Korea's long-range missile launch, in addition to the fourth nuclear test, is a clear violation of the U.N. resolutions," it said.

South Korean lawmakers also said they will cooperate with the government and the international community to come up with strong countermeasures to stop the recurrence of such provocations.

It marks the second resolution denouncing the North since the assembly unanimously passed a resolution condemning its fourth nuclear test last month.

South Korea is currently working with the U.S., Japan and other regional powers for the swift adoption of a U.N. resolution to slap strong sanctions on North Korea.

North Korea has already been under U.N. sanctions for its three previous nuclear tests: in 2006, 2009 and 2013.
Reuters

North Korea satellite in stable orbit but not transmitting - U.S. sources

Wednesday, 10 February 2016

Section: general

North Korea's recently launched satellite has achieved stable orbit but is not believed to have transmitted data back to Earth, U.S. sources said of a launch that has so far failed to convince experts that Pyongyang has significantly advanced its rocket technology.
Sunday's launch of what North Korea said was an earth observation satellite angered the country's neighbours and the United States, which called it a missile test. It followed Pyongyang's fourth nuclear test in January.

"It's in a stable orbit now. They got the tumbling under control," a U.S. official said on Tuesday.

That is unlike the North's previous satellite, launched in 2012, which never stabilized, the official said. However, the new satellite was not thought to be transmitting, another source added.

U.S. President Barack Obama spoke with the leaders of South Korea and Japan by phone on Monday night and reassured them of Washington's support, while also calling for a strong international response to the launch, the White House said.

Obama will also address North Korea's "provocations" when he hosts the leaders of the Association of Southeast Asian Nations in California early next week, aides said.

The United States and China, Pyongyang's only major ally, are negotiating the outline of a new U.N. sanctions resolution that diplomats hope will be adopted this month.

The U.N. Security Council has imposed sanctions against North Korea for its nuclear tests and long-range rocket launches dating back to 2006, banning arms trade and money flow that can fund the country's arms programme.

But a confidential U.N. report, seen by Reuters, concluded that North Korea continues to export ballistic-missile technology to the Middle East and ship arms and materiel to Africa in violation of U.N. restrictions.

The report by the U.N. Security Council's Panel of Experts on North Korea, which monitors implementation of sanctions, said there were "serious questions about the efficacy of the current United Nations sanctions regime."

Western diplomats told Reuters that restricting North Korean access to international ports is among the measures Washington is pushing Beijing to accept in the wake of the Jan. 6 nuclear test and the weekend rocket launch.

"PROVOCATIVE, DISTURBING AND ALARMING"

Missile experts say North Korea appears to have repeated its earlier success in putting an object into space, rather than broken new ground. It used a nearly identical design to the 2012 launch and is probably years away from building a long-range nuclear missile, the experts said.

Vice Admiral James Syring, director of the U.S. Missile Defense Agency, told reporters that North Korea's launch was "provocative, disturbing and alarming," but could not be equated with a test of an intercontinental ballistic missile.

He said North Korea had never attempted to flight test the KN-08 intercontinental ballistic missile it is developing.

Syring said U.S. missile defences would be able to defend against the new North Korean missile given efforts to improve the reliability of the U.S. system and increase in the number of ground-based U.S. interceptors from 30 to 44.

"I'm very confident that we're, one, ahead of it today, and that the funded improvements will keep us ahead of ... where it may be by 2020," he said.

The latest North Korea rocket was based on engines taken from its massive stockpile of mid-range missiles based on Soviet-era technology and electrical parts too rudimentary to be targeted by a global missile control regime, experts said.

South Korea's defence ministry believes the three- stage rocket, named Kwangmyongsong, had a potential range of 12,000 km (7,457 miles), Yonhap news agency reported, similar to that of the 2012 rocket and putting the U.S. mainland in reach.

"I suspect the aim of the launch was to repeat the success, which itself provides considerable engineering knowledge," said Michael Elleman, a missile expert at the International Institute for Strategic Studies.

Separately, U.S. National Intelligence Director James Clapper said on Tuesday that North Korea could begin to recover plutonium from a restarted nuclear reactor within weeks.

Clapper said that in 2013, following its third nuclear test, the North had announced its intention to "refurbish and restart" facilities at its Yongbyon nuclear complex.

"We assess that North Korea has followed through on its announcement by expanding its Yongbyon enrichment facility and restarting the plutonium production reactor," Clapper said in prepared testimony to the Senate Armed Services Committee.

Sunday Telegraph (UK)

Hunt for LinkedIn terrorist

Sunday, 14 February 2016

Byline: Robert Verkaik

Section: general

London - A dangerous British terrorist who helped recruit the Isil executioner "Jihadi John" is being hunted by the security services after fleeing to Turkey and setting up an account with LinkedIn, the business networking site.
Rabah Tahari, from Birmingham, is the leader of a jihadist group linked to al-Qaeda who the Home Office claim founded a terrorist militia in Syria four years ago which recruited many British fighters. Now British and Turkish security services are concerned that he has fled the battlefield and moved to Turkey, where he gave away his location when he joined LinkedIn.

Fears are mounting that Tahari, 44, will make his way back to Europe to carry out terrorist attacks. Tahari has taken part in key operations in Syria where he and his fighters were trained in a range of weapons. It is estimated that up to 50 British jihadists are hiding out in Turkey, where they can plan terror attacks against the West without fear of coalition bombing raids.

Wall Street Journal

Tensions Rise Over Refugees

Saturday, 13 February 2016

Byline: Miriam Jordan

Section: general

Boise, Idaho - For decades, refugees have augmented the workforce of this sparsely populated state. Refugees operate machines at the research- and-development facility for memory chips at Boise-based Micron Technology Inc. About a third of workers at Chobani Inc.'s yogurt plant in Twin Falls, the nation's largest, are refugees.

But since terror attacks in Paris and San Bernardino by people at least inspired by Islamic extremists, there has been a backlash against settling refugees here and elsewhere, particularly from Iraq and Syria. That has created tension between politicians sensitive to their constituents' concerns and business leaders who say that the state needs the newcomers to keep thriving.

"I hope that will go away," said Tim Komberec, chief executive of Idaho-based Empire Airlines, of anti-refugee rhetoric, at an event convened to tackle the state's labor shortage. "We need workers in this state." He said his company values a diverse workforce.

Home to 1.6 million people, Idaho is among the states with the largest number of refugees relative to overall population, having absorbed nearly 30,000 from 53 countries since Vietnamese evacuees first arrived in the 1970s. Since 2008, the state has received about 1,000 refugees annually -- mostly from Africa, Asia and the Middle East -- out of 70,000 that have been resettled in the country each year. About 70% have been sent to Boise, the capital, with the rest going to Twin Falls, its commercial hub. Idaho recently has received refugees from Iraq, Somalia and Bhutan, among others.

"Refugees have become a valuable workforce," said Bob Naerebout, executive director of the Idaho Dairymen's Association, a lobbying group.

Still, Idaho Gov. Butch Otter is among about two dozen governors, primarily Republicans, who have called for at least a temporary halt to the refugee program over fears that it could allow terrorists to sneak into America.

"I have never seen this much attention in Idaho to refugee resettlement from elected officials or the general public," said Patrice Haller, assistant director of the Idaho Office of Refugees, which coordinates resettlement in the state.

President Barack Obama has agreed to take 85,000 people fleeing their homelands, including 10,000 Syrians, in the fiscal year that ends Sept. 30. Alabama and Texas have sued the federal government to stop refugee settlement in the wake of the terror attacks.

Proponents say refugees are the most thoroughly vetted of any travelers, undergoing background checks, multiple interviews, iris scans and other screening. Critics say Washington lacks control over the process, which involves the United Nations and U.S. subcontractors, as well as U.S. intelligence agencies.

Idaho's unemployment rate of 3.9% is well below the national rate, and its year-on-year job growth of 4.4% in December was the fastest of any state. But Idaho says over the next decade it will see a widening gap between job growth and the growth of its working-age population. It has a shortage of workers in high-tech, manufacturing and other sectors, and among transplants to the state are many retirees.

Many refugees have university degrees and often fill higher-tech jobs. While working at a Wal-Mart for six months, Mudhafar Poules, an Iraqi computer programmer, prepared a resume and brushed up on his English. Last July, he landed an IT position at Boise State University.

In Twin Falls, they have been a diverse and committed part of Chobani's workforce, a spokesman said. Snack maker Clif Bar & Co. has begun hiring workers, including immigrants, for a baking facility set to start operating this spring, according to a spokeswoman.

Republican state Rep. Stephen Hartgen praised refugees' work ethic, saying they have started businesses, toiled in dairies, and joined the school board and police force in his district. But now, he said, "The security concern is real; people are conflicted."

The state remains divided. In January, about 150 people lined a hall at the Idaho Capitol to show support for refugees, while about as many gathered in a Capitol auditorium to hear two guest speakers who criticized the U.S. refugee program and highlighted the jihadist threat.

College student Elia Sherman, standing at the Capitol event, said refugees bring diversity. "We want an inclusive community," she said.

Inside the auditorium, Frank Marcos, a retired baseball-league scout, said, "I'm concerned about individuals wanting to do us harm."

Meanwhile, refugees continue filling jobs in Idaho, including Rasha Al-Zaidi, a 33-year-old Iraqi mother of two girls whose family arrived in Boise 18 months ago.

Ms. Al-Zaidi, who was a hospital pharmacist in Baghdad, got counseling from a program that helps refugees transfer skills to the U.S. workplace. After interning at Ladd Family Pharmacy last year, Ms. Al-Zaidi was hired full-time as a pharmacy technician, earning $14 an hour.

Said pharmacy owner Elaine Ladd: "There is a shortage of people with the skills I need; Rasha deserved an opportunity."

The Advertiser

French teen link to school bomb threats

Saturday, 13 February 2016

Byline: Katrina Stokes

Section: general

Canberra - A teenager linked to school bomb threats across the world, including in Adelaide, is being quizzed by anti-terror police in France.
Vincent Lauton, 18, is being held in connection with hoax threats in Europe, Asia, the US and Australia.

The threats - allegedly with the message "You Will Die" - have led to mass evacuations. More than 20 South Australian schools have been targeted in the past week, including at least two yesterday.

Lauton is known to be a hacker and is described as a "sophisticated computer operative", according to French police. He is linked to the "Evacuators 2K16" bomb hoaxers, who called on children to tweet if they wanted their school shut down.

Heavily armed police descended on Lauton's family home in the village of Marsannay le Bois, near Dijon, on Monday. He was taken to a Paris police station and his custody extended under emergency powers in place since the jihadist shootings and bombings that killed 130 people in Paris on November 13.

Lauton is reportedly the administrator of the darkness.su domain where the other alleged hoaxers are operating.

Sources said police arrested him in connection with the investigation into telephoned hoax bomb threats that forced schools in Paris to be evacuated. He was tracked down through his internet IP address.

Police and investigation sources said computer equipment had been taken from the house he shares with his parents for examination.

Between January 26 and February 1, schools in France and England received pre- recorded phone calls telling staff bombs had been planted. Police found no evidence of any explosive devices.

"The probe is trying to establish if there is a link between calls targeting high schools in Paris and threats against schools in other parts of the country, mainly in Lyon. We can't rule anything out," a judiciary source said.Schools in Adelaide including Adelaide High, Magill Primary, Norwood Morialta High and Banksia Park International High School have received hoax bomb threats in the past two weeks, causing mass student evacuations and classroom lockdowns.

The Daily Telegraph

GCHQ wins legal backing for hacking

Saturday, 13 February 2016

Byline: Tom Whitehead

Section: general

London - A fifth of GCHQ intelligence comes from hacking into phones and computers, the agency has revealed, as it won a human-rights victory in defence of its once-secret technique.
The spy agency admitted last year that it regularly hacks into electronic devices - known as equipment interference - to gather data on suspects. It was forced to defend the power before the Investigatory Powers Tribunal after a civil-liberties group and internet companies claimed that it breached human-rights laws. But the panel, which hears challenges against the security and intelligence agencies, yesterday ruled the methods were lawful. In submissions to the hearing, it emerged that in 2013 about 20 per cent of GCHQ intelligence reports contained information derived from hacking.

The tactic, also known as computer network exploitation, allows authorities to interfere with electronic devices such as smartphones, tablets and PCs to obtain data.

Operations range from using a target's login credentials to access information on a computer, to remotely installing a piece of software to obtain the desired intelligence and covertly downloading the contents of a mobile phone.

The methods are seen as an increasingly crucial tool as advanced encryption makes it more difficult for security services to keep track of terrorists.

The tribunal concluded that the legal regime under which warrants are issued for the agency to carry out equipment interference in the UK is compatible with European Convention on Human Rights articles.

Washington Post

British teen arrested in hacking of U.S. intelligence officials

Saturday, 13 February 2016

Byline: Matt Zapotosky & Ellen Nakashima

Section: general

Washington - British authorities have arrested a 16-year-old suspected of being involved with a group that hacked into the private email accounts of high-ranking U.S. intelligence officials, according to U.S. officials and British police.
The teen is said to be connected to the cohort that calls itself Crackas With Attitude, which has claimed to have broken into the private email accounts of CIA Director John O. Brennan and Director of National Intelligence James R. Clapper. What part the teen played is unclear, and U.S. officials, who spoke on the condition of anonymity to discuss the case, said they are still investigating the roles of others.

Spokespeople for the FBI and Justice Department declined to comment. The South East Regional Organized Crime Unit - a British police force cooperative - confirmed in a statement it arrested a 16-year-old boy Tuesday on suspicion of three computer-related charges, but it would not comment on links to the hacking of American officials. The group said the boy was released on bail until June.

The teen's arrest and connection to the hacks on U.S. intelligence officials were first reported by CNN.

FBI agents and federal prosecutors in the Eastern District of Virginia have been investigating Crackas With Attitude for months, working to build a case that they hope might land at least some of them in a U.S. courtroom. The group has been outspoken about its cyber mischief, providing reporters with evidence that members successfully broke into the personal files of top U.S. intelligence officials.

The group is also thought to have leaked the names and work email addresses and phone numbers of thousands of Homeland Security and FBI employees. In that case, none of the email addresses and numbers was personal, but they still could be of use to overseas intelligence agencies.

The teen's arrest is a significant development in the case, although as yet, no one is facing any U.S. charges.

A person claiming to be an American high school student told the New York Post last year that he used "social engineering" to dupe Verizon workers into turning over Brennan's personal information and AOL into resetting his password. The person apparently accessed Brennan's personal email account, which contained a 47-page application for a top-secret security clearance.

Early this year, a person going by the nickname "Cracka" told the magazine Motherboard that he had accessed a series of accounts linked to Clapper, including his home telephone and Internet, his personal email and his wife's Yahoo email account.

Vice News Canada

A Former Special Forces Soldier is Setting Up a Massive Private Military Facility in Ontario

Saturday, 13 February 2016

Byline: Sandro Frenguelli

Section: general

Ottawa - On the surface, Brockville is just another quaint small town in Ontario. Situated in the Thousand Islands, residents enjoy tasteful concerts and exhibits at the historic Brockville Arts Centre and tourism writeups will inevitably refer to the town of 20,000 as "charming."
But just out of town, Steve Day, a former special forces soldier, wants to show people the best way to breach buildings and take down targets using assault rifles, shotguns, and semi-automatic pistols.

The retired lieutenant- colonel and former commander of Canada's secretive JTF-2 special operations unit and his company, Reticle Ventures Canada, plan to invest $50 million to transform a 400-acre section of Tackaberry Airport into Canada's most advanced private training facility for militaries and first responders.

"This is going to be an innovation arena for leading-edge soldier systems technology," says Day, whose specialty was combat engineering.

Brockville is the landlord and the owner of the property, but the airport also falls within the jurisdiction of neighboring Elizabethtown- Kitley. Brockville will sign the lease agreement, while Elizabethtown must approve the site plan.

Plans for the facility, which is partially operational and is slated for a grand opening at the beginning of April, include a 10,000-square foot schoolhouse, a 50-meter outdoor firing range, a 25-meter indoor firing range and an aircraft hangar. Reticle also wants to construct a "simulation village" to give students as much realism as possible when learning how to deal with urban assaults and hostage situations on Canadian soil.

The military contracting industry isn't especially new to Canada. There are several aerospace contractors and other specialty manufacturers based here and London, Ontario-based General Dynamics landed a controversial $15-billion deal to supply Saudi Arabia with light armoured vehicles. However, Brockville residents, among others in Canada, are witnessing the growth a little known offshoot: a private military training business.

Tundra Strategies, based in Stayner, Ontario, and Millbrook Tactical, based in Stittsville, Ontario, have both worked with the Canadian Department of National Defence (DND). Millbrook has trained DND

employees in the use of firearms and Tundra has taught drivers how to keep their vehicles shiny-side up in conflict zones.

"We have trained the OPP, RCMP, military, and government agencies. We can't keep up with business at the moment," says Francois Paquette, president of Millbrook Tactical.

Reticle's Brockville project, however, represents an ambitious departure for Canada's private military training industry. Paquette says, "Nothing like this exists in the Canadian private sector." Tundra, for example, runs a training facility of its own but it just has classrooms for theory based learning. For practical training, they use local off-site facilities. The Tackaberry site will see straight-up live-fire exercises. As such, the facility is proving worrisome to quite a few people in the community.

"It doesn't seem to make sense to have bullets flying around at a small municipal airport," says Brant Burrow, a member of the Elizabethtown-Kitley Residents Association.

Tackaberry is a special case: training amenities will be on-site while the airport itself will stay operational as a public airport.

This means that those looking to be trained in the art of war will have to play nice with those trying to land their Cessnas. Rob Smith, an Elizabethtown-Kitley councillor, says, "Reticle is building earth berms between the firing point, the runway, and the airport buildings that will be tall enough to obstruct the line of sight."

Though the above mentioned features, along with strict government safety guidelines, are designed to provide protection from projectiles and noise, residents are still troubled. During Reticle's own on-site ammunition sound tests last summer, nearby residents thought they were in the middle of a war zone, says Burrow.

"There just seems to be a risk there even if the risk is low. I don't dispute that there might be a one-in-a-million chance of a stray bullet hitting a plane or a person or what have you. It may be a low risk but the consequences are dire of that one incident," he adds.

Day is hoping to attract Canadian first responders and to repatriate Canadian dollars spent on sending our men and women abroad to train. He says that he has also had ample interest from private domestic and international clients, which has raised yet more concern for residents. "Just exactly who is Reticle going to be training here? What if someone gets a hold of a gun that shouldn't have one?" asks Burrow.

Brockville has yet to sign the lease agreement with Steve Day, and, according to Mayor David Henderson, the city has imposed its standard noise bylaws on the agreement. And while everything about the project seems to be moving forward, Burrow assures me that he is going to continue being vigilant. "We're in it for the long haul. We are not against these facilities by any means. We are not against Reticle. We said right from the beginning that it's a good project, but it's the wrong place."

Reticle's project is likely to change the face of the Canadian private military training industry for the simple fact that nothing like this exists here. The one-stop shop model of tactical training made famous by sprawling US compounds, like Academi's Moyock, North Carolina facility, is moving north of the border. In the very near future, innocent and idyllic Brockville could be playing host to a much more hardcore tourist.

iPolitics.ca

What happens when our spies break the law? Nothing, apparently.

Saturday, 13 February 2016

Byline: Andrew Mitrovica

Section: general

Comment: The past few weeks have offered a sobering reality check for anyone who actually believes Liberal governments differ from Conservative governments when it comes to holding the nation's spies to account.
What we've seen and heard are the same tired excuses offered up by ministers with the same titles, trying to explain away the inexcusable while mouthing the same vague promises to finally keep our spooks in check.

First, we learned that CSIS was up to its old, dirty tricks when it was revealed that the civilian spy service repeatedly obtained the tax records of an unknown number of Canadians without troubling to get a warrant from a judge.

We were told not to get too bent out of shape about it, since this shady trafficking in Canadians' confidential tax information was the work of a "rogue" Canada Revenue Agency official who has since left the CRA, voluntarily or involuntarily. (The lone gunman strikes again.)

Then, we were belatedly informed that the super-secret electronic snoops working at the Communications Security Establishment (CSE) illegally shared the supposedly private "metadata" of an untold number of Canadians with a spate of foreign spy agencies. This, we were told, was the result of a technical glitch.

Eva Plunkett, former Inspector General for CSIS, has heard these cockamamie cover stories before, and she still isn't buying any of it. In report after report, Plunkett warned Canadians and a revolving cast of

Public Safety ministers that leaving too much power in the hands of even well-intentioned spies is not only dangerous, it leads inevitably to these sorts of illegal shortcuts.

"That's often the explanation -- 'Oh, it was inadvertent or misplaced,'" Plunkett told iPolitics in an exclusive interview last week. "These are words these agencies often use. They have a problem with being frank ... (with) saying, 'This is what happened and we will be honest about it.'"

(Plunkett retired in 2012 shortly before Stephen Harper shuttered her tiny operation because accountability-allergic spymasters complained that she was a bothersome burr in their hides.)

Plunkett says that Prime Minister Justin Trudeau needs to seize the moment by doing what successive Liberal and Conservative governments have failed to do: establish real and robust parliamentary oversight -- not after-the-fact review bodies -- to train a keen eye on these extraordinarily powerful intelligence services.

"There's an opportunity now to do something that might be effective in terms of oversight," Plunkett said. "I'm a believer in a Parliamentary committee. That would be a good thing."

Public Safety Minister Ralph Goodale appears to be a believer too ... with a convenient caveat. At a hastily-arranged press conference late last month, a slightly rattled Goodale -- with Defence Minister Harjit Sajjan in tow (he's responsible for CSE) -- repeated his pledge to set up a parliamentary "mechanism" to ensure that the spooks are "properly respecting Canadian rights and freedoms."

What many missed in Goodale's polished statement was the absence of any acknowledgement or condemnation of the fact that these intelligence agencies broke the damn law. Goodale and Sajjan don't need to wait for the findings of their "review" of Canada's national security infrastructure to act. They can call in the Mounties right now. They should.

Failing to do so means sending the same message to Canadians their predecessors sent -- that our intelligence services operate somewhere beyond the law, immune from the consequences that ordinary people face.

Word is that Goodale's parliamentary "mechanism" to watch the watchers may resemble those already in place in a variety of Commonwealth countries, including Australia, Great Britain and New Zealand.

The problem -- as the Toronto Star's Thomas Walkom recently pointed out -- is that these mechanisms often provide only an illusion of accountability. The so-called parliamentary leashes -- to the degree they exist on paper -- tend to be rather loose.

Plunkett says that without the proper resources, expertise, money, political will and legal power, no mechanism Goodale comes up with will amount to more than window dressing.

"You have to have a group of experienced researchers that know the subject matter, that know how to do the analysis and (have) no fear in bringing forward negative information," she said.

Plunkett insists that a parliamentary committee will work only if Goodale establishes a well-staffed, well-funded "independent office" that reports its findings to the committee for further review. "Parliamentarians obtain the information, but they don't actually do any of the detailed work themselves, beyond posing questions."

Some media-friendly academics welcomed Goodale's appointment as Public Safety minister as a sign that this government is committed to oversight. Like Plunkett, I'm not convinced. Recall that Prime Minister Trudeau kept Richard Fadden on as his national security advisor. Fadden was Harper's loyal national security advisor when he told a Senate committee that CSIS already has too many eyes prying into its business.

And earlier this week, Trudeau took up Harper's cowardly court fight to withhold a federal apology and compensation for three Canadians tortured in the Middle East (despite having championed their pursuit of justice while in Opposition) -- in part to protect the identities of CSIS officers implicated in their cases.

Sunny ways? Or just the same old methods of operating beyond the law, in the dark?

Andrew Mitrovica is a writer and journalism instructor. For much of his career, Andrew was an investigative reporter for a variety of news organizations and publications including the CBC's fifth estate, CTV's W5, CTV National News -- where he was the network's chief investigative producer -- the Walrus magazine and the Globe and Mail, where he was a member of the newspaper's investigative unit. During the course of his 23-year career, Andrew has won numerous national and international awards for his investigative work.

USA Today

IRS crash was technical, not cyber

Monday, 15 February 2016

Byline: Kevin McCoy

Section: general

Washington - The computer outage that halted IRS tax return processing for more than a day resulted from not just one hardware failure but two, the tax agency says.

An electrical voltage regulator on the computer server that handles tax returns for millions of Americans started to fail on Feb.3, Terence Milholland, the IRS' chief technology officer, testified at a Thursday hearing of the House Committee on Oversight and Government Reform.

As a technician worked to address the problem, a backup voltage regulator also failed, he said. Approximately 30 hours elapsed before the IRS was able to fix the regulators and resume normal service.

Seeking to allay any fears that something more sinister might have been to blame, Milholland said, "This was, with absolute certainty, not a cyberattack. It was a failure of mechanical devices."

The episode marked the latest in a series of computer problems that have embarrassed the IRS, and, in some cases, raised the risk that personal information could be accessed, used to steal taxpayers' identities, file fraudulent tax returns and collect refunds.

The tax agency this week disclosed that it detected unauthorized efforts to gain access to e-file personal identification numbers for more than 450,000 Social Security numbers in late January. Approximately 101,000 of those efforts succeeded in accessing an e- file ID number, the IRS said.

No personal taxpayer information on the computer system was compromised, the tax agency said. IRS personnel are now mailing affected taxpayers alerts about the problem.

"Until the IRS takes steps to improve its security program deficiencies and fully implement all security program areas in compliance with (Department of Homeland Security-directed) requirements, taxpayer data will remain vulnerable to inappropriate and undetected use, modification or disclosure," a September 2015 inspector general report concluded.

Colombia Reports

Twitter suspends accounts of Colombia's ELN rebels

Monday, 15 February 2016

Byline: Staff report

Section: general

Bogota - Social media platform Twitter has shut down the official account of Colombia's second largest rebel group, the ELN, just when the guerrillas were stepping up violence ahead of possible formal peace talks.
The guerrillas used their accounts, @ELN_Colombia and @ELN_Ranpal, to disseminate political propaganda and updates on the preliminary talks with the Colombian government.

However, over the past week, the ELN has been promoting an "armed strike," a shutdown of economic activity across Colombia. Violations of these imposed guerrilla shutdowns are commonly retaliated, for example by burning trucks or buses that refuse to adhere to the strike.

According to weekly Semana, the ELN ban was due to the fact that Twitter considered this a call to violence, a violation of the social media platform's rules, and the fact the ELN is considered a terrorist group by the US government and not formally engaged in peace talks.

The Twitter Rules disallows users to "make threats of violence or promote violence, including threatening or promoting terrorism."

Additionally, the social media platform's guidelines also "do not allow accounts whose primary purpose is inciting harm towards others on the basis of these categories."

The ELN's website, hosted by a radically leftist server provider in Spain, is accessible as usual. The group is not active on Facebook, the world's largest social media platform.

Twitter did not block the accounts used by Colombia's largest rebel group, the FARC, which has been engaged in peace talks since late 2012 and has mainly been dedicated to the promotion of these peace talks and the publication of their demands.

Asharq Al-Awsat

New App Helps Young Iranians Dodge "Morality Police" Checkpoints

Monday, 15 February 2016

Byline: Staff Report

Section: general

Undisclosed placeline - An anonymous Iranian team of app developers have come up with a new smartphone application that helps Iranians dodge the Islamic Republic's "morality police" known in

Persian as "Ershad" or guidance. The app widely spread among young, tech-savvy population but has quickly fallen foul of the authorities.
The data for the Gershad app is crowdsourced. It depends on reports from users to help others being stopped at checkpoints set up by the morality police, who enforce Islamic dress and behavior codes. Users can tag their location on a Google map with an icon of a bearded man, enabling others to steer clear of them. When the number decreases, the alert will fade gradually from the map.

Gershad is a contraction of the full title of the Gashte Ershad (guidance patrol), which is part of efforts to eliminate Western culture from the country following the Islamic revolution which overthrew a Western-backed king in 1979.

Ershad's notoriety comes out of their role to check for "immoral behavior"--women wearing too much makeup or failing to cover their heads, men too much influenced with Western fashion, or unmarried men and women traveling together are a few examples. The Ershad can issue warnings, demand formal written statements of "repentance," or arrest and prosecute people at their discretion.

The app's developers explained their motives in a statement on their web page saying: "Why do we have to be humiliated for our most obvious right which is the right to wear what we want? Social media networks and websites are full of footage and photos of innocent women who have been beaten up and dragged on the ground by the Ershad patrol agents."

The app was blocked by the authorities soon after it was released for Android devices on Monday but many Iranians bypass Internet restrictions by using a Virtual Private Network.

It is already trending on social media and has received almost 800 reviews on the Google Play app store, nearly all of them positive, although Google Play does not show how many times Gershad had been downloaded.

Gershad is seen by some as a "social movement" setting a precedent for "digital protest" with Iranians turning to technology to evade checks on their everyday lives. This step has surfaced as elections in Iran come into view and the country emerges from years of isolation following the lifting of international sanctions imposed over its nuclear program.

"This is an innovative idea and I believe it will lead to many other creative apps which will address the gap between society and government in Iran," said Hadi Ghaemi, executive director of the International Campaign for Human Rights in Iran.

Ghaemi said the app's developers were based outside Iran but had grown up in the country and experienced the problem firsthand.

"It's really an indigenous product... these are the kind of people who have been stopped at checkpoints," he said.

"It's showing a trend in digital protest... I see it as a precedent for future apps of its kind," said Amir-Esmaeil Bozorgzadeh, a Dubai-based consultant for app makers in the Iranian market.

Smartphone messaging applications are popular among young Iranians who use apps to share news and jokes that would not be allowed in the tightly controlled traditional media.

Many Iranians, especially the young, are hoping that an easing of cultural restrictions follow the lifting of sanctions and the elections on Feb. 26.

However, so far, thousands of moderate and reformist candidates have been barred from standing in the elections.

Le Figaro

Bras de fer pour le contrôle des données des Européens

Monday, 15 February 2016

Byline: Lucie Ronfaut

Section: general

Non identifié - Le ciel leur est presque tombé sur la tête. Le 6 octobre, la Cour de justice de l'Union européenne a déclaré illégal le système dit « Safe Harbor » , qui régissait les transferts de données entre les États-Unis et l'Europe. Au travers de cette invalidation, la justice européenne s'est attaquée à l'empire des grandes entreprises américaines du Web, qui hébergent souvent les données de leurs clients européens dans des centres situés aux États-Unis. Trop dangereux pour la Cour, qui a rappelé dans sa décision les révélations d'Edward Snowden sur la surveillance de la NSA. Comment garantir que les données stockées par Facebook, Google ou Microsoft ne soient pas de nouveaux espionnées par le gouvernement américain ? Même après la négociation d'un nouvel accord pour remplacer le Safe Harbor, appelé « Privacy Shield » , la question demeure.
La solution avancée par les géants du Web est simple : déménager leurs serveurs en dehors des États-Unis. Les plans de construction de data centers en Europe se multiplient. Apple a annoncé début 2015 un investissement d'1,7 milliard d'euros dans la construction de deux centres en Irlande et au Danemark. Microsoft va lui aussi inaugurer trois data centers en Allemagne et en Angleterre. Google va investir 600 millions d'euros aux Pays-Bas. Facebook, enfin, a ouvert une infrastructure à Luleå, en Suède.

La France hors jeu

Depuis l'affaire Snowden, la pression s'était accrue sur les géants du Web pour qu'ils assurent une meilleure protection des données de leurs utilisateurs. « L'annonce de nos nouveaux data centers en Europe après l'invalidation du Safe Harbor est une coïncidence » , confirme Bernard Ourghanlian, directeur technique et sécurité chez Microsoft France. Le géant américain de l'informatique dispose déjà de deux data centers en Europe, en Irlande et aux Pays-Bas. Les deux nouveaux centres allemands seront gérés par une filiale de l'opérateur Deutsche Telekom, en accord avec la loi allemande. De cette manière, Microsoft n'aura pas accès aux données stockées et ne pourra pas être forcé à les transmettre.

La France, elle, ne bénéficie pas encore des attentions des géants du Web. La faute à un cadre juridique trop instable en matière d'hébergement de données. Plusieurs lois concernant directement l'activité des data centers (loi de programmation militaire, loi renseignement...) ont été votées en peu de temps, certaines toujours en attente de décrets d'application. « Il n'y a pas de volonté particulière d'éviter la France » , assure Bernard Ourghanlian. « Mais on ne peut pas prendre de décisions si les règles du jeu ne sont pas claires. » La loi renseignement, adoptée en juin 2015, avait été critiquée par les hébergeurs français, qui craignaient de perdre la confiance de clients étrangers. L. R.

Kapitalis

Poste frontalier de Dhehiba: Installation d'un scanner de véhicules

Sunday, 14 February 2016

Byline: N.H.

Section: general

Dhehiba, Tunisie - Les autorités tunisiennes accélèrent la mise en place des moyens de contrôle aux frontières avec la Libye. Un scanner vient d'être installé à Dhehiba.
Afin de renforcer le contrôle et d'optimiser la surveillance des personnes à ses frontières sud avec la Libye,la Tunisie vient d'installer un scanner pour la surveillance des véhicules de petite cylindrée au passage frontalier de Dhehiba (gouvernorat de Médenine).

Ces équipements sont installés en prévision d'une éventuelle intervention militaire internationale contre les camps de l'Etat islamique (Daêch) et des autres organisations terroristes basés en Libye et qui pourrait provoquer un afflux massif de réfugiés vers la Tunisie.

Il est à rappeler que suite à l'attentat de Tunis, contre un bus présidentiel, le 24 novembre 2015, des scanners avaient été mis en place au poste frontalier de Ras Jedir, le 10 décembre 2015, pour y

renforcer la surveillance. Ces scanners sont destinés à contrôler les poids lourds et à prévenir, notamment, l'entrée d'armes et de produits explosifs pouvant être utilisés par les groupes terroristes.

Yonhap News Agency

N. Korea hackers behind massive spam emails to S. Korea: police chief

Monday, 15 February 2016

Section: general

North Korean hackers sent massive amounts of spam emails to South Korean public organizations last month, South Korea's police chief said Monday, the latest in a series of cyberattacks against the South in recent years.
"We are at a stage to be assured that it was committed by a North Korean hacking organization," said Kang Sin-myeong, commissioner-general of the National Police Agency, announcing the interim outcome of their probe into the case.

The hackers allegedly sent emails disguised as being sent by either the presidential office or the foreign ministry related to North Korea's recent nuclear test.

The Internet Protocol address -- the online equivalent of a street address or phone number -- used to send the spam emails was traced to China's northeastern province of Liaoning bordering North Korea. The network can be used wirelessly from North Korean territory, according to police.

It is the same Internet network behind a cyberattack on South Korea's nuclear power operator in 2014, according to Kang. North Korea is suspected of orchestrating the attack, though it has denied the charges.

Police said similar emails pretending to be from the presidential office or other government bodies have been sent from June 2015 to a total of 759 people.

After probing into 460 of the recipients' occupations, police said 87.8 percent have jobs related to North Korea.

"Looking at the probe results, there is a trace of an intentional and deliberate targeting process that cannot be deemed as a coincidence," Kang said.

Police also said some words in the mails are used only in North Korea.

Although South and North Koreans speak the same language, South Koreans do not understand some North Korean expressions.

The police chief said no major damage to national security has been confirmed due to the attack.

Police said they are planning to conduct an international joint investigation as they found two European servers used to send other spam mails disguised as a notice from a major South Korean portal site.

North Korea has a track record of waging cyber attacks on South Korea and the United States in recent years, though it has flatly denied any involvement.

The latest hacking attempt came amid heightened tensions on the Korean Peninsula after North Korea claimed in January that it successfully carried out its first hydrogen bomb test.

In response, South Korea is working with the U.S. and other regional powers to punish the communist country for its nuclear test and long-range missile launch that shortly followed the January provocation.

Toronto Sun
Trudeau government to take on cybersecurity threats
Friday, 19 February 2016
Byline: David Akin

Ottawa - With Internet-based child sex-ploitation crimes skyrocketing, the Justin Trudeau government intends to launch a "credible and comprehensive" review this spring of cybersecurity threats in Canada. Officials with Public Safety Canada said Thursday that while the details of that review are still being hammered out by Public Safety Minister Ralph Goodale, a review will determine how Canada can best deal with everything from online predators to digital jihadists.

Kathy Thompson, the assistant deputy minister in charge of the Community Safety and Countering Crime Branch at Public Safety Canada, said while the crime rate continues to decline across the country, "there are some exceptions. One of those exceptions is child sexual exploitation over the Internet -- that is going up exponentially, year over year."

Thompson made her remarks at the House of Commons Public Safety and National Security Committee, where MPs are looking for topics their group can zero in on during the current parliamentary session.

A cybersecurity review that looks at legal gaps and shortcomings in police resources could form a plan for the way the Trudeau government approaches law-and-order issues.

"It is our intent to conduct a review that is going to be credible and comprehensive and reaches out to all stakeholders across Canada. And also to our international partners," said Monik Beauregard, the senior assistant deputy minister at Public Safety's national and cyber-security branch.

Liberal MP Marco Mendocino, a former Crown prosecutor who played a key role in putting some of the Toronto 18 terrorists in jail, told the committee he is particularly concerned about financial crime -- the use of computers and telecom networks by organized criminals, including terrorists, to move and hide money -- as well as the use of social media as a breeding ground for online hatred and incitement.

"The fact that we are now so invested in cyberspace can make us vulnerable," said Mendocino.

He wanted to know what the top public safety issues were for Canada's most senior security bureaucrats.

Child sex- ploitation is right at the top of the list, Thompson said.

"That is one of the areas that's keeping us awake. We're working very actively on that. We're partnering not just in Canada but internationally," said Thompson.

Thompson said identify theft and intellectual property crime are two other areas where the crime rate has been rising because of the widespread adoption of the Internet.

Canadian Press
Canada's electronic spy service to take more prominent role in ISIS fight
Friday, 19 February 2016
Byline: Murray Brewster

Ottawa - The Communications Security Establishment, Canada's electronic spy service, is set to play a more prominent role in the war against the Islamic State of Iraq and the Levant, The Canadian Press has learned.
Multiple sources familiar with the plans, speaking on condition of anonymity owing to the sensitivity of the matter, say the government is deploying a capability that only a "handful of countries" in the world can provide.

CSE is part of the so-called "Five Eyes" community, along with the U.S. National Security Agency -- the NSA.

CSE spokesman Ryan Foreman acknowledged the agency is helping the Canadian Armed Forces under the umbrella of Operation Impact, the name of Canada's anti-ISIL mission in the Middle East, but refused to discuss specifics.

"While we are proud of our contributions to CAF's missions, CSE is obligated to respect the Security of Information Act, and cannot address specific operational questions," Foreman said.

Defence Minister Harjit Sajjan has for weeks been signalling that the military will introduce a "more robust" intelligence-gathering regime, one that allies -- chastened by the withdrawal of the six CF-18s -- are happy to be bring to the fight.

Separately, Public Safety Minister Ralph Goodale confirmed Thursday that the Canadian Security Intelligence Service will also play a stepped-up role in the fight against the Islamic State, but he also refused to be specific.

"We are providing new and additional intelligence capabilities in the region and while by its very nature I cannot elaborate, CSIS will have a role to play," Goodale said.

"It will certainly be an increased role to accomplish larger objectives."

The defence conference where Goodale and Sajjan were speaking heard Thursday about how CSIS agents cultivated human sources in Afghanistan.

But CSE played a pivotal role alongside the Canadian Army during the Afghan war, providing by its own admission half of the crucial battlefield intelligence on Taliban militants, their movements and the locations of key commanders.

The information was used to plan military operations and for targeted capture or kill missions by special forces. But one official, speaking on condition of anonymity, said Canadians would provide targeting only and not take part in any "direct action."

Although he's been eager to trumpet the "doubling" of the intelligence effort, Sajjan has been decidedly opaque about what that means, even last week when he announced the retooled mission.

"Enhanced intelligence capability will help protect our forces in theatre as well as those of our coalition and host nation partners," Sajjan said.

"Therefore, we will significantly increase the resources we dedicate to intelligence, both in northern Iraq and theatre-wide. Our intelligence capabilities will help the coalition and Iraqi security forces develop a more sophisticated picture of the threat and improve our ability to target, degrade and defeat ISIL."

What that likely means in practical terms, according to sources and intelligence experts, is the involvement of the secretive CSE and specialists from the 21st Electronic Warfare Regiment.

It also means deploying Canadian intelligence officers into the highly secure all-source intelligence centre in Kuwait, and potentially hacking ISIL computers and smartphones.

When pressed, Sajjan refused to discuss the details.

"Unfortunately, I'm not going to talk (about it) in public for operational security reasons," he said.

"The last thing you want to be able to do is show your hand to (ISIL) and let them know what type of capability you are bringing in, but we have very unique capabilities for the coalition, and what I will say is capabilities for theatre-wide for the entire coalition and then we have very specific capabilities for our troops in the north as well."

Bill Robinson, a blogger and expert on signals intelligence, said it is a matter of public record that the military and CSE have an integrated operational model for field operations, which proved highly successful in Afghanistan.

"It was a pretty substantial contribution on the intelligence side," said Robinson, who noted that signals kept watch over not only the movement of Taliban units and commanders, but also provided early warning of threats -- such as the planting of roadside bombs -- and even kept tabs on local Afghan government officials.

Deploying a similar capability to northern Iraq would, in Robinson's estimation, be a significant step-up in terms of the fight.

"It's a plausible argument that this is a contribution that would be valued just as much as the fighter-bombers," he said. "Increasingly, I think this kind of warfare is down to intelligence."

It is likely filling a gap that the Americans are unable to cover themselves, Robinson added.

Throughout the war against the Islamic State, U.S. commanders have repeatedly called for more intelligence data, mostly in the form of extra drone flights. Washington was forced to strip the remote-controlled aircraft from operations in Afghanistan, according to published reports.

Documents leaked by former NSA contractor Edward Snowden indicate "that in the Horn of Africa and Afghanistan, they were not getting all the signal intelligence they wanted," Robinson said.

That's one of the reasons Canada deployed its own capability to Kandahar during the war, he added.

The game could be upped even further with the purchase of special tactical intelligence surveillance planes, similar to the King Air turboprop aircraft used by special forces in Afghanistan under a contract with the U.S. Army. The federal government quietly floated a letter of interest in September to see if defence contractors could deliver three aircraft.

In addition, Robinson says Canadian intelligence officers are highly valued in multi-national intelligence hubs like the one in Kuwait, because they "are cleared into the Five Eyes community."

Toronto Star
Has Apple secretly leaked your data to government?
Friday, 19 February 2016
Byline: Frederick Ghahramani

OpEd: Apple CEO Tim Cook's now widely shared "Message to our Customers" is an attempt to make the best PR move in a bad situation.
Were Apple to comply with the FBI's request to access information locked on a suspected San Bernardino shooter's phone, it probably wouldn't be the first time that the government has deputized Apple to breach its customers' privacy.

According to documents revealed by Edward Snowden in 2013, Apple was one of the participants in the U.S. National Security Agency's PRISM program, giving authorities access to its customers' information including their emails, messages and photos.

Apple for its part has denied any such involvement, but given the secretive nature of the United States Foreign Intelligence Surveillance Court (FISA Court), Apple and other technology companies would be prohibited to publicly acknowledge their involvement in such programs.

Hence the frustrating catch-22 - is Apple really a champion of privacy rights? Or is all this bluster just an act to score PR points with their customers, despite the fact that legislative conditions already exist to force Apple to co-operate in secret?

Maybe we'll never know, and it probably doesn't matter, because the real lesson that can be learned from this episode is the importance of open source software.

While Apple has invested heavily in encryption and security, most of its systems and applications are closed. For all we know, Apple could already have been secretly compelled to program backdoors into its popular services such as iCloud and iMessage - even against the wishes of its CEO.

In fact, rumours such as this one have been circulating for quite some time. If true, this means that millions of customers could already have had their privacy invaded without ever knowing and, more importantly, the decision to do so would be adjudicated in a secret court, completely out of Apple's hands.

In contrast, in an open source model, the source code of an application is available to the general public, and a global community of curious engineers (there are millions of us) could effectively "look under the hood" to ensure that no backdoors existed. Such transparency can only be achieved in an open-source environment, and Apple has historically chosen to operate contrary to this model.

The second and more important lesson is that situations such as this distil the abstract concept of encryption into frightfully political sound bites. Recently, John J. Escalante, chief of detectives for Chicago's police department, went so far as to suggest that "Apple will become the phone choice for the pedophile."

The truth about encryption is obviously far more nuanced. Encryption is not a dirty word, nor is it something that's only useful to terrorists and pedophiles. Consider going a day without encryption - being unable to use your credit card, withdraw funds from an ATM, or simply make a mobile phone call - and you quickly realize how any legislation that weakens encryption would have far-reaching social, political and economic consequences.

It has been argued that mathematically crippling encryption systems to grant the government a so-called "master key" would be a good way to protect our safety and security. That's a strange case to make when most people would never agree to give the police a master key to open every house in the country (even if pedophiles and terrorists also live in some of those houses).

Furthermore, such arguments naively assume that only the "good guys" would retain (or devise) such master keys. At a time when accidental data losses by governments around the world have become an all too common occurrence, it's no wonder Apple is concerned about being forced to grant the government such access.

The U.S. government has painted not just Apple but the entire technology industry into a corner. The industry's answer needs to lie in advances in encryption technology and open source software. Given the opaque and Byzantine nature of the security apparatuses in both the U.S. and Canada, it will soon be impossible to decipher who's been compelled to do what or when - no matter what their press release states.

Frederick Ghahramani is the CEO and founder of just10.com, an ad- free private social network.

Globe and Mail
Museveni temporarily bans social media and has rival arrested, while police fire tear gas to disperse protesting voters
Friday, 19 February 2016
Byline: Geoffrey York

Johannesburg - Authorities blocked access to social media and police arrested an opposition leader as Uganda's President sought to extend his 30- year grip on power in a bitterly contested election on Thursday.
President Yoweri Museveni, who seized power in 1986 and is heavily favoured to win the latest election, said the temporary ban on Facebook and Twitter on election day was necessary because some Ugandans were "telling lies" and "misusing" social media.

"There must be steps taken for security, to stop so many creating trouble," the President told Ugandan media. "You know how they misuse them, telling lies. If you want a right, then use it properly."

Police fired tear gas to disperse voters who protested long delays in providing ballots and election materials at some voting stations. The main opposition leader, Kizza Besigye, was arrested for the second time in four days.

He was charged with "criminal trespass" when he went to the gates of an unmarked police-intelligence building, which he alleged was a vote-rigging centre.

Mr. Museveni, 71, is just the latest African leader to attempt to orchestrate the continuation of his rule, despite growing calls for term limits. At least 15 leaders across Africa have served more than two terms or announced plans to do so. In a youthful continent where the average age is 19, many leaders are elderly and unwilling to give up any power. The average age of the 10 oldest African presidents is 78. The oldest, Robert Mugabe of Zimbabwe, turns 92 on Sunday.

Mr. Museveni himself had once scathingly criticized African leaders for their tendency to cling endlessly to power. In 1986, after a five-year bush war in which he led his guerrilla army to victory, he proclaimed: "The problem of Africa in general and Uganda in particular is not the people, but leaders who want to overstay in power." But once he got a taste of power, Mr. Museveni seemed to forget those words. He became increasingly dominant in a system that revolved around his personal rule, backed by the military. In 2005, he allowed multi-party elections for the first time, but he also scrapped term limits, allowing himself to rule indefinitely. He is also now expected to get rid of the constitutional age limit of 75.

Mr. Besigye, his former ally and personal physician, has run unsuccessfully against Mr. Museveni in three past elections, often suffering harassment by the police. He has been repeatedly arrested, roughed up or confined to house arrest. On Monday, he was tear- gassed again when police broke up an opposition rally.

Mr. Museveni has always exploited the advantages of power to ensure that the opposition has little chance of beating him. A recent study by an independent civil society group found that he has spent more than $7-million (U.S.) on his current presidential election campaign. That's 12 times more than the amount spent by his top two opponents combined, the study found.

His supporters, including a controversial unit of pro-regime "Crime Preventers," have routinely used intimidation tactics against the opposition. A police chief, for example, warned that the "Crime Preventers" would be armed with guns and ready for "war" against anti-government protesters. A senior member of the ruling party told opponents that the government will "kill your children" if they protest the election results this week.

The ban on social media was sharply criticized by humanrights groups and diplomats. But it was part of a larger trend of harassment of the media, including physical attacks on journalists and the closing of radio stations.

Though the Museveni government is often criticized for human-rights abuses and crackdowns on the opposition, it has benefited from the strong support of the United States, which sees Uganda as a key ally in the fight against Islamist radicals in Somalia. In recent years, Uganda has become one of the top African recipients of U.S. security assistance.

Official results of Thursday's election are expected to be released by Saturday. Votecounting was continuing on Thursday night, sometimes by the light of lamps and cellphones in darkened voting stations. Early provisional results, from less than 5 per cent of voting stations, showed Mr. Museveni in the lead.

Globe and Mail

Tech giant defends privacy by refusing to give in to government order to hack its own phones
Friday, 19 February 2016

Editorial: Apple Inc.'s refusal to help the United States government hack into the iPhone of a dead terrorism suspect is a difficult but necessary decision. In the end, the tech company has to weigh a concrete threat to its customers' privacy against the ambiguous needs of the police.
Apple and companies like it build smartphones and tablets with the promise to customers that the personal information they keep on their devices will be protected from hackers and prying eyes. It is a critical aspect of the companies' sales pitches, and also a responsibility in the digital age.

Once a customer has purchased one of Apple's most recent phones and tablets, its contents are inaccessible even to the company that manufactured it without the user's permission. Any repeated attempt at access that isn't authorized by the user causes the devices to automatically erase all of their contents.

A judge in California, however, has ordered Apple to bypass this security system on the iPhone of Syed Farook, who along with his wife killed 14 people in a mass shooting in San Bernardino in December. The FBI asked for the order because it believes - though it does not know for certain - that there could be information on the phone that will help explain the shooters' motives and possibly lead to accomplices. The police are on a fishing expedition, looking for any clues, anywhere.

Apple won't comply for a simple reason: If it creates a bypass around the security system of one iPhone, it is necessarily doing so for all iPhones. This would be a violation of its promise to protect customers' privacy.

In fact, it would blow a hole in expectations of privacy. Once such a breach is made, it can't be unmade. Customers would know it and might lose confidence in Apple products, along with those of any other manufacturer met with a similar government order.

There is also the broader issue of governments' rapacious hunger for private citizens' personal data. If Apple yields to the U.S. government, there can be little doubt that other governments will come demanding the same thing. All they will need to do is raise the charged issue of fighting terrorism to make their case.

It's better, then, for Apple to keep saying no. It has co-operated with the FBI as much as it can, but should go no further.

Journal de Montréal
L'Oncle Sam veut voir dans votre iPhone
Friday, 19 February 2016
Byline: Pierre Martin

Opinion - Le jeu du chat et de la souris entre les services de renseignement et les défenseurs de la vie privée expose quelques dilemmes et contradictions de la lutte contre le terrorisme.
Après les attentats de San Bernardino, les enquêteurs ont récupéré l'iPhone d'un des meurtriers. Le FBI exige qu'Apple lui fournisse le moyen de débloquer l'accès aux données précieuses qu'il pourrait contenir. Le fabricant refuse.

Apple allègue ne pas pouvoir désactiver la sécurisation du téléphone, mais l'entreprise craint surtout qu'une telle clé puisse tomber entre des mains malveillantes ou que ce cas constitue un précédent pour des régimes répressifs ailleurs dans le monde.

Un dilemme cornélien

De plus en plus, la menace terroriste provient d'individus radicalisés de l'intérieur des sociétés occidentales plutôt que de groupes extérieurs. Ce changement incite les États à accentuer la surveillance interne, au détriment du droit à la vie privée de leurs citoyens.

Il n'y a pas de solution évidente, mais à ceux qui croient qu'aucune limite ne peut être imposée à l'action antiterroriste de l'État, il faut rappeler que ce phénomène représente encore un risque assez minime. Le Nord-Américain moyen a plus de chances d'être frappé par la foudre que d'être victime d'un attentat islamiste.

Personne à l'abri des contradictions

Il est louable qu'Apple défende avec vigueur la vie privée de ses clients, mais il n'en demeure pas moins que le fabricant tire un énorme bénéfice de la vente de ses produits à des usagers qui ont intérêt à rester discrets.

La palme de l'hypocrisie, dans cette histoire, ne va toutefois pas à Apple. Elle revient plutôt à une certaine droite qui proclame que l'État a perdu toute légitimité pour agir, tout en soutenant que la branche de l'État la plus obscure et la moins redevable de ses actions devrait avoir carte blanche pour tenir ses citoyens à l'oeil.

Ottawa Citizen
Laser strikes on aircraft a growing threat to safety
Friday, 19 February 2016
Byline: Andrew Duffy

Ottawa - A Transport Canada database reveals that 33 laser strikes were reported by aircraft in the National Capital Region during the past year - part of an alarming trend that places pilots and their passengers at risk.
The latest incidents occurred in January when three planes were targeted in Ottawa's skies, including an Air Canada Jazz flight from New York City and a nighttime Ornge air ambulance flight.

The incidents are outlined in the federal government's Civil Aviation Daily Occurrence Reporting System (CADORS), which acts as the repository for all safety and security-related incidents in Canadian airspace.

Although Transport Canada tries to ensure the accuracy of the reports, it still considers them preliminary and "subject to change."

The number of laser strikes on aircraft has been rising sharply in recent years.

Last year, according to a Citizen analysis of the CADORS database, there were 663 laser strikes directed at aircraft in Canada - a 32 per cent increase from 2014. The numbers have been climbing since 2008 when 80 laser incidents were reported by pilots in Canadian airspace.

Capt. Dan Adamus, Canada board president for the Air Line Pilots Association, International, called laser attacks a serious concern. "When it happens, there's a big green glow - it's usually a green laser - that fills the cockpit," Adamus said. "You can be looking for the runway, and you catch this light out of the corner of your eye, and your natural tendency is to look towards it."

Two pilots in the United States, he said, have lost their medical clearance to fly after suffering eye damage from cockpit laser strikes.

In Canada, pointing a laser at an aircraft is an offence under the federal Aeronautics Act, and those convicted can face up to five years in prison and a $100,000 fine.

Adamus wants the federal government to make laser interference with an aircraft an offence under the Criminal Code, and launch the kind of public awareness campaign conducted by the F.B.I., which offered $10,000 for information that led to arrests.

"They have to get the word out," he said, "because nine times out of 10, I think it's curious people with a laser, saying, 'I wonder if this will reach that aircraft.' " Adamus also wants the government to better regulate the sale of lasers, and limit the power output of hand-held pointers - sometimes known as laser pens - to 5 milliwatts or less. More powerful devices should be tightly controlled, he said, and come with explicit warnings about the danger they pose. Transport Canada says it is working closely with police, other government departments and the aviation industry to reduce the number of laser incidents. The high-intensity light strikes are considered particularly dangerous during the takeoff and landing phases of a flight, when pilots can least afford to be distracted or temporarily blinded.

In the Ottawa region, medevac helicopters, small planes and commercial jets have all been targeted. Last April, an Ornge helicopter flying from Pembroke Regional Hospital to the Children's Hospital of Eastern Ontario reported being hit by a green laser coming from the vicinity of the Champlain Bridge.

One month later, the pilot of an Air Transat Airbus en route from Toronto to Venice said the plane's cabin was lit up by a green laser as it cruised at 31,000-feet over Ottawa. That same month, a WestJet Boeing 737, originating in Calgary, reported that it was targeted three times by a green laser as it approached Ottawa International Airport.

Ten of the local incidents reported last year involved members of the Ottawa Flying Club, one of whom was targeted by a green laser for a full 20 seconds.

Bryce Hanna, general manager of the club, said laser strikes pose "a fundamental safety issue" since many small aircraft have a single pilot on board. "There's no one to take the controls so potentially the aircraft could even be lost because of that," Hanna said.

Laser strikes are an international problem. This month, the Alitalia flight crew taking Pope Francis to Mexico reported a laser beam coming from the ground as the plane prepared to land in Mexico City. Days later, a Virgin Atlantic flight en route to New York from London turned back after laser light struck the eyes of the co-pilot.

The incident prompted the British Airline Pilots Association to demand that the government categorize powerful laser pointers as "offensive weapons" to aid in a police crackdown on their use against planes.

The Hindustan Times
Deloitte expands its Cyber Intelligence Centre in Gurgaon (Canada).
Friday, 19 February 2016

Kolkata - Deloitte India on Thursday announced the expansion of its Cyber Intelligence Centre (CIC) in Gurgaon. This facility integrates technology with industry insights to provide round-the-clock business-focused cyber and operational security.
Krishan Pal Gurjar, Minister of State for Social Justice Empowerment, Government of India, was the Chief Guest for the occasion. Other dignitaries at the inauguration ceremony included P.R. Ramesh, Chairman, N. Venkatram, CEO, Deloitte India along with the India board and Executive Committee members of Deloitte India firm.

With 24x7 coverage, the CIC has the capability to monitor and assess threats specific to clients, enabling Deloitte to effectively mitigate risk and strengthen cyber resilience. Deloittes Gurgaon CIC will be part of a globally interconnected set of cyber intelligence centres to provide leading insights and services to its clients. Speaking about CIC, Shree Parthasarathy, Partner, Deloitte India, said,

The pervasiveness of technology throughout major business processes coupled with the brand and regulatory impact of a cyber-breach or attack, clearly makes cyber risk a boardroom issue. With always-on, always-connected systems, exposure to cyber threat increases, creating the need for businesses to get access to timely and actionable threat intelligence.

Our CIC is one of the largest in the region and is linked to Deloittes existing Cyber Intelligence Centres in Australia, Japan, UK, Spain, Canada and the United States to bring a collective set of capabilities to our clients based in India.

The CIC propels our Cyber capability to the next level and helps solidify our presence in the market as a global leader in Cyber Risk Services. Said Amry Junaideen, President, Enterprise Risk Services, Deloitte India: Threats posed to organizations by Cybersecurity-related issues have increased rapidly. So many organizations have suffered significant brand impact, financial loss, and systems outages due to Cybersecurity issues.

With new attack potentials and insider threats on the rise, securing proprietary information and other critical business assets is becoming exponentially more difficult for Indian enterprises. As a rapidly growing market, India holds immense potential for Deloitte to make meaningful impact for our clients. We believe the CICpositions us well to address the cyber risk priorities of organizations in all industries with a full suite of business- focused security solutions, he added.

Jerusalem Post
Reports of IDF airstrikes against Syria cause waves in cyberspace
Friday, 19 February 2016
Byline: Noam Amir, Maariv Hashavua

Jerusalem - Foreign reports attributing strikes against the Syrian regime to the IDF may only rarely elicit a military response, such as a barrage of rockets, however they certainly result in a direct threat to Israel's security systems.
A military source confirmed this week that in some instances where Israel has been fingered for a particular military operation, such as the strike which killed notorious terrorist Samir Kuntar last year, an immediate reaction has been seen in cyberspace.

In the case of Kuntar, a day after his death a group of hackers carried out a successful attack on the Israel Air Force (IAF) website.

According to sources in Israel, a group of hackers operating from a long distance overseas and styling itself "Qalamoun boys" was behind the attack on the IAF site. While it may be true that the attack caused no damage to the army in any significant way, and the attackers were repelled quickly, it appears to the IDF that in a general sense hackers are often curious about circulating rumors of Israeli strikes, and look for ways to confirm or deny the reports by breaking into the IDF's systems.

According to the military source, there is no paucity of attacks against the Israeli military. "Enemies want to know what's going on here," he said. "At the end of the day, computers and information systems do hold secrets, but there is a very low probability of success of such an intrusion because the cyber capabilities of the IDF are very high."

In the world today there are five major cyber powers. Israel is one of them, the other four being the US, Iran, Germany and the UK. In the case of the alleged IAF attacks against Syria, the regime does not address the foreign reports at all. Instead, it will do anything within its power to keep the ambiguity regarding incidents such as these in place. However, under the radar, they hope that one of the world cyber powers will try to access the information.

Iran is of course one of these players, having carried out attacks of increasing quality and frequency in recent years, particularly between 2013-2014.

The significant decrease in cyber attacks in 2015 has been attributed, among other factors, to the nuclear agreement. During the tumultuous years of 2013 and 2014, the region was hot, with all sides attempting to extract information. However the signing of the agreement seemed to calm the flurry of attacks in both directions.

It is very possible that Wednesday night, with the publication of further reports of an attack on Syria, that there has been a raised alert in the preparedness of the IDF. Even if the army is not expecting to deal with a barrage of missiles, at least in cyberspace it will be bracing for combat, as there are those who will be looking for verification, making cyberspace one of the most fascinating areas of the world.

The military like to call this space "the most crowded playing field in the Middle East." Even without swings and sandboxes, cyberspace is equally as fascinating as the conventional threats faced by the IDF.

Washington Times
PLA on cyberwarfare buildup
Thursday, 18 February 2016
Byline: Bill Gertz

Washington - A Chinese military official revealed last month that Beijing plans to rapidly build a new People's Liberation Army cyberwarfare force in response to U.S. military cyberforces.
Col. Li Minghai of the PLA's National Defense University wrote in the Communist Party-affiliated Global Times newspaper that a new cyberwarfare force is needed to counter the United States as the Pentagon is building up its cyberattack capabilities.

"It is more necessary for us to build a brand new 'operation force,'" said Col. Li, identified as deputy director of the NDU's Center for Cyberspace Security.

As a sign of the sensitivity of the report, Chinese censors quickly removed the posting in Chinese from the Global Times website shortly after it appeared Jan. 21.

Col. Li is one of China's most senior cyberwarfare specialists, and his remarks provide some of the first clues to Beijing's military priorities in future cyberwarfare operations. Military cyberoperations are among China's most closely guarded secrets.

The 3rd Department of the PLA general staff, known as 3PLA, is China's main military cyberwarfare force and is said to have up to 100,000 cyberwarriors. A copy of the colonel's translated article was obtained by Inside the Ring.

Col. Li stated that the U.S. military's cybersecurity strategy for the past four years has emphasized offensive electronic attacks on information systems and regards China as "one of the greatest threats to the United States' cybersecurity."

Noting that current cyberthreats to China are "not sensational or alarmist talk," Col. Li said reforms to PLA cyberforces should not be limited to "tinkering," but require "the rebuilding of a new- breed cyberforce in our country."

"We should apply the brand-new development model in the information age to remold our cyberwarfare preparedness against the threat of the United States' new cyberstrategy and guarantee our nation's cybersecurity," he said.

A key feature will be what is described as a "winning mechanism" for warfare in the cyberspace domain.

"In the 21st century, seizing control of cyberspace is of decisive significance, like seizing control of the sea in the 19th century and seizing control of the air in the 20th century," Col. Li wrote. "Cyberoperations in the future will follow the new battlefield rules determined by the winning mechanisms of 'real-time sensing, sensitive response, source destruction and chain cutoff, joint winning.'"

Also, cyberpower must be combined with conventional military power "with winning being based on information power."

Cyberwarfare troops will target information technology infrastructure networks like the Internet, telecommunications systems and computer systems, including imbedded processors and controllers in major sectors.

A third priority for the cyberwarfare force will be adding more trained military hackers.

"At present, our country still lacks high-end specialists with both knowledge about network technology and knowledge about military command, so it is imperative that we step up the efforts for building the cyberoperation force," Col. Li concluded.

Publication of the report coincided with China's creation of a Strategic Support Force, announced Dec. 31, that will include dedicated cyberwarfare forces, along with space warfare units.

Cybersecurity expert Joe McReynolds disclosed last year that China's cyberwarfare forces were outlined for the first time in a Chinese military paper. The PLA cyberwar force has three elements, including a cadre of dedicated military specialists devoted to network warfare that conduct cyberattacks and defense, Mr. McReynolds told The Daily Beast.

Other forces include teams of specialists working in civilian intelligence, police and security organs who conduct military cyberoperations. Last are units outside government that will be mobilized for network warfare.

Press Trust of India
Government to ask Twitter to block accounts with Hafiz Links
Friday, 19 February 2016

New Delhi - Security agencies will approach Twitter India to block all accounts having links with Lashkar-e-Taiba founder Hafiz Saeed and Jamaat-ud-Dawa which are often found to be spreading venom against India.
There are several accounts which have links with LeT's front outfit, Jamaat-ud-Dawa, as well as terror mastermind Saeed and it has become necessary to shut these down as quickly as possible, officials said.

"We are approaching Twitter India which in turn will tell its US-based parent company to deactivate the accounts. Hopefully, it will be done soon," a official said.

Earlier, Twitter had blocked several accounts operated by Jamaat-ud-Dawa, headed by Saeed, following requests from security agencies in different countries, including India and the US. However, such accounts again cropped up after a gap of several months.

A fake account of Saeed had recently asked Pakistanis to support the JNU students who are protesting against the registration of a case of sedition against JNUSU president Kanhaiya Kumar. It had also asked users to trend the topic #PakStandWithJNU with the posts sparking a huge controversy.

Last Sunday, Home Minister Rajnath Singh had said the event organised at JNU to protest against the hanging of Parliament attack convict Afzal Guru had the backing of Saeed.

Even though the Home Ministry clarified that Singh's statement was based on inputs from different agencies, it was reportedly made in the wake of the posts on the fake Saeed Twitter account.

Gulf News
Tech giants support Apple in privacy fight
Friday, 19 February 2016
Byline: Staff Report

Dubai - Apple chief Tim Cook has picked a fight with the United States government and Silicon Valley is joining his side.
Apple Inc.'s chief executive officer took his stand after the Federal Bureau of Investigation won a court order to make Apple help investigators unlock an iPhone used by Syed Rizwan Farook, one of the shooters in a deadly December 2 attack in San Bernardino, California.

From Google Inc. to Facebook Inc., the industry's biggest names rallied around Cook after he vowed to resist the court order. Cook described the request as an "unprecedented step that threatens the security of our customers" and called for a public debate.

The escalation with the FBI, which has been pushing for access to mobile devices since Apple tightened its encryption in late 2014, galvanised the firm's US peers and forced them to choose between helping the government fight crime and protecting their customers' privacy. The decision in the Apple case could apply to the broader tech industry and it may spur requests from China and other nations that want similar abilities to access users' encrypted content.

Reform Government Surveillance, a group representing firms including Google, Facebook, Microsoft Corp. and Twitter Inc., have issued a statement reiterating that, while it's "extremely important" to deter crime and terrorism, no company should be required to build backdoors to their own technology.

National Security Agency whistleblower Edward Snowden has also backed Apple, tweeting that the company's stance was defending the rights of its customers.

"We're here to say to Apple, "We're going to back you all the way," ' said Electronic Frontier Foundation (EFF) chief Cindy Cohn outside a San Francisco store. When about two dozen privacy advocates stood shoulder to shoulder in front of the downtown San Francisco Apple store on Wednesday, it may have been the first time a demonstration was held in support of the tech company.

"Silicon Valley stands with Apple," Bret Taylor, co-founder of Quip and former chief technology officer of Facebook and co-creator of Google Maps, posted on Twitter. Steven Sinofsky, an ex-executive at Microsoft, called for "broad support from full stack of technology companies."

Khaleej Times

Re-strategising IT security

Friday, 19 February 2016

Byline: Aji Joseph

Dubai - Digital industrial espionage is becoming a greater threat for companies in all industries. An additional danger is presented by numerous secret services, with an aim of spying on businesses and organisations. What should companies, the potential victims, do? They must work harder than ever to protect themselves and their data from increasingly complex attacks in order to avoid the kind of corporate disadvantage, which might even threaten their very existence.

There are various forms of attack which have the declared aim of spying on business secrets. Malware is introduced into databases, applications and systems. Transmitted data is spied on and read at network connections. Trojans can make their way into companies with completely innocent software purchases. Software updates can also be used as a transmission vehicle for spying programs. If there are no proper defence mechanisms available, attackers can spy on business secrets as long as they like without the company noticing.

The attackers can usually leave the network in the same way as they got in - unnoticed by the victims. Annual losses to corporate espionage are estimated to be billions.

The EU published a report on industrial espionage as early as 2001. The list includes two suspected cases against France. These were in relation to the delivery of high-speed trains to South Korea. The French manufacturer Alstom (TGV) was said to have gained a competitive advantage over the competitor Siemens (ICE) by means of industrial espionage.

In 2013, France came under suspicion again. The New York Times reported on the country's alleged industrial espionage programme, which had the aim of obtaining technical secrets from the USA.

In 2015, the newspaper Libération reported that approximately one hundred French companies, including all companies listed in the French stock market index CAC 40, had been spied on. The report was based on information provided in US documents supplied by Wikileaks. The German Federal Intelligence Service (BND) was also in the headlines for several weeks. It has been accused of having helped the US secret service NSA to spy on European institutions and companies.

Although defence mechanisms such as signature-based anti-virus software, firewall and network monitoring software are still required, they are no longer sufficient.

Only a comprehensive shield can help in the face of the intensified threat. It must cover the entire company, include all the necessary IT security services, maintain an overview of all security incidents, be adaptable to new threat scenarios and detect unknown forms of attack.

Though today several IT experts and managers have the expertise and skills to manage cyber risk/ attacks; you need an intelligence-based approach - one that uses knowledge combined with tools - 24x7 to identify threats and protect your assets. In view of this and the high human resources and financial costs; companies have to consider whether they can operate on their own or they should use specialist expertise and tools.

To manage IT security more effectively and efficiently; it's time for organisations to refocus and re-strategize their overall IT security shield - to reduce time until risk is detected and therewith reduce potential damage of attacks.

Companies should consider outsourcing their IT security monitoring needs to highly specialised experts and therewith ensure their infrastructure is monitored every hour - seven days a week ensuring a more proactive approach in protecting their company assets. At the same time this should offer significant cash savings for a company in the long run such as a reduction of costs for purchasing and managing a vast number of complex stand-alone IT security solutions.

Bloomberg News
Secret Memo Details U.S.'s Broader Strategy to Crack Phones
Friday, 19 February 2016
Byline: Michael Riley, Jordan Robertson

Washington - Silicon Valley celebrated last fall when the White House revealed it would not seek legislation forcing technology makers to install "backdoors" in their software -- secret listening posts where investigators could pierce the veil of secrecy on users' encrypted data, from text messages to video chats. But while the companies may have thought that was the final word, in fact the government was working on a Plan B.
In a secret meeting convened by the White House around Thanksgiving, senior national security officials ordered agencies across the U.S. government to find ways to counter encryption software and gain access to the most heavily protected user data on the most secure consumer devices, including Apple Inc.'s iPhone, the marquee product of one of America's most valuable companies, according to two people familiar with the decision.

The approach was formalized in a confidential National Security Council "decision memo," tasking government agencies with developing encryption workarounds, estimating additional budgets and identifying laws that may need to be changed to counter what FBI Director James Comey calls the "going dark" problem: investigators being unable to access the contents of encrypted data stored on mobile devices or traveling across the Internet. Details of the memo reveal that, in private, the government was honing a sharper edge to its relationship with Silicon Valley alongside more public signs of rapprochement.

On Tuesday, the public got its first glimpse of what those efforts may look like when a federal judge ordered Apple to create a special tool for the FBI to bypass security protections on an iPhone 5c belonging to one of the shooters in the Dec. 2 terrorist attack in San Bernardino, California that killed 14 people. Apple Chief Executive Officer Tim Cook has vowed to fight the order, calling it a "chilling" demand that Apple "hack our own users and undermine decades of security advancements that protect our customers." The order was not a direct outcome of the memo but is in line with the broader government strategy.

White House spokesman Josh Earnest said Wednesday that the Federal Bureau of Investigation and Department of Justice have the Obama administration's "full" support in the matter. The government is "not asking Apple to redesign its product or to create a new backdoor to their products," but rather are seeking entry "to this one device," he said.

Security specialists say the case carries enormous consequences, for privacy and the competitiveness of U.S. businesses, and that the National Security Council directive, which has not been previously reported, shows that technology companies underestimated the resolve of the U.S. government to access encrypted data.

"My sense is that people have over-read what the White House has said on encryption," said Robert Knake, a senior fellow at the Council of Foreign Relations who formerly served as White House Director of Cybersecurity Policy. "They said they wouldn't seek to legislate 'backdoors' in these technologies. They didn't say they wouldn't try to access the data in other ways."

"Backdoors" refer to security holes that are intentionally inserted into software to create the equivalent of a skeleton key for law enforcement -- what wiretapping systems are for telephone lines, for instance. The problem with backdoors in computer networks is they create vulnerabilities for any hacker to find.

What the court is ordering Apple to do, security experts say, does not require the company to crack its own encryption, which the company says it cannot do in any case. Instead, the order requires Apple to create a piece of software that takes advantage of a capability that Apple alone possesses to modify the permanently installed "firmware" on iPhones and iPads, changing it so that investigators can try unlimited guesses at the terror suspect's PIN code with high-powered computers. Once investigators get the PIN, they get the data.

Knake said that the Justice Department's narrowly crafted request shows both that FBI technical experts possess a deep understanding of the way Apple's security systems work and that they have identified potential vulnerabilities that can provide access to data the company has previously said it can't get.

In this case, the government wants Apple's help in exploiting such weaknesses. But experts say they could find ways to do it themselves, and the NSC "decision memo" could lead to more money and legal authorization for a smorgasbord of similar workarounds.

National Security Council spokesman Mark Stroh declined to comment on the memo. But he provided a statement from a senior Obama administration official: "We should not preemptively conclude that technical and policy options to address this challenge are out of reach. While creating mechanisms for accessing encrypted information does create vulnerabilities, there may be technical and process steps that can be implemented to limit such risks."

The memo was approved by the NSC's Deputies Committee, according to the people familiar with it. While the deputies' committee changes depending on the subject matter, it typically includes at least a dozen sub-cabinet level officials, among them the deputy attorney general, the vice chairman of the joint chiefs of staff, and the deputy national security adviser.

Such memos can have lasting impact. A similar decision memo was used in the early years of the Iraq war to address the problem of Improvised Explosive Devices, which were then killing hundreds of U.S servicemen. The response ultimately led to new anti-IED technology and expanded intelligence capabilities to disrupt the cells building and planting the bombs.

Silicon Valley and Washington have had a decades-long distrust of each other over encryption, stemming from a failed Clinton administration push in the 1990s for a government backdoor in telecommunications networks. In that case, the National Security Agency developed a technology called the Clipper Chip, which the White House approved as a government standard. Security experts assailed it as insecure and a violation of privacy.

Security experts say the U.S.'s insistence on finding ways to tap into encrypted data comes in direct conflict with consumers' growing demands for privacy.

"The government's going to have to get over it," said Ken Silva, former technical director of the National Security Agency and currently a vice president at Ionic Security Inc., an Atlanta-based data security company. "We had this fight 20 years ago. While I respect the job they have to do and I know how hard the job is, the privacy of that information is very important to people."

In addition to the demands against Apple, the FBI will almost certainly seek more money and expanded legal authorization to track suspects and access encrypted data, without the involvement of companies that make the technologies, several experts say. Intelligence services already have sophisticated tools for cracking encryption, and the White House's efforts will likely lead to broader use of those techniques across the government, even in ordinary criminal investigations that don't involve foreign intelligence or national security.

The workarounds could involve trying to force companies like Apple to develop their own tools to help law enforcement or enlisting government hackers to find previously unknown software vulnerabilities that enable the decryption of large amounts of data flowing across networks.

Apple infuriated law enforcement when it announced in 2014 that it would encrypt data stored on users' iPhones and iPads with a PIN code that the company could not access, even if ordered to by a judge. Prior to that decision, the FBI and local police agencies routinely sent seized devices to Apple to extract data relevant to their investigations.

To security experts, creating hacking tools -- capabilities to gain access to encrypted data -- is simply a matter of money and focused effort.

"My guess is you could spend a few million dollars and get a capability against Android, spend a little more and get a capability against the iPhone. For under $10 million, you might have capabilities that will work across the board," said Jason Syversen, a former manager of advanced cyber security programs at the Defense Advanced Research Projects Agency (DARPA), and now the CEO and co-founder of Siege Technologies in Manchester, New Hampshire.

This week's federal court order undermines years of effort by Apple to design a system that makes accessing encrypted data impossible without the participation of the phone's legitimate user. Company officials appeared to believe the enhanced encryption would remove Apple from the efforts of any government to sabotage the security of their customers. Instead, federal agents have detailed in a public document several ways in which that encryption can be bypassed.

"Apple has two options now: They can go back to the judge and say this isn't possible. Or they can service the warrant," said James Lewis, a senior cyber security fellow at the Center for Strategic and International Studies in Washington. "I don't think they can say it's not possible, because it looks like it is."

New York Times
A Web Crime on the Rise: Hackers Lock Out Users and Demand a Ransom
Friday, 19 February 2016
Byline: Stacy Cowley, Liam Stack

New York - It sounds like the plot of a Hollywood thriller, but the all-too-real scenario played out this month at a large Los Angeles hospital: Hackers seized control of critical computer systems and the hospital paid a $17,000 ransom to release them.
So-called ransomware attacks have increased significantly in the past year, security experts say, and the hospital, Hollywood Presbyterian Medical Center, is not the first to fall victim.

The Titus Regional Medical Center, a small hospital in Mount Pleasant, Tex., experienced a similar attack last month, which knocked its core electronic medical record system offline. It, too, paid the ransom, according to Shannon Norfleet, a hospital spokeswoman.

Those in the security industry say such attacks are becoming more prevalent, but are rarely made public.

"We get over 100 calls and emails a month from different organizations that have had some form of ransomware impact their environment," said Charles Carmakal, who oversees breach investigations for clients of Mandiant, a consulting unit of the security firm FireEye. "Nobody talks to the media about it."

In a statement released Wednesday, Allen Stefanek, the president of Hollywood Presbyterian, described the two- week battle that his hospital fought to regain control of its data after a malware attack was detected on Feb. 5.

The attack did not disrupt medical care or compromise the personal information of employees or patients, he said. Instead, it blocked hospital employees from using email and other forms of electronic communication by using encryption to lock them out of the system.

Mr. Stefanek said hospital administrators were told that if they wanted to gain access to their network again, they would have to pay the attackers, who would then give them the decryption key. Mr. Stefanek said that the hospital had contacted the authorities when the malware attack was first detected.

"The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Mr. Stefanek said. "In the best interest of restoring normal operations, we did this."

Heath care providers are required to tell patients of any breaches that compromise their personal information or health data, but a typical ransomware attack would not fall into that category. The attackers do not need to gain access to the underlying data in order to encrypt it and prevent others from viewing it.

Once compromised, an organization has little choice but to pay up or say farewell to its data, according to Levi Gundert, who oversees information security strategy for Recorded Future, a threat analysis firm.

"There's really no workarounds for it," he said. "It's very frustrating for both law enforcement and the victims themselves."

Hollywood Presbyterian's attackers demanded their payment in the

form of 40 Bitcoins, a difficult-to-trace currency that has become the currency of choice for online criminals.

Ransomware attacks are on the rise, industry researchers say, because they work. A research team at Dell gathered data from one ransom-payment server and found that it collected $1.1 million in a six-month period. McAfee Labs, Intel's security research unit, detected 638,000 new ransomware variants in 2014. Last year, that number shot up to nearly 3.8 million.

Many ransomware attacks are random, and comparatively low-tech and blunt. Victims are most often infected by clicking a malicious link in an email or by malware delivered through a web browser, frequently hidden in advertisements. The average payment demanded is just $300, according to the security firm Symantec, a sum that is within reach for the individuals and small businesses that most often fall prey to these schemes.

But Mr. Carmakal said he was seeing a growing number of attackers targeting businesses and other organizations with deeper pockets. In those attacks, the hackers may go to greater lengths to remove data -- not just lock access to it -- and threaten to release it publicly if they are not paid.

"Automated malware doesn't know if an organization has $100,000 or not. A human knows," he said. "We've seen an uptick in those kinds of attacks over the past year. We've seen attackers ask for $10,000 to seven-figure values to delete the data" in their possession.

As ransomware attacks grow more frequent, they are increasingly hitting organizations that deal in public safety and other critical functions. Over the past year, the attacks have affected police departments and school districts across the country.

Health care organizations seem to be particularly vulnerable to hacking attacks because they have been slower to embrace sophisticated backup systems and other security measures than other industries, like financial services, said Katherine Keefe, the head of breach response services at Beazley, an insurance company.

Her team investigated 1,200 breaches last year, about half of them at health care providers. The rate of ransomware attacks has noticeably increased in the last six to eight months, she said.

"The criminals see that there's money to be made, and I think they believe they can hold organizations over a barrel," Ms. Keefe said.

The cost of an attack goes far beyond the usually modest sum demanded for ransom. It took Hollywood Presbyterian 10 days to restore its systems, Mr. Stefanek said.

Laura Eimiller, a spokeswoman for the Federal Bureau of Investigation in Los Angeles, said the agency had begun an inquiry into the attack, but she provided no further details.

USA Today
Apple faces uphill battle
Friday, 19 February 2016
Byline: Brad Heath

Washington - The U.S. Justice Department's demand that Apple help it break into a locked iPhone is the latest in a series of legal disputes with tech companies over users' privacy that has been going on for more than a decade.
Nearly all of those contests ended the same way.

"Historically, the judiciary has been very deferential to law enforcement," University of California-Hastings law professor Ahmed Ghappour said. "And history could be very indicative of how this will play out."

The latest episode began this week, when a federal magistrate judge in California ordered Apple to help FBI agents break into the locked iPhone used by Syed Rizwan Farook, one of the armed attackers in December's massacre in San Bernardino, Calif. Apple CEO Tim Cook said the company would fight the order, and Apple has refused to help unlock at least one other locked phone.

For tech companies, such battles have often not gone well.

In 2007, Yahoo balked at a secret order from the Foreign Intelligence Surveillance Court requiring it to turn over customer records to the NationalSecurity Agency. The company relented when a judge on the surveillance court threatened to impose a fine of $250,000 a day -- and double it every week. A federal appeals court upheld the surveillance court's order.

In 2013, a federal judge held the founder of Lavabit -- an email service that had been used by former NSA contractor Edward Snowden - - in contempt for not turning over the electronic key the company used to encrypt users' communications. Lavabit founder Ladar Levison eventually gave the key to the FBI but did so by printing it out in very small type.

Most such disputes have involved federal agents seeking access to troves of information tech companies keep about their users -- everything from contents of emails to records that can precisely track the location of someone's cellphone. The fight with Apple comes with one important difference.

Instead of asking the computer maker to turn over information, a federal magistrate ordered the company to create software for the FBI that would bypass some security features on newer versions of the iOS operating system. The order requires Apple to add an electronic signature to the new software, so Farouk's phone will recognize it.

"The fight here is that the software the government wants does not exist. They're trying to force engineers to write a special version of iOS, then sign it," said Christopher Soghoian, the American Civil Liberties Union's principal technologist. He said such an order raises the prospect that the FBI could force makers to push compromised versions of their software directly to users' phones and computers in a way that would be difficult to detect.

Apple has also rebuffed efforts to help agents unlock older versions of the iPhone, using tools it had already created for the job.

Last year in Brooklyn, federal prosecutors asked a magistrate to force Apple to unlock a phone running iOS 7, so they could use the phone's contents in a drug case. The company declined, even though it had "repeatedly assisted law enforcement officers in federal criminal cases by extracting data from passcode-locked iPhones pursuant to court orders," prosecutors said in a court filing.

Apple has argued that complying with the request would be burdensome. A judge has yet to decide whether to force Apple to comply.

Justice Department lawyers told a different federal judge in Brooklyn last year that the government has the ability to crack newer versions of the iPhone on its own. "The lack of a passcode is not fatal to the government's ability to obtain the records," Assistant U.S. Attorney Karen Koniuszy wrote in a court filing.

Wall Street Journal
Apple Standoff Escalates Local Cases
Friday, 19 February 2016
Byline: Nicole Hong. Pervaiz Shallwani

New York - State and local law-enforcement authorities are looking to follow the lead of the Federal Bureau of Investigation in its standoff with Apple Inc. over access to the contents of a terror suspect's smartphone.
Earlier this week, a federal magistrate judge in California ordered Apple to help the government unlock a passcode on the phone used by one of the suspects in the attack last year in San Bernardino, Calif., which killed 14 people. Apple has said it would fight the judge's order.

On Thursday, Manhattan District Attorney Cyrus Vance said his office is in the process of determining which cases involving encrypted smartphones they should bring before a New York state judge for a similar review.

Mr. Vance called the Apple case "the most visible example of how Silicon Valley's decisions are thwarting criminal investigations and impeding public safety." Other district attorneys may be following Mr. Vance's moves.

Jake Wark, a spokesman for the Suffolk County district attorney's office in Boston, said that although the office hasn't yet taken steps to bring a specific case for judicial review, "We can't rule that out. It may be a question of finding the right case."

The fight between Washington and Silicon Valley is exposing law enforcement's long-simmering concerns over the challenges posed by encryption during investigations. Federal and local law-enforcement officials are increasingly voicing frustration with encrypted smartphones, which they say provide a haven for criminals and hinder investigations by keeping potentially valuable evidence out of reach.

The battle over encrypted smartphones is part of a broader debate that dates back over a decade. Following the attacks on Sept. 11, 2001, Congress won broad support to pass the USA Patriot Act, which became the legal underpinning for roving wiretaps on terrorism suspects and bulk collection of phone records by the NationalSecurity Agency.

Over time, however, concerns about privacy and civil liberties escalated, reaching an apex following the 2013 disclosures of government surveillance by former national-security contractor Edward Snowden. Last June, Congress approved a new bill called the USA Freedom Act, which curbed the government's spying powers and reined in the NSA's bulk collection.

Moves by the telecom industry to address privacy concerns, especially the creation of stronger encryption on devices, have sparked outrage from law enforcement.

"There is not an investigation today at the local, state or federal level that doesn't touch a cyber platform," said Don Mihalek, who represents Secret Service members in the Federal Law Enforcement Officers Association. "Encryption has made it impossible now for law enforcement to do their jobs."

Apple's defiance, meanwhile, is garnering support from privacy advocates who say complying with the order could hurt the personal privacy of Americans and make smartphone users more vulnerable to hacks.

"This case is not about that one phone," said Alex Abdo, a staff attorney at the American Civil Liberties Union. "This case is about the government trying to establish an illegal precedent that it can force a U.S. company to hack its users' devices."

Supporters of Apple have said that giving the government even limited access to encrypted iPhones and similar devices will just spur criminals to communicate on other encrypted platforms.

Federal Bureau of Investigation Director James Comey has said that terrorists made a more concerted effort after the Snowden revelations to shield their communications on encrypted devices.

Since September 2014, when Apple began encrypting its new phones by default, approximately 25% of the 670 Apple devices (with the iOS 8 operating system or higher) examined by the Manhattan district attorney office's cybercrime lab were encrypted and not accessible, Mr. Vance said Thursday.

In a recent speech, Mr. Comey said encryption hindered the investigation into the attack last May of people at an exhibit featuring cartoons of the Prophet Muhammad in Garland, Texas, where the two shooters were both killed after they opened fire.

The morning of the attack, one of the shooters exchanged 109 messages with a known terrorist overseas using an encrypted mobile messaging app, Mr. Comey said. The terrorist group Islamic State has claimed responsibility for the Texas shooting.

"All the judicial orders in the world are not going to tell us what they said that morning," Mr. Comey said.

Although encryption in terrorism investigations has gained the most attention, officials say the issue now has a nexus to all sorts of crimes, including drug trafficking, kidnappings and child pornography. In New York, officials are struggling to access an encrypted iPhone 5 used by an associate during a shooting in the Bronx two weeks ago that injured two police officers. New York Police Department Commissioner William Bratton said Thursday that the encrypted iPhone was "impeding" the case from going forward.

Mr. Bratton said fixing the issue is going to require more significant rulings by the courts, including likely the Supreme Court, and legislation from Congress and state legislatures. He said both sides were early on in the process.

"The Constitution guarantees no absolute right to privacy," Mr. Bratton said. "It guards against unreasonable search and seizure. How is what we are talking at all unreasonable?"

Local law enforcement in Louisiana say an encrypted smartphone may be the last lead for solving the murder of Brittany Mills, a 28-year-old who was shot to death last April. In a typical investigation with an encrypted phone, investigators either try to ask the iPhone user to give up the passcode or search for any data in the user's cloud, according to Hillar Moore, the district attorney in Baton Rouge, La. Neither option was available in Ms. Mills's case.

"The frustrating part about this is the bad guys know that no one can get in beyond search warrants," Mr. Moore said. "They brag that cops can't touch their phones. They're using the phone as a shield to allow them to deal drugs, traffic women and threaten national security."

Wall Street Journal
How Using The 'Cloud' Undercuts Encryption
Friday, 19 February 2016
Byline: Jack Nicas

New York - While the increasing use of encryption helps smartphone users protect their data, another sometime related technology, cloud computing, can undermine those protections.

The reason: encryption can keep certain smartphone data outside the reach of law enforcement. But once the data is uploaded to companies' computers connected to the Internet -- referred to as "the cloud" -- it may be available to authorities with court orders.

Major cloud-computing suppliers, including smartphone providers such as Alphabet Inc.'s Google, Microsoft Corp. and Apple Inc., routinely comply with court orders and search warrants to turn over data that in many cases would have been harder for law enforcement to obtain had users kept it solely on their devices.

"The safest place to keep your data is on a device that you have next to you," said Marc Rotenberg, head of the Electronic Privacy Information Center. "You take a bit of a risk when you back up your device. Once you do that it's on another server."

Encryption and cloud computing "are two competing trends," Mr. Rotenberg said. "The movement to the cloud has created new privacy risks for users and businesses. Encryption does offer the possibility of restoring those safeguards, but it has to be very strong and it has to be under the control of the user."

Apple is fighting a government request that it help the Federal Bureau of Investigation unlock the iPhone of Syed Rizwan Farook, the shooter in the December terrorist attack in San Bernardino, Calif.

The FBI believes the phone could contain photos, videos and records of text messages that Mr. Farook generated in the final weeks of his life.

The data produced before then? Apple already provided it to investigators, under a court search warrant. Mr. Farook last backed up his phone to Apple's cloud service, iCloud, on Oct. 19.

Encryption scrambles data to make it unreadable until accessed with the help of a unique key. The most recent iPhones and Android phones come encrypted by default, with a user's passcode activating the unique encryption key stored on the device itself. That means a user's contacts, photos, videos, calendars, notes and, in some cases, text messages are protected from anyone who doesn't have the phone's passcode. The list includes hackers, law enforcement and even the companies that make the phones' software: Apple and Google.

However, Apple and Google software prompt users to back up their devices on the cloud. Doing so puts that data on the companies' servers, where it is more accessible to law enforcement with court orders.

Apple says it encrypts data stored on its servers, though it holds the encryption key. The exception is so-called iCloud Keychain data that stores users' passwords and credit-card information; Apple says it can't access or read that data.

Officials appear to be asking for user data more often. Google said that it received nearly 35,000 government requests for data in 2014 and that it complies with the requests in about 65% of cases.

Apple's data doesn't allow for a similar comparison since the company reported the number of requests from U.S. authorities in ranges in 2013.

Whether they back up their smartphones to the cloud, most users generate an enormous amount of data that is stored outside their devices, and thus more accessible.

New York Times
For Apple's C.E.O., a Journey to Bulwark for Digital Privacy
Friday, 19 February 2016
Byline: Katie Benner, Nicole Perlroth

San Francisco - Letters from around the globe began pouring into the inbox of Timothy D. Cook not long after the publication of the first revelations from Edward J. Snowden about mass government surveillance
Do you know how much privacy means to us? they asked Apple's chief executive. Do you understand?

Mr. Cook did. He was proud that Apple sold physical products -- phones, tablets and laptops -- and did not traffic in the intimate, digital details of its customers' lives.

That stance crystallized on Tuesday when Mr. Cook huddled for hours with lawyers and others at Apple's headquarters to figure out how to respond to a federal court order requiring the company to let the United States government break into the iPhone of one of the gunmen in a San Bernardino, Calif., mass shooting. Late Tuesday, Mr. Cook took the fight public with a letter to customers that he personally signed.

"We feel we must speak up in the face of what we see as an overreach by the U.S. government," wrote Mr. Cook, 55. "Ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect."

Mr. Cook's standoff with law enforcement officials is indicative of his personal evolution from a behind-the-scenes operator at Apple to one of the world's most outspoken corporate executives. During that time, he has moved a once secretive Silicon Valley company into the center of highly charged social and legal issues. While Mr. Cook's predecessor, Apple co-founder Steven P. Jobs, was considered a business icon, he never took aggressive positions on such matters as Mr. Cook now has.

Being at loggerheads with the United States government is risky for Apple and may draw a torrent of public criticism of the world's most valuable company at a time when its growth rate has significantly decelerated.

Yet people who know Mr. Cook said he did not believe he had a choice but to be vocal. Mr. Cook, who became Apple's chief executive in 2011, has long said that businesses and their leaders should think of

themselves as important members of civic society. In September, he emphasized that this responsibility "has grown markedly in the last couple of decades or so as government has found it more difficult to move forward."

Mr. Cook "says what he believes, especially in difficult situations," said Don Logan, the former chairman of Time Warner Cable who has been friends with Mr. Cook since he became chief executive of Apple, bonding over their shared alma mater, Auburn University. Of Mr. Cook's opposition to the court order, Mr. Logan said: "Tim is currently dealing with a very difficult situation and he knows the decision he has made has lots of ramifications, good or bad. But he wants to do the right thing."

Apple declined to make Mr. Cook available for an interview. The company is preparing to file an opposition brief against the court order.

Mr. Cook's ideas about civic duty were partly formed during his childhood in rural Alabama. In a speech at the United Nations in 2013, he recounted how Ku Klux Klansmen had once burned a cross on the lawn of a black family's home and how he yelled for them to stop. "This image was permanently imprinted in my brain, and it would change my life forever," he said.

At Apple, which he joined as a senior executive in 1998, Mr. Cook was a quiet figure for much of the period when he worked for Mr. Jobs, a showman who prized secrecy at the company. After Mr. Jobs stepped down because of ailing health, Mr. Cook began making Apple more open, publishing an annual report on suppliers and working conditions for more than a million factory workers.

In 2014, Mr. Cook revealed he was gay, a move widely seen as making a statement about gay rights. Last year, he wrote an editorial decrying religious freedom laws that had been proposed in more than two dozen states that would let people skirt anti-discrimination laws that conflicted with their religious beliefs.

His outspokenness has drawn criticism, with some investors questioning how nonbusiness initiatives -- including some of Apple's environmental moves -- would contribute to the company's bottom line. Mr. Cook responded at a shareholder meeting that it is important for Apple to do things "because they're just and right."

Privacy has long been a priority for Mr. Cook. At a tech conference in 2010, he said Apple "has always had a very different view of privacy than some of our colleagues in the Valley." He cited the iPhone's feature that shows where a phone -- and presumably its user -- is and said fears about abuse and stalking had compelled the company to let consumers decide whether or not their apps could use their location data.

Mr. Cook's views on privacy hardened over time as customers globally began entrusting more personal data to Apple's iPhones. At the same time, Apple was growing tired of requests from government officials worldwide asking the company to unlock smartphones.

Each data-extraction request was carefully vetted by Apple's lawyers. Of those deemed legitimate, Apple in recent years required that law enforcement officials physically travel with the gadget to the company's headquarters, where a trusted Apple engineer would work on the phones inside Faraday bags, which block wireless signals, during the process of data extraction.

Processing these requests was extremely tedious. More worrisome, the data stored on its customers iPhones was growing more personal, including photos, messages and bank, health and travel data.

And some government officials were not exactly instilling confidence in Apple's engineers. In one case, after law enforcement officials rushed a phone to Apple's headquarters for data extraction, the engineers discovered their target had not enabled the device's passcode feature.

So Mr. Cook and other Apple executives resolved not only to lock up customer data, but to do so in a way that would put the keys squarely in the hands of the customer, not the company. By the time Apple rolled out a new mobile operating system, iOS7, in September 2013, the company was encrypting all third-party data stored on customers' phones by default.

"People have a basic right to privacy," Mr. Cook has said.

By then, Mr. Snowden's disclosures about how the NationalSecurity Agency had cozied up to some tech companies and hacked others to gain user data were reverberating worldwide. The disclosures included revelations of a comprehensive, decade-long Central Intelligence Agency program to compromise Apple's products; C.I.A. analysts tampered with the products so the government could collect app makers' data. In other cases, the agency was embedding spy tools in Apple's hardware, and even modifying an Apple software update that allowed government analysts to record every keystroke.

Letters from alarmed Apple customers started flooding into Mr. Cook's inbox, fortifying his stance on privacy. Apple's eighth mobile operating system, iOS8, which rolled out in September 2014, made it basically impossible for the company's engineers to extract any data from mobile phones and tablets.

For officials at the world's law enforcement agencies, the new software was a clear signal that Apple was growing defiant. A month after iOS8's release, James Comey, the director of the F.B.I., told an audience at the Brookings Institution that Apple had gone "too far" with the expanded encryption, arguing that the operating system effectively sealed off any chance of tracking kidnappers, terrorists and criminals.

Government agencies began to press Apple and other tech companies for so-called back doors that could bypass strong security measures. With tensions rising, some form of technical compromise -- whether in the form of a chip, a back door or a key -- was off the table by 2015.

At Apple, Mr. Cook and others continued to work with investigators to the extent the company could and complied with court orders. Last October, a federal judge in New York said the government was overstepping its boundaries by using a centuries-old law, the All Writs Act, as the basis for its request that Apple open an iPhone for a drug investigation. Apple's lawyer sided with the judge in the case. The matter has not been resolved.

After December's San Bernardino attack, Apple worked with the F.B.I. to gather data that had been backed up to the cloud from a work iPhone issued to one of the assailants, according to court filings. When investigators also wanted unspecified information on the phone that had not been backed up, the judge this week granted the order requiring Apple to create a special tool to help investigators more easily crack the phone's passcode and get into the device.

Apple had asked the F.B.I. to issue its application for the tool under seal. But the government made it public, prompting Mr. Cook to go into bunker mode to draft a response, according to people privy to the discussions, who spoke on condition of anonymity. The result was the letter that Mr. Cook signed on Tuesday, where he argued that it set a "dangerous precedent" for a company to be forced to build tools for the government that weaken security.

"Compromising the security of our personal information can ultimately put our personal safety at risk," he wrote. "That is why encryption has become so important to all of us."

Far from backing down from the fight, Mr. Cook has told colleagues that he still stands by the company's longstanding plans to encrypt everything stored on Apple's myriad devices, services and in the cloud, where the bulk of data is still stored unencrypted.

"If you place any value on civil liberties, you don't do what law enforcement is asking," Mr. Cook has said.

Wall Street Journal
Apple Has More Leeway Than Carriers
Friday, 19 February 2016
Byline: Ryan Knutson

Washington - For U.S. phone companies like AT&T Inc. and Verizon Communications Inc., the notion of resisting a court order like Apple Inc. Chief Executive Tim Cook recently did is probably inconceivable. The reason is legal.

In 1994, Congress passed the Communications Assistance for Law Enforcement Act, which required that carriers build surveillance capability into their networks. That law was later expanded to cover voice calls placed over the Internet, but not all Internet communication. Other attempts to further expand the law to cover technology companies such as Apple have failed.

Mr. Cook earlier this week said Apple would oppose a federal judge's order to help the Justice Department unlock a phone used by a gunman in the San Bernardino attack, which killed 14 people last December.

These days, the nation's telecom carriers receive thousands of information requests from the government and law enforcement in both national security, and civil and criminal matters.

In the last six months of 2015, Verizon and AT&T combined received more than a quarter-million requests from law- enforcement agencies in civil and criminal matters and as many as 998 requests in the first six months of 2015 to access customer accounts for national-security reasons, according to transparency reports published by the companies.

By comparison, Apple says it received 971 law-enforcement requests for account data stored in users' iCloud or iTunes accounts. In the first half of 2015, the latest data available, and provided at least some data to 81% of them. As many as 499 additional requests were related to national security, according to Apple's transparency report.

With much communications traffic shifting from the phone networks to data packets on the Internet, monitoring is becoming more complicated.

"Back in the day, it was AT&T -- they had everything, so you just talked to AT&T," said Michael Sussmann, a former Justice Department official who is now a partner at Perkins Coie LLP.

AT&T CEO Randall Stephenson on Thursday reiterated comments he made last month that Congress should determine whether law enforcement should have the ability to access encrypted data on cellphones.

Congress "should decide the proper balance between public safety and personal privacy," Mr. Stephenson said in an emailed statement. "The rapid pace of technological innovation is challenging laws crafted in a very different era for totally different, and much less complex situations. Recent developments, in particular, bring home the need for legal clarity."

Senate Intelligence Committee Chairman Richard Burr (R., N.C.) has decided against a proposal circulating quietly on Capitol Hill to create criminal penalties for companies that decline to comply with court orders to decipher encrypted communications, a spokeswoman said Thursday night.

San Bernardino shooter Syed Rizwan Farook was provided a phone by his employer, which was allegedly subscribed to Verizon, according to government's legal filings. Verizon declined to comment on Mr. Farook's phone.

But the information that Verizon would be able to provide would only be records of phone and text messages placed over its network. The carrier can't provide access to vast amounts of other data, such as message content or calls made over mobile apps like WhatsApp, Skype or the blue iMessages sent between two iPhones.

Phone carriers can see when data is traveling over their networks on a service like WhatsApp or Facebook, but they can't see the content, experts say. That includes the "metadata," such as the time a message is sent, or who it is sent to.

The government and law-enforcement agencies can ask phone and Internet companies to turn over any customer information they possess, such as Facebook for messages retained on their services, and increasingly the government is asking tech companies to do so. But there is no requirement for phone companies or Internet firms as to how long the content of such data is to be stored. The requirement on phone companies is that the government has the ability to intercept traffic in real time.

Apple says it can provide customer data stored in its iCloud service, such as phone backups that can include stored photos, email, documents, contacts, calendars, and bookmarks. In the San Bernardino case, Apple has provided such data for Mr. Farook until Oct. 19, the last time his phone synced to his iCloud. That means there 44 days of data -- such as iMessages and FaceTime calls -- that may only exist on his locked iPhone.

Los Angeles Times
Battle lines drawn over encryption
Friday, 19 February 2016
Byline: Paresh Dave, Tracey Lien

Los Angeles - As hackers prove time and again that they can and will invade our digital lives, Apple Inc. has strengthened its security system to make its services nearly impossible to penetrate -- even for top cops.
Those seemingly airtight protections are great for the company's millions of customers, and rival device makers have rushed to emulate Apple. But as tech companies build virtual fortresses, authorities are mounting a battle to make sure the tech industry doesn't completely shut them out -- as it contends Apple has done by making its iPhone impossible for the FBI to crack.

At the heart of the issue is encryption, a way to secure a digital file by scrambling its contents so that it can be read only by someone who has the key. Tech firms are increasingly encrypting their software, and Apple has been at the forefront.

But sealing off the personal information of customers extends to everyone -- the good guys and the bad guys. That's uncharted territory for tech companies, government agencies and consumers, leaving everyone struggling to figure out how far, exactly, encryption protections should extend.

"We need privacy and security, and frankly Apple has done a better job than most," said Mark Mollineaux Pollitt, adjunct professor at Syracuse University and former director of the FBI's Regional Computer Forensic Laboratory Program. "We shouldn't punish them for doing that. We should find a way to broaden that and make that more effective, but we have to realize there are instances where we have to breach that security to protect all of us."

But not everyone sees it as a gray area, where exceptions can be made for extreme cases like terrorism or child pornography.

This week, Apple Chief Executive Tim Cook took a defiant stance, saying his company would fight a court order in the San Bernardino terror investigation that asks the company to develop, for the first time, software that would allow authorities to circumvent the passcode on the encrypted phone.

Apple's decision isn't without critics, who say courts should be the arbiter of where the line is drawn.

"Apple is obstructing the course of law enforcement and effectively aiding terrorists," said Vivek Wadhwa, a corporate governance fellow at Stanford University. "They changed the technology, so they have to keep up with the ability to unlock the device if the government asks them do it. That's not unreasonable."

As it is, the FBI is publicly admitting that it is locked out, said Jeff Kelley, an iOS developer at software firm Detroit Labs who builds apps for iPhones, iPods, iPads and Mac OS.

"If you're Apple, you couldn't ask for a better ad for iPhone encryption."

That's a nightmare for the FBI.

The agency wants to retrieve whatever resides on the iPhone 5c of Syed Rizwan Farook, one of the two slain shooters who killed 14 people in the Dec. 2 attack.

But the smartphone's iOS operating system is locked by a numeric passcode, likely four digits long. The FBI potentially has only 10 guesses before the phone's contents self-destruct.

Older versions of the operating system provided ways for Apple and even law enforcement to access at least some contents on the phone, even if it was password-protected. For example, older iPhone models were susceptible to unlimited password guessing. In other cases, Apple held a master key, and authorities could ship the company an iPhone and get a DVD or hard drive back with the data from it.

But Apple, in effect, threw away its master key when it deployed a new version of iOS in 2014. Farook's phone runs one of the newer iOS versions.

Adding to the FBI's problems is that Apple is judge, jury and executioner when deciding what software runs on an iPhone: An app or program won't work without a special signature from Apple.

The set-up is aimed at stopping viruses or malware from infecting iPhones, and it also gives Apple latitude to ban apps it doesn't want to support, including for competitive or cultural reasons.

That's significantly more control than Google exercises over smartphones running its open-source Android operating system. Many Android phones support so-called unsigned programs, providing one of the key doors through which law enforcement has been able to extract data from locked phones.

About 80% of the world's smartphones run Android, and about 15% run iOS, according to various estimates.

In general, hardware makers have been making stricter security settings a default on their devices. But while those measures and more have deflected thieves, they left room for law enforcement to acquire data when needed.

Not so with Apple. Besides encryption, the company in 2013 introduced Touch ID, a fingerprint scanner that allows users to unlock their phones by pressing their fingers on the device's home button.

This week's court order requires the FBI and Apple to work in tandem to develop a tool that preserves the data on Farook's phone while allowing an app devised by the FBI to input an unlimited number of passcodes until it guesses the right one.

"That has never before been seen," said Kevin Bocek, vice president of threat intelligence and security strategy at cybersecurity company Venafi. "Apple has very aggressively maintained security, and this is the way the government is going to get around it."

Generating the new software for the FBI wouldn't be trivial, but it's certainly doable, experts said.

Apple would need to make the special code run on the iPhone's short-term memory to ensure it doesn't tamper photos, text messages and other potentially critical evidence, said Dan Guido, chief executive of security start-up Trail of Bits.

The code would get rid of the barriers that normally arise when someone tries too many times to guess a user's passcode. Last, it would have to include a funnel for automated guessing, freeing the FBI from manually entering potentially tens of thousands of numeric combinations.

Even though it's technically capable of carrying out the FBI's orders, Apple and its supporters reject the notion that this would be a one-time thing.

Jonathan Zdziarski, one of the top experts on iPhone security, said the work doesn't end there. If Apple ends up creating a tool, it would need to be tested, including by outside forensic specialists, to stand up to legal scrutiny if evidence retrieved from the phone is ever used in court. That vetting process could drag on for months and risks exposing the tool to people with malicious intent.

There's fear that once a safe-cracking tool is developed, law enforcement agencies from all over the world will repeatedly request its use.

"They've brought a phone that would be easy to justify developing a tool for -- a terrorist's -- but it will be much easier for a court to compel Apple to use it in the future once it's out there," Zdziarski said.

Apple could update iOS to stop the tool developed for Farook's iPhone from working on other ones by requiring consumer consent to run it, but the precedent of making it is irreversible, technologists say.

"You can rationalize it, these are known bad people, this is a known domestic terrorism case and it's one iPhone," said Oren Falkowitz, chief executive of security firm Area 1 Security and a former director of technology and data science programs at U.S. Cyber Command. "But it has implications for all technologies across the globe. We have to be doing more to strengthen the security of the Internet ... or we'll suffer consequences, ... greater than whatever information might be on this one phone."

New York Times
Apple's Strong Stand on Encryption
Friday, 19 February 2016
Byline: Editorial Board

Editorial - It is understandable that federal investigators want to unlock an iPhone used by one of the attackers who killed 14 people in San Bernardino, Calif., in December. And it's understandable that the government would turn to Apple for help. But Apple is doing the right thing in challenging the federal court ruling requiring that it comply.
In an order issued on Tuesday, Magistrate Judge Sheri Pym says Apple must create new software that would bypass security features on the iPhone used by the terrorist, Syed Rizwan Farook. That would allow the Federal Bureau of Investigation to unlock the device and retrieve the pictures, messages and other data on it. Her ruling was based on the All Writs Act of 1789, which is used to require people or businesses not involved in a case to execute court orders. Another federal magistrate judge in New York is considering a similar request to unlock an iPhone in a narcotics case.

Law enforcement agencies have a legitimate need for evidence, which is all the more pressing in terrorism cases. But the Constitution and the nation's laws limit how investigators and prosecutors can collect evidence. In a 1977 case involving the New York Telephone Company, the Supreme Court said the government could not compel a third party that is not involved in a crime to assist law enforcement

if doing so would place "unreasonable burdens" on it. Judge Pym's order requiring Apple to create software to subvert the security features of an iPhone places just such a burden on the company.

Apple has already given the F.B.I. data from the phone that was backed up and stored on its iCloud service; the last backup was made about a month before the attacks. But the company's chief executive, Timothy Cook, has said that requiring it to create software to bypass a feature that causes the phone to erase its data if 10 incorrect passwords are entered would set a dangerous precedent and could undermine the security of its devices. The Department of Justice has argued that the software would be used on that phone only and notes that Apple has previously helped law enforcement unlock phones. The company changed how it encrypts phones after the surveillance revelations by Edward Snowden.

But writing new code would have an effect beyond unlocking one phone. If Apple is required to help the F.B.I. in this case, courts could require it to use this software in future investigations or order it to create new software to fit new needs. It is also theoretically possible that hackers could steal the software from the company's servers.-

There are certainly other ways for law enforcement agencies to collect evidence. They already have the power to get data stored on online services like iCloud and Google's Gmail through search warrants. And they can get records of phone calls and text messages from companies like Verizon and AT&T. A recent study published by Harvard's Berkman Center for Internet and Society concluded that the proliferation of Internet-connected sensors, cameras and other devices provides the government ever-expanding opportunities to collect information about people.

Even if the government prevails in forcing Apple to help, that will hardly be the end of the story. Experts widely believe that technology companies will eventually build devices that cannot be unlocked by company engineers and programmers without the permission of users. Newer smartphones already have much stronger security features than the iPhone 5c Mr. Farook used.

Some officials have proposed that phone and computer makers be required to maintain access or a "back door" to encrypted data on electronic devices. In October, the Obama administration said it would not seek such legislation, but the next president could have a different position.

Congress would do great harm by requiring such back doors. Criminals and domestic and foreign intelligence agencies could exploit such features to conduct mass surveillance and steal national and trade secrets. There's a very good chance that such a law, intended to ease the job of law enforcement, would make private citizens, businesses and the government itself far less secure.

Wall Street Journal
U.S. Clash With Apple Was Months in Making
Friday, 19 February 2016
Byline: Devlin Barrett, Daisuke Wakabayashi

Washington - At a congressional hearing on Feb. 9, Federal Bureau of Investigation Director James Comey discussed obstacles of prying open electronic devices such as smartphones, zeroing in on a case in point: the San Bernardino, Calif., terrorist attack.
"We still have one of those killers' phones that we have not been able to open," he said. "It's been over two months now, and we're still working on it."

Although few realized it at the time, Mr. Comey's comments were a shot across the bow of Apple Inc. The company had been refusing for weeks to help the FBI unlock the phone used by Syed Rizwan Farook, one of the perpetrators of the attack, according to people familiar with matter.

Justice Department officials had even considered filing court papers against Apple a month earlier, only to hold off in the hope of gaining more cooperation.

The standoff, a precedent-setting case on privacy and security in the digital age, culminated this week when a judge ordered Apple to help the FBI circumvent passcode protection on the phone and Apple said it would fight the order. That set the stage for a possible landmark decision on the relationship between government and technology companies. The industry has steadfastly resisted the government's demands for help in unlocking encrypted communications.

It is a legal battle that holds risks for both sides. State and local law-enforcement authorities are already looking to follow the lead of the FBI in its face-off with Apple. On Thursday, Manhattan District Attorney Cyrus Vance said his office is in the process of determining which cases involving encrypted smartphones it should bring before a New York state judge for a similar review.

The legal fight between the Justice Department and Apple over encryption had been building for months. When Mr. Farook and his wife walked into a holiday party for his co-workers on Dec. 2 and began firing -- killing 14 people and injuring 22 -- the government and technology companies had already been feuding publicly and privately over how encryption puts some data beyond the reach of criminal investigators.

In a meeting more than a year ago, the No. 2 Justice Department official told Apple that some day there would be a crucial case involving a locked phone and a missing or murdered child. It would be better for Apple to help on encryption issues before such a case, rather than after, then-deputy attorney general James Cole told an Apple lawyer.

While a terror attack is a different scenario, several federal law-enforcement officials said this week the San Bernardino case was just the kind of thing they had warned about.

Apple executives believed they had worked extensively with law enforcement on the San Bernardino matter. The government's legal documents note that Apple had turned over phone information that Mr. Farook backed up on its iCloud service through mid- October, a month and a half before the attack.

Apple CEO Tim Cook and his colleagues viewed the government's request to create software to get around its own security as a step too far. Apple feels very strongly about two tenets -- data must be encrypted, and its software can't have any "back doors" allowing government access -- Mr. Cook said last year at The Wall Street Journal's technology conference.

Apple's position dovetails with its business interests. It has used its vocal stance on privacy to distinguish itself from rivals that make money on ads targeted at users based on their online data.

And two-thirds of Apple's business comes from outside the U.S., where sentiment about government surveillance is different. Europeans, for example, value privacy highly, and have expressed growing concerns about the control U.S. tech companies exercise over personal data. Government access to user data is also a concern in countries with authoritarian governments.

In the San Bernardino case, a search turned up Mr. Farook's work iPhone. It was owned by San Bernardino County, but the county didn't know the passcode. FBI agents worked to retrieve data on it, including data backed up to cloud storage.

But Mr. Farook had apparently turned off his cloud-storage backup function about Oct. 19, suggesting there still was information on the phone. The FBI and Apple discussed the issue in December without reaching an agreement on how Apple might help open the phone.

Justice Department lawyers prepared in early January to file court papers seeking to force Apple to help, said people familiar with the matter. Some officials weren't optimistic but felt it was worth sending a warning.

At the last minute, prosecutors decided there was a technical question to resolve with Apple, so the two sides kept talking. The technical issue took a few more weeks to sort out. Then the federal government told Apple again it was planning to file court papers to force the company to cooperate.

Privately, government officials hoped Mr. Comey's allusion to the San Bernardino phone before Congress on Feb. 9 would send a signal to Apple that the Justice Department would soon go public with its concerns about the case and the broader issue of encrypted phones.

Percolating in the background was a case with similar issues: In Brooklyn, a federal magistrate judge had asked Apple in late 2015 if there were legal grounds to reject a prosecutor's request for a similar order concerning a drug suspect.

Apple lawyer Marc Zwillinger wrote to Magistrate Judge James Orenstein saying, "Apple has received additional requests similar to the one underlying the case before this court." The judge hasn't decided the matter.

USA Today
Are Android devices more easily hacked than iPhones?
Friday, 19 February 2016
Byline: Brett Molina, Elizabeth Weise

Washington - If Syed Rizwan Farook had carried a phone running on the Android or Windows operating system, the FBI may not have needed to ask anyone for help getting in.
Of the three main phone operating systems, only Apple builds the ability to have the phone erased after a certain number of failed passcode attempts into its operating system, security experts say.

Apple's use of an "Erase Data" feature connected to passcodes is one of the security features that separates it from other smartphones on the market.

That separation became a part of the national discussion Tuesday when a federal judge required Apple to create software to disable the feature that erases the data on the iPhone after 10 failed login attempts.

The FBI wants to get past the feature in Farook's phone to see if there is information on it that will give the agency insight into the mass shooting attack by Farook and his wife Tashfeen Malik in December.

In a letter to customers posted on Apple's website, CEO Tim Cook says the company will fight the order, comparing the request to creating a "backdoor" on all iPhones.

Disabling Apple's "Erase Data" feature, which is what the FBI wants the company to do, would allow it to use a "brute force" attack, entering countless passcodes until they discovered the correct one and gain access to the phone.

The functionality can be added to Android and Windows phones, but it's difficult and meant for system administrators, said Filip Chytr, director of threat intelligence for Avast Software, a Prague- based computer security company.

Google, the creator of Android software, and Microsoft did not respond to a request for information for this report.

Android does include a Remote Wipe option, where a user can remotely erase the contents of their smartphone.

Third-party apps which bring this functionality to Android and Windows phones are readily available but require extra work on the user's part as they're not a built-in functionality that's easily turned on.

In encryption, the encoding of what's on the phone so it's not readable by anyone without the proper code keys, Apple is ahead of the game.

Apple has made encryption the default on its phones since the 3GS. Android only began making it the default with its most recent phone.

New York Times
Line in the Sand Over iPhones Was Over a Year in the Making
Friday, 19 February 2016
Byline: Multiple reporters

Washington - Time and again after the introduction of the iPhone nearly a decade ago, the Justice Department asked Apple for help opening a locked phone. And nearly without fail, the company agreed. Then last fall, the company changed its mind. In a routine drug case in a Brooklyn federal court, prosecutors sought a court order demanding that Apple unlock a methamphetamine dealer's iPhone 5S running old, easy-to-unlock software. The company acknowledged that it could open the phone, as it had before. But this time, it pushed back.

"We're being forced to become an agent of law enforcement," the company's lawyer, Marc Zwillinger, protested in court.

That stance foreshadowed this week's showdown between the Obama administration and Apple over the locked iPhone belonging to one of the suspects in the San Bernardino, Calif., shooting rampage. By the time of Mr. Zwillinger's statement, Apple and the government had been at odds for more than a year, since the debut of Apple's new encrypted operating system, iOS 8, in late 2014.

The new technology repeatedly stymied investigators -- the New York authorities said on Thursday that they had been locked out of 175 iPhones in cases they were pursuing. But both sides held out hope for a compromise that would avoid the type of confrontation that occurred this week when a federal magistrate judge ordered Apple to comply with the Justice Department's request.

With last October's court filing, the confrontation became all but inevitable. The company left no doubt that it would fight any effort to crack its new, encrypted phones. The only real question was what crime the government would use to press its case.

Apple's stance that day in Brooklyn caught the Justice Department off guard. Despite the issue with iOS 8, the company had continued to cooperate. In the first half of 2015 alone, the company provided data

in response to more than 3,000 law enforcement requests, Apple said. And company lawyers gave prosecutors no indication that the drug case against Jun Feng would be any different.

Mr. Feng, 45, claimed to have forgotten his passcode, making his cooperation a moot point even if he were willing to extend it, according to a government filing. Unlike the phone in the San Bernardino case, Mr. Feng's ran iOS 7, an older version of Apple's operating system that does not automatically encrypt its data. The Justice Department figured it would have the information from Mr. Feng's phone within a day.

Mr. Zwillinger said the drug case would be Apple's line in the sand. "Customer data is under siege from a variety of different directions," he said. "Never has the privacy and security of customer data been as important as it is now."

It was a delicate period for the Obama administration, which was focused on finding a way to break into the new encrypted iPhones. The F.B.I., in particular, was lobbying hard to win support for that idea in the face of skepticism from Silicon Valley, Congress and the public.

Timothy D. Cook, Apple's chief executive, described data privacy as a human rights issue. Backed by leading technologists, Mr. Cook argued that if the company designed a way to defeat encryption for the United States government, that tool would be exploited by hackers or foreign governments like China.

Under the attorney general Eric H. Holder Jr., the Justice Department was sympathetic to that point of view, even in the face of an aggressive campaign from the F.B.I. director, James B. Comey. Mr. Holder favored meeting with technology executives in the hope of finding common ground, current and former Justice Department officials said.

Others in the department strongly disagreed. National security and criminal prosecutors argued that, with the introduction of the encrypted iOS 8, Apple (along with Google, which had started its own encrypted Android phone software) had made thumbing its nose at the government a business strategy. The only hope, these prosecutors argued, was a court fight or an act of Congress requiring companies to provide the government unencrypted data.

Local law enforcement officials, too, were sounding alarms. "This has become, ladies and gentlemen, the Wild West in technology," Cyrus R. Vance Jr., the district attorney in Manhattan, said at a news conference Thursday, echoing complaints he and others have made for many months. "Apple and Google are their own sheriffs. There are no rules."

When the attorney general Loretta E. Lynch and her deputy, Sally Q. Yates, took office last year, the F.B.I. and its law enforcement allies found more receptive ears. Ms. Yates, in particular, took up the issue, giving speeches and testifying before Congress alongside Mr. Comey.

Despite the campaign, the White House showed no appetite for legislation. And Apple showed no signs of budging. In a few instances, the two sides appeared bound for a court fight, only to resolve it at the last moment. Last summer, Apple refused to give the Justice Department real-time access to iMessages -- the company's proprietary text messages -- in a gun case. The matter nearly escalated, but Apple eventually turned over some messages that had been backed up to the company's iCloud servers. It was not all that the government wanted, but authorities viewed it as a sign of cooperation.

Such compromises forestalled a major court showdown, but increased the frustration at the Justice Department. Several current and former career prosecutors involved in the issue said they viewed it as hypocritical that Apple encouraged its customers to save its data to iCloud -- which it would turn over to the government -- but regarded the cellphone as sacrosanct.

Then came the Feng case. By refusing to help, the Justice Department thought Apple was sending a clear signal. If it would no longer cooperate with requests to help unlock old phones, there was little chance it would give in and build a way to unlock the new encrypted phones running iOS 8.

"Forcing Apple to extract data in this case, absent clear legal authority to do so, could threaten the trust between Apple and its customers and substantially tarnish the Apple brand," Mr. Zwillinger said.

By that time, 90 percent of Apple devices were running iOS 8 or newer versions. The F.B.I. warned that it was only a matter of time before its agents were locked out of a phone in a case with lives at stake.

The San Bernardino attacks, which killed 14 people, presented the F.B.I. with a seemingly perfect test case. One of the shooters, Syed Rizwan Farook, was killed by the police and left behind a locked, encrypted iPhone 5c. The F.B.I. has not been able to unlock it.

Mr. Farook's phone is protected by a password that Apple says it does not keep and Apple says it cannot break the encryption without the password. The F.B.I. wants to write a program to send the phone an unlimited combination of passwords until it finds one that works.

But Apple built its phones to protect against that tactic. Each wrong guess causes a short delay, which would significantly slow the F.B.I.'s effort. After too many incorrect guesses, the phone will automatically erase its memory.

The authorities are still interested in more than just Mr. Farook's phone. On Thursday, a team of F.B.I. agents raided the Southern California home of his brother, Syed Raheel Farook, and carted off boxes of belongings. The authorities would not say what they were searching for.

But there is no telling what is on Mr. Farook's phone -- maybe clues to accomplices or his inspiration, maybe nothing -- but nobody in the government questioned the need for obtaining access to that data. From a public relations standpoint, Apple had been on the side of privacy advocates and civil libertarians. This case put the company on the side of a terrorist.

"They need to figure that out now before there is that bigger body count. So this is as good a test case as any to have that fight," said Ron Hosko, who until 2014 led the F.B.I.'s criminal division. "Crack that thing for me now, Tim Cook, because it's only going to get worse."

This week, the Justice Department got its wish when Apple was ordered to override its defenses, even if it meant building a tool that did not exist.

Law enforcement officials cheered the ruling, though they acknowledged that the fight was not over. Apple promised to appeal. In New York, William Bratton, the police commissioner, held up a phone that he said was used by an associate of a man who shot and wounded two police officers in the Bronx recently.

"Despite having a court order, we cannot access this iPhone," Mr. Bratton said. "Just one example, a very significant example in which two of my officers were shot, that impeding that case going forward is our inability to get into this device."

The case in Brooklyn continues, even though Mr. Feng has already pleaded guilty. While the Justice Department sees the San Bernardino incident as its ideal test case, Apple is hoping for a legal win in Brooklyn.

Judge James Orenstein has given the company reason to be hopeful. In the past, he has been skeptical of the way the government uses an 18th-century law -- the All Writs Act -- that the Justice Department is now claiming gives it the authority to force Apple to unlock the phones. He once even described the Justice Department's use of it as a "Hail Mary play."

But he has yet to rule.

Wall Street Journal
The FBI vs. Apple
Friday, 19 February 2016
Byline: Editorial Board

Editorial - The encryption cold war that for two years has pitted Silicon Valley against law enforcement finally turned hot this week, as a California judge ordered Apple to unlock an iPhone used by the San Bernardino terrorists. Perhaps public safety and modern digital security methods were bound to collide, but the danger as always in such conflicts is that both sides end up annihilated.
The Federal Bureau of Investigation is attempting to bypass the security system on an iPhone recovered from Syed Rizwan Farook, who with his wife Tashfeen Malik killed 14 people and injured 22 others. The problem is that no one knows the phone's password.

Apple has turned over information that Farook stored to its cloud servers, but he did not back up his phone for several weeks proceeding the attack. The FBI wants to retrieve this encrypted data that exists only on the device itself, which potentially include text messages, photos, location tracking or connections to the Islamic State or perhaps even other terror cells that could be operating in the U.S.

Apple's iOS operating system is designed to automatically erase local data after too many incorrect passcode attempts. Because iPhones can only run software with Apple's proprietary cryptographic signature, the FBI wants Apple to create and upload a custom version of iOS to Farook's device that overrides this mechanism. The bureau can then hook up an external computer that will make unlimited guesses to unlock the phone's contents, known as "brute forcing." Magistrate Judge Sheri Pym agreed.

In a public letter, Apple CEO Tim Cook refused to comply with this "unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority" and said the company would appeal. "The U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone," he wrote.

Yet the reality seems to be more complicated than either Mr. Cook or the FBI allow. The encryption debate began in 2014 when Apple released a feature that generates random security "keys" that are unknown to Apple and in combination with the user's passcode to decrypt the device's data. Without such mathematical formulas, the data are unreadable.

This two-step "full disk" encryption process makes iPhones more secure, but it also means Apple can't unlock its own products. Neither can Google after adopting the same practice. Encrypted communication platforms have been available since the early 1990s, but Apple and Google have now made them the default for the 96% of global customers who use their operating systems.

The fear among law enforcement and the national-security agencies is that jihadists and criminals are going dark. FBI chief James Comey and Manhattan District Attorney Cy Vance warn they are losing the capacity to execute bona fide search warrants granted under the Fourth Amendment. So they support a mandate that the U.S. tech industry install a master security key -- the "backdoor" Mr. Cook invokes -- to unlock any device.

The CEO has a strong case when he says that backdoors create more problems than they solve. Introducing security vulnerabilities that third parties like cops and spooks can use as needed can also be exploited by hackers, crooks and spies. Nations can mandate backdoors, but there will always be some encrypted channels outside of their jurisdiction where the likes of ISIS can plot. The result would be weaker products for law-abiding consumers that leave U.S. companies less competitive with little security benefit.

Stronger cybersecurity is more important than ever in a world of corporate espionage, millions of compromised credit-card numbers and the stolen identities at the Office of Personnel Management. Encryption may lead to fewer antiterror intercepts, though the universe of signals that can be tapped has expanded radically and on balance more secure phones are a major advance for human freedom. Ask the Chinese pastors or Russian dissidents who are targeted by authoritarian regimes and want encrypted iPhones.

One question is whether the San Bernardino terror case should be an exception to Mr. Cook's strong argument against backdoors. In this case Apple is not being ordered to create a universal backdoor for all phones, and some digital security experts believe it is technologically possible to assist the FBI in the San Bernardino investigation with a unique iOS to brute-force this single device.

"Apple does not dispute that it has, in prior instances, complied with data extraction demands that have been contained in the body of search warrants or, less often, All Writs Act orders," Apple conceded in a New York court filing last year. The government is citing this to show that its request is reasonable.

But in those cases the company's engineers have never been conscripted to create a new architecture to defeat their own security measures. Apple believes that if it caves even once, every prosecutor in America will be lining up for forensic help with misdemeanors. A supposedly one-time emergency fix in an antiterror case could well become a de facto backdoor in practice over time.

There's also the question of whether the government currently has the legal authority to force Apple to become the government's agent. Safe manufacturers are not obligated to crack their own locks when the FBI calls. Apple contends the All Writs Act has never been used to compel what the government now wants from Apple, and the question is far from clear-cut. The litigation to settle this could take months or years.

It's an understatement to say that Apple is taking a risk by challenging the Administration in a high-profile domestic terror incident with unpredictable politics. "Apple chose to protect a dead ISIS terrorist's privacy over the security of the American people," said Arkansas Republican Tom Cotton, and Donald Trump has been no more subtle.

But for the same reason, the Administration ought to have resolved the situation confidentially before it reached legal and political Defcon One. Terror cases by their nature are different from run-of-the-mill law enforcement, and San Bernardino requires more than the government's typical show of incompetence.

The White House never supplied Congress with specific backdoor statutory language even as Mr. Comey made the public rounds, only for President Obama to renounce any attempt at forging a legislative

solution. Yet spokesman Josh Earnest defended the FBI and Justice Department on Wednesday. Is there a grownup in the White House?

So a word on behalf of Michael McCaul, the Chairman of the House Homeland Security Committee, who has proposed convening an expert panel on technology and security in the modern era. Blue-ribbon commissions are usually a form of Beltway escapism, but in this case a detailed report and recommendations from leading minds in technology, law, computer science, police and intelligence could help shape a rough consensus -- or at least establish a common set of facts. Such a halfway house might also help calm political tempers and marginalize the absolutists.

A mature democracy -- if America still is one -- ought to be able to work out these crucial matters of national security through legislative deliberation. The public interest on encryption is best served with a rational debate, not the ad hoc nuclear legal exchange that the Administration is inviting.

Washington Post
Wrong bite of the Apple
Friday, 19 February 2016
Byline: Editorial Board

Editorial - Until Tuesday, Apple appeared to be winning its fight with law enforcement. President Obama announced last year that he would not pursue legislation forcing tech companies to give law enforcement access to users' encrypted data. But on Tuesday, the FBI persuaded a judge to order Apple to create software that would help federal investigators crack into the iPhone 5C that Syed Rizwan Farook used before he shot up a San Bernardino, Calif., banquet room in December. Apple immediately promised to fight the order.
In essence, the FBI is attempting to explore and establish the limits of its legal powers to combat terrorism - as well as more mundane domestic crimes - under existing laws, in the absence of action by Congress and the White House. We think that's the wrong call. The nation should not ask the courts to strike a balance between device security and law enforcement access. The political branches of government should do that.

The FBI relied on the two-century-old All Writs Act, a law that helps the government execute search warrants, to compel Apple to create hacking software for Farook's phone. The order was nominally tailored to Farook's specific device, but its implications are larger. To what extent is it reasonable to force companies to write code and harm their international reputations for data security - and, therefore, their business models - in order to help the U.S. government hack into suspects' phones? Should this be a routine investigative tool, or reserved for extraordinary situations, or beyond the pale? Farook's is an extreme case, but it is easy to foresee the government attempting to apply All Writs to

less important investigations. What sorts of software can the government compel tech companies to write?

The answers to these questions have major implications for online safety and security. The more government-ordered hacking techniques are developed and used, the more likely they eventually will fall into the hands of malicious actors. This risk seems small but is difficult to estimate. Even if technology companies and the government kept the techniques they developed secret, their hacking activities would still threaten the technology ecosystem. Fearful of government-mandated malware, fewer people might accept automatic updates from software companies. This would make devices more vulnerable. The anti-terrorism benefits, meanwhile, would wane over time, as high-level terrorist groups turned to software from places beyond the reach of U.S. law enforcement.

The public has reason to be frustrated that investigators cannot execute valid search warrants; this is a worrying impediment to legitimate law enforcement. We believe Apple should help search for a workable solution. If there is a Paris-style attack in the United States, decisions may be imposed on it in a far less benign atmosphere. But the decisions should be made by Congress.

Meanwhile, Apple's role as a leading exponent of data security brings special responsibilities. Whatever U.S. officials decide, the policy will be the legitimate product of a democratic government and the rule of law. That will not be true in countries such as China, where dictators would use anti- terrorism tools to crack down on dissenters. We hope that Apple will fight as hard to safeguard its users' privacy from authoritarian abuse.

Motherboard (Vice)
Police Arrest Second Alleged Member of Teen Group that Hacked CIA Director
Thursday, 18 February 2016
Byline: Lorenzo Franceschi-Bicchierai

New York - The grip seems to be tightening around the infamous group of teenage hackers that's been targeting US government agencies and high- level officials for months.
On Tuesday, police in Scotland arrested a 15- year-old boy from Glasgow, whom a source told Motherboard is one of the main members of the hacking group known as "Crackas With Attitude," or CWA. The teenager, according to the source, is the hacker known as "Cubed."

The arrest of the teenage hacker comes only a week after UK police, working with the FBI, arrested another alleged member of the group, a 16-year-old boy suspected of being Cracka, another main member of the group. Following the arrest of the boy in the UK, other members of the group, including Cubed, pledged to keep hacking and threatened the US government with more attacks.

A close friend of the arrested hacker confirmed he was the CWA member known as Cubed. The close friend spoke to Motherboard on condition of anonymity.

"I hope he's okay, he was like a brother to me," the source said.

A spokesperson from Police Scotland confirmed the arrest of a boy suspected of hacking crimes, but declined to answers questions on whether he was one of the members of the hacking group.

"Following a search of a property in the Glasgow area on Tuesday the 16th of February, a 15-year old male was arrested in connection with alleged offenses under the Computer Misuse Act 1990," the spokesperson said in a prepared statement. "He has since been released from custody and he is subject of a report to the procurator fiscal."

The arrest was first reported by the local tabloid the Daily Record on Thursday. The paper also reported that FBI agents flew to Glasgow to question the boy. Before that, on Wednesday morning (US time) another member of CWA tweeted that Cubed had been arrested.

The member, known as IncursioSubter, did not respond to a request for comment. Other members of the group declined to comment as well.

In a phone call, an FBI spokesperson didn't respond to questions regarding the arrest. And a spokesperson from the South East Regional Organised Crime Unit (SEROCU), the UK agency who arrested the teenager suspected of being Cracka, also declined to comment.

In October, Cracka and Cubed claimed to have broken into the AOL email account of John Brennan. This was just the first in a long list of attacks on high profile officials such as FBI's executive assistant Amy Hess, US spy chief James Clapper, a former senior executive at the National Geospatial-Intelligence Agency, and President Barack Obama's senior advisor on science and technology John Holdren.

More recently, the hackers were also apparently involved in a breach at the US Department of Justice, which ended up with the dump of almost 29,000 names, titles, email addresses and phone numbers from the FBI and the Department of Homeland Security.

The Daily Record (Scotland)
FBI swoop on schoolboy Scots hacker accused of breaking into their top-secret computer system
Thursday, 18 February 2016
Byline: Stephen Stewart

Glasgow - FBI agents swooped on a Scots schoolboy accused of trying to hack into their top-secret computer system.
Operatives from the US crimebusting agency travelled to Glasgow after detectives arrested the 15- year-old on Tuesday and searched his home.

It is understood the FBI agents sat in as Police Scotland officers interviewed the boy, who could face extradition and imprisonment in the United States.

A source said: "The boy is believed to have hacked into the FBI's computer systems.

"Agents then travelled to Scotland to sit in on him being questioned by detectives. He could be extradited to the US where he would face a long jail term."

Police confirmed that the boy had been arrested and later released.

A spokesman said: "Following a search of a property in the Glasgow area on Tuesday, February 16, a 15-year-old male was arrested in connection with alleged offences under the Computer Misuse Act 1990.

"He has since been released and is the subject of a report to the procurator fiscal. It would be inappropriate to comment further at this time."

A source close to the case said the boy's family were shocked at the turn of events, adding: "He comes from a respectable family."

The Glasgow operation comes just months after a Scot was dubbed the most dangerous hacker of all time by activist group Anonymous.

IT whizz Gary McKinnon, 49 - who has Asperger's syndrome - broke into 97 Pentagon and NASA computers, stealing passwords, deleting files and shutting down net-works on military bases.

He faced trial in the US and up to 70 years in jail if convicted - but Home Secretary Theresa May blocked his extradition under human rights laws.

In December, Anonymous labelled McKinnon the best-ever "black hat" hacker - the term for hackers who indulge in illegal activity.

Just days ago, police in the East Midlands arrested the alleged teenage mastermind of cyber attacks targeting US government officials

It is not known if the Glasgow teenager's case is linked to those events.

Reuters
Islamic State finds 'diminishing returns' on Twitter: report
Thursday, 18 February 2016

Washington - The Islamic State's English-language reach on Twitter has stalled in recent months amid a stepped-up crackdown against the extremist group's army of digital proselytizers, who have long relied on the site to recruit and radicalize new adherents, according to a study being released on Thursday. Suspensions of English-speaking users affiliated with Islamic State from June to October 2015 have limited the group's growth and in some cases devastated the viral reach of specific users, according to the report from George Washington University's Program on Extremism, which analyzed a list of accounts promoted by the militant group.

The report found that easily discoverable English accounts sympathetic to Islamic State was usually under 1,000, and that those users' activity was mostly insular, limited to interacting with each other. Islamic State has seized control of wide swaths of Iraq and Syria and claimed credit for attacks in Paris in November that killed 130. The U.S. and other governments consider it a terrorist organization.

Twitter Inc. has long been criticized by government officials for its relatively lax approach to policing content, even as other Silicon Valley companies like Facebook Inc. began to more actively police their platforms.

Under intensified pressure from the White House, presidential candidates and some civil society groups, Twitter announced earlier this month it had shut down more than 125,000 terrorism-related accounts since the middle of 2015, most of them linked to the Islamic State group.

In a blog post, the company said that while it only takes down accounts reported by other users it had increased the size of teams monitoring and responding to reports and has decreased its response time "significantly."

J.M. Berger, a co-author of the report, said Twitter is still less active than many of its rivals but that part of that is due to its relative youth as a company.

"Each company has been dragged into this kicking and screaming," he said in an interview.

Reporting of Twitter accounts affiliated with Islamic State is a steady, low-level activity generally, but occasionally events lead to "periodic purges," Berger said.

The study took place prior to the Paris attacks, which the researchers said likely led to a heavy wave of suspensions mostly in French and Arabic networks.

The average tweets per day measured across the lifetime of an account also declined during the monitored interval, from a peak of approximately 14.5 in June to a low of 5.5 by October, the report found. The average number of followers was measured between 300 and 400.

La Dépêche du Midi (Toulouse)

Amende pour le webmaster indélicat
Friday, 19 February 2016
Byline: J.R.

Albi, France - T.R., webmaster gaillacois de 31 ans et papa d'un enfant de 4 ans, comparaissait hier à la barre du tribunal correctionnel d'Albi présidé par la présidente Brigitte Schildknecht pour «accès frauduleux dans un système de traitement automatisé de données et collecte de données à caractère personnel par un moyen frauduleux », des faits commis courant septembre 2014 au préjudice du conseil général du Tarn puisque c'est, on s'en souvient, son site internet qui avait fait l'objet de nombreuses cyberattaques à cette époque. Une époque, rappelons-le quand même fortement marquée alors par «la bataille de Sivens entre Zadistes et pro- barrage. Le prévenu est un sympathisant zadiste et ne s'en cache pas mais réfute toute intention frauduleuse. «Je ne me suis jamais introduit sur le site du conseil général et je n'ai jamais collecté la moindre donnée».
«Pourtant, lui rétorque la présidente, les enquêteurs de la direction générale de la sécurité intérieure (DGSI) qui ont perquisitionné chez vous et avec qui vous avez passé quelques heures en garde à vue parlent de 100 000 requêtes suspectes.» «J'en ai seulement fait 150 depuis mon adresse IP (IP pour Internet Protocol), reconnaît T.R. à la barre. D'ailleurs, je ne me suis jamais caché. Je n'ai pas mis d'image et encore moins de vidéo sur ce site. J'ai juste mis un lien dans une barre d'adresse du site. Après, je n'y suis pour rien si durant cette période, les Anonymous dont je ne fais absolument pas partie, ont attaqué le site du Département. La seule chose que je n'aurais pas dû faire est de repartager des données du conseil général. Mais jamais je ne pensais qu'un simple copier/coller allait me conduire à la barre d'un tribunal.»

L'avocate du Département du Tarn s'insurgera ensuite «contre les préjudices subis avec un serveur piraté et remplacé, trente sites web affectés, des usagers pénalisés et réclamera 20 700 euros, 10 700 euros et 6 000 euros respectivement aux titres des préjudices technique, d'atteinte à l'image et opérationnel sans oublier 3 000 euros au titre de l'article 475-1.»

Selon Pascal Suhard, vice- procureur de la République, on reconnaît volontiers que vous n'appartenez pas aux Anonymous mais vous minimisez votre responsabilité en parlant d'une bêtise que vous n'auriez pas dû faire. Je requiers à votre encontre deux mois de prison avec sursis.»

Guillaume Pressec, avocat de T.R., demandera purement et simplement la relaxe de son client arguant que «les deux infractions retenues contre lui ne sont pas caractérisées. Il n'a en effet dénaturé aucun site. Il n'est par ailleurs pas poursuivi pour avoir inséré une vidéo sur ce site. Ensuite, on lui reproche du vol informatique. Or, il n'a jamais collecté frauduleusement de données. Elles étaient en vente libre sur internet. Il n'a fait qu'un copier/coller. Ce dossier est celui des fantômes, les Anonymous, condamnées pour certains par d'autres juridictions.»

Pas de prison avec sursis pour T.R. qui écope de plusieurs amendes pour un montant total de 4 000 euros.

Toronto Sun
Trudeau government to take on cybersecurity threats
Friday, 19 February 2016
Byline: David Akin

Ottawa - With Internet-based child sex-ploitation crimes skyrocketing, the Justin Trudeau government intends to launch a "credible and comprehensive" review this spring of cybersecurity threats in Canada. Officials with Public Safety Canada said Thursday that while the details of that review are still being hammered out by Public Safety Minister Ralph Goodale, a review will determine how Canada can best deal with everything from online predators to digital jihadists.

Kathy Thompson, the assistant deputy minister in charge of the Community Safety and Countering Crime Branch at Public Safety Canada, said while the crime rate continues to decline across the country, "there are some exceptions. One of those exceptions is child sexual exploitation over the Internet -- that is going up exponentially, year over year."

Thompson made her remarks at the House of Commons Public Safety and National Security Committee, where MPs are looking for topics their group can zero in on during the current parliamentary session.

A cybersecurity review that looks at legal gaps and shortcomings in police resources could form a plan for the way the Trudeau government approaches law-and-order issues.

"It is our intent to conduct a review that is going to be credible and comprehensive and reaches out to all stakeholders across Canada. And also to our international partners," said Monik Beauregard, the senior assistant deputy minister at Public Safety's national and cyber-security branch.

Liberal MP Marco Mendocino, a former Crown prosecutor who played a key role in putting some of the Toronto 18 terrorists in jail, told the committee he is particularly concerned about financial crime -- the use of computers and telecom networks by organized criminals, including terrorists, to move and hide money -- as well as the use of social media as a breeding ground for online hatred and incitement.

"The fact that we are now so invested in cyberspace can make us vulnerable," said Mendocino.

He wanted to know what the top public safety issues were for Canada's most senior security bureaucrats.

Child sex- ploitation is right at the top of the list, Thompson said.

"That is one of the areas that's keeping us awake. We're working very actively on that. We're partnering not just in Canada but internationally," said Thompson.

Thompson said identify theft and intellectual property crime are two other areas where the crime rate has been rising because of the widespread adoption of the Internet.

Canadian Press
Canada's electronic spy service to take more prominent role in ISIS fight
Friday, 19 February 2016
Byline: Murray Brewster

Ottawa - The Communications Security Establishment, Canada's electronic spy service, is set to play a more prominent role in the war against the Islamic State of Iraq and the Levant, The Canadian Press has learned.
Multiple sources familiar with the plans, speaking on condition of anonymity owing to the sensitivity of the matter, say the government is deploying a capability that only a "handful of countries" in the world can provide.

CSE is part of the so-called "Five Eyes" community, along with the U.S. National Security Agency -- the NSA.

CSE spokesman Ryan Foreman acknowledged the agency is helping the Canadian Armed Forces under the umbrella of Operation Impact, the name of Canada's anti-ISIL mission in the Middle East, but refused to discuss specifics.

"While we are proud of our contributions to CAF's missions, CSE is obligated to respect the Security of Information Act, and cannot address specific operational questions," Foreman said.

Defence Minister Harjit Sajjan has for weeks been signalling that the military will introduce a "more robust" intelligence-gathering regime, one that allies -- chastened by the withdrawal of the six CF-18s -- are happy to be bring to the fight.

Separately, Public Safety Minister Ralph Goodale confirmed Thursday that the Canadian Security Intelligence Service will also play a stepped-up role in the fight against the Islamic State, but he also refused to be specific.

"We are providing new and additional intelligence capabilities in the region and while by its very nature I cannot elaborate, CSIS will have a role to play," Goodale said.

"It will certainly be an increased role to accomplish larger objectives."

The defence conference where Goodale and Sajjan were speaking heard Thursday about how CSIS agents cultivated human sources in Afghanistan.

But CSE played a pivotal role alongside the Canadian Army during the Afghan war, providing by its own admission half of the crucial battlefield intelligence on Taliban militants, their movements and the locations of key commanders.

The information was used to plan military operations and for targeted capture or kill missions by special forces. But one official, speaking on condition of anonymity, said Canadians would provide targeting only and not take part in any "direct action."

Although he's been eager to trumpet the "doubling" of the intelligence effort, Sajjan has been decidedly opaque about what that means, even last week when he announced the retooled mission.

"Enhanced intelligence capability will help protect our forces in theatre as well as those of our coalition and host nation partners," Sajjan said.

"Therefore, we will significantly increase the resources we dedicate to intelligence, both in northern Iraq and theatre-wide. Our intelligence capabilities will help the coalition and Iraqi security forces develop a more sophisticated picture of the threat and improve our ability to target, degrade and defeat ISIL."

What that likely means in practical terms, according to sources and intelligence experts, is the involvement of the secretive CSE and specialists from the 21st Electronic Warfare Regiment.

It also means deploying Canadian intelligence officers into the highly secure all-source intelligence centre in Kuwait, and potentially hacking ISIL computers and smartphones.

When pressed, Sajjan refused to discuss the details.

"Unfortunately, I'm not going to talk (about it) in public for operational security reasons," he said.

"The last thing you want to be able to do is show your hand to (ISIL) and let them know what type of capability you are bringing in, but we have very unique capabilities for the coalition, and what I will say is capabilities for theatre-wide for the entire coalition and then we have very specific capabilities for our troops in the north as well."

Bill Robinson, a blogger and expert on signals intelligence, said it is a matter of public record that the military and CSE have an integrated operational model for field operations, which proved highly successful in Afghanistan.

"It was a pretty substantial contribution on the intelligence side," said Robinson, who noted that signals kept watch over not only the movement of Taliban units and commanders, but also provided early warning of threats -- such as the planting of roadside bombs -- and even kept tabs on local Afghan government officials.

Deploying a similar capability to northern Iraq would, in Robinson's estimation, be a significant step-up in terms of the fight.

"It's a plausible argument that this is a contribution that would be valued just as much as the fighter-bombers," he said. "Increasingly, I think this kind of warfare is down to intelligence."

It is likely filling a gap that the Americans are unable to cover themselves, Robinson added.

Throughout the war against the Islamic State, U.S. commanders have repeatedly called for more intelligence data, mostly in the form of extra drone flights. Washington was forced to strip the remote-controlled aircraft from operations in Afghanistan, according to published reports.

Documents leaked by former NSA contractor Edward Snowden indicate "that in the Horn of Africa and Afghanistan, they were not getting all the signal intelligence they wanted," Robinson said.

That's one of the reasons Canada deployed its own capability to Kandahar during the war, he added.

The game could be upped even further with the purchase of special tactical intelligence surveillance planes, similar to the King Air turboprop aircraft used by special forces in Afghanistan under a contract with the U.S. Army. The federal government quietly floated a letter of interest in September to see if defence contractors could deliver three aircraft.

In addition, Robinson says Canadian intelligence officers are highly valued in multi-national intelligence hubs like the one in Kuwait, because they "are cleared into the Five Eyes community."

Toronto Star
Has Apple secretly leaked your data to government?
Friday, 19 February 2016
Byline: Frederick Ghahramani

OpEd: Apple CEO Tim Cook's now widely shared "Message to our Customers" is an attempt to make the best PR move in a bad situation.
Were Apple to comply with the FBI's request to access information locked on a suspected San Bernardino shooter's phone, it probably wouldn't be the first time that the government has deputized Apple to breach its customers' privacy.

According to documents revealed by Edward Snowden in 2013, Apple was one of the participants in the U.S. National Security Agency's PRISM program, giving authorities access to its customers' information including their emails, messages and photos.

Apple for its part has denied any such involvement, but given the secretive nature of the United States Foreign Intelligence Surveillance Court (FISA Court), Apple and other technology companies would be prohibited to publicly acknowledge their involvement in such programs.

Hence the frustrating catch-22 - is Apple really a champion of privacy rights? Or is all this bluster just an act to score PR points with their customers, despite the fact that legislative conditions already exist to force Apple to co-operate in secret?

Maybe we'll never know, and it probably doesn't matter, because the real lesson that can be learned from this episode is the importance of open source software.

While Apple has invested heavily in encryption and security, most of its systems and applications are closed. For all we know, Apple could already have been secretly compelled to program backdoors into its popular services such as iCloud and iMessage - even against the wishes of its CEO.

In fact, rumours such as this one have been circulating for quite some time. If true, this means that millions of customers could already have had their privacy invaded without ever knowing and, more importantly, the decision to do so would be adjudicated in a secret court, completely out of Apple's hands.

In contrast, in an open source model, the source code of an application is available to the general public, and a global community of curious engineers (there are millions of us) could effectively "look under the hood" to ensure that no backdoors existed. Such transparency can only be achieved in an open-source environment, and Apple has historically chosen to operate contrary to this model.

The second and more important lesson is that situations such as this distil the abstract concept of encryption into frightfully political sound bites. Recently, John J. Escalante, chief of detectives for Chicago's police department, went so far as to suggest that "Apple will become the phone choice for the pedophile."

The truth about encryption is obviously far more nuanced. Encryption is not a dirty word, nor is it something that's only useful to terrorists and pedophiles. Consider going a day without encryption - being unable to use your credit card, withdraw funds from an ATM, or simply make a mobile phone call - and you quickly realize how any legislation that weakens encryption would have far-reaching social, political and economic consequences.

It has been argued that mathematically crippling encryption systems to grant the government a so-called "master key" would be a good way to protect our safety and security. That's a strange case to make when most people would never agree to give the police a master key to open every house in the country (even if pedophiles and terrorists also live in some of those houses).

Furthermore, such arguments naively assume that only the "good guys" would retain (or devise) such master keys. At a time when accidental data losses by governments around the world have become an all too common occurrence, it's no wonder Apple is concerned about being forced to grant the government such access.

The U.S. government has painted not just Apple but the entire technology industry into a corner. The industry's answer needs to lie in advances in encryption technology and open source software. Given the opaque and Byzantine nature of the security apparatuses in both the U.S. and Canada, it will soon be impossible to decipher who's been compelled to do what or when - no matter what their press release states.

Frederick Ghahramani is the CEO and founder of just10.com, an ad- free private social network.

Globe and Mail
Museveni temporarily bans social media and has rival arrested, while police fire tear gas to disperse protesting voters
Friday, 19 February 2016
Byline: Geoffrey York

Johannesburg - Authorities blocked access to social media and police arrested an opposition leader as Uganda's President sought to extend his 30- year grip on power in a bitterly contested election on Thursday.
President Yoweri Museveni, who seized power in 1986 and is heavily favoured to win the latest election, said the temporary ban on Facebook and Twitter on election day was necessary because some Ugandans were "telling lies" and "misusing" social media.

"There must be steps taken for security, to stop so many creating trouble," the President told Ugandan media. "You know how they misuse them, telling lies. If you want a right, then use it properly."

Police fired tear gas to disperse voters who protested long delays in providing ballots and election materials at some voting stations. The main opposition leader, Kizza Besigye, was arrested for the second time in four days.

He was charged with "criminal trespass" when he went to the gates of an unmarked police-intelligence building, which he alleged was a vote-rigging centre.

Mr. Museveni, 71, is just the latest African leader to attempt to orchestrate the continuation of his rule, despite growing calls for term limits. At least 15 leaders across Africa have served more than two terms or announced plans to do so. In a youthful continent where the average age is 19, many leaders are elderly and unwilling to give up any power. The average age of the 10 oldest African presidents is 78. The oldest, Robert Mugabe of Zimbabwe, turns 92 on Sunday.

Mr. Museveni himself had once scathingly criticized African leaders for their tendency to cling endlessly to power. In 1986, after a five-year bush war in which he led his guerrilla army to victory, he proclaimed: "The problem of Africa in general and Uganda in particular is not the people, but leaders who want to overstay in power." But once he got a taste of power, Mr. Museveni seemed to forget those words. He became increasingly dominant in a system that revolved around his personal rule, backed by the military. In 2005, he allowed multi-party elections for the first time, but he also scrapped term limits, allowing himself to rule indefinitely. He is also now expected to get rid of the constitutional age limit of 75.

Mr. Besigye, his former ally and personal physician, has run unsuccessfully against Mr. Museveni in three past elections, often suffering harassment by the police. He has been repeatedly arrested, roughed up or confined to house arrest. On Monday, he was tear- gassed again when police broke up an opposition rally.

Mr. Museveni has always exploited the advantages of power to ensure that the opposition has little chance of beating him. A recent study by an independent civil society group found that he has spent more than $7-million (U.S.) on his current presidential election campaign. That's 12 times more than the amount spent by his top two opponents combined, the study found.

His supporters, including a controversial unit of pro-regime "Crime Preventers," have routinely used intimidation tactics against the opposition. A police chief, for example, warned that the "Crime Preventers" would be armed with guns and ready for "war" against anti-government protesters. A senior member of the ruling party told opponents that the government will "kill your children" if they protest the election results this week.

The ban on social media was sharply criticized by humanrights groups and diplomats. But it was part of a larger trend of harassment of the media, including physical attacks on journalists and the closing of radio stations.

Though the Museveni government is often criticized for human-rights abuses and crackdowns on the opposition, it has benefited from the strong support of the United States, which sees Uganda as a key ally in the fight against Islamist radicals in Somalia. In recent years, Uganda has become one of the top African recipients of U.S. security assistance.

Official results of Thursday's election are expected to be released by Saturday. Votecounting was continuing on Thursday night, sometimes by the light of lamps and cellphones in darkened voting stations. Early provisional results, from less than 5 per cent of voting stations, showed Mr. Museveni in the lead.

Globe and Mail

Tech giant defends privacy by refusing to give in to government order to hack its own phones
Friday, 19 February 2016

Editorial: Apple Inc.'s refusal to help the United States government hack into the iPhone of a dead terrorism suspect is a difficult but necessary decision. In the end, the tech company has to weigh a concrete threat to its customers' privacy against the ambiguous needs of the police.
Apple and companies like it build smartphones and tablets with the promise to customers that the personal information they keep on their devices will be protected from hackers and prying eyes. It is a critical aspect of the companies' sales pitches, and also a responsibility in the digital age.

Once a customer has purchased one of Apple's most recent phones and tablets, its contents are inaccessible even to the company that manufactured it without the user's permission. Any repeated attempt at access that isn't authorized by the user causes the devices to automatically erase all of their contents.

A judge in California, however, has ordered Apple to bypass this security system on the iPhone of Syed Farook, who along with his wife killed 14 people in a mass shooting in San Bernardino in December. The FBI asked for the order because it believes - though it does not know for certain - that there could be information on the phone that will help explain the shooters' motives and possibly lead to accomplices. The police are on a fishing expedition, looking for any clues, anywhere.

Apple won't comply for a simple reason: If it creates a bypass around the security system of one iPhone, it is necessarily doing so for all iPhones. This would be a violation of its promise to protect customers' privacy.

In fact, it would blow a hole in expectations of privacy. Once such a breach is made, it can't be unmade. Customers would know it and might lose confidence in Apple products, along with those of any other manufacturer met with a similar government order.

There is also the broader issue of governments' rapacious hunger for private citizens' personal data. If Apple yields to the U.S. government, there can be little doubt that other governments will come demanding the same thing. All they will need to do is raise the charged issue of fighting terrorism to make their case.

It's better, then, for Apple to keep saying no. It has co-operated with the FBI as much as it can, but should go no further.

Journal de Montréal
L'Oncle Sam veut voir dans votre iPhone
Friday, 19 February 2016
Byline: Pierre Martin

Opinion - Le jeu du chat et de la souris entre les services de renseignement et les défenseurs de la vie privée expose quelques dilemmes et contradictions de la lutte contre le terrorisme.
Après les attentats de San Bernardino, les enquêteurs ont récupéré l'iPhone d'un des meurtriers. Le FBI exige qu'Apple lui fournisse le moyen de débloquer l'accès aux données précieuses qu'il pourrait contenir. Le fabricant refuse.

Apple allègue ne pas pouvoir désactiver la sécurisation du téléphone, mais l'entreprise craint surtout qu'une telle clé puisse tomber entre des mains malveillantes ou que ce cas constitue un précédent pour des régimes répressifs ailleurs dans le monde.

Un dilemme cornélien

De plus en plus, la menace terroriste provient d'individus radicalisés de l'intérieur des sociétés occidentales plutôt que de groupes extérieurs. Ce changement incite les États à accentuer la surveillance interne, au détriment du droit à la vie privée de leurs citoyens.

Il n'y a pas de solution évidente, mais à ceux qui croient qu'aucune limite ne peut être imposée à l'action antiterroriste de l'État, il faut rappeler que ce phénomène représente encore un risque assez minime. Le Nord-Américain moyen a plus de chances d'être frappé par la foudre que d'être victime d'un attentat islamiste.

Personne à l'abri des contradictions

Il est louable qu'Apple défende avec vigueur la vie privée de ses clients, mais il n'en demeure pas moins que le fabricant tire un énorme bénéfice de la vente de ses produits à des usagers qui ont intérêt à rester discrets.

La palme de l'hypocrisie, dans cette histoire, ne va toutefois pas à Apple. Elle revient plutôt à une certaine droite qui proclame que l'État a perdu toute légitimité pour agir, tout en soutenant que la branche de l'État la plus obscure et la moins redevable de ses actions devrait avoir carte blanche pour tenir ses citoyens à l'oeil.

Ottawa Citizen
Laser strikes on aircraft a growing threat to safety
Friday, 19 February 2016
Byline: Andrew Duffy

Ottawa - A Transport Canada database reveals that 33 laser strikes were reported by aircraft in the National Capital Region during the past year - part of an alarming trend that places pilots and their passengers at risk.
The latest incidents occurred in January when three planes were targeted in Ottawa's skies, including an Air Canada Jazz flight from New York City and a nighttime Ornge air ambulance flight.

The incidents are outlined in the federal government's Civil Aviation Daily Occurrence Reporting System (CADORS), which acts as the repository for all safety and security-related incidents in Canadian airspace.

Although Transport Canada tries to ensure the accuracy of the reports, it still considers them preliminary and "subject to change."

The number of laser strikes on aircraft has been rising sharply in recent years.

Last year, according to a Citizen analysis of the CADORS database, there were 663 laser strikes directed at aircraft in Canada - a 32 per cent increase from 2014. The numbers have been climbing since 2008 when 80 laser incidents were reported by pilots in Canadian airspace.

Capt. Dan Adamus, Canada board president for the Air Line Pilots Association, International, called laser attacks a serious concern. "When it happens, there's a big green glow - it's usually a green laser - that fills the cockpit," Adamus said. "You can be looking for the runway, and you catch this light out of the corner of your eye, and your natural tendency is to look towards it."

Two pilots in the United States, he said, have lost their medical clearance to fly after suffering eye damage from cockpit laser strikes.

In Canada, pointing a laser at an aircraft is an offence under the federal Aeronautics Act, and those convicted can face up to five years in prison and a $100,000 fine.

Adamus wants the federal government to make laser interference with an aircraft an offence under the Criminal Code, and launch the kind of public awareness campaign conducted by the F.B.I., which offered $10,000 for information that led to arrests.

"They have to get the word out," he said, "because nine times out of 10, I think it's curious people with a laser, saying, 'I wonder if this will reach that aircraft.' " Adamus also wants the government to better regulate the sale of lasers, and limit the power output of hand-held pointers - sometimes known as laser pens - to 5 milliwatts or less. More powerful devices should be tightly controlled, he said, and come with explicit warnings about the danger they pose. Transport Canada says it is working closely with police, other government departments and the aviation industry to reduce the number of laser incidents. The high-intensity light strikes are considered particularly dangerous during the takeoff and landing phases of a flight, when pilots can least afford to be distracted or temporarily blinded.

In the Ottawa region, medevac helicopters, small planes and commercial jets have all been targeted. Last April, an Ornge helicopter flying from Pembroke Regional Hospital to the Children's Hospital of Eastern Ontario reported being hit by a green laser coming from the vicinity of the Champlain Bridge.

One month later, the pilot of an Air Transat Airbus en route from Toronto to Venice said the plane's cabin was lit up by a green laser as it cruised at 31,000-feet over Ottawa. That same month, a WestJet Boeing 737, originating in Calgary, reported that it was targeted three times by a green laser as it approached Ottawa International Airport.

Ten of the local incidents reported last year involved members of the Ottawa Flying Club, one of whom was targeted by a green laser for a full 20 seconds.

Bryce Hanna, general manager of the club, said laser strikes pose "a fundamental safety issue" since many small aircraft have a single pilot on board. "There's no one to take the controls so potentially the aircraft could even be lost because of that," Hanna said.

Laser strikes are an international problem. This month, the Alitalia flight crew taking Pope Francis to Mexico reported a laser beam coming from the ground as the plane prepared to land in Mexico City. Days later, a Virgin Atlantic flight en route to New York from London turned back after laser light struck the eyes of the co-pilot.

The incident prompted the British Airline Pilots Association to demand that the government categorize powerful laser pointers as "offensive weapons" to aid in a police crackdown on their use against planes.

The Hindustan Times
Deloitte expands its Cyber Intelligence Centre in Gurgaon (Canada).
Friday, 19 February 2016

Kolkata - Deloitte India on Thursday announced the expansion of its Cyber Intelligence Centre (CIC) in Gurgaon. This facility integrates technology with industry insights to provide round-the-clock business-focused cyber and operational security.
Krishan Pal Gurjar, Minister of State for Social Justice Empowerment, Government of India, was the Chief Guest for the occasion. Other dignitaries at the inauguration ceremony included P.R. Ramesh, Chairman, N. Venkatram, CEO, Deloitte India along with the India board and Executive Committee members of Deloitte India firm.

With 24x7 coverage, the CIC has the capability to monitor and assess threats specific to clients, enabling Deloitte to effectively mitigate risk and strengthen cyber resilience. Deloittes Gurgaon CIC will be part of a globally interconnected set of cyber intelligence centres to provide leading insights and services to its clients. Speaking about CIC, Shree Parthasarathy, Partner, Deloitte India, said,

The pervasiveness of technology throughout major business processes coupled with the brand and regulatory impact of a cyber-breach or attack, clearly makes cyber risk a boardroom issue. With always-on, always-connected systems, exposure to cyber threat increases, creating the need for businesses to get access to timely and actionable threat intelligence.

Our CIC is one of the largest in the region and is linked to Deloittes existing Cyber Intelligence Centres in Australia, Japan, UK, Spain, Canada and the United States to bring a collective set of capabilities to our clients based in India.

The CIC propels our Cyber capability to the next level and helps solidify our presence in the market as a global leader in Cyber Risk Services. Said Amry Junaideen, President, Enterprise Risk Services, Deloitte India: Threats posed to organizations by Cybersecurity-related issues have increased rapidly. So many organizations have suffered significant brand impact, financial loss, and systems outages due to Cybersecurity issues.

With new attack potentials and insider threats on the rise, securing proprietary information and other critical business assets is becoming exponentially more difficult for Indian enterprises. As a rapidly growing market, India holds immense potential for Deloitte to make meaningful impact for our clients. We believe the CICpositions us well to address the cyber risk priorities of organizations in all industries with a full suite of business- focused security solutions, he added.

Jerusalem Post
Reports of IDF airstrikes against Syria cause waves in cyberspace
Friday, 19 February 2016
Byline: Noam Amir, Maariv Hashavua

Jerusalem - Foreign reports attributing strikes against the Syrian regime to the IDF may only rarely elicit a military response, such as a barrage of rockets, however they certainly result in a direct threat to Israel's security systems.
A military source confirmed this week that in some instances where Israel has been fingered for a particular military operation, such as the strike which killed notorious terrorist Samir Kuntar last year, an immediate reaction has been seen in cyberspace.

In the case of Kuntar, a day after his death a group of hackers carried out a successful attack on the Israel Air Force (IAF) website.

According to sources in Israel, a group of hackers operating from a long distance overseas and styling itself "Qalamoun boys" was behind the attack on the IAF site. While it may be true that the attack caused no damage to the army in any significant way, and the attackers were repelled quickly, it appears to the IDF that in a general sense hackers are often curious about circulating rumors of Israeli strikes, and look for ways to confirm or deny the reports by breaking into the IDF's systems.

According to the military source, there is no paucity of attacks against the Israeli military. "Enemies want to know what's going on here," he said. "At the end of the day, computers and information systems do hold secrets, but there is a very low probability of success of such an intrusion because the cyber capabilities of the IDF are very high."

In the world today there are five major cyber powers. Israel is one of them, the other four being the US, Iran, Germany and the UK. In the case of the alleged IAF attacks against Syria, the regime does not address the foreign reports at all. Instead, it will do anything within its power to keep the ambiguity regarding incidents such as these in place. However, under the radar, they hope that one of the world cyber powers will try to access the information.

Iran is of course one of these players, having carried out attacks of increasing quality and frequency in recent years, particularly between 2013-2014.

The significant decrease in cyber attacks in 2015 has been attributed, among other factors, to the nuclear agreement. During the tumultuous years of 2013 and 2014, the region was hot, with all sides attempting to extract information. However the signing of the agreement seemed to calm the flurry of attacks in both directions.

It is very possible that Wednesday night, with the publication of further reports of an attack on Syria, that there has been a raised alert in the preparedness of the IDF. Even if the army is not expecting to deal with a barrage of missiles, at least in cyberspace it will be bracing for combat, as there are those who will be looking for verification, making cyberspace one of the most fascinating areas of the world.

The military like to call this space "the most crowded playing field in the Middle East." Even without swings and sandboxes, cyberspace is equally as fascinating as the conventional threats faced by the IDF.

Washington Times
PLA on cyberwarfare buildup
Thursday, 18 February 2016
Byline: Bill Gertz

Washington - A Chinese military official revealed last month that Beijing plans to rapidly build a new People's Liberation Army cyberwarfare force in response to U.S. military cyberforces.
Col. Li Minghai of the PLA's National Defense University wrote in the Communist Party-affiliated Global Times newspaper that a new cyberwarfare force is needed to counter the United States as the Pentagon is building up its cyberattack capabilities.

"It is more necessary for us to build a brand new 'operation force,'" said Col. Li, identified as deputy director of the NDU's Center for Cyberspace Security.

As a sign of the sensitivity of the report, Chinese censors quickly removed the posting in Chinese from the Global Times website shortly after it appeared Jan. 21.

Col. Li is one of China's most senior cyberwarfare specialists, and his remarks provide some of the first clues to Beijing's military priorities in future cyberwarfare operations. Military cyberoperations are among China's most closely guarded secrets.

The 3rd Department of the PLA general staff, known as 3PLA, is China's main military cyberwarfare force and is said to have up to 100,000 cyberwarriors. A copy of the colonel's translated article was obtained by Inside the Ring.

Col. Li stated that the U.S. military's cybersecurity strategy for the past four years has emphasized offensive electronic attacks on information systems and regards China as "one of the greatest threats to the United States' cybersecurity."

Noting that current cyberthreats to China are "not sensational or alarmist talk," Col. Li said reforms to PLA cyberforces should not be limited to "tinkering," but require "the rebuilding of a new- breed cyberforce in our country."

"We should apply the brand-new development model in the information age to remold our cyberwarfare preparedness against the threat of the United States' new cyberstrategy and guarantee our nation's cybersecurity," he said.

A key feature will be what is described as a "winning mechanism" for warfare in the cyberspace domain.

"In the 21st century, seizing control of cyberspace is of decisive significance, like seizing control of the sea in the 19th century and seizing control of the air in the 20th century," Col. Li wrote. "Cyberoperations in the future will follow the new battlefield rules determined by the winning mechanisms of 'real-time sensing, sensitive response, source destruction and chain cutoff, joint winning.'"

Also, cyberpower must be combined with conventional military power "with winning being based on information power."

Cyberwarfare troops will target information technology infrastructure networks like the Internet, telecommunications systems and computer systems, including imbedded processors and controllers in major sectors.

A third priority for the cyberwarfare force will be adding more trained military hackers.

"At present, our country still lacks high-end specialists with both knowledge about network technology and knowledge about military command, so it is imperative that we step up the efforts for building the cyberoperation force," Col. Li concluded.

Publication of the report coincided with China's creation of a Strategic Support Force, announced Dec. 31, that will include dedicated cyberwarfare forces, along with space warfare units.

Cybersecurity expert Joe McReynolds disclosed last year that China's cyberwarfare forces were outlined for the first time in a Chinese military paper. The PLA cyberwar force has three elements, including a cadre of dedicated military specialists devoted to network warfare that conduct cyberattacks and defense, Mr. McReynolds told The Daily Beast.

Other forces include teams of specialists working in civilian intelligence, police and security organs who conduct military cyberoperations. Last are units outside government that will be mobilized for network warfare.

Press Trust of India
Government to ask Twitter to block accounts with Hafiz Links
Friday, 19 February 2016

New Delhi - Security agencies will approach Twitter India to block all accounts having links with Lashkar-e-Taiba founder Hafiz Saeed and Jamaat-ud-Dawa which are often found to be spreading venom against India.
There are several accounts which have links with LeT's front outfit, Jamaat-ud-Dawa, as well as terror mastermind Saeed and it has become necessary to shut these down as quickly as possible, officials said.

"We are approaching Twitter India which in turn will tell its US-based parent company to deactivate the accounts. Hopefully, it will be done soon," a official said.

Earlier, Twitter had blocked several accounts operated by Jamaat-ud-Dawa, headed by Saeed, following requests from security agencies in different countries, including India and the US. However, such accounts again cropped up after a gap of several months.

A fake account of Saeed had recently asked Pakistanis to support the JNU students who are protesting against the registration of a case of sedition against JNUSU president Kanhaiya Kumar. It had also asked users to trend the topic #PakStandWithJNU with the posts sparking a huge controversy.

Last Sunday, Home Minister Rajnath Singh had said the event organised at JNU to protest against the hanging of Parliament attack convict Afzal Guru had the backing of Saeed.

Even though the Home Ministry clarified that Singh's statement was based on inputs from different agencies, it was reportedly made in the wake of the posts on the fake Saeed Twitter account.

Gulf News
Tech giants support Apple in privacy fight
Friday, 19 February 2016
Byline: Staff Report

Dubai - Apple chief Tim Cook has picked a fight with the United States government and Silicon Valley is joining his side.
Apple Inc.'s chief executive officer took his stand after the Federal Bureau of Investigation won a court order to make Apple help investigators unlock an iPhone used by Syed Rizwan Farook, one of the shooters in a deadly December 2 attack in San Bernardino, California.

From Google Inc. to Facebook Inc., the industry's biggest names rallied around Cook after he vowed to resist the court order. Cook described the request as an "unprecedented step that threatens the security of our customers" and called for a public debate.

The escalation with the FBI, which has been pushing for access to mobile devices since Apple tightened its encryption in late 2014, galvanised the firm's US peers and forced them to choose between helping the government fight crime and protecting their customers' privacy. The decision in the Apple case could apply to the broader tech industry and it may spur requests from China and other nations that want similar abilities to access users' encrypted content.

Reform Government Surveillance, a group representing firms including Google, Facebook, Microsoft Corp. and Twitter Inc., have issued a statement reiterating that, while it's "extremely important" to deter crime and terrorism, no company should be required to build backdoors to their own technology.

National Security Agency whistleblower Edward Snowden has also backed Apple, tweeting that the company's stance was defending the rights of its customers.

"We're here to say to Apple, "We're going to back you all the way," ' said Electronic Frontier Foundation (EFF) chief Cindy Cohn outside a San Francisco store. When about two dozen privacy advocates stood shoulder to shoulder in front of the downtown San Francisco Apple store on Wednesday, it may have been the first time a demonstration was held in support of the tech company.

"Silicon Valley stands with Apple," Bret Taylor, co-founder of Quip and former chief technology officer of Facebook and co-creator of Google Maps, posted on Twitter. Steven Sinofsky, an ex-executive at Microsoft, called for "broad support from full stack of technology companies."

Khaleej Times

Re-strategising IT security

Friday, 19 February 2016

Byline: Aji Joseph

Dubai - Digital industrial espionage is becoming a greater threat for companies in all industries. An additional danger is presented by numerous secret services, with an aim of spying on businesses and organisations. What should companies, the potential victims, do? They must work harder than ever to protect themselves and their data from increasingly complex attacks in order to avoid the kind of corporate disadvantage, which might even threaten their very existence.

There are various forms of attack which have the declared aim of spying on business secrets. Malware is introduced into databases, applications and systems. Transmitted data is spied on and read at network connections. Trojans can make their way into companies with completely innocent software purchases. Software updates can also be used as a transmission vehicle for spying programs. If there are no proper defence mechanisms available, attackers can spy on business secrets as long as they like without the company noticing.

The attackers can usually leave the network in the same way as they got in - unnoticed by the victims. Annual losses to corporate espionage are estimated to be billions.

The EU published a report on industrial espionage as early as 2001. The list includes two suspected cases against France. These were in relation to the delivery of high-speed trains to South Korea. The French manufacturer Alstom (TGV) was said to have gained a competitive advantage over the competitor Siemens (ICE) by means of industrial espionage.

In 2013, France came under suspicion again. The New York Times reported on the country's alleged industrial espionage programme, which had the aim of obtaining technical secrets from the USA.

In 2015, the newspaper Libération reported that approximately one hundred French companies, including all companies listed in the French stock market index CAC 40, had been spied on. The report was based on information provided in US documents supplied by Wikileaks. The German Federal Intelligence Service (BND) was also in the headlines for several weeks. It has been accused of having helped the US secret service NSA to spy on European institutions and companies.

Although defence mechanisms such as signature-based anti-virus software, firewall and network monitoring software are still required, they are no longer sufficient.

Only a comprehensive shield can help in the face of the intensified threat. It must cover the entire company, include all the necessary IT security services, maintain an overview of all security incidents, be adaptable to new threat scenarios and detect unknown forms of attack.

Though today several IT experts and managers have the expertise and skills to manage cyber risk/ attacks; you need an intelligence-based approach - one that uses knowledge combined with tools - 24x7 to identify threats and protect your assets. In view of this and the high human resources and financial costs; companies have to consider whether they can operate on their own or they should use specialist expertise and tools.

To manage IT security more effectively and efficiently; it's time for organisations to refocus and re-strategize their overall IT security shield - to reduce time until risk is detected and therewith reduce potential damage of attacks.

Companies should consider outsourcing their IT security monitoring needs to highly specialised experts and therewith ensure their infrastructure is monitored every hour - seven days a week ensuring a more proactive approach in protecting their company assets. At the same time this should offer significant cash savings for a company in the long run such as a reduction of costs for purchasing and managing a vast number of complex stand-alone IT security solutions.

Bloomberg News
Secret Memo Details U.S.'s Broader Strategy to Crack Phones
Friday, 19 February 2016
Byline: Michael Riley, Jordan Robertson

Washington - Silicon Valley celebrated last fall when the White House revealed it would not seek legislation forcing technology makers to install "backdoors" in their software -- secret listening posts where investigators could pierce the veil of secrecy on users' encrypted data, from text messages to video chats. But while the companies may have thought that was the final word, in fact the government was working on a Plan B.
In a secret meeting convened by the White House around Thanksgiving, senior national security officials ordered agencies across the U.S. government to find ways to counter encryption software and gain access to the most heavily protected user data on the most secure consumer devices, including Apple Inc.'s iPhone, the marquee product of one of America's most valuable companies, according to two people familiar with the decision.

The approach was formalized in a confidential National Security Council "decision memo," tasking government agencies with developing encryption workarounds, estimating additional budgets and identifying laws that may need to be changed to counter what FBI Director James Comey calls the "going dark" problem: investigators being unable to access the contents of encrypted data stored on mobile devices or traveling across the Internet. Details of the memo reveal that, in private, the government was honing a sharper edge to its relationship with Silicon Valley alongside more public signs of rapprochement.

On Tuesday, the public got its first glimpse of what those efforts may look like when a federal judge ordered Apple to create a special tool for the FBI to bypass security protections on an iPhone 5c belonging to one of the shooters in the Dec. 2 terrorist attack in San Bernardino, California that killed 14 people. Apple Chief Executive Officer Tim Cook has vowed to fight the order, calling it a "chilling" demand that Apple "hack our own users and undermine decades of security advancements that protect our customers." The order was not a direct outcome of the memo but is in line with the broader government strategy.

White House spokesman Josh Earnest said Wednesday that the Federal Bureau of Investigation and Department of Justice have the Obama administration's "full" support in the matter. The government is "not asking Apple to redesign its product or to create a new backdoor to their products," but rather are seeking entry "to this one device," he said.

Security specialists say the case carries enormous consequences, for privacy and the competitiveness of U.S. businesses, and that the National Security Council directive, which has not been previously reported, shows that technology companies underestimated the resolve of the U.S. government to access encrypted data.

"My sense is that people have over-read what the White House has said on encryption," said Robert Knake, a senior fellow at the Council of Foreign Relations who formerly served as White House Director of Cybersecurity Policy. "They said they wouldn't seek to legislate 'backdoors' in these technologies. They didn't say they wouldn't try to access the data in other ways."

"Backdoors" refer to security holes that are intentionally inserted into software to create the equivalent of a skeleton key for law enforcement -- what wiretapping systems are for telephone lines, for instance. The problem with backdoors in computer networks is they create vulnerabilities for any hacker to find.

What the court is ordering Apple to do, security experts say, does not require the company to crack its own encryption, which the company says it cannot do in any case. Instead, the order requires Apple to create a piece of software that takes advantage of a capability that Apple alone possesses to modify the permanently installed "firmware" on iPhones and iPads, changing it so that investigators can try unlimited guesses at the terror suspect's PIN code with high-powered computers. Once investigators get the PIN, they get the data.

Knake said that the Justice Department's narrowly crafted request shows both that FBI technical experts possess a deep understanding of the way Apple's security systems work and that they have identified potential vulnerabilities that can provide access to data the company has previously said it can't get.

In this case, the government wants Apple's help in exploiting such weaknesses. But experts say they could find ways to do it themselves, and the NSC "decision memo" could lead to more money and legal authorization for a smorgasbord of similar workarounds.

National Security Council spokesman Mark Stroh declined to comment on the memo. But he provided a statement from a senior Obama administration official: "We should not preemptively conclude that technical and policy options to address this challenge are out of reach. While creating mechanisms for accessing encrypted information does create vulnerabilities, there may be technical and process steps that can be implemented to limit such risks."

The memo was approved by the NSC's Deputies Committee, according to the people familiar with it. While the deputies' committee changes depending on the subject matter, it typically includes at least a dozen sub-cabinet level officials, among them the deputy attorney general, the vice chairman of the joint chiefs of staff, and the deputy national security adviser.

Such memos can have lasting impact. A similar decision memo was used in the early years of the Iraq war to address the problem of Improvised Explosive Devices, which were then killing hundreds of U.S servicemen. The response ultimately led to new anti-IED technology and expanded intelligence capabilities to disrupt the cells building and planting the bombs.

Silicon Valley and Washington have had a decades-long distrust of each other over encryption, stemming from a failed Clinton administration push in the 1990s for a government backdoor in telecommunications networks. In that case, the National Security Agency developed a technology called the Clipper Chip, which the White House approved as a government standard. Security experts assailed it as insecure and a violation of privacy.

Security experts say the U.S.'s insistence on finding ways to tap into encrypted data comes in direct conflict with consumers' growing demands for privacy.

"The government's going to have to get over it," said Ken Silva, former technical director of the National Security Agency and currently a vice president at Ionic Security Inc., an Atlanta-based data security company. "We had this fight 20 years ago. While I respect the job they have to do and I know how hard the job is, the privacy of that information is very important to people."

In addition to the demands against Apple, the FBI will almost certainly seek more money and expanded legal authorization to track suspects and access encrypted data, without the involvement of companies that make the technologies, several experts say. Intelligence services already have sophisticated tools for cracking encryption, and the White House's efforts will likely lead to broader use of those techniques across the government, even in ordinary criminal investigations that don't involve foreign intelligence or national security.

The workarounds could involve trying to force companies like Apple to develop their own tools to help law enforcement or enlisting government hackers to find previously unknown software vulnerabilities that enable the decryption of large amounts of data flowing across networks.

Apple infuriated law enforcement when it announced in 2014 that it would encrypt data stored on users' iPhones and iPads with a PIN code that the company could not access, even if ordered to by a judge. Prior to that decision, the FBI and local police agencies routinely sent seized devices to Apple to extract data relevant to their investigations.

To security experts, creating hacking tools -- capabilities to gain access to encrypted data -- is simply a matter of money and focused effort.

"My guess is you could spend a few million dollars and get a capability against Android, spend a little more and get a capability against the iPhone. For under $10 million, you might have capabilities that will work across the board," said Jason Syversen, a former manager of advanced cyber security programs at the Defense Advanced Research Projects Agency (DARPA), and now the CEO and co-founder of Siege Technologies in Manchester, New Hampshire.

This week's federal court order undermines years of effort by Apple to design a system that makes accessing encrypted data impossible without the participation of the phone's legitimate user. Company officials appeared to believe the enhanced encryption would remove Apple from the efforts of any government to sabotage the security of their customers. Instead, federal agents have detailed in a public document several ways in which that encryption can be bypassed.

"Apple has two options now: They can go back to the judge and say this isn't possible. Or they can service the warrant," said James Lewis, a senior cyber security fellow at the Center for Strategic and International Studies in Washington. "I don't think they can say it's not possible, because it looks like it is."

New York Times
A Web Crime on the Rise: Hackers Lock Out Users and Demand a Ransom
Friday, 19 February 2016
Byline: Stacy Cowley, Liam Stack

New York - It sounds like the plot of a Hollywood thriller, but the all-too-real scenario played out this month at a large Los Angeles hospital: Hackers seized control of critical computer systems and the hospital paid a $17,000 ransom to release them.
So-called ransomware attacks have increased significantly in the past year, security experts say, and the hospital, Hollywood Presbyterian Medical Center, is not the first to fall victim.

The Titus Regional Medical Center, a small hospital in Mount Pleasant, Tex., experienced a similar attack last month, which knocked its core electronic medical record system offline. It, too, paid the ransom, according to Shannon Norfleet, a hospital spokeswoman.

Those in the security industry say such attacks are becoming more prevalent, but are rarely made public.

"We get over 100 calls and emails a month from different organizations that have had some form of ransomware impact their environment," said Charles Carmakal, who oversees breach investigations for clients of Mandiant, a consulting unit of the security firm FireEye. "Nobody talks to the media about it."

In a statement released Wednesday, Allen Stefanek, the president of Hollywood Presbyterian, described the two- week battle that his hospital fought to regain control of its data after a malware attack was detected on Feb. 5.

The attack did not disrupt medical care or compromise the personal information of employees or patients, he said. Instead, it blocked hospital employees from using email and other forms of electronic communication by using encryption to lock them out of the system.

Mr. Stefanek said hospital administrators were told that if they wanted to gain access to their network again, they would have to pay the attackers, who would then give them the decryption key. Mr. Stefanek said that the hospital had contacted the authorities when the malware attack was first detected.

"The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Mr. Stefanek said. "In the best interest of restoring normal operations, we did this."

Heath care providers are required to tell patients of any breaches that compromise their personal information or health data, but a typical ransomware attack would not fall into that category. The attackers do not need to gain access to the underlying data in order to encrypt it and prevent others from viewing it.

Once compromised, an organization has little choice but to pay up or say farewell to its data, according to Levi Gundert, who oversees information security strategy for Recorded Future, a threat analysis firm.

"There's really no workarounds for it," he said. "It's very frustrating for both law enforcement and the victims themselves."

Hollywood Presbyterian's attackers demanded their payment in the

form of 40 Bitcoins, a difficult-to-trace currency that has become the currency of choice for online criminals.

Ransomware attacks are on the rise, industry researchers say, because they work. A research team at Dell gathered data from one ransom-payment server and found that it collected $1.1 million in a six-month period. McAfee Labs, Intel's security research unit, detected 638,000 new ransomware variants in 2014. Last year, that number shot up to nearly 3.8 million.

Many ransomware attacks are random, and comparatively low-tech and blunt. Victims are most often infected by clicking a malicious link in an email or by malware delivered through a web browser, frequently hidden in advertisements. The average payment demanded is just $300, according to the security firm Symantec, a sum that is within reach for the individuals and small businesses that most often fall prey to these schemes.

But Mr. Carmakal said he was seeing a growing number of attackers targeting businesses and other organizations with deeper pockets. In those attacks, the hackers may go to greater lengths to remove data -- not just lock access to it -- and threaten to release it publicly if they are not paid.

"Automated malware doesn't know if an organization has $100,000 or not. A human knows," he said. "We've seen an uptick in those kinds of attacks over the past year. We've seen attackers ask for $10,000 to seven-figure values to delete the data" in their possession.

As ransomware attacks grow more frequent, they are increasingly hitting organizations that deal in public safety and other critical functions. Over the past year, the attacks have affected police departments and school districts across the country.

Health care organizations seem to be particularly vulnerable to hacking attacks because they have been slower to embrace sophisticated backup systems and other security measures than other industries, like financial services, said Katherine Keefe, the head of breach response services at Beazley, an insurance company.

Her team investigated 1,200 breaches last year, about half of them at health care providers. The rate of ransomware attacks has noticeably increased in the last six to eight months, she said.

"The criminals see that there's money to be made, and I think they believe they can hold organizations over a barrel," Ms. Keefe said.

The cost of an attack goes far beyond the usually modest sum demanded for ransom. It took Hollywood Presbyterian 10 days to restore its systems, Mr. Stefanek said.

Laura Eimiller, a spokeswoman for the Federal Bureau of Investigation in Los Angeles, said the agency had begun an inquiry into the attack, but she provided no further details.

USA Today
Apple faces uphill battle
Friday, 19 February 2016
Byline: Brad Heath

Washington - The U.S. Justice Department's demand that Apple help it break into a locked iPhone is the latest in a series of legal disputes with tech companies over users' privacy that has been going on for more than a decade.
Nearly all of those contests ended the same way.

"Historically, the judiciary has been very deferential to law enforcement," University of California-Hastings law professor Ahmed Ghappour said. "And history could be very indicative of how this will play out."

The latest episode began this week, when a federal magistrate judge in California ordered Apple to help FBI agents break into the locked iPhone used by Syed Rizwan Farook, one of the armed attackers in December's massacre in San Bernardino, Calif. Apple CEO Tim Cook said the company would fight the order, and Apple has refused to help unlock at least one other locked phone.

For tech companies, such battles have often not gone well.

In 2007, Yahoo balked at a secret order from the Foreign Intelligence Surveillance Court requiring it to turn over customer records to the NationalSecurity Agency. The company relented when a judge on the surveillance court threatened to impose a fine of $250,000 a day -- and double it every week. A federal appeals court upheld the surveillance court's order.

In 2013, a federal judge held the founder of Lavabit -- an email service that had been used by former NSA contractor Edward Snowden - - in contempt for not turning over the electronic key the company used to encrypt users' communications. Lavabit founder Ladar Levison eventually gave the key to the FBI but did so by printing it out in very small type.

Most such disputes have involved federal agents seeking access to troves of information tech companies keep about their users -- everything from contents of emails to records that can precisely track the location of someone's cellphone. The fight with Apple comes with one important difference.

Instead of asking the computer maker to turn over information, a federal magistrate ordered the company to create software for the FBI that would bypass some security features on newer versions of the iOS operating system. The order requires Apple to add an electronic signature to the new software, so Farouk's phone will recognize it.

"The fight here is that the software the government wants does not exist. They're trying to force engineers to write a special version of iOS, then sign it," said Christopher Soghoian, the American Civil Liberties Union's principal technologist. He said such an order raises the prospect that the FBI could force makers to push compromised versions of their software directly to users' phones and computers in a way that would be difficult to detect.

Apple has also rebuffed efforts to help agents unlock older versions of the iPhone, using tools it had already created for the job.

Last year in Brooklyn, federal prosecutors asked a magistrate to force Apple to unlock a phone running iOS 7, so they could use the phone's contents in a drug case. The company declined, even though it had "repeatedly assisted law enforcement officers in federal criminal cases by extracting data from passcode-locked iPhones pursuant to court orders," prosecutors said in a court filing.

Apple has argued that complying with the request would be burdensome. A judge has yet to decide whether to force Apple to comply.

Justice Department lawyers told a different federal judge in Brooklyn last year that the government has the ability to crack newer versions of the iPhone on its own. "The lack of a passcode is not fatal to the government's ability to obtain the records," Assistant U.S. Attorney Karen Koniuszy wrote in a court filing.

Wall Street Journal
Apple Standoff Escalates Local Cases
Friday, 19 February 2016
Byline: Nicole Hong. Pervaiz Shallwani

New York - State and local law-enforcement authorities are looking to follow the lead of the Federal Bureau of Investigation in its standoff with Apple Inc. over access to the contents of a terror suspect's smartphone.
Earlier this week, a federal magistrate judge in California ordered Apple to help the government unlock a passcode on the phone used by one of the suspects in the attack last year in San Bernardino, Calif., which killed 14 people. Apple has said it would fight the judge's order.

On Thursday, Manhattan District Attorney Cyrus Vance said his office is in the process of determining which cases involving encrypted smartphones they should bring before a New York state judge for a similar review.

Mr. Vance called the Apple case "the most visible example of how Silicon Valley's decisions are thwarting criminal investigations and impeding public safety." Other district attorneys may be following Mr. Vance's moves.

Jake Wark, a spokesman for the Suffolk County district attorney's office in Boston, said that although the office hasn't yet taken steps to bring a specific case for judicial review, "We can't rule that out. It may be a question of finding the right case."

The fight between Washington and Silicon Valley is exposing law enforcement's long-simmering concerns over the challenges posed by encryption during investigations. Federal and local law-enforcement officials are increasingly voicing frustration with encrypted smartphones, which they say provide a haven for criminals and hinder investigations by keeping potentially valuable evidence out of reach.

The battle over encrypted smartphones is part of a broader debate that dates back over a decade. Following the attacks on Sept. 11, 2001, Congress won broad support to pass the USA Patriot Act, which became the legal underpinning for roving wiretaps on terrorism suspects and bulk collection of phone records by the NationalSecurity Agency.

Over time, however, concerns about privacy and civil liberties escalated, reaching an apex following the 2013 disclosures of government surveillance by former national-security contractor Edward Snowden. Last June, Congress approved a new bill called the USA Freedom Act, which curbed the government's spying powers and reined in the NSA's bulk collection.

Moves by the telecom industry to address privacy concerns, especially the creation of stronger encryption on devices, have sparked outrage from law enforcement.

"There is not an investigation today at the local, state or federal level that doesn't touch a cyber platform," said Don Mihalek, who represents Secret Service members in the Federal Law Enforcement Officers Association. "Encryption has made it impossible now for law enforcement to do their jobs."

Apple's defiance, meanwhile, is garnering support from privacy advocates who say complying with the order could hurt the personal privacy of Americans and make smartphone users more vulnerable to hacks.

"This case is not about that one phone," said Alex Abdo, a staff attorney at the American Civil Liberties Union. "This case is about the government trying to establish an illegal precedent that it can force a U.S. company to hack its users' devices."

Supporters of Apple have said that giving the government even limited access to encrypted iPhones and similar devices will just spur criminals to communicate on other encrypted platforms.

Federal Bureau of Investigation Director James Comey has said that terrorists made a more concerted effort after the Snowden revelations to shield their communications on encrypted devices.

Since September 2014, when Apple began encrypting its new phones by default, approximately 25% of the 670 Apple devices (with the iOS 8 operating system or higher) examined by the Manhattan district attorney office's cybercrime lab were encrypted and not accessible, Mr. Vance said Thursday.

In a recent speech, Mr. Comey said encryption hindered the investigation into the attack last May of people at an exhibit featuring cartoons of the Prophet Muhammad in Garland, Texas, where the two shooters were both killed after they opened fire.

The morning of the attack, one of the shooters exchanged 109 messages with a known terrorist overseas using an encrypted mobile messaging app, Mr. Comey said. The terrorist group Islamic State has claimed responsibility for the Texas shooting.

"All the judicial orders in the world are not going to tell us what they said that morning," Mr. Comey said.

Although encryption in terrorism investigations has gained the most attention, officials say the issue now has a nexus to all sorts of crimes, including drug trafficking, kidnappings and child pornography. In New York, officials are struggling to access an encrypted iPhone 5 used by an associate during a shooting in the Bronx two weeks ago that injured two police officers. New York Police Department Commissioner William Bratton said Thursday that the encrypted iPhone was "impeding" the case from going forward.

Mr. Bratton said fixing the issue is going to require more significant rulings by the courts, including likely the Supreme Court, and legislation from Congress and state legislatures. He said both sides were early on in the process.

"The Constitution guarantees no absolute right to privacy," Mr. Bratton said. "It guards against unreasonable search and seizure. How is what we are talking at all unreasonable?"

Local law enforcement in Louisiana say an encrypted smartphone may be the last lead for solving the murder of Brittany Mills, a 28-year-old who was shot to death last April. In a typical investigation with an encrypted phone, investigators either try to ask the iPhone user to give up the passcode or search for any data in the user's cloud, according to Hillar Moore, the district attorney in Baton Rouge, La. Neither option was available in Ms. Mills's case.

"The frustrating part about this is the bad guys know that no one can get in beyond search warrants," Mr. Moore said. "They brag that cops can't touch their phones. They're using the phone as a shield to allow them to deal drugs, traffic women and threaten national security."

Wall Street Journal
How Using The 'Cloud' Undercuts Encryption
Friday, 19 February 2016
Byline: Jack Nicas

New York - While the increasing use of encryption helps smartphone users protect their data, another sometime related technology, cloud computing, can undermine those protections.

The reason: encryption can keep certain smartphone data outside the reach of law enforcement. But once the data is uploaded to companies' computers connected to the Internet -- referred to as "the cloud" -- it may be available to authorities with court orders.

Major cloud-computing suppliers, including smartphone providers such as Alphabet Inc.'s Google, Microsoft Corp. and Apple Inc., routinely comply with court orders and search warrants to turn over data that in many cases would have been harder for law enforcement to obtain had users kept it solely on their devices.

"The safest place to keep your data is on a device that you have next to you," said Marc Rotenberg, head of the Electronic Privacy Information Center. "You take a bit of a risk when you back up your device. Once you do that it's on another server."

Encryption and cloud computing "are two competing trends," Mr. Rotenberg said. "The movement to the cloud has created new privacy risks for users and businesses. Encryption does offer the possibility of restoring those safeguards, but it has to be very strong and it has to be under the control of the user."

Apple is fighting a government request that it help the Federal Bureau of Investigation unlock the iPhone of Syed Rizwan Farook, the shooter in the December terrorist attack in San Bernardino, Calif.

The FBI believes the phone could contain photos, videos and records of text messages that Mr. Farook generated in the final weeks of his life.

The data produced before then? Apple already provided it to investigators, under a court search warrant. Mr. Farook last backed up his phone to Apple's cloud service, iCloud, on Oct. 19.

Encryption scrambles data to make it unreadable until accessed with the help of a unique key. The most recent iPhones and Android phones come encrypted by default, with a user's passcode activating the unique encryption key stored on the device itself. That means a user's contacts, photos, videos, calendars, notes and, in some cases, text messages are protected from anyone who doesn't have the phone's passcode. The list includes hackers, law enforcement and even the companies that make the phones' software: Apple and Google.

However, Apple and Google software prompt users to back up their devices on the cloud. Doing so puts that data on the companies' servers, where it is more accessible to law enforcement with court orders.

Apple says it encrypts data stored on its servers, though it holds the encryption key. The exception is so-called iCloud Keychain data that stores users' passwords and credit-card information; Apple says it can't access or read that data.

Officials appear to be asking for user data more often. Google said that it received nearly 35,000 government requests for data in 2014 and that it complies with the requests in about 65% of cases.

Apple's data doesn't allow for a similar comparison since the company reported the number of requests from U.S. authorities in ranges in 2013.

Whether they back up their smartphones to the cloud, most users generate an enormous amount of data that is stored outside their devices, and thus more accessible.

New York Times
For Apple's C.E.O., a Journey to Bulwark for Digital Privacy
Friday, 19 February 2016
Byline: Katie Benner, Nicole Perlroth

San Francisco - Letters from around the globe began pouring into the inbox of Timothy D. Cook not long after the publication of the first revelations from Edward J. Snowden about mass government surveillance
Do you know how much privacy means to us? they asked Apple's chief executive. Do you understand?

Mr. Cook did. He was proud that Apple sold physical products -- phones, tablets and laptops -- and did not traffic in the intimate, digital details of its customers' lives.

That stance crystallized on Tuesday when Mr. Cook huddled for hours with lawyers and others at Apple's headquarters to figure out how to respond to a federal court order requiring the company to let the United States government break into the iPhone of one of the gunmen in a San Bernardino, Calif., mass shooting. Late Tuesday, Mr. Cook took the fight public with a letter to customers that he personally signed.

"We feel we must speak up in the face of what we see as an overreach by the U.S. government," wrote Mr. Cook, 55. "Ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect."

Mr. Cook's standoff with law enforcement officials is indicative of his personal evolution from a behind-the-scenes operator at Apple to one of the world's most outspoken corporate executives. During that time, he has moved a once secretive Silicon Valley company into the center of highly charged social and legal issues. While Mr. Cook's predecessor, Apple co-founder Steven P. Jobs, was considered a business icon, he never took aggressive positions on such matters as Mr. Cook now has.

Being at loggerheads with the United States government is risky for Apple and may draw a torrent of public criticism of the world's most valuable company at a time when its growth rate has significantly decelerated.

Yet people who know Mr. Cook said he did not believe he had a choice but to be vocal. Mr. Cook, who became Apple's chief executive in 2011, has long said that businesses and their leaders should think of

themselves as important members of civic society. In September, he emphasized that this responsibility "has grown markedly in the last couple of decades or so as government has found it more difficult to move forward."

Mr. Cook "says what he believes, especially in difficult situations," said Don Logan, the former chairman of Time Warner Cable who has been friends with Mr. Cook since he became chief executive of Apple, bonding over their shared alma mater, Auburn University. Of Mr. Cook's opposition to the court order, Mr. Logan said: "Tim is currently dealing with a very difficult situation and he knows the decision he has made has lots of ramifications, good or bad. But he wants to do the right thing."

Apple declined to make Mr. Cook available for an interview. The company is preparing to file an opposition brief against the court order.

Mr. Cook's ideas about civic duty were partly formed during his childhood in rural Alabama. In a speech at the United Nations in 2013, he recounted how Ku Klux Klansmen had once burned a cross on the lawn of a black family's home and how he yelled for them to stop. "This image was permanently imprinted in my brain, and it would change my life forever," he said.

At Apple, which he joined as a senior executive in 1998, Mr. Cook was a quiet figure for much of the period when he worked for Mr. Jobs, a showman who prized secrecy at the company. After Mr. Jobs stepped down because of ailing health, Mr. Cook began making Apple more open, publishing an annual report on suppliers and working conditions for more than a million factory workers.

In 2014, Mr. Cook revealed he was gay, a move widely seen as making a statement about gay rights. Last year, he wrote an editorial decrying religious freedom laws that had been proposed in more than two dozen states that would let people skirt anti-discrimination laws that conflicted with their religious beliefs.

His outspokenness has drawn criticism, with some investors questioning how nonbusiness initiatives -- including some of Apple's environmental moves -- would contribute to the company's bottom line. Mr. Cook responded at a shareholder meeting that it is important for Apple to do things "because they're just and right."

Privacy has long been a priority for Mr. Cook. At a tech conference in 2010, he said Apple "has always had a very different view of privacy than some of our colleagues in the Valley." He cited the iPhone's feature that shows where a phone -- and presumably its user -- is and said fears about abuse and stalking had compelled the company to let consumers decide whether or not their apps could use their location data.

Mr. Cook's views on privacy hardened over time as customers globally began entrusting more personal data to Apple's iPhones. At the same time, Apple was growing tired of requests from government officials worldwide asking the company to unlock smartphones.

Each data-extraction request was carefully vetted by Apple's lawyers. Of those deemed legitimate, Apple in recent years required that law enforcement officials physically travel with the gadget to the company's headquarters, where a trusted Apple engineer would work on the phones inside Faraday bags, which block wireless signals, during the process of data extraction.

Processing these requests was extremely tedious. More worrisome, the data stored on its customers iPhones was growing more personal, including photos, messages and bank, health and travel data.

And some government officials were not exactly instilling confidence in Apple's engineers. In one case, after law enforcement officials rushed a phone to Apple's headquarters for data extraction, the engineers discovered their target had not enabled the device's passcode feature.

So Mr. Cook and other Apple executives resolved not only to lock up customer data, but to do so in a way that would put the keys squarely in the hands of the customer, not the company. By the time Apple rolled out a new mobile operating system, iOS7, in September 2013, the company was encrypting all third-party data stored on customers' phones by default.

"People have a basic right to privacy," Mr. Cook has said.

By then, Mr. Snowden's disclosures about how the NationalSecurity Agency had cozied up to some tech companies and hacked others to gain user data were reverberating worldwide. The disclosures included revelations of a comprehensive, decade-long Central Intelligence Agency program to compromise Apple's products; C.I.A. analysts tampered with the products so the government could collect app makers' data. In other cases, the agency was embedding spy tools in Apple's hardware, and even modifying an Apple software update that allowed government analysts to record every keystroke.

Letters from alarmed Apple customers started flooding into Mr. Cook's inbox, fortifying his stance on privacy. Apple's eighth mobile operating system, iOS8, which rolled out in September 2014, made it basically impossible for the company's engineers to extract any data from mobile phones and tablets.

For officials at the world's law enforcement agencies, the new software was a clear signal that Apple was growing defiant. A month after iOS8's release, James Comey, the director of the F.B.I., told an audience at the Brookings Institution that Apple had gone "too far" with the expanded encryption, arguing that the operating system effectively sealed off any chance of tracking kidnappers, terrorists and criminals.

Government agencies began to press Apple and other tech companies for so-called back doors that could bypass strong security measures. With tensions rising, some form of technical compromise -- whether in the form of a chip, a back door or a key -- was off the table by 2015.

At Apple, Mr. Cook and others continued to work with investigators to the extent the company could and complied with court orders. Last October, a federal judge in New York said the government was overstepping its boundaries by using a centuries-old law, the All Writs Act, as the basis for its request that Apple open an iPhone for a drug investigation. Apple's lawyer sided with the judge in the case. The matter has not been resolved.

After December's San Bernardino attack, Apple worked with the F.B.I. to gather data that had been backed up to the cloud from a work iPhone issued to one of the assailants, according to court filings. When investigators also wanted unspecified information on the phone that had not been backed up, the judge this week granted the order requiring Apple to create a special tool to help investigators more easily crack the phone's passcode and get into the device.

Apple had asked the F.B.I. to issue its application for the tool under seal. But the government made it public, prompting Mr. Cook to go into bunker mode to draft a response, according to people privy to the discussions, who spoke on condition of anonymity. The result was the letter that Mr. Cook signed on Tuesday, where he argued that it set a "dangerous precedent" for a company to be forced to build tools for the government that weaken security.

"Compromising the security of our personal information can ultimately put our personal safety at risk," he wrote. "That is why encryption has become so important to all of us."

Far from backing down from the fight, Mr. Cook has told colleagues that he still stands by the company's longstanding plans to encrypt everything stored on Apple's myriad devices, services and in the cloud, where the bulk of data is still stored unencrypted.

"If you place any value on civil liberties, you don't do what law enforcement is asking," Mr. Cook has said.

Wall Street Journal
Apple Has More Leeway Than Carriers
Friday, 19 February 2016
Byline: Ryan Knutson

Washington - For U.S. phone companies like AT&T Inc. and Verizon Communications Inc., the notion of resisting a court order like Apple Inc. Chief Executive Tim Cook recently did is probably inconceivable. The reason is legal.

In 1994, Congress passed the Communications Assistance for Law Enforcement Act, which required that carriers build surveillance capability into their networks. That law was later expanded to cover voice calls placed over the Internet, but not all Internet communication. Other attempts to further expand the law to cover technology companies such as Apple have failed.

Mr. Cook earlier this week said Apple would oppose a federal judge's order to help the Justice Department unlock a phone used by a gunman in the San Bernardino attack, which killed 14 people last December.

These days, the nation's telecom carriers receive thousands of information requests from the government and law enforcement in both national security, and civil and criminal matters.

In the last six months of 2015, Verizon and AT&T combined received more than a quarter-million requests from law- enforcement agencies in civil and criminal matters and as many as 998 requests in the first six months of 2015 to access customer accounts for national-security reasons, according to transparency reports published by the companies.

By comparison, Apple says it received 971 law-enforcement requests for account data stored in users' iCloud or iTunes accounts. In the first half of 2015, the latest data available, and provided at least some data to 81% of them. As many as 499 additional requests were related to national security, according to Apple's transparency report.

With much communications traffic shifting from the phone networks to data packets on the Internet, monitoring is becoming more complicated.

"Back in the day, it was AT&T -- they had everything, so you just talked to AT&T," said Michael Sussmann, a former Justice Department official who is now a partner at Perkins Coie LLP.

AT&T CEO Randall Stephenson on Thursday reiterated comments he made last month that Congress should determine whether law enforcement should have the ability to access encrypted data on cellphones.

Congress "should decide the proper balance between public safety and personal privacy," Mr. Stephenson said in an emailed statement. "The rapid pace of technological innovation is challenging laws crafted in a very different era for totally different, and much less complex situations. Recent developments, in particular, bring home the need for legal clarity."

Senate Intelligence Committee Chairman Richard Burr (R., N.C.) has decided against a proposal circulating quietly on Capitol Hill to create criminal penalties for companies that decline to comply with court orders to decipher encrypted communications, a spokeswoman said Thursday night.

San Bernardino shooter Syed Rizwan Farook was provided a phone by his employer, which was allegedly subscribed to Verizon, according to government's legal filings. Verizon declined to comment on Mr. Farook's phone.

But the information that Verizon would be able to provide would only be records of phone and text messages placed over its network. The carrier can't provide access to vast amounts of other data, such as message content or calls made over mobile apps like WhatsApp, Skype or the blue iMessages sent between two iPhones.

Phone carriers can see when data is traveling over their networks on a service like WhatsApp or Facebook, but they can't see the content, experts say. That includes the "metadata," such as the time a message is sent, or who it is sent to.

The government and law-enforcement agencies can ask phone and Internet companies to turn over any customer information they possess, such as Facebook for messages retained on their services, and increasingly the government is asking tech companies to do so. But there is no requirement for phone companies or Internet firms as to how long the content of such data is to be stored. The requirement on phone companies is that the government has the ability to intercept traffic in real time.

Apple says it can provide customer data stored in its iCloud service, such as phone backups that can include stored photos, email, documents, contacts, calendars, and bookmarks. In the San Bernardino case, Apple has provided such data for Mr. Farook until Oct. 19, the last time his phone synced to his iCloud. That means there 44 days of data -- such as iMessages and FaceTime calls -- that may only exist on his locked iPhone.

Los Angeles Times
Battle lines drawn over encryption
Friday, 19 February 2016
Byline: Paresh Dave, Tracey Lien

Los Angeles - As hackers prove time and again that they can and will invade our digital lives, Apple Inc. has strengthened its security system to make its services nearly impossible to penetrate -- even for top cops.
Those seemingly airtight protections are great for the company's millions of customers, and rival device makers have rushed to emulate Apple. But as tech companies build virtual fortresses, authorities are mounting a battle to make sure the tech industry doesn't completely shut them out -- as it contends Apple has done by making its iPhone impossible for the FBI to crack.

At the heart of the issue is encryption, a way to secure a digital file by scrambling its contents so that it can be read only by someone who has the key. Tech firms are increasingly encrypting their software, and Apple has been at the forefront.

But sealing off the personal information of customers extends to everyone -- the good guys and the bad guys. That's uncharted territory for tech companies, government agencies and consumers, leaving everyone struggling to figure out how far, exactly, encryption protections should extend.

"We need privacy and security, and frankly Apple has done a better job than most," said Mark Mollineaux Pollitt, adjunct professor at Syracuse University and former director of the FBI's Regional Computer Forensic Laboratory Program. "We shouldn't punish them for doing that. We should find a way to broaden that and make that more effective, but we have to realize there are instances where we have to breach that security to protect all of us."

But not everyone sees it as a gray area, where exceptions can be made for extreme cases like terrorism or child pornography.

This week, Apple Chief Executive Tim Cook took a defiant stance, saying his company would fight a court order in the San Bernardino terror investigation that asks the company to develop, for the first time, software that would allow authorities to circumvent the passcode on the encrypted phone.

Apple's decision isn't without critics, who say courts should be the arbiter of where the line is drawn.

"Apple is obstructing the course of law enforcement and effectively aiding terrorists," said Vivek Wadhwa, a corporate governance fellow at Stanford University. "They changed the technology, so they have to keep up with the ability to unlock the device if the government asks them do it. That's not unreasonable."

As it is, the FBI is publicly admitting that it is locked out, said Jeff Kelley, an iOS developer at software firm Detroit Labs who builds apps for iPhones, iPods, iPads and Mac OS.

"If you're Apple, you couldn't ask for a better ad for iPhone encryption."

That's a nightmare for the FBI.

The agency wants to retrieve whatever resides on the iPhone 5c of Syed Rizwan Farook, one of the two slain shooters who killed 14 people in the Dec. 2 attack.

But the smartphone's iOS operating system is locked by a numeric passcode, likely four digits long. The FBI potentially has only 10 guesses before the phone's contents self-destruct.

Older versions of the operating system provided ways for Apple and even law enforcement to access at least some contents on the phone, even if it was password-protected. For example, older iPhone models were susceptible to unlimited password guessing. In other cases, Apple held a master key, and authorities could ship the company an iPhone and get a DVD or hard drive back with the data from it.

But Apple, in effect, threw away its master key when it deployed a new version of iOS in 2014. Farook's phone runs one of the newer iOS versions.

Adding to the FBI's problems is that Apple is judge, jury and executioner when deciding what software runs on an iPhone: An app or program won't work without a special signature from Apple.

The set-up is aimed at stopping viruses or malware from infecting iPhones, and it also gives Apple latitude to ban apps it doesn't want to support, including for competitive or cultural reasons.

That's significantly more control than Google exercises over smartphones running its open-source Android operating system. Many Android phones support so-called unsigned programs, providing one of the key doors through which law enforcement has been able to extract data from locked phones.

About 80% of the world's smartphones run Android, and about 15% run iOS, according to various estimates.

In general, hardware makers have been making stricter security settings a default on their devices. But while those measures and more have deflected thieves, they left room for law enforcement to acquire data when needed.

Not so with Apple. Besides encryption, the company in 2013 introduced Touch ID, a fingerprint scanner that allows users to unlock their phones by pressing their fingers on the device's home button.

This week's court order requires the FBI and Apple to work in tandem to develop a tool that preserves the data on Farook's phone while allowing an app devised by the FBI to input an unlimited number of passcodes until it guesses the right one.

"That has never before been seen," said Kevin Bocek, vice president of threat intelligence and security strategy at cybersecurity company Venafi. "Apple has very aggressively maintained security, and this is the way the government is going to get around it."

Generating the new software for the FBI wouldn't be trivial, but it's certainly doable, experts said.

Apple would need to make the special code run on the iPhone's short-term memory to ensure it doesn't tamper photos, text messages and other potentially critical evidence, said Dan Guido, chief executive of security start-up Trail of Bits.

The code would get rid of the barriers that normally arise when someone tries too many times to guess a user's passcode. Last, it would have to include a funnel for automated guessing, freeing the FBI from manually entering potentially tens of thousands of numeric combinations.

Even though it's technically capable of carrying out the FBI's orders, Apple and its supporters reject the notion that this would be a one-time thing.

Jonathan Zdziarski, one of the top experts on iPhone security, said the work doesn't end there. If Apple ends up creating a tool, it would need to be tested, including by outside forensic specialists, to stand up to legal scrutiny if evidence retrieved from the phone is ever used in court. That vetting process could drag on for months and risks exposing the tool to people with malicious intent.

There's fear that once a safe-cracking tool is developed, law enforcement agencies from all over the world will repeatedly request its use.

"They've brought a phone that would be easy to justify developing a tool for -- a terrorist's -- but it will be much easier for a court to compel Apple to use it in the future once it's out there," Zdziarski said.

Apple could update iOS to stop the tool developed for Farook's iPhone from working on other ones by requiring consumer consent to run it, but the precedent of making it is irreversible, technologists say.

"You can rationalize it, these are known bad people, this is a known domestic terrorism case and it's one iPhone," said Oren Falkowitz, chief executive of security firm Area 1 Security and a former director of technology and data science programs at U.S. Cyber Command. "But it has implications for all technologies across the globe. We have to be doing more to strengthen the security of the Internet ... or we'll suffer consequences, ... greater than whatever information might be on this one phone."

New York Times
Apple's Strong Stand on Encryption
Friday, 19 February 2016
Byline: Editorial Board

Editorial - It is understandable that federal investigators want to unlock an iPhone used by one of the attackers who killed 14 people in San Bernardino, Calif., in December. And it's understandable that the government would turn to Apple for help. But Apple is doing the right thing in challenging the federal court ruling requiring that it comply.
In an order issued on Tuesday, Magistrate Judge Sheri Pym says Apple must create new software that would bypass security features on the iPhone used by the terrorist, Syed Rizwan Farook. That would allow the Federal Bureau of Investigation to unlock the device and retrieve the pictures, messages and other data on it. Her ruling was based on the All Writs Act of 1789, which is used to require people or businesses not involved in a case to execute court orders. Another federal magistrate judge in New York is considering a similar request to unlock an iPhone in a narcotics case.

Law enforcement agencies have a legitimate need for evidence, which is all the more pressing in terrorism cases. But the Constitution and the nation's laws limit how investigators and prosecutors can collect evidence. In a 1977 case involving the New York Telephone Company, the Supreme Court said the government could not compel a third party that is not involved in a crime to assist law enforcement

if doing so would place "unreasonable burdens" on it. Judge Pym's order requiring Apple to create software to subvert the security features of an iPhone places just such a burden on the company.

Apple has already given the F.B.I. data from the phone that was backed up and stored on its iCloud service; the last backup was made about a month before the attacks. But the company's chief executive, Timothy Cook, has said that requiring it to create software to bypass a feature that causes the phone to erase its data if 10 incorrect passwords are entered would set a dangerous precedent and could undermine the security of its devices. The Department of Justice has argued that the software would be used on that phone only and notes that Apple has previously helped law enforcement unlock phones. The company changed how it encrypts phones after the surveillance revelations by Edward Snowden.

But writing new code would have an effect beyond unlocking one phone. If Apple is required to help the F.B.I. in this case, courts could require it to use this software in future investigations or order it to create new software to fit new needs. It is also theoretically possible that hackers could steal the software from the company's servers.-

There are certainly other ways for law enforcement agencies to collect evidence. They already have the power to get data stored on online services like iCloud and Google's Gmail through search warrants. And they can get records of phone calls and text messages from companies like Verizon and AT&T. A recent study published by Harvard's Berkman Center for Internet and Society concluded that the proliferation of Internet-connected sensors, cameras and other devices provides the government ever-expanding opportunities to collect information about people.

Even if the government prevails in forcing Apple to help, that will hardly be the end of the story. Experts widely believe that technology companies will eventually build devices that cannot be unlocked by company engineers and programmers without the permission of users. Newer smartphones already have much stronger security features than the iPhone 5c Mr. Farook used.

Some officials have proposed that phone and computer makers be required to maintain access or a "back door" to encrypted data on electronic devices. In October, the Obama administration said it would not seek such legislation, but the next president could have a different position.

Congress would do great harm by requiring such back doors. Criminals and domestic and foreign intelligence agencies could exploit such features to conduct mass surveillance and steal national and trade secrets. There's a very good chance that such a law, intended to ease the job of law enforcement, would make private citizens, businesses and the government itself far less secure.

Wall Street Journal
U.S. Clash With Apple Was Months in Making
Friday, 19 February 2016
Byline: Devlin Barrett, Daisuke Wakabayashi

Washington - At a congressional hearing on Feb. 9, Federal Bureau of Investigation Director James Comey discussed obstacles of prying open electronic devices such as smartphones, zeroing in on a case in point: the San Bernardino, Calif., terrorist attack.
"We still have one of those killers' phones that we have not been able to open," he said. "It's been over two months now, and we're still working on it."

Although few realized it at the time, Mr. Comey's comments were a shot across the bow of Apple Inc. The company had been refusing for weeks to help the FBI unlock the phone used by Syed Rizwan Farook, one of the perpetrators of the attack, according to people familiar with matter.

Justice Department officials had even considered filing court papers against Apple a month earlier, only to hold off in the hope of gaining more cooperation.

The standoff, a precedent-setting case on privacy and security in the digital age, culminated this week when a judge ordered Apple to help the FBI circumvent passcode protection on the phone and Apple said it would fight the order. That set the stage for a possible landmark decision on the relationship between government and technology companies. The industry has steadfastly resisted the government's demands for help in unlocking encrypted communications.

It is a legal battle that holds risks for both sides. State and local law-enforcement authorities are already looking to follow the lead of the FBI in its face-off with Apple. On Thursday, Manhattan District Attorney Cyrus Vance said his office is in the process of determining which cases involving encrypted smartphones it should bring before a New York state judge for a similar review.

The legal fight between the Justice Department and Apple over encryption had been building for months. When Mr. Farook and his wife walked into a holiday party for his co-workers on Dec. 2 and began firing -- killing 14 people and injuring 22 -- the government and technology companies had already been feuding publicly and privately over how encryption puts some data beyond the reach of criminal investigators.

In a meeting more than a year ago, the No. 2 Justice Department official told Apple that some day there would be a crucial case involving a locked phone and a missing or murdered child. It would be better for Apple to help on encryption issues before such a case, rather than after, then-deputy attorney general James Cole told an Apple lawyer.

While a terror attack is a different scenario, several federal law-enforcement officials said this week the San Bernardino case was just the kind of thing they had warned about.

Apple executives believed they had worked extensively with law enforcement on the San Bernardino matter. The government's legal documents note that Apple had turned over phone information that Mr. Farook backed up on its iCloud service through mid- October, a month and a half before the attack.

Apple CEO Tim Cook and his colleagues viewed the government's request to create software to get around its own security as a step too far. Apple feels very strongly about two tenets -- data must be encrypted, and its software can't have any "back doors" allowing government access -- Mr. Cook said last year at The Wall Street Journal's technology conference.

Apple's position dovetails with its business interests. It has used its vocal stance on privacy to distinguish itself from rivals that make money on ads targeted at users based on their online data.

And two-thirds of Apple's business comes from outside the U.S., where sentiment about government surveillance is different. Europeans, for example, value privacy highly, and have expressed growing concerns about the control U.S. tech companies exercise over personal data. Government access to user data is also a concern in countries with authoritarian governments.

In the San Bernardino case, a search turned up Mr. Farook's work iPhone. It was owned by San Bernardino County, but the county didn't know the passcode. FBI agents worked to retrieve data on it, including data backed up to cloud storage.

But Mr. Farook had apparently turned off his cloud-storage backup function about Oct. 19, suggesting there still was information on the phone. The FBI and Apple discussed the issue in December without reaching an agreement on how Apple might help open the phone.

Justice Department lawyers prepared in early January to file court papers seeking to force Apple to help, said people familiar with the matter. Some officials weren't optimistic but felt it was worth sending a warning.

At the last minute, prosecutors decided there was a technical question to resolve with Apple, so the two sides kept talking. The technical issue took a few more weeks to sort out. Then the federal government told Apple again it was planning to file court papers to force the company to cooperate.

Privately, government officials hoped Mr. Comey's allusion to the San Bernardino phone before Congress on Feb. 9 would send a signal to Apple that the Justice Department would soon go public with its concerns about the case and the broader issue of encrypted phones.

Percolating in the background was a case with similar issues: In Brooklyn, a federal magistrate judge had asked Apple in late 2015 if there were legal grounds to reject a prosecutor's request for a similar order concerning a drug suspect.

Apple lawyer Marc Zwillinger wrote to Magistrate Judge James Orenstein saying, "Apple has received additional requests similar to the one underlying the case before this court." The judge hasn't decided the matter.

USA Today
Are Android devices more easily hacked than iPhones?
Friday, 19 February 2016
Byline: Brett Molina, Elizabeth Weise

Washington - If Syed Rizwan Farook had carried a phone running on the Android or Windows operating system, the FBI may not have needed to ask anyone for help getting in.
Of the three main phone operating systems, only Apple builds the ability to have the phone erased after a certain number of failed passcode attempts into its operating system, security experts say.

Apple's use of an "Erase Data" feature connected to passcodes is one of the security features that separates it from other smartphones on the market.

That separation became a part of the national discussion Tuesday when a federal judge required Apple to create software to disable the feature that erases the data on the iPhone after 10 failed login attempts.

The FBI wants to get past the feature in Farook's phone to see if there is information on it that will give the agency insight into the mass shooting attack by Farook and his wife Tashfeen Malik in December.

In a letter to customers posted on Apple's website, CEO Tim Cook says the company will fight the order, comparing the request to creating a "backdoor" on all iPhones.

Disabling Apple's "Erase Data" feature, which is what the FBI wants the company to do, would allow it to use a "brute force" attack, entering countless passcodes until they discovered the correct one and gain access to the phone.

The functionality can be added to Android and Windows phones, but it's difficult and meant for system administrators, said Filip Chytr, director of threat intelligence for Avast Software, a Prague- based computer security company.

Google, the creator of Android software, and Microsoft did not respond to a request for information for this report.

Android does include a Remote Wipe option, where a user can remotely erase the contents of their smartphone.

Third-party apps which bring this functionality to Android and Windows phones are readily available but require extra work on the user's part as they're not a built-in functionality that's easily turned on.

In encryption, the encoding of what's on the phone so it's not readable by anyone without the proper code keys, Apple is ahead of the game.

Apple has made encryption the default on its phones since the 3GS. Android only began making it the default with its most recent phone.

New York Times
Line in the Sand Over iPhones Was Over a Year in the Making
Friday, 19 February 2016
Byline: Multiple reporters

Washington - Time and again after the introduction of the iPhone nearly a decade ago, the Justice Department asked Apple for help opening a locked phone. And nearly without fail, the company agreed. Then last fall, the company changed its mind. In a routine drug case in a Brooklyn federal court, prosecutors sought a court order demanding that Apple unlock a methamphetamine dealer's iPhone 5S running old, easy-to-unlock software. The company acknowledged that it could open the phone, as it had before. But this time, it pushed back.

"We're being forced to become an agent of law enforcement," the company's lawyer, Marc Zwillinger, protested in court.

That stance foreshadowed this week's showdown between the Obama administration and Apple over the locked iPhone belonging to one of the suspects in the San Bernardino, Calif., shooting rampage. By the time of Mr. Zwillinger's statement, Apple and the government had been at odds for more than a year, since the debut of Apple's new encrypted operating system, iOS 8, in late 2014.

The new technology repeatedly stymied investigators -- the New York authorities said on Thursday that they had been locked out of 175 iPhones in cases they were pursuing. But both sides held out hope for a compromise that would avoid the type of confrontation that occurred this week when a federal magistrate judge ordered Apple to comply with the Justice Department's request.

With last October's court filing, the confrontation became all but inevitable. The company left no doubt that it would fight any effort to crack its new, encrypted phones. The only real question was what crime the government would use to press its case.

Apple's stance that day in Brooklyn caught the Justice Department off guard. Despite the issue with iOS 8, the company had continued to cooperate. In the first half of 2015 alone, the company provided data

in response to more than 3,000 law enforcement requests, Apple said. And company lawyers gave prosecutors no indication that the drug case against Jun Feng would be any different.

Mr. Feng, 45, claimed to have forgotten his passcode, making his cooperation a moot point even if he were willing to extend it, according to a government filing. Unlike the phone in the San Bernardino case, Mr. Feng's ran iOS 7, an older version of Apple's operating system that does not automatically encrypt its data. The Justice Department figured it would have the information from Mr. Feng's phone within a day.

Mr. Zwillinger said the drug case would be Apple's line in the sand. "Customer data is under siege from a variety of different directions," he said. "Never has the privacy and security of customer data been as important as it is now."

It was a delicate period for the Obama administration, which was focused on finding a way to break into the new encrypted iPhones. The F.B.I., in particular, was lobbying hard to win support for that idea in the face of skepticism from Silicon Valley, Congress and the public.

Timothy D. Cook, Apple's chief executive, described data privacy as a human rights issue. Backed by leading technologists, Mr. Cook argued that if the company designed a way to defeat encryption for the United States government, that tool would be exploited by hackers or foreign governments like China.

Under the attorney general Eric H. Holder Jr., the Justice Department was sympathetic to that point of view, even in the face of an aggressive campaign from the F.B.I. director, James B. Comey. Mr. Holder favored meeting with technology executives in the hope of finding common ground, current and former Justice Department officials said.

Others in the department strongly disagreed. National security and criminal prosecutors argued that, with the introduction of the encrypted iOS 8, Apple (along with Google, which had started its own encrypted Android phone software) had made thumbing its nose at the government a business strategy. The only hope, these prosecutors argued, was a court fight or an act of Congress requiring companies to provide the government unencrypted data.

Local law enforcement officials, too, were sounding alarms. "This has become, ladies and gentlemen, the Wild West in technology," Cyrus R. Vance Jr., the district attorney in Manhattan, said at a news conference Thursday, echoing complaints he and others have made for many months. "Apple and Google are their own sheriffs. There are no rules."

When the attorney general Loretta E. Lynch and her deputy, Sally Q. Yates, took office last year, the F.B.I. and its law enforcement allies found more receptive ears. Ms. Yates, in particular, took up the issue, giving speeches and testifying before Congress alongside Mr. Comey.

Despite the campaign, the White House showed no appetite for legislation. And Apple showed no signs of budging. In a few instances, the two sides appeared bound for a court fight, only to resolve it at the last moment. Last summer, Apple refused to give the Justice Department real-time access to iMessages -- the company's proprietary text messages -- in a gun case. The matter nearly escalated, but Apple eventually turned over some messages that had been backed up to the company's iCloud servers. It was not all that the government wanted, but authorities viewed it as a sign of cooperation.

Such compromises forestalled a major court showdown, but increased the frustration at the Justice Department. Several current and former career prosecutors involved in the issue said they viewed it as hypocritical that Apple encouraged its customers to save its data to iCloud -- which it would turn over to the government -- but regarded the cellphone as sacrosanct.

Then came the Feng case. By refusing to help, the Justice Department thought Apple was sending a clear signal. If it would no longer cooperate with requests to help unlock old phones, there was little chance it would give in and build a way to unlock the new encrypted phones running iOS 8.

"Forcing Apple to extract data in this case, absent clear legal authority to do so, could threaten the trust between Apple and its customers and substantially tarnish the Apple brand," Mr. Zwillinger said.

By that time, 90 percent of Apple devices were running iOS 8 or newer versions. The F.B.I. warned that it was only a matter of time before its agents were locked out of a phone in a case with lives at stake.

The San Bernardino attacks, which killed 14 people, presented the F.B.I. with a seemingly perfect test case. One of the shooters, Syed Rizwan Farook, was killed by the police and left behind a locked, encrypted iPhone 5c. The F.B.I. has not been able to unlock it.

Mr. Farook's phone is protected by a password that Apple says it does not keep and Apple says it cannot break the encryption without the password. The F.B.I. wants to write a program to send the phone an unlimited combination of passwords until it finds one that works.

But Apple built its phones to protect against that tactic. Each wrong guess causes a short delay, which would significantly slow the F.B.I.'s effort. After too many incorrect guesses, the phone will automatically erase its memory.

The authorities are still interested in more than just Mr. Farook's phone. On Thursday, a team of F.B.I. agents raided the Southern California home of his brother, Syed Raheel Farook, and carted off boxes of belongings. The authorities would not say what they were searching for.

But there is no telling what is on Mr. Farook's phone -- maybe clues to accomplices or his inspiration, maybe nothing -- but nobody in the government questioned the need for obtaining access to that data. From a public relations standpoint, Apple had been on the side of privacy advocates and civil libertarians. This case put the company on the side of a terrorist.

"They need to figure that out now before there is that bigger body count. So this is as good a test case as any to have that fight," said Ron Hosko, who until 2014 led the F.B.I.'s criminal division. "Crack that thing for me now, Tim Cook, because it's only going to get worse."

This week, the Justice Department got its wish when Apple was ordered to override its defenses, even if it meant building a tool that did not exist.

Law enforcement officials cheered the ruling, though they acknowledged that the fight was not over. Apple promised to appeal. In New York, William Bratton, the police commissioner, held up a phone that he said was used by an associate of a man who shot and wounded two police officers in the Bronx recently.

"Despite having a court order, we cannot access this iPhone," Mr. Bratton said. "Just one example, a very significant example in which two of my officers were shot, that impeding that case going forward is our inability to get into this device."

The case in Brooklyn continues, even though Mr. Feng has already pleaded guilty. While the Justice Department sees the San Bernardino incident as its ideal test case, Apple is hoping for a legal win in Brooklyn.

Judge James Orenstein has given the company reason to be hopeful. In the past, he has been skeptical of the way the government uses an 18th-century law -- the All Writs Act -- that the Justice Department is now claiming gives it the authority to force Apple to unlock the phones. He once even described the Justice Department's use of it as a "Hail Mary play."

But he has yet to rule.

Wall Street Journal
The FBI vs. Apple
Friday, 19 February 2016
Byline: Editorial Board

Editorial - The encryption cold war that for two years has pitted Silicon Valley against law enforcement finally turned hot this week, as a California judge ordered Apple to unlock an iPhone used by the San Bernardino terrorists. Perhaps public safety and modern digital security methods were bound to collide, but the danger as always in such conflicts is that both sides end up annihilated.
The Federal Bureau of Investigation is attempting to bypass the security system on an iPhone recovered from Syed Rizwan Farook, who with his wife Tashfeen Malik killed 14 people and injured 22 others. The problem is that no one knows the phone's password.

Apple has turned over information that Farook stored to its cloud servers, but he did not back up his phone for several weeks proceeding the attack. The FBI wants to retrieve this encrypted data that exists only on the device itself, which potentially include text messages, photos, location tracking or connections to the Islamic State or perhaps even other terror cells that could be operating in the U.S.

Apple's iOS operating system is designed to automatically erase local data after too many incorrect passcode attempts. Because iPhones can only run software with Apple's proprietary cryptographic signature, the FBI wants Apple to create and upload a custom version of iOS to Farook's device that overrides this mechanism. The bureau can then hook up an external computer that will make unlimited guesses to unlock the phone's contents, known as "brute forcing." Magistrate Judge Sheri Pym agreed.

In a public letter, Apple CEO Tim Cook refused to comply with this "unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority" and said the company would appeal. "The U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone," he wrote.

Yet the reality seems to be more complicated than either Mr. Cook or the FBI allow. The encryption debate began in 2014 when Apple released a feature that generates random security "keys" that are unknown to Apple and in combination with the user's passcode to decrypt the device's data. Without such mathematical formulas, the data are unreadable.

This two-step "full disk" encryption process makes iPhones more secure, but it also means Apple can't unlock its own products. Neither can Google after adopting the same practice. Encrypted communication platforms have been available since the early 1990s, but Apple and Google have now made them the default for the 96% of global customers who use their operating systems.

The fear among law enforcement and the national-security agencies is that jihadists and criminals are going dark. FBI chief James Comey and Manhattan District Attorney Cy Vance warn they are losing the capacity to execute bona fide search warrants granted under the Fourth Amendment. So they support a mandate that the U.S. tech industry install a master security key -- the "backdoor" Mr. Cook invokes -- to unlock any device.

The CEO has a strong case when he says that backdoors create more problems than they solve. Introducing security vulnerabilities that third parties like cops and spooks can use as needed can also be exploited by hackers, crooks and spies. Nations can mandate backdoors, but there will always be some encrypted channels outside of their jurisdiction where the likes of ISIS can plot. The result would be weaker products for law-abiding consumers that leave U.S. companies less competitive with little security benefit.

Stronger cybersecurity is more important than ever in a world of corporate espionage, millions of compromised credit-card numbers and the stolen identities at the Office of Personnel Management. Encryption may lead to fewer antiterror intercepts, though the universe of signals that can be tapped has expanded radically and on balance more secure phones are a major advance for human freedom. Ask the Chinese pastors or Russian dissidents who are targeted by authoritarian regimes and want encrypted iPhones.

One question is whether the San Bernardino terror case should be an exception to Mr. Cook's strong argument against backdoors. In this case Apple is not being ordered to create a universal backdoor for all phones, and some digital security experts believe it is technologically possible to assist the FBI in the San Bernardino investigation with a unique iOS to brute-force this single device.

"Apple does not dispute that it has, in prior instances, complied with data extraction demands that have been contained in the body of search warrants or, less often, All Writs Act orders," Apple conceded in a New York court filing last year. The government is citing this to show that its request is reasonable.

But in those cases the company's engineers have never been conscripted to create a new architecture to defeat their own security measures. Apple believes that if it caves even once, every prosecutor in America will be lining up for forensic help with misdemeanors. A supposedly one-time emergency fix in an antiterror case could well become a de facto backdoor in practice over time.

There's also the question of whether the government currently has the legal authority to force Apple to become the government's agent. Safe manufacturers are not obligated to crack their own locks when the FBI calls. Apple contends the All Writs Act has never been used to compel what the government now wants from Apple, and the question is far from clear-cut. The litigation to settle this could take months or years.

It's an understatement to say that Apple is taking a risk by challenging the Administration in a high-profile domestic terror incident with unpredictable politics. "Apple chose to protect a dead ISIS terrorist's privacy over the security of the American people," said Arkansas Republican Tom Cotton, and Donald Trump has been no more subtle.

But for the same reason, the Administration ought to have resolved the situation confidentially before it reached legal and political Defcon One. Terror cases by their nature are different from run-of-the-mill law enforcement, and San Bernardino requires more than the government's typical show of incompetence.

The White House never supplied Congress with specific backdoor statutory language even as Mr. Comey made the public rounds, only for President Obama to renounce any attempt at forging a legislative

solution. Yet spokesman Josh Earnest defended the FBI and Justice Department on Wednesday. Is there a grownup in the White House?

So a word on behalf of Michael McCaul, the Chairman of the House Homeland Security Committee, who has proposed convening an expert panel on technology and security in the modern era. Blue-ribbon commissions are usually a form of Beltway escapism, but in this case a detailed report and recommendations from leading minds in technology, law, computer science, police and intelligence could help shape a rough consensus -- or at least establish a common set of facts. Such a halfway house might also help calm political tempers and marginalize the absolutists.

A mature democracy -- if America still is one -- ought to be able to work out these crucial matters of national security through legislative deliberation. The public interest on encryption is best served with a rational debate, not the ad hoc nuclear legal exchange that the Administration is inviting.

Washington Post
Wrong bite of the Apple
Friday, 19 February 2016
Byline: Editorial Board

Editorial - Until Tuesday, Apple appeared to be winning its fight with law enforcement. President Obama announced last year that he would not pursue legislation forcing tech companies to give law enforcement access to users' encrypted data. But on Tuesday, the FBI persuaded a judge to order Apple to create software that would help federal investigators crack into the iPhone 5C that Syed Rizwan Farook used before he shot up a San Bernardino, Calif., banquet room in December. Apple immediately promised to fight the order.
In essence, the FBI is attempting to explore and establish the limits of its legal powers to combat terrorism - as well as more mundane domestic crimes - under existing laws, in the absence of action by Congress and the White House. We think that's the wrong call. The nation should not ask the courts to strike a balance between device security and law enforcement access. The political branches of government should do that.

The FBI relied on the two-century-old All Writs Act, a law that helps the government execute search warrants, to compel Apple to create hacking software for Farook's phone. The order was nominally tailored to Farook's specific device, but its implications are larger. To what extent is it reasonable to force companies to write code and harm their international reputations for data security - and, therefore, their business models - in order to help the U.S. government hack into suspects' phones? Should this be a routine investigative tool, or reserved for extraordinary situations, or beyond the pale? Farook's is an extreme case, but it is easy to foresee the government attempting to apply All Writs to

less important investigations. What sorts of software can the government compel tech companies to write?

The answers to these questions have major implications for online safety and security. The more government-ordered hacking techniques are developed and used, the more likely they eventually will fall into the hands of malicious actors. This risk seems small but is difficult to estimate. Even if technology companies and the government kept the techniques they developed secret, their hacking activities would still threaten the technology ecosystem. Fearful of government-mandated malware, fewer people might accept automatic updates from software companies. This would make devices more vulnerable. The anti-terrorism benefits, meanwhile, would wane over time, as high-level terrorist groups turned to software from places beyond the reach of U.S. law enforcement.

The public has reason to be frustrated that investigators cannot execute valid search warrants; this is a worrying impediment to legitimate law enforcement. We believe Apple should help search for a workable solution. If there is a Paris-style attack in the United States, decisions may be imposed on it in a far less benign atmosphere. But the decisions should be made by Congress.

Meanwhile, Apple's role as a leading exponent of data security brings special responsibilities. Whatever U.S. officials decide, the policy will be the legitimate product of a democratic government and the rule of law. That will not be true in countries such as China, where dictators would use anti- terrorism tools to crack down on dissenters. We hope that Apple will fight as hard to safeguard its users' privacy from authoritarian abuse.

Motherboard (Vice)
Police Arrest Second Alleged Member of Teen Group that Hacked CIA Director
Thursday, 18 February 2016
Byline: Lorenzo Franceschi-Bicchierai

New York - The grip seems to be tightening around the infamous group of teenage hackers that's been targeting US government agencies and high- level officials for months.
On Tuesday, police in Scotland arrested a 15- year-old boy from Glasgow, whom a source told Motherboard is one of the main members of the hacking group known as "Crackas With Attitude," or CWA. The teenager, according to the source, is the hacker known as "Cubed."

The arrest of the teenage hacker comes only a week after UK police, working with the FBI, arrested another alleged member of the group, a 16-year-old boy suspected of being Cracka, another main member of the group. Following the arrest of the boy in the UK, other members of the group, including Cubed, pledged to keep hacking and threatened the US government with more attacks.

A close friend of the arrested hacker confirmed he was the CWA member known as Cubed. The close friend spoke to Motherboard on condition of anonymity.

"I hope he's okay, he was like a brother to me," the source said.

A spokesperson from Police Scotland confirmed the arrest of a boy suspected of hacking crimes, but declined to answers questions on whether he was one of the members of the hacking group.

"Following a search of a property in the Glasgow area on Tuesday the 16th of February, a 15-year old male was arrested in connection with alleged offenses under the Computer Misuse Act 1990," the spokesperson said in a prepared statement. "He has since been released from custody and he is subject of a report to the procurator fiscal."

The arrest was first reported by the local tabloid the Daily Record on Thursday. The paper also reported that FBI agents flew to Glasgow to question the boy. Before that, on Wednesday morning (US time) another member of CWA tweeted that Cubed had been arrested.

The member, known as IncursioSubter, did not respond to a request for comment. Other members of the group declined to comment as well.

In a phone call, an FBI spokesperson didn't respond to questions regarding the arrest. And a spokesperson from the South East Regional Organised Crime Unit (SEROCU), the UK agency who arrested the teenager suspected of being Cracka, also declined to comment.

In October, Cracka and Cubed claimed to have broken into the AOL email account of John Brennan. This was just the first in a long list of attacks on high profile officials such as FBI's executive assistant Amy Hess, US spy chief James Clapper, a former senior executive at the National Geospatial-Intelligence Agency, and President Barack Obama's senior advisor on science and technology John Holdren.

More recently, the hackers were also apparently involved in a breach at the US Department of Justice, which ended up with the dump of almost 29,000 names, titles, email addresses and phone numbers from the FBI and the Department of Homeland Security.

The Daily Record (Scotland)
FBI swoop on schoolboy Scots hacker accused of breaking into their top-secret computer system
Thursday, 18 February 2016
Byline: Stephen Stewart

Glasgow - FBI agents swooped on a Scots schoolboy accused of trying to hack into their top-secret computer system.
Operatives from the US crimebusting agency travelled to Glasgow after detectives arrested the 15- year-old on Tuesday and searched his home.

It is understood the FBI agents sat in as Police Scotland officers interviewed the boy, who could face extradition and imprisonment in the United States.

A source said: "The boy is believed to have hacked into the FBI's computer systems.

"Agents then travelled to Scotland to sit in on him being questioned by detectives. He could be extradited to the US where he would face a long jail term."

Police confirmed that the boy had been arrested and later released.

A spokesman said: "Following a search of a property in the Glasgow area on Tuesday, February 16, a 15-year-old male was arrested in connection with alleged offences under the Computer Misuse Act 1990.

"He has since been released and is the subject of a report to the procurator fiscal. It would be inappropriate to comment further at this time."

A source close to the case said the boy's family were shocked at the turn of events, adding: "He comes from a respectable family."

The Glasgow operation comes just months after a Scot was dubbed the most dangerous hacker of all time by activist group Anonymous.

IT whizz Gary McKinnon, 49 - who has Asperger's syndrome - broke into 97 Pentagon and NASA computers, stealing passwords, deleting files and shutting down net-works on military bases.

He faced trial in the US and up to 70 years in jail if convicted - but Home Secretary Theresa May blocked his extradition under human rights laws.

In December, Anonymous labelled McKinnon the best-ever "black hat" hacker - the term for hackers who indulge in illegal activity.

Just days ago, police in the East Midlands arrested the alleged teenage mastermind of cyber attacks targeting US government officials

It is not known if the Glasgow teenager's case is linked to those events.

Reuters
Islamic State finds 'diminishing returns' on Twitter: report
Thursday, 18 February 2016

Washington - The Islamic State's English-language reach on Twitter has stalled in recent months amid a stepped-up crackdown against the extremist group's army of digital proselytizers, who have long relied on the site to recruit and radicalize new adherents, according to a study being released on Thursday. Suspensions of English-speaking users affiliated with Islamic State from June to October 2015 have limited the group's growth and in some cases devastated the viral reach of specific users, according to the report from George Washington University's Program on Extremism, which analyzed a list of accounts promoted by the militant group.

The report found that easily discoverable English accounts sympathetic to Islamic State was usually under 1,000, and that those users' activity was mostly insular, limited to interacting with each other. Islamic State has seized control of wide swaths of Iraq and Syria and claimed credit for attacks in Paris in November that killed 130. The U.S. and other governments consider it a terrorist organization.

Twitter Inc. has long been criticized by government officials for its relatively lax approach to policing content, even as other Silicon Valley companies like Facebook Inc. began to more actively police their platforms.

Under intensified pressure from the White House, presidential candidates and some civil society groups, Twitter announced earlier this month it had shut down more than 125,000 terrorism-related accounts since the middle of 2015, most of them linked to the Islamic State group.

In a blog post, the company said that while it only takes down accounts reported by other users it had increased the size of teams monitoring and responding to reports and has decreased its response time "significantly."

J.M. Berger, a co-author of the report, said Twitter is still less active than many of its rivals but that part of that is due to its relative youth as a company.

"Each company has been dragged into this kicking and screaming," he said in an interview.

Reporting of Twitter accounts affiliated with Islamic State is a steady, low-level activity generally, but occasionally events lead to "periodic purges," Berger said.

The study took place prior to the Paris attacks, which the researchers said likely led to a heavy wave of suspensions mostly in French and Arabic networks.

The average tweets per day measured across the lifetime of an account also declined during the monitored interval, from a peak of approximately 14.5 in June to a low of 5.5 by October, the report found. The average number of followers was measured between 300 and 400.

La Dépêche du Midi (Toulouse)

Amende pour le webmaster indélicat
Friday, 19 February 2016
Byline: J.R.

Albi, France - T.R., webmaster gaillacois de 31 ans et papa d'un enfant de 4 ans, comparaissait hier à la barre du tribunal correctionnel d'Albi présidé par la présidente Brigitte Schildknecht pour «accès frauduleux dans un système de traitement automatisé de données et collecte de données à caractère personnel par un moyen frauduleux », des faits commis courant septembre 2014 au préjudice du conseil général du Tarn puisque c'est, on s'en souvient, son site internet qui avait fait l'objet de nombreuses cyberattaques à cette époque. Une époque, rappelons-le quand même fortement marquée alors par «la bataille de Sivens entre Zadistes et pro- barrage. Le prévenu est un sympathisant zadiste et ne s'en cache pas mais réfute toute intention frauduleuse. «Je ne me suis jamais introduit sur le site du conseil général et je n'ai jamais collecté la moindre donnée».
«Pourtant, lui rétorque la présidente, les enquêteurs de la direction générale de la sécurité intérieure (DGSI) qui ont perquisitionné chez vous et avec qui vous avez passé quelques heures en garde à vue parlent de 100 000 requêtes suspectes.» «J'en ai seulement fait 150 depuis mon adresse IP (IP pour Internet Protocol), reconnaît T.R. à la barre. D'ailleurs, je ne me suis jamais caché. Je n'ai pas mis d'image et encore moins de vidéo sur ce site. J'ai juste mis un lien dans une barre d'adresse du site. Après, je n'y suis pour rien si durant cette période, les Anonymous dont je ne fais absolument pas partie, ont attaqué le site du Département. La seule chose que je n'aurais pas dû faire est de repartager des données du conseil général. Mais jamais je ne pensais qu'un simple copier/coller allait me conduire à la barre d'un tribunal.»

L'avocate du Département du Tarn s'insurgera ensuite «contre les préjudices subis avec un serveur piraté et remplacé, trente sites web affectés, des usagers pénalisés et réclamera 20 700 euros, 10 700 euros et 6 000 euros respectivement aux titres des préjudices technique, d'atteinte à l'image et opérationnel sans oublier 3 000 euros au titre de l'article 475-1.»

Selon Pascal Suhard, vice- procureur de la République, on reconnaît volontiers que vous n'appartenez pas aux Anonymous mais vous minimisez votre responsabilité en parlant d'une bêtise que vous n'auriez pas dû faire. Je requiers à votre encontre deux mois de prison avec sursis.»

Guillaume Pressec, avocat de T.R., demandera purement et simplement la relaxe de son client arguant que «les deux infractions retenues contre lui ne sont pas caractérisées. Il n'a en effet dénaturé aucun site. Il n'est par ailleurs pas poursuivi pour avoir inséré une vidéo sur ce site. Ensuite, on lui reproche du vol informatique. Or, il n'a jamais collecté frauduleusement de données. Elles étaient en vente libre sur internet. Il n'a fait qu'un copier/coller. Ce dossier est celui des fantômes, les Anonymous, condamnées pour certains par d'autres juridictions.»

Pas de prison avec sursis pour T.R. qui écope de plusieurs amendes pour un montant total de 4 000 euros.

National Post
Four charged with export of tech to China
Tuesday, 01 March 2016
Byline: Douglas Quan

Mounties have charged four men with illegally exporting restricted information from Canada to China to help develop that country's space satellites.
Investigators allege two employees of a Waterloo, Ont., technology company stole "technical data" from the company and then created a separate firm to broker contracts abroad.

The two men, along with a former employee, landed contracts with two Chinese companies, including one that was state-owned, to create microelectronics that would "enhance" China's satellite cameras, police said. The fourth man was an employee of one of the Chinese companies.

"Canada has an international responsibility to safeguard its exports which potentially may be used against Canadians and their allies," RCMP Supt. Jamie Jagoe said in a statement.

"This investigation is an example of foreign governments having an interest in Canadian-based controlled technology and it highlights the RCMP's commitment to keeping Canadian's safe from the potential misuse of that technology."

Protecting Canadian trade secrets from prying foreign eyes has become a growing priority for intelligence officials.

A briefing document prepared for Ralph Goodale, the federal public safety minister, last fall by the Canadian Security Intelligence Service said that in addition to terrorist threats, Canada continued to grapple with the targeting of classified information and advanced technology from foreign entities. "Hostile state-sponsored actors continue to target Canadian public and private resources, including computer networks, to advance their economic, military and political agendas," said the document, obtained under access- to-information laws.

Police say the investigation, dubbed Project OSensor, began in early 2014 after officials from Teledyne DALSA, the Waterloo firm, sent a written complaint to the federal government. The government then forwarded the complaint to the RCMP.

"The matter involves controlled goods and technologies being shipped between Canada and China in violation of the Canadian Controlled Goods Program and related export laws," the RCMP said in a release.

"Police allege that the four accused involved themselves in Chinese contracts for the design and development of controlled goods intended for space satellite use."

One of the contracts was with the Beijing Institute of Space Mechanics and Electricity, the Waterloo Region Record reported.

Police announced numerous theft and fraud-related charges against Arthur Xin Pang, 46, of Pierrefonds, Que., and his company, Global Precision Inc.; Binqiao Li, 59, of Waterloo; Nick Tasker, 62, of Britain, and his Montreal company 3D Microelectronics; and Hugh Ciao, 50, of California.

Pang and Li were arrested and had their first court appearance Monday. Pang remains in custody, while Li was released on conditions. Arrest warrants were issued for Tasker and Ciao.

"I can confirm that Mr. Pang and Mr. Li are no longer employees of Teledyne DALSA, and that Teledyne DALSA brought this matter to the attention of the Canadian government," company spokeswoman Geralyn Miller said Monday in an email.

"Unfortunately, we won't be commenting further on the pending criminal investigations."

Teledyne DALSA specializes in digital imaging and semi- conductor products for the industrial, defence, aerospace, medical and transport sectors, according to its website. It employs about 1,000 people.

The company has co-operated fully with the investigation, police said.

Pang's LinkedIn profile shows he worked as a sales manager until June 2014 handling "China/Taiwan key accounts of big projects (sensor and camera design)."

Li taught at Tianjin University and was an engineer at Samsung Electronics, according to an online resumé. The Canadian Space Agency, Canada Border Services Agency, Department of National Defence, Public Services and Procurement Canada, Global Affairs Canada, as well as the U.S. Department of Homeland Security, and Federal Bureau of Investigation helped in the probe.

None of the charges has been proven in court.

Canadian Press
Police charge 4 people with trading controlled satellite camera tech to China
Tuesday, 01 March 2016
Byline: Liam Casey

Four people and two Canadian companies are facing charges over their alleged roles in exporting controlled goods and technologies to China that could enhance that country's satellite cameras, RCMP said Monday.
The Mounties allege the four were involved in creating and selling microelectronics, specifically a sensor, to two Chinese companies _ one of them state-owned.

They allege the goods and technologies were being shipped from Canada to China in violation of the Canadian Controlled Goods Program and other export laws.

Two Canadians _ who worked at Waterloo, Ont.-based Teledyne DALSA Inc. _ stole technology from their employer and set up a company with a former employee in order to get a contract to make the sensor, police alleged in a statement.

Investigators say the fourth accused works with one of the Chinese companies allegedly involved.

"Project OSensor commenced in early 2014 after the RCMP was requested to conduct a criminal investigation by Public Services and Procurement Canada _ Controlled Goods Directorate and Global Affairs Canada, as a result of a written complaint ... from Teledyne DALSA," police said.

Teledyne co- operated fully with the investigation, they said.

Arthur Xin Pang, of Pierrefonds, Que., and his company Global Precision Inc., Bianqiao Li, of Waterloo, Ont., Nick Tasker of the United Kingdom and his Montreal-based company, 3D Microelectronics Inc., and Hugh Ciao, of California, face numerous offences related to the alleged incident.

Police said Pang and Li were to appear for a bail hearing in a Waterloo court on Monday, while warrants have been issued for Tasker and Ciao.

Canada has a controlled goods program designed to prevent proliferation of weapons, satellite communication equipment, military equipment and intellectual property.

"Canada has an international responsibility to safeguard its exports which potentially may be used against Canadians and their allies," said RCMP Supt. Jamie Jagoe.

"This investigation is an example of foreign governments having an interest in Canadian-based controlled technology and it highlights the RCMP's commitment to keeping Canadian's safe from the potential misuse of that technology."

The Canadian Space Agency, the Department of National Defence, Global Affairs Canada, the U.S. Department of Homeland Security, and the FBI were among the agencies involved in the investigation, police said.

Globe and Mail
Chinese censors tighten screws on freewheeling online videos
Tuesday, 01 March 2016
Byline: Nathan Vanderklippe

Section: general

China's dour censors have long maintained a lengthy naughty list, and used it to keep the country's television sets unsullied by anything deemed to "lack positive thoughts and meaning."
Now, the Chinese Communist Party under President Xi Jinping has vowed to apply the same rules online, slamming shut an era of looser rules for Internet video, amid a sweeping campaign to reassert strict new controls over the country's cultural life - a campaign motivated in part by fears that speech must be controlled lest a slowing economy sow dangerous unhappiness.

Chinese video websites such as youku.com, iqiyi.com and le.com, which blend the features of YouTube and Netflix, have flourished in recent years, attracting enormous audiences for their content, some of it bawdy and boundary-pushing.

The makers of online video had largely been allowed to self-regulate, with shows dropped only if they caused too much of a stir after people started watching.

But China now says it will extend its strict censorship rules to Internet video, under the principle that "what can't play on TV can't play online," a change that promises to end what had been an avenue for freer expression.

Authorities have already knocked at least seven popular shows offline in recent months, including Web dramas dealing with time-travel, homosexuality, journalistic ethics and elder abuse. Together, those shows had attracted billions of views, before gaining scorn from censors as being too prurient, violent or superstitious. One reappeared weeks later, with a third of its content gone. Censors have also taken a hard-line approach recently to plunging necklines in an imperial court drama.

In China, one online comment was as searing as it was succinct: "Is this North Korea?" Only two months in, 2016 has already become the year of the Chinese media crackdown, a campaign driven by parallel efforts to assert Communist Party supremacy and keep a lid on dissent that might emerge amid a slowing economy.

This weekend, Ren Zhiqiang became the highest-profile target. The bold property developer was nicknamed "the Cannon" for his willingness to challenge the party line, through sometimes scathing posts to social media.

He accumulated 38 million followers - until Sunday, when China's Internet regulator deleted his social-media accounts.

Weeks earlier, Mr. Xi visited the central organs of the state media apparatus - Xinhua, CCTV and the People's Daily - on a smilesand-handshakes tour intended to strike fear into the country's journalists.

"The media run by the party and the government are the propaganda fronts and must have the party as their family name," Mr. Xi said. Party media "must love the party, protect the party and closely align themselves with the party leadership in thought, politics and action."

That mandate has grown particularly important as China's economic growth rate slows and its stock markets fall, while the closings of factories and mines affects ever-larger numbers of people. Last summer, amid a market rout, authorities arrested hundreds for "rumour-mongering," including a journalist who reported non-public information about internal financial policy debate. In late February, the state-run China Daily explicitly tied Mr. Xi's new media mandate to the weakening prospects.

"It is necessary for the media to restore people's trust in the Party, especially as the economy has entered a new normal and suggestions that it is declining and dragging down the global economy have emerged," the paper wrote in an editorial.

The same strict mindset is being applied to cultural matters, leading to the pledge Sunday by Chinese authorities to halt the different treatment for online video, which had largely been allowed to self-regulate, with shows dropped only if they caused too much of a stir after people started watching.

Luo Jianhui, head of the online audio visual program department at the State Administration of Press, Publication, Radio, Film and Television, criticized online production for its poor writing and bad quality control, which he said yielded absurd, bizarre and vulgar content, in comments reported by Chinese media.

He pledged to "strengthen" management of online video and increase punishment for offenders.

"The government thinks online security is equivalent to national security, so it's not something that they can let slide," said Will Tao, an independent China Internet expert in Beijing.

It's a catchup game by Beijing, as its people stampede away from traditional media.

Last year, for the first time, Chinese spent more than half of their media-consumption time on the Internet, with TV coming in second at 46.3 per cent, according to estimates by Beijing-based iResearch, which conducts online audience research.

The country now counts 460 million online video viewers; in early 2014, they watched 5.7 billion hours of content a month, a figure that has since risen - in part because viewers lapped up edgier online content.

Those sites had broadcast serious work online, too, including Under The Dome, a groundbreaking environmental documentary by a Chinese journalist that racked up 200 million hits before it was taken down.

Now, viewers are bracing for a tide of boring.

David Moser, a China commentator who is academic director at CET Chinese Studies at Beijing Capital Normal, called it "a death of anything that smacks of subversion or alternative content or uncomfortable reality."

Making online video look like television "puts everything down to the lowest common denominator. It's all equally stultifying, all equally bland, all equally conservative."

Waterloo Region Record
Former employees charged in alleged plot to rip off Dalsa
Tuesday, 01 March 2016
Byline: Greg Mercer

Two former employees of Waterloo's Teledyne Dalsa have been charged with stealing sensitive satellite imaging technology and selling it to China, in violation of Canada's export laws.
The charges are the result of a two-year investigation by the RCMP's organized crime unit - dubbed Operation OSensor - which started after a complaint from the Waterloo company in early 2014.

That Kitchener-based probe crossed international borders, and involved the Canadian Space Agency, Canada Border Service Agency, Department of National Defence, Public Services and Procurement Canada, Global Affairs Canada, the U.S Department of Homeland Security and the FBI.

Two men, Arthur Pang, 46, and Binqiao Li, 59, are accused of exporting proprietary Dalsa technology to China, in violation of the Canadian Controlled Goods Program, while they worked for the Waterloo company.

Both have been arrested and face a string of charges.

The charges include theft, fraud, conspiracy to commit fraud and possession of property obtained by crime. Pang is also accused of breaking Canada's export and customs laws.

Arrest warrants have also been issued for two other men, Britain's Nick Tasker - a Dalsa employee between 2002 and 2003, according to LinkedIn - and Hugh Ciao of California, who worked for one of the Chinese firms allegedly involved in the deal. They face several charges, including fraud over $5,000.

Li and Pang are accused of stealing Dalsa technology while they worked for the company and using it to outbid their former employer for a contract with the state-owned Beijing Institute of Space Mechanics and Electricity.

After Pang - who was arrested Friday when he landed at the airport in Montreal - left Dalsa, he started his own company, Global Precision Inc. Li, meanwhile, still worked for Dalsa when the charges were laid.

The Canadian-made technology was allegedly to be used in commercial Chinese satellites, according to Lisa Mathews, the federal prosecutor who is handling both men's bail hearings.

The alleged scheme is also a matter of national security, according to the RCMP.

Canada has a Controlled Goods Program that regulates the spread of "tactical and strategic assets including weapons, satellite global positioning systems and communications equipment, military equipment and related intellectual property."

"Canada has an international responsibility to safeguard its exports which potentially may be used against Canadians and their allies," Superintendent Jamie Jagoe, southwest district commander for the RCMP in Ontario, said in a statement.

"This investigation is an example of foreign governments having an interest in Canadian-based controlled technology and it highlights the RCMP's commitment to keeping Canadians safe from the potential misuse of that technology."

It's alleged the scheme started back in June 2011 and lasted until last summer, court heard Monday.

Li, a Chinese-born Canadian citizen who lives in Waterloo, was released on $500,000 bail Monday from a Kitchener courtroom.

He wore a black winter coat, sweater and collared shirt, and relied on a Mandarin translator for the appearance. Li's wife appeared in court, and swore under oath that she'd report him if he broke any of the conditions of his bail.

His lawyer, Hal Mattson, said Li turned himself in to the RCMP in Kitchener on Monday morning. Li, who was set free after handing in his passport and given strict limits on his movements, declined to comment outside of court.

Li is a former professor of electronic and information engineering at Tianjin University, and joined Dalsa's research staff in 1998, specializing in image sensors. Prior to that, he worked for Samsung, according to his online resumé.

The investigation began after the Waterloo company tipped off the authorities two years ago, the RCMP said. A federal agency forwarded Dalsa's complaint to the police, who received the company's full help.

"The company co-operated fully with our investigation," said Sgt. Penny Hermann of the RCMP.

Li continued to be employed by Dalsa for many months after the investigation began, court heard Monday.

A spokesperson for Dalsa declined to comment.

Toronto Star
CSE chief must break her silence
Tuesday, 01 March 2016
Section: editorial

Bring our spies to heel, Editorial Feb. 25
I am happy the Star has articulated the outrage that some readers probably feel over the recent Senate testimony of the commissioner of the Communications Security Establishment.

Last Monday, Commissioner Jean-Pierre Plouffe was unable to assess for the Senate the scale of the leak of partially anonymous information on Canadians from our electronic spy agency, the Communications Security Establishment (CSE), to its foreign partners, including the U.S. National Security Agency. He has indicated, essentially, that there is no way to know how many Canadians have been affected and for how long the problem has persisted.

To me, it is inconceivable that scientists and engineers at the CSE, who are using systems with known performance characteristics, could not provide the commissioner with at least a minimum number of potential victims of the leak. I have to wonder whether all the details relevant to the problem have been made available to him.

The commissioner has the legal authority to subpoena witnesses in pursuit of an answer to the question of how many victims there may be. The Inquiries Act gives him the power to chase down evidence that people within the CSE may not want to divulge. If ever there was a time to press harder on the public's behalf using these admittedly blunt tools, this is probably it.

And what of the chief of the CSE, Greta Bossenmaier, our nation's top electronic spy who oversees the actual day-to-day operations of the agency? Not a peep. In fact, she's been peep-less without peer during this unprecedented debacle.

Now is the time for her to break with the CSE's tradition of reticence during public discussions of intelligence activities and face our legitimate concerns.

Brian Alexander, Mississauga

London Times
You won't catch terrorists by this snooper's charter
Tuesday, 01 March 2016
Byline: Bill Binney

Op-ed - When a government draws up a landmark surveillance law to "protect national security and public safety", you'd assume they'd ask: what's the most effective method of doing that -- is it bulk interception of everyone's communications, or is there a better way? The Investigatory Powers Bill will affect everyone in the UK. It will fundamentally alter the relationship between individual and state with its mass interception, mass hacking, mass acquisition of communications data, and retention of huge databases of innocent people's most sensitive information.
Three major parliamentary reports in less than ten days concluded the case hasn't been made for all of these powers. The joint committee on the draft bill made 86 major recommendations for change -- but just three weeks later the government will publish the bill today.

If ministers care about citizens' rights and national security, they must forensically examine whether bulk spying powers actually help in the fight against terror and serious crime. The answer -- as I said in my evidence to the joint committee -- is no. They hinder it.

I worked in intelligence for 36 years. I know from experience that mass surveillance inundates analysts with too much data, and that makes it harder for them to find the people intent on doing harm.

Theresa May, the home secretary, submitted anecdotal evidence to convince the committee that mass surveillance is necessary. But each example she used was of targeted surveillance. The committee's report rightly concluded the case hadn't been made to justify the bill's incredibly intrusive proposals.

GCHQ's bulk collection does not work. By scanning every single person's communications and profiling everyone's web browsing habits, GCHQ is overloaded with data and false targets. One system, for example, collects around 1,000 records for every person in the UK every day -- about 64 billion. The result is that, while details of potential attacks might be collected, people are killed before we can find them.

Intelligence gathering has to be intelligent -- it has to be targeted. Communications data should be collected on known suspects and their social networks; on visitors to websites hosting illegal or extremist content; and on certain geographical areas, like conflict zones.

This bill is a chance for the UK to shore up the safety of its people -- to think again and re-draft for the sake of our freedom and security. I hope MPs will take that chance.

Note: Bill Binney is former technical director of the US National Security Agency.

Washington Post
Apple's congressional testimony: 'Dangerous precedent' would weaken all iPhones
Monday, 29 February 2016
Byline: Andrea Peterson

Washington - Apple's general counsel plans to argue Tuesday on Capitol Hill that the FBI's request to unlock the smartphone used by one of the San Bernardino, Calif. terrorists would set "a dangerous precedent" of the federal government ordering a company to weaken the security of its own products, according to a copy of his testimony obtained by The Washington Post.
Bruce Sewell, the general counsel, plans to say that Apple has "no sympathy for terrorists." But he will argue that once the iPhone is weakened in this way, hackers and cyber criminals could wreak havoc on the personal safety and privacy of the hundreds of millions of people who own an Apple device.

"They are asking for a backdoor into the iPhone," Sewell's testimony states. "Building that software tool would not affect just one iPhone. It would weaken the security for all of them.... We can all agree this is not about access to just one iPhone."

Sewell's testimony also states that FBI Director James Comey has acknowledged that the FBI would likely use the precedent in other cases involving iPhones.

The Justice Department has argued that the request is limited in scope and is necessary because it has been unable to unlock the iPhone used by Syed Rizwan Farook, who, along with his wife, killed 14 people and injured nearly two dozen in a shooting rampage in December

"Maybe the phone holds the clue to finding more terrorists. Maybe it doesn't. But we can't look the survivors in the eye, or ourselves in the mirror, if we don't follow this lead," FBI Director James Comey, who will also testify Tuesday, said in a column on the Lawfare Blog last week. In the same column, Comey said the case San Bernardino case "isn't about trying to set a precedent or send any kind of message."

But in testimony before the House Intelligence Committee last week, Comey suggested the case "will be instructive for other courts."

Manhattan District Attorney Cyrus Vance, who will also be testifying Tuesday, previously said his office has 175 phones it is unable to unlock -- and told Charlie Rose he would "absolutely" push forward for access to them if the government prevailed in the case.

Apple formally challenged the FBI's request last week. On Tuesday, Sewell will put several questions before lawmakers at the hearing.

"Do we want to put a limit on the technology that protects our data, and therefore our privacy and our safety, in the face of increasingly sophisticated cyber attacks? Should the FBI be allowed to stop Apple, or any company, from offering the American people the safest and most secure product it can make?

"Should the FBI have the right to compel a company to produce a product it doesn't already make, to the FBI's exact specifications and for the FBI's use?"

The Guardian (London)
Home Office to publish revised draft of snooper's charter
Tuesday, 01 March 2016
Byline: Alan Travis

London - The home secretary, Theresa May, has revised some elements of her controversial "snooper's charter" legislation in an attempt to address criticism by MPs and peers of the surveillance powers it confers.
Home Office sources say the revised bill, to be published on Tuesday, will reflect a majority of the 129 recommendations made by three parliamentary committees in reports published over the last three weeks.

The committees called for a fundamental rewrite of the draft investigatory powers bill, for privacy safeguards to be made the backbone of the legislation and for safeguards to be created against new powers to track everyone's web browsing histories - known as internet connection records. The bill will not meet demands that the most intrusive snooping operations should be authorised by a judge - and not by a minister as is the case at present.

The Home Office's proposed changes include

. six codes of practice setting out how the security services will use the powers in the bill, including access to personal communications data, state computer hacking and bulk acquisition of data.

. stronger privacy safeguards including the need for a senior judge to approve security service access to a journalist's communications data. The Home Office said this was needed to ensure the willingness of sources to provide information to journalists.

. a "double-key" ministerial warrant backed by judicial approval when UK security services ask foreign intelligence agencies to undertake work on their behalf.

. a pragmatic approach to encryption that will require technology companies to remove encryption that they have themselves applied where it is practicable for them to do so.

. the period for "urgent" warrants issued for the most intrusive surveillance without judicial approval is to be reduced from five to three days.

A Home Office source said: "We have considered the committees' reports carefully and the bill we are bringing forward today reflects the majority of their recommendations. We have strengthened safeguards, enhanced privacy protections and bolstered oversight arrangements.

"This is world-leading legislation, setting out in unprecedented detail the powers available to the police and security services to gather and access communications and communications data, subject to a robust regulatory regime."

The revised bill commits to working with industry to retain internet connection records but does not provide judicial oversight of this new power.

The changes are unlikely to go far enough to satisfy political critics and privacy campaigners who have called for the 299-page "snooper's charter" to be split so that full parliamentary scrutiny can be undertaken.

The bill has been introduced after disclosure of the security services' mass surveillance capabilities by whistleblower Edward Snowden and was published in draft form before Christmas to allow for a short period of pre-legislative scrutiny.

MPs and peers were particularly critical of new powers requiring internet and phone companies to store everyone's web-browsing histories - known as internet connection records - for 12 months, saying the case for it had not been made and the cost and other practical implications had not been worked out.

The parliamentary intelligence and security committee said that privacy safeguards needed to be made the backbone of the legislation rather than treated as an "add- on".

Other criticisms of the earlier draft of the bill from the parliamentary committees included:

* the description of security service capabilities - computer hacking and collecting bulk data - was too broad and lacked clarity

* it failed to provide a comprehensive framework for surveillance powers as it did not include undercover police surveillance, nor computer hacking for attack purposes

* the independent reviewer of terrorism legislation, David Anderson QC, called for judicial authorisation of the intrusive surveillance warrants but the scrutiny committee endorsed the government's "dual key" approach with more resources for judicial commissioners.

Privacy campaigners are sceptical that the revised bill will meet their concerns: "We are gravely concerned that the significant flaws within the bill will not have been addressed," said a spokesman for the Don't Spy on Us coalition.

"We understand the government's desire to to pass the investigatory powers bill before December 2016 when the Data Retention and Investigatory Powers Act (Dripa) sunset clause expires.

New York Times
Judge Rules for Apple in New York iPhone Case
Tuesday, 01 March 2016
Byline: Katie Benner, Joseph Goldstein

New York - A federal magistrate judge on Monday denied the United States government's request that Apple extract data from an iPhone in a drug case in New York, giving the company's pro-privacy stance a boost as it battles law enforcement officials over opening up the device in other cases.
The ruling, from Judge James Orenstein in New York's Eastern District, is the first time that the government's legal argument for opening up devices like the iPhone has been put to the test. The denial could influence other cases where law enforcement officials are trying to compel Apple to help unlock iPhones, including the standoff between Apple and the F.B.I. over the iPhone used by one of the attackers in a mass shooting in San Bernardino, Calif., last year.

Judge Orenstein, in his 50-page ruling on Monday, took particular aim at a 1789 statute called the All Writs Act that underlies many government requests for extracting data from tech companies. The All Writs Act broadly says that courts can require actions to comply with their orders when not covered by existing law. Judge Orenstein said the government was inflating its authority by using the All Writs Act to force Apple to extract data from an iPhone seized in connection with a drug case.

The government's view of the All Writs Act is so expansive as to cast doubt on its constitutionality if adopted, Judge Orenstein wrote.

The All Writs Act is also being invoked in the fight over an iPhone in the San Bernardino shooting, which has publicly pitted Apple against the government. Apple's chief executive, Timothy D. Cook, has refused to comply with a federal court order to help break into the phone, saying that he needs to protect the data of all customers. That has set off a far-reaching debate over privacy and security.

Both the F.B.I. and Apple have called for Congress to step in to help settle the question of when law enforcement should get access to citizens' private data. On Tuesday, Apple's general counsel, Bruce Sewell, and James B. Comey, the F.B.I. director, will testify about balancing privacy and safety before the House Judiciary Committee.

"It's important that a judge for the first time recognizes the All Writs Act doesn't provide the lawful authority the government has been claiming in these cases," said Esha Bhandari, a lawyer with the A.C.L.U., which supports Apple's position. "It demonstrates that when the government's arguments are put to the test, a federal court has decided they were not actually right."

In a statement on Monday in response to Judge Orenstein's ruling, the Justice Department said it would ask the judge to review the decision. Apple had previously agreed to help open up the iPhone in the drug case, and has complied with past All Writs Act orders, the Justice Department said.

"This phone may contain evidence that will assist us in an active criminal investigation, and we will continue to use the judicial system in our attempt to obtain it," the Justice Department said.

An Apple senior executive said Monday's ruling makes clear that helping to open an iPhone is a constitutional issue that should be taken up by Congress.

Judge Orenstein's ruling stands out because the courts have largely been absent on the major questions of electronic surveillance and privacy of our day. While judges around the country have signed at least 70 orders at the request of the government compelling Apple to access data on phones, this was the first time that a judge and Apple have pushed back.

The legal back and forth between Judge Orenstein, the Justice Department and Apple began last October, when federal prosecutors applied for a court order to force Apple to unlock an iPhone 5s seized by the Drug Enforcement Administration in a 2014 drug case, according to court documents.

After federal prosecutors requested the order, Judge Orenstein argued in an 11-page memo last October that prosecutors were misusing the All Writs Act. The judge asked Apple to weigh in, and the company filed a brief that same month. In addition to agreeing with the judge, the company also said the request could create an undue burden and threatened to "substantially tarnish the Apple brand."

"This reputational harm could have a longer-term economic impact beyond the mere cost of performing the single extraction at issue," Apple said in a brief.

The government then called Apple's decision to side with the judge a "stunning reversal." Saritha Komatireddy, a Brooklyn federal prosecutor, said the government's application in this case "was just a simple routine request for assistance in carrying out a valid search warrant issued by a federal court, as Apple has done so many times before."

During the case, Judge Orenstein said he found it puzzling that Apple had not previously resisted the use of the All Writs Act, including in other cases where Apple had complied with the order.

"You have had apparently 70 prior instances where you have not taken the steps available to you," Judge Orenstein said to Apple's lawyers during a hearing.

Ultimately, Judge Orenstein argued that the government couldn't use the All Writs Act to ask Apple to help extract information from a device just because a different law, the Communications Assistance for Law Enforcement Act, or Calea, addresses the issue and does not include an "information services" company like Apple. Congress has been debating whether to amend Calea to include tech companies such as Apple, Facebook and Alphabet's Google.

Still, the decision is not binding for the San Bernardino case, said Eric A. Berg, a litigation lawyer and special counsel with Foley & Lardner, who is a former Justice Department lawyer.

"From a technical, legal standpoint, it doesn't really have much of an effect in the California districts," Mr. Berg said. But "if you start with public opinion, this is going to be viewed as a victory for the privacy lobby and a defeat for the government in that battle over privacy."

USA Today
Apple-FBI dispute looms large at RSA
Tuesday, 01 March 2016
Byline: Elizabeth Weise

San Francisco - The cyber security conference that comes to San Francisco every year -- might have flown past most people's radars if this was a typical year.
That changed this month when the Apple vs. FBI iPhone battle became public. While the keynotes and workshop titles aren't changing, the topics of privacy, security and government intrusion will loom over every panel.

The furor over whether Apple will be forced to aid the government in creating a program that will allow the FBI to hack into the iPhone used by San Bernardino killer Syed Rizwan Farook is hitting just as an expected 34,000 cryptographers, chief information security officers, programmers and the like gather here.

Overall, this year's conference focuses on the nuts and bolts of computer security: encryption, industrial control systems, digital identity, breaches and how to fight them.

While always important to tech companies, the Apple case is raising awareness about the technical issues that create the security and privacy, or lack thereof, in the products we use daily.

There will always be a tension between the public's expectation of protection from the government and concerns about government intrusion, Cisco CEO Carl Bass told USA TODAY last week.

"I don't think we will ever get to the point where nothing can be broken. Go back in history -- there were locks and people who picked locks. There were secret codes and code breakers. These things will always be able to be broken," he said.

The U.S. security establishment will be working to get its voice heard at the conference. Tuesday, Attorney General Loretta Lynch will deliver a keynote on cyber security and then participate in an armchair conversation on the topic. Assistant Attorney General John Carlin of the National Security Division will also talk about terrorists' use of social media and the Internet.

A topic likely to garner lots of interest is the hackability of self-driving cars. The duo who made news last year by hacking into a Jeep Cherokee, Charlie Miller and Chris Valasek, will offer a workshop titled "Intro to Car Hacking."

Both now work at Uber's Advanced Technology Center in Pittsburgh, a strategic partnership between Uber and Carnegie Mellon University.

The center focuses on research and development in areas like vehicle safety, mapping and self-driving cars.

The conference ends Friday with a question and answer session with actor Sean Penn. He'll be interviewed by RSA President Amit Yoranabout his philanthropy and public advocacy and the relationship between Hollywood stardom and privacy.

Penn most recently was in the news in January for a controversial meeting with Mexican drug lord Joaqun "El Chapo" Guzmn for Rolling Stone magazine.

The exact nature of Penn's expertise is unclear. He himself wrote in Rolling Stone in January that he is "the single most technologically illiterate man left standing. At 55 years old, I've never learned to use a laptop. Do they still make laptops? No (expletive) idea!"

Washington Free Beacon
Pentagon Wages First Cyber War on ISIS
Monday, 29 February 2016
Byline: Bill Gertz

Washington - Senior Pentagon leaders on Monday revealed the military's first use of cyber warfare operations against the Islamic State terrorist group they said are aimed at disrupting its military communications and operations.
Defense Secretary Ash Carter said the use of cyber attacks against ISIS control centers in Syria and Iraq is a new warfare capability.

The operations are being carried out to "disrupt ISIL's command and control, to cause them to lose confidence in their networks, to overload their network so that they can't function, and do all of these things that will interrupt their ability to command and control forces there, control the population and the economy," Carter told reporters at the Pentagon, using an alternative acronym for the Islamic State.

"So this is something that's new in this war, not something you would've seen back in the Gulf War," Carter added. "But it's an important new capability and it is an important use of our Cyber Command and the reason that Cyber Command was established in the first place."

Gen. Joseph Dunford, chairman of the Joint Chiefs of Staff, said cyber warfare attacks are being used as part of the overall military campaign to defeat ISIS, including cutting off the group's strongholds in Syria and Iraq, namely Raqqa and Mosul.

"I think conceptually, that's exactly the same thing we're trying to do in the cyber world," Dunford said.

"In other words, we're trying to both physically and virtually isolate ISIL, limit their ability to conduct command and control, limit their ability to communicate with each other, limit their ability to conduct operations locally and tactically."

Last week, apparently in response to the stepped-up cyber warfare attacks on ISIS, supporters of the group threatened to attack Facebook chief Mark Zuckerberg and Twitter chief Jack Dorsey. Both social media groups recently cracked down on the group's use of their platforms.

Carter and Dunford spoke to reporters at the Pentagon, outlining plans to enhance efforts against ISIS in the Middle East as well as countering its spread to North Africa and other regions.

Cyber warfare involves the use of trained computer hackers, backed by electronic and human intelligence, to break into foreign computer networks and information systems. Once inside, the attackers can implant viruses or other malware to disrupt information systems or fool them into taking action that can cause damage to their organization and its information technology.

The capability has been developed for the past several decades by the National Security Agency, which has been breaking into foreign networks for intelligence gathering since the 1980s.

The use of military cyber warfare operations is different from the covert intelligence operation, known as Olympic Games, targeting Iran's nuclear program in the late 2000s.

Carter also said cyber warfare is different from traditional electronic warfare, which has been used in previous conflicts to disrupt communications or disable radar.

"It is beyond that. We do that, too. The two enable one another and complement each other," Carter said.

Carter said the new cyber warfare capability is being distributed to all U.S. war-fighting forces through the Cyber Command.

"Cybercom itself was devised specifically to make the United States proficient and powerful in this tool of war," Carter said.

Dunford said the use of cyber attacks in Syria and Iraq will not be the same as methods used in other conflicts.

"You can't replicate what we're doing today against ISIL in Iraq and Syria elsewhere in the world," Dunford said. "What you can do is leverage the tools that have been developed for this particular operation, for other operations down the road."

Dunford declined to provide details of the operations in order to prevent the enemy learning about the activities, including the timing, location, and operational methods of the attacks.

"We don't want them to have information that will allow them to adapt over time," the four-star general said. "We want them to be surprised when we conduct cyber operations, and frankly, they're going to experience some friction that's associated with us and some friction that's just associated with the normal course of events in dealing in the information age."

The comments by Carter and Dunford are the first acknowledged use of cyber warfare in a conflict since Cyber Command, a component of the U.S. Strategic Command, was set up in 2010.

The command, co-located with the National Security Agency in Fort Meade, Md., remains one of the military's most secret organizations.

The command is still in the process of creating 133 cyber mission forces that will be deployed with the military's combatant and functional commands.

For example, the U.S. Pacific Command currently has a group known as CyberPac that supports military operations and countermeasures for that command. U.S. Forces Korea also has a cyber mission force charged with countering North Korean cyber attacks and conducting offensive operations against the North Koreans in wartime.

Carter dismissed concerns that blocking social media sites will limit intelligence gathering on the group.

Sometimes the efforts to block social media use drives terrorists to use other means of communicating, but some of those other communications are easier to intercept, he said.

The effort to use cyber attacks is a necessary part of the military campaign against ISIS, Carter said.

"We can't allow them to freely command and control forces that are enemy forces, so it's just like any other war," he said. "We have to attack their command-and-control. This is one of the ways of doing it. But it may have, actually, a beneficial effect of driving them to the kinds of communications that it's in fact easier for us to disrupt, and listen to also."

Dunford said the potential loss of intelligence as a consequence of cyber operations is examined carefully, and is "one of the variables we consider in whether or not you conduct an operation and how to conduct an operation."

The cyber and other attacks are part of the effort to put pressure on the terrorist group, which controls large swathes of territory in Iraq and Syria.

"We're trying to make life difficult for ISIL and we're trying to stay step ahead of them," Dunford said. "So we're trying to force them to make changes. We're trying to disrupt their communications, and then we can anticipate some of the adaptations they're going to make and be a step ahead of them, and that's what we're trying to do."

New York Times
National Briefing | Washington; 2002 Letter on Eavesdropping Is Made Public
Tuesday, 01 March 2016
Byline: Charlie Savage, Eric Lichtblau

Washington - The Obama administration on Monday made public a previously classified letter from 2002 about the Bush administration's secret program that allowed the National Security Agency to eavesdrop on Americans' international communications without court orders.
The release of the 22-page letter, written by John Yoo, then a top lawyer in the Justice Department's Office of Legal Counsel, adds to the historical record of one of the most controversial pieces of the Bush administration's response to the terrorist attacks of Sept. 11, 2001: The surveillance and bulk data collection program known by the code name Stellarwind.

The letter explained to Colleen Kollar-Kotelly, who at that time was the new chief judge of the Foreign Intelligence Surveillance Court, why the Justice Department considered the program lawful even though, as Mr. Yoo acknowledged, it clashed with wiretapping laws laid out in the Foreign Intelligence Surveillance Act.

The letter appeared to track a memorandum Mr. Yoo had written in Nov. 2, 2001, soon after President George W. Bush directed the N.S.A. to begin the program. A previously released inspector general report about the program included a partially redacted summary of that memo.

Among other things, Mr. Yoo claimed in the letter that the president's constitutional authority as commander-in-chief overruled statutory prohibitions and that under the circumstances the program complied with the Fourth Amendment, which bars unreasonable searches and usually requires warrants.

In the letter, Mr. Yoo wrote that, "We face a situation here where the government's interest on one side -- that of protecting the Nation from direct attack -- is the highest known to the Constitution. On the other side of the scale, the intrusion into individual privacy interests is greatly reduced due to the international nature of the communications."

In 2004, after Mr. Yoo had returned to teaching, a new leader of the Office of Legal Counsel, Jack Goldsmith, rejected parts of Mr. Yoo's legal analysis, leading to a now-famous confrontation in March of that year in the hospital room of then-Attorney General John Ashcroft and a threat by top Justice Department officials to resign.

To avert that threat, Mr. Bush then accepted some new limits on the program, which The New York Times partially disclosed 21 months later. The legal basis for the program also evolved. The spy court secretly blessed its bulk data collection components in 2004 and 2006, and Congress authorized warrantless wiretapping in a 2008 law, the Foreign Intelligence Surveillance Amendments Act.

New York Times
Last Batch of Clinton Emails Is Released
Tuesday, 01 March 2016
Byline: Steven Lee Myers, Julie Hirschfeld Davis

Washington - The State Department on Monday released the last set of emails from the 30,000 messages on Hillary Clinton's private computer server, including an email about North Korea that remains a point of dispute between the department and one of the nation's spy agencies over the secrecy of information that passed through the server.
That email -- written on July 3, 2009, after a North Korean ballistic missile test -- was one of four that prompted intensified scrutiny of the emails for classified information and a referral last year to the F.B.I. for a review of the handling of classified information by Mrs. Clinton, her aides and other State Department officials while she was secretary of state.

It was released as part of a chain of five replies and forwards on Monday with portions blocked out on the grounds that they contained information now classified "secret," though not "top secret," the higher classification that the spy agency, the National Geospatial-Intelligence Agency, had cited last summer.

"The original assessment was not correct, and the document does not contain top secret information," a State Department spokesman, John Kirby, said. He added that the department had agreed to classify

some of it "provisionally" pending further review, an indication that the dispute over the contents had not yet been resolved.

A spokesman for Mrs. Clinton's presidential campaign, Brian Fallon, said the "ongoing disagreement" about the North Korean test "means that the intelligence community's inspector general was wrong in his belief that this email was 'top secret.' "

Mrs. Clinton and her aides have said that the intelligence agencies are overzealously classifying information, and in this case the State Department agreed. The designation of "secret" nevertheless added to the list of emails that the department has released only after removing information that is now considered sensitive on national security grounds.

Among the final 1,723 emails released on Monday were 23 that the department upgraded to "secret," bringing the total classified as such to 65. Another 2,028 have had portions blocked out, or redacted, because the information is now "confidential."

Of the four emails that prompted the referral to the F.B.I., only one has now been classified as "top secret." It was among 22 emails that the State Department -- at the demand of the C.I.A. -- said it would not disclose, even in part, because they contained some of the nation's most closely guarded secrets.

In addition to the email involving North Korea's missile test, another was released last fall in full, while the third was released with portions blocked out as "confidential," the lowest level of classification. Officials have declined to specify those.

In all, less than 10 percent of the emails that passed through Mrs. Clinton's server contained confidential or secret information. That was enough to prompt reviews by the inspectors general of the State Department and the intelligence agencies, and by Congress and the F.B.I., over the mishandling of classified information.

The focus of those reviews, officials have said, has been on the advisers privy to her personal email address and on diplomats who sent messages that were forwarded by those aides, like Huma Abedin and Jake Sullivan, who served as a deputy chief of staff during Mrs. Clinton's term.

None of the emails were marked as classified at the time they were sent. And while the State Department has said that the "upgrades" do not reflect any judgment of their sensitivity at the time, the designations nonetheless suggested that at least some of the information should not have been sent over an unsecured system like hers, officials have said.

Mr. Kirby also announced that one more email between Mrs. Clinton and President Obama would not be released, adding to 18 that the State Department said in January it would not release, citing longstanding precedent that the White House controls presidential communications. Another email was

being withheld, Mr. Kirby said, at the request of a law enforcement agency, presumably because it was related to a continuing investigation.

Mr. Kirby declined to discuss either email, except to say that both were unclassified.

The end of the department's releases of the 30,068 emails, which came in 14 batches, including four in February, did not mean the end of the legal and political controversy over Mrs. Clinton's use of the private server.

In the case of the email about North Korea, the State Department also disputed the initial effort to assert that it contained classified information. The assertion came through the inspector general for the intelligence agencies, I. Charles McCullough III.

The email in question was written by a senior watch officer in the department's operations center, Shelby Smith-Wilson, and sent to Mrs. Clinton's executive staff. Although that portion was entirely redacted, one government official familiar with the contents said it described a conference call among senior officials, including Mrs. Clinton, about the ballistic missile test that North Korea conducted that day in violation of United Nations Security Council resolutions.

The email chain was forwarded with additional comments and the unofficial translation of a statement by the Japanese Foreign Ministry to Mrs. Clinton's closest aides, including Ms. Abedin, Mr. Sullivan and Cheryl D. Mills, her chief of staff.

In another email later marked as classified, Mr. Sullivan forwarded Mrs. Clinton a news article about a likely move by the Obama administration to shift some decisions on drone strikes to the White House from the Pentagon. "What Panetta is raising," Mr. Sullivan wrote in the May 2011 note, referring to Leon E. Panetta, then the head of the C.I.A.

Yahoo News
Apple will tell Congress strong codes protect against terrorists
Monday, 29 February 2016
Byline: Aaron Pressman

New York - Apple general counsel Bruce Sewell plans to tell Congress on Tuesday that strong encryption in iPhones protects users from terrorist and hacker attacks while rejecting calls from the FBI to weaken the popular phone's security protections.
"We feel strongly that our customers, their families, their friends and their neighbors will be better protected from thieves and terrorists if we can offer the very best protections for their data," Sewell said in a copy of his opening statement released by the House Judiciary Committee on Monday. "And at the same time, the freedoms and liberties we all cherish will be more secure."

Sewell is scheduled to speak on a panel with with New York District Attorney Cyrus Vance and Worcester Polytechnic Institute professor Susan Landau before the committee at a hearing starting at 1 p.m. The three speakers will be proceeded by FBI director James Comey, who will address the committee first and by himself.

The hearing comes as Apple and law enforcement agencies remain locked in a bitter dispute over the security measures the company added to the iPhone in recent years. Two weeks ago, a U.S. magistrate judge in California ordered Apple to create new software at the behest of the the FBI to weaken the security on a phone used by deceased San Bernardino shooter Syed Rizwan Farook so the agency could try to guess Farook's passcode more easily.

The FBI says it can't get access to data on the phone, which may provide evidence of further terrorist activities, without Apple's help. Apple is appealing the order, arguing that the new software it has been ordered to create could also be used by other governments and hackers, thus weakening the security of hundreds of millions of iPhone users around the world.

Comey has defended the FBI request in testimony at other Congressional hearings last week and in a blog post. The Judiciary Committee did not provide an advance copy of Comey's expected remarks, however.

"We simply want the chance, with a search warrant, to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly," Comey wrote in a short blog post on Feb 21. "That's it. We don't want to break anyone's encryption or set a master key loose on the land."

Vance plans to tell the committee that Apple's 2014 decision to encrypt most of the data stored on iPhones in a way that the company can't crack "severely harms" many criminal cases around the country. "Smartphone encryption has real-life consequences for public safety, for crime victims and their families," Vance's prepared remarks noted.

WPI professor Landau, an expert on cybersecurity, plans to warn the committee that the FBI's views are outdated and inconsistent with recent technological developments. "Instead of embracing the communications and device security we so badly need for securing US public and private data, law enforcement continues to press hard to undermine security in the misguided desire to preserve simple, but outdated, investigative techniques," she said in her prepared testimony.

As the security dispute moves from the courtroom to the policy arena, Apple's lawyer also plans to mention several recent government efforts backing strong encryption, including a 2013 report requested by President Obama in the wake of the Edward Snowden revelations.

That may be to counter a remark by Obama press secretary Josh Earnest on Feb. 17. "Obviously, the Department of Justice and the FBI can count on the full support of the White House as they conduct an investigation to learn as much as they possibly can about this particular incident," Earnest said when asked about the Apple-FBI legal dispute.

But, a section of the 2013 report by the Review Group on Intelligence and Communications Technologies that Sewell plans to reference, concluded that the government should make clear it will not "in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption."

BBC News
Ukraine cyber-attacks 'could happen to UK'
Tuesday, 01 March 2016
Byline: Chris Vallance

London - A recent cyber-attack on Ukraine's electricity network could be replicated in the UK, according to a member of a US investigation into the resulting blackout.
"I've been getting interest and calls from the UK, Norway, Germany and all over," said Robert Lee.

"The answer is yes [they could be vulnerable]."

Last week, the US Department of Homeland Security formally blamed hackers for December's power cuts.

It did not, however, name the suspected perpetrators.

The US government is expected to publish more details of the investigation shortly.

About 225,000 people were left without power for several hours when the Ukraine suffered what is believed to be the first successful cyber-attack on an electricity distribution network.

"The way the Ukrainians set up the grid and the type of the equipment they are using is also the way a lot of other nations do it," said Mr Lee, an infrastructure specialist at cybersecurity firm the Sans Institute.

He added the attack could have been worse, as the attackers could have shut off power to a much wider area.

"This was a shot across the bows," he told the BBC.

Individual UK power firms declined to comment on their security measures.

However, a source close to the industry - who asked to remain anonymous - confirmed that "given sufficient sophistication and funding", the UK's electricity infrastructure could be hacked.

A spokesperson for the Energy Networks Association - the body that represents the UK and Ireland's gas and electricity distributors - said cybersecurity was a top priority.

The Department for Energy and Climate Change told the BBC: "The UK has... dedicated cyber experts and teams to keep it protected."

How was the hack carried out?

In Mr Lee's view, the attack was highly likely to have originated in Russia.

But he said it was not possible to say whether it was the "Russian government or a well-funded [non-government] team".

At least six months before the power was shut off, he explained, attackers had begun sending phishing emails to Ukraine's power utility companies' offices, containing Microsoft Word documents. When opened, they installed malware.

Firewalls separated the affected computers from the power control systems.

But the malware - known as BlackEnergy 3 - allowed the hackers to gather passwords and logins, with which they were able to mount an attack.

After months of work, they gained the ability to remotely log in to vital controls, known as supervisory control and data acquisition (Scada) systems.

Finally on 23 December, Mr Lee said, the attackers "remote desk-topped" into the Scada computers and cut power at 17 substations.

At the same time, they jammed company phone lines, making it hard for engineers to determine the extent of the blackout.

How do you recover?

The power outages in Ukraine lasted for several hours. They were only reversed by switching to manual operations.

The attackers went to great lengths, according to Mr Lee, to make sure power supplies could not be turned back on automatically.

He said the hackers rewrote firmware in the electronic devices used to communicate with the substations' circuit breakers.

That meant that the power could not be turned on remotely even after engineers had regained control of the Scada computers.

In the end, the engineers had to visit the substations and operate them manually.

In the UK, this would take between one to two hours, the source close to the industry told the BBC.

Could it happen here?

UK power companies' systems are constantly under attack.

A breach "is entirely possible", said Eireann Leverett of Cambridge University's Centre for Risk Studies, but he added "there's a lot of people working very hard to stop it".

Mr Leverett is now working on a report about what the consequences might be, due to be published in April.

Glasgow University's Professor Chris Johnson has highlighted that some of the control systems used by power distribution companies can be found for sale online.

He warns that these could be used by hackers to hunt for security weaknesses.

But Mr Lee's view can be summarised as "where there's a will, there's a way".

Companies are unlikely to be able to prevent every assault on their systems, he warns. Ukraine's hackers were "inside" the electricity companies' systems for six months, he notes, highlighting the lengths they went to.

So one lesson, he says, is that power providers must ensure they can detect attacks quickly when they occur and have staff primed to respond.

That costs money, meaning more expensive bills for consumers.

In a speech to GCHQ last year, the chancellor George Osborne said an attack on the UK's electricity network could lead to "loss of life".

He announced an extra £1.9bn of taxpayer's money over five years to bolster GCHQ's cyber capabilities.

The chancellor also said countries must work together to call out those "acting outside the boundaries of acceptable behaviour".

Mr Lee has a similar view, adding that the international community must "take a stand" if responsibility for the attacks is finally determined.

How do you prevent attacks?

New York Times
Utilities Cautioned About Potential for a Cyberattack
Tuesday, 01 March 2016
Byline: David E. Sanger

Washington - The Obama administration has warned the nation's power companies, water suppliers and transportation networks that sophisticated cyberattack techniques used to bring down part of Ukraine's power grid two months ago could easily be turned on them.
After an extensive inquiry, American investigators concluded that the attack in Ukraine on Dec. 23 may well have been the first power blackout triggered by a cyberattack -- a circumstance many have long predicted. Working remotely, the attackers conducted "extensive reconnaissance" of the power system's networks, stole the credentials of system operators and learned how to switch off the breakers, plunging more than 225,000 Ukrainians into darkness.

In interviews, American officials said they have not completed their inquiry into who was responsible for the attack. But Ukrainian officials have blamed the Russians, saying it was part of the effort to intimidate the country's political leaders by showing they could switch off the lights at any time.

"They could be right," said one senior administration official. "But so far we don't have the complete evidence, and the attackers went to some lengths to hide their tracks."

Even after it has reached a conclusion, the White House might decide not to name the attackers, just as it decided not to publicly blame China for the theft of 22 million security files from the Office of Personnel Management.

But American intelligence officials have been intensely focused on the likelihood that the attack was engineered by the Russian military, or "patriotic hackers" operating on their behalf, since the first reports of the December blackout. The officials have found it intriguing that the attack did not appear designed to shut down the entire country. "This appears to be message-sending," said one senior administration official with access to the intelligence, who requested anonymity to discuss the ongoing inquiry.

Equally interesting to investigators was the technique used: The malware designed for the Ukrainian power grid was directed at "industrial control systems," systems that act as the intermediary between computers and the switches that distribute electricity and guide trains as they speed down the track, the valves that control water supplies, and the machinery that mixes chemicals at factories.

The most famous such attack was the Stuxnet worm, which destroyed the centrifuges that enriched uranium at the Natanz nuclear site in Iran. But that is not an example often cited by American officials -- largely because the attack was conducted by the United States and Israel, a fact American officials have never publicly acknowledged.

Experts in cybersecurity regard the Ukraine attack as a teaching moment, a chance to drive home to American firms the vulnerability of their own systems. "There's never been an intentional cyberattack that has taken the electric grid down before," said Robert M. Lee of the SANS Institute. Mr. Lee said that while it was still not possible to determine who conducted the attack - - what is called "attribution" in the cyber industry -- he noted that it was clearly designed to send a political message.

"It was large enough to get everyone's attention," he said, "and small enough not to prompt a major response."

The warning issued last Thursday by the Department of Homeland Security provided the first detailed account of the Ukrainian attack, based on the findings of a series of government experts who traveled to Ukraine to gather evidence.

The attack described by the Homeland Security document was highly sophisticated. The attackers gained entry, it appears, by sending a series of "spearphishing" messages that led someone in Ukraine to unintentionally give them access. Once they had that, the attackers mapped the system, much as the North Koreans mapped Sony Entertainment's computers before attacking them in the fall of 2014.

Then a series of cyberattacks were carefully coordinated to occur within 30 minutes of one another on Dec. 23. The "breakers" that disconnected power were operated "by multiple external humans" through secure communication channels. The hackers then wiped many of the systems clean using a form of malware aptly named "KillDisk" which erased files on the systems and disabled them. They wiped out the "human-machine interface" that enables operators of the electric system to run those systems -- or get them back in service -- from their computers.

For extra measure, the hackers even managed to disconnect backup power supplies, so that once the power failed, the computers could not turn them back on.

Investigators say that in the end, the Ukrainians may have been saved by the fact that their country relies on old technology and is still not as fully wired as many Western nations -- meaning they were able to restore power by manually flipping old- style circuit breakers.

"The bad news for the United States is that we can't do the same thing," said Ted Koppel, the former ABC News anchor who published a best seller last year, entitled "Lights Out," about the vulnerability of the American electric grid.

"We have 3,200 power companies, and we need a precise balance between the amount of electricity that is generated and the amount that is used," he said. "And that can only be done over a system run on the Internet. The Ukrainians were lucky to have antiquated systems."

The report from Homeland Security recommended a series of common-sense steps: Make sure that outsiders accessing power systems or other networks that operate vital infrastructure can monitor the system, but not change it; close "back doors" -- system flaws that can give an intruder unauthorized access; have a contingency plan to shut down systems that have been infected, or invaded, by outsiders.

But all those systems make it harder for legitimate operators to use the Internet to keep vast systems operating, from a smartphone or laptop if necessary.

London Daily Telegraph
Google, Apple and others not forced to break in to encryption unless 'practicable', snoopers bill to say
Tuesday, 01 March 2016
Byline: Tom Whitehead

London - Twitter, Apple, Google and other communication companies will not be forced to decrypt messages unless it is "practicable" as ministers will today admit they are powerless to stop unbreakable encryption.
Theresa May, the Home Secretary, will publish a revamped snooping bill after draft proposals on surveillance powers last year received widespread criticism.

The revised Investigatory Powers Bill will make it clear that communication providers will only be asked to remove encryption "where it is practicable for them to do so", sources said.

The move will reignite concerns that terrorists and criminals are increasingly hiding behind so-called "end-to-end encryption" in online messages, which even the provider cannot access.

It comes as figures show major communication companies are still rejecting up to half of requests for customer data from UK police and intelligence agencies.

In other measures to try and get the legislation through parliament, the Government will take the unprecedented step of publishing an "operational case" on why MI5, MI6 and GCHQ need to carry out bulk collection of data.

The document will attempt to allay fears of mass surveillance by demonstrating that even when data is scooped up, only information on suspects is targeted.

Extra safeguards for journalists and lawyers will also be included along with additional authorisation checks on UK spy agencies when they need help from foreign intelligence agencies.

Mrs May is facing a backbench revolt over the legislation amid concerns it has to be rushed in to law before the end of the year, when laws governing some existing powers fall away.

The bill will require internet and phone companies to keep a record of websites visited by every citizen for 12 months.

It also details powers for the security services to perform bulk collection of personal communications data and for the agencies and police to hack in to computers and phones.

The draft legislation, published in November, was criticised by three parliamentary committees as being "flawed" and failing to make a case for many of the controversial measures.

A source said: "We have considered the committees' reports carefully and the Bill we are bringing forward today reflects the majority of their recommendations. We have strengthened safeguards, enhanced privacy protections and bolstered oversight arrangements.

"This is world-leading legislation, setting out in unprecedented detail the powers available to the police and security services to gather and access communications and communications data, subject to a robust regulatory regime."

However, on encryption, the bill will clarify and "put beyond doubt" that companies "can only be asked to remove encryption that they themselves have applied and only where it is practicable for them to do so".

The source said that this will "make clear that the Government is not asking companies to weaken their security by undermining encryption".

Separate figures show that in the first half of 2015, Apple provide information following a UK request in 56 per cent of cases relating to a device and 63 per cent in connection with a customer account.

Google provided data in 75 per cent of requests over the same period while Facebook met 78 per cent of requests.

Twitter met 52 per cent of request in the first six months but that increased to 76 per cent in the second half of the year.

Washington Post
In New York, Apple wins a battle in its legal war with the U.S.
Tuesday, 01 March 2016
Byline: Ellen Nakashima

Washington - A federal judge in New York ruled in favor of Apple on Monday, saying that an obscure Colonial-era law did not authorize him to force the firm to lift data from an iPhone at the government's request.
The ruling is not binding in any other court, but it takes on an outsize importance as the U.S. government battles Apple in a separate case in California over whether the tech firm should help unlock a phone used by one of the shooters in the San Bernardino terrorist attack in December.

The two cases involve different versions of iPhone's operating system and vastly different requests for technical help, but they both turn on whether a law from 1789 known as the All Writs Act can be applied to cases in which the government cannot get at encrypted data stored on suspects' devices.

Magistrate Judge James Orenstein in Brooklyn, who sits in the Eastern District of New York, has become the first federal judge to rule that the act does not permit a court to order companies to pull encrypted data off a customer's phone or tablet.

In a 50-page opinion disdainful of the government's arguments, Orenstein found that the All Writs Act does not apply in instances where Congress had the opportunity but failed to create an authority for the government to get the type of help it was seeking, such as having firms ensure they have a way to obtain data from encrypted phones.

He wrote that the government's interpretation of the 200-year-old law was "absurd" in that it would authorize what they were seeking even if every member of Congress had voted against granting such authority. It would, he added, undermine "the more general protection against tyranny that the Founders believed required the careful separation of governmental powers."

He also found that ordering Apple to help the government by extracting data from the iPhone - which belonged to a drug dealer - would place an unreasonable burden on the company.

None of the factors he reviewed in the case, Orenstein said, "justifies imposing on Apple the obligation to assist the government's investigation against its will."

A Justice Department spokeswoman said the department was disappointed in the ruling and would appeal. "As our prior court filings make clear, Apple expressly agreed to assist the government in accessing the data on this iPhone - as it had many times before in similar circumstances - and only changed course when the government's application for assistance was made public by the court,"

spokeswoman Emily Pierce said in a statement. "This phone may contain evidence that will assist us in an active criminal investigation and we will continue to use the judicial system in our attempt to obtain it."

Alex Abdo, staff attorney with the American Civil Liberties Union, said Orenstein's ruling "sends a strong message that the government can't circumvent the national debate by trying to manufacture new authorities through the courts."

Following Orenstein's reasoning, Abdo said, "If the court rejects the government's request in New York, then the FBI's request in San Bernardino is necessarily illegal, too."

But other analysts say that other courts could well rule in the opposite direction. In Riverside, Calif., Magistrate Judge Sheri Pym, at the Justice Department's request, last month issued an order requiring Apple to build software to override a safety feature in a different iPhone operating system to enable the FBI to try its hand at cracking the phone's password.

The government had never before asked a firm to build software to undo a security feature that it had built in to protect a phone's encrypted data. In this case, the feature wipes data from the phone after 10 incorrect tries to guess the password. Experts said that once the feature was overridden, it should take about 20 to 30 minutes to crack a four-digit password. Apple fears that if it is forced to comply with that request, countless more will follow to help it unlock phones in even routine criminal investigations.

The prospect that the California ruling could go against Apple has tech firms rushing to file briefs in support of Apple by Thursday's filing deadline.

Because of the nature of the request, the outcome of the California case is more significant than the Brooklyn case, analysts say. "It has the potential to alter the landscape permanently," said Al Gidari, a former partner at Perkins Coie who represented tech firms and is now at Stanford University.

The Guardian (London)
Four charged in Canada with selling stolen satellite equipment to China
Tuesday, 01 March 2016
Byline: Jessica Murphy

Ottawa - Canadian federal police have charged an American, a Briton and two Canadians with stealing sensitive satellite imaging technology and selling it to China in violation of export laws.
Two of them stole a sensor from their employer Teledyne Dalsa of Waterloo, Ontario, with help from a former employee, according to the Royal Canadian Mounted Police.

They sold it to two Chinese firms, one of them state-owned, in violation of the Canadian Controlled Goods Program and other laws.

The fourth accused works for one of the Chinese companies allegedly involved in the scheme.

The microelectronics were "intended for space satellite use", the RCMP said in a statement.

"This investigation is an example of foreign governments having an interest in Canadian-based controlled technology and it highlights the RCMP's commitment to keeping Canadian's safe from the potential misuse of that technology," said RCMP Superintendent Jamie Jagoe.

The two-year probe also involved the Canadian Space Agency, the military, US homeland security and the FBI.

Canadians Arthur Xin Pang, 46, and Binqiao Li, 59, were arrested and charged with more than a dozen related crimes including theft, fraud and possession, and transfer of controlled goods contrary to the Defense Production Act.

The RCMP said both were due in a Waterloo court for a bail hearing on Monday.

Arrest warrants were issued for Nick Tasker, 62, of Britain, and Hugh Ciao, 50, of California, who is currently in China.

Michel Juneau-Katsuya, former Asia-Pacific bureau chief for the Canadian Security Intelligence Service, said Canada's knowledge-based, hi- tech sectors were a prime target for corporate espionage, which he estimated cost the economy about $100bn annually.

Canadian companies, the government and national security agencies were not doing enough to tackle the problem, he said.

"We have weak laws, law enforcement is ill equipped, the government does not assume leadership and, at the end of the day, the general population and business leaders aren't aware of what's going on," he said.

Teledyne Dalsa, a tech company that specializes in digital imaging, circuit and electronic technology software, has offices in Canada, the US, Europe, and Asia.

Jason VanWees, a senior vice-president with the company, told the Guardian that "any kind of corporate espionage is a concern and that's why when we detected it, we let people know". He declined to comment further on the matter to the Guardian on Monday.

The RCMP said the company cooperated fully with the investigation, which was launched in early 2014 after Teledyne Dalsa's complaint with the force.

Canada has seen a number of high-profile corporate espionage incidents in the past.

Telecommunications giant Nortel Network's 2009 collapse and bankruptcy has been linked to its targeting for years by hackers allegedly operating out of China.

In 2014 the Canadian government pointed to a "highly sophisticated Chinese state-sponsored actor" as being responsible for hacking into computers at the National Research Council of Canada, a federal research and development body.

Canada has a domestic industrial security programme - the controlled goods programme - that aims to strengthen the country's defence trade controls and prevent the proliferation of strategic assets including satellite GPS systems and communications equipment.

Le Monde
En Iran, l'application Telegram connaît un succès fulgurant
Tuesday, 01 March 2016
Byline: Martin Untersinger, et Louis Imbert

Téhéran, Iran - Contrairement aux réseaux sociaux Twitter ou Facebook, le service d'échange de messages sécurisés n'est pas filtré par les autorités
En Iran, les élections législatives et de l'Assemblée des experts, se sont déroulées vendredi 26 février. Dans ce pays, l'application Telegram a pris une place considérable. Ce service d'échange de messages sécurisé à deux ou en groupe, où chacun peut ouvrir une " chaîne " de publication ouverte au public, n'est pas filtré par les autorités, contrairement à Twitter ou à Facebook. Les quelque 40 % d'Iraniens ayant accès à Internet peuvent y suivre et commenter la campagne avec une liberté inconnue des médias d'Etat, dans un mélange d'information et de rumeur difficile à démêler.

Selon une étude faite en décembre 2015 par le Centre de sondage des étudiants iraniens, environ 20 millions de personnes disposent d'un compte sur Telegram dans le pays, soit près d'un quart de la population. Tous les sites politiques, une large partie du gouvernement, comme des figures conservatrices, y ont ouvert une chaîne publique. Les candidats méconnus y trouvent un outil de campagne peu coûteux. Le bureau du Guide suprême, l'ayatollah Khamenei, y partage avec ses 225 000 abonnés de courts extraits vidéo de ses discours ou des communiqués - tout comme sur Twitter, malgré l'interdiction du réseau.

Telegram a construit son succès sur sa réputation : celle d'être un service sûr, qui permet de discuter à l'abri des oreilles indiscrètes en chiffrant les messages. Elle a pris la place, dans les téléphones des Iraniens, de l'application Viber.

Une activiste londonienne cibléeLes autorités n'ont pas tardé à réagir. Des politiques et des religieux ont critiqué l'application, l'accusant de propager des contenus " immoraux " , et menaçant de la bloquer. Une tentative lancée le 5 janvier, par la Commission de détermination des cas de contenus criminels - elle décide des sites à bloquer - a échoué, faute d'un nombre suffisant de voix. Ses membres, nommés par le gouvernement, l'autorité judiciaire et des institutions proches d'Ali Khamenei, ont l'application dans le viseur. Le 19 novembre 2015, cette commission tenait une réunion au sujet de Telegram et a décidé d'accorder un délai au ministère des télécommunications pour régler le problème des contenus " immoraux " . " Si Telegram ne prend pas, à court terme, des mesures pour appliquer nos lois, nous devrons la filtrer ", a indiqué son secrétaire, Abdul Samad Khorram Abadi.

A l'automne 2015, les Iraniens ont d'ailleurs cru que la censure avait repris ses droits. Le 20 octobre, l'application était devenue très lente. Deux jours plus tôt, le fondateur et dirigeant russe de Telegram, Pavel Durov, avait indiqué sur Twitter avoir été contacté par les autorités iraniennes, lui demandant de mettre en place des mécanismes de surveillance et de censure. Une demande qu'il a refusée tout net.

Mais une semaine plus tard, le ministre des télécommunications iranien, Mahmoud Vaezi, expliquait lors d'une conférence de presse avec son homologue russe que la " ligne rouge, c'est le respect des questions éthiques. Nous avons averti Telegram, et ils ont filtré les contenus immoraux " . M. Vaezi a attribué les lenteurs de l'application à des problèmes sur les câbles sous-marins connectant l'Iran à Internet. Le 13 janvier, il a indiqué que " Telegram avait donné son accord pour bloquer tous - les comptes publics - désignés par le ministère des communications ".

Le pouvoir iranien a-t-il réussi à mettre la main sur Telegram? Non, a assuré M. Durov. Il explique que sur Telegram, seuls les comptes publics sont soumis à un contrôle, qui ne concerne que la pornographie et le terrorisme, une thématique sensible : l'application est populaire chez les combattants de l'organisation Etat islamique. Telegram n'a que récemment pris des mesures pour perturber cette utilisation, en fermant de nombreuxcomptes appartenant au groupe djihadiste.

Surtout, M. Durov a expliqué n'avoir jamais bloqué de contenu politique ni passé d'accord avec quelque gouvernement que ce soit. Pas suffisant pour dissiper les inquiétudes sur les relations entre Telegram et les autorités. " Beaucoup s'inquiètent d'une possible collaboration entre Telegram et Téhéran pour la censure ", ditNariman Gharib, responsable de la chaîne de télévision Manoto, installée à Londres et bannie comme toute chaîne satellitaire en Iran.

Le pouvoir iranien dispose-t-il d'une porte dérobée lui permettant de pirater l'application? Peu probable : les autorités semblent recourir à d'autres techniques pour parvenir à leurs fins. Lors d'une arrestation, la police a confisqué un ordinateur portable et un téléphone sur lesquels était installé Telegram. Ils ont inspecté les contacts, repéré une activiste installée à Londres, avec laquelle ils ont conversé, se faisant passer, avec succès, pour la personne arrêtée. Pour prendre le contrôle du compte Telegram de l'activiste, les autorités ont demandé une réinitialisation de son mot de passe, la convainquant de leur fournir ce nouveau code, au prétexte de l'ajouter à une discussion de groupe. Le stratagème a

fonctionné. La police a tenté de répliquer cette méthode aux contacts de l'activiste. Mais elle a réussi à reprendre le contrôle de son compte qui aura été, pendant deux heures, aux mains des autorités. Ce scénario semble indiquer que ces dernières ne disposent pas de moyens techniques pour pénétrer à l'intérieur de l'application.

Début novembre 2015, l'agence semi-officielle Fars News, proche des gardiens de la révolution, indiquait que 170 personnes avaient déjà été arrêtées pour avoir partagé des contenus " immoraux " , notamment sur Telegram. Sur les huit derniers mois de 2015, 609 hommes et 114 femmes ont été arrêtés pour des crimes " économiques, moraux et sociaux " commis sur Internet, selon des chiffres officiels cités par l'AFP.

The Australian Financial Review
Corporate networks risk becoming terrorist tools
Tuesday, 01 March 2016
Byline: Aidan Tudehope

Catch a plane to the Middle East and so much as train with a terrorist organisation and you can expect to be sent to a dark place behind bars for a long time the moment you return to Australia.
The community would demand nothing less. But what if your fridge launches an attack on an airliner? Or your corporate network attempts to disrupt a military operation on behalf of a terrorist enemy?

Those scenarios might be extreme, but they are by no means far fetched.

The question is not if, but when, a serious security incident will be launched leveraging inadequately secured corporate networks.

Two years ago, well before the Internet of Things (IoT) had become a mainstream discussion, it was reported that a fridge, along with thousands of internet-connected TVs, had been part of a bot network that launched a distributed-denial-of-service attack.

Opportunities for connected personal and business infrastructure to be secretly "occupied" and used for nefarious purposes are expanding at an explosive rate, as devices are added to the internet at ever greater bandwidth. Inside a medium-sized business there are likely to be hundreds of devices capable of being exploited, and maybe a dozen in a small business - printers, TVs, modems and fridges just for a start.

Further, the standard defence response to an international DDOS attack - "sinking" the unwelcome traffic by diverting it into a series of dead-end destinations - is far less effective against an attack originating within Australia. There are simply fewer safe places to which the traffic can be diverted.

But even as the risk grows day by day, there is still a tendency to see cyber security as a black art. Too many senior managers do not ask the tough, penetrating questions of their technology teams they are expected to ask of experts in other fields, like finance.

If senior managers are looking for an incentive to make cyber security their business, they need only look at US retailer Target, where the loss of credit card details of 40 million customers cost the chief executive and chief information officer their jobs.

A limited subset of the business community are treating cyber security with the appropriate gravity - typically Australia's largest companies and financial institutions. The picture elsewhere is much more mixed.

Ignorance is not an excuse in the law, but there has to date been a reasonably generous attitude from lawmakers when it comes to cyber security.

The room for ignorance will be much narrower when the federal government releases its new national cyber security statement in coming weeks.

The statement is expected to highlight the importance of a few protective measures that, properly implemented, prevent the majority of common attacks and security breaches.

It is no accident that these are described as "hygiene" measures - they really should be as basic as a food service business requiring staff to wash their hands, or for a car company meeting minimum quality and safety standards.

The government's initiatives are likely to take the form of helpful advice and guidance, and some tools for businesses to lift their security stance, rather than introducing punitive measures for poor performance. It is also expected to leverage the work that the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) has done in helping the government protect itself better from cyber attack.

Aidan Tudehope is managing director of government and hosting at Macquarie Telecom and was a member of the Prime Minister's cyber security business roundtable process.

Le Monde
La contre-attaque d'Apple face au FBI
Tuesday, 01 March 2016
Byline: Damien Leloup

Washington - La firme, qui s'oppose aux exigences du service fédéral, prépare une riposte juridique et technologique

Tim Cook, le PDG d'Apple, avait annoncé qu'il contesterait les demandes du FBI - le service fédéral américain de police judiciaire et de renseignement intérieur - par tous les moyens possibles, y compris en allant jusqu'à la Cour suprême des Etats-Unis. L'entreprise a rempli, jeudi 25 février, la première étape, en introduisant un recours formel contre la demande qui lui est faite de fournir au FBI un " outil de déverrouillage " qui permettrait " d'ouvrir " un iPhone chiffré ayant appartenu à l'un des terroristes ayant commis l'attentat de San Bernardino (Californie), le 2 décembre 2015. Ce jour-là, quatorze personnes ont été tuées par deux assaillants.

Dans un document communiqué à la justice vingt-quatre heures avant la fin de l'ultimatum fixé par un tribunal à Apple pour fournir ledit outil au FBI, les avocats de l'entreprise ont donné une série d'arguments, justifiant la position de la firme à la pomme. La plupart portent sur des points de jurisprudence et tentent de montrer que la demande des enquêteurs impose une contrainte déraisonnable, et que la création d'un tel outil de déverrouillage représenterait un danger pour la vie privée des utilisateurs d'iPhone. Ils relèvent, au passage, que le FBI n'a apporté aucune preuve que le téléphone pouvait contenir des éléments nécessaires à l'enquête, et que les enquêteurs ont eux-mêmes bloqué l'avancée de l'enquête en changeant - par erreur ou volontairement - le mot de passe iCloud de l'appareil, le service de sauvegarde en ligne d'Apple.

Mais les avocats de la firme de Cupertino (Californie) ont aussi mis en avant un argument massue : le code informatique, estiment-ils, est une forme d'expression écrite. En tant que tel, il est protégé par le premier amendement de la Constitution américaine qui consacre la liberté d'expression, et le FBI ne peut contraindre l'entreprise à " s'exprimer " en produisant un logiciel contre sa volonté, expliquent-ils.

Cet argument, s'il venait à être validé par les tribunaux américains, pourrait avoir de profondes répercussions sur des centaines d'autres affaires. Mais la jurisprudence actuelle ne penche pas, sur ce point, en faveur d'Apple. Dans les procédures, le géant américain pourra toutefois compter sur le soutien de plusieurs de ses rivaux. Google, Microsoft, ou Facebook ont annoncé qu'ils déposeraient, dans la première semaine de mars, une motion de soutien à la société fondée par Steve Jobs auprès du tribunal.

Fermer la " porte " d'iCloudSans attendre les résultats de son recours, Apple a lancé une autre contre-attaque, sur le plan technologique cette fois. Le groupe a commencé à travailler sur des mises à jour de sécurité qui rendraient inopérantes de futures demandes du FBI. Jusqu'à présent, l'entreprise acceptait, sur présentation d'un mandat d'un juge, de fournir aux enquêteurs américains des copies de fichiers iCloud, son système de sauvegarde de documents en ligne.

Mais selon les informations du Financial Times , Apple cherche à mettre en place un système de protection similaire à celui utilisé pour chiffrer le contenu de ses téléphones. Depuis les dernières mises à jour de son système d'exploitation iOS, le contenu chiffré n'est déverrouillable que par le propriétaire de l'appareil, qui est le seul à en connaître le mot de passe - Apple ne peut ni le communiquer à un tiers ni en décrypter le contenu.

Dans plusieurs enquêtes, les forces de l'ordre américaines ont utilisé le système de sauvegarde iCloud pour contourner ce verrouillage : quand le propriétaire laisse la synchronisation des données activées, il n'y a pas besoin de déverrouiller le téléphone, puisqu'une copie des photos et des autres documents présents sur l'appareil est transférée automatiquement sur les serveurs d'Apple. La fermeture de cette " porte " s'apparenterait à une nouvelle déclaration de guerre au FBI, et le début d'une seconde course aux armements technologique et judiciaire.

De son côté, le FBI et son patron, James Comey, ainsi que plusieurs figures politiques ont multiplié les déclarations appelant le Congrès américain à se saisir du dossier. Les demandes d'accès du service fédéral de police judiciaire sont en effet dans une zone grise juridique - aux Etats-Unis, la loi encadre les obligations des opérateurs de téléphonie et des fournisseurs d'accès à Internet, mais elle est vague en ce qui concerne les informations que les forces de l'ordre peuvent collecter auprès des constructeurs informatiques.

Engagés dans la campagne pour les primaires, les politiques n'ont pas manqué de prendre position dans la controverse qui oppose le FBI à Apple. Les principaux candidats à l'investiture républicaine ont tous, à des degrés divers, exprimé leur soutien aux enquêteurs. Côté démocrate, Hillary Clinton, qui fait la course en tête, a refusé de prendre position tandis que son rival, Bernie Sanders, a renvoyé dos à dos le " Big Brother " étatique et celui des " multinationales ". Mais la longue bataille qui s'annonce devant les tribunaux laisse présager que le futur Congrès américain devra s'emparer du sujet sous peine de blocage.

Le Temps (Suisse)
Un nouvel accord recadre l'espionnage américain
Tuesday, 01 March 2016
Byline: Ram Etwareea

Bruxelles - Protection de données
Les citoyens européens obtiennent de nombreuses garanties et diverses possibilités pour faire recours s'ils s'estiment lésés par des services de renseignement ou des entreprises américains

« Safe Harbour », le règlement transatlantique en matière de transmission et de protection des données, est mort. Vive « Privacy Shield », qui entrera en vigueur dès qu'il aura obtenu le feu vert des vingthuit Etats membres de l'Union européenne (UE) ainsi que celui du Parlement européen. En gros, les Etats-Unis promettent de moins espionner les citoyens européens. « Notre objectif est d'assurer la protection des droits fondamentaux de nos citoyens et d'apporter une sécurité juridique à nos entreprises », a expliqué lundi un haut fonctionnaire européen. Du côté des Etats-Unis, le président Barack Obama a signé la semaine dernière le Judicial Redress Act qui accorde aux Européens les mêmes droits qu'aux Américains en matière de protection des données.

Programme américain d'espionnage à grande échelle

Pour rappel, tout avait commencé en 2012 lorsque le lanceur d'alerte américain Edward Snowden avait révélé que la National Security Agency (NSA) américaine avait un programme à grande échelle dit « Prism » pour espionner les courriels des citoyens et même des dirigeants politiques européens.

Même les communications de la chancelière allemande Angela Merkel étaient interceptées par les services de renseignement, ce qui avait choqué beaucoup d'Européens. Dans un acte de contrition, le président américain avait signé en janvier 2014 un décret qui limitait la collecte d'informations sur des citoyens non-américains seulement en cas de risques liés à l'espionnage, au terrorisme, à l'usage des armes de destruction massive ou encore aux menaces contre les forces armées américaines.

Course contre la montre pour combler le vide juridique

Mais en Europe, des revendications pour une meilleure protection des données n'ont pas cessé. C'est un procès gagné par un citoyen autrichien auprès de la Cour de justice de l'UE en octobre dernier qui a conduit à l'invalidation du « Safe Harbour » . Dès lors, l'UE et les Etats-Unis se sont engagés dans une course contre la monte pour combler le vide juridique.

« Il ne sera désormais plus possible de transférer ou de stocker les données de nos citoyens et de nos entreprises de façon illégale », a poursuivi le spécialiste européen. C'est un fait que les consommateurs fournissent beaucoup d'informations personnelles lors d'une souscription, d'un achat ou encore d'une réservation en ligne d'un billet d'avion ou d'un hôtel sur des sites internet comme Hotel.com, Google, Yahoo, WhatsAppp ou Facebook. Les entreprises technologiques américaines ont montré de l'empressement pour trouver un nouvel accord. En janvier dernier, elles ont tiré la sonnette d'alarme, disant qu'un échec pourrait empêcher certaines d'entre elles de travailler en Europe.

Voies de recours

Sous « Privacy Shield », les Etats-Unis garantissent formellement que l'accès aux informations à des fins de sécurité nationale sera subordonné à des critères bien définis. Pour la première fois, les citoyens européens disposeront de voies de recours à divers niveaux. « Les Etats-Unis ne se livreront plus à des surveillances de masse à l'égard des Européens », a rassuré le haut fonctionnaire. Le nouvel instrument prévoit un ombudsman indépendant de la NSA qui recueillera les plaintes. Les plaignants obtiendront les réponses dans un délai maximal de 45 jours. En cas de non-satisfaction, ils pourront se référer à un tribunal d'arbitrage.

Lorsqu'il s'agit de plaintes visant les agissements d'entreprises, « Privacy Shield » préconise que ces dernières adoptent d'abord un code de bonnes pratiques. Ensuite, en cas de plaintes, elles doivent réagir dans un délai de 45 jours. Les Européens se sentant lésés peuvent aussi référer leur cas au Département américain du commerce qui a l'obligation d'apporter une réponse dans un délai de 90 jours. Pour les cas non résolus, l'accord prévoit également un tribunal d'arbitrage ayant le pouvoir de convoquer les entreprises.

De son côté, l'UE tiendra une consultation annuelle avec les organisations non gouvernementales actives dans ce domaine. Un rapport annuel sera également soumis au Conseil et au Parlement européens.

« Il ne sera désormais plus possible de transférer ou de stocker les données de nos citoyens et de nos entreprises de façon illégale »

The Local (Norway)
China stealing military information from Norway
Monday, 29 February 2016
Byline: Staff report

Oslo - In its annual threat assessment, the Norwegian Intelligence Service, reports The Local, said that both Russia and China present security challenges to Norway and that Beijing has most likely stolen military intelligence from Norwegian companies.
While much of the NIS report - like that of the threat assessment released by the Norwegian Police Security Service (PST) earlier this month - focused on the dangers posed by Russian spies, it also revealed that China has stolen information from Norwegian weapons companies.

"We believe that they [China, ed.] have succeeded in extracting information that they are using in their own weapons technology," NIS head Morten Haga Lunde told TV2.

The NIS report calls Russia and China "the most active players behind network-based intelligence operations aimed at Norway" and said that both nations "have high competencies and show a high degree of assertiveness in their approach to Norwegian goals".

Lunde told TV2 that China is targeting Norwegian companies as part of a global strategy to obtain valuable technological information.

"First and foremost as we say in the report, we can see that China is inside and operating within Norwegian networks to obtain information that it can use in its own technological development," he said.

Lunde stressed that Chinese espionage wasn't only aimed at Norway but is a "global challenge".

Norway's southern neighbour Denmark saw its domestic defence industry successfully hacked for years by a foreign operator, widely believed to be China. Between 2008 and 2012, an advanced cyber attack was carried out on the IT systems of at least five Danish defence companies, including it's largest weapons company.

Reuters
Major powers team up to tell China of concerns over new laws (Canada)
Tuesday, 01 March 2016

The United States, Canada, Germany, Japan and the European Union have written to China to express concern over three new or planned laws, including one on counterterrorism, in a rare joint bid to pressure Beijing into taking their objections seriously.
The U.S., Canadian, German and Japanese ambassadors signed a letter dated Jan. 27 addressed to State Councilor and Minister of Public Security Guo Shengkun, voicing unease about the new counterterrorism law, the draft cyber security law, and a draft law on management of foreign non-governmental organisations (NGOs).

In what sources said was a coordinated move, the ambassador of the European Union Delegation to China, Hans Dietmar Schweisgut, sent a letter expressing similar concerns, dated Jan. 28.

Reuters reviewed copies of both letters.

The cyber security and counterterrorism laws codify sweeping powers for the government to combat perceived threats, from widespread censorship to heightened control over certain technologies.

Critics of the counterterrorism legislation, for one, say that it could be interpreted in such a way that even non-violent dissidents could fall within its definition of terrorism.

The four ambassadors said areas of the counterterrorism law, which the National People's Congress passed in December, were vague and could create a "climate of uncertainty" among investors. They did not specify which areas.

The EU ambassador used the same phrase to describe the law's impact, and both letters expressed an interest in engaging with China as it worked out implementing regulations around the law, to try to mitigate those concerns.

Guo could not be reached for comment. China's State Council Information Office, Ministry of Public Security and Foreign Ministry did not immediately respond to requests for comment.

While countries often give feedback on proposed legislation in China, the rare joint response by several major powers, and coordination with the EU, signals an increased readiness to lend weight of numbers to their argument.

It also points to growing frustration that the low-key, individual approach taken in the past may not be working.

"While we recognize the need for each country to address its security concerns, we believe the new legislative measures have the potential to impede commerce, stifle innovation, and infringe on China's obligation to protect human rights in accordance with international law," said a strongly-worded letter co-signed by the four ambassadors.

China has defended the new and draft laws, saying such steps, including heightened censorship, were necessary to ensure stability in the country of over 1.3 billion people.

'CLIMATE OF UNCERTAINTY'

The diplomatic push comes as Beijing arguably needs cooperation from the signatories to the letters more than ever.

A slowing Chinese economy and fragile markets highlight the importance of foreign investors' confidence.

Chinese companies are increasingly looking to get approvals from foreign governments for acquisitions, and the European Union is debating whether to give China "market economy" status.

On the draft cyber security law, all five ambassadors were particularly concerned by provisions requiring companies to store data locally and to provide encryption keys, which technology firms worried may impinge on privacy and mean they would have to pass on sensitive intellectual property to the government in the name of security.

Both letters said the draft NGO management law had the potential to hinder academic exchanges and commercial activities, calling them "crucial elements" of their relationships with China.

Critics have said the draft legislation risked choking off NGOs' work by requiring them to get official sponsors and giving broad powers to police to regulate their activities.

In the letters, the ambassadors asked China to open both draft laws to another round of public consultations.

The U.S. and Canadian embassies in Beijing did not immediately respond to requests for comment for this article. A spokesman for the EU Delegation had no comment when reached by Reuters.

German embassy spokesman Nikolas Bader said: "The Embassy does not comment on the letter. But we are clearly concerned about these issues and have repeatedly raised them in the past."

The Japanese embassy said: "We pay attention to Chinese movement over relevant laws or drafts of laws."

The parties to the letters decided to express their concerns together after it became unclear to what degree China was taking their individual input on the laws on board, said a person with knowledge of the matter.

"We're trying to avoid the divide and conquer approach (by China). They like to do that on any possible occasion. We wanted to send a counter- signal that when we have shared interests, we cannot so easily be split," the person said, adding that there had been no clear response by China so far to the letters.

"We don't plan to establish a pen-pal relationship. We want something to happen."

Wall Street Journal

Apple Is Right on Encryption

Wednesday, 02 March 2016

Byline: Editorial Board

Section: editorial

Editorial - The Apple encryption conflict has turned nasty, as the Obama Administration, most Republicans and public opinion turn against the tech company. But, lo, Apple won its first court test on Monday, and its legal briefs against the court order to unlock an iPhone used by the San Bernardino jihadists show it has a better argument than the government.

The FBI is attempting to extract information on Syed Rizwan Farook's device but has been frustrated by Apple's encryption. So a California magistrate ordered the company to design a custom version of its operating software that will disable certain security features and permit the FBI to break the password. Apple has cooperated with the probe but argues that forcing it to write new code is illegal.

One confusion promoted by the FBI is that its order is merely a run-of-the-mill search warrant. This is false. The FBI is invoking the 1789 All Writs Act, an otherwise unremarkable law that grants judges the authority to enforce their orders as "necessary or appropriate." The problem is that the All Writs Act is not a catch-all license for anything judges want to do. They can only exercise powers that Congress has granted them.

Congress knows how to require private companies to serve public needs. The law obligates telecoms, for example, to assist with surveillance collection. But Congress has never said the courts can commandeer companies to provide digital forensics or devise programs it would be theoretically useful for the FBI to have -- even if they are "necessary" for a search.

Congress could instruct tech makers from now on to build "back doors" into their devices for law-enforcement use, for better or more likely worse. But this back-door debate has raged for two years. In the absence of congressional action, the courts can't now appoint themselves as a super legislature to commandeer innocent third parties ex post facto.

What makes the FBI's request so extraordinary is that the iPhone encryption and security methods were legal when they were created and still are. Apple has no more connection to the data on Farook's phone than Ford does to a bank robber who uses an F-150 as a getaway vehicle.

If the government can compel a manufacturer to invent intellectual property that does not exist in order to invade its own lawful products, then there is no limiting legal principle. Could the FBI require a tech maker, for example, to send a malware worm to a user's device in the form of a routine update?

The other myth is that Apple is merely being asked to crack "one phone in the entire world," as Marco Rubio puts it. This is also false. The Justice Department is beseeching Apple to provide software retrofits in at least a dozen public cases, and state and local prosecutors have stacks of backlogged iPhones they want unlocked too. In the New York case Apple won this week, prosecutors want Apple to unlock an iPhone even though the owner has pleaded guilty.

If Apple now writes the program the G-men desire, then the technique will be used in investigations that have nothing to do with terrorism as other prosecutors use the same argument. This is the back door by degrees that Apple CEO Tim Cook describes.

FBI director James Comey told Congress last week that the Apple case was "unlikely to be a trailblazer" and that it also would be "instructive for other courts." Well, which is it? This contradiction isn't the only reason to wonder if Mr. Comey prefers an encryption legal precedent over Farook's actual data.

One question is why the phone wasn't immediately shipped in a faraday bag to Fort Meade. The NationalSecurity Agency has a formidable decryption unit, and U.S. spooks probably have the ability to hack Farook's phone without Apple's services, especially because it is an older, less sophisticated model.

We bow to no one in defense of antiterror programs whose political popularity waxes and wanes, especially on surveillance. But this case isn't about "privacy." This is about engineering security and its implications for the security of all Americans.

Back doors are engineering vulnerabilities that make devices less secure. But terrorists and criminals will always be able to find some underground encrypted communication channel, so regulating back doors into legal devices achieves little national-security benefit. To borrow a line from James Burnham, if there's no alternative, there's no problem.

If Congress is really going to outlaw stronger encryption for law-abiding Americans, well, the political class has the right to make mistakes. But it would be a far more dangerous precedent for the courts to do so without guidance from Capitol Hill.

Mr. Comey may be leading the government to defeat, which makes the White House's incoherence -- backing this unnecessary showdown while claiming to oppose back doors -- all the stranger. If this debate really is critical to protecting public safety, then Mr. Comey should appeal to Congress to change the law, rather than insist that the courts should resolve a major policy dispute in his favor.

New York Times

Tracking Devices in Teeth, and Other Bin Laden Worries

Wednesday, 02 March 2016

Byline: Matthew Rosenberg

Section: general

Washington - American drones were devastating the upper ranks of Al Qaeda, his men were killing suspected spies, and Osama bin Laden wondered: Could an Iranian dentist have planted a tracking device in his wife's tooth?
"The size of the chip is about the length of a grain of wheat and the width of a fine piece of vermicelli," he wrote, using the nom de guerre Abu Abdallah.

A few paragraphs later, Bin Laden signed off and then added, "Please destroy this letter after reading it."

The letter was among thousands of pages of documents and other materials seized by Navy SEALs during the raid on Bin Laden's compound in Abbottabad, Pakistan, in May 2011, and it was declassified on Tuesday with 112 other pieces of writings and letters found in the Qaeda leader's hide-out.

American officials have said that the intelligence seized by the SEALs during the raid included letters, spreadsheets, books and pornography. Yet only a fraction of the materials have been made public -- Tuesday's release was the second set of documents from the raid to be declassified -- and experts have cautioned against drawing broad conclusions until there is more.

The bulk of the materials released Tuesday come from the last decade of Bin Laden's life, and include letters to lieutenants and loved ones, drafts of speeches he was preparing to release and stray bits of operational minutiae. Though there do not appear to be any major revelations, the materials provide a glimpse of Bin Laden's thinking and his struggle to keep Al Qaeda's main branch and its offshoots in line as American drones killed the group's senior leaders and demoralized its foot soldiers.

An undated will that Bin Laden is believed to have written by hand in the late 1990s was included in the documents released on Tuesday.

In it, Bin Laden reviewed his finances, saying he had received $12 million from one of his brothers and that he had $29 million in Sudan, where he lived from 1991 to 1996. If he was killed, he wrote, he hoped his family would "spend all the money that I have left in Sudan on Jihad."

A senior intelligence official, who the Central Intelligence Agency insisted speak on the condition of anonymity, said the agency did not know what became of the money, or if any of it remained at the time of Bin Laden's death. But the will, the official said, was probably important to Bin Laden, because he carried it with him for years.

The fixation on the possibility of his own premature death, and the fear of the American efforts to track him and kill him, is a theme that surfaces again and again. In one letter, Bin Laden warns that a suitcase used to deliver a ransom could contain a tracking device.

Even people presenting themselves as friends were not trusted. In another letter, which does not appear to have been written by Bin Laden, the author relates that a Qatari diplomat visited Qaeda members in Jalalabad, Afghanistan, and brought gifts, including a "huge" watch.

But after the diplomat left, a militant identified by the pseudonym Abu Umamah took the watch and "smashed it with a hammer" because he was afraid of it.

The latest documents include new details of Bin Laden's apparent struggle to impose bureaucratic uniformity across his terrorist network, including an educational syllabus for new fighters.

Titled a "Course of Islamic Study for Soldiers and Members," it includes a list of subjects and skills to be taught. (No. 1 is reading and writing.) There is also a reading list of mostly books about Islam as well as lectures ranging from the history of jihad in the Horn of Africa to "a brief word on raising children."

Bin Laden, who considered himself a student of history, tended to view events through a conspiratorial lens that often distorted his conclusions. The documents made clear, for example, that he believed the West, and the United States in particular, was controlled by a Jewish cabal.

But Bin Laden did not reject all things Western. One document released on Tuesday outlines the structure of a "chief of staff committee" replicating the structure of a military command staff that originated in 19th century France and is now used by almost all North Atlantic Treaty Organization members, including the United States.

The various branches of the staff are laid out numerically, much like the Pentagon. No. 1 is personnel, No. 2 is intelligence and No. 3 is operations. No. 4 is logistics, or what the Qaeda document calls its "provisions and supplies wing." The unidentified author added Al Qaeda's own No. 5 role, which could be translated as a morals branch.

The intelligence officials could not say whether the group ever tried to put the command staff structure into practice.

Tuesday's release was at the insistence of Congress, which in 2014 directed the Office of the Director of National Intelligence to review the material seized in the raid and make as much of it public as possible.

It has been a slow process. The review began in May 2014, and the first release, which included nearly 80 documents, books, news media clippings and other materials, did not occur until May 2015.

Most of the documents released in 2015 were notes from Bin Laden and his top deputies, and they suggested that the Qaeda leader spent his final years seeking to direct a terrorist network that appeared to have grown far beyond his control. There was talk of training recruits and of how to select the most talented to carry out major attacks in the West. There were discussions of whom to promote and how to deal with the group's franchises in the Middle East and North Africa.

In the 2015 release, the intelligence director's office also made public a list of books found in the compound. There were sober works of history and current affairs, such as "Obama's Wars," by Bob Woodward, and wild conspiracy theories, like "The Secrets of the Federal Reserve," by Eustace Mullins, a Holocaust denier.

Then there was the application for new Qaeda recruits, which was perhaps the oddest find in the first set of declassified materials. The application blended the mundanely bureaucratic with the frighteningly absurd, asking questions like "Do you wish to execute a suicide operation?" and "Who should we contact in case you become a martyr?"

Whether it was ever used is a question that American officials have not answered.

New York Times

Brazilian Police Arrest a Facebook Executive in a WhatsApp Data Access Case

Wednesday, 02 March 2016

Byline: Vinod Sreeharsha, Mike Isaac

Section: general

Rio de Janeiro - Brazilian federal police arrested a Facebook executive on Tuesday after the company failed to turn over information from a WhatsApp messaging account that a judge had requested for a drug trafficking investigation.
Diego Dzodan, a Facebook vice president, was taken into custody, or what Brazilian authorities call "preventive prison," which is often less than a week but can be extended, federal police said in a statement.

The arrest was made because of Facebook "repeatedly failing to comply with judicial orders," according to the statement. "The information was required to be utilized in an investigation of organized crime and drug trafficking."

WhatsApp is owned by Facebook.

No other details were provided. The criminal case was filed in a court in the northeastern state of Sergipe.

The arrest comes as a debate over the access that law enforcement officials should get to tech companies' data has escalated. In the United States, Apple is in a fight with the government over whether to build a special tool to help law enforcement break into an iPhone used by one of the attackers in a mass shooting in San Bernardino, Calif., last year.

In Brazil, Facebook has run into other hurdles with authorities in recent months over access to its information. Tuesday's arrest comes less than three months after another judge ordered a temporary shutdown of WhatsApp in a similar case. An appeals court quickly overruled the shutdown.

The drug trafficking case that led to Tuesday's arrest is a separate case, according to a spokeswoman at the courthouse in Sergipe. The Sergipe court said in a statement that it had given Facebook three previous chances to provide the information. Yet the issue echoes past instances, with Brazilian police and authorities contending that they should be able to access information in such investigations.

Facebook's chief executive, Mark Zuckerberg, has long considered Brazil a crucial market and previously praised its Internet governance. He was one of a small group of Silicon Valley executives who met with President Dilma Rousseff of Brazil in a private meeting at Stanford University last July, according to individuals who attended.

Facebook on Tuesday said it was "disappointed with the extreme and disproportionate measure of having a Facebook executive escorted to a police station in connection with a case involving WhatsApp."

The company added, "Facebook has always been and will be available to address any questions Brazilian authorities may have."

It is unclear if the information that Brazilian authorities are seeking in the drug case in Sergipe can even be provided as WhatsApp does not store users' messages. It also increasingly has end-to-end encryption.

WhatsApp said in a statement that it disagreed with the Brazilian authorities on the case. "We are disappointed that law enforcement took this extreme step," the messaging business said. "WhatsApp cannot provide information we do not have."

USA Today

Cyber security execs firm in defense of Apple

Wednesday, 02 March 2016

Byline: Elizabeth Weise

Section: general

San Francisco - The cybersecurity industry came out swinging Tuesday in favor of Apple in its fight against the FBI's demand that it build a backdoor into an iPhone operating system.
"The path to hell starts at the backdoor, and we need to make sure that encryption technology remains strong," Microsoft President Brad Smith told a packed ballroom as the RSA computer security conference began here.

More than 40,000 people from across the globe are attending RSA this week, a record. The issue of Apple and the FBI featured in almost every speaker's remarks during the opening plenaries.

RSA President Amit Yoran began the barrage by saying that weakening encryption is solely for the ease and convenience of law enforcement for pursuing petty criminals.

"No credible terrorists or nation states would ever use technology that is knowingly weakened. However, if we weaken our encryption, you can sure bet that the bad guys will use that and exploit it against us," he said. Such policies will hurt U.S. economic interests and unconscionably undermine those working to protect the digital environment, he said.

His words were being heard not just by cryptographers, computer security companies and programmers but also by Michael Rogers, director of the NationalSecurity Agency, U.S. Secretary of Defense Ashton Carter, U.S. Attorney General Loretta Lynch, members of Congress and national cyber security czars from around the world, he told the audience. All were planning to attend the conference.

That attention wasn't license to go on the attack. "We need to be respectful, but we also must make sure that our voices are heard loud and clear," he said.

The U.S. government realizes how important the field is.

"Cyber is the new black. Everyone cares about it. Every government cares about it," U.S. State Department Coordinator for Cyber Issues Chris Painter said. He won an excellence in public policy award at RSA.

Opposing the FBI's request doesn't mean technology companies don't realize they play a crucial role in security and law enforcement work, Smith said.

After the Paris attacks in November, Microsoft received 14 requests from law enforcement seeking information about terrorist suspects at large in France and Belgium, Smith said. Once the company confirmed they were lawful, the average response time to get the information to law enforcement was 30 minutes, he said. But security doesn't mean allowing unlawful requests.

"We also need to stand up for customers," he said. In the end, "there is no such thing as national security without cyber security. We cannot keep people safe in the real world if we cannot keep people safe on the Internet," he said.

London Times

Intelligent Security

Wednesday, 02 March 2016

Byline: Editorial Board

Section: editorial

Editorial - Britain is not an oppressive nation. Our security services exist to protect citizens and the state, rather than to protect the state from citizens. Terrorism is a great and growing threat to the British people. There is a good deal of evidence that GCHQ, MI5 and MI6 work tirelessly to thwart attacks on British soil and British interests. There is scant evidence, indeed, next to none, that they have worked to the detriment of the population at large. This makes us fortunate. Too few other countries can say the same.
The Investigatory Powers Bill, tabled in parliament yesterday is at its best a forward-thinking attempt to clarify precisely what the security services can, should, and need to do to best fulfil their role. Debates about the balance between privacy and national security may never end, but in the face of terrorist aggression there are strong arguments for prioritising the latter. Electronic communications are a powerful tool in the hands of terrorists. If the security services are powerless to scrutinise them, we all suffer.

The same bill, to put it mildly, is less convincing on the subject of domestic law enforcement. In draft form, published last year, it gave police forces enhanced abilities to hack private communications and to

monitor the web history of the public when investigating "serious crimes". Since then, police lobbying of the home secretary has clearly had an effect. The actual bill provides powers far broader.

Rather than only in the context of "serious crime", hacking powers may now be used for the purpose of "mitigating any injury or damage to a person's physical or mental health". This can be authorised by a chief constable. Moreover, whereas the draft bill allowed police to see when members of the public had accessed a "red-flag" list of websites, including those providing social media, the new bill allows police to see a list of all websites visited. This is too much power, with too little scrutiny, in the hands of people with too poor a track record of trust.

Quite unlike the security services, there is a long and regrettable history of British police exploiting for other purposes powers that were designed to combat serious crime. The existing Regulation of Investigatory Powers Act (Ripa) has been used frequently to expose the sources of journalists reporting on the police themselves, most notoriously in the Metropolitan police's investigation into The Sun newspaper's reporting of the "Plebgate" scandal involving the MP Andrew Mitchell. In 2013 Cumbria police arrested whistleblowers who had leaked details of the local crime commissioner's expenses. The ability to impose police bail has been exploited to allow police to sidestep the rules about how long they can keep people in custody. Even the power of arrest itself has arguably been abused, with police keen to make a public show of activity in high-profile cases, or those involving celebrities.

Britain's security services are known to use their powers discerningly. The same cannot be said about Britain's police. The House of Commons should be wary of gifting them new powers requiring little oversight from anybody other than senior police officers. The home secretary, meanwhile, should not have jeopardised the vital preservation of national security by packaging it alongside new domestic powers that are almost certain to be abused.

Wall Street Journal

FBI: 'Mistake' Made Over iPhone

Wednesday, 02 March 2016

Byline: Devlin Barrett, Daisuke Wakabayashi

Section: general

Washington - James Comey, director of the Federal Bureau of Investigation, conceded Tuesday that a mistake was made in the early days of the investigation into the San Bernardino, Calif., terrorism attack, making it harder to get data from one of the shooters' phones.

Mr. Comey said, however, that even without that error, the government would still need Apple Inc.'s help to open the locked iPhone.

The FBI director's discussion of the San Bernardino case came during a House Judiciary Committee hearing on the issue of encryption -- the subject of a major legal battle between the FBI and Apple about the company's refusal to help investigators open a phone seized in the probe of the California shooting that left 14 dead in December.

The hearing created the unusual spectacle of Mr. Comey, one of the nation's highest-ranking law enforcement officers, squaring off against Bruce Sewell, the top lawyer for Apple, one of the world's most visible technology companies. Mr. Comey testified first, followed by Mr. Sewell.

Apple is fighting a court order to help the FBI bypass the passcode-security measures on the phone used by Syed Rizwan Farook, one of the two assailants. The FBI wants to disable a security feature that erases the phone's memory after 10 failed password attempts.

Apple has argued that if San Bernardino County officials had not reset the cloud storage account connected to that phone, the FBI might have been able to access much more of the data on the phone by connecting the device to the Wi-Fi system in Mr. Farook's apartment.

Mr. Comey conceded Tuesday that there is some truth to that argument, though he noted that even if the account hadn't been reset, the two sides would still be in court.

"There was a mistake made in that 24 hours after the attack, where the county at the FBI's request took steps that made it impossible later to cause the phone to back up to the iCloud," Mr. Comey told the congressional committee. He added, "We would still be in litigation, because there was no way we would have gotten everything off the phone from a backup."

Apple and privacy experts are likely to seize on those comments to make the case that the company shouldn't be forced to compensate for investigators' mistake.

Mr. Sewell said Apple has helped officials and wants to continue to do so, but that the company must draw a line when the government tries to force its employees to weaken the overall security of its products. He took umbrage at Mr. Comey's repeated assertion that Apple's move toward encryption is a marketing decision, rather than a question of principle or technological standards.

"Every time I hear this my blood boils," Mr. Sewell said. "This is not a marketing issue. That's a way of demeaning the other side of the argument."

Mr. Sewell said the company's increasingly tough encryption is designed to improve security against hackers and criminals. "We see ourselves as being in an arm's race" with those trying to steal customers' data, he said.

Manhattan District Attorney Cyrus Vance Jr., who has been outspoken about law enforcement's need to access encrypted devices, said: "We really need Congress to help solve this problem for us."

"Criminals understand that this new operating system provides them with a cloak of secrecy. And they are, ladies and gentlemen, quite literally laughing at us," he said.

Mr. Sewell also told the committee that Apple had not been ordered to help any other country unlock an iPhone, but if the U.S. compels the company to do this "it will be a hot minute before we get those requests from other" nations.

Separately, at a technology conference in San Francisco, Attorney General Loretta Lynch said she was "disappointed" by a federal judge's ruling on Monday in New York that the government can't compel Apple to help investigators extract data from a locked iPhone in a drug probe.

Ms. Lynch said Apple had agreed to help the government in similar instances in the past but pushed back in the New York case. She said she believes technology companies are subject to a "social compact" to comply with the law, but said law enforcement also need to be clear in what data it wants from devices.

In prepared remarks, Ms. Lynch took a conciliatory tone, saying Washington and Silicon Valley should work together. But the subsequent question-and-answer session reflected the tension between Apple and law enforcement. "Do we let one company, no matter how great the company, no matter how beautiful their devices, decide this issue for all of us?" Ms. Lynch asked.

At the congressional hearing, Mr. Comey disputed Apple's argument that forcing it to help open the San Bernardino phone would mean creating software that would weaken security for millions of other phones.

"I have a lot of faith -- maybe I don't know them well enough -- in the company's ability to secure their information," he said. "They are very, very good at protecting their information and their innovation."

Mr. Comey acknowledged that the Justice Department suffered a blow in the New York drug case on Monday, but he predicted the legal fight between the government and Apple would be "bumpy," with dueling rulings. Like Mr. Vance, Mr. Comey said lawmakers ultimately will have to address the broader questions surrounding encryption.

"This collision between public safety and privacy, the courts can't resolve that," he said.

The Justice Department's argument that law enforcement must be able to open phones when it obtains a valid court order was met by skepticism from some lawmakers.

Rep. John Conyers, (D., Mich.), the Judiciary Committee's top Democrat, said he has been reluctant to support the Justice Department and the FBI on the issue. The growth of encryption means "we will all have lockboxes in our lives that only we can open and in which we can store all that is valuable to us," he said. "There are lots of good things about this."

Others were more open to law-enforcement's viewpoint.

"The question for Americans and lawmakers is not whether or not encryption is essential, but instead, whether law enforcement should be granted access to encrypted communications when enforcing the law and pursuing their objectives to keep our citizens safe," said Rep. Robert Goodlatte, (R., Va.), the committee's chairman.

Rep. Trey Gowdy (R., S.C.) said national security concerns should trump privacy worries. "You can go into people's bodies and remove bullets, but you can't look in a dead person's phone," Mr. Gowdy said. "I just find it baffling."

The Register (UK)

NSA boss reveals top 3 security nightmares that keep him awake at night

Wednesday, 02 March 2016

Byline: Iain Thomson

Section: general

San Francisco - Admiral Michael Rogers, head of the NSA and the US Cyber Command, has told delegates during his keynote address at RSA 2016 the three things that keep him awake at night.
His first fear is an online attack against US critical infrastructure, which he said was a matter of when it will happen, not if. Citing the recent Ukrainian power grid hack as an example, Rogers said that the target was an obvious one and security systems in the US national critical infrastructure were not strong enough.

Number two on his insomnia list was data tampering. We're used to data being stolen, he said, or even deleted as in the case of Sony. But if data has been subtly altered rather than stolen, then the results could be severe.

"What happens when attacks are used to manipulate data or some of its products?" he asked the conference. "You can no longer trust the data we are seeing and we are used to just seeing and accepting it."

His third nightmare was down to the actions of non-state terrorist groups changing their use of online resources. At the moment, such groups are using the internet to recruit members, raise funds, and distribute propaganda. But if they go on the offensive against a country, the results are going to be grim.

"What happens when they use cyber for destruction?" he asked. "These groups are not interested in maintaining the status quo, but in tearing it down."

The NSA can't handle all of this itself, he said, and pleaded with the assembled security experts to bring their skills to the government in partnerships. He recognized that the current debate of encryption was harmful and the two sides aren't cooperating with each other.

Rogers, who is on the record as supporting strong crypto, said that he was worried that the encryption arguments have seen both sides of the debate talking at each other, or even not talking at all. But, he suggested, unless we hang together, we shall all hang separately.

Washington Post

Apple's strategy could be risky

Wednesday, 02 March 2016

Byline: Brian Fung

Section: general

Analysis - Apple reiterated its request Tuesday that Congress rule on whether the FBI can force the company to help authorities unlock iPhones in criminal cases.
But relying on Capitol Hill is a risky strategy for Apple. An analysis of voting patterns in major privacy and security legislation over the past two years shows that the company may be facing an uphill battle, especially in the Senate, where lawmakers have consistently voted to empower intelligence officials.

The voting record also reveals that the legislative body has not broken evenly along partisan lines. Democrats are particularly split, analysts say, between more hawkish members and those more aligned with Silicon Valley.

And although some Republicans take the libertarian view that the government should not be able to spy on Americans' technology, many others find themselves drawn toward strong national security arguments.

No-back-doors amendment

In 2014, for instance, several House members proposed an amendment to a yearly defense funding bill that aimed to limit the government's ability to circumvent encryption - the technology that protects digital data from prying eyes. The amendment ultimately was included in the defense authorization bill, which was approved by both chambers and signed into law by President Obama.

Because the defense bill is a vast, sprawling piece of legislation, it is useful to focus on the House vote on whether to include the "no back doors" amendment introduced by Reps. Zoe Lofgren (D-Calif.) and Thomas Massie (R-Ky.). That vote saw House Democrats and Republicans approve the amendment in overwhelming numbers, with the measure passing 293 to 123.

Those who opposed the amendment included the chairman of the House Judiciary Committee, Rep. Bob Goodlatte (R-Va.). Joining him were top GOP members such as then-Majority Leader Eric Cantor (R-Va.) and the top Democrat on the House Intelligence Committee, Rep. C.A. Dutch Ruppersberger (Md.). The Democrat who succeeded Ruppersberger on the committee, Rep. Adam B. Schiff (D-Calif.), also voted no.

The split shows that a vote on the Apple-FBI matter may not come down along party lines. Indeed, some top Democrats are likely to side with the FBI because they have voted with national security interests in the past, said a left-leaning lobbyist who spoke on the condition of anonymity in order to talk more freely.

"It'll be interesting to see what Democrats do," said the lobbyist. "[The Apple-FBI fight] splits us a little bit."

USA Freedom Act

The USA Freedom Act was approved by both the House and Senate last summer. Although it proposed to end the NationalSecurity Agency's practice of collecting millions of Americans' phone records in bulk, it also gave intelligence officials the opportunity to resurrect the program in a different form with greater restrictions.

In the end, the bill passed the Senate by a vote of 67 to 32. The USA Freedom Act is one of the few bills in the recent debate over security and civil liberties that received votes in both chambers, contained comparable language in both and had a recorded vote tally. But its compromise nature makes it hard to draw clear conclusions about why lawmakers voted the way they did.

Looking ahead, expect various House committees to come up with "dueling legislation" on the Apple-FBI battle, said one Republican congressional staffer, who spoke on the condition of anonymity because the discussions are private. The different flavors of these bills could spark a divide among conservatives.

CISA

The Cybersecurity Information Sharing Act is one of the clearest examples of a bill that divided lawmakers on the question of privacy. Widely panned by privacy advocates, CISA drove Sens. Patrick J. Leahy (D-Vt.), Ron Wyden (D- Ore.), Christopher A. Coons (D-Del.), Al Franken (D-Minn.) and Dean Heller (R-Nev.) each to offer changes that were shot down by proponents of the bill, such as Sens. Dianne Feinstein (D-Calif.) and Richard Burr (R- N.C.).

Apple made clear in this case that it disagreed with the legislation. The company told The Washington Post that it did not support CISA days before the Senate approved the bill 67 to 32.

Although the House did not take a recorded vote on CISA - the measure later wound up in a giant budget bill passed by both chambers and signed by Obama - the Senate's decision to overwhelmingly approve a bill that Apple criticized reflects how little its voice shifted the balance.

There are "very few members that you can say are supportive of Apple" specifically, said a former congressional staffer, who spoke on the condition of anonymity in order to talk more freely.

London Times

Bill stretches far and wide

Wednesday, 02 March 2016

Byline: Fiona Hamilton

Section: general

Analysis - This complex bill sets out the powers available to the security services and police to gather and access communications data.
It is an ambitious aim to outline all powers provided to the services in a single piece of legislation.

The government has been accused of disregarding campaigners' concerns over privacy and rushing the Investigatory Powers Bill through, but ministers are hoping that it can grapple with the changing nature of technology, which has meant that many aspects of current legislation are not considered fit for purpose.

Many of these powers have been used for years but were not explicit in law. They include the ability of the security services to harvest private data, known as bulk collection, and hack into phones and computers, known as equipment interference.

The government has insisted that agencies have "never collected data indiscriminately" but the revelation that private data had been harvested for years brought concerns. Campaigners say that their issues have not been addressed.

Encryption, or securing data, is the elephant in the room.

Communications companies will remain obliged to decrypt messages only "so far as is practicable" because the government is powerless to go further.

There is no point in writing a law that it cannot enforce and that cannot compel MAJOR technology companies based in America.

New York Times

Obama Administration Officials Soften Approach at Tech Symposium

Wednesday, 02 March 2016

Byline: Nicole Perlroth

Section: general

San Francisco - Attorney General Loretta E. Lynch joined a parade of Obama administration officials to tech's home turf on Tuesday. Their message: National security depends on the industry's cooperation. The heavyweights from Washington arrived against the backdrop of Apple's fight with the Federal Bureau of Investigation over access to an iPhone and a growing fissure between Washington and Silicon Valley.

The F.B.I. is trying to force Apple to write software to help it break into the phone of one of the gunmen in December's mass shooting in San Bernardino, Calif. The phone is protected by a security scheme that would wipe its data after a series of incorrect password attempts. Apple has so far refused to cooperate, and the company is fighting a court order requiring it to aid investigators.

In a speech Tuesday at the RSA Conference, arguably the world's largest gathering of computer security experts, Ms. Lynch avoided directly addressing the fight with Apple, and emphasized the need to find middle ground.

"I know that neither our technology companies nor their leaders have any sympathy for terrorists or criminals who target Americans," Ms. Lynch told an audience at the city's Moscone Center. "And the Department of Justice will never sacrifice the safety of the American people or the ideals we all cherish."

But in a stage interview with a Bloomberg journalist, Emily Chang, after her speech, Ms. Lynch was asked what the middle ground would be between the F.B.I. and Apple.

"For me, the middle ground" is to do "what the law requires," Ms. Lynch responded, which drew a smattering of laughter and hisses from the audience. She said law enforcement has for years had Apple's help getting access to iPhones without controversy, and that "having the inability to obtain evidence that could save lives is a real risk."

Though it is focused on a tough password mechanism, the Apple controversy is an extension of a decades-long fight between the tech industry and the federal government over the use of encryption technology. Once considered a carefully regulated munition, not unlike a tank, encryption came into wide use with the advent of the commercial Internet and was the key to modern e-commerce.

The encryption fight was considered by many in Silicon Valley to have been settled in the 1990s, but the widespread government monitoring of Internet traffic revealed in documents released by Edward J. Snowden, the former government contractor, in 2013 led to the renewal of industry efforts to toughen security.

Apple's fight with the F.B.I. has added to that tension, and a number of other tech companies are expected in the coming days to file court briefs in support of Apple. Among their fears is that creating the software to break into the iPhone could create a backdoor that could be used repeatedly by law enforcement or the spy agencies of other countries.

The director of the NationalSecurity Agency, Admiral Michael S. Rogers, also attempted a conciliatory tone at the RSA event. Admiral Rogers did not speak to the Apple case, or even mention the word encryption, but repeatedly emphasized the need for partnership and dialogue to fight cyberthreats. "I implore all of us to be part of that constructive dialogue," he said. "It's time to stop talking past each other."

In a speech made nearby at San Francisco's Commonwealth Club, Defense Secretary Ashton B. Carter acknowledged that encryption had been a "hot topic here in the Bay Area," but said he could not address the Apple case because of the ongoing litigation. Instead, he noted that the Pentagon had a vested interest in strong encryption and that the Defense Department is "the largest user of encryption in the world."

Security experts in the tech industry may not be so quick to embrace conciliation. "You're opening a can of worms," Ron Rivest, a cryptographer and professor at the Massachusetts Institute of Technology, told a separate RSA audience.

"The systems we have are so fragile that trying to have extra keys, or extra ways in, or ways to take them apart is asking for all kinds of trouble," Mr. Rivest said. "The good of the country depends on having strong security."

Other cryptographers on the panel with Mr. Rivest agreed, with one notable exception: Adi Shamir, an Israeli cryptographer and co-inventor, with Mr. Rivest and Len Adleman, of the RSA encryption algorithm that became the namesake of the annual security conference.

Mr. Shamir argued that Apple had "goofed" by not complying in the San Bernardino case and for not anticipating that the F.B.I. would ask for help to crack the shooter's iPhone password.

"Even though Apple helped in countless numbers of previous cases, they decided not to comply this time," Mr. Shamir said. "My advice would have been, comply this time, and wait for a better test case when the case is not so clearly in favor of the F.B.I."

Wall Street Journal

Apple Fight Pushes Judges Into New Role --- Magistrate judges are helping shape boundaries between technology and law

Wednesday, 02 March 2016

Byline: Nicole Hong

Section: general

New York - The fight over smartphone encryption is shining a spotlight on federal magistrate judges, low-level jurists who have become influential in shaping unsettled areas of privacy and surveillance law. Two weeks ago, it was a magistrate judge's order in California that ignited a national debate over the legal boundaries between law enforcement and technology.

At issue in the case: whether the government can use an 18th century law to compel Apple Inc. to help unlock a cellphone used by a shooter in the San Bernardino, Calif., attack. U.S. Magistrate Judge Sheri

Pym sided with the government, prompting strong opposition from Apple and other tech companies. The iPhone maker filed papers last week appealing the decision.

But on Monday, U.S. Magistrate Judge James Orenstein sided with Apple in a drug case in Brooklyn, N.Y., saying the 18th century All Writ's Act doesn't give the government the authority to force Apple to extract data from a locked phone.

The rulings have put the lowest level of the federal judiciary in the center of one of the most sensitive policy debates facing the U.S.: where to draw the line between privacy and national security. The discussion is likely to reach the highest courts and lawmakers.

Magistrate judges are generally responsible for pretrial matters such as initial court appearances for criminal defendants and government applications for search warrants.

But magistrate judges are at the forefront of interpreting an area of law with little precedent, especially as it relates to the use of new technologies and investigative tools by the government. Magistrate judges have been the first to reason through the legality of computer- hacking by the government, as well as the use of stingrays, a cellphone- tracking tool often used without a search warrant. Routine surveillance requests from the government increasingly carry constitutional implications around privacy, former government officials say.

The situation "is very unusual," said Michael Vatis, a former official at the Justice Department and Federal Bureau of Investigation, now a partner at Steptoe & Johnson LLP. Magistrate judges are "not generally trying to set important precedents."

The magistrate position was created by Congress in 1968 to relieve the congestion on federal court dockets. The nation's 500 or so full-time magistrate judges serve eight-year terms that can be renewed.

Aspiring magistrate judges, who are often former federal prosecutors, must apply for the position and are chosen by a selection committee in each district court. The current annual salary is $186,852.

Data on magistrates' decisions are hard to come by. Most aren't public; government applications for search warrants or surveillance are almost always under seal so the target isn't tipped off. Former government officials say magistrate judges historically have granted the bulk of applications by the government. Such applications are typically unopposed, and the government often presents magistrates with enough evidence for "probable cause," the legal standard needed to grant the request. Magistrate judges also may fear running afoul of the government that would be nominating them for a promotion, say legal experts.

However, in 2005, U.S. Magistrate Judge Stephen Smith in Texas denied a government request to track a cellphone's location without a search warrant. The ruling paved the way for denials by other magistrates

and set off what has been dubbed the "magistrates' revolt," involving a handful of judges, including Judge Orenstein, who have been vocal in questioning the constitutionality of government applications.

"Magistrate judges are uniquely positioned to see this increasing use of technology by law enforcement," said Andrew Crocker, a staff attorney at the Electronic Frontier Foundation, a nonprofit privacy organization. "They're on the front lines, and they're asking questions."

Legal experts say because the rulings are usually secret, it is difficult to know whether the revolt is gathering or losing steam. Aside from Judge Pym's ruling, U.S. Magistrate Judge Gabriel Gorenstein in Manhattan, N.Y., granted the government's request in 2014 to compel an unnamed phone maker to unlock a cellphone during a credit-card fraud investigation.

Because of the renewed attention to these types of government requests, experts say magistrates are likely to give more scrutiny to routine applications -- and reach out for help among colleagues.

Jenny Durkan, a former Seattle U.S. attorney who is a partner at Quinn Emanuel Urquhart & Sullivan LLP, said while magistrate judges may be shaping the debate in the short term, the ultimate arbiter of these issues may be the Supreme Court or Congress.

In his order on Monday, Judge Orenstein said the debate "must take place among legislators who are equipped to consider the technological and cultural realities of a world their predecessors could not begin to conceive."

New York Times

F.B.I. Error Led to Loss of Data in Rampage

Wednesday, 02 March 2016

Byline: Ceciilia Kang, Eric Lichtblau

Section: general

Washington - The head of the F.B.I. acknowledged on Tuesday that his agency lost a chance to capture data from the iPhone used by one of the San Bernardino attackers when it ordered that his password to the online storage service iCloud be reset shortly after the rampage.
"There was a mistake made in the 24 hours after the attack," James B. Comey Jr., the director of the F.B.I., told lawmakers at a hearing on the government's attempt to force Apple to help "unlock" the iPhone.

F.B.I. personnel apparently believed that by resetting the iCloud password, they could get access to information stored on the iPhone. Instead, the change had the opposite effect -- locking them out and eliminating other means of getting in.

The iPhone used by Syed Rizwan Farook, one of the assailants in the Dec. 2 attack in which 14 people were killed, is at the center of a fierce legal and political fight over the balance between national security and consumer privacy. Many lawmakers at Tuesday's hearing of the House Judiciary Committee seemed torn over where to draw the line.

"The big question for our country is how much privacy are we going to give up in the name of security," Representative Jason Chaffetz, a Utah Republican, told Mr. Comey. "And there's no easy answer to that."

While some lawmakers voiced support for Apple's privacy concerns, others attacked the company's position, saying it threatened to deprive the authorities of evidence in critical cases involving newer iPhones.

"We're going to create evidence-free zones?" asked Representative Trey Gowdy, a South Carolina Republican who once served as a federal prosecutor. "Am I missing something?"

"How the hell you can't access a phone, I just find baffling," he said.

Bruce Sewell, Apple's general counsel, told committee members that the F.B.I.'s demand for technical help to unlock Mr. Farook's iPhone 5c "would set a dangerous precedent for government intrusion on the privacy and safety of its citizens." Apple has said that in many cases investigators have other means to gain access to crucial information, and in some instances it has turned over data stored in iCloud.

Mr. Sewell reacted angrily to the Justice Department's suggestion that Apple's branding and marketing strategy was driving its resistance to helping the F.B.I., an assertion that he said made his "blood boil."

"We don't put up billboards that market our security," he said. "We do this because we think protecting security and privacy of hundreds of millions of iPhones is the right thing to do."

F.B.I. officials say that encrypted data in Mr. Farook's phone and its GPS system may hold vital clues about where he and his wife, Tashfeen Malik, traveled in the 18 minutes after the shootings, and about whom they might have contacted beforehand. While investigators believe that the couple was "inspired" by the Islamic State, they have not found evidence that they had contact with any extremists overseas.

A judge last month ordered Apple to develop software that would disable security mechanisms on Mr. Farook's phone so that the F.B.I. could try multiple passwords to unlock the phone through a "brute

force" attack, without destroying any data. Once the systems were disabled, it would take only about 26 minutes to find the correct password, Mr. Comey said.

He rejected an idea expressed by several lawmakers that the F.B.I. was trying to force Apple to build a "back door" to decrypt its own security features. He used a different analogy to explain the government's demands.

"There's already a door on that iPhone," Mr. Comey said. "Essentially, we're saying to Apple 'take the vicious guard dog away and let us pick the lock.' "

But the F.B.I. did not help its case with lawmakers when Mr. Comey acknowledged the mistake of changing the iCloud password.

When the dispute over Mr. Farook's iPhone erupted two weeks ago, the Justice Department blamed technicians at San Bernardino County, which employed Mr. Farook as an environmental health specialist and which owned the phone he used. But county officials said their technicians had changed the password only "at the F.B.I.'s request."

Mr. Comey acknowledged at the hearing that the F.B.I. had directed the county to change the password.

Mr. Sewell, the Apple lawyer, explained to the committee that before F.B.I. officials ordered the password reset, Apple first wanted them to try to connect the phone to a "known" Wi-Fi connection that Mr. Farook had used. Doing so might have recovered information saved to the phone since October, when it was last connected to iCloud.

"The very information that the F.B.I. is seeking would have been available, and we could have pulled it down from the cloud," he said.

The F.B.I.'s handling of the password change drew criticism from both Democrats and Republicans at the hearing.

"If the F.B.I. hadn't instructed San Bernardino County to change the password to the iCloud account, all this would have been unnecessary, and you would have had that information," said Representative Jerrold Nadler, Democrat of New York.

Mr. Gowdy leveled a similar criticism during the more than two and a half hours of testimony from Mr. Comey.

"With all due respect to the F.B.I., they didn't do what Apple had suggested they do in order to retrieve the data, correct?" Mr. Gowdy asked the director. "I mean, when they went to change the password, that kind of screwed things up, did it not?"

But Mr. Comey said that even if the F.B.I. had not mishandled the password, he did not think the bureau could have gotten everything it wanted from the phone and would still have needed Apple to help disable the security features in the phone.

"We would still be in litigation," he said, "because the experts tell me there's no way we would have gotten everything off the phone from a backup."

Mr. Comey stressed that the fight with Apple was about trying to get as much information as possible about the San Bernardino attack -- not about gaining a powerful law enforcement tool elsewhere.

But when he was asked whether the F.B.I. would seek to unlock other encrypted phones if it prevailed in the San Bernardino case, he responded, "Of course."

In the audience were relatives of a Louisiana woman, Brittney Mills, who was shot to death at her doorstep last year when she was about eight months pregnant.

Mr. Comey said the data in her phone could help investigators determine whether she was shot by someone she knew, but they had been unable to break the passcode.

New York Times

U.S. Captures ISIS Operative, Ushering In Tricky Phase

Wednesday, 02 March 2016

Byline: Multiple reporters

Section: general

Washington - An elite American Special Operations force has captured a significant Islamic State operative in Iraq and is expected to apprehend and interrogate a number of others in coming months, ushering in a new and potentially fraught phase in the fight against the extremist Sunni militant group. American defense officials described the capture as a crucial development in battling the Islamic State but said it also raised questions about handling what is likely to be a growing group of detainees.

Although American commandos have captured a handful of Islamic State fighters in Iraq and Syria in discrete operations in recent years, the Pentagon is now faced with the prospect of detaining a larger group of captives and potentially reprising some of the darkest images of the war in Iraq, particularly the abuses at Abu Ghraib prison.

The American military has largely fought the Islamic State, also known as ISIS or ISIL, from the sky, and large numbers of Islamic State fighters have been killed in Iraq and Syria by American airstrikes. The 200-member Special Operations team, made up of many Delta Force commandos, arrived in Iraq in recent weeks and is the first major American combat force on the ground there since the United States pulled out of the country at the end of 2011.

Defense officials said the team had set up safe houses and worked with Iraqi and Kurdish forces to establish informant networks and conduct raids on Islamic State leaders and other important militants.

Officials said the detainee, whom they declined to identify, was being interrogated by American officials at a temporary detention facility in the city of Erbil in northern Iraq. They said the plan was to eventually turn him over to Iraqi or Kurdish officials.

Several Defense Department officials declined to say how much information or cooperation they have received from the detainee. They said it could take weeks or months to finish questioning the operative.

As is protocol, Defense Department officials notified the International Committee of the Red Cross, which monitors the treatment of detainees, that they were holding an Islamic State fighter. A Red Cross spokesman, Trevor Keck, declined to comment on the matter, including on whether Red Cross personnel were observing the detainee's treatment at the facility in Erbil.

Defense Department officials said that the United States had no plans to hold the detainee or others indefinitely, and that they would be handed over to Iraqi or Kurdish authorities after they have been interviewed. The officials said they did not intend to establish a long-term American facility to hold Islamic State detainees, and Obama administration officials ruled out sending any to the United States military prison at Guantánamo Bay, Cuba.

One of President Obama's major objectives before he leaves office is to close Guantánamo.

Captain Jeff A. Davis, a Pentagon spokesman, reiterated Tuesday that there were no plans to detain Islamic State captives long term. "Any detention would be short term and coordinated with Iraqi authorities," he said.

Defense Department officials say the commandos, referred to at the Pentagon as a "specialized expeditionary targeting force," will almost certainly increase the intelligence on the Islamic State available to the United States, including information about current operations extracted from laptops and cellphones.

Josh Earnest, the White House press secretary, has said the commandos are to "go and scoop up paperwork and hard drives and other information that can be critical to our ongoing efforts as a central part of this strategy."

Defense Secretary Ashton B. Carter told reporters Monday that the commando force was going strong. "It's a tool that we introduced as part of the accelerated operations to conduct raids of various kinds, seizing places and people, freeing hostages and prisoners of ISIL, and making it such that ISIL has to fear that anywhere, anytime, it may be struck," Mr. Carter said.

Senior Defense Department officials said the model for handling detainees seized by the new commando unit was a Delta Force raid in May, when two dozen American commandos from Iraq entered Syria aboard Black Hawk helicopters and V-22 Ospreys and killed Abu Sayyaf, described by American officials as the Islamic State's emir for oil and gas. Abu Sayyaf's wife, Umm Sayyaf, was captured and taken to a screening facility in Iraq, where she was questioned and detained. American forces seized laptop computers, cellphones and other materials from the site.

Umm Sayyaf was kept for three months by the American authorities and provided them information, officials said. Last August, she was transferred to Kurdish custody, and last month, the Justice Department filed an arrest warrant charging her with conspiring to provide material support to the Islamic State in an offense that officials said resulted in the death of Kayla Mueller, the American aid worker who was killed in Syria in February 2014.

Defense officials said only that the commando operation that led to the capture of the Islamic State militant was conducted in recent weeks in Iraq.

Washington Post

Privacy is part of wiretap talks

Wednesday, 02 March 2016

Byline: Ellen Nakashima

Section: general

Washington - Attorney General Loretta E. Lynch said Tuesday that recently launched transatlantic talks to enable British access to wiretap data from U.S. firms would protect privacy and human rights.
In remarks at a major cybersecurity conference in San Francisco, Lynch said that under any agreement, the British government would have to accept provisions designed to safeguard such rights.

The negotiations are aimed at establishing a framework that would permit British authorities to serve orders directly on U.S. companies for live intercepts and stored data in cases in which the investigation targets accounts not used by Americans or people in the United States.

"It would help one of our oldest and closest allies perform high- priority criminal investigations that keep its citizens safe," said Lynch, speaking at the RSA Conference.

The talks are the latest instance of an effort to reconcile the borderless nature of the Internet with sometimes conflicting laws created by sovereign states.

The talks, which were first reported by The Washington Post, are also aimed at easing the plight of U.S. companies, which are increasingly under pressure from foreign governments such as Britain's to comply with their orders for data in criminal and terrorism investigations. Such data might include online chats, for instance.

Congress, however, has barred U.S. firms from providing intercepts to anyone except the U.S. government after law enforcement has obtained a court order. This clash of laws has put U.S. companies in a difficult position, Lynch said. "Either they comply with a foreign order, and risk a violation of American law - or they refuse to comply, and risk a violation of foreign law," she said.

To obtain stored emails from U.S. companies, a foreign government must rely on a mutual legal assistance treaty by which the country makes a formal diplomatic request for the data, and the Justice Department then seeks a court order on its behalf - a process that can take many months.

Officials at U.S. technology firms have voiced concerns that if no resolution is reached, foreign governments, including Britain's, will force them to host their data in those countries. They also fear passage of laws requiring foreign firms to comply with surveillance orders. Britain has passed such a law, although it has not tried to enforce it against a U.S. firm.

Privacy advocates, however, are worried that the agreement will fail to adequately protect British users' privacy and human rights and permit U.S. firms to conduct wiretaps for foreign governments without the same legal standards based on probable cause that exist in the United States.

In Britain, rather than a judge approving search and wiretap warrants, the home secretary, who oversees police and internal affairs, issues the warrant if that cabinet member finds that it is "necessary" for national security or to prevent serious crime and that it is "proportionate" to the intrusion.

Lynch noted that the agreement would require action from Congress. That probably would mean amendments to laws such as the Wiretap Act. The pact is intended to be reciprocal, which, Lynch said, could help U.S. investigations in the future.

If the agreement proves successful, she said, it might be replicated with other countries "if - and only if - their laws adequately protect privacy and civil liberties."

The negotiations are expected to take months. The White House in January gave the Justice and State departments the go-ahead to begin the talks.

London Times

Terror plots thwarted by bulk data

Wednesday, 02 March 2016

Byline: Fiona Hamilton

Section: general

London - Spies' ability to carry out bulk interception and bulk hacking is one of the most controversial aspects of the Investigatory Powers Bill. The government insists that powers to hoover up vast amounts of data is "integral to the work of the security and intelligence agencies".
Yesterday it set out a detailed case for the bulk collection of data and gave examples of where it thwarted terrorist attacks and helped investigations. The Home Office document cited the plan to bring down aircraft using homemade bombs in 2006 and the 2010 plot to bomb symbolic locations such as the London Stock Exchange. Both investigations required complex analysis of large volumes of data to identify the attackers and understand the links between them.

In another case, the name of an individual reported to be storing a weapon used in a terrorist attack was identified. Spies used bulk datasets of private information to identify the suspect from hundreds of candidates.

The collection of bulk data has also helped to identify people going to Join Islamic State in Syria.

Bulk capabilities played a part in every MAJOR counterterrorism investigation in the past decade, including seven attack plots disrupted since November 2014, it said, and were essential in identifying 95 per cent of cyberattacks on people and businesses in the UK in the past six months.

Washington Post

What's on that iPhone? Fight goes to Congress

Wednesday, 02 March 2016

Byline: Mark Berman, Ellen Nakashima

Section: general

Washington - Lawmakers on Tuesday pressed FBI Director James B. Comey about the bureau's demands that Apple help it unlock an iPhone used by one of the San Bernardino attackers.
The Justice Department and FBI have tried to cast the issue as narrowly focused on one iPhone, but Comey acknowledged that if the government succeeds in this case it could set a precedent for others.

He also said he believed that soon, all conversations and personal documents would be hidden behind encryption "that nobody else can get into." This, he said, would challenge law enforcement efforts that depend on officers obtaining warrants to access personal conversations or materials.

"Our job is simply to tell people there is a problem," Comey said. "Everybody should care about it. Everybody should want to understand. If there are warrant-proof spaces in American life, what does that mean and what are the costs of that?"

The hearing before the House Judiciary Committee came a day after a federal judge in New York ruled in favor of Apple in a separate case that also focuses on whether the government can force the tech giant to help it access locked devices. That case, however, involves a different operating system from than the one in the San Bernardino phone, and a much less burdensome request for assistance.

But both cases turn on a 220-year-old law, the All Writs Act, and whether it provides authority for a court to force the firm to provide the technical assistance the government seeks.

Comey acknowledged that if the federal government prevails in the California case, agents could seek assistance in unlocking other devices in the future. He said other judges and lawyers could look to the case for guidance. But he also said he thought there were "limits" to how useful the precedent would be, given what he described as its narrow application to an older model phone.

Bruce Sewell, Apple's general counsel, asserted that Apple's defiance of the government's court order in the San Bernardino case was not motivated by financial concerns.

"This is not a marketing issue," he said, rejecting suggestions by the Justice Department, which he said "diminishes" the serious issues being debated.

"We're doing this because we think that protecting the security and the privacy of hundreds of millions of iPhone users is the right thing to do," he said.

Sewell said Apple's move toward strong encryption in recent years arose out of a concern about customer security. "Some of you might have an iPhone in your pocket right now, and if you think about it, there's probably more information stored on that iPhone than a thief could steal by breaking into your house," Sewell said.

He said the company was "in an arms race with criminals, cyberterrorists [and] hackers."

The debate between Apple and the government has played out in recent weeks across court filings, public statements, open letters and television interviews, with both sides seeking to stake out the higher ground in a conflict centered on one iPhone but with far-reaching implications in an era where personal information is increasingly stored on digital devices and platforms.

Comey told lawmakers that the iPhone recovered after the San Bernardino attack - one of three phones that were found, though the other two were smashed - could provide information about other terrorists. The FBI, he said, was seeking to answer lingering questions: "Is there somebody else? And are there clues to what else might have gone on here?" Comey said, adding that answering those questions "is our job."

He said the NationalSecurity Agency, the world's most sophisticated electronic spy agency, had been consulted for help with the phone. Asked who the FBI had turned to, he said: "All elements of the U.S. government have focused on the problem."

Later in the hearing, when asked specifically if the FBI had talked to other government agencies, including the NSA, he replied: "Yes is the answer. We've talked to anybody who will talk to us about it."

The NSA did not immediately respond to a request for comment Tuesday.

Comey also admitted that the FBI made a "mistake" when it asked San Bernardino County technicians to reset the iCloud password for the phone, which forestalled the possibility of trying to back it up again after that occurred. But he said even if that had not occurred, the FBI and Apple might have wound up in the same situation, since some data on the phone may not have been backed up.

Sewell, though, disputed that notion, saying that if the password was not changed, the court fight might have been averted.

"The very information that the FBI is seeking would have been available and we could have pulled it down from the cloud," he said. "By changing the [iCloud] password . . . it was no longer possible."

The government is seeking to unlock an iPhone 5c used by Syed Rizwan Farook, one of two shooters in the attack that killed 14 people. Last month, a magistrate judge in California issued an order directing Apple to write software that would disable a feature that deletes the data on the phone after 10 incorrect tries at entering a password. The bureau wants to try to crack the password without risking data deletion.

The Guardian (London)

Technology firms' hopes dashed by 'cosmetic tweaks' to snooper's charter

Tuesday, 01 March 2016

Byline: Alex Hern

Section: general

Analysis - Here comes the new snooper's charter, same as the old snooper's charter.
Many in the technology sector had been hoping that the final version of the investigatory powers bill, released on Tuesday, would backtrack on some of the more controversial aspects of October's draft bill. But the final version, which will now be presented to parliament, contains only the mildest of tweaks, and even doubles-down on some areas.

A fierce lobbying effort over the winter, from firms including Apple, Facebook, Microsoft and Twitter, had focused on three specific parts of the legislation where the Home Office bill looked set to do real damage to the technology industry.

The draft bill had concerned the major US technology companies for a number of reasons.

* There was a claim of "extraterritorial jurisdiction" that would allow warrants for bulk surveillance to be served to companies even if they weren't headquartered in the UK.

* There was a requirement for firms to provide assistance with "computer network exploitation", which they worried could lead to the UK mandating their aid in hacking their own customers - a fear which has taken on a less hypothetical sheen with the revelation that the US government is currently taking Apple to court demanding the company do just that.

* There was language suggesting that tech firms could be forced to break the encryption on messages sent using their technology - a requirement which could force companies like Apple and Facebook,

which offer encrypted messaging apps, to choose between operating in Britain or breaking their own messaging apps on an international scale.

The new version of the bill does soften that last requirement, just. It offers a "pragmatic approach" on the part of the government, and makes clear that no company will be required to remove encryption of their own services if it is not technically feasible. The definition of what, exactly, constitutes technical feasibility is, however, left as an exercise for the reader - and for a lot of lawyers in the future.

But on the other areas, no changes were made.

In its response to the bill committee's recommendations, the government said that concerns over extraterritoriality were already dealt with. "The government is engaging in preliminary discussions with international partners on how a new international framework for access to data across jurisdictions might operate in principle. This would be based on strong, human rights-compliant domestic regulatory oversight," it said.

And the bill actually extended the proposed powers for the state to hack computers. Previously, the draft bill had only allowed the security services to carry out computer hacking (enshrining into law an ability believed to already be widely used). But the new version of the bill also allows the police to start hacking when they are dealing with a "threat to life" or missing persons, as well as the security services.

The Open Rights Group's executive director Jim Killock concluded that "the revised bill barely pays lip service to the concerns raised by the committees that scrutinised the draft bill.

"If passed, it would mean that the UK has one of the most draconian surveillance laws of any democracy with mass surveillance powers to monitor every citizen's browsing history."

Eric King, the director of the Don't Spy on Us coalition, warned that "Rather than a full redraft, we've been given cosmetic tweaks to a heavily criticised, deeply intrusive bill."

King added: "There simply isn't time for proper scrutiny of all these powers in the timeframe proposed." On that, he was backed up by the Web Foundation, founded by the inventor of the world wide web, Tim Berners-Lee, which called the final bill "a slap in the face for British democracy".

The time-frame is, according to the Foundation, "not only unrealistic, but dangerous."

One major US technology firm told the Guardian that it was "hugely disappointing that the government hasn't moved on any of the core issues, despite a wealth of evidence". As the bill moves through parliament, that opposition is likely to intensify.

London Daily Telegraph

Snoopers' charter: Police have powers to hack into phones and computers for 'routine investigations'

Tuesday, 01 March 2016

Byline: Tom Whitehead

Section: general

London - Police have sweeping powers to hack in to phones and computers and access web browsing histories for routine investigations, under laws unveiled on Tuesday.
Measures in the Investigatory Powers Bill allow officers to break in to electronic devices to investigate or prevent "serious crime".

But they can also covertly glean personal data for purposes of "preventing death or injury or damage to a person's physical or mental health".

It raises the prospect that police can access devices or communications data for common investigations such as assaults, missing persons or suicide risks.

So-called "equipment interference" can include remotely hacking in to phones or computers, which is restricted to a small number of police forces or law enforcement agencies, or by-passing security and passwords on seized equipment.

Officials stressed warrants to carry out such interference have to be signed off by a designated officer and a judge in a "double lock" safeguard.

The tactic was included in a revised version of the surveillance legislation, which had to be reviewed after the draft bill published last year was criticised by three parliamentary committees.

The final bill also includes an extension to the type of web histories officers can ask for.

Police access to internet connection records was to be limited to communications sites, identifying who sent a message and where it was suspected an individual was accessing illegal material.

But the bill has been amended to allow access to any web use if it is "necessary and proportionate for a specific investigation".

It was included after police chiefs warned their powers were too limited.

Access is restricted to the details of the main website visited and not individual pages or content within that.

The bill will require internet companies to store their customers' web records for up to a year.

The Government also made a raft of changes to the surveillance legislation, which aims to bring all existing powers under one bill, after accusations it was flawed and failed to make its case.

It earlier emerged that Twitter, Apple, Google and other communication companies will not be forced to decrypt messages unless it is "practicable" as ministers admitted they are powerless to stop unbreakable encryption.

The move will reignite concerns that terrorists and criminals are increasingly hiding behind so-called "end-to-end encryption" in online messages, which even the provider cannot access.

It comes as figures show major communication companies are still rejecting up to half of requests for customer data from UK police and intelligence agencies.

In other measures to try and get the legislation through parliament, the Government will take the unprecedented step of publishing an "operational case" on why MI5, MI6 and GCHQ need to carry out bulk collection of data.

The document attempts to allay fears of mass surveillance by demonstrating that even when data is scooped up, only information on suspects is targeted.

Extra safeguards for journalists and lawyers will also be included along with additional authorisation checks on UK spy agencies when they need help from foreign intelligence agencies.

Mrs May is facing a backbench revolt over the legislation amid concerns it has to be rushed in to law before the end of the year, when laws governing some existing powers fall away.

Theresa May, the Home Secretary, said: "This is vital legislation and we are determined to get it right."

But Shami Chakrabarti, director of human rights group Liberty, said: "Minor botox has not fixed this Bill."

Kate Allen, of Amnesty International, said it "beggars belief that the Government is blundering on with its snooping power-grab".

The draft legislation, published in November, was criticised by three parliamentary committees as being "flawed" and failing to make a case for many of the controversial measures.

A source said: "We have considered the committees' reports carefully and the Bill we are bringing forward today reflects the majority of their recommendations. We have strengthened safeguards, enhanced privacy protections and bolstered oversight arrangements.

"This is world-leading legislation, setting out in unprecedented detail the powers available to the police and security services to gather and access communications and communications data, subject to a robust regulatory regime."

However, on encryption, the bill will clarify and "put beyond doubt" that companies "can only be asked to remove encryption that they themselves have applied and only where it is practicable for them to do so".

The source said that this will "make clear that the Government is not asking companies to weaken their security by undermining encryption".

Separate figures show that in the first half of 2015, Apple provide information following a UK request in 56 per cent of cases relating to a device and 63 per cent in connection with a customer account.

Google provided data in 75 per cent of requests over the same period while Facebook met 78 per cent of requests.

Twitter met 52 per cent of request in the first six months but that increased to 76 per cent in the second half of the year.

The Guardian (London)

Snooper's charter: wider police powers to hack phones and access web history

Tuesday, 01 March 2016

Byline: Alan Travis

Section: general

London - Powers for the police to access everyone's web browsing histories and to hack into phones are to be expanded under the latest version of the snooper's charter legislation.
The extension of police powers contained in the investigatory powers bill published on Tuesday indicates the determination of the home secretary, Theresa May, to get her legislation on to the statute

book by the end of this year despite sweeping criticism by three separate parliamentary committees in the past month.

The bill is designed to provide the first comprehensive legal framework for state surveillance powers anywhere in the world. It has been developed in response to the disclosure of state mass surveillance programmes by the whistleblower Edward Snowden. The government hopes it will win the backing of MPs by the summer and by the House of Lords this autumn.

May said the latest version reflected the majority of the 122 recommendations made by MPs and peers, including strengthening safeguards, enhancing privacy protections and bolstering oversight arrangements.

She has, in particular, made changes to meet concerns within the technology industry that the surveillance law would undermine encryption. The latest draft makes clear that the government will take a pragmatic approach, and no company will be required to remove encryption of their own services if it is not technically feasible. The likely costs involved will also be taken into account.

But the publication of the detailed bill has also revealed that, far from climbing down over her proposals, May intends to expand the scope of its most controversial new powers - the collection and storage for 12 months of everyone's web browsing history, known as internet connection records - and state powers to hack into computers and smartphones.

The bill will now allow police to access all web browsing records in specific crime investigations, beyond the illegal websites and communications services specified in the original draft bill.

It will extend the use of state remote computer hacking from the security services to the police in cases involving a "threat to life" or missing persons. This can include cases involving "damage to somebody's mental health", but will be restricted to use by the National Crime Agency and a small number of major police forces.

Four hours after the bill's publication the Home Office issued a highly unusual 'clarification' claiming that its official response published on Tuesday listing the powers to allow the police to use computer and phone hacking as a "key change" was because they had been missed out from the draft bill.

"Documents published alongside the bill today describe the position as having changed as it was not referenced in the draft bill. However it reflects current police practice. The fact that it was not included in the draft bill was an omission that is being corrected in the final bill."

The Home Office said the hacking powers dated from the 1997 Police Act and would most likely only be used in "exceptional circumstances" such as finding missing people. They would require a "double-lock" warrant with ministerial authorisation and judicial approval.

However evidence given to the scrutiny committee by the head of the Metropolitan police technical unit, Det Supt Paul Hudson, said such hacking powers were used "in the majority of serious crime cases" but refused to give further details in a public forum.

He described it as a "covert activity so nothing that we do under equipment interference would cause any damage or leave any trace, otherwise it would not remain covert for very long". His colleague said they could provide MPs and peers with data on its use but it was "very confidential" and would have to remain unpublished.

Hudson acknowledged that the technology has long moved on since 1997. Legalised hacking now allows a third party to even take remote control of a phone's camera or microphone to record video and conversations taking place.

The Home Office claims that the legalised hacking powers had been missed out of the original draft bill and so escaped the process of pre-legislative scrutiny was greeted with scepticism by at least one member of the scrutiny committee.

The expansion of police powers to access web browsing history as part of their investigations follows pressure from the police, and the use of these powers does not need the "double-lock" ministerial authorisation.

The home secretary told MPs she had rejected the committees' recommendations to exclude the use of state surveillance powers for the "economic wellbeing" of the UK. She also resisted their demand to scrap warrants allowing GCHQ to undertake bulk computer hacking, describing them as a "key operational requirement".

May also underlined the "vital part" played by the security agencies' "bulk powers" - the mass collection and storage of everyone's communications data in Britain and the bulk interception of the content of communications of those based overseas to acquire intelligence.

The Home Office has made detailed tweaks to the original draft of the bill, including stronger protections for journalists and lawyers, six codes of practice setting out how the powers will be used, and the use of a "double-lock" authorisation of the most intrusive surveillance methods by a minister backed by the approval of a judicial commissioner.

The Home Office has acknowledged that the initial costing of the bill, at around £247m, is not set, and a final figure will be published after detailed consultations with industry.

May said: "This is vital legislation and we are determined to get it right. The revised bill we introduced today reflects the majority of the committees' recommendations - we have strengthened safeguards, enhanced privacy protections and bolstered oversight arrangements - and will now be examined by parliament before passing into law by the end of 2016.

"Terrorists and criminals are operating online and we need to ensure the police and security services can keep pace with the modern world and continue to protect the British public from the many serious threats we face."

As part of the pre-legislative process, the bill was examined by a draft scrutiny committee, the intelligence and security committee and the science and technology committee.

The MPs and peers called for a fundamental rewrite of the draft bill, with the ISC calling for privacy safeguards to be made the backbone of the legislation and the draft scrutiny committee saying the case had not yet been made for the introduction of new powers to store and access everyone's web browsing history.

Eric King, director of the Don't Spy On Us coalition, which includes Liberty, Privacy International and other privacy and digital rights groups, called for a rethink of the bill.

"Rather than a full redraft, we've been given cosmetic tweaks to a heavily criticised, deeply intrusive bill," he said. "Reshuffling safeguards without meaningfully improving protections, authorisations or oversight does nothing to address widespread concerns about mass surveillance. The unsettling absence of a robust, technical, detailed evaluation of those bulk powers means the case still hasn't been made, and parliament won't have the information it needs to do its job.

"There simply isn't time for proper scrutiny of all these powers in the timeframe proposed. More than 100 experts called on the Home Office to put on the brakes. The government must think again."

Shami Chakrabarti, director of Liberty, said: "Less than three weeks ago MPs advised 123 changes to the majorly flawed draft bill. The powers were too broad, safeguards too few and crucial investigatory powers entirely missing.

"Minor Botox has not fixed this bill. Government must return to the drawing board and give this vital, complex task appropriate time. Anything else would show dangerous contempt for parliament, democracy and our country's security."

Lord Strasburger, a Liberal Democrat member of the scrutiny committee on the draft bill, said nothing had changed since they published their report three weeks ago: "The Home Office just doesn't do privacy. It does security and ever more intrusive powers they claim will make us safer, but not privacy. The fact that they see simply changing the name of one section to include the word 'privacy' as addressing the fundamental concerns about privacy protections in this bill is breath- taking," he said.

"The speed with which the home secretary is trying to force this bill through parliament shows no respect to the joint committee and ISC who worked so hard to give them workable solutions to problems in the draft bill, to parliament, or to the British people."

Le Devoir

Vie privée - Le précédent Apple

Wednesday, 02 March 2016

Byline: Brian Myles

Section: editorial

Editorial - Le bras de fer entre Apple et le FBI sur le décryptage du iPhone marquera un tournant dans l'évolution du droit à la vie privée. Un droit en érosion constante à l'ère de la surveillance de masse. Ils ont tous les deux raison. Apple veut protéger la crédibilité de sa marque et la vie privée des utilisateurs du iPhone en refusant de répondre aux demandes d'assistance du FBI dans l'enquête sur l'attentat terroriste de San Bernardino. Et la police fédérale souhaite explorer toutes les avenues possibles afin de débusquer des complices potentiels de l'auteur du massacre qui a fait 14 morts, Syed Rizwan Farook. Rien n'est simple quand le droit à la vie privée est mis en opposition à la sécurité nationale. Jusqu'à tout récemment, Apple prêtait assistance aux policiers, notamment pour déverrouiller des iPhone, pour autant que les enquêteurs obtiennent une autorisation judiciaire.

À la suite de la tuerie de San Bernardino, Apple a même partagé sans broncher les données du cellulaire de Farook déjà stockées sur son compte iCloud. Le problème ? La dernière sauvegarde du téléphone de Farook remonte à environ un mois avant son passage à l'acte. Le FBI s'en voudrait de ne pas " retourner toutes les pierres " et de laisser filer de présumés complices de l'auteur du pire attentat terroriste en sol américain depuis le 11 septembre 2001.

Le poids des symboles est lourd, mais il ne saurait occulter la gravité des exigences formulées par le FBI, avec l'assentiment du gouvernement Obama. Le FBI demande à Apple de créer un logiciel sur mesure afin de passer outre le système de cryptage de la nouvelle génération d'appareils mobiles.

À la suite des révélations d'Edward Snowden sur la surveillance de masse, Apple a considérablement renforcé la technologie de cryptage de ses appareils. Au-delà de dix tentatives erronées d'entrer le mot de passe, la mémoire du iPhone s'efface. Le FBI a besoin de l'aide d'Apple pour créer l'équivalent d'une " porte arrière " lui permettant de faire intrusion dans l'appareil sans risquer de compromettre les données.

L'avancement de l'enquête sur la tragédie de San Bernardino est le moindre des soucis dans cette affaire. À preuve, quelque 175 enquêtes, entre autres pour trafic de drogue et homicide, sont

présentement dans un cul-de-sac aux États-Unis parce que les policiers sont incapables d'accéder aux appareils iPhone des suspects ou des victimes.

Si les tribunaux devaient donner gain de cause au FBI, le pouvoir d'intrusion des forces de l'ordre dans la vie privée des citoyens serait encore plus grand. Cette " porte arrière " pourrait être utilisée par des organisations criminelles, des pirates informatiques ou des agences de surveillance domestiques et étrangères. Il s'agirait d'un pas important vers la banalisation de la sursurveillance dans les nouvelles sociétés du numérique.

Le problème déborde largement les frontières américaines, puisque les précédents en matière d'enquête policière et d'entrave aux libertés civiles ont tendance à trouver un écho législatif au Canada, surtout lorsqu'il s'agit de lutter contre le terrorisme.

Lundi à New York, un juge a donné raison à Apple, qui refusait cette fois d'aider les policiers à accéder au cellulaire d'un présumé vendeur de drogue. Dans cette cause comme celle de San Bernardino, le débat juridique est centré sur une loi vieille de 1789, réinterprétée en 1977 par les tribunaux. Elle force les compagnies privées à prêter assistance aux policiers et à leur fournir des données (tel un registre des appels), sur autorisation judiciaire.

Le Congrès américain a entendu le FBI et Apple à ce sujet mardi. Il lui faudra prendre un virage vers la modernité sans compromettre les libertés civiles, le tout dans un climat de polarisation exacerbée de la politique américaine.

Le Droit

La justice freinée par le « Web profond »

Wednesday, 02 March 2016

Byline: Louis-Denis Ebacher

Section: general

Québec - Alertes à la bombe dans les écoles du Québec et de l'Ontario
Le Web profond (Dark Web) est la partie cachée d'Internet, innavigable par les moyens conventionnels.

La Sûreté du Québec (SQ) semble avoir de la difficulté à percer les profondeurs du Web pour cerner le ou les auteurs d'alertes à la bombe ayant visé plusieurs établissements scolaires du Québec et de l'Ontario, l'automne dernier.

-- FRANCOIS GERVAIS, ARCHIVES LE NOUVELLISTE

Les quatre jeunes de la région étaient accusés d'avoir lancé des alertes à la bombe dans plus de 70 écoles du Québec, le 3 novembre dernier.

Le Directeur des poursuites criminelles et pénales (DPCP) a arrêté les procédures judiciaires entamées contre eux.

La Couronne en a fait la demande au tribunal de la Jeunesse, vendredi dernier. L'arrêt des procédures a pris effet le même jour, ce qui veut dire que les chefs d'accusation sont en quelque sorte sur la glace pour une période d'un an.

Les quatre jeunes de 16 et 17 ans, des résidents de l'Outaouais, étaient accusés d'avoir lancé des alertes à la bombe dans plus de 70 écoles du Québec, le 3 novembre dernier. On leur reprochait aussi d'avoir envoyé des messages menaçants à des écoles d'Ottawa, et d'avoir répété l'envoi de courriels inquiétants au Cégep Héritage de Gatineau pendant plusieurs jours.

La défense reprochait à la Couronne de manquer de preuves.

« L'arrêt des procédures nous permet de reprendre le dossier au courant de la prochaine année, a précisé le porte- parole du DPCP, Me René Verret. L'enquête continue, et nous prenons cette affaire très au sérieux. »

Les conditions imposées aux adolescents visés sont aussi suspendues. Lors de leur mise en accusation, la cour leur avait entre autres interdit de communiquer entre eux et d'accéder à Internet. L'avocat de la défense, Me Michel Swanston, n'a pas commenté le dossier mardi.

DOSSIER DÉLICAT

Selon nos informations, le Cégep Héritage a reçu d'autres messages menaçants ces derniers jours.

L'enquête policière serait rendue difficile par l'utilisation du Web profond (Dark Web) par les auteurs de ce qui est, pour l'instant, une série de canulars. Le « Dark

Web » est la partie cachée d'Internet, introuvable par les moteurs de recherche conventionnels comme Google ou Yahoo.

Ce modus operandi pourrait en partie expliquer pourquoi il est si difficile pour les autorités de relier les messages à leurs auteurs.

Les jeunes ont été arrêtés par les autorités cet automne, après qu'un groupe autobaptisé « Sceptre rouge » ait fait des menaces auprès d'institutions d'Ottawa, de Gatineau, puis de la province de Québec. Les enquêteurs de la SQ les avaient longuement interrogé.

Le Devoir

Pilleurs de banque, nouvelle génération

Wednesday, 02 March 2016

Byline: Karl Rettino-Parazelli

Section: general

Non identifié - Les cybercriminels peuvent geler vos données et vous rançonner pour les libérer
La menace est invisible, mais les dirigeants d'entreprise et les chefs d'État provenant des quatre coins de la planète savent qu'elle est bien réelle. La cybercriminalité est en " forte croissance " et ne cesse de se raffiner, causant bien des sueurs froides. En ce début du Mois de la prévention de la fraude, les analyses démontrent l'ampleur du défi auquel font face les organisations en tous genres.

La firme KPMG donne le ton dans son Rapport de cyberveille, diffusé mardi, en rapportant une augmentation du nombre de tentatives d'extorsion par l'entremise des systèmes informatiques. Les cybercriminels infiltrent par exemple le système d'une entreprise, cryptent les données et réclament une rançon pour les rendre à nouveau accessibles. En cas de refus, ils volent les fichiers.

" Il y a lieu de croire que ces pratiques vont augmenter au Canada, particulièrement dans les organisations du secteur public, et dans les sociétés des secteurs juridiques et financiers, en raison de la nature privée et sensible des renseignements qu'elles détiennent ", souligne KPMG.

Il ne s'agit-là que d'un des types d'attaques perpétrées chaque jour par les cybercriminels, dans le but d'extorquer des informations ou de l'argent. Selon un sondage dévoilé la semaine dernière par PwC, 59 % des répondants canadiens jugeaient en 2015 que la cybercriminalité gagne du terrain, comparativement à 47 % en 2014.

" Ce qu'on voit, c'est une nette progression [des attaques], confirme Francis Beaudoin, leader Cybersécurité chez KPMG. Dans mon équipe, je vous dirais que nous sommes débordés de travail. De plus en plus d'organisations font appel à nous parce qu'il y a de plus en plus de cas. Et ce n'est pas seulement vrai à Montréal, c'est vrai partout au Canada et ailleurs dans le monde. "

Dans le plus récent rapport sur les risques mondiaux du Forum économique mondial (FEM) dévoilé en janvier, les résultats d'un sondage mené auprès de dirigeants d'entreprises ont confirmé cette tendance. Les répondants américains et canadiens, tout comme ceux provenant de l'Allemagne, du Japon, de la Suisse ou des Pays-Bas estiment que les cyberattaques figurent parmi les menaces les plus susceptibles de nuire à la conduite des affaires.

" Les récentes avancées technologiques ont été bénéfiques à plusieurs égards, mais elles ont aussi ouvert la porte à une vague grandissante de cyberattaques [...] qui ciblent de plus en plus les entreprises ", fait remarquer le FEM dans son rapport.

Le document rappelle par ailleurs que la cybercriminalité coûte près de 445 milliards $US par année à l'économie mondiale, selon les données compilées en 2014 par le Center for Strategic and International Studies.

Motivation différente

À l'origine, les cybercriminels voulaient essentiellement nuire aux entreprises qu'ils attaquaient, constate Francis Beaudoin, de KPMG. Mais depuis quatre ou cinq ans, la motivation est différente. " On voit l'infiltration du crime organisé dans des groupes de hackers,et le but est de faire des gains financiers. "

M. Beaudoin admet qu'il est difficile de mesurer l'ampleur des crimes économiques commis par l'entremise du cyberespace, notamment parce que les délits ne sont pas tous déclarés. Certaines entreprises gardent le secret sur les dommages qu'elles ont subis pour éviter d'entacher leur réputation, alors que d'autres ne croient pas que les autorités policières pourront leur venir en aide.

Les plus récentes données annuelles fournies par le Centre antifraude du Canada, qui travaille en partenariat avec la Gendarmerie royale du Canada et le Bureau de la concurrence, indiquent qu'en 2014, les entreprises canadiennes ont signalé des pertes financières totalisant plus de 26 millions de dollars.

Ces sommes perdues, sans doute sous-évaluées, sont généralement le résultat d'une protection inadéquate. Le rapport du FEM soulignait à ce titre que les dirigeants d'entreprise sont préoccupés par la montée de la cybercriminalité, mais que plusieurs d'entre eux ne savent pas comment y répondre. Dans certaines organisations, le manque de clarté dans la définition des rôles nuit également à la prévention des risques.

Même si de plus en plus d'entreprises canadiennes se préparent au pire, elles ne sont pas complètement immunisées pour autant, concède Francis Beaudoin.

" C'est comme avec le virus de la grippe. Le vaccin annuel nous protège contre les souches de l'année dernière, mais pas nécessairement contre toutes les souches, illustre-t-il. Donc, oui, nous sommes souvent quelques pas derrière le hacker. "

France 3 - (Régions)

Huit ans requis en appel à Paris pour un "cyberjihadiste" tunisien arrêté à Toulon

Wednesday, 02 March 2016

Byline: Journaliste maison

Section: general

Paris - Il se présentait comme l'administrateur du "plus grand forum jihadiste du monde", lié à Al-Qaïda: huit ans de prison ont été requis en appel lundi à Paris à l'encontre d'un "cyberjihadiste" tunisien. Nabil Amdouni avait été arrêté à son domicile en 2012 à Toulon. AR avec AFP
Dans son réquisitoire, l'avocat général a également assorti sa demande d'une peine de sûreté des deux tiers. "M. Nabil Amdouni nous dit que du musulman radical qu'il était, il est devenu un musulman tolérant avec une toute nouvelle vision de sa religion", a ironisé le représentant du ministère public. "Mais ces propos ne doivent pas nous faire oublier ce qu'il a fait."

En première instance, le procureur avait déjà requis en sus une interdiction définitive du territoire français contre celui qu'il avait qualifié "d'un des maîtres du jeu d'un autre jihad, le jihad médiatique".

L'un des administrateur du "plus grand forum jihadiste du monde"Nabil Amdouni, 37 ans, avait été arrêté en juillet 2012 à Toulon, où il vivait avec son épouse et leurs deux enfants. Les services de renseignement l'avaient identifié depuis environ un an comme administrateur du site "Choumoukh al-islam", "le plus grand forum jihadiste du monde", selon les propres mots de M. Amdouni.

Il avait créé ce site hébergé sur un serveur en Malaisie, en juin 2007, après avoir gravi les échelons (simple membre, modérateur puis administrateur) d'un autre site web jihadiste. "Choumoukh al-islam" (fierté de l'islam) avait reçu l'agrément d'Al-Fajr, la branche médiatique d'Al-Qaïda.

Nombre des messages dans la partie privée des forums étaient cryptés et Choumoukh, en lien régulier avec Al-Qaïda dans la péninsule arabique et Al-Qaïda au Maghreb islamique.

Ont ainsi été transmis des détails sur des personnalités cibles potentielles, la fabrication d'explosifs, ou encore des revendications d'enlèvement. Des filières de recrutement ou de financement étaient également promues, mais M. Amdouni a affirmé avoir aidé "seulement deux" candidats jihadistes à partir au Yémen.

"Je me condamne moi-même""Je me condamne moi-même. J'ai fait des choses immorales. Je le sais maintenant", a reconnu lundi Nabil Amdouni, qui n'a jamais nié les faits au cours de ses deux procès.

"Il y a autre chose à faire que la prison pour mon client", a plaidé son avocat Me Éric Bourlion, brandissant un rapport de la maison d'arrêt d'Osny (Val d'Oise) qui démontre que "(s)on client a changé".

Pour l'avocat, expulser son client "vers la Tunisie est contre notre intérêt car après quatre années de déradicalisation en maison d'arrêt, on pourrait espérer un retour sur investissement".

La cour d'appel de Paris rendra sa décision le 5 avril.

Le Temps (Suisse)

Big Brother, Big Data, Big Problem Il était une fois

Wednesday, 02 March 2016

Byline: Joëlle Kuntz

Section: oped

Opinion - Les personnages: - Olibrius Connecticus, habitant ordinaire de la planète numérique. Il a adhéré à la religion des codes de sécurité qui lui promet l'épanouissement de son moi sous la protection de ses mots de passe confidentiels. Il vénère saint Assange et saint Snowden, qui ont risqué leur vie pour démontrer combien sa liberté est menacée: Big Brother voit tout, écoute tout, contrôle tout. Big Brother, c'est tantôt la NSA qui enregistre Angela Merkel même quand elle dort, tantôt Google et ses caméras du coin de la rue. Olibrius se couche le soir avec l'impression contradictoire que ses codes sont sûrs mais qu'ils ne servent à rien contre Big Brother. Il s'arrange comme il peut de cette bizarrerie.
- Foreign Bureau of Investigation, FBI. Superpuissance policière prise en flagrant délit d'incompétence en matière électronique: après une fausse manoeuvre sur un iPhone abandonné par un terroriste sur la scène du massacre de San Bernadino, en Californie, le FBI a perdu tout moyen d'entrer dans la mémoire de l'appareil. Il somme Apple de lui en fournir un. Il y va de la sécurité des citoyens des Etats-Unis. L'Etat ne peut assumer la tâche de protection que ceux-ci lui délèguent démocratiquement que si chacun consent à sacrifier sa part de souveraineté.

- Apple, entreprise admirée dans la vente de connectivité confidentielle. Elle compte parmi les plus grandes capitalisations boursières de tous les temps. Elle résiste aux demandes gouvernementales. Produirait-elle une entrée - une seule - dans un téléphone vendu comme sécurisé qu'elle perdrait toute

la confiance placée en elle (exprimée en monnaie). Ce n'est pas la première fois qu'on la cherche, sous des prétextes bons ou moins bons et presque à chaque fois elle dit non.

- Silicon Valley, chef-lieu de l'utopie technologique, équivalent américain d'un Arc-et-Senans qui aurait réussi avec l'idéologie libertaire ce qui a échoué avec le communisme primitif. Là s'élaborent les conditions matérielles de l'Homme augmenté, maître de l'Information. Big Data étant aussi Big Money, Silicon Valley est unie derrière Apple contre FBI. Il y va des milliards investis dans la promesse d'une libération par les machines. Dans ce milieu de chercheurs et de marionnettistes qui inventent les moyens de tout savoir sur tout le monde règne le culte de la vie privée, du secret et de la protection des données.

- Daech, nom générique pour terrorisme, emprunté à la faction criminelle irako-syrienne qui sème la terreur et la mort un peu partout dans le monde. C'est le mal. Syed Rizwan Farook et sa femme Tashfeen Malik, les deux auteurs présumés de la tuerie de San Bernardino (14 morts, 21 blessés, le 2 décembre 2015) auraient agi au nom de Daech dont, aux dires des enquêteurs, ce serait la première attaque sur sol américain. Comme il se doit, le mal est le déclencheur de la contradiction dramatique. Par le scandale du crime, il expose la vraie situation des protagonistes.

La scène: Olibrius est la figure tragique. Doté des deux pouvoirs qui comptent, le pouvoir d'achat et le pouvoir politique, il est impuissant à déterminer lequel est pour son bien ou comment combiner les deux, si même ils se combinent. Le consommateur de machines, en lui, dispute la prérogative au citoyen électeur. Où sa liberté est-elle la mieux placée? Dans la défense de sa vie privée vendue par Apple? Dans la défense de la loi proclamée par le FBI? Seul devant son écran, Olibrius, qui n'est pas un mauvais bougre, soupèse les enjeux. Big Brother, Big Data, Big Problem. Dans quel monde est-il? Il écoute plein tube les choeurs de Silicon Valley qui accablent l'Etat fouineur. Musique agréable aux fidèles interconnectés des Nouveaux Territoires de l'humain machinisé.

C'est alors que la bombe explose, signée Daech. Le moi blindé d'Olibrius éclate en petits morceaux. Ses mots de passe se répandent sur le parquet, des chiffres et des lettres sans plus d'utilité. Ses illusions s'écoulent, goutte à goutte, jusqu'à la dernière.

Le Figaro

Le patron du FBI demande au Congrès d'obliger Apple à collaborer

Wednesday, 02 March 2016

Byline: Pierre-Yves Dugua

Section: general

Washington - En plein bras de fer judiciaire et technique avec la firme à la pomme, il veut la contraindre à ouvrir l'iPhone d'un des terroristes impliqué dans l'attaque de San Bernardino.
Apple a crée depuis 2014 une génération de smartphones inviolables et les polices américaines en sont outrées. Elles veulent renouer avec la situation qui prévalait avant septembre 2014, date de la sortie du système d'exploitation «iOS 8», logiciel au coeur des iPhone, perfectionné depuis avec l'iOS 9.

Devant la Commission judiciaire de la Chambre des représentants, mardi à Washington, le patron du FBI et le procureur de l'État de New-York ont plaidé leur cause, dans le contexte de la controverse suscitée par le refus d'Apple d'aider les autorités fédérales à accéder aux données de l'iPhone d'un des terroristes de l'attaque de San Bernardino le 2 décembre dernier.

Au même moment, à San Francisco, la Secrétaire à la Justice, Loretta Lynch, a prôné un dialogue entre le gouvernement et toute l'industrie de la haute- technologie, en déclarant qu'on ne pouvait «laisser une seule société trancher à elle-seule le débat sur l'encryptage».

«En mai 2012, Apple expliquait que son iOS 7 offrait «une protection solide contre les virus, le malware et les autres méthodes qui compromettent la sécurité d'autres plateformes». Et pourtant avec iOS 7, Apple conservait sa capacité à aider - pour reprendre leurs mots de l'époque - «la police à enquêter sur les vols et autres délits, à rechercher les enfants disparus, à localiser un patient souffrant d'Alzheimer ou à prévenir un suicide». Apple elle-même démontrait alors qu'un cryptage fort et qu'un respect des décisions de justice n'étaient pas incompatibles» a rappellé mardi Cyrius Vance Jr., procureur élu du comté de New-York.

«Nous voulons que les fabricants de smartphones offrent le même type d'encryption qu'Apple employait avant l'iOS 8» a résumé ce démocrate. Il s'exprimait aussi au nom de ses collègues d'autres États, de l'Illinois et du Texas par exemple. Son laboratoire se trouve aujourd'hui incapable de déchiffrer les données présentes dans 175 iPhone et iPad.

Un iPhone sur deux saisis par la police de New York ne peut être exploité

Désormais un de ces appareils sur deux saisis par la police de New York ne peut être exploité. Or «dossier après dossier, nous avons vu des homocides aux kidnappings, des trafics de drogue à la fraude financière et à l'exploitation des enfants, que les preuves décisives venaient des smartphones, des ordinateurs et des communications sur internet» a renchéri James Comey, le Directeur du FBI.

Les procureurs et policiers ne demandent pas de pouvoirs nouveaux. Ils souhaitent simplement le retour à la situation passée: celle antérieure au traumatisme de la Silicon Valley par l'affaire Snowden. À cette époque les géants de la technologie acceptaient les protections mises en place par la constitution américaine. Au terme de son 4ième amendement, les perquisitions et fouilles sont possibles, à condition qu'elles soient autorisées par un juge indépendant sur la base de présomptions sérieuses. «Les iPhones

sont maintenant les premiers produits de consommation de l'histoire américaine à se trouver hors de portée des mandats de perquisition prévus par le 4ième amendement» résume Cyrius Vance Jr..

Forcer Apple à changer de politique et de technologie

Sa démarche, tout comme celle du FBI, vise donc explicitement à créer un précédent, contrairement à ce que James Comey avait dit la semaine passée. En profitant du traumatisme de l'attaque terroriste de San Bernardino le 2 décembre 2015, ils tentent de forcer Apple à changer de politique et de technologie. Ils ne veulent pas simplement qu'on les laisse décrypter l'iPhone d'un terroriste islamique, assassin de 14 personnes. Ils veulent un nouveau régime législatif encadrant et garantissant ce privilège à l'avenir.

Apple, représenté mardi à Washington, par son Directeur juridique, Bruce Sewell, réplique que le FBI et les procureurs étatiques demandent de dégrader la sécurité de tous ses nouveaux iPhone. Créer un outil pour dévérrouiller ses smartphones est inacceptable aux yeux d'Apple: cela reviendrait à ouvrir une brèche dans laquelle potentiellement des criminels pourraient s'engouffrer pour violer les secrets de millions de personnes.

Asharq Al-Awsat

Facebook Executive Jailed in Brazil

Wednesday, 02 March 2016

Byline: Staff Report

Section: general

Sao Paulo - Court officials in Sergipe state confirmed that a judge had ordered the jailing of Facebook Vice President for Latin America Diego Dzodan. Thus the Brazilian police arrested the senior Facebook executive on Tuesday as a dispute accelerated over a court's demand that the company provide data from its WhatsApp messaging service to help in a private drug- trafficking investigation.
However the federal police in Sao Paulo state said he was being held there for questioning. To avoid compromising the ongoing criminal investigation, the law enforcement officials withheld further information about the nature of their request to the messaging service that Facebook Inc acquired in 2014.

The arrest came as social media and Internet companies face mounting pressure from governments around the world to help them spy on users and filter content. Such arrests of officials from social media companies are very rare, though not exceptional, since the companies typically comply with local court

orders, especially from countries where they have branch offices. However Facebook called this arrest as an "extreme and disproportionate measure".

Marcia Hoffmann, Internet law attorney, said that WhatsApp is a company that was launched very focused on U.S. laws, however now that it's owned by a company with people and resources in other countries, there is more leverage for those governments to put pressure in new and in different ways. Consequently arresting executives is one of them.

Internet freedom activist, Rebecca MacKinnon stated that "Precisely because these large global Internet companies have staff in many countries who are vulnerable to legal action including arrest and criminal charges, they generally do comply with legally binding requests from authorities for user data or to remove or block content in those countries where they have 'boots on the ground".

Because it did not have staffs scattered around the globe; unlike and previous to its acquisition by Facebook, California-based WhatsApp had less skin in the game in disputes with governments outside the United States.

Meanwhile details of the case remain foggy; court officials said the judge in Brazil resorted to the arrest after issuing a fine of 1 million reais ($250,000) to compel Facebook to assist investigators to access WhatsApp messages that are relevant to their drug-trafficking investigation.

Which is probably impossible since WhatsApp began using end-to-end encryption technology in 2014 that prevents the company from monitoring messages that travel across its network, said Christopher Soghoian, principal technologist with the American Civil Liberties Union.

Soghoian said that the arrest raised as Apple Inc finds itself at odds with the United States government on parallel grounds. "They are on use of technology in an attempt to take themselves out of the surveillance business,".

Apple has refused the U.S. prosecutors' request of the company to build a software tool that helps investigators unlock the iPhone used by one of the shooters in the San Bernardino, California, attacks. The refuse came as with Apple stating that this would set a dangerous precedent that would make its customers vulnerable to spying.

Although the confrontations hardly rise to the prominence of Apple's current standoff with the U.S. authorities, yet privacy concerns have previously put Facebook at odds with Brazilian law enforcement seeking evidence in criminal cases.

In December, a judge suspended Facebook's popular WhatsApp phone-messaging service in Brazil for about 12 hours after it failed to fulfill both of the court orders when demanded to share information in a criminal case.

According to legal expert Ronaldo Lemos, a chief architect of that 2014 law, Brazil passed an Internet law two years ago intended at streamlining thorny legal issues, but lower courts still have vast discretionary powers.

Lemos stated that the "The court of appeals tends to be more sensitive in these cases, but the lower courts are still tough, as today's decision shows".

Xinhua News Agency

S.Korean PM warns of cyber attacks from DPRK

Wednesday, 02 March 2016

Section: general

South Korean Prime Minister Hwang Kyo-Ahn on Wednesday warned of possible cyber attacks from the Democratic People's Republic of Korea (DPRK), instructing officials to block such attacks in advance. Hwang visited a center in Seoul for countermeasures to Internet infringement, saying that a close cooperation system should be built between the military, the government and the civilian sector to blockade the DPRK's possible attacks in cyberspace in advance.

The prime minister said that top DPRK leader Kim Jong Un had ordered officials to muster up capability for anti- South Korea terrorist attacks, which raised possibility for the DPRK's cyber provocations.

South Korea's spy agency reportedly made mention of Kim's such order without elaborating on where the agency got the information.

Hwang said the DPRK had staged massive cyber attacks against South Korea after conducting nuclear tests, instructing officials to detect such attacks at a right time and recover attacked networks successfully.

He also urged people to update security vaccines on their PCs and smartphones and to refrain from opening suspicious emails or text messages in order to minimize possible cyber attacks from Pyongyang.

His comments came amid rising concerns about DPRK's terror attacks following its fourth nuclear test on Jan. 6 when the DPRK tested what it claimed was its first hydrogen bomb. On Feb. 7, Pyongyang launch a long-range rocket, which was condemned by outsiders as a test of banned missile technology.

L'Actualité
En 2012, le Service canadien du renseignement de sécurité (SCRS) a cherché à savoir
Wednesday, 02 March 2016
Byline: Vincent Destouches

Ottawa - En 2012, le Service canadien du renseignement de sécurité (SCRS) a cherché à savoir si Anonymous avait réellement l'intention de s'en prendre au réseau électrique.
Wikimedia

Le 21 février 2012, le Wall Street Journal a révélé l'inquiétude dont avait fait part le général Keith Alexander, alors directeur de la National Security Agency (NSA), à de hauts fonctionnaires de la Maison-Blanche. Il craignait que le groupe «hacktiviste» Anonymous «puisse avoir la capacité, d'ici un an ou deux, de provoquer une panne de courant limitée».

Ces allégations, qui seraient plus tard qualifiées d'alarmistes, ont eu des répercussions jusqu'au Canada. Au printemps de la même année, la spécialiste en piratage informatique Gabriella Coleman s'est rendue dans la banlieue d'Ottawa sur invitation du Service canadien du renseignement de sécurité (SCRS). Pour l'agence, Gabriella Coleman représentait un atout unique, puisqu'elle avait passé «plus de temps devant [son] écran d'ordinateur à "chatter" avec des membres d'Anonymous que toute autre personne étrangère au collectif, à part peut- être les informateurs», selon les propres mots de l'intéressée.

Paralysée d'appréhension, et encore plus anxieuse de dévoiler des détails qu'elle aurait préféré taire, Gabriella Coleman s'est vite rendu compte que la quarantaine d'espions canadiens venus à sa rencontre avaient un but autre que celui d'écouter son exposé: le SCRS souhaitait savoir si, à la lumière des propos tenus par la NSA, Anonymous pouvait réellement avoir l'intention de s'en prendre au réseau électrique. «J'imagine que le Canada a été amené à s'intéresser de plus près à ce groupe énigmatique sous la pression de son voisin du Sud», a écrit Coleman -- qui est aujourd'hui à la tête de la Chaire Wolfe en littératie scientifique et technologique de l'Université McGill -- dans son journal d'enquête anthropologique Anonymous: Hacker, activiste, faussaire, mouchard, lanceur d'alerte (récemment publié en français).

Même si elle ne pouvait scruter tous les salons de discussion - - d'autant qu'Anonymous ressemble à un labyrinthe générateur d'autres labyrinthes --, Coleman leur a alors répondu qu'aucun indice ne permettait de l'envisager. Anonymous, qui ne défend ni philosophie ni programme politique clair, n'avait même jamais appelé à perpétrer ce genre d'attaques. «D'ailleurs, le moindre projet d'action radicale, y compris la divulgation de données privées touchant des policiers hostiles, suscite de houleux débats moraux.»

À ses interlocuteurs de l'agence du renseignement, elle a résumé l'état d'esprit d'Anonymous, à cheval entre l'humour noir (le lulz, terme dérivé de lol) et l'irrévérence, par un trait d'esprit qu'un Anon (membre du collectif) avait partagé dans la foulée des accusations de la NSA.

«C'est vrai. Nous allons bel et bien foutre en l'air le réseau électrique. Nous saurons que nous avons réussi quand tout l'équipement dont nous avons eu besoin pour organiser la campagne sera devenu complètement inutilisable.»

Et Coleman de décrire le soulagement des agents du renseignement:

«Les postures se décontractent aussitôt. Le rire se fait de nouveau entendre chez les espions canadiens. J'ai vraiment l'impression que mon témoignage les a soulagés. Ils peuvent maintenant retourner à des affaires plus pressantes.»

Au coeur d'Anonymous se trouvent le maintien de l'anonymat, la libre circulation de l'information et la défense de la liberté d'expression - rien de plus normal pour un groupe né sur Internet. Mais ses préoccupations ne se limitent pas aux libertés civiles. Les membres ont participé à diverses campagnes au cours des dernières années, de la dénonciation de viols (notamment à Halifax) au soutien actif des militants du Printemps arabe, en 2011. Bref, l'eau a coulé sous les ponts depuis l'époque antérieure à 2008, où le nom d'Anonymous servait «presque exclusivement à ce qu'un Anon a qualifié de "salopage sur Internet" (Internet motherfuckery)».

«Il est pratiquement impossible de connaître à l'avance le moment et les motifs de la prochaine action d'Anonymous, pas plus qu'on ne peut prédire l'apparition d'un nouveau noeud, le succès d'une campagne et un changement d'orientation ou de stratégie en cours d'opération. C'est sans doute en raison de son comportement imprévisible qu'Anonymous fait si peur aux gouvernements et aux entreprises du monde entier», écrit Coleman dans son livre.

Son caractère imprévisible est également lié à la diversité des sensibilités qui coexistent au sein du dédale infini qu'est Anonymous. Le groupe repose sur le principe selon lequel n'importe qui peut revendiquer le nom d'Anonymous en toute légitimité, ce qui lui a permis de se répandre aux quatre coins du monde, devenant le visage populaire de l'agitation. La diversité de formes par lesquelles Anonymous se manifeste donne ainsi lieu à des guerres intestines, tant les réseaux et les sous-groupes sont nombreux et parfois en désaccord.

«La plupart d'entre nous sommes motivés par l'humour. C'est pourquoi il ne faut pas s'étonner de nos disputes fréquentes avec des groupes qui, tout en se réclamant d'Anonymous, n'ont plus nos bonnes grâces, comme [...] les nouveaux Anons strictement militants d'Occupy Wall Street, les adeptes des théories du complot ou d'autres entités beaucoup trop sérieuses qui se parent de ce nom», a expliqué un conférencier d'Anonymous à une classe d'étudiants de Coleman.

L'auteure a fourni un exemple de ces désaccords: une campagne de protestation contre l'Accord commercial anticontrefaçon (ACTA), qui visait «la mise en place d'une réglementation d'envergure qui criminaliserait toute violation du droit d'auteur et inciterait les fournisseurs d'accès Internet à pister et à surveiller leurs clients en vue d'établir leur profil». La discussion entourant l'ACTA sur un canal IRC (Internet Relay Chat) a montré l'étendue des visions qui s'affrontent, d'autant qu'il y a au sein

d'Anonymous un débat virulent sur la dimension éthique de l'attaque informatique par saturation. (La distributed denial-of- service (DDoS) est une tactique visant à bloquer l'accès à des serveurs Web en les submergeant de requêtes.) La question est de savoir si elle est un «acte de liberté d'expression ou un acte visant à priver autrui de ladite liberté». L'échange a aussi permis de mettre en valeur le processus peu commun par lequel un projet peut être décrété officiel: il suffit que quelqu'un le déclare comme tel et qu'assez de monde y soit favorable.

«Fin août 2010, un Anon s'exprimant sous le nom de golum (qui n'est pas son pseudo habituel) se connecte au forum et y annonce hardiment son intention de faire avancer le dossier en menant une attaque par saturation contre le site du bureau du représentant au commerce des États-Unis, ustr.gov, le 19 septembre à 21 heures HNE. [...] L'annonce de golum suscite des questionnements chez beaucoup de participants.

[...] pourquoi si vite?

Parce que c'est un dimanche et que tout le monde aime les dimanches

mais encore... pourquoi si vite?

Parce que j'ai lancé un dé

Et qu'il est tombé sur 19

Je prédis que le 19 septembre les gens auront une prise de conscience

Fais-moi confiance. Le 19 septembre.

fais-moi confiance à propos d'une date choisie sur un coup de dé

Même si tous les participants à la discussion rejettent violemment sa proposition, golum reste inflexible:

Peu importe. Écoutez, j'ai entendu tous vos arguments contre une attaque par saturation. Mais le fait est que nous devons les réveiller.

[...]

Je sais bien qu'une attaque par saturation pourrait nuire à notre cause.

Mais je crois que le jeu en vaut la chandelle.

en ce qui me concerne, n'étant pas d'accord, je ne participerai pas à une attaque par saturation

Nous devons attirer l'attention

<+void> OMG C'EST ANONYMOUS, TOUT CE QU'ILS FONT C'EST DES ATTAQUES PAR SATURATION, OMGOMGOMGOMGOMG [...]

Non.

matty, comment ça s'est passé ta prise de contact avec les politiciens?

Ouais, j'ai toujours haï les attaques par saturation

Écoutez. J'ai saisi tous les arguments, je voulais juste dire qu'on devrait le faire.

Nous ne sommes PAS en train de mener une attaque par saturation. C'est seulement dans 20 jours.

20 jours, c'est long.

Quelques Anons énumèrent alors les risques juridiques d'une telle opération en soulignant le fait que le gouvernement des États-Unis n'est pas une cible comme les autres, puis jugent la discussion terminée. (Notons que leur évaluation des risques d'arrestation s'avérera juste: au moins 27 individus seront mis en accusation pour la série d'attaques par saturation qui suivra; d'autant qu'aux États-Unis, s'en prendre à quiconque un tant soit peu célèbre peut attirer de graves ennuis.)

c'est pas justin beiber, c'est le gouv américain bordel [...]

SVP, tous, écoutez-moi quand je parle

Je vais bien me marrer quand tu iras en prison

je suis pas là pour le foutu lulz

C'est officiel. Commencez à vous préparer. »

Pour plus de détails, consultez le livre Anonymous: hacker, activiste, faussaire, mouchard, lanceur d'alerte (Lux Éditeur).

Toronto Star
Use of metadata crucial, CSE insists
Thursday, 03 March 2016
Byline: Greta Bossenmaier

Bring our spies to heel, Editorial Feb. 25
In response to your editorial related to the Communications Security Establishment (CSE), I would like to provide a few clarifying facts.

First, CSE's authority to acquire and use metadata is founded in the National Defence Act.

Secondly, CSE discovered the issue on its own, proactively disclosed it and took steps to address it.

Thirdly, the potential privacy impact to Canadians has been assessed as low because the metadata that was shared did not contain enough information on its own or contextual details to identify individuals associated with it. Additionally, other important safeguards and privacy protection measures are in place, and applied, as confirmed by the CSE commissioner, by both CSE and its Five Eyes partners.

CSE's work is critical to the national security of Canada and Canadians. Our work directly helps protect the lives of deployed Canadian Armed Forces and coalition members (most recently in support of Canada's Operation Impact), we detect foreign-based extremist plots against Canada and our allies, we identify hostile intelligence agencies' activities against Canada and against our national interests and we detect and thwart over 100 million malicious cyber attempts against government of Canada networks every day.

None of this is possible without the use of metadata. Metadata is critical to understanding the communications environments in which CSE operates and the behaviours of our foreign intelligence targets. It is the context but not the content of a communication. Context, not content.

CSE is committed to continuous improvement, to protecting the privacy of Canadians and to contributing to Canada's national security.

Greta Bossenmaier, chief, Communications Security Establishment, Ottawa

ABC (Australia)
Former Anonymous member Adam John Bennett given suspended sentence for website hacking
Thursday, 03 March 2016
Byline: Staff reporter

A Perth judge has given a former member of online activism group Anonymous a suspended sentence for helping hack into websites in 2012.
Adam John Bennett, 42, pleaded guilty to six charges including aiding another person to cause the unauthorised impairment of electronic communications.

Five of the offences occurred in November 2012, when members of the group Anonymous hacked into websites around the world.

Bennett used the pseudonym 'Lorax' for his online activities, and had an online radio show, as well as thousands of followers.

The court was told when Bennett's Scarborough home was searched in 2014, a Guy Fawkes mask was found, along with audio streaming and studio equipment.

It was alleged there were plans for a "mass defacement" of sites planned to mark Guy Fawkes' Day in 2012.

The court was told Bennett helped a juvenile in NSW dubbed 'Juzzy' to hack into a variety of sites, including those operated by the Australian Agency for Education and Training, the Australian Film Institute, Anchor Foods, and the Food Industries Association of Queensland.

When the public tried to access a hacked site, they found a message from the group in red text on a black background.

Prosecutor Patricia Aloi told the court "the plan was to get a much larger number of sites".

She said the "impact could be described as a nuisance, could be described as lost productivity", and such offending could escalate.

Ms Aloi said the Commonwealth believed a custodial sentence was appropriate.

Lawyer argues rant was one of 'political ideology'

Acting on behalf of Bennett, Darren Renton told the court the hacked web pages were accessible, and only the front page had the Anonymous "rant".

He agreed with Justice Phillip McCann's description of the offences as being "like barricading the front door and not the side door".

Mr Renton said the Anonymous rant was one of "political ideology" and there was no suggestion of financial or monetary gain, or sensitive information being accessed.

While the result was something akin to "digital graffiti", he said his client accepted he was breaking the law, and it was an illegal way to put forward a political view.

A sixth offence involved the website of Bennett's employer Cancer Support WA and that of HotCopper.

Bennett tested the sites for vulnerability to the Heartbleed security bug, and tried to access confidential information.

Mr Renton spoke of other communications Bennett had with various companies, and the Supreme Court of Tasmania, and Senator Nick Xenophon, in which he highlighted how they were vulnerable to hacking.

Bennett used the Anonymous Australia Twitter account, and Mr Renton said his client was being "altruistic".

But Justice McCann said the actions were more like bullying and intimidation, including when Velocity Internet was told "you have been warned".

'Immature rants of the schoolyard'

Justice McCann was highly critical of Bennett, who he referred to as a "creepy pest" and an "immature creep who doesn't mind his own business".

He said "as a private citizen he has no business pestering people like Nick Xenophon".

Justice McCann said there was a "high level conspiracy to commit anarchist acts".

He highlighted part of the rant which said information about corporation and governments should be publicly available, and called it "a recipe for anarchy".

Justice McCann said it was not a political ideology, more like "immature rants of the schoolyard".

He said Bennett, who was in his late thirties when the offences occurred, was "grossly immature" with an "unjustified sense of self worth".

But he said to jail Bennett, who had "basically never grown up", would make him a martyr, and he should instead be given the "21st century equivalent" of being in the stocks.

Justice McCann said while there was "insufficient evidence of damage" by the hacking in 2012, there was malice.

He said the use of the internet was a privilege and not a right.

Bennett was given a sentence of two years' imprisonment, suspended for two years, as well as 200 hours of community service and an intensive supervision order.

Bennett, a long-time lifesaver at Scarborough Beach, first entered guilty pleas in October 2015, and the fact he had shown remorse was taken into account.

Le Soir (Belgique)
Un « bouclier » de papier mâché
Thursday, 03 March 2016
Byline: Alain Jennotte

Bruxelles - Technologies Les critiques se multiplient contre le traité Privacy shield
Le traité entre l'Europe et les Etats-Unis pour la protection des données risque d'être l'objet de recours. Son contenu ne répond guère aux standards européens en matière de protection de la vie privée.

A peine dévoilé par la Commission européenne, le nouvel accord Privacy shield, conclu entre l'Europe et les Etats-Unis sur la protection des données personnelles, reçoit déjà une volée de bois vert. Ce « bouclier de confidentialité », dont les détails ont été publiés lundi, est le futur cadre juridique énumérant les garanties pour la protection des données personnelles des Européens, lorsqu'elles sont transférées aux Etats-Unis par des entreprises américaines, comme Google ou Facebook.

Privacy shield a été négocié pour remplacer l'accord précédent, Safe Harbor, conclu en 2000. Celui-ci avait été sèchement dégommé par la Cour européenne de justice, dans un arrêt très ferme rendu en octobre dernier. La Cour estimait notamment qu'en raison de la surveillance massive des données par ses agences gouvernementales, les Etats-Unis n'offraient plus un niveau suffisant de protection pour les données.

Le nouveau texte est loin de faire l'unanimité. « La Commission a fait fi de l'arrêt de la Cour de justice , note Emmanuel Foulon, porte-parole du député européen Marc Tarabella (PS). Le texte précise que les Américains auront le droit d'épier toutes les données qu'ils voudront, dès qu'ils estimeront avoir un motif pour le faire et cela sans avoir à donner la moindre justification » .

Le nouveau traité va mettre en oeuvre de nouveaux mécanismes de supervision afin de s'assurer que les entreprises américaines qui stockent des données européennes respectent toutes leurs obligations, sous peine de sanctions. Un ombudsman indépendant sera mis en place, permettant aux citoyens qui le souhaitent de vérifier que l'intégrité de leurs données a bien été respectée. Mais il sera également possible pour les citoyens et les entreprises de s'adresser à leur autorité nationale de protection des données pour porter plainte.

Pour la première fois, se félicite la Commission européenne, les Etats-Unis se sont engagés par écrit à s'abstenir d'un accès généralisé aux données européennes stockées chez eux. Mais tout aussitôt, l'engagement américain s'est vu assorti d'une série de conditions tellement large qu'il ne signifie plus grand-chose. Ainsi, dans les courriers officiels annexés au traité, les Etats-Unis précisent qu'ils pourront procéder à de la collecte massive de données dans six cas spécifiques. Parmi ceux-ci, la cybersécurité, la lutte contre le terrorisme, les menaces criminelles transnationales ou la détection de certaines activités menées par des pays étrangers. Les exceptions ratissent très large.

Pour l'Autrichien Max Schrems, dont le recours avait été à l'origine de l'arrêt de la Cour européenne de Justice, ces licences que s'accordent les Etats-Unis montrent que, malgré des améliorations sur des points périphériques, le nouveau texte ne répond en rien aux exigences de la Cour européenne de Justice. Un échec qui s'explique par les profondes différences entre la législation américaine sur la protection des données et la nôtre.

« Les négociations se sont enlisées parce que les Etats-Unis ont refusé jusqu'au bout de lâcher du lest et ont joué la montre , estime Joe McNamee, le directeur exécutif d'Edri, une plateforme d'associations pour la défense des droits civils numériques. Et pour tenir le calendrier qui leur avait été imposé par le groupe européen des régulateurs des données personnelles, la Commission a fait une chose étonnante, début février : elle a affirmé qu'il y avait un accord. Mais son contenu n'existait pas vraiment. Ce n'est que cette semaine que les textes ont été rendus publics. La Commission s'est donc piégée elle-même et les négociateurs américains n'ont plus eu besoin de rien négocier du tout » .

Ils sont écrits dans les astres si le contenu du traité n'est pas modifié. En avril, les régulateurs européens des données doivent rendre un avis sur le texte. Il n'est pas contraignant mais pourrait peser politiquement. Cependant, ces régulateurs vont être mis sous haute pression. Un membre officiel de la Commission, cité par la newsletter spécialisée Euractiv , estime qu'il ne serait « pas sage »de la part des régulateurs européens de faire traîner le texte jusqu'à l'année prochaine et une nouvelle présidence aux Etats-Unis. Tous les ingrédients semblent déjà réunis pour que la Cour de Luxembourg soit de nouveau saisie du dossier.

The Australian Financial Review
Cyber threat is rising
Thursday, 03 March 2016
Byline: Tony Boyd

An Australian chief executive involved in a potential M&A transaction recently received a phone call telling him his computer systems had been hacked by a state-owned enterprise believed to be in China. He was shocked and immediately asked how the caller, Richard Bergman from PwC, knew what was happening when his own chief information officer had said nothing.

Bergman told Chanticleer his team at PwC had been monitoring activity on the "dark web" and picked up a significant increase in traffic between known offshore hacker-owned computers and the company in question.

PwC was subsequently called in to clean up the company's entire IT environment. The CEO's decision to make a large investment in his IT systems is in keeping with the findings of a survey into cyber security released this week by Cisco Systems.

Cisco said in its annual security report that security breaches forced companies to rethink their investment in protection.

When the security breaches are public the incentive to act is even greater.

Bergman is not a scare monger when it comes to cyber security. He uses examples from recent contractual arrangements to make rational statements about the readiness of Australian companies for cyber attacks.

His worrying conclusion is that apart from the big four banks and Telstra, there are very few companies that have made the necessary investments in cyber security.

The lack of preparedness for cyber attacks can partly be explained by the fact that companies are not matching their security measures with the way business is done.

The proliferation of joint ventures, minority investments in other companies, collaboration with third parties and the use of outsourcing have created a raft of opportunities for those seeking to break into computer systems.

A survey by PwC released in October last year found Australia had the highest number of cyber security incidents in the previous 12 months.

The total number of incidents was 9434, more than double the previous year. The growth in the rest of the world was about 38 per cent.

Bergman's dire analysis of the readiness of companies to deal with cyber security threats is timely.

Submissions close this Friday for the federal government's mandatory data breach notification discussion paper. PwC's draft submission to that process highlights the need for many amendments to clarify the obligations of companies.

The bigger picture in relation to cyber security policy in Australia is in a state of flux.

Lynwen Connick, first assistant secretary cyber policy and intelligence in the Department of Prime Minister and Cabinet, is leading a review of cyber security.

This has involved wide consultation and includes advice from an expert panel that includes Telstra's chief information security officer Mike Burgess and Business Council of Australia CEO Jennifer Westacott.

The review has already identified that the single biggest weakness in Australia's approach to cyber security is the lack of co- ordination between all those involved in protecting information, intellectual property, intelligence and privacy.

As Bergman says, the sovereign states and organised criminals are sharing information about how to attack companies and identify their weaknesses and it would be crazy for the defenders against cyber security not to do the same.

ANZ fluffs it

ANZ Banking Group's 60-year flirtation with wealth management has ended in ignominy.

The bank set up ANZ Funds Management in 1957. The bank started to take the business seriously in the late 1980s and early 1990s.

By that time the bank had expanded into a range of different wealth management product lines including life insurance, trustee services, unit trusts and funds management. But this hotch-potch of entities were never properly consolidated or given a common purpose.

The bank's wealth management division never actually figured out the answer to one simple question: Why do we exist?

The result was that the bank stumbled from one failed strategy to another. This was compounded by failures in execution.

If there is a pecking order of notable mistakes made by ANZ in wealth management the one involving Frank Russell would have to at the top.

The bank set up a partnership with the American firm, which is famous for its indices, to offer ANZ clients a range of multi-manager investment products.

This partnership exhibited confusion about where the value resided in the wealth management chain. ANZ appeared to put growth in total funds under management ahead of profit margins.

It paid Frank Russell about 60 basis points for the privilege of having its relatively vanilla funds management products. It would have been smarter for ANZ to have its own actively managed funds earning 100 basis points.

By the time ANZ moved to a new business model in 2002 it had about $2.3 billion in the Russell multi-manager products.

The next iteration of the strategy ranks second in the list of notable mistakes. This was the 50-50 joint venture with ING in the platform space. ANZ kept 100 per cent of the distribution and handed all asset management to ING.

This mistake was compounded by the fact that ANZ never addressed the problem of how to unwind the joint venture should that be necessary.

It did become necessary and the result was a mess. The global financial crisis meant ING was distressed and it was willing to change the arrangements.

The latter years of the wealth management business caused much frustration for former CEO Mike Smith, who never really got his head around why it was a failure.

The departure of Joyce Phillips spells the death knell of the wealth management experiment.

For some reason, a succession of chief executives and talented wealth management executives never figured out how to sell quality retail financial services products through the branch network.

It sounds simple but other three major banks have also struggled to achieve this marriage of banking and wealth.

National Australia Bank bought one of the best wealth management companies in Australia, MLC in 2000 and then spent the next 15 years taking the business nowhere.

It is being dismembered to ease the capital burdens within the group.

Commonwealth Bank of Australia's purchase of Colonial should have provided the perfect foundation for building the country's premier bancassurance business.

But the combination of the wrong remuneration incentives and slack oversight of the financial planning division was incredibly destructive.

It severely damaged the CBA financial planning brands. Just as important was the damage done to the reputation of the bank's financial planners within the CBA retail network.

The referral of highly prospective clients from the branch network to quality financial planners only works if there is a strong foundation of trust. It will take time to rebuild that at CBA.

Westpac Banking Corp stands out as the only one of the big four banks to have shown considerable success in using its powerful distribution network to sell wealth products.

Duopoly stigma

The High Court decision in relation to the non-renewal of the gaming licences in Victoria for Tatts and Tabcorp contains some damming comments about duopolies.

It is clear from the fact that these cases went all the way to the High Court that the duopolists had inflated ideas about their own importance.

The five learned High Court judges have made the not so startling comment that Tatts and Tabcorp could not see what any reasonable business person should have seen - the government power to end a duopoly.

Le Monde
Apple contre FBI, les dessous d'une polémique
Thursday, 03 March 2016
Byline: Ted Goranson

Chronique - Le refus d'Apple de déverrouiller l'iPhone de l'un des auteurs de l'attentat de San Bernardino, en Californie, le 2 décembre 2015, a déclenché une polémique publique qui va bien au-delà d'un simple conflit entre sécurité publique et droit individuel à la vie privée.
J'ai fait partie, pendant une longue période, de la communauté du renseignement des Etats-Unis. Ainsi, je pense que le FBI a déjà accès à l'iPhone en question : c'est un ancien modèle, qui utilise une technologie déjà mise en défaut dans d'autres contextes.

La demande du FBI à Apple a d'ailleurs un autre aspect étrange : pour quelle raison le gouvernement a-t-il ouvert un débat public sur cette question? Le FBI est la plus puissante organisation policière du pays, et Apple sera, en fin de compte, obligé d'obtempérer.

Pour mieux comprendre, il faut examiner la dernière gamme de téléphones d'Apple, qui diffère, sur un point crucial, de celle de l'iPhone incriminé : ils contiennent une nouvelle puce conçue en utilisant une technique développée par l'Agence nationale de la sécurité (NSA) américaine, et qui a ensuite été partagée avec les Israéliens. On retrouve à présent cette technologie dans les produits Apple, par l'intermédiaire de l'entreprise israélienne qui a mis au point cette puce.

Chacune de ces nouvelles puces possède une signature unique utilisée pour le chiffrement, associée à l'empreinte digitale de son utilisateur. Sans cette signature, il est impossible de décrypter un téléphone Apple sans accès physique aux éléments internes de sa puce, qui est elle-même impénétrable. Ce cryptage s'applique également à toute information communiquée par le téléphone à un service apparié, comme le système de messagerie du géant américain.

Dans le passé, l'accès immédiat aux périphériques de téléphonie n'était pas pertinent pour le FBI, parce que les autorités disposaient d'un libre accès aux communications entrantes et sortantes de tout

téléphone. Mais, avec ses nouvelles améliorations de sécurité, Apple vient de fermer cet accès. L'entreprise ne refuse pas simplement un nouvel accès : elle retirera bientôt celui qui existe. Bien sûr, cela dérange le FBI.

Il est intéressant de noter que la NSA a pris une position différente. Les " portes dérobées " (backdoors) ont été reconnues comme dangereuses par le directeur de la NSA, l'amiral Mike Rogers, qui estime que " le cryptage est fondamental pour l'avenir. " Si l'accès aux communications privées est possible, n'importe qui peut l'utiliser dans n'importe quel but. Si un téléphone a une porte dérobée, il peut être ouvert par toutes les personnes qui ont une motivation suffisante : criminels, extrémistes ou gouvernements. Les autorités chinoises, par exemple, seraient ravies si Apple devait se conformer aux demandes du FBI...

Equilibre remis en question Cela fait des années que le FBI demande une porte dérobée à Apple. Alors qu'il effectue, en général, ces demandes en secret, il a fait le choix inhabituel de la rendre publique : l'objectif est, en prononçant le mot-clé " terrorisme ", d'inciter les médias et le législateur à répondre à l'indignation du public.

La plupart des arguments juridiques contre le " déverrouillage " de ce téléphone particulier font référence au droit à la liberté d'expression, protégé par la Constitution. Mais un meilleur parallèle est celui du droit de détention d'armes aux Etats-Unis.

A la fin du XVIIIe siècle, aucune autre technologie que celle des armes à feu n'était aussi avancée. La Constitution américaine a donc précisé que ces dernières ne pouvaient servir à limiter la liberté d'expression (premier amendement), que leur détention ne pouvait être refusée aux citoyens (deuxième amendement) et que les soldats armés ne pouvaient pas être cantonnés chez les citoyens (troisième amendement). Les neuvième et dixième amendements interdisent l'utilisation d'armes à feu dans le but de compromettre d'autres droits implicites le cas échéant.

Les technologies les plus puissantes à l'heure actuelle concernent l'information relative à nos pensées, à nos comportements et à notre santé. Si les rédacteurs de la Constitution américaine étaient vivants aujourd'hui, et aussi éclairés qu'ils l'étaient à cette période, le Bill of Rights se concentrerait probablement sur l'équilibre de l'accès à cette information, afin de s'assurer que le gouvernement n'outrepasse pas les limites de son pouvoir.

Avec cette demande publique du FBI, l'équilibre entre les citoyens et le maintien de l'ordre est remis en question. Nous devons nous demander s'il est pertinent, légalement ou d'un point de vue politique, que tout le monde (forces de l'ordre, pirates informatiques et terroristes) soit en mesure de posséder ou d'accéder à l'information.

L'affaire d'Apple penche déjà en la défaveur des citoyens. Une réponse plus réfléchie que l'envoi hystérique de tweets sera nécessaire de la part des femmes et hommes politiques américains. Compte

tenu du pouvoir actuel de l'information, ils doivent réfléchir aux conséquences juridiques de la demande du FBI.

Los Angeles Times
Phones lose place as hack target
Thursday, 03 March 2016
Byline: Paresh Dave

Los Angeles - Computer hacker Will Strafach had no trouble seizing control of the original iPhone. Same went for later generations over the next five years.
But by now, Apple Inc. has introduced so many layers of protection inside its flagship device that Strafach and others have moved on. As the frenzied hacking has subsided, publicly shared solutions to crack iPhone security are becoming harder to come by.

The frustration he and other hackers felt has hit law enforcement too. That's why agencies around the country say Apple is its last hope to unlock hundreds of smartphones important to investigations, and why the FBI is so forcefully going after Apple in its effort to get into the work iPhone of San Bernardino terrorist Syed Rizwan Farook.

Whereas a generation of hackers grew up tinkering with iPhones and Androids for fun, today's up-and-comers -- thwarted by the near- ironclad security of smartphones -- are shifting their focus to virtual reality headsets, self-driving cars, the cloud, mobile apps and other emerging online systems with less-tested locks.

Hackers like Strafach are instrumental in rooting out vulnerabilities in software and hardware. Their findings are used by specialty technology companies to design tools that extract and analyze data from devices, which are in turn used by law enforcement, technical consultants for attorneys and repair shops.

Nowadays, the more difficult task of smartphone hacking is falling to large, more well-financed teams at cybersecurity firms and secretive government departments, all of which are prone to closely guarding those vulnerabilities for national security reasons rather than sharing them with police.

"The better technology gets, the more rarefied and the smaller pool of true old-school hackers you'll have," said Greg Buckles, co-founder and principal analyst of forensics industry research firm EDJ Group.

IPhone software developer Ryan Petrich said he expects hobbyists to be outgunned within the next two years.

"It will be infeasible to develop an exploit outside a large team with very experienced security researchers," he said. "They will do things like attack specific parts of the system, but you aren't going to see ... full system access."

Strafach was a big part of the iPhone jailbreaking community, which finds holes in the iPhone operating system that can unleash unauthorized privileges.

For example, Apple allows installation of only apps it approves. A jailbroken phone eliminates the restriction.

The downside is that jailbreaking risks corrupting the phone permanently if the technical process goes awry. And demand for jailbreaking tools relaxed as iPhones began to include some of the functionality once available only on jailbroken devices.

As a teenager, Strafach would trade jailbreaking tips with about 10 buddies -- the Chronic Dev team -- in a private online chat room. They'd share their findings for others to use.

Jailbreaking tools have been "bit-for-bit critical" for forensics software makers to provide easy ways to read the contacts, messages, app data and other information on smartphones, he said.

Getting into the first- generation iPhone, released in 2007, was easy -- Strafach compares it with finding a loose brick in a wall.

But the time he and his collaborators spent looking for loose bricks increased with each new iPhone and iPhone operating system -- and there were additional hurdles.

It was as if the prize they were after was now also protected by cannons, a moat filled with alligators and a chain-link fence. To make matters worse, software updates would change the order and strength of obstacles.

By iOS 7 in 2013, the multilayered defense was overwhelming. Apple went "wild," over-securing systems "that didn't need more security," Strafach said.

He went on to start Groton, Conn.-based Sudo Security Group Inc., which is developing software for businesses to control which apps employees may download onto their mobile devices.

Nowadays, hackers can generally get only a piecemeal view into the iPhone. There is scanning software as well as passcode- guessing gadgets that can get some data from newer iPhones that are locked and running iOS 8 or iOS 9.

But no publicly known process can extract their entire contents the way they could on earlier operating systems.

One upside, Strafach said, is that the dried-up market "makes me feel safe to have an iPhone."

Strengthened mobile device security has been a major force holding back growth of the forensics-tools industry.

Other jailbreakers left for technology companies as they aged, typically driven off like Strafach by a variety of reasons -- stronger security among them. Others like George Hotz, who's developing a self-driving car, are getting ahead of tech's next big trends.

Jailbreaking remains big in China, where technology giants and advertisers sponsor efforts, labor costs are lower than those in the U.S. and demand for the pirated content available through unauthorized apps is incredible.

But security concerns and language barriers make their tools less viable outside of China.

Others haven't given up. Irvine-based Susteen Inc. dedicated several employees to uncovering vulnerabilities in iOS 9, spokesman Jeremy Kirby said.

And the company is actively looking to pay outside researchers for ideas.

British tools shop Fonefun has turned to makeshift solutions, like taping down the power button on iPhones, tearing open the device and soldering in new wiring to overcome restrictions on passcode-guessing.

"It's all about persevering until you find something that works," said Fonefun's Mark Strachan. "And hopefully we can get something positive out of that before Apple releases a new iOS and closes it."

Since iOS 9 debuted in September, Apple already has addressed more than 70 security issues through updates, according to mobile security provider NowSecure. Such figures give experts confidence that there always will be a way in.

But they acknowledge the only surefire way to penetrate Apple's top security measures is to get a hold of the company's digital stamp, which is what the FBI is seeking in the San Bernardino terrorism investigation.

Otherwise, "law enforcement is kind of in a pickle," Petrich said.

Wall Street Journal
Beijing Looms Large in iPhone Battle
Thursday, 03 March 2016

Byline: Li Yuan

Beijing - Apple's refusal of the Federal Bureau of Investigation's request to help unlock a shooter's iPhone has been a hot topic not only in its home country but in its biggest foreign market: China. Some Chinese have questioned whether the move is a marketing stunt, but others have supported Apple for standing up to the government -- something unimaginable for Chinese companies. Some also have asked: What if the Chinese government asked Apple to do the same thing? Could Apple say no?
That question points to a significant issue for the company in the current standoff: Complying with the FBI in the San Bernardino, Calif., iPhone case could make it much harder for Apple to rebuff the demands of repressive governments in China and elsewhere abroad for access to the phones of, say, dissidents. It's an important concern for Apple, which gets most of its revenue from outside the U.S. The company derives roughly 25% of its revenue from the greater China region, which includes the mainland, Hong Kong, Macau and Taiwan.

Apple hasalluded to this issue, without naming China. In its filing to a federal court in California last week, Apple warned about the dangers of building a backdoor into the iPhone. "Once developed for our government, it is only a matter of time before foreign governments demand the same tool," the filing says.

Benjamin Qiu, a partner in law firm Loeb & Loeb's Beijing office, says if Apple were to lose the battle with the FBI, China's government would have every reason to make similar requests.

"Compared to the Chinese government, FBI is a pushover," he says.

China's State Internet Information Office, which regulates the Internet, didn't respond to requests for comment.

On its privacy Web page, Apple says it "has never worked with any government agency from any country to create a 'backdoor' in any of our products or services."

Chinese technology companies are used to accommodating their government's demands. Executives say they have to surrender whatever user information the government requests, and abide by frequent updates on content to be censored.

Says an executive at one Chinese Internet company, "When government says, 'Jump,' we're expected to ask, 'How high?' "

Increasingly, Beijing is trying to regulate Western tech companies in a similar fashion.

A new Internet regulation, effective next week, bars foreign companies from publishing online content in China without prior approval. A draft Cyber Security Law, under review, would require Internet network operators to provide authorities with technological support for national security and criminal

investigations -- which Amnesty International, a rights group, says could make it easier to involve companies incensorship and surveillance.

"Since China emphasizes national security more than personal-data protection, tech companies may well be required to follow the authorities' orders," says Yun Zhao, a law professor at the University of Hong Kong.

Edward Snowden's revelations that the U.S. government tapped into electronics gear overseas to spy on other governments have fed fears about foreign technology in China. As a result, many U.S. tech companies have lost market share in a critical market.

Apple's business has been a rare bright spot among multinational tech companies in China. In fiscal 2015, its revenue in China soared 84% to $58.7 billion. In the rest of the world, it grew 16%.

But Apple, like others, faces increasing scrutiny from China's government and state-run media. In 2014, after state television called the iPhone a "national security risk," Apple moved Chinese customers' data from overseas into a domestic facility operated by state-run China Telecom. Some critics said the move could make Apple products less secure.

At the time, Apple said the move would improve performance for its Chinese customers, adding that the data are encrypted and not accessible by China Telecom.

Jonathan Zdziarski, who researches Apple's software security, posted on Twitter that Apple stores iCloud data on China Telecom with the encryption keys outside the country. "This makes sense and reduces risk of data breach," he wrote.

Still, Chinese authorities have appeared eager to make Apple seem cooperative.

In an English poston its Twitter account in January 2015, People's Daily, the Communist Party newspaper, wrote "#Apple has agreed to accept China's security checks, 1st foreign firm to agree to rules of Cyberspace Admin of China." The post was accompanied by a photo of Apple Chief Executive Tim Cook shaking hands with Lu Wei, head of the State Internet Information Office.

All telecommunications manufacturers need to submit their products for government security testing in China, as in other countries, says a person close to Apple.

New York Times
Defense Secretary Says He's Not in Favor of a Data 'Back Door'
Thursday, 03 March 2016
Byline: Nicole Perlroth

San Francisco - Defense Secretary Ashton B. Carter assured an audience of computer security experts Wednesday that he was not in favor of a "back door" that would give the government access to data that is protected by encryption.
Speaking at the annual RSA Conference, Secretary Carter sought common ground with companies worried by Apple's fight with the Federal Bureau of Investigation over access to an iPhone.

"Just to cut to the chase, I'm not a believer in back doors or a single technical approach," Secretary Carter said to loud applause during a panel discussion at the conference. "I don't think it's realistic. I don't think that's technically accurate."

Apple is resisting a court order that would require it to create software to break the password mechanism in an iPhone used by one of the assailants in the December mass shooting in San Bernardino, Calif.

The F.B.I. argues that it is not asking for any sort of permanent back door and is merely asking for help in circumventing a single phone's password protection. People in the tech industry worry, however, that the request for help in the San Bernardino case is merely a prelude and point to a number of other pending cases in which law enforcement authorities would like Apple's assistance.

The software Apple is being asked to create could be considered a back door because it could provide special access to information that would otherwise be inaccessible thanks to passwords or encryption.

Secretary Carter's comments, though short on specifics, highlight the challenges various government agencies will face as they seek cooperation from Silicon Valley as the court fight between Apple and F.B.I. continues.

Also on Wednesday, Secretary Carter said Alphabet's executive chairman, Eric Schmidt, would head a new Defense Innovation Board to help connect tech companies and entrepreneurs with various Pentagon initiatives. And he announced a Hack the Pentagon initiative, which would reward hackers who find and turn over vulnerabilities in the Pentagon's computer systems.

"I don't think we ought to let one case drive a single solution," Secretary Carter said, referring to the F.B.I.-Apple dispute. "We have to innovate our way to a sensible result. And we need to do that because you can easily think of alternatives. One is a law written by people who don't have the technical expertise, one written in anger or grief, and that's not likely to work."

Many at the conference have compared the F.B.I's software request -- some are even calling it "GovtOS," short for government operating system -- to asking journalists to write a false article, or turn over a source, on national security grounds.

Dan Kaminsky, a well-known security researcher, likened the government's approach to persecuting firefighters during a firestorm. The point being, he wrote in an article on Wired.com, that at a time when data breaches happen regularly, the F.B.I. is trying to force Apple to weaken the security of its phones instead of advocating stronger security.

Secretary Carter echoed the need for stronger security but avoided taking a side in the F.B.I.-Apple dispute. "The problems of data security are many," he said. "There isn't going to be one answer. There are lots of different parts to this."

If Silicon Valley and Washington cannot find some alternative solution through innovation, Secretary Carter added, the most likely result would be a poorly written law, "or a solution written by China or Russia."

"And you know what their view of data access and security is," he said.

The Guardian (London)
US defense chief tells Silicon Valley: 'encryption is essential'
Thursday, 03 March 2016
Byline: Spencer Ackerman, Danny Yadron

San Francisco - The escalating encryption fight between Apple and the FBI has a prominent dissenter inside the government: US defense secretary Ashton Carter.
The powerful Pentagon chief has not publicly undercut the FBI's demands for Apple to write software undermining security features on its iPhone, which the bureau says is necessary to investigate the San Bernardino terrorist attack.

Yet Carter, according to people familiar with his thinking, has grown concerned that the increasingly bitter showdown between Apple and the bureau is jeopardizing his own efforts to forge closer ties with Silicon Valley - a major priority of his tenure at the Pentagon. As Comey fights encryption, Carter is bear-hugging it.

His current trip to the west coast, only the latest in a series of California jaunts, is devoted primarily to appealing for help with securing US defense networks - embracing the robust encryption that the FBI warns will lock law enforcement out of judicially-authorized criminal and national security investigations.

"I'm just speaking for the [Defense Department] - data security, including encryption, is absolutely essential to us," Carter said on stage at the RSA security conference in San Francisco on Wednesday.

Defense Department top brass, including some leaders at the National Security Agency, also have a different set of interests in the encryption debate compared to law enforcement. The military has more

of an interest in iron-clad data security as it traffics in highly classified secrets. Meanwhile, the NSA tends to have more hacker tricks up its sleeve to get around intelligence targets' security measures, including encryption, compared to the typical FBI agent or local police investigator.

Carter said, for instance, that he would be opposed to building a function into commercial encryption that would give the government access to data. "I'm not a believer in backdoors or a single technical approach. I don't think that's realistic," he said.

Congress may end up drafting legislation 'in anger and grief'

Carter declined to comment specifically on the Apple case other than to say one incident shouldn't determine the final outcome of the privacy fight. But he is understood to think the FBI is not unreasonable in its demand in the Apple case. The defense chief is concerned that the fight is leaving the tech industry confused about how the government views encryption, and the acrimony surrounding it is deepening the post-Edward Snowden rift between the government and Silicon Valley.

Still, the defense secretary in conversation with the venture capitalist Ted Schlein, who is himself close to Washington, urged technology companies to look for ways to compromise with the government. If they don't, the pair warned, both the industry and the government will have to deal with legislation written by Congress "who don't have the technical knowledge", Carter said. "It may be written in an atmosphere of anger and grief."

Pentagon wants to attract 'vetted hackers'

In 2015, Carter became the first defense secretary to travel to the Bay Area in 20 years, signaling his concern that the US military is losing the technological advantages it has had for a generation.

Carter wants to attract what the Pentagon called "vetted hackers" for Hack the Pentagon, a hackathon to test the tensile strength of US military cybersecurity, officials said on 3 March. The Pentagon will invite hackers to search for vulnerabilities on its public webpages that hackers might exploit - a task familiar to Silicon Valley but not the the Pentagon. It is expressly aimed at the very coders who might feel alienated by the Apple-FBI clash. The one requirement is that hackers be US citizens, Carter said.

"Bringing in the best talent, technology and processes from the private sector not only helps us deliver comprehensive, more secure solutions to the DoD, but it also helps us better protect our country," said Chris Lynch, the director of the Defense Digital Service, another Carter initiative to bolster the department's digital defense.

As Comey was defending to Congress his pursuit of unlocking an iPhone 5C used by a terrorist in December's San Bernardino attacks, Carter explicitly called Apple a "partner" during a speech at the Commonwealth Club on 1 March.

Carter waxed lyrical about the "garages and dorm rooms and home offices and research laboratories" of tech-sector giants and pledged to "preserve access to a free, open and secure internet" that technologists say the FBI will undermine by compelling Apple to write software that rolls back the company's user-security features.

Even as Carter delicately tiptoed around the Apple-FBI clash, he urged continued "partnership" with Silicon Valley and warned against China's "intent to require backdoors to all new technologies" - a point Apple has made to underscore the unintended consequences of the FBI's push.

Carter, more so than any other Washington official these days, appears to have had some success befriending Silicon Valley even as it wages a war of words with other parts of the Obama administration.

On Wednesday he announced a new defense innovation board that will try to use the valley's smarts to solve major defense problems, to be led by Alphabet executive Eric Schmidt.

Google, Facebook and Microsoft all expected to file supporting briefs

Despite Carter's plea for partnership, the battle lines between law enforcement and Silicon Valley are hardening.

Major tech companies including Microsoft, Google and Facebook are expected to file a legal brief supporting Apple by 3 March.

On 2 March Apple filed its formal objection to the federal judge's order to help the FBI unlock an iPhone used by one of the San Bernardino attackers.

The digital-rights groups AccessNow and the Wickr Foundation, as well as the American Civil Liberties Union, on 2 March filed briefs strongly backing Apple, warning that the "far-reaching consequences" of the FBI's position include "deliberately compromised digital security [that] would undermine human rights groups around the globe".

The ACLU argued that the FBI has exceeded the bounds of both the almost 230-year-old law enabling judges to enforce warrants and the Constitution by effectively "enlist[ing] private parties as its investigative agents to seek out information they do not possess or control".

Washington Post
Hacked U.S. companies have more options, departing cybersecurity official says
Thursday, 03 March 2016
Byline: Ellen Nakashima

Washington - The Obama administration's power to impose economic sanctions in response to malicious cyberspace acts gives companies that have been hacked by foreign governments a new way to deter adversaries and prevent them from reaping the rewards of their intrusions, a former senior U.S. official said.
The sanctions tool, which was authorized by an executive order last April 1, has not been used yet. But it is one of the cutting-edge initiatives that Luke Dembosky, until this week the top cybersecurity official in the Justice Department's national security division, was involved in during his 14 years at the department.

It is important that the sanctions tool "be used soon so that those who carry out significant cyberattacks on U.S. interests know that we mean business," said Dembosky, who will soon join the law firm of Debevoise & Plimpton.

At the Justice Department, Dembosky was involved in many of the most significant cybersecurity cases, including North Korea's hack of Sony Pictures; the intrusions into the Office of Personnel Management, widely attributed to China; the breaches of Target, Home Depot and Anthem; and the takedowns of the GameOver Zeus botnet and the illicit Silk Road online bazaar.

Dembosky has also taken part in other leading-edge efforts. In 2009, he won the conviction of Max Ray Vision, who was at the time the most notorious hacker in U.S. history. Iceman, as he called himself, had stolen and sold nearly 2 million credit card numbers and caused losses of $86 million. He got 13 years behind bars, what was then a record sentence in a cybercrime case.

Dembosky, 47, also was part of a small team of administration officials who last fall negotiated a historic cybersecurity accord with Beijing that led to President Xi Jinping's announcement in September that China would not engage in economic cyberespionage. Until that point, China had never acknowledged that cybertheft of intellectual property for a country's commercial advantage violated international norms.

"It was, in my mind, a breakthrough on behalf of businesses to protect their valuable intellectual property," Dembosky said.

But it remains to be seen whether China will uphold its pledge, he acknowledged.

Dembosky, who will help lead Debevoise's global cybersecurity practice, noted that most companies traditionally have been wary of cooperating with government investigations into breaches. They fear that disclosing sensitive company materials will expose them to regulatory actions, privacy suits or other civil litigation.

But recent moves by the administration have the potential to change the calculus, he said. Faced with the rapid rise of national-security cyberthreats, he said, the government has expanded its arsenal of

weapons to use against cyber adversaries. Besides criminal prosecutions, there are export license restrictions, trade and diplomatic actions, and now sanctions.

"More tools give a savvy victim company a broader range of choices in working with the government," he said.

That is, if a company decides to let federal investigators examine the forensic evidence left by the intruders, the government may be able to build a case against individuals who conducted or directed the hack or who, such as officials in a rival overseas company, stood to benefit from it.

In cases where the perpetrators are overseas and are unlikely to be extradited if indicted, it may be that through sanctions their assets can be frozen and banks can be barred from doing business with them. The same penalties can apply to a sanctioned company.

But having the United States impose sanctions on, say, a Chinese or Russian company may not always be the best move for the victim company, Dembosky noted. Some may make the calculation that such a move may result in retaliation against them and that the risk is not worth it.

The point is, he said, there are more powers the government is able and willing to use to hold adversaries accountable and thus more reasons for companies to work with the government in cybersecurity investigations.

But firms also fear regulators' whips. Last year, the Federal Trade Commission settled a high-profile lawsuit with Wyndham Hotels and Resorts over a series of data breaches that exposed the credit card information of hundreds of thousands of customers. The settlement required Wyndham to set up a program to protect cardholder data as well as conduct annual information security audits, among other steps.

The Securities and Exchange Commission has begun to fine and hold accountable investment adviser firms for data breaches, and the New York State Department of Financial Services has alerted federal agencies that it is considering imposing cyberspace regulations on financial institutions in the state.

"So for companies, there is risk and opportunity in cooperating with government," Dembosky said.

Judith Germano, a former federal prosecutor who is now a senior fellow at New York University Law School's Center on Law and Security and a cybersecurity consultant, noted that the FTC has said it will take into account a firm's cooperation with law enforcement in a breach investigation in evaluating whether the firm has done all it can to reduce the harm from the breach.

She also said that the sanctions tool may be useful but that it is too soon to tell, given it has not been deployed yet.

Dembosky began his cybersecurity career 14 years ago prosecuting Eastern European criminals stealing credit card data to sell on online black markets. In 2010, he moved to Moscow as the Justice Department's attache, helping establish a cybersecurity "hotline" and other measures with Russia aimed at defusing tensions in cyberspace. In 2013, he came to Washington to oversee litigation in the department's computer crime and intellectual-property section. And in 2014, he moved to the national security division.

His national security experience is in demand now, said Bruce Yannett, Debevoise deputy presiding partner. "It is clear that the greatest cyberthreats that companies face are state actors and quasi-state actors" who have the resources and skill to cause the most harm, he said. "If you're shut down, the way Sony Pictures was, or if your deepest, darkest trade secrets are stolen, that can pose an existential threat to any company."

Le Figaro
Europe et États-Unis s'accordent sur les données
Thursday, 03 March 2016
Byline: Lucie Ronfaut

Bruxelles - Le « Privacy Shield » doit apporter stabilité et sécurité aux entreprises et internautes. Internet L'accord Privacy Shield, ou « bouclier de confidentialité » , se dévoile mais doit encore convaincre. Après plusieurs mois de négociations, les autorités américaines et l'Union européenne ont publié les principales mesures du nouvel accord régissant les échanges de données entre les deux puissances.

Il est très attendu à la fois par les entreprises américaines (comme Facebook ou Google) et les sociétés européennes hébergeant une partie ou la totalité des données de leurs utilisateurs aux États-Unis.

Signé au mois de février, le Privacy Shield a désormais la lourde tâche de faire oublier son prédécesseur, le Safe Harbor. Cet accord vieux d'une quinzaine d'années a été invalidé fin 2015 par la Cour européenne de justice. D'après cette dernière, il ne garantissait pas suffisamment la sécurité des données personnelles des Européens, notamment au regard des révélations d'Edward Snowden sur la surveillance exercée par la NSA sur les géants du Web américains.

Des mesures cosmétiques

Le Privacy Shield répond à ces inquiétudes par plusieurs mesures. Il crée un nouveau poste de médiateur aux États-Unis chargé de recueillir les plaintes des citoyens européens inquiets de l'exploitation de leurs données par les services de renseignements américains. Les entreprises faisant l'objet d'une plainte de la part des citoyens européens auront 45 jours maximum pour répondre. La Commission européenne assure également que « tout accès à des données par les autorités publiques pour des raisons de sécurité nationales fera l'objet de limitations claires et de mécanismes de contrôle, afin d'empêcher la

surveillance généralisée » . Le nouvel accord prévoit la publication d'un rapport annuel pour contrôler la bonne application de ces mesures. Il doit désormais être examiné par le groupe des autorités européennes de protection des données (le G29) avant d'être définitivement voté.

Le Privacy Shield, tout juste présenté, compte déjà de nombreux opposants, qui estiment que rien ou presque n'a changé depuis le Safe Harbor . Max Schrems, l'étudiant autrichien à l'origine de la procédure judiciaire qui a mis fin à l'accord, a dénoncé « un cochon à qui on aurait mis dix couches de rouge à lèvres. Ce n'est pas pour autant qu'on a envie de lui faire un câlin ! » . Il pointe notamment un document envoyé au département du Commerce américain, en charge des négociations, par Robert Litt, directeur juridique du renseignement national.

Cette lettre, récupérée par l'agence Reuters, prévoit six « cas spécifiques » où la surveillance généralisée des données restera autorisée. Ce qui va à l'encontre de la décision de la Cour européenne de justice, qui dénonçait justement le manque de contrôle du renseignement américain. « Malheureusement, cette décision de la Commission devrait vite retourner devant la justice, prédit Max Schrems. Il est regrettable qu'elle n'ait pas profité de cette situation pour fournir une solution stable à la fois pour les internautes et les entreprises . »

London Daily Telegraph
Two thirds of cyber-attack businesses keep silent
Thursday, 03 March 2016
Byline: Kate Palmer

London - Two thirds of cyber-attacked companies have kept silent about the breach rather than report it to the police, a poll of British businesses suggests, ahead of plans to force all companies to notify the authorities. One-in-10 British businesses suffered financial loss from cybercrime in the past year, according to a poll of 1,000 Institute of Directors members. Yet of these companies, just 28pc said they reported the attack to the police, citing fear of reputational damage.
Companies that have publicly fallen victim to a security breach have seen their share price suffer and lost customers as a result.

TalkTalk is still recovering from last year's hack, when stock fell by almost 20pc in the weeks following the breach. The full scale of the attack, which cost TalkTalk £60m in lost revenues and costs, was revealed last month in the company's full-year trading update that also showed 101,000 customers had left in the aftermath of the hack.

Currently only telecoms companies are legally required to report cyber breaches, which they must do within 24 hours or a face a £1,000 fine.

However, European Parliament is currently planning minimum cyber security standards that mean companies in key sectors - such as banks, energy and water companies - would be forced to report such incidents too.

London Daily Telegraph
Isil making £14m a month playing currency markets with looted bank cash
Thursday, 03 March 2016
Byline: Colin Freeman

London - ISIL is making millions of dollars for its war chest by playing foreign currency markets under the noses of bank chiefs, it was revealed yesterday.
The terrorist group is earning up to $20 million (£14 million) a month by funnelling dollars looted from banks during its takeover of the Iraqi city of Mosul into legitimate currency markets in the Middle East.

It then makes huge returns on currency speculation, which are wired back via unsuspecting financial authorities in Iraq and Jordan, a parliamentary committee was told.

Islamic State of Iraq and the Levant's (Isil) white collar crime is now a major source of income, along with oil smuggling and extortion from people living in Isil-controlled areas.

Details of the scam emerged during a hearing of a specially convened foreign affairs subcommittee set up to examine Britain's role in Isil financing.

The hearing was told that Isil finance chiefs would play the international stock markets using cash looted during their 2014 takeover of Mosul, in which the group got its hands on an estimated $429 million from the city's central bank.

They also used money "siphoned off " from pension payments that are still being made by the Iraqi government to civil servants living in the city. The details were revealed to the hearing by John Baron, the subcommittee's chair, who demanded to know whether the British government - which has pledged to help cut off Isil's finance networks - was taking proper action against it.

"The cash that Isil has looted, along with siphoned off pension payments, is routed into Jordanian banks and brought back into the system via Baghdad," he said. "That allows the system to be exploited by Isil, in that they take a turn [profit] on the foreign currency actions and siphon that cash back."

The profits were channelled back into Isil coffers by "hawala" transfers, an unregulated system of money transfer whereby cash payments are made via agents in one country after a similar amount is presented as collateral in another.

Tobias Ellwood, a junior Foreign Of-fice minister, admitted to the committee that there was a "porousness" in the financial system but said that work was now under way to shut it down. It had been done without the active connivance of bank staff, he added.

In December, the central bank of Iraq named 142 currency-exchange houses in Iraq that the US suspected of moving funds for Isil. It banned them from its twice-monthly dollar auctions.

But Mr Ellwood conceded: "Iraq could have moved faster on this".

Breakthrough seizure US captures Isil commander in Iraq

An American Special Operations force has captured an Isil commander in northern Iraq in what the Pentagon said may be a crucial development.

The unnamed operative was being questioned at a detention facility in Erbil, the capital of Iraq's Kurdistan region. US officials said the interrogation could take weeks or months, and that the man would then be turned over to Kurdish authorities.

A 200-strong unit, the expeditionary targeting force has been arriving in the area in recent weeks, ready to expand operations as part of the first major American combat presence in the country since US forces withdrew in 2011. The team is working with Iraqi and Kurdish forces to establish informant networks and to conduct further raids on Isil safehouses and compounds.

The possibility of future raids now raises questions about what will happen to the detainee and others like him, given that President Barack Obama has ruled out sending any more suspects to Guantánamo Bay and that the US does not want to create a holding centre for Isil captives in Iraq.

York Times
Silicon Valley Rallies to Apple's Defense, but Not Without Some Hand-Wringing
Thursday, 03 March 2016
Byline: Nick Wingfield, Mike Isaac

New York - It is a remarkable moment for the technology industry, with many different companies and organizations rallying around a single company -- Apple -- in a major legal case against the United States government over privacy and security.
Yet behind the scenes, it took time for some of the tech companies to make the decision to support Apple. Several feared the showdown with the government was too risky and could have far-reaching implications for the tech industry if Apple lost.

Those misgivings ultimately did not win the day. About 40 companies and organizations are expected to file court briefs on Thursday backing Apple as it fights a judge's order to help law enforcement break into an iPhone used by a gunman in the San Bernardino, Calif., terrorist attack last year.

Dropbox, Facebook, Google, Microsoft, Snapchat and Yahoo are among the tech companies expected to sign on to briefs in the case, according to people with knowledge of the plans who spoke on the condition of anonymity. More than 40 individuals, including prominent security experts and academics, are also planning to sign briefs, which will focus on themes like free speech, the importance of encryption and concerns about government overreach.

The show of support -- including briefs filed on Wednesday by groups like the American Civil Liberties Union and Access Now -- is unusual in its breadth, showing that many in Silicon Valley believe that it could have profound implications on the trustworthiness of their products.

"Given the years of companies' reluctance to be at the barricades around intelligence discussions, this is significant," said Jules Polonetsky, chief executive of the Future of Privacy Forum, an industry-financed think tank in Washington.

Still, several executives at tech companies supporting Apple said they were worried that Apple had picked a fight that could end up backfiring on the rest of the industry. In the days since a magistrate judge in California ordered Apple to bypass security measures on the iPhone, lawyers in some of the companies debated these issues with one another and peers at other firms.

All of the executives asked to remain anonymous because their deliberations were private, but their views are shared among others in Silicon Valley.

Keith Rabois, a venture capitalist with the firm Khosla Ventures, said he was a strong believer in privacy and encryption -- "all the normal Silicon Valley views," he said -- but worried that Apple could lose the case, setting a legal precedent that could force other companies to compromise the security of their products for law enforcement.

"In my view, this is the wrong case to fight," Mr. Rabois said. "There are plenty of other cases with a lot less sympathetic case for the government."

For Mr. Rabois and others, the circumstances working against Apple include the iPhone's connection to a terrorist attack that left 14 people dead, rather than to a less highly charged crime. Furthermore, the iPhone was owned by the employer of the gunman, Syed Rizwan Farook, which consented to a search of the device.

Apple's defenders said the company did not pick this fight -- the government did. Critics of Apple's approach believe that the company could have quietly complied with the government's request to help

break into the iPhone and then taken a public stand in a more favorable case. But Apple has said that once a tool exists for extracting data from the phone, that tool cannot be made to disappear.

Yet whatever doubts Apple's allies voiced privately, they were in the end insufficient to keep a large number of big companies from signing on to the cause.

Dropbox's general counsel, Ramsey Homsany, said in a statement, "We stand against the use of broad authorities to undermine the security of a company's products."

Bruce Sewell, Apple's general counsel, said in a statement, "We are humbled by the outpouring of support we've received from our customers, our colleagues in business, nonprofit organizations, the security community and many others." He added, "The groups filing briefs with the court understand, as more and more people have come to realize, that this case is not about one phone -- it is about the future and how we protect our safety and our privacy."

On Tuesday, Apple filed its formal objection to the government order to open up the iPhone, citing the reasons set forth in a previously filed motion.

For many tech companies that were initially concerned by Apple's opposition to opening up the iPhone in the San Bernardino case, the worries centered not only on whether this was the right case for challenging the government but also on how public perceptions of the fight might reflect on the rest of the industry, according to tech executives involved in the discussions, who spoke on the condition of anonymity.

A report by Pew Research Center last week said 51 percent of Americans believed that Apple should unlock the iPhone to assist the Federal Bureau of Investigation in the case, while only 38 percent found Apple in the right.

Some of the companies were also concerned that the relationships they had forged with the government might degrade because of Apple's battle, according to the people involved in the tech industry discussions. In the years since the disclosures by Edward J. Snowden, the former intelligence contractor who released a trove of details on United States government surveillance tactics, some tech companies have been trying to educate members of Congress about online privacy practices.

Others were also anxious that Apple's defiance of the government could lead to congressional efforts to reshape, in ways unfavorable to the tech industry, the Electronic Communications Privacy Act, which privacy advocates and tech companies have long claimed needs an overhaul.

And these companies are watching what effect the fight could have on a proposal to establish a national commission that would explore ways to obtain encrypted data from consumers while working to safeguard users' privacy. The proposed commission, the bill for which was introduced on Monday,

would be led by the House Homeland Security Committee chairman Michael McCaul, Republican of Texas, and Senator Mark Warner, Democrat of Virginia.

On Monday, Apple got good news that could help soothe lingering tech industry doubts about its defense in the San Bernardino case. A federal magistrate judge in a separate drug case in New York ruled against a government request to extract data from an iPhone, a decision that could influence the San Bernardino case.

Silicon Valley's arc in supporting Apple -- an initial flurry of concerns followed by an eventual coming around to the idea -- is epitomized by Max Levchin, the co-founder of PayPal and chief executive of Affirm, an online financial services firm. Last week in an interview on CBS, Mr. Levchin said his views on the case over the previous several days had shifted from a "clear-cut, black-and-white" stance of helping the F.B.I. He has since sided with Apple.

Asharq Al-Awsat
U.S. Military Invites Experts to "Hack the Pentagon"
Thursday, 03 March 2016
Byline: Staff Report

San Francisco - As a very novel program to ever be offered by the federal government, the Pentagon declared on Wednesday that it planned to invite vetted outside hackers to detect and examine the cybersecurity of some public U.S. Defense Department websites as part of a pilot project next month. Seeking to discover gaps in the security of their networks, competitions known as "bug bounties" are conducted by big U.S companies, including United Continental Holdings Inc. and by the same token "Hack the Pentagon" is modeled after the aforementioned competitions to inspect its cybersecurity. It's worth noting that similar programs permit cyber experts to find and identify problems before malicious hackers can exploit them. This saves both money and time in the event of damaging network breaches.

Defense Secretary Ash Carter said in a statement unveiling the pilot program "I am confident that this innovative initiative will strengthen our digital defenses and ultimately enhance our national security".

Thousands of qualified participants were expected to join the initiative, as said by one senior defense official. Further on this subject the Pentagon stated that more details and rules are still being worked out but the competition could involve monetary awards. It's worth noting that the Pentagon has long tested its own networks using internal so-called "red teams," but this initiative would open at least some of the department's vast network of computer systems to cyber challenges from across industry and academia.

Before being turned loose on a predetermined public-facing computer system all participants aught to be U.S. citizens and will have to register and submit to a background check, stated the Pentagon. It said other more sensitive networks or key weapons programs would not be included, at least initially. "The

goal is not to comprise any aspect of our critical systems, but to still challenge our cybersecurity in a new and innovative way," said the official.

The Pentagon's Defense Digital Service (DDS) is leading the initiative which was set up last November to bring experts from the U.S. technology industry into the military for short stints.

Chris Lynch, a former Microsoft executive and technology entrepreneur who heads DDS stated that bringing in the greatest talent along with technology and processes from the private sector will aid in delivering comprehensive, and more secure solutions to the DOD.

Carter introduced Lynch during a speech to the Commonwealth Club on Tuesday and said he had already recruited coders from companies like Google and Shopify for a Pentagon "tour of duty."

Christian Science Monitor
State Department reverses course on cybersecurity exports
Wednesday, 02 March 2016
Byline: Joe Uchill

Washington - After nearly 10 months of intense pressure from cybersecurity experts, the Obama administration will send the State Department to renegotiate a controversial arms control agreement meant to limit surveillance software exports.
The decision represents a turnabout for the State Department, which had resisted reopening talks with the 41 nations that are signatories of the Wassenaar Arrangement. But after widespread criticism that the trade pact would hamper the trade of legitimate security software, the US is aiming to return to the negotiating table.

"There is simply no way to interpret the plain language of the text in a way that does not sweep up a multitude of important security products," said Rep. Jim Langevin (D) of Rhode Island in a statement. "The Administration is staking out a clear position that the underlying text must be changed."

Representative Langevin says National Security Advisor Rice also became a strong factor in swaying Foggy Bottom to renegotiate the deal. Obama administration officials unanimously called for a new agreement at a meeting last week.

The controversy around Wassenaar began heating up last May when the Department of Commerce released proposed export regulations based on the pact's terms. Experts feared the broad language in the proposed rules would even ban some cybersecurity researchers in the US from jointly conducting security work abroad.

In addition to cybersecurity experts, US lawmakers and Department of Homeland Security officials also worried that Wassenaar's language could limit threat information-sharing initiatives and damage domestic security.

At a congressional hearing in January, the State Department publicly opposed renegotiating Wassenaar - citing the difficulty of signing another deal with the 31 countries that had already adopted the terms. Instead, the agency had hoped to satisfy critics by creating exemptions in the trade restrictions.

But those claims were met with Congressional skepticism. Soon after the hearing, however, State Department officials reached out to industry experts to work on a new proposal.

"The [House Oversight] hearing hammered home the national security implications of the Wassenaar language," said Katie Moussouris, the chief policy officer of the bug bounty firm HackerOne.

A vocal critic of the regulations, Ms. Moussouris was one of the industry experts called in to work on the new proposal. She says the new draft language shifts the focus of the Wassenaar guidelines with a narrower focus on surveillance software itself.

Moussouris cautions that the State Department's evolving position on cybersecurity exports does not mean the issue is closed. Other nations will still have to agree to change.

"We'll consider the issue settled when we see it settled," she said.

The Hill
Cyber experts invited to 'Hack the Pentagon'
Wednesday, 02 March 2016
Byline: Kristina Wong, Cory Bennett

Washington - The Defense Department is inviting "vetted hackers" to test its cybersecurity in a new pilot program called "Hack the Pentagon."
"This innovative project is a demonstration of [Secretary of Defense Ashton] Carter's continued commitment to drive the Pentagon to identify new ways to improve the department's security measures as our interests in cyberspace evolve," the Pentagon said in a statement Wednesday announcing the initiative.

It's the first "cyber bug bounty program in the history of the federal government" and is modeled after similar competitions held by the nation's biggest companies, the Pentagon said.

Hackers are required to register and submit to a background check to participate in the program. Hackers must be U.S. citizens, according to Reuters.

Qualified participants will then try to identify vulnerabilities in Pentagon applications, websites and networks. They could be eligible for monetary awards and other recognition. The program launches in April.

"I am always challenging our people to think outside the five-sided box that is the Pentagon," said Carter in a statement.

"Inviting responsible hackers to test our cybersecurity certainly meets that test. I am confident this innovative initiative will strengthen our digital defenses and ultimately enhance our national security."

"Critical, mission-facing systems" will not be part of the program, the Pentagon said.

The initiative is being led by the Defense Digital Service (DDS), a small team of engineers and data experts launched by Carter in November, as part of the White House's U.S. Digital Service.

"Bringing in the best talent, technology and processes from the private sector not only helps us deliver comprehensive, more secure solutions to the DOD, but it also helps us better protect our country," said DDS Director and technology entrepreneur Chris Lynch.

The Pentagon announced the program as Carter and other top officials are on a swing through Silicon Valley to meet with tech executives.

Carter said the trip is part of the military's efforts to "rebuild bridges between the Department of Defense and some of our nation's most innovative industries."

The two sides have been at odds since former National Security Agency contractor Edward Snowden in 2013 revealed through a series of leaks the extent of the government's secret surveillance efforts.

But the Defense Department has its sights set on Silicon Valley as a major talent pool for developing its cyber team. The Pentagon is in the midst of building out the half-staffed U.S. Cyber Command. The cyber division is expected to reach 6,200 personnel across 133 teams by 2018.

London Daily Telegraph

Tech companies must unite, says GCHQ chief in privacy row

Wednesday, 09 March 2016

Byline: Martin Evans

Section: general

London - An offer by the head of GCHQ to build bridges with technology companies over the ongoing encryption row has been cautiously welcomed by the industry.
Robert Hannigan, who is in charge of the intelligence agency, said it was time for the security services and large tech companies, such as Google and Apple, to put differences aside and find ways of collaborating in order to stop criminals and terrorists from using the internet to further their aims.

Both the British and American authorities have been at loggerheads with some of the major companies over the need to access information which is protected by complex encryption.

But Mr Hannigan, who had previously accused tech companies of being the "command and control networks of choice" for terrorists, struck a more conciliatory tone earlier this week and called for all sides to tackle the problem together and in a "less highly charged atmosphere".

In a speech at the Massachusetts Institute of Technology on Monday, Mr Hannigan said a "new forum" was needed to hold a "frank dialogue". He also suggested that the conflict between the two sides risked deflecting focus from combating terrorism.

"Of course some people will find new places to hide unlawful activities, and new channels of communication, but our agencies were created to tackle those hiding places," he said. "We should apply our collective goodwill and technical brilliance to meeting the hardest threats to society."

His comments have been welcomed by representatives from the tech industry who believe solutions can only be found through greater collaboration.

Antony Walker, deputy chief executive of techUK, the trade body which represents the industry, said: "We welcome Robert Hannigan's commitment to constructive dialogue with the tech industry. The solutions lie in government, academia and industry working together."

The controversy over encryption and privacy has come to a head in a bitter legal case between Apple and the FBI over attempts to access data on the iPhone of Syed Rizwan Farook, the extremist who, along with his wife, shot 14 people dead in San Bernardino, California, in December.

The FBI won a court order requiring Apple to help it get around encryption and passwords on the device but the company is challenging it.

Apple chief executive Tim Cook has described the case as "dangerous, chilling and unprecedented".

CBC.CA

Ralph Goodale says Ukraine cyberattack caused 'international anxiety'

Wednesday, 09 March 2016

Byline: Susan Lunn

Section: general

Ottawa - Prime Minister Justin Trudeau has asked his public safety minister to review all government operations to see if Canada is well protected against a possible cyberattack.
This review comes on the heels of the cyberattack on Ukraine's power grid last December that caused a blackout for hundreds of thousands of people.

Conservative MP Cheryl Gallant raised the incident in Ukraine with Ralph Goodale at a parliamentary committee today.

"The concern is that this type of sophisticated, planned, synchronized attack could occur in North America," Gallant told the committee.

"What measures are in place to make sure that just such a coordinated attack or perhaps a more sophisticated one does not impede our electricity system and all the items attached to the grid that we depend on?" she added.

Goodale says what happened in Ukraine came up at a recent meeting in Washington with Canada's closest security partners. The "Five Eyes" group includes the United States, United Kingdom, Australia and New Zealand.

"It's a matter of international anxiety," Goodale said.

To that end, Goodale said he has been asked by the prime minister to do a government-wide review of the state of cyber security operations "to make sure that we are on top of this kind of operation and the problem that hit Ukraine will be properly defended against in Canada."

"We think that is the case today, but the review will ask that critical question: Are we sure? And we want to be sure," he added.

Canada not immune

An attack on the computers at the National Research Council in July 2014 was eventually blamed on the Chinese.

That same year, the Canada Revenue Agency had to shut down its website for a few days after the Heartbleed Internet bug breached the computer system. About 900 social security numbers were stolen.

The deputy minister at public safety, François Guimont, told the committee he believes the critical response team set up to deal with cyberattacks does a good job.

"They keep literally a laboratory of viruses that they study, understand, and they're very quick at disseminating this information to other constituents in Canada for them to take action to protect themselves," Guimont said.

"So progress has been made, but I will tell members of the committee, the cyber file, unlike other files if you wish, is always evolving."

The public safety department isn't alone is dealing with cybercrime.

The RCMP has received an extra $110 million in recent supplementary spending estimates. Part of that money is earmarked for cyberterrorism.

Guimont says the government-wide review of the cyberstrategy is timely.

"The strategy is not that old. But the file is moving so quickly it's time to step back, see where we are and carry out actions where we think we may have weaknesses," Guimont told the committee.

As he was wrapping up his testimony, Goodale asked the committee members if they had changed their passwords today, reminding them to do that frequently.

CBC.CA

Armed drones: Should the Canadian military use the controversial weapons?

Wednesday, 09 March 2016

Byline: Laura Wright

Section: general

Ottawa - Canada's chief of defence staff announced this week that the Canadian military needs new drones and he wants those drones to be armed -- an upgrade that doesn't come without its share of controversy.
Gen. Jonathan Vance's comments came on the heels of a U.S. air strike in Somalia over the weekend that killed 150 militants linked to al-Shabaab. The strike was partly carried out by unmanned drones.

But military use of armed drones is fraught with controversies, from the perceived ease at which drone operators pull the trigger, to the number of civilian deaths associated with drone strikes.

The benefits of using drones, however, are difficult to ignore -- namely the fact drone operators don't run the risk of dying in a strike, as fighter-pilots do.

"It's high time that Canada bought that kind of a drone," says Elinor Sloan, an international relations professor at Carleton University. "Arming them simply provides options in a war zone."

As Canada gets set for a possible debate on the topic, here's a look at some of the pros and cons of using armed drones.

The use of armed drones is just the next step in the increasing "stand-off character" of warfare, Sloan argues. Humans used to fight hand-to-hand and developed tools to get further and further away from close-up combat.

"Drones just put that effort still further away from direct human contact," she says. "But a human is still in charge and directly tethered to that platform."

Drones are safer for those operating them since pilots can be thousands of kilometres away from their targets, with no risk of physical injury.

And they're relatively cheap, says Stephanie Carvin, an assistant professor of international affairs, also at Carleton University. "There are multiple different uses for them -- not just killing machines."

Drones can be better for warfare because of their precision; their surveillance capabilities allow them to follow a target for hours or days before deciding whether to strike.

This allows for what Jesse Kirkpatrick calls "tactical patience."

"It allows individuals to be operating in a cool remove that will allow them to maybe not engage in atrocities that some do after the stress of battle takes its toll on them," says Kirkpatrick, the assistant director of the Institute for Philosophy and Public Policy at Virginia's George Mason University.

Sloan and Carvin both say drone pilots often don't act alone -- up to 25 people can be involved in a mission, including the U.S. president.

Despite drones' ability to be more effective, Kirkpatrick says that "cool remove" can be unsettling.

"You have someone who seems to be hunting individuals from 3,000 miles away and can patiently wait for them," he says. "I think that image bothers people."

Civilian casualties

Despite the benefits, some say there is a high civilian death toll associated with drone strikes. The problem is those numbers are incredibly difficult to verify.

"We just don't have good data," says Carvin. "Those reports are based on the U.S. program, and are based on reports from far-off areas that we don't have access to."

She adds that some of the reports only looked at a small number of drone strikes, which can skew the data. "They're deeply methodologically flawed."

Drone pilots are sometimes disparagingly called "chair pilots," as there is a perception that their distance from the scene of a strike allows them to more easily pull the trigger.

But Kirkpatrick says he found drone pilots suffer psychological trauma at a comparable rate to fighter pilots.

"That can lead us to speculatively conclude that it's not like playing a video game -- the killing and the harm feels very real," he says.

Secrecy, myths

The public perception of the U.S. drone program in particular has not been helped by the fact it is shrouded in secrecy.

"One of the main issues is its lack of transparency, and there are significant issues for democratic oversight, participation and civilian control of the military," says Kirkpatrick. He adds this secrecy makes it very difficult to determine how many civilians are being harmed.

The U.S. government claims no civilians have been killed, but that's debatable based on who they define as a combatant.

"Observers say the only reason you can claim this is that the definition of what it means to be a combatant is way too broad," says Sarah Kreps, an associate professor of governance and law at Cornell University who has written two books about drones.

Whether the Canadian military eventually moves to using armed drones may be a debate that's missing the point; Carvin says it doesn't make a difference if the military kills people with F-18 fighter jets or with armed drones.

"[Drones] are a shiny object and we all get distracted because it's a new technology and that's understandable," she says. "But what we need to be asking is: 'What is the actual policy that we're using this for?'"

Canada should consider buying drones, she says, if they can potentially contribute to the country's future military missions -- not just because everyone else has them.

Toronto Star

In terror fight, 'drones are not a silver bullet'

Wednesday, 09 March 2016

Byline: Olivia Ward

Section: Analysis

Analysis: Defence chief Gen. Jonathan Vance this week came out in favour of modernizing Canada's armed forces with drones, including ones capable of striking at enemies abroad. The unmanned vehicles have been used increasingly by the U.S. as a way of limiting military and civilian casualties.
But critics say that such a move needs a down-to-earth assessment.

"First you need an ethically defined foreign policy. Then you have to know what kind of interventions you expect that you can realistically make," says Prof. Derek Gregory of the University of British Columbia, an expert in aerial warfare. "If you're going to join the big boys, you have to know why."

There are also doubts about the value of drones against terrorism. "All the evidence we've gathered is that they killed large numbers, and the remaining population is terrorized and traumatized," says Kat Craig, legal director for the counterterrorism team at the London-based charity Reprieve.

"Drones are not a silver bullet."

Some factors for Ottawa to consider:

Loss of control

It's unlikely Canada will decide on its own drone targets as Ottawa has always worked closely with NATO and the U.S. in "coalitions of the willing." But taking the initiative from the U.S. in a program of deadly force could have unintended consequences.

For one thing, U.S. President Barack Obama, who has expanded the drone program, will be out of office soon. A new president, warn Jameel Jaffer and Brett Max Kaufman, of the ACLU, in the New York Times, "will inherit a sweeping power to use lethal force against suspected terrorists and militants, including Americans." And, possibly, Canadians. It could also lead to wider "collateral damage" to civilians.

Targeting

If Canada adopts U.S.-designated targets it will be in murky territory. The CIA maintains a covert program that only came to light through leaks and freedom-of-information requests. But strikes are also carried out by the military under the similarly secretive Joint Special Operations Command. Nor is it clear who is being targeted - only terrorist kingpins, or fellow travellers? In Somalia this week, rank-and-file fighters from the terror group Al Shabab were also killed in larger numbers than ever before. If Canada goes it alone, it would have to sort out the same issues of who should be targeted and by what lines of command.

Intelligence

Drone targeting relies heavily on intelligence from the ground. In countries such as Iraq, Libya, Somalia, Yemen, Afghanistan and Pakistan, that means developing trusted sources of information whose reliability is difficult to test. Spotters may be subject to local pressures or executed if they are discovered. They may also be acting on information based on local resentments. Although satellite surveillance of suspects can be highly accurate, without deep knowledge of the region, it may be impossible for command and control personnel to be sure they are aiming only at "high- value" targets.

Civilian casualties

The debate between the ethics and effectiveness of aerial bombing from warplanes, versus drone strikes has taken off since the beginning of the drone program in the early 2000s. Obama chose drones as a way of limiting civilian casualties and sparing U.S. military personnel. But monitors of drone deaths have noted hundreds of dead civilians, although counts are notoriously difficult as the U.S. has classified drone casualties as militants. The numbers may or may not be clearer soon when the U.S. tables promised figures for those killed in strikes, including civilians.

Blowback

"Civilians have died, but in my firm opinion the death toll from terrorist attacks would have been much higher if we had not taken action," said former CIA director Michael Hayden in the New York Times. But for people living under the threat of drones, witnesses say there's more grief than gratitude. People arrested for foiled terrorist attacks have cited drone warfare as a motive. "In my overwhelming experience in countries where there is a secret drone war, there's little benefit and a huge amount of destruction, despair and death," says Craig of Reprieve.

Recruiting and training

Canada would need to hire "pilots," who are likely to be young recruits familiar with the technical side of targeting and carrying out strikes, but unprepared for the stresses of a job that involves the life and death of strangers. In spite of their safe distance from the battlefield, pilots are under psychological pressure from isolation, secrecy, guilt and the boredom of long hours of surveillance. They will need psychological support and monitoring to prevent leaks of classified information.

Liability and rule of law

In the U.S., Obama has used constitutional responsibility to protect Americans from terrorism and the national right to self-defence as legal justifications. That still leaves vexed legal questions - such as the option to capture and try suspects instead of killing them without recourse to due process. It could also leave Ottawa open to prosecution, such as a case against CIA officials for wrongful civilian deaths in Pakistan in 2009. And it would make Canadian leaders responsible for individual life-and-death decisions.

Cost

Drone warfare is far from cheap, including repairs and maintenance. Experts say they're more expensive than manned F-16 fighter jets to maintain, and take up to 170 personnel to keep one combat mission in the sky at a time. "You can't just buy one," says UBC's Gregory. "Combat air patrol is four drones because they have a short range. They're also susceptible to weather, even clouds. Confusing a military drone with a hobby drone is a mistake. This is big kit."

Times of Israel

US giant Lockheed-Martin releases Israeli-based cyber-security system

Wednesday, 09 March 2016

Byline: David Shamah

Section: general

Jerusalem - After more than a year of working with Israeli cyber- security start-up Cybereason, US aerospace and data protection firm Lockheed Martin officially released a cyber-security solution based on the Israeli firm's technology.
"We often look to our partners to help shape and create best practices and products," said Angie Heise, vice president, Lockheed Martin Commercial Cyber. "We have been working with Cybereason to do just that. Cybereason's market-leading endpoint threat detection and response capabilities complement our cyber security offerings, providing customers a solution that is driven by our unique threat feed intelligence and enhanced by our powerful 'analyst on demand' program."

Although known mostly for its defense and weapons work, Lockheed-Martin has a large information technology division - and in fact, the company is the number one IT solutions provider to the U.S. federal government. According to the company, its does nearly $9 billion in cyber-security business annually with clients in the private sector, government, and defense arena.

In 2013, Lockheed Martin, EMC Israel, and Ben Gurion University signed a deal in which the three organizations committed to work together to ferret out promising Israeli cyber-security start-ups, and help them develop their technology into commercial products. One company they came up with was Cybereason, which takes a different approach to cyber-security.

"Most people think of cyber-security as an IT issue, and that if a computer 'appears' clean and acts normally, it is," said Lior Div, CEO of Cybereason. "That isn't usually the case, though, as hackers can act in a very stealthy manner without the victim of an attack even realizing what is going on."

Cybereason uses what Div calls silent sensors to discover attacks. "We use a big data approach, checking every piece of data going into or out of a machine," said Div. "We collect and analyze the information and present customers with a full snapshot of what is going on at any particular time, and alert them not just to specific anomalies that they need to follow up on, but whether they are actually under the attack."

Two principles guide Cybereason, said Div; one is that "the system has to be simple enough for all customers, enabling them to understand what is happening and what needs to be done even if they are not experts in security. The second is that "hackers are probably already in your system; there is no way to keep them out, so we don't even try. The key is to eliminate the attack as soon as it is discovered, and that is what we concentrate on, very successfully."

The sensor system was one thing Lockheed-Martin liked about Cybereason, and after collaborating together for more than a year, the companies developed and released at last week's RSA security conference in San Francisco the Lockheed Martin Threat intelligence with Cybereason's Endpoint Detection and Response (EDR) Platform.

The system place software sensors on all end points within an enterprise, continuously collecting and transparently communicating to the Cybereason Malop Hunting Engine, a big data, behavioral analytics platform designed to reveal malicious operations, otherwise known as Malops.

Customers see the Malops on the system's Incident and Response Console, so customers know exactly what is happening, and where on the network it is taking place. Lockheed Martin takes this capability to its next logical step, enhancing the Malops Hunting Engine's data analytics capability with threat feed intelligence from the Lockheed Martin-Computer Incidence Response Team (LM-CIRT) and providing assistance to the end user with help from its "Analyst on Demand" program.

Thus, customers can mitigate cyber-attacks at their root, and better understand the nature of the breach that allowed hackers in, so that they it can be repaired, the companies said.

"The combination of Lockheed Martin's Threat Intelligence, the Cybereason Detection and Response Platform and Lockheed Martin's leading Analyst services is a winning trifecta for enterprises combating advance persistent threats targeting their organizations," said Div,. "Launching Wisdom EDR, powered by Cybereason, is proof positive that market leaders like Lockheed Martin believe in the merits of our enterprise EDR platform to detect and mitigate advanced attacks."

National Post

Canada's drones above

Wednesday, 09 March 2016

Byline: Lauren Heuser

Section: oped

OpEd: The Canadian government is shopping for military drones. Although a National Defence spokesperson has said they would be used "primarily" for surveillance purposes, Canada's air force has indicated it hopes they will be capable of "carrying and employing precision-guided munitions." Canada should learn from the United States, and not try to bring this important technology in through the back door.

The Obama administration - which has used drones to kill an estimated 3,300 individuals - has faced mounting criticism of its secretive drone program. It's not difficult to see why. It only formally acknowledged that drone strikes were being used against suspected terrorists in 2012, years after they'd become a fixture of its counter-terrorism strategy. Presidential assistant John Brennan justified them on grounds that the U.S. was in "an armed conflict with al-Qaida, the Taliban, and associated forces, in response to the 9/11 attacks."

In 2014, the administration released a memorandum justifying its attack on an American-born terrorist, but only after being compelled to do so by a court. It has resisted disclosure of other documents. Groups such as Human Rights Watch and the American Civil Liberties Association have called on the government to adopt a more "transparent and accountable approach" to its operations.

There are lessons here for Canada. The government should be transparent about drones' benefits and risks, and should set clear rules of engagement and accountability to govern their use. Drones' benefits are considerable. Industry experts say they're already being used for activities that would be far riskier and less effective if carried out by humans. Search and rescue operations and forest fire monitoring are but two examples of ways in which they're used.

Drones also present risks, although it's important to be clear about what those are. The fact they may be capable of killing is not, of itself, cause for concern. Military planes, after all, have been armed for decades. If one accepts that lethal force is necessary in warfare, there is no moral or legal distinction between using drones (where the operator is miles away) or a bomber (where the pilot is in the cockpit) to strike a target. Indeed, of the two, drones would seem the more favourable choice, as their greater precision reduces the likelihood of collateral damage.

The risk "killer" drones present, then, relates less to their lethal capabilities, and more to what they have made possible: executing targeted individuals. International and domestic law affords all people basic rights, like the right to life, a fair trial and due process. How can rights-respecting nations disregard these when it comes to people suspected of bad things?

In short, because international law relaxes the standards to which states are held during times of war. Under the laws of armed conflict, states are permitted to kill combatants outside of the judicial process - not because they are guilty (although they may be) - but because the combatants are enemy agents. The state is not recognized as pursuing a law enforcement agenda against individuals in this circumstance.

Targeted killings hinge, then, on a country being at war. The controversy over the U.S.'s drone strikes relates in part to experts being divided over whether the government can legitimately consider itself to be at war, when the "war on terror" has spanned so many years, different territories and different terrorist organizations. If it no longer is, the continuation of its targeted killings is unlawful.

A second concern about drones relates to their surveillance capabilities, which enable them to gather far more information on individuals than was previously possible. While some would argue this is an advantage to be exploited, others would say it risks abusing individuals' privacy rights.

Both sides have a point, which is why a full airing of the security and civil liberties issues is so important. Should judicial authorization be required to conduct surveillance on individuals? Should targeted killings be permitted in certain circumstances? If so, when and what level of intelligence on a person must first be obtained? These are just a few

of the questions we need to address.

While international law provides the minimum rules to which we must adhere, Canada could choose to hold itself to a higher standard. The important thing is that it develops rules ahead of any attacks, not on an ad hoc or after-the-fact basis.

In addition to setting rules of engagement, Canada should establish a politically accountable body to oversee drone activities. Following the template of the U.S.'s security committee, which includes Congressional and Senate representatives, Canada could establish a parliamentary committee that reviews droneobtained intelligence and investigates alleged abuses of the rules.

Like any new technology, drones present opportunities but also risks. Canada should manage the introduction of this technology with a view to ensuring that, in both appearance and fact, it not only operates on the right side of the law, but also does right by its citizens and the world.

Lauren Heuser is a lawyer and journalism fellow at the Munk School of Global Affairs.

One News Now New Zealand

Spy review suggests allowing GCSB to watch New Zealanders

Wednesday, 09 March 2016

Byline: Andrea Vance

Section: general

Wellington - A review into the security services has just been published - with 107 recommendations that include expanded powers and greater oversight.
It proposes the GCSB - long-seen as the foreign spy agency - be allowed to carry out surveillance on Kiwis.

The powers of the Bureau came under intense public scrutiny after it was found to be illegally spying on more than 80 New Zealanders.

New laws were rushed through Parliament in 2014 that would allow GCSB to carry out surveillance on behalf of the Security Intelligence Service, police and the Defence Force.

But the review authors say those laws are still unclear - and GCSB is now refusing to do that work.

Former deputy prime minister Michael Cullen, one of the authors, said: "They can't use the GCSB capacity ... if you look at section 8C [of the 2014 GCSB Act] it looks as if they will be able to ...but the view taken by GCBS is that they can't... they have felt that the legislation is insufficiently clear ...because of some mistakes that have been made over recent years...the GCSB has inevitably become extremely risk adverse around interpretation of its act...that's why I think it is wrong to say it is a widening of powers - I think it is actually clarifying what ought to be able to be done."

Cullen claims the GCSB couldn't intercept the communications of a Kiwi who is in trouble, or kidnapped overseas.

The review also recommends more powers for the SIS and GCSB to carry out visual surveillance.

Under emergency foreign fighters legislation passed in 2014, this could be carried out for 24 hours without a warrant.

A period of 48 hours was initially propsed but rejected by Parliament.

The review suggests it should also be broadened for other cases, not just counter terrorism - but with stronger oversight.

The passport of suspected jihadis travelling overseas would also be cancelled for a maximum three years - up from the current 12 month limit.

Another proposal would see the agencies also be able to access and retain electronic records from other government departments.

This would include customs information, immigration databases, police info, and births, deaths, marriages and relationship registers and citizen registers. This would be through a joint agreement between ministers.

Other personal information - tax info, driver license photos, and National Student Identification Numbers would also be able to be accessed on a case-by-case basis, with authorisation.

As well as broader powers, Cullen and fellow reviewer Dame Patsy Reddy have also suggested a stronger authorisation regime which has three tiers.

The first - and strictest stage - would require a warrant from the Attorney-General and a judicial commissioner. This would be required for spying on Kiwis. There would be a panel of three judicial commissioners, with one available at all times.

In "situations of urgency and emergency" the agencies could start surveillance without this "tier one" authorisation - and the Chief Commissioner of Warrants can order it be stopped.

The agencies must provide an explanation and get proper authorisation within 48 hours.

This "'tier one'" sign-off could also be used for surveillance done for training employees.

"Tier two" would see just the Attorney-General approve a warrant for non-Kiwis.

The lowest level of authorisation would be a "policy statement" from the Security Services Minister and would cover the collection of surveillance from public places or other publicly available info.

Cullen said the terms of reference for the review meant his report could not recommend the GCSB and the SIS be merged. But the agencies will be covered by one piece of legislation.

Radio New Zealand News

Security analyst says rise in number of financial transactions linked to terrorism a worry

Wednesday, 09 March 2016

Byline: Staff Writer

Section: general

Wellington - A security analyst says a massive number of transactions possibly linked to terrorism can get through New Zealand's financial systems without being picked up.
Figures released to RNZ News by the police's Financial Intelligence Unit show the number of financial transactions suspected of being linked to terrorism almost doubled from 21 in 2014 to 40 in 2015.

Paul Buchanan says some people are using New Zealand's financial systems to make transactions linked to terrorism.

Paul Buchanan says New Zealand is seen as a soft target due to its loose financial regulations.

The Hill

DHS: No evidence of Ukraine power grid hack in US

Wednesday, 09 March 2016

Byline: Cory Bennett

Section: general

Washington - The Department of Homeland Security said the U.S. power grid is not under threat from the historic cyberattack that recently took out a portion of Ukraine's power grid.
The December digital assault, widely believed to be the first example of hackers causing a widespread power outage, put energy companies around the world on edge as U.S. officials flew in to assist with the investigation.

The attack "should be, and must be, a wake-up call for those who haven't already been awakened by this problem and this risk," Homeland Security Secretary Jeh Johnson said Tuesday at a Senate hearing about his agency's budget.

The DHS concluded the malicious software that downed the grid in Ukraine has not extended to the U.S. for the time being.

In a blog post, the agency said it was planning an "expanded outreach campaign" to discuss the Ukraine incident with all critical infrastructure industries.

"We are working with critical infrastructure all the time," Johnson said on Tuesday. "I've spoken to CEOs and utilities about this problem."

"There's certainly more to do," he added.

The Ukraine outage caused roughly 200,000 households to lose power for up to six hours. Researchers and Ukranian authorities have blamed Russia for the digital assault, but the DHS has not publicly named a suspect.

Senate Homeland Security Committee Chairman Ron Johnson (R-Wis.), who was overseeing the hearing, suggested he would explore legislative options to help bolster U.S. grid security.

"I want to work very closely with you over the next few months to do whatever we can legislatively in working with your department," he told the Homeland Security head.

In the last few years, policymakers have been searching for ways to secure the nation's power grid from a major cyberattack as security experts repeatedly warn the industry's digital defenses are dangerously lagging and underfunded.

National Security Agency Director Adm. Michael Rogers has told lawmakers that China and likely "one or two" other countries are currently sitting on the grid, with the ability to literally turn out the lights if they wanted to.

Johnson pressed the DHS chief about what steps the agency has taken to thwart this scenario.

"Where are we on that?" he asked.

"Better than we were, but there's more to do," Johnson replied, citing better partnerships with the private sector and a freer flow of data between government and industry.

"We're in a better place than we were," he said.

Federal News Radio

DHS chief: Agency 'not where we should be' for hiring cyber talent

Wednesday, 09 March 2016

Byline: Merideth Sommers

Section: general

Washington - Homeland Security Secretary Jeh Johnson defended his department's fiscal 2017 budget on Capitol Hill, telling the Senate Homeland Security Committee that increasing the agency's cyber workforce and capabilities is important to strengthening national security.
Johnson testified before the committee on March 8. He explained to lawmakers that the agency needs to build up its workforce in order to meet growing threats in cyberspace and compete with the private sector, which is where many qualified candidates end up working.

"We are competing in a tough marketplace against the private sector, that is in a position to offer a lot more money," Johnson said. "[Homeland Security undersecretary for the National Protection and Programs Directorate] Susan Spaulding and her people are making very aggressive efforts to A) Implement the 2014 legislation you passed and B) in the interim do a lot of things in terms of recruitment; expediting the hiring process and so forth. We need more cyber talent without a doubt in DHS, in the federal government, and we are not where we should be right now, that is without a doubt."

DHS requested $40.6 billion in appropriated funding, with an increase in total spending to $66.8 billion.

According to Johnson's submitted testimony, the fiscal 2017 DHS budget proposes:

* An increase in total workforce from 226,157 to 229,626

* A 1.6 percent pay raise

* $274.8 million for the Continuous Diagnostic Mitigation program, which provides hardware, software and services designed to support activities that strengthen the operational security of federal ".gov" networks

* $47.1 million to sustain the EINSTEIN program

* Expanding DHS' 10 cyber response teams to 48

A 'sense of patriotism'

While committee members had questions and concerns about how the budget would address certain issues related to national security -- including resources for northern border security, drug smuggling and aviation security -- some lawmakers pledged their support to the secretary for building up the agency's cyber workforce.

"I have stated repeatedly, I'm very impressed with... the quality of the federal workforce; these people are patriots, they take their mission seriously about keeping the nation safe," said Committee Chairman Ron Johnson (R-Wis.). "But I also understand the constraints. I know what the private sector will pay for talent and you're constrained there. So we're going to have to put our heads together and figure out what do we need to do so that your department is staffed with the best and the brightest. There are

plenty of patriots in America that will do it and will do it at a really great financial sacrifice. Let's try and break down barriers we create bureaucratically, to resource you."

Sen. Tom Carper (D-Del.) suggested the agency stress the importance of serving one's country in its message to potential hires.

Carper pointed out that Phyllis Schneck, the deputy undersecretary of cybersecurity in the National Protection and Programs Directorate at DHS, told him she felt an obligation and desire to give back to her country, which is why she left the private sector to work for the federal government.

"It's all well and good cyber warriors work for other companies and businesses and so forth, but in this case, there's something to be said for appealing to people's sense of patriotism," Carper said. "I think that's what one of the things that draws her. That's a calling card if you will, that we can use and I'm sure that we do."

Secretary Johnson said he agreed with the senator, suggesting the agency "ought to appeal to people's sense of patriotism."

Secretary Johnson said in his testimony that among some of the other human capital goals for DHS this fiscal year is improving employee morale.

"We've been on an aggressive campaign to improve morale over the last two years," he said. "It takes time to turn a 22-component workforce of 240,000 people in a different direction. Though the overall results last year were still disappointing, we see signs of improvement. This year we will see an overall improvement in employee satisfaction across DHS."

The Secretary also said DHS will be working to develop a Cybersecurity Assurance Program "to test and certify networked devices within the 'Internet of Things.'"

Johnson said in his testimony that the agency was asking Congress to officially authorize the Joint Task Forces that were stood up to help with southern border security. The Task Forces creation is part of the Unity of Effort initiative.

Johnson also highlighted that DHS is looking to reform its human resources process.

"We are making our hiring process faster and more efficient," he said ."We are using all the tools we have to recruit, retain and reward personnel."

CBP incentive, hazardous duty pay

Sen. John McCain (R-Ariz.) voiced his concern about filling vacancies and offering incentives to customs and border protection officers in high- traffic areas, adding that he was introducing legislation to address this potential pay increase.

"I am of the view that we need to have some kind of incentive pay or hazardous duty pay at ports of entry that experience high- traffic flows," McCain said. "It's a very tough environment... I can understand how tough a duty it is. I think just as we in the military, we provide incentive pay for hardship positions, I hope that you would look at that and I'll be introducing legislation on it, because it's just not sufficient as you know. We're well over 100 customs agents short, it's either there's something with the level of staffing required or something wrong with the level of personnel."

Secretary Johnson said he would be happy to look at the proposed legislation and similar to the cyber workforce, "we're not where we need to be, no argument from me there."

"CBP needs to and is making aggressive efforts to hire, to bring on people faster, get them through the polygraph exams," Secretary Johnson said. "I fully support the hiring of veterans and making it easier to hire veterans."

Scoop News New Zealand

Spy report a dream come true for Five Eyes

Wednesday, 09 March 2016

Byline: Valerie Morse

Section: general

Opinion: The release of the Independent review of intelligence and security recommends a range of changes that are dangerous to ordinary people, both within NZ and elsewhere, and represents a massive concentration of state power.
The major recommendation is the consolidation of the two acts governing the GCSB and the SIS into a single law. As Radio NZ reported, "A single piece of legislation would mean both agencies operated under the same objectives, functions and powers and warrant authorisation framework." This is deeply problematic.

It must be understood at the outset that both GCSB and the SIS are essentially political police: they exist to identify threats to the New Zealand state, essentially "national security." These agencies do not exist to root out criminal activity, that is the job of the Police. And, although in 2013, the GCSB was given the

power to assist police with any matter, it is not an objective of that organisation (or the SIS) to prevent, detect or prosecute criminal offending. While the definition of criminal offences are spelled out quite clearly in law with identifiable components and evidentiary thresholds, threats to "national security" are at best vague and difficult to define. Even the Law Commission, an eminent body of NZ legal practitioners, struggled to explain what the national security is, noting "While the New Zealand courts have not yet been called upon to define national security, we expect that they will also face difficulties in pinning down the concept although there are varying definitions in use." (National Security Information in Proceedings, p.14).

Historically, the GCSB and the SIS have been organisations with quite different functions within the ambit of political policing. The SIS has been responsible for internal security, monitoring Maori, political dissidents, refugee and migrant populations, and extremist groups. The GCSB, on the other hand, is entirely a child of the US National Security Agency, is New Zealand's contribution to the Five Eyes Network, and until relatively recently, worked on external signals intelligence (satellite, radio and internet).

Now, however, the argument goes, because of the global reach of the internet, the lines that existed between internal and external no longer matter. Thus, rationalising the two agencies into one makes sense. This reasoning dovetails nicely into the review's recommendation that the current restriction on the GCSB to intercept the private communications of New Zealanders for its intelligence function be removed. The enormous powers of the GCSB can then be unleashed to capture all electronic communications freed of the restrictions on nationality, legalising all of the programmes that Edward Snowden told us were happening (XKeyscore, Prism, etc), but which the government has consistently denied for the past three years. These capabilities can be coupled with that of the SIS who can now install a video camera in your home for up to 24 hours with no warrant to provide "total information awareness".

Michael Cullen's ridiculous argument that the GCSB needs to spy on New Zealanders to protect them, providing the example of how hamstrung the GCSB would be should someone be lost at sea ignores the fact that the GCSB can already provide any assistance to the Police (with no thresholds whatsoever about what the Police are doing). And it is most likely that the Police would be the agency leading any missing person investigation. Cullen's example demonstrates either a stunning lack of knowledge of the GCSB's current powers or a desire to promulgate false examples of how such additional powers would be used. In either case, this person should not be leading a so-called "Independent review."

After all, we should ask, just exactly how many New Zealanders lives have been protected by the GCSB/SIS ability to spy on them already? We have no evidence of any people being brought to justice for attempts to undermine national security - and surely if there was evidence of such offences, they would be followed up by both police and the courts. One New Zealander whose life was most definitely not protected by the GCSB's ability to spy on him was Daryl Jones, a NZ citizen killed in a US drone attack in Yemen. He was subject to an intelligence warrant (we must assume a GCSB interception warrant as it is the agency with such capability) that provided the NSA with at least some data about him. Whatever

your view about Daryl Jones, he was not an existential threat to New Zealand (or the US for that matter) nor did he received any due process of law (e.g. he was never brought before any court or accused of any crime). So the evidence we actually do have is of these agencies violating the rights of New Zealanders, not protecting them. There is a list of other violations of rights regarding both agencies that have been well canvassed in the media.

The recommendation that existing laws were "inconsistent, and a lack of clarity meant both the agencies and their oversight bodies were at times uncertain about what the law does or does not permit, which makes it difficult to ensure compliance" also beggar's belief. The GCSB law was totally overhauled in 2013, the SIS Act has been amended a half a dozen times since 2007 - and somehow at none of these points were the "inconsistencies and lack of clarity" identified and cleared up? In fact, clarity was a major issue in the GCSB Act of 2013 debate: people could see that the law allowed the agency to spy on them in a way that had previously been unlawful. The idea that the GCSB interpretation of its law makes it "risk-averse" as the review notes, (in other words, unwilling to spy on people they aren't sure they are allowed to) is a GOOD thing that should be applauded not something that needs to be amended to widen its scope even further.

Curiously, the government is hot-footing it to change the law to eliminate this "lack of clarity" but no such urgency has been extended to the Solicitor-General's 2007 view that the Terrorism Suppression Act was "unnecessarily complex, incoherent...and almost impossible to apply to a domestic situation'" Rather it seems the government wants clarity to spy but not clarity on the reasons for its spying.

One final note is the commentary about the need for "bipartisan" support for intelligence law changes, such support ostensibly giving legitimacy to, and public confidence in, these agencies. But from their start, these agencies have been shrouded in secrecy and half-truths (if not outright lies). The public is hardly able to make an "informed decision" under these circumstances. What the public does know, however, has given rise to significant public unease - and that unease is not something new. In 1977, tens of thousands marched against the expansion of the SIS. In 2013, such demonstrations were repeated. These agencies act in the shadows and as such, most New Zealanders are unaware of what they are doing. It is not that they are unconcerned, but rather that other things are more obviously of urgent pressing concern: health, education, welfare and work. But when the realities of these agencies are exposed, it takes little for the public opposition to be mobilised. It is unlikely that this would ever be a make or break election issue, but that doesn't mean that people in New Zealand consent to these agencies or to these powers, or that cross-party support gives them any legitimacy with ordinary people.

The Hill

Snowden: FBI's stance in Apple case is 'horses---'

Wednesday, 09 March 2016

Byline: Julian Hattem

Section: general

Washington - National Security Agency leaker Edward Snowden on Tuesday had harsh words regarding the FBI's claim that only Apple can break into the iPhone used by one of the San Bernardino, Calif., terrorists.
"Respectfully, that's horses---," the former government contractor said during a conference hosted by liberal advocacy group Common Cause.

The FBI has been aware of hardware attacks "since the '90s" that could gain access to otherwise locked information on Syed Rizwan Farook's phone, Snowden said via a Google hangout from Russia, where he has been living to evade federal charges for leaking government secrets.

He later added in a post on Twitter that the "global technological consensus is against the FBI."

As one example, Snowden linked to an American Civil Liberties Union (ACLU) blog post alleging that the FBI can "easily work around" a security mechanism on the iPhone.

"The FBI wants us to think that this case is about a single phone, used by a terrorist," ACLU technology fellow Daniel Kahn Gillmor wrote in the post. "But it's a power grab."

Justice Department lawyers have refuted the point in legal filings, and FBI Director James Comey has backed up the claim on Capitol Hill.

"If we could have done this quietly and privately, we would have done it," he testified on Capitol Hill earlier this month.

Snowden, a frequent antagonist of U.S. intelligence and law enforcement agencies, has previously defended Apple in its opposition to the FBI request.

On Tuesday, he claimed that the company's insistence on strong digital protections was "a good example" of technology's ability to flip the script on government officials.

"The FBI would not be as pissed off as they are if it was not effective," he said.

The Guardian (London)

FBI quietly changes its privacy rules for accessing NSA data on Americans

Wednesday, 09 March 2016

Byline: Spencer Ackerman

Section: general

New York - The FBI has quietly revised its privacy rules for searching data involving Americans' international communications that was collected by the National Security Agency, US officials have confirmed to the Guardian.
The classified revisions were accepted by the secret US court that governs surveillance, during its annual recertification of the agencies' broad surveillance powers. The new rules affect a set of powers colloquially known as Section 702, the portion of the law that authorizes the NSA's sweeping "Prism" program to collect internet data. Section 702 falls under the Foreign Intelligence Surveillance Act (Fisa), and is a provision set to expire later this year.

A government civil liberties watchdog, the Privacy and Civil Liberties Oversight Group (PCLOB), alluded to the change in its recent overview of ongoing surveillance practices.

The watchdog confirmed in a 2014 report that the FBI is allowed direct access to the NSA's massive collections of international emails, texts and phone calls - which often include Americans on one end of the conversation. The activists also expressed concern that the FBI's "minimization" rules, for removing or limiting sensitive data that could identify Americans, did not reflect the bureau's easy access to the NSA's collected international communications.

FBI officials can search through the data, using Americans' identifying information, for what PCLOB called "routine" queries unrelated to national security. The oversight group recommended more safeguards around "the FBI's use and dissemination of Section 702 data in connection with non- foreign intelligence criminal matters".

As of 2014, the FBI was not even required to make note of when it searched the metadata, which includes the "to" or "from" lines of an email. Nor does it record how many of its data searches involve Americans' identifying details - a practice that apparently continued through 2015, based on documents released last February. The PCLOB called such searches "substantial", since the FBI keeps NSA-collected data with the information it acquires through more traditional means, such as individualized warrants.

But the PCLOB's new compliance report, released on Saturday, found that the administration has submitted "revised FBI minimization procedures" that address at least some of the group's concerns about "many" FBI agents who use NSA-gathered data.

"Changes have been implemented based on PCLOB recommendations, but we cannot comment further due to classification," said Christopher Allen, a spokesman for the FBI.

Sharon Bradford Franklin, a spokesperson for the PCLOB, said the classification prevented her from describing the rule changes in detail, but she said they move to enhance privacy. She could not say when the rules actually changed - that, too, is classified.

"They do apply additional limits" to the FBI, Franklin said.

Timothy Barrett, a spokesman for the office of the director of national intelligence, also confirmed the change to FBI minimization rules.

Barrett also suggested that the changes may not be hidden from public view permanently.

"As we have done with the 2014 702 minimization procedures, we are considering releasing the 2015 procedures. Due to other ongoing reviews, we do not have a set date that review will be completed," he said.

Until that hypothetical release, it remains unknown whether the FBI will now make note of when and what it queries in the NSA data. The PCLOB did not recommend greater record-keeping.

Last February, a compliance audit alluded to imminent changes to the FBI's freedom to search the data for Americans' identifying information.

"FBI's minimization procedures will be updated to more clearly reflect the FBI's standard for conducting US person queries and to require additional supervisory approval to access query results in certain circumstances," the review stated.

The reference to "supervisory approval" suggests the FBI may not require court approval for their searches - unlike the new system Congress enacted last year for NSA or FBI acquisition of US phone metadata in terrorism or espionage cases.

Privacy advocates say that this leeway for searches that NSA and FBI officials enjoy is a "backdoor" around warrants that the law should require. In 2013, documents leaked to the Guardian by Edward Snowden revealed an internal NSA rule that Senator Ron Wyden has called the "backdoor search provision", for instance.

While the NSA performs warrantless collection, internal rules permit the FBI to nominate surveillance targets. Those targets are supposed to be non-Americans abroad, but Americans' data is often swept up in the surveillance.

The legal underpinnings for the dragnet, a 2008 amendment to the Foreign Intelligence Surveillance Act, are set to expire this year. A scheduled expiration of the Patriot Act last year gave critical leverage to legislators who wanted to rein in the bulk collection of domestic phone records, and intelligence officials last month implored Congress to reauthorize the measure wholesale.

"Reasonable people could and did argue about how important the telephone metadata collection was," FBI director James Comey told the House intelligence committee last month. "This is not even a close call. This is - if we lost this tool, it would be a very bad thing for us."

Several civil- libertarian legislators have vowed to push for an expiration of Section 702, arguing that it represents a growing surveillance authority that has moved beyond terrorism and espionage, and into the hunt for general weaknesses in the internet. The chief lawyer for the intelligence community, Robert Litt, said in 2014 that the law provides surveillance authorities the powers are "not only about terrorism, but about a wide variety of threats to our nation".

A representative for the Fisa court deferred comment to the administration.

The Intercept

The FBI vs. Apple Debate Just Got Less White

Tuesday, 08 March 2016

Byline: Jenna McLaughlin

Section: column

Column - The court fight between Apple and the FBI prompted a slew of letters and legal briefs last week from outside parties, including many tech companies and privacy groups. But a particularly powerful letter came from a collection of racial justice activists, including Black Lives Matter.
The letter focused on potential civil rights abuses, should the FBI gain the power to conscript a technology company into undermining its own users' security.

"One need only look to the days of J. Edgar Hoover and wiretapping of Rev. Martin Luther King, Jr. to recognize the FBI has not always respected the right to privacy for groups it did not agree with," wrote the signatories, including arts and music nonprofit Beats, Rhymes & Relief, the Center for Media Justice, the Gathering for Justice, Justice League NYC, activist and writer Shaun King, and Black Lives Matter co-founder and Black Alliance for Just Immigration executive director Opal Tometi.

Those tactics haven't ended, they argue. "Many of us, as civil rights advocates, have become targets of government surveillance for no reason beyond our advocacy or provision of social services for the underrepresented."

In Washington and Silicon Valley, the debate over unbreakable encryption has an aura of elite, educated, mostly male whiteness -- from the government representatives who condemn it to the experts who explain why it's necessary.

But the main targets of law enforcement surveillance have historically been African-American and Muslim communities.

Malkia Cyril, co-founder of the Center for Media Justice, one of the letter's signatories, gave a speech at one of several nationwide protests outside Apple stores two weeks ago, supporting the tech giant and pointing out the FBI's history of surveilling black activists. "In the context of white supremacy and police violence, Black people need encryption," she wrote in a tweet.

Others representing Black Lives Matter attended protests across the country, including in front of the FBI headquarters itself -- the J. Edgar Hoover building -- in downtown Washington, D.C.

"I've been reviewing the Apple vs. FBI lawsuit and now realize how important it is that that Apple wins the lawsuit. #DontHackApple," DeRay Mckesson, Baltimore mayoral candidate and prominent Black Lives Matter organizer, tweeted on February 22. "When I was arrested in protest, my iPhones were in police custody. They were secure. The police couldn't access my info," he added. "If Apple has to create an insecure iPhone iOS app, all of the private data that we store on our phones is at risk."

The letter to California federal Magistrate Judge Sheri Pym, who will hear arguments March 22 on the case, is the start of more to come.

"I think racial justice organizations have a clear stake in the fight for encryption," the Center for Media Justice's Cyril said. "It was really important to me that our voices were raised here ... because they wouldn't be [represented] by others."

Cyril, a poet and grassroots organizer born to an editor of the Black Panther newspaper, wants the average person to understand how surveillance impacts low-income communities of color -- where she argues that government spying was born.

"The mundane surveillance of people of color is what gives rise to bulk surveillance at a federal level ... not the other way around," she said. "Whatever has been considered normal at a local level" -- including systems of suspicious activity reports, predictive policing, and other tactics -- "has now been considered normal at the federal level."

Tometi, another signatory, wrote in an email to The Intercept that "one of the most alarming parts of that history has been the ways that surveillance has been misused against Black people who have been advocating for their justice. It's been used to discredit, abuse, and incarcerate them. It's important we speak out now before it's too late."

King said the Apple fight, and the phone security at risk if Apple loses, is "out of sight, out of mind for a lot of people." But it ties into a greater problem, he said: the continuous monitoring that racial justice activists experience.

He said he is "concerned about how the government may abuse its opportunity to call us threats when we're not," and then use that assumption as justification for hacking into their cellphones or using other invasive spying techniques.

Over the summer, a cybersecurity firm, described Black Lives Matter organizers Mckesson and Johnetta Elzie as "threat actors" who needed "continuous monitoring" to maintain public safety. The company, ZeroFox, briefed members of an FBI intelligence partnership program in Maryland on its analysis of the Freddie Gray protests -- which it later delivered to Baltimore City officials.

"It's only a matter of time until someone says, 'We really need to access Shaun's King's cell phone,'" King said. "We're not that many steps away from that."

"I have deep concerns about how various methods of surveillance are already being used against social justice and human rights defenders in the Black Lives Matter movement," Tometi wrote.

"Basically, what people need to understand is that to protect your First and Fourth Amendment rights in the digital age, we need to update the law to the digital age," Cyril said. "Everything we do is online ... encryption is necessary for a democracy."

Cyril calls for a public debate, so that people can understand the real stakes. "Let's be clear. Everybody has everything to hide. I want to hide my banking info from thieves -- everything that is mine. I think the public needs to understand that."

NBC News

Bill Gates: Apple Could Propose a Balance in FBI Dispute

Tuesday, 08 March 2016

Byline: Matthew Deluca

Section: general

New York - Bill Gates answered some questions about Apple's ongoing dispute with the FBI during a Reddit "Ask Me Anything" on Tuesday -- and stuck solidly to the same neutral position he's maintained in earlier comments.
"I think there needs to be a discussion about when the government should be able to gather information," Gates said in response to one Redditor's question.

"What if we had never had wiretapping? Also the government needs to talk openly about safeguards."

Gates first gave his thoughts on the matter -- in which Apple is refusing a court order to help the FBI unlock an iPhone used by one of the shooters in San Bernardino -- in a Feb. 23 interview with the Financial Times.

The Microsoft co-founder later said that he felt those quotes, which were widely characterized as putting him in the FBI's camp, did not accurately represent his full opinion on the case.

But Gates' answers on Tuesday, much like those he gave in another interview with Bloomberg TV, also didn't do much to clear up where the tech pioneer personally stands on the contentious case. Asked what he would do if he were in Apple's position, Gates said the company could offer a Plan B.

"Maybe they could propose an overall plan for striking the balance between government being able to know things in some cases and having safeguards to make sure those powers are confined to appropriate cases," Gates said. "There is no avoiding this debate and they could contribute to how the balance should be struck."

Gates is no longer involved in the day-to-day operations of Microsoft, which along with nearly every other major tech company has filed a "friend of the court" brief supporting Apple in the California case.

BBC News

Nigeria's Buhari says MTN fuelled Boko Haram insurgency

Tuesday, 08 March 2016

Byline: Staff report

Section: general

London - Mobile phone giant MTN fuelled the Islamist-led insurgency in Nigeria by failing to disconnect unregistered sim cards, the Nigerian president has said.
Muhammadu Buhari made the comment during a visit to Nigeria by his South African counterpart Jacob Zuma.

Last year, Nigeria fined the South African-owned firm $3.4bn (£2.7bn) for missing a deadline to disconnect cards.

Nigeria believes Boko Haram militants use unregistered sim cards to co-ordinate attacks.

BBC Nigeria reporter Martin Patience says fine has overshadowed talks in the capital, Abuja, between the leaders of Africa's two largest economies.

"You know how the unregistered [sim cards] are being used by terrorists and between 2009 and today, at least 10,000 Nigerians were killed by Boko Haram," President Buhari said at a joint press conference with Mr Zuma.

Other mobile phone operators complied with a mid- 2015 deadline to register all sim cards, but "unfortunately, MTN was very very slow and contributed to the casualties", Mr Buhari added, in his first comments on the issue.

Nigeria initially imposed a $5.2bn fine on MTN in October, but brought it down to $3.4bn.

Mr Buhari said MTN, which was in talks with Nigeria to reduce the fine further, could make gradual payments, Reuters news agency reports.

Last month, MTN said it had dropped court action to challenge the fine, and had paid $250m as part of efforts to reach an "amicable settlement".

MTN has 231 million subscribers in 22 countries across Africa, Asia and the Middle East. However, Nigeria is its biggest market.

In September, the company was named as most-admired brand in Africa in the Brand Africa 100 awards, beating Samsung, while it was also awarded the continent's most valuable brand, worth $4.6bn.

MTN was South Africa's second mobile operator when it was set up in 1994 after the end of apartheid.

It began its expansion across Africa four years later with operations in Rwanda, Uganda and Swaziland.

The six-year insurgency in north-eastern Nigeria has killed some 17,000 people and forced more than 2.6 million from their homes.

Mr Buhari said in December that Boko Haram was "technically" defeated but attacks have continued.

The National (UAE)

Cyber experts needed to stay ahead of developing threats

Wednesday, 09 March 2016

Byline: Caline Malek

Section: general

Abu Dhabi - Training the region's next generation of cyber experts will be vital in fighting evolving military threats in the future, according to defence experts at the Global Aerospace Summit.
They said the threat is especially felt in the Middle East where there is a shortfall in manpower and human capital development.

As terrorist groups become more technologically-savvy, governments and the defence industry will have to stay ahead of the curve and design weapons in such a way to keep their enemies at bay.

"The future is uncertain," said Robert Harward, retired vice admiral US Navy Seal and chief executive of UAE Lockheed Martin. "We know these existential threats in the region like Iran and you look at newer existential threats that we had missed like radical jihadists gaining capabilities. I think all these are indicative of the threats we'll have to deal with."

He said the defence industry was bringing technology to stay ahead of some of these curves. "The UAE is the perfect example of this," he said. "In partnership with the US, the UAE was able to bring top line capabilities, enabling them to defend themselves against imminent threats. We're going to need to work with the services and our allies to stay ahead of the threats and I think a big issue for all of us is do we collectively with our allies and the defence industry have the capacity to stay ahead of the threats?"

A US study by global information company IHS found that the UAE and Saudi Arabia were named the region's top importers of defence systems in 2014, most of which were advanced military aircraft and missiles.

The Emirates was ranked seventh in defence spending and fastest growing budgets the previous year, with 14.6 per cent. "It is important for us to maintain this technology lead," said Dr Theodore Karasik, senior adviser at Gulf State Analytics. "The reason why I argue this is because the 'bad guys' are getting very smart about the use of technology, even if you look at Isis, they're actually quite smart at trying to experiment with UAVs, which can be weaponised, and there has been evidence of some of them doing

that. These ideas are still continuing to percolate and it challenges us to be ahead of that curve to make sure we're ready for that kind of event. These are some of the trendlines that go about how we design weapons and working on a concept of operations that are needed to keep enemies at bay."

But the country's growing defence sector puts into question its security and opens a potential window to cyber attacks. A US report compiled by Going Global Defence Intitiative of the Virginia Economic Development Partnership two years ago found that UAE Government websites were vulnerable to cyber attacks which sought to exploit defence and security flaws. It said the country's integrated missile defence system would require comprehensive protection from cyber threats.

"The question that gets a lot of thought these days is where do cyber attacks fit in the next generation of military threats, whether it's directly on the battlefield or not," said Christopher Davis, country leader and president of UAE Raytheon. "Cyber attacks are going to be a fact of life. It's a big issue for us with our future warfare and I think a real question for us all is how do we train and retain the human capital who are the cyber experts for the next generation. Regionally, it's a real issue especially in the Middle East where manpower and human capital development is a real priority and where there is a shortfall."

The impetus is on the defence industry and regional defence forces, according to Simon Carroll, president and general manager of Saab Middle East, to find a way to work together more regularly to develop the technology needed to defeat the threat. "I think in this region in particular, we need to find a balance because not all the organisations that the battle is against at the moment are [able] to use their technical capability," he said. "We need to use our cyber asymmetry to our advantage and work more closely with defence partners and forces to be that one step ahead so we can avoid these tragedies that lead into a next generation of technology development."

Ottawa Citizen
Canada needs to educate more tech grads: Report
Thursday, 10 March 2016
Byline: Vito Pilieci

Ottawa - There will be as many as 182,000 high-paying technology jobs up for grabs in Canada by 2019, but the country's school systems aren't producing enough high technology expertise to fill those positions, according to a new research paper.
The solution? Putting computer science courses on par with literacy and arithmetic, and teaching those courses beginning in kindergarten.

Teaming with Microsoft Corp. and dozens of other corporations and public institutions, including the Ottawa Catholic School Board, the Information and Communications

Technology Council (ICTC) - a technology trend researcher - released a 51-page paper Wednesday called Digital Talent: Road to 2020. It calls on the federal government to oversee the creation and implementation of a nationwide Digital Talent Strategy aimed at encouraging more Canadian youth to pursue studies in information and communications technologies.

ICTC, founded in 1992 to research issues and lobby on behalf of Canada's technology industry, released the research paper at a formal event at the Canadian Museum of Nature in downtown Ottawa.

The research paper said there will be at least 182,000 information and communications technology jobs on offer by 2019, and at least another 32,000 will be available in 2020.

Those numbers could increase, depending on how quickly emerging areas such as virtual reality, robotics, cyber- security and advanced manufacturing (including 3D printing technologies) expand.

There are 877,470 people working in information and communications technology jobs in Canada, the research showed, and more than 43 per cent of all technology workers are employed in the professional and technical services industry. But they also have a significant showing in health care, the public sector and in manufacturing.

These are high-paying and stable jobs, according to ICTC. But despite the potential for a highpaying career, not enough Canadians are pursuing education in technology-related fields.

Of the 2.21 million Canadians enrolled in post-secondary institutions, only six per cent, or 126,000 students, are enrolled in programs that will help them land a job in the technology sector, the report said. In 2015, 12,800 students graduated from Canadian universities with degrees in information and communications technology-related studies.

The research paper came out just two days after the Entertainment Software Association of Canada's (ESAC) released its own report calling on the federal government to take a leadership role in creating a national plan to better prepare Canada's students for careers in the burgeoning technology sector.

ESAC, a lobby group for Canada's booming video game industry, said 1,400 video game-related jobs will be available over the next 12 to 24 months and the industry cannot find Canadian talent to fill those high- paying positions.

In 2015, the average salary of a worker in Canada's video game industry was $71,300.

The ICTC argues far more needs to be done to encourage youth to pursue careers in information technology-related fields, including exposing more minorities, disabled people and females to studies involving information and communications technologies and introducing children to computer science and coding as early as the age of five.

ICTC is calling on the federal government to make computer science mandatory for children, beginning in kindergarten. Recent studies suggest students are less likely to continue in computer and science courses as they age, so introducing them to these courses earlier and continuing them throughout elementary and secondary schools as part of a regular curriculum could help maintain interest in more students.

The idea isn't radical. In September 2014, the United Kingdom introduced changes to its national education curriculum to incorporate computer science into all education programs for children, starting with students as young as five years old.

In subsequent polls to monitor the initiative, more than 85 per cent of teachers have reported students have responded positively and are showing more interest in subjects that include coding and information technologies.

Wall Street Journal
Internet Providers Face Privacy Fight
Thursday, 10 March 2016
Byline: John D. McKinnon

Washington - Federal Communications Commission officials soon will seek to impose new customer-privacy rules on Internet access providers, a move expected to fuel an already fierce conflict with the industry.
The new rules, which could be brought up at an FCC meeting as soon as this month are intended to help shield tens of millions of consumers from potentially unwanted use of their Internet data by the providers, many of whom are looking to boost profits by using customer data to sell more targeted advertising online.

The Internet access companies -- which include cable and wireless firms -- are digging in for a regulatory fight, arguing that tough new FCC rules could put them at a disadvantage, particularly against Internet-services firms such as Alphabet Inc.'s Google unit or Facebook Inc. that wouldn't be covered by the new FCC rules.

Until recently, online privacy has largely been the domain of the Federal Trade Commission, another independent regulatory agency which has a long track record in privacy enforcement but which some privacy advocates believe is hamstrung by limited legal authority.

Google and Facebook -- which also use customer data -- are regulated by the FTC.

The fast-growing digital advertising market is worth tens of billions of dollars each year, and the ability to use customers' data can give telecommunications firms an important edge. That makes the FCC's effort to impose new restrictions on data a potentially high-stakes battle for Internet service providers.

It is also fueling a long-running conflict between FCC Chairman Tom Wheeler and the providers, who have sparred recently over net-neutrality rules as well as the agency's efforts to open up the market for pay-TV set-top boxes.

Mr. Wheeler is hoping to put the new privacy rules up for a preliminary vote at this month's commission meeting. He is expected to announce his plans as soon as Thursday.

On one level the new rules likely will be mundane stuff. They are expected to require the companies to explain more clearly to customers how their data would be handled.

The rules are likely to give customers more ability to opt-in or opt-out of various data uses, depending on the specific types of data involved. And they will lay down new standards for keeping data secure from breaches.

Still, they are expected to spark a contentious industry battle. Some advocates worry the FCC move could open the door to more onerous regulation of telecommunications firms' practices than they have previously experienced under the FTC.

"Despite objections and concerns I have about the FTC, which are significant, it's still a far saner regime" than the new FCC system is likely to be, said Berin Szoka, president of TechFreedom, a market-oriented think tank. That is partly because of the FCC's sweeping powers to classify practices as improper under the law.

But many privacy advocates believe FCC regulation would be an improvement. They regard the FTC as somewhat hamstrung when it comes to protecting privacy, for example because of its limited ability to impose fines on offending companies.

Privacy advocates also say telecommunications firms have access to so much data -- even more than Google or Facebook -- that they ought to be regulated differently.

"The larger and deeper the data set, the more able I am to target you personally," said Harold Feld, a senior vice president at Public Knowledge, a consumer group.

Reuters
Senators close to finishing encryption penalties legislation: sources
Thursday, 10 March 2016

Washington - Technology companies could face civil penalties for refusing to comply with court orders to help investigators access encrypted data under draft legislation nearing completion in the U.S. Senate, sources familiar with continuing discussions told Reuters on Wednesday.
The long- awaited legislation from Senators Richard Burr and Dianne Feinstein, the top Republican and Democrat on the Senate Intelligence Committee, may be introduced as soon as next week, one of the sources said.

It would expose companies like Apple Inc, which is fighting a magistrate judge's order to unlock an iPhone connected to the mass-shooting in San Bernardino, California, to contempt of court proceedings and related penalties, the source said.

Senators are expected to circulate the draft bill among interested parties next week and hope to introduce it soon after, though a timetable is not final, the source said.

The Senators' proposal would not seek criminal penalties, as some media reports have stated, the sources said.

The controversial proposal faces an uphill climb in a gridlocked Congress during an election year and would likely be opposed by Silicon Valley.

Tech companies have largely supported Apple in its legal fight against the Justice Department, which is seeking access to a phone used by Rizwan Farook, one of two shooters in the San Bernardino attack last December in which 14 were killed and 22 wounded.

It is particularly unlikely the proposal will gain traction in the U.S. House of Representatives, which staked out positions strongly supporting digital privacy in the wake of revelations about government-sanctioned surveillance of communications by former National Security Agency contractor Edward Snowden.

Last year, amid stiff private sector opposition, the White House backed away from pushing for legislation to require U.S. technology firms to provide investigators with mechanisms to overcome encryption protections.

But the issue found renewed life after the shootings in San Bernardino and Paris. An August email from Robert Litt, the top U.S. intelligence community lawyer, obtained by the Washington Post, noted that momentum on the issue "could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."

Separately, Democratic Senator Mark Warner and Republican Representative Michael McCaul last week introduced legislation to create a national commission to further explore solutions to the so-called "going dark" problem, where strong encryption has made it more difficult for law enforcement to access communications belonging to criminal suspects.

Sputnik (Russia)
Russia Main Threat to EU, NATO Cyber Security - Estonian Intelligence
Wednesday, 09 March 2016

Tallinn - Russia poses a major cyber security threat to the European Union and NATO, a report by the Estonian Information Board, released on Wednesday, said.
"In cyberspace, Russia is the source of the greatest threat to Estonia, the European Union and NATO. Estonia is a target of hostile cyber acts both as an individual country, and as a member of the EU and NATO. Russia is actively adding to its cyber-attack capacity and has a wide range of tools and resources necessary for carrying out attacks," the report, titled "International Security and Estonia," said.

The Information Board, which is Estonia's foreign security service and intelligence agency, alleged that Russia employs attacks involving denial-of-service, malware and security vulnerabilities to wage an information war against the European Union and NATO. Russia employs hackers and cyber activists to manipulate social media, the press and thus public opinion to enforce its geopolitical power, the report said.

The report also alleged Russian to be waging a "hybrid war" in Ukraine, disrupting information and other infrastructure to ferment dissatisfaction with the government and legitimize anti-government militia groups.

The report comes just a day after a meeting between US Secretary of State John Kerry and Estonian Foreign Minister Marina Kaljurand. The meeting focused on the situation in Ukraine and current European security issues, as well as the upcoming NATO summit in Warsaw, the situation in Syria, energy and cyber security, according to Kaljurand.

Since 2014, NATO has been building up its military presence in Europe, particularly in eastern European countries bordering Russia, including Estonia, using Moscow's alleged interference in Ukraine as a pretext for the move.

Russia has repeatedly expressed concerns over NATO's military buildup along its western borders, warning that the alliance's expansion undermines regional and global security.

Ottawa Citizen
Computer virus strikes hospital
Monday, 14 March 2016
Byline: Vito Pilieci

The Ottawa Hospital has confirmed that four computers in its network of 9,800 were hit with ransomware last week, encrypting the information on those machines and making it inaccessible to hospital administrators. "No patient information was affected. The malware locked down the files and the hospital responded by wiping the drives," said Kate Eggins, a spokeswoman for the hospital. "We are confident we have appropriate safeguards in place to protect patient information and continue to look for ways to increase security. We would like to reiterate that no patient information was obtained through the attempt."
The hospital wouldn't divulge what was on the machines that were infected. However, Eggins said the computers were wiped clean of the infection and the information on the computers was restored through the use of backup copies of the data.

The infection on hospital systems comes at a time when ransomware is surging to a fever pitch, attacking personal home computers and businesses alike. Ransomware, which is a virus and not an attempt to hack a computer system, starts by tricking a computer user to install malicious software on a personal or work computer.

The dangerous software usually comes in the form of a spam email, which is being sent in the form of an invoice, a website or video.

When the computer user opens the attachment, the software then gets to work encrypting all the data on the user's computer. By encrypting the data, it locks out the user, making the data inaccessible to the computer user. To regain access to the files on the computer, the user is told to pay a ransom. The ransom is usually requested in Bitcoin, which cannot be traced. However, there is no guarantee that paying the ransom will see the machine unlocked.

The Ottawa Hospital is the second hospital to report being hit by ransomware in recent weeks. Last month, Hollywood Presbyterian Medical Centre in Los Angeles was hit by a widespread infection of ransomware that locked down a vast majority of computers and computer systems in the hospital, significantly impacting its ability to operate. The hospital was forced to pay a ransom of US$17,000 in Bitcoin.

Computer security researcher McAfee has named ransomware as one of the biggest security threats of 2016. It's one that will affect consumers and businesses equally, as the criminals behind the malicious software don't care who the virus infects as long as people are paying ransoms. According to the researcher, more than four million samples of ransomware were floating around on the Internet last year, and more than 1.2 million of those samples were new.

It should be mentioned that with last week's discovery of ransomware targeting people running Apple computers, criminals have spread their nets as wide as possible in a bid to catch as many people as possible.

In recent days, a new version of ransomware, named "Locky" by researchers, has hit a fever pitch online. According to security researcher Trustwave, as many as four million spam emails containing Locky ransomware have been detected in the past seven days alone. The researcher said the emails containing Locky just started to be sent in the past month, and that last week as many as 200,000 per hour were being detected by Trustwave's Spam Research Database.

Eggins could not confirm it was Locky that hit The Ottawa Hospital's computers.

Mark Nunnikhoven, vice-president of cloud research at computer security firm Trend Micro, said ransomware is a serious threat of which consumers and businesses need to be aware.

"It's quickly becoming the 'goto' move for cyber-criminals. The reason why ransomware is increasingly in prevalence is because it's extremely profitable for the criminals. This is a low-effort, highreturn campaign."

Nunnikoven said Locky is something that people need to be concerned about. He said he received three emails on Sunday alone that were attempting to get him to install Locky on his home computer. By locking down a person's home computer using ransomware, any photos, videos, contact information or important financial documents that may be saved to that hard drive could be lost forever.

Consumers and businesses are being reminded by computer security professionals to avoid opening any email attachments that are unsolicited. If an unexpected email does arrive with an attachment, contact the sender to verify that they actually intended to send the message. Back up all important data to an external hard drive or online cloud computing service, and ensure that anti- virus programs are kept up to date.

Globe and Mail
RCMP fight to keep lid on high-tech investigation tool
Monday, 14 March 2016

Police in Canada are fighting to keep secret the specifics of advanced technology they've used to spy on mobile phones in a criminal investigation into organized crime.
Court documents filed in the Quebec Court of Appeal show government lawyers have acknowledged that the RCMP used an extraordinary communications-interception technique involving "mobile device identifier" equipment.

But the Crown will be fighting to keep details of the operation under wraps during a court hearing scheduled for March 30 in Montreal.

Chris Parsons, a researcher with the Citizen Lab at the University of Toronto's Munk School, said this case "wouldn't be the first time [these devices] have been used - but it would be the first time [authorities] have been caught out in court."

The public is bound to want to know more, Mr. Parsons said. "These are fundamentally devices of mass surveillance," he said.

"Authorities using them will also be collecting information about law-abiding Canadians."

Between 2010 and 2012, detectives in RCMP "Project Clemenza" used a high-tech device to eavesdrop on a group of reputed mafia members who were sending each other encrypted messages on BlackBerry phones. Police believed the suspects were out to settle scores during the power vacuum that had emerged after the jailing of mob boss Vito Rizzuto.

On Nov. 24, 2011, a New Yorker named Salvatore (Sal the Ironworker) Montagna was shot dead on the outskirts of Montreal. Fearing more bloodletting was imminent, an RCMP-led team divulged its ongoing operation to local police, so they could make arrests in that gangland slaying.

Defence lawyers suggest the machinery the RCMP used in the case works by mimicking a cellphone tower and can trick all mobile phones within a specific radius into giving up data to police.

That would make this equipment similar to dragnet devices - known as "Stingrays," "cell-site simulators" or "IMSI catchers"- that have become ubiquitous and controversial in the United States. The New York Police Department, for example, was recently forced to release documents showing it had secretly used similar tracking technology more than 1,000 times since 2008.

The Mounties will not comment about their investigative techniques. "Seeing that this matter is still before the courts, it would be inappropriate for the RCMP to comment," said Sergeant Harold Pfleiderer.

The Mounties' use of the equipment is documented - in broad strokes - in a Crown brief sent to the appeal court in December, as part of the organized-crime case.

Nearly five years after the murder, most of the seven accused conspirators in the murder still await trial, as lawyers and prosecutors argue how much of the RCMP's techniques should be disclosed to the defence.

Last November, Quebec Superior Court Judge Michael Stober ordered the Crown to acknowledge its use of RCMP "mobile device identifier" (MDI) technology, and added that the accused are entitled to know details about it.

Crown lawyers immediately appealed. "The information sought would tend to identify the RCMP's methods and give a way to circumvent them," says the Dec. 14 appeal brief. Arguing that the technology is shielded by "police investigative techniques privilege," the brief says any disclosure will "hinder the RCMP's capabilities to lead criminal investigations."

The filing shows the Crown is resisting the defence's bid for the "manufacturer, make, model" of the device in question, as well as its "practical range." The defence wants "confirmation the device is a cell-site simulator" and, also, to know whether federal authorities have studied the privacy, safety and technical impact of such surveillance.

The filings do not make clear how powerful the RCMP equipment was.

Some such devices can intercept voice conversations or text messages. Others merely collect what is known as "metadata" - or information relating to phone numbers, SIM cards, or handset identifiers - on all phones that show up in a given radius.

The Crown brief suggests the RCMP used the technique to lay the legal groundwork for warrants that could facilitate lawful eavesdropping against suspects who were proving hard to track.

The crux of the alleged murder-conspiracy centres on a circle of eight suspected mobsters, one of whom is now dead. Some were known to police at the time only by the aliases they used on their phones, such as "Gateau," "Aaaaaaacounts," "Shadow," and "JJ."

The brief says the Mounties used their device as a targeting method to figure out which specific BlackBerrys to target. "The fruits of the MDI were sometimes used as grounds to connect [BlackBerry] PIN numbers pursuant to ... wiretap authorizations," the filing says.

There is no mention of verbal or typed conversations being collected by this equipment. The prosecution "will not use the MDI in its case," the brief says.

RCMP Project Clemenza has made headlines before, after the Mounties revealed they had figured out how to snoop on BlackBerry's supposedly secure messaging system. In 2014, the police force issued a press release claiming it had intercepted and read more than a million such messages as part of the wider investigation.

Now, defence lawyers are asking for details as to how exactly the Waterloo-based company may have helped police do that. Or, failing that, "how the RCMP came into possession of the BlackBerry global encryption key."

But this disclosure, too, has been resisted by the Crown.

Le Devoir
Éradiquer Facebook pour sauver la démocratie
Monday, 14 March 2016
Byline: Fabien Deglise

Québec - Richard Stallman, le père des logiciels libres, appelle les citoyens à reprendre le contrôle de leur vie
Pour le fondateur du mouvement du logiciel libre, Richard Stallman, impossible de vivre libre dans des environnements où la socialisation et où l'informatique sont assujetties à des entreprises privées qui balisent les activités humaines avec des logiciels privateurs ou avec des services dont les codes et leurs intentions sont gardés secrets.

L'homme, de passage au Québec cette semaine, où il a été invité par l'Université Laval et par le Collège Dawson à parler de liberté numérique et de logiciel libre, demande d'ailleurs aux gouvernements et aux citoyens de prendre conscience des injustices qui accompagnent ces nombreuses soumissions et appelle même au démantèlement du réseau Facebook, pour sauver la démocratie.

" Il faut éliminer Facebook pour protéger la vie privée", a lancé en entrevue au Devoir le célèbre programmeur américain, président-fondateur de la Free Software Foundation et militant de longue date pour une informatique libre et ouverte. L'homme est, par exemple à l'origine du système d'exploitation GNU/Linux qui, depuis des années, fait la nique aux systèmes informatiques privateurs développés par Apple ou Microsoft. Sans cette vie privée, sans la possibilité de communiquer et d'échanger sans être surveillé, la démocratie ne peut plus perdurer. " Pour M. Stallman, dans un monde où les communications sont surveillées, les possibilités de dénoncer les abus, de savoir ce que l'État fait diminuent forcément, avec à la clé une perte de contrôle du citoyen sur ce même État.

Utiliser ou se faire utiliser ?

Le réseau social numérique de Mark Zuckerberg " utilise bien plus ses usagers que ses usagers ne l'utilisent ", dit-il en boutade. " C'est un service parfaitement calculé pour extraire et pour amasser beaucoup de données sur la vie des gens. C'est un espace de contraintes qui profile et fiche les individus, qui entrave leur liberté, qui induit forcément une perte de contrôle sur les aspects de la vie quotidienne que l'on exprime à cet endroit. " Et selon lui, même si le plaisir d'utilisation accentue une certaine dépendance chez plusieurs utilisateurs, les conséquences sociales et politiques ne peuvent être que délétères à moyen ou long terme, surtout si le pouvoir de ce réseau se voit renforcé au fil du temps par les abonnés qui se multiplient en son sein.

" On le voit avec l'informatique privative [celle portée par les Apple et Microsoft de ce monde] qui, depuis des années, ne laisse aucune place à l'alternative de l'informatique libre, résume M. Stallman. Les entreprises qui soumettent les gens avec ces produits gagnent beaucoup d'argent, argent qu'elles utilisent pour amplifier l'inertie sociale qui bloque toutes les portes de sortie. "

Liberté sous surveillance

Et pourtant, une telle domination est néfaste pour les gouvernements assure-t-il. En laissant leurs administrations publiques se placer sous le joug d'entreprises, ils perdent de leur pouvoir tout en ne servant pas très bien les citoyens qu'ils représentent. " Une informatique publique dans l'intérêt du peuple n'est pas une informatique dont le contrôle est dans les mains d'entreprises privées qui cultivent le secret sur leurs codes informatiques, dit cet ancien du Massachusetts Institute of Technology (MIT) qui pourfend les brevets logiciels et la gestion des droits numériques. Le logiciel privateur surveille ses utilisateurs, décide de ce qu'il est possible de faire avec ou pas, contient des portes dérobées universelles qui permettent des changements à distance par le propriétaire, impose de la censure. Lorsqu'on l'utilise, on se place forcément sous l'emprise de la compagnie qui le vend. Avec ce pouvoir, le propriétaire est tenté d'imposer des fonctionnalités pour profiter des utilisateurs. On ne peut décider librement du code que l'on installe ou pas. On est donc forcément soumis et moins libre. "

À Québec mercredi, lors d'une conférence organisée par l'Institut Technologies de l'information et Sociétés (ITIS) de l'Université Laval, puis à Montréal jeudi, au Collège Dawson, l'homme va d'ailleurs réitérer les appels qu'il lance désormais aux quatre coins du globe à se défaire de ces chaînes numériques pour retrouver la liberté de créer, de partager, de construire des données, loin des contraintes imposées par les géants du numérique. " Les gouvernements ont un rôle important à jouer pour combattre ces injustices en s'échappant des cadres privateurs dans lesquels ils se sont placés, dit-il. Le système scolaire, aussi, doit apporter sa contribution en n'imposant plus la dépendance des élèves à des entités informatiques privées. Il ne devrait enseigner que le logiciel libre. C'est la seule façon de regagner collectivement la liberté perdue et de reprendre le contrôle sur des activités qui nous ont d'ores et déjà échappé ", conclut-il.

Toronto Star
Canada's master of messaging
Saturday, 12 March 2016
Byline: Patty Winsa

Ottawa - Ted Livingston, CEO of the billion-dollar tech company Kik, is sitting at a glass conference table in his Waterloo offices.
He's wearing the same thing he wears most days: a purple T-shirt that clashes with his strawberry blond hair, under a black hoodie.

And he's adamant about not posing for the camera, which has resulted in an online trail of unflattering photographs, many with his mouth open, taken while he's being interviewed.

But those quirks, which make it difficult to lay out a splashy magazine spread, may be the least interesting parts of Livingston.

The life of the Toronto native, only 28, has been entwined with some of the events that have defined the early 21st century - the rise and fall of Research In Motion, the release of the iPhone and the global banking crisis.

In that riptide Livingston managed to create Kik, a cross-platform messaging app originally for BlackBerry - where he once worked - that would connect BlackBerry users to iPhones and vice versa. The app exploded in popularity until the phone maker kicked it off its platform in 2010 and effectively shut it down.

(BlackBerry, which changed its name from Research In Motion in 2013, declined to comment for this story.)

"They disabled it," Livingston says matter-of-factly. "They completely destroyed it on BlackBerry even if you had already downloaded it.

"It was mean, not just to us, but to all those people. They all got this fastest-growing thing in human history," he says of the app, downloaded a million times in its first 15 days, "and then they took it away."

Kik "was written off for a year or two," says Blair Livingston, Ted's younger brother. Meanwhile, Ted remained in Waterloo, where he was a university student, and "formulated a plan to retake over the world."

"There are lots of examples in human history of a company or group of people who lose the battle but win the war," says Blair, the founder of a financial tech service.

Last year, Kik Interactive Inc. was valued at $1 billion (U.S.) after Tencent, the Chinese developer of messaging app WeChat, invested $50 million in return for a 5-per-cent stake, although that value is mostly on paper.

"We are making money now," says Ted Livingston. "For a long time we weren't. It was all focused on growing the user base." That base has reached 275 million, according to the Kik website.

The company says it's used by 40 per cent of teens and young adults in the U.S. Livingston speculates it caught on because it could be used on Wi-Fi with no phone number, appealing to kids with an iPod Touch or a parent's old iPhone. But that feature is being criticized for allowing people to sign up and connect to friends and strangers with a user name and personal information that may not be real.

Last month, two suspects, freshmen at Virginia Tech, were charged in the murder of Nicole Lovell, a 13-year-old cancer survivor who told friends she met the male suspect on Kik.

There have been a number of other high-profile cases, including one in November, when a 15-year-old girl from Cleveland was abducted and raped by a man she met on Kik, police allege. Police found her only after the 41-year- old man posed as the teen on Facebook.

Spokesman Rod McLeod says the company helped police identify the suspects in the Virginia case and that it shuts down accounts that are misused. He doesn't believe Kik "is used for nefarious purposes more or less than similar communications services."

"Kik co-operates with law enforcement to combat child predators anywhere in the world, either upon provision of a court order, or in emergency situations such as this one," wrote McLeod in an email.

Whether Kik and other social media sites are putting kids at risk is hard to quantify, says David Finkelhor, director of the Crimes Against Children Research Center in the U.S.

Police may report that more crimes are occurring because of a certain social media platform, he says - but does that mean the platform itself is riskier or just that it's a new medium where more people are interacting with each other?

"The argument from law enforcement has been that the anonymity that is particular to the Kik type of approach is more facilitative for these kinds of crimes. That may or may not be the case," says Finkelhor, noting that kids face much higher risk of sexual assault from people they know.

Meanwhile, messaging apps continue to grow in popularity. By 2018, it's expected nearly 80 per cent of smartphone owners - about two billion people - will have used one, according to online site eMarketer.

One of the most advanced is China's WeChat. People can chat with friends or computerized "chatbots" that can be used to market companies' products.

The race is on in the West to create a similar mobile messaging platform, where users don't have to leave the app to say, order a cab, send money to a friend or buy a shirt. There are rumours Facebook's Messenger app could introduce the technology in April.

Kik is an early adopter: users can connect to clothing lines and movie tickets, as well as their friends.

"I have a Kik user name," says Livingston. "I just ask you, 'What's your Kik?' That's what all these teenagers are doing."

Living in our smartphone world

before anybody else

When Livingston was young, all he wanted to do was build robots.

As a child in North York, he had a passion for building, anything from Lego to K'NEX, or battling with automated machines called Sumobots in his basement. He started making robots in high school.

Livingston lived with his three brothers and his parents - Bob Livingston, a financial adviser on Bay Street, and Laurel Hobbs, who met her husband while at York's MBA program, worked in advertising and later stayed home with the kids.

His older brother, Michael, 31, is a doctor. Blair, 26, runs Street Contxt, a cloud-based financial information service. Michael, Ted and Blair were educated at Toronto's prestigious private school Crescent. His youngest brother, Jack, born with severe cerebral palsy, died three years ago at 19.

The siblings' privileged upbringing - weekends skiing at a private club in Collingwood, summers at a cottage in Muskoka - never gave the older kids a sense of entitlement.

"There's an idea that people play out their lives. And if you worked hard, you're successful. You deserved that," says Livingston. "But for my brothers and I, we look at Jack and we're like, 'Well, he worked hard and he deserved it. But he didn't get anything.' It's hard for us to reconcile those two things."

After high school, Livingston pursued his dream of building robots and enrolled at the University of Waterloo in mechatronics, a co-op program that teaches students how to build computer-controlled electromechanical systems.

"The funny thing is I get to Waterloo in 2005 and I never get to build robots," says Livingston, who almost dropped out. "The big scam of engineering is you never get to build things. You just do a lot of math."

He alternated four months of school with four months of co-op work, first at Honda and then with the city of Toronto, where he painstakingly measured thousands of feet of sod and curb to determine what to pay contractors. He tried to introduce some time-saving changes.

"Eventually my boss pulled me aside," Livingston recalls. "He said, 'Ted, the government is like a train. It's on its set of rails. And unless it's going to crash, it's just going to keep going that way.'"

After that, the Waterloo student was determined to get a better placement and landed at BlackBerry.

"I felt like we were going to change the world. It was amazing to be there," he says. "It was a huge source of inspiration, even to this day, that something that big was built right here."

He lived in a social circle of interns who were connected day and night because they all had free BlackBerrys and full data plans at a time when Livingston says only bankers on Wall Street could afford them.

"That to me is a huge opportunity BlackBerry gave to me," he says, "letting me live in this world before anybody else."

But he turned down a full-time job after a couple of co-op terms and went back to school at Velocity, Waterloo's incubator program for entrepreneurs. He started building the app with a group of students including co-founder Chris Best, who is now Kik's chief technology officer.

When the next co-op term came up, what Livingston wanted most was a job with a global consulting firm, but two of the three biggest cancelled their programs in the wake of the global financial crisis.

With only one firm hiring in Canada, Livingston didn't make the cut.

"And because I didn't get that, I thought, 'Oh, I might as well keep working on this Kik thing.'"

Not ready to cash in on 'the gold rush'

Ted Livingston started the company with a $25,000 inheritance from his grandfather and money he saved from co-op jobs.

"There were no salaries," says Livingston. "Of course we're not going to pay each other," he says of his partner, Chris Best.

"This is basically a school project. Money went to pay for computers, a server, all the operational costs of things we couldn't afford.

"We'd go out to celebrate things when we launched them and pay for the pizza and beer."

The first private investors were a group of Toronto doctors and lawyers who planned to give a total of $50,000, but threw in three times that after meeting Livingston. When investments reached $1 million, the company started hiring people in Waterloo and paying them salaries.

"The way these companies work is you take a bunch of money, you burn it and you hope the ashes are worth something," says Livingston.

"That's the name of the game and why Canada is not good at consumer startups - because it's high, high risk. It's why Silicon Valley is very good at it. You have to be a little bit irrational to get into it."

High-risk or not, Kik has now been bankrolled for $120 million (U.S.). And many of those private investors must be eagerly anticipating the takeover bid or the IPO that could make them all rich, or richer.

One of them is legendary U.S. venture capitalist Fred Wilson, who went from broke to multimillionaire in one week after his investment in GeoCities paid off with a sale to Yahoo in 1999.

Wilson lost it all when the dot-com boom went bust soon after, but his company - Union Square Ventures - has since rolled the dice on startups like Tumblr, which was founded in 2007 and sold to Yahoo for $1.1 billion in 2013, as well as Twitter, Kickstarter and Foursquare, to name just a few.

This time it could be a long wait.

"If you're a minority shareholder in a company that is controlled by a founder with a long-term vision," says Wilson of Kik, "you might be in it for 20 years."

Livingston confirmed last year that his company had hired a San Francisco investment bank to explore options to partner or sell. But Kik remained independent and instead took a $50-million investment from Tencent, aligning itself with a Chinese company that has pioneered the chat platform.

"If it was up to me, we would never sell the company," says Livingston, although he is keenly aware his employees, all part-owners, could pay off mortgages with the profits. (To that end, the company let employees sell 5 per cent of their shares to a private investor a year and a half ago.)

Livingston, who is married to Christine Thayer, a product manager at Kik, would rather build the company into something "huge."

He says Kik is at the frontier of a technology that could be the biggest thing since the invention of the smartphone - building an app into a platform as powerful as Tencent's WeChat.

WeChat, which has been around for six years, has 650 million monthly active users.

The messaging app also has five million automated bots, pieces of software that users can "chat with like a friend to do things that deliver value," says Livingston. Scan one of Tencent's proprietary codes - similar to QR codes - and you can have a chat with a vending machine that will give you a Coke. Start a conversation with another bot and buy a shirt.

"Everybody realizes this ability for chat apps to be a new platform with bots," says Livingston.

In the West, competition is heating up. WhatsApp messenger, which Facebook purchased in 2014 for $19 billion in cash and stock, according to Forbes, reportedly hit a billion users in February, surpassing Facebook's own Messenger app.

"Messaging is the primary way people use their phones," says Wilson. "If they can, from that same text input line, order lunch or get a car to take them to the airport or do a search query or find out when the movie they want to go see is playing and get tickets, people are going to do that."

Livingston sees it as the next "gold rush in technology." But he's not ready to cash in just yet. He's turned down purchase offers, and when he did have a million dollars - he sold some of his own shares to give an investor a bigger cut - he gave it away.

"We just got kicked off BlackBerry," recalls Livingston. "Growth is back down to zero. Everybody's demoralized. And here's Ted with a million-dollar golden parachute. So I took the parachute and threw it out the window."

Livingston, who was 23 at the time, donated the money to Velocity, the Waterloo incubator, to fund two $25,000 startups a year.

That same reasoning and desire for modesty make it easy for him to say no to a couple of portrait photographs, which he believes would set him apart.

"He appreciates the fact that it's not just him building Kik," says Blair. "It takes a team to build a product.

"And I think this superhero CEO thing is a little bit overplayed."

Toronto Star
Lift the veil of secrecy
Saturday, 12 March 2016

Agency who have died in custody since 2000.
It's a disturbing total, and it's made worse by the fact that their names, the circumstances of their deaths and why they were being detained are kept secret by the agency. It's as if they didn't exist.

This should not be allowed in a supposedly open, accountable, caring democracy.

So it's no surprise that the announcement of the most recent death has led to yet another round of calls by human rights advocates for more transparency within the agency, the creation of an oversight body to hold it to account and the establishment of an outside body to investigate deaths in custody.

That's the least the federal government should do.

Human rights organizations are also urging the government not to hold immigration detainees in maximum security prisons, but in immigration holding cells, and for an end to indefinite detention.

And as the Star has previously argued, the agency should act on recommendations from a study it commissioned and release some detainees into the community, where they can be monitored electronically.

The five human rights organizations, including the B.C. Civil Liberties Association and Amnesty International, are not alone in their call for more openness and accountability. Last year, a report issued by the Senate national security committee called for establishment of a civilian watchdog over the agency to ensure transparency and avoid any abuse of power.

But still the agency operates in secrecy. All it said in a March 7 announcement about the most recent death was that it had been notified by the Ontario Ministry of Community Safety and Correctional Services that an individual under immigration detention at the Toronto East Detention Centre had passed away. It did not release his name or the cause of death.

It took an investigation by the Star's Debra Black to find out that the man who died was Melkioro Gahungu, who hanged himself as he awaited deportation to Burundi. He had been in prison after killing his wife in 2009.

Gahungu's death brings to mind that of Lucia Vega Jimenez. When the 41-year-old Mexican migrant hanged herself from a shower stall in an immigration holding centre at Vancouver airport in 2013, the agency did not initially even issue a bulletin of any kind.

Border agency officials hide behind the federal Privacy Act when pressed for details. But correctional officials can make public the names of people who die in their care and the details of their deaths. The Privacy Act should also be lifted for immigration detainees.

And immigration and refugee detainees should not be held at maximum security jails, where nearly one-third languish behind razor-wire fences with the worst offenders because immigration detention centres are already full.

We are not talking about a handful of people. At any given time about 600 immigrants and refugees are in detention, with some 10 per cent held for more than a year. Indeed, in 2014, five detainees had been held for five years or more.

As Star columnist Desmond Cole noted this week, the United Nations has said Canada's practice of indefinite detention amounts to cruel and unusual punishment of migrants.

But the bottom line, as Mitch Goldberg, of the Canadian Association of Refugee Lawyers, notes, is this: "Nobody should die while they are in the custody of the CBSA."

He is right. The Trudeau government should act on these sensible recommendations, starting with independent oversight of the agency, before yet another detainee dies.

New York Times
Obama Calls for Law Enforcement Access in Encryption Fight
Saturday, 12 March 2016
Byline: Michael D Shear

Astin, Tex - President Obama said Friday that law enforcement must be legally able to collect information from smartphones and other electronic devices, making clear, despite disagreement within his administration, that he opposes the stance on encryption taken by technology companies like Apple. Speaking to an audience of about 2,100 technology executives and enthusiasts at the South by Southwest festival here, Mr. Obama delivered his most extensive comments on an issue that has split the technology community and pitted law enforcement against other national security agencies. Mr. Obama declined to comment specifically on the efforts by the F.B.I. to require Apple's help in gaining data from an iPhone used by one of the terrorists in the December attack in San Bernardino, Calif.

But the president warned that America had already accepted that law enforcement can "rifle through your underwear" in searches for those suspected of preying on children, and he said there was no reason that a person's digital information should be treated differently.

"If, technologically, it is possible to make an impenetrable device or system, where the encryption is so strong that there is no key, there is no door at all, then how do we apprehend the child pornographer?" Mr. Obama said. "How do we disrupt a terrorist plot?"

If the government has no way into a smartphone, he added, "then everyone is walking around with a Swiss bank account in your pocket."

Mr. Obama's decision to embrace the law enforcement position on encryption represents a fundamental break with a tech community that has strongly supported his political career. For years, the president nurtured close ties to Silicon Valley, tapping the youthful talent there to help him reshape the federal government's aging technology infrastructure and seeking out leading executives for private advice and millions in campaign cash.

That partnership was in part a result of a philosophical affinity between Mr. Obama and technology executives that included broad agreement about gay rights, immigration, civil liberties and health care. Mr. Obama has repeatedly said he remains a fierce defender of civil liberties, including the right to privacy.

Within the administration, there is a division over encryption between the F.B.I., along with other law enforcement agencies, which says it must have a way of breaking into encrypted devices, and the intelligence community, which worries that the same techniques could be used against the American government. In his comments, which were greeted with polite silence, Mr. Obama said he, too, supported the development of strong encryption to make sure that the government can protect banks and critical infrastructure. And he said he wanted proper oversight of law enforcement. But, he said, technology executives who are "absolutist" on the issue are just wrong.

"This notion that somehow our data is different and can be walled off from those other trade-offs we make, I believe, is incorrect," he said.

Mr. Obama spoke broadly at the music, film and technology festival about the need for technology to be used to support civic life and the functioning of democracy.

He became the first sitting president to visit the festival, which in the past three decades has become a mecca for the high-tech, social-media set. He made his comments during an hourlong conversation with Evan Smith, the editor in chief of The Texas Tribune.

At the festival, the president sought to make the case that the technologies behind today's entertainment and communication apps should also be directed at solving the problems of voter turnout, access to information and civic engagement. "We want to create a pipeline where there is a continuous flow of talent that is helping to shape the government," he told the audience.

Mr. Obama is something of a technology geek, so his presence at the festival does not come as much of a surprise. He enjoys dinners with technology moguls and has tapped the wealth of Silicon Valley for his two presidential campaigns.

He has talked to his closest advisers about creating a high-tech presidential center when he leaves office, in part to help visitors engage with his legacy and in part to encourage better use of technology in society.

He has also sought to lure more tech executives and engineers to government to make federal agencies more responsive to their customers. Mr. Obama created the United States Digital Service as a kind of troubleshooting team to upgrade the technology associated with government services, and he has filled its staff largely with veterans of Google, Microsoft and other such companies.

"The work they're doing is impactful -- and it's hard to see how they don't become a permanent feature of our government," Jason Goldman, the chief digital officer for the White House, said in an article posted on the Medium website on Thursday. "Indeed, this might be President Obama's most important accomplishment as the First Tech President: establishing a lasting legacy of service that will carry on long after he leaves office."

Still, questions about how to harness the power of Twitter, Facebook and Snapchat to help government are not always clear, especially when the companies involved are, above all, designed to make money for their shareholders.

This spring, the White House will host what it is calling a summit meeting on civic engagement, and aides said the president would use it to continue the conversation about the role that technology could play.

Follow The New York Times's politics and Washington coverage on Facebook and Twitter , and sign up for the First Draft politics newsletter .

Xinhua News Agency
China concludes 6,221 criminal cases involving cyber
Sunday, 13 March 2016

Beijing - China in 2015 concluded 6,221 criminal cases using cyber for fraud, crimes of provoking troubles or other crimes, a work report of the Supreme People's Court (SPC) said Sunday.
In the work report to be delivered by Chief Justice Zhou Qiang to the annual session of the national legislature, the SPC said it cracked down upon cyber crimes such as rumormongering, gambling and disseminating pornography in a bid to clean up the online environment.

It also fought in accordance with law against online crimes involving leaking private information and illegally trading information, for better safeguarding information security of individuals.

A work report of the Supreme People's Procuratorate (SPP), which was also released Sunday and to be delivered by Procurator-General Cao Jianming to the national legislature, said it actively took part in fighting new-type crimes involving telecommunications and the Internet, especially fraud through telephone, text message and the Internet.

Haaretz
Israeli Businesses Learning to Insure Themselves Against Cyber Attacks
Monday, 14 March 2016
Byline: Assa Sasson

Jerusalem - When Bank of Jerusalem discovered its database of securities accounts had been hacked, the task of investigating what happened and assessing the damage wasn't just a job for the bank and law enforcement authorities. Bank of Jerusalem's insurance company, AIG Israel, took an active part, too.

Policies against cyber attacks are an up-and-coming business in the insurance industry in Israel and worldwide, where high- profile hacking attacks heightened awareness of the problem both by businesses and their customers. Premiums for cyber coverage run about $2.5 billion to $3 billion a year but by 2020 they could reach as much as $10 billion, according to one estimate, with the market growing by 32% a year.

"The moment a business keeps personal data on its customers, like credit card numbers or their identity numbers, it's at risk of a cyber attack," said Elad Shelef, deputy CEO of Menorah Insurance. "One of the things we've seen is that hackers don't attack credit card companies directly. It's more complicated and very troublesome. They prefer to attack weaker links in the chain, which is to say businesses that keep customer records, so they are more exposed than they think."

In Israel, the market is just getting started. AIG worldwide is one of the biggest underwriters of cyber insurance and its Israeli unit has been active for some time. Menora began offering cyber protection in 2014 as an add-on to its business policies and today counts 1,000 policyholders, most of them small and medium-sized businesses.

Unlike most insurance, cyber policies involve the insurance company long before the first attack occurs. Insuring against cyber damage is complicated and involves assessing a lot more than the direct and immediate damage from an attack.

At the underwriting stage, an insurer will examine the client's risk for an attack, what defenses it has already set up and policies for things like changing passwords. Insurers know they can't prevent an attack, but they will do what they can to reduce the risk.

The most critical stage is immediately after an attack has been detected, said Shai Feldman, CEO of AIG Israel.

"When an attack occurrs the first 24-72 hours afterwards are the most important. It's an emergency in which many specialists have to be brought in to understand what happened and to undertake operative decisions," he said.

On the technology side, the company that's been attacked must be able to restore operations as quickly as possible, Feldman said. On the legal side, it has to report to law enforcement authorities and regulators. And then there is the marketing aspect. "For instance, what do you say to the media, how to do you tell customers ... It's like operating a war room," he said.

Finally, the insurer has to assess the damage, which is complicated by the fact that the damage can often go beyond lost work days or downed production lines, both of which can be sized up relatively easily. Damage to a company's reputation can be harder to quantify.

In the case of Bank of Jerusalem, the bank was relatively lucky. The hackers, who were apparently affiliated with the global hacking group Anonymous, stole information but weren't able to manipulate accounts by making trades or altering information. Only 6,000 of the 38,000 accounts were current clients of the bank.

Banks, in fact, are the biggest customers of cyber insurance, in large part due to regulatory requirements. Cyber insurance is less prevalent among other businesses. "It's a complicated risk for a business. For example, something like fire insurance is clear. Everyone understands how it works. By contrast, cyber insurance is more amorphous, so a business [owner] tends to think, 'it won't happen to me,'" said Shelef.

Gulf Daily News
Bahrain facing cyber threats warns expert
Monday, 14 March 2016
Byline: Sandeep Singh Grewal

Manama - It is just a matter of time before Bahrain is the target of a major cyber attack, a leading security expert has warned.
Computer hackers from Iran and China have been targeting several organisations and government entities in the region for years, said independent consultant Tom Lockhart.

"Bahrain has not faced any major cyber attack such as the one in 2012 on Saudi Aramco but eventually it will happen," Mr Lockhart told the GDN.

In a matter of hours 35,000 computers at Aramco were partially wiped or totally destroyed, in a cyber attack dubbed "the world's biggest hack in history".

Bahrain, along with Kuwait and Saudi Arabia, are prime targets for Iranian hackers seeking to disrupt business and steal classified data, said Mr Lockhart, who provides consultancy to independent British specialist security and risk management firm Le Beck International in Bahrain.

The hackers are targeting websites on a daily basis in order to infiltrate servers to get hold of valuable data. Investment in new technologies is needed to combat emerging new threats, said Mr Lockhart.

"Hackers from Iran and China have targeted several organisations and government departments in the region and internationally for different reasons and these hackers are both skilled and capable of achieving their goal.

"Bahrain, Kuwait and Saudi Arabia are the big targets for Iranian hackers and based on the patterns we have seen this is not something that will change in the near future.

"They are using multiple intrusion methods to discredit firms, disrupt systems and business activities which can have serious financial and strategic impact."

Cyber criminals with links to Iran were said to be responsible for hacking the Housing Ministry in 2011 and the GDN website.

Mr Lockhart said Bahrain is presently a relatively small target compared to Dubai, Abu Dhabi, Kuwait and Saudi Arabia, which are bigger financial hubs, but this did not mean that it is not under threat.

"The more businesses rely on technology to run their day-to-day activities, the more exposed and vulnerable they are to cyber attacks.

"Financial organisations, the stock exchange, energy sector and government systems, such as immigration and the Labour Market Regulatory Authority will be considered high-profile targets as they will have a significant impact on other sectors and thereby making the attack much more effective."

Mr Lockhart said if there is anything big happening in the country, then the chances of cyber attacks are high.

"We have the new UK naval base coming up and the annual Formula One race which all generates interest among cyber criminals who could target the logistics and organisational services."

Mr Lockhart, who works with several regional and international companies, urged IT professionals and security specialists in Bahrain to invest in new technologies to protect against cyber attacks.

More importantly, he stressed that these systems need continued and timely upgrading in order to address new threats before they can cause damage. "We have to be a step ahead of them, to identify vulnerabilities and prevent security breaches."

He was speaking to the GDN on the sidelines of an event organised by the Rotary Club of Adliya at the Diplomat Radisson Blu Hotel, Residence and Spa, where he gave a presentation on corporate and personal espionage. Terror groups such as the Islamic State are specialised in online warfare, he added.

The Central Informatics Organisation (CIO) officials have previously said that they have been capable of confronting any cyber attacks because of advanced training of its staff and the use of high-tech security programmes.

Officials in Bahrain said they found over one million malicious programmes and viruses that targeted government institutions in 2014 and hackers also targeted 10 government websites.

A government-wide Internet Security Study conducted for the CIO by Fresh Insight Associates last year showed that of the 83 million e-mails sent to the organisations, 75 per cent were spam and 0.09pc

contained viruses. It surveyed more than 20,000 people working in government ministries and authorities.

Data shows that 44pc of those surveyed opened attachments without knowing the sender and 5pc felt there was nothing wrong with opening such e-mails. The study also showed that 20pc of government staff shared their office passwords with one or more people, posing a major threat to security.

New York Times
China's Censors Denounced in Online Attack
Saturday, 12 March 2016
Byline: Chris Buckley

Beijing - China's formidable propaganda apparatus came under renewed attack on Friday, when a denunciation spread online in the name of an employee of Xinhua, the main state-run news agency. The letter accused censors of using tactics reminiscent of Maoist times to silence and smear critics.
The letter reflected a growing discontent among journalists, academics and even party insiders about the tighter censorship and about the giddy exultation of President Xi Jinping in state-run media.

"Under the crude rule of the Internet control authorities, online expression has been massively suppressed, and the public's freedom of expression has been violated to an extreme degree," said the letter, which spread quickly online in China and was taken down just as swiftly.

The letter was issued in the name of Zhou Fang, who gave his work address as Xinhua News Agency headquarters in Beijing, and included his cellphone number and identity card number. A man who answered the phone at that number said that he was Mr. Zhou, an employee of Xinhua, and that he had written the letter.

"I don't deny that," he said. He said that he had been an editor at the news agency and that he now held an administrative job. "I can't say anything more, because you're foreign media," he said.

The letter appeared after an uproar over Ren Zhiqiang, a blunt-speaking businessman, who was bitterly denounced by state-run media in recent weeks after he chided comments by Mr. Xi, who also serves as the Communist Party.

This week, Caixin, a prominent business magazine, issued an unusually candid denunciation of censorship, after one of its articles -- touching on censorship -- was taken down.

The new letter criticized the denunciations of Mr. Ren on party-run websites, which called him a traitor and a subversive for taking issue with Mr. Xi's demand that state-run media unfailingly obey the party.

"The recent Internet security incident of 'surrounding and attacking Ren Zhiqiang' in a kind of Cultural Revolution-style mass criticism brought the delinquency of responsibilities and abuses of power by the Internet authorities to an extreme," said the letter, which was dated Monday but spread widely only on Friday.

"This has triggered tremendous fear and outrage among the public," the letter said. People, it said, have begun to "worry about another Cultural Revolution."

An administrator at Xinhua said it did have an employee named Zhou Fang. But the administrator said she had not heard of the letter and declined to check the personal details in it.

Zhu Xiaoding, a Chinese lawyer who issued the letter via Weibo, a microblog service similar to Twitter, said he had done so at the behest of a friend and was sure it was from Mr. Zhou of Xinhua.

Mr. Xi visited Xinhua and other major state-media news outlets last month, and emphasized that they must unswervingly serve the party.

The suggestion that Mr. Xi could take China back to the turmoil of the Mao era appeared likely to irritate the authorities, who describe Mr. Xi as a bulwark of unflappable order.

This year is the 50th anniversary of the start of the Cultural Revolution in 1966, when Mao Zedong brought his methods of mass denunciation and vilification of foes to an extreme.

Some people fear that Mr. Xi is too willing to use harsh tactics that echo that time, said Zhang Lifan, a businessman and historian in Beijing whose father was persecuted under Mao.

"This era is different from the Cultural Revolution, when we were completely closed off," Mr. Zhang said. "Some of the mentality and methods from that time might persist. But people inside the system wouldn't like to see that happen again."

Adam Wu contributed research.

NewsTalk ZB (New Zealand)
Spy agencies may have been breaking the law
Saturday, 12 March 2016

Wellington - An intelligence expert is suggesting the country's spies may have been breaking the law.
It comes after recommendations in a review of intelligence laws that recommend GCSB and SIS staff be immune from criminal liability for actions undertaken in obtaining and operating under warrants.

Counter intelligence expert Dr Paul Buchanan said it's remarkable there's been no legal cover to the undercover agents of the SIS.

"And because there has been no legal cover then what they do to begin with, and assuming a false identity, is illegal".

Felix Marwick: Should the GCSB and SIS be immune from prosecution?

Dr Buchanan said the language around the immunity clauses needs to be tightened.

He said it's not good enough to say "act in good faith" or, "within the intentions of the Act".

Dr Buchanan said they'll have to specify more closely what is, and what is not, acceptable behaviour for undercover agents.

Labour leader Andrew Little said some scope has to be allowed for the fact intelligence agencies deal with people that act on the edge, if not the other side, of the law.

"In the end it comes down to making sure that there isn't some sort of carte blanche license to wholesale break the law and do whatever they like," he said.

"There's no security agency that could possibly be tolerated or justified that works in that sort of way."

Last year the High Court ruled evidence for the bulk of charges laid by Nelson police against members of the Red Devils gang was improperly obtained because a fake warrant was used to arrest an undercover officer.

Dr Buchanan said he has a strong feeling this was the precipitating event for immunity protections now being recommended for intelligence officers employed by the SIS and GCSB.

He said it must have been a red flag to the SIS in particular because it's very likely they do similar things in pursuit of their duties

SIS and GCSB Minister Chris Finlayson is still considering the review's recommendations and was unavailable to be interviewed on the matter.

The Intercept
Obama Wants Nonexistent Middle Ground on Encryption, Warns Against "Fetishizing Our Phones"
Saturday, 12 March 2016
Byline: Jenna McLaughlin

Washington - President Barack Obama says he wants strong encryption, but not so strong that the government can't get in.
"The question we now have to ask technologically is if it is possible to make an impenetrable device or system where the encryption is so strong that there is no key, there is no door at all?" he asked, speaking at the South By Southwest (SXSW) festival in Austin on Friday.

"Then how do we apprehend the child pornographer? How do we solve or disrupt a terrorist plot? What mechanisms do we have available to do even simple things like tax enforcement? If in fact you can't crack that all, if the government can't get in, then everybody is walking around with a Swiss bank account in their pocket. There has to be some concession to the need to be able to get into that information somehow."

It was Obama's first extended disquisition on the contentious issue of encryption. There have been many reports about a rift in his administration between those who recognize that unbreakable encryption is inevitable, and those who think there must be an alternative. But Obama appears to be hearing only one side.

Obama insisted that there is a middle ground. "My conclusion so far is that you cannot take an absolutist view on this," he said. "If your argument is strong encryption no matter what, and we can and should create black boxes, that I think does not strike the kind of balance we have lived with for 200, 300 years, and it's fetishizing our phones above every other value. And that can't be the right answer."

But the problem is that you can't have strong encryption without it being unbreakable.

Being absolutist about encryption is "the only way [it] works" tweeted Jake Laperruque, privacy fellow for the Constitution Project and the Open Technology Institute.

"It's not like no one has thought about this problem before. It's a fundamentally difficult problem, and it won't be solved anytime soon," wrote Matt Blaze, a computer science researcher and professor at the University of Pennsylvania.

Trying to come up with some solution that satisfies the desire for easy, ubiquitous law enforcement access while simultaneously upholding device security is what scientists call a "magic pony." Any hole for the government is a hole criminals and foreign adversaries could exploit, too.

And although Obama accused encryption supporters of being absolutist, he echoed the absolutist view that the widespread use encryption was tantamount to law enforcement "going dark". It's not.

The technology isn't universally marketable and there are plenty of other ways to amass evidence in criminal investigations, argued a group of scientists, privacy advocates, and members of the intelligence community in a Harvard Berkman Center report published in February. And the Internet of Things offers

many new ways to spy on us-- something the Director of National Intelligence James Clapper has mentioned himself.

Obama said he's "way on the civil liberties side of this thing," but civil liberties advocates didn't seem to agree.

"Why isn't 'government must always have the ability to access plaintext' the more 'absolutist' view?" asked Julian Sanchez, privacy and technology senior fellow at the Cato Institute in a tweet. "'Swallow arsenic.' No. 'Ok, a little hemlock then.' No. 'Well, c'mon, you can't be an ABSOLUTIST about this,'" he joked.

Kevin Bankston, the Director of the Open Technology Institute tweeted that he was "disappointed" Obama resorted to fear mongering. "Opens w/child kidnapping & terror, closes w/child porn & terror, vague talk of balance," he wrote.

Vancouver Sun
For drones, the sky's the limit in B.C.
Saturday, 12 March 2016
Byline: Derrick Penner

Vancouver - West Vancouver's Lofty Media uses drones like this Freefly Alta model to shoot aerial video for real estate companies. Marketing director Andrew Fyfe says the company intends to move into bigger film productions and is preparing to shoot crop surveying video for farmers.
It used to be to figure out what was going on in B.C.'s forests, foresters had the choice of walking into them and looking up from the ground, or hopping into a helicopter or airplane and looking down from high in the air.

Enter unmanned aerial vehicles, commonly called drones. Now foresters can get a view right at treetop level.

"You're not very high but close to the canopy, so you get much more detail about the forest," said Nicholas Coops, a forest researcher at the University of B.C. "Individual trees, gaps between trees, nests of birds, very, very detailed information about the understorey -- things you wouldn't get if you were in a plane."

The immediate payoff is that drone-captured images can give quick bird's-eye assessments of whether logging in a particular block has gone well or whether replanting after harvesting has gone as planned.

Researchers believe the longer-term benefit will come from marrying these drone-captured images with powerful computer processing to generate high-definition two-dimensional and three-dimensional maps of forests.

It is difficult to estimate the number of drones in commercial use. But over the past three years, the number of applications to Transport Canada for special flight operations certificates more than doubled to 2,300 in 2015 from 949 in 2013.

The certificates are Transport Canada's method of regulating professional uses, ensuring operators fly drones in compliance with regulations and while avoiding other aircraft.

Drones more typically make the news for the trouble that unregulated amateur operators cause, such as the unauthorized quadcopter spotted inside airspace over a forest fire near Oliver last August that forced the grounding of firefighting aircraft for several hours.

However, drones are increasingly being put to work in commerce and research, capturing stunning aerial shots for promotional videos and film, observing wildlife for biologists, helping police take overhead pictures for accident reconstructions, aiding transportation planners and more. They've also been put to use for inspection work, such as checking stability of cliffs after rock slides onto highways and checking power lines for BC Hydro.

In the evolution of drone technology in forestry, B.C. researchers and companies are on the leading edge of turning drone- captured imagery into high-value data for forest management.

"It's also the timeliness aspect, flying them when we want to, how we want to," said Coops, the associate dean for research and innovation in UBC's faculty of forestry, and a Canada research chair in remote sensing.

So far, Coops said, the key use of drones in B.C. forests has been in evaluating the regeneration of recently replanted forests.

"There is a lot of interest in using drones for that, because (they) work to the advantage of observing small things, and to the advantage of (being able to) go and fly every six months," he said.

He also sees them as an excellent tool for companies to do more detailed inventories of standing timber more cheaply, or to plan logging to avoid poor ground conditions after rainfall or spring run-off.

The convergence of computers, smaller high-quality cameras and improved drones to carry them is opening up this sector of the industry, said Patrick Crawford, co-founder of Vancouver-based Spire Aerobotics.

He started exploring the potential for drones while studying engineering at UBC. He put school on hold about 18 months ago to pursue a business opportunity with partner Mike Willcocks.

Crawford, who originally comes from Kamloops, came by his interest in drones naturally through a long-term passion for flight (he once held a glider pilot's licence and started work on his qualification for powered flight) and an interest in developing technology.

"I'd argue we're still in the infancy of drone technology in many ways," Crawford said.

Spire found its initial niche in using drones to scan wood chip piles at pulp mills, lumber yards, sawmills and wood-pellet plants and provide volume estimates for their inventory work.

Crawford said that is work that is traditionally done using manned aircraft and light sensors. Using drones, however, they can do the flights more cheaply and more frequently. They've also applied their data-processing techniques for researchers such as Coops.

Crawford said they've developed most of their company's intellectual property in the forestry sector, refining their capability to fly over forests and collect a great deal of two- and three-dimensional data, and turning that into maps.

"That next level of processing, you have that data -- what can you tell a business about it that can benefit them?" Crawford said. "That's where we want to focus our energy, and it's an application for business, for government or for any organization trying to sustainably manage the land base."

It might take more time to develop and incorporate some of the more "analytical" mapping applications, said Denis Cormier, a senior manager at FP Innovations, a key R&D organization in the Canadian forest industry.

First, there's the matter of making sure provincial forestry regulators accept that the level of detail provided by drone- generated aerial maps meets their standards for reporting.

Cormier said FP Innovations is comparing some of its B.C. drone-mapping results against ground-based surveys, and so far the province is on board with the new technology, "if it can meet their standards."

"It's not something you can easily do within a season. It's something that's evolving." he said. "At the research level, it's a pace that we're used to, (but) if you're a service provider that just bought a (drone) that cost you $50,000, you feel like things aren't moving fast enough."

Cormier added that while drones can be used more flexibly than manned aircraft, they are so new to the industry that existing work patterns are too set to fit them in.

For instance, forest companies that are used to hiring a helicopter or plane to conduct aerial surveys over a wide area once a year might not see the need to replace that effort with drones, which are limited to flying smaller areas, even if they are capturing more detailed visual information, he said.

For the time being, Cormier said, high-quality drone imagery is also an expensive proposition for forest companies because it costs of about $15 to $25 a hectare to turn drone-captured images into 3D maps.

As operators refine the computing process, "what we're hoping is that eventually we'll be able to meet a $5-a-hectare target," he said.A bigger limitation, however, is Transport Canada's regulation that operators don't let drones out of their sight.

"Trees are always going to be in your line of sight," Cormier said. That makes it hard for drones to cover wide areas of forest, unless operators can get a high viewpoint.

"Until we're solving the line-of-sight issue, it's going to be quite difficult to develop (drone operations) on a larger scale," he said.

But drone operators are confident that permission to fly beyond line of sight is only a matter of time, said David Bird, editor of the Journal of Unmanned Vehicle Systems, a publication of the national association Unmanned Systems Canada.

Bird, a wildlife biologist and professor emeritus at McGill University, said researchers like him are anxious to use drones for covering large areas of landscape using drones. Meanwhile, companies that want to use drones for inspecting transmission lines or large-scale survey work are also pressuring to change the rules.

Unmanned Systems Canada is preparing a position paper for Transport Canada on crafting regulations for beyond-visual-line-of-sight flight.

"It's going to come," Bird said.

Transport Canada is planning more formal regulation for drone operations, including clear rules for allowing unlicensed recreational use of drones and a drone licensing and registration system for operators in specified commercial and other drone uses, said Aaron McCrorie, director general of civil aviation.

The growth of the industry means existing regulations "are no longer adequate and we need more prescriptive regulations," McCrorie said.

Transport Canada proposed new regulations in 2015 and has held meetings across the country to gather comment. McCrorie said his department is reviewing that public comment and refining a set of regulations for Transport Minister Marc Garneau's consideration.

However, those regulations will be based on line-of-sight operations.

"A number of years down the road, we will look at regulations for beyond visual line of sight," McCrorie said. "But there's a lot more work to be done."

In the meantime, drone use continues to soar.

The B.C. Ministry of Transportation bought two drones last year for a pilot project to get aerial photos for planning work, but they've also proved useful in helping geotechnical engineers assess cliff safety after rock slides, said Mike Lorimer, the department's regional director for the southern Interior.

Lorimer said they typically hire helicopters to do that -- at a cost of $1,200 to $1,300 an hour. Replace them with drones a couple of times and "they pay for themselves," he said.

"It's helping us with design (work)," Lorimer added. "We're sort of on the verge of everyone figuring out how to use these things better, and we'd like to be at the front edge of that."

And despite their bad experience with drones grounding firefighting aircraft near Oliver last summer, the B.C. Wildfire Service tested drones during the Elaho and Boulder Creek fires near Pemberton by flying them near nightfall to look for hot spots with thermal-imaging cameras.

"It was very much a trial over a couple of days," chief fire information officer Kevin Skrepnek said.

West Vancouver-based Lofty Media started out shooting aerial video for promotional real-estate videos, but is angling to get into bigger film productions and is preparing to try crop surveying for farmers, said Andrew Fyfe, the company's marketing director.

"We haven't done any of those (crop-survey) jobs yet, but I definitely see that as a part of it as we grow," Fyfe said. "With thermal-imaging cameras, you can fly down a row of fruit trees and the camera will pick up how many fruit are on the trees, which will give the farmer a pretty accurate yield of what their crop is going to be, and it's pretty valuable information."

New York Times
In the Apple Case, a Debate Over Data Hits Home
Monday, 14 March 2016
Byline: Multiple reporters

Washington - Three years ago, reeling from Edward J. Snowden's disclosure of the government's vast surveillance programs and uncertain how to respond, President Obama said he welcomed a vigorous public debate about the wrenching trade-offs between safeguarding personal privacy and tracking down potential terrorists.
"It's healthy for our democracy," he told reporters at the time. "I think it's a sign of maturity."

But the national debate touched off this winter by the confrontation between the Justice Department and Apple over smartphone security is not exactly the one Mr. Obama had in mind.

Mr. Snowden's revelations produced modest changes and a heightened suspicion of the government's activities in cyberspace. Because the issue now centers on a device most Americans carry in their pockets, it is concrete and personal in a way that surveillance by the National Security Agency never was.

The trade-offs seem particularly stark because they have been framed around a simple question: Should Apple help the F.B.I. hack into an iPhone used by a gunman in the massacre last December in San Bernardino, Calif.?

Law enforcement officials have been adamant they must be able to monitor the communications of criminals. They received a vote of confidence from Mr. Obama on Friday, when he said the "absolutist" position taken by companies like Apple is wrong. But the pushback has been enormous.

In the month since a judge ordered Apple to comply with the F.B.I., the debate has jumped from the tech blogs to the front pages of daily newspapers and nightly newscasts. Supporters of the company's position have held rallies nationwide. Late-night comedians have lampooned government snoopers. Timothy D. Cook, the usually publicity-shy Apple chief executive, pleaded his case on "60 Minutes" last December. On Twitter, "#encryption" fills the screen with impassioned debate on both sides.

"Discussing the case with my friends has become a touchy subject," said Matthew Montoya, 19, a computer science major at the University of Texas, El Paso. "We're a political bunch with views from all across the spectrum."

Like many of her friends, Emi Kane, a community organizer in Oakland, Calif., recently found herself arguing via Facebook with a family friend about the case. Ms. Kane thought Apple was right to refuse to hack the phone; her friend, a waitress in Delaware, said she was disgusted by Apple's lack of patriotism.

After exchanging several terse messages, they agreed to disagree. "It was a hard conversation," Ms. Kane said.

The novelist Russell Banks, who signed a letter to Attorney General Loretta Lynch on behalf of Apple, said he had spoken with more than a dozen people about the case just in the last week.

"It's not just people in the tech industry talking about this," Mr. Banks, the author of "Affliction" and "The Sweet Hereafter," said. "It's citizens like myself."

That may be because the Apple case involves a device whose least interesting feature is the phone itself. It is a minicomputer stuffed with every detail of a person's life: photos of children, credit card purchases, texts with spouses (and nonspouses), and records of physical movements.

Mr. Obama warned Friday against "fetishizing our phones above every other value." After avoiding taking a position for months, he finally came down on the side of law enforcement, saying that using technology to prevent legal searches of smartphones was the equivalent of preventing the police from searching a house for evidence of child pornography.

"That can't be the right answer," he said at the South by Southwest festival in Texas, even as he professed deep appreciation for civil liberties and predicted both sides would find a way to cooperate. "I'm confident this is something that we can solve."

But polls suggest the public is nowhere near as certain as Mr. Obama. In surveys, Americans are deeply divided about the legal struggle between the government and one of the nation's most iconic companies. The polls show that Americans remain anxious about both the threat of terrorist attacks and the possible theft of personal digital information.

A Wall Street Journal/NBC News survey released last week found that 42 percent of Americans believed Apple should cooperate with law enforcement officials to help them gain access to the locked phone, while 47 percent said Apple should not cooperate. Asked to weigh the need to monitor terrorists against the threat of violating privacy rights, the country was almost equally split, the survey found.

That finding may have seemed unlikely in the wake of terrorist attacks last year in Paris and San Bernardino. In December, eight in 10 people said in a New York Times/CBS News survey that it was somewhat or very likely that there would be a terrorist attack in the United States in the coming months. A CNN poll the same month found that 45 percent of Americans were somewhat or very worried that they or someone in their family would become a victim of terrorism.

But despite the fears about terrorism, the public's concern about digital privacy is nearly universal. A Pew Research poll in 2014 found more than 90 percent of those surveyed felt that consumers had lost control over how their personal information was collected and used by companies.

The Apple case already seems to have garnered more public attention than the Snowden revelations about "metadata collection" and programs with code names like Prism and XKeyscore. The comedian John Oliver once mocked average Americans for failing to know whether Mr. Snowden was the WikiLeaks guy or the former N.S.A. contractor (he was the latter).

Now, people are beginning to understand that their smartphones are just the beginning. Smart televisions, Google cars, Nest thermostats and web-enabled Barbie dolls are next. The resolution of the legal fight between Apple and the government may help decide whether the information in those devices is really private, or whether the F.B.I. and the N.S.A. are entering a golden age of surveillance in which they have far more data available than they could have imagined 20 years ago.

"It's an in-your-face proposition for lots more Americans than the Snowden revelation was," said Lee Rainie, director of Internet, science and technology research at Pew Research Center.

Cindy Cohn, executive director of the Electronic Frontier Foundation, said: "Everyone gets at a really visceral level that you have a lot of really personal stuff on this device and if it gets stolen it's really bad. They know that the same forces that work at trying to get access to sensitive stuff in the cloud are also at work attacking the phones."

For the F.B.I. and local law enforcement agencies, the fight has become a high-stakes struggle to prevent what James B. Comey, the bureau's director, calls "warrant-free zones" where criminals can hide evidence out of reach of the authorities.

Officials had hoped the Apple case involving a terrorist's iPhone would rally the public behind what they see as the need to have some access to information on smartphones. But many in the administration have begun to suspect that the F.B.I. and the Justice Department may have made a major strategic error by pushing the case into the public consciousness.

Many senior officials say an open conflict between Silicon Valley and Washington is exactly what they have been trying to avoid, especially when the Pentagon and intelligence agencies are trying to woo technology companies to come back into the government's fold, and join the fight against the Islamic State. But it appears it is too late to confine the discussion to the back rooms in Washington or Silicon Valley.

The fact that Apple is a major consumer company "takes the debate out of a very narrow environment -- the universe of technologists and policy wonks -- into the realm of consumers where barriers like the specific language of Washington or the technology industry begins to fall away," said Malkia Cyril, the executive director of the Center for Media Justice, a grass-roots activist network.

That organization and other activist groups like Black Lives Matter have seized on the issue as important for their members. In February the civil liberties group Fight for the Future organized the day of protest against the government order that resulted in rallies in cities nationwide.

"When we heard the news and made a call for nationwide rallies, one happened in San Francisco that same day," said Tiffiniy Cheng, co-founder of Fight for the Future. "Things like that almost never happen."

Ms. Cyril says the public angst about the iPhone case feels more urgent than did the discussion about government surveillance three years ago.

"This is one of those moments that defines what's next," she said. "Will technology companies protect the privacy of their users or will they do work for the U.S. government? You can't do both."

Le Monde
Pour vivre heureux, vivons cryptés
Monday, 14 March 2016
Byline: Yves Eudes

Non identifié - Les moindres détails de notre existence sont enregistrés dans nos smartphones. Et nous sommes tous susceptibles d'être espionnés. Pas par la NSA une femme jalouse ou un patron trop curieux suffira. Face à ces risques, il faut verrouiller sa vie privée. Pas si simple.
Dans l'un de ses sketchs, le jeune humoriste Norman raconte que, depuis qu'il vit en couple, il ne peut plus jamais se séparer de son smartphone. Si par malheur il le laissait traîner dans l'appartement, sa copine pourrait s'en emparer, consulter l'historique de ses appels, lire ses courriels, ses SMS, ses messageries, ses comptes sur les réseaux sociaux, et découvrir qu'il est en contact avec d'autres femmes, dont certaines sont peut-être ses amantes.

Résultat, même quand il va prendre une douche, Norman emporte son téléphone avec lui - ce qui, bien sûr, suffit à éveiller les soupçons... La vidéo a bien marché sur YouTube, car, dans la vraie vie, ces accidents téléphoniques provoquent tous les jours d'innombrables scènes de ménage, ruptures et actes de vengeance.

Si votre conjoint veut aller jusqu'au divorce, il pourra utiliser les traces d'adultère trouvées dans votre téléphone. Article 1316-1 du code civil : " L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane (...). " Pire : vous ne pourrez pas invoquer la violation du secret des correspondances pour refuser ce moyen de preuve, sauf s'il a été obtenu par la violence.

Le danger ne vient pas seulement de votre amant(e). Méfiez-vous de l'ado qui chope votre portable pour envoyer un SMS urgentissime, de la bonne copine qui vous soupçonne de coucher avec son mari, des parents qui se font du souci pour votre avenir, et des collègues malintentionnés - sans parler des inconnus qui trouvent le téléphone que vous avez oublié au restaurant et qui vont vous pourrir la vie, juste pour le plaisir.

Bien entendu, vous pouvez verrouiller votre appareil avec un code ou un schéma à points. Mais le plus souvent, le verrouillage se déclenche après plusieurs minutes - un délai suffisant pour un espion déterminé. Par ailleurs, si votre code est votre date d'anniversaire, si c'est le même que celui de la porte de votre immeuble, ou si c'est l'année où la France a gagné la coupe du monde de foot, vous êtes vulnérable. Le schéma à points a aussi ses faiblesses : si vous ne nettoyez pas votre écran, votre doigt laisse une trace grasse reproduisant le tracé, qui sera visible grâce à une lumière rasante.

Se méfier aussi des services multi- plates-formes, si pratiques pour glisser en douceur de votre PC vers votre smartphone. Un exemple pour les possesseurs d'un téléphone Android enregistré chez Google via une adresse Gmail : si vous laissez votre compte Google ouvert en quittant votre ordinateur, un proche

ou un collègue pourra, en trois clics, aller sur votre page personnelle " Google Device Manager ". De là, il pourra localiser votre téléphone et le pister en temps réel, le faire sonner, effacer sa mémoire et même changer le mot de passe. De même, si vous avez sauvegardé vos données dans le cloud, un espion domestique pourra aussi s'attaquer à vos comptes en ligne, souvent mal protégés.

Si les choses vont très mal, votre mari jaloux pourra subtiliser votre appareil et le porter chez un réparateur pour le faire déverrouiller. Ces artisans de quartier possèdent souvent le matériel nécessaire pour casser les codes des téléphones bas de gamme ou un peu anciens, qui restent très répandus. Ils se laisseront parfois convaincre, pour 100 à 200 euros - la vérité, ça n'a pas de prix. Un réparateur du 12e arrondissement de Paris explique que, parfois, des policiers viennent le voir discrètement pour qu'il déverrouille un téléphone. Sa méthode prend plusieurs jours, mais, chez lui, on gagne du temps sur la procédure.

Dans l'univers professionnel, les risques sont décuplés. Le plus souvent, les téléphones distribués aux employés par les entreprises contiennent des logiciels permettant de prendre la main sur les appareils, et donc de savoir en détail comment ils sont utilisés. Les marchands d'équipements d'extraction de données annoncent sur Internet qu'ils les vendent " aux services de police, aux militaires, aux professionnels du renseignement ", mais aussi aux " professionnels de la sécurité en entreprise " et aux " industries de -l'e-discovery " - une catégorie mystérieuse qui englobe différentes sortes d'enquêteurs privés. Certains groupes possèdent des appareils illicites permettant de - géolocaliser les téléphones des équipes commerciales de leurs concurrents.

Mesures, contre-mesures... la surenchère semble sans fin. Les nouveaux smartphones haut de gamme chiffrent les données automatiquement, et permettent de choisir un verrou très résistant (code à six chiffres, empreinte digitale, phrase de passe...). Ils proposent aussi une fonction spéciale, qui efface toutes les données si on tape un mauvais code dix fois de suite - imparable, mais les données sont perdues à tout jamais, y compris pour vous. Déjà, les polices et les services secrets du monde entier cherchent à casser ces nouvelles protections ou à les faire interdire - sans parler des hackeurs. Des sociétés basées en Israël et en Europe de l'Est affirment qu'elles sont capables de déverrouiller presque tous les smartphones grand public actuellement en vente dans le commerce.

Bannir Angry BirdsLa solution la plus radicale consiste donc à s'offrir un téléphone ultrasécurisé, qui chiffrera à la fois les communications et les données stockées en mémoire. Il résistera aux interceptions à distance comme aux intrusions physiques, et sera paramétré dès l'origine pour offrir les protections maximales. Attention, les appels et les SMS ne seront cryptés que si votre correspondant possède aussi un téléphone sécurisé. Par ailleurs, vous ne pourrez pas télécharger les applis de votre choix : les petits jeux apparemment anodins comme Angry Birds, qui vous géolocalisent à votre insu, seront bannis. En France, un simple particulier ne peut pas acheter ce type de téléphone, en vertu d'un décret officiel - car c'est bien connu, les honnêtes gens n'ont rien à cacher. Pour s'en procurer, il faut être patron ou cadre supérieur, et passer commande au nom de son entreprise.

Pour ceux qui ne sont pas PDG, heureusement, il existe des solutions. Vous pouvez conserver votre vieux téléphone et télécharger une application qui cryptera vos communications via Internet, pourvu que votre correspondant possède la même. Si un intrus parvient à s'emparer de votre appareil et à l'ouvrir, vos conversations seront protégées par un deuxième mot de passe. Selon les cas, ces pare-feu ont été créés par des militants de l'Internet libre ou par des start-up commerciales installées dans des pays comme la Suisse ou la Suède, où les lois sont très protectrices.

Si vous vous contentez de demi-mesures, sachez qu'Apple, Google et WhatsApp ont aussi renforcé la protection de leurs messageries. Ainsi sur iPhone, un iMessage (en bleu, envoyé à un autre iPhone) sera plus difficile à intercepter qu'un SMS ordinaire (en vert). Il n'est jamais trop tard pour agir, mais le temps presse, car Internet n'oublie rien : même si vous vous êtes racheté une conduite depuis des années, les traces numériques de vos infidélités passées pourront être retrouvées jusqu'à la fin des temps.

The Guardian (London)
Snooper's charter: Labour threatens to hold up bill over privacy fears
Monday, 14 March 2016
Byline: Rowena Mason

London - Labour is threatening to hold up the government's new investigatory powers bill that extends the internet surveillance powers of the state unless ministers address concerns about privacy.
Andy Burnham, the shadow home secretary, said there would be "no blank cheque" of Labour support for the bill when it comes to the House of Commons for its next stage on Tuesday.

Labour supports the aims of the bill, which gives the state powers to force communications firms to store individuals' internet connection records - the addresses of websites visited - for 12 months.

But Burnham said the party was prepared to delay the legislation until concerns were allayed that it intrudes too far into people's lives.

"Britain needs a new legal framework in this crucial area that is fit for the digital age, balancing powers with proper safeguards. So Labour will put party politics aside and work constructively with the government to that end," he said. "But there will be no blank cheque."

Burnham said the home secretary, Theresa May, needed to make substantial changes before the bill would be acceptable.

He added: "While I share her wish to see a comprehensive bill on the statute book by the end of this year, we can't let the timetable dictate the quality. On Tuesday, I will make clear to the home secretary that, if she fails to listen to our concerns, Labour will be prepared to delay this legislation so that we get it right.

"We believe the bill must start with a presumption of privacy, as

recommended by the intelligence and security committee, include a clearer definition of the information that can be held in an internet connection record and set a higher threshold to justify access to them. There also needs to be a higher degree of protection for journalists and their sources.

"On the left of politics, there are deeply held concerns that, in our country's past, investigatory powers have been misused against trades unionists and ordinary people who are campaigning for justice. This is why the government will have to work hard to earn our support."

The government argues the bill is needed to address a gap in police and intelligence powers that means some communication cannot be tracked.

It revives some of the aims of a previous surveillance bill, which

became dubbed the snooper's charter in the last parliament and was eventually blocked by the Liberal Democrats.

Over the weekend, the US president, Barack Obama, questioned the way tech companies were making smartphones so strongly encrypted that they could not be broken into by law enforcement agencies.

Obama told a technology festival in Texas: "The question we now have to ask is, if technologically it is possible to make an impenetrable device or system, where the encryption is so strong there's no key, there's no door at all, then how do we apprehend the child pornographer? How do we solve or disrupt a terrorist plot?"

It comes after the FBI took Apple to court in an attempt to force it to break into a smartphone owned by one of the shooters in the San Bernadino massacre.

The Independent (UK)
Snooper's Charter: Tech companies will have to give police 'back- door' access to customers' data
Monday, 14 March 2016
Byline: Matt Broomfield

London - Internet service providers and technology companies will be forced to install "back-door" flaws into their products, so British police and security services can access them on demand.
The move was announced in draft documents published in support of Theresa May's controversial Investigatory Powers Bill, announced in November 2015.

Companies will also be banned from revealing whether they had been made to install "back-door" access routes, leaving customers unable to know whether their messages and search history are truly secure.

And if the draft documents are approved and the Bill known as the "Snoopers' Charter" is passed in Parliament, the controversial measures will be partially paid for by British taxpayers.

The move, intended to prevent criminals and terrorists from networking and organising illegal activities online, follows a legal dispute between the FBI and technology company Apple over a similar issue.

An American court ruled that Apple had to help the FBI bypass encryption on an iPhone belonging to Syed Farook, one of the San Bernadino killers. Farook and his wife killed 14 people in a mass shooting in December 2015.

But Apple launched a highly-publicised appeal, arguing that while they could unlock the phone, it would set a dangerous precedent and compromise their customers' privacy and security.

When announced, the Investigatory Powers Bill also sparked an immediate backlash from privacy campaigners. It requires internet and phone companies to store the search history of web users for a year and hand this information over to the police upon request, and made explicit for the first time the power of the police to hack phones and computers.

The new documents, expanding on Theresa May's initial proposal, indicate how companies will be forced to help the police hack into their own customers' data.

Any firm with more than 10,000 customers providing a "telecommunications service" to UK citizens could be subject to the legislation, forcing them to provide the "technical capability" for "interception" of personal data. Apple, Google, Facebook and a number of broadband companies are among the organisations affected by the measures.

They would also be bound by an effective gagging order, "under a duty not to disclose the existence and contents" of the order to hand over personal data.

An independent "investigatory powers commissioner" would be available to assess cases where companies felt their rights were being infringed, while the orders would have to be reviewed every two years regardless of circumstance.

However, there is no apparent way for private citizens to find out if their personal data is being scrutinised by the police, let alone appeal against this process.

60 Minutes
The Encryption debate
Sunday, 13 March 2016
Byline: Lesley Stahl

The argument over encryption between Apple and the FBI reminds us that the world is facing a far more tech-savvy terror threat. While not that long ago al Qaeda often handled its communications by going back to the Stone Age relying on mules and couriers, the Islamic State, or ISIS, proved it can be done with just a push of a button using everyday tools of 21st century teenagers: the latest smartphones and messaging apps.
The encryption debate centers around an iPhone found in San Bernardino, where 14 men and women were killed in a terror attack last December. But before that, there was the massacre in Paris. We went there to meet the city's chief prosecutor who is confronting some of the same issues.

Francois Molins: The terrorists are able to communicate with total impunity.

Voiceover: Francois Molins is the head prosecutor of Paris -- he's investigated all the big acts of terrorism here, including Charlie Hebdo, the kosher supermarket, and now the November 13 attacks where 130 people were killed, more than 350 wounded.

Lesley Stahl: Do you have phones in terrorist attacks that you have not been able to get into because of encryption?

Francois Molins: Oui oui. With all these encryption software programs, we can't penetrate into certain conversations and we're dealing with this gigantic black hole, a dark zone where there are just so many dangerous things going on.

Voiceover: It's not just phones. One of the things he's looking into is a texting app favored by ISIS called Telegram which, like the new Apple iPhone -- offers advanced encryption.

Lesley Stahl: How often have you run in, in all your investigations, into Telegram?

Francois Molins: Yes, very often. Telegram, we can't penetrate, we can't get into it.

Voiceover: Pavel Durov is the inventor of Telegram. He's a young man without a country. He's Russian born but wanders the world now, in exile. He created Telegram so he could communicate in complete secrecy. It has taken off, used by over 100 million people.

Lesley Stahl: But it's also used by terrorists now. Is this a concern for you?

Pavel Durov: Oh definitely. And in our 100 million users, probably this illegal activity we're discussing are only a fraction of a fraction of a fraction of the potential usage. And still we're trying to, you know, prevent it.

Voiceover: Telegram has become a go-to site for ISIS. They use it to widely disseminate propaganda like this video of the Paris attackers training in Syria. But ISIS fighters can also use Telegram to send private messages to each other to covertly plan and coordinate attacks.

Lesley Stahl: Is there something on your site on Telegram that allows any messages, emails, to just disappear, vanish?

Pavel Durov: Yes. So in private messages we have this secret chat feature which provides you with a self-destruct timer.

Lesley Stahl: Self-destruct timer.

Pavel Durov: You could set a specific amount of time, like a few seconds, or a minute or a week, after which the message would disappear.

Voiceover: Durov's obsession with secrecy and security stems from his own personal history. Long before Telegram he was known as the Mark Zuckerberg of Russia because he built a popular equivalent of Facebook. But in 2011, when anti- Putin marchers filled Moscow's streets, the Kremlin demanded he take down the organizers' sites.

Pavel Durov: And I refused to do that publicly. And the next day I had armed policemen at my doorstep...

Lesley Stahl: Wonder why.

Pavel Durov: ...and tried to break into my apartment.

Voiceover: There was continual pressure on him to hand over users' personal data culminating in 2014 when, under Kremlin duress, Durov was ousted from his own company.

Lesley Stahl: How long did you stay in Russia after that?

Pavel Durov: Not a single day.

Lesley Stahl: Oh, then you fled.

Pavel Durov: I certainly feel that I am not welcome at that country anymore.

Voiceover: That's when he created Telegram and encrypted it, he says, so activists could be assured that no government could ever access their personal data. He managed to leave Russia with a reported $300 million which he uses to singled-handedly fund Telegram, costing him, he says, over a million dollars a month.

Lesley Stahl: This was something that you created to allow democracy to flourish, to allow dissidents in Russia and in other countries to communicate with each other. And then all of a sudden you find out that this terrorist group uses your site for completely different reasons.

Voiceover: Pavel Durov: Yeah, we were horrified.

Lesley Stahl: There's an irony there.

Pavel Durov: There is. But you know there's little you can do because if you allow this tool to be used for good, there will always be some people who would misuse it.

Voiceover: Just hours after the terrorists hit Paris on the night of November 13, ISIS used Telegram to take credit for the attacks. It was a wake-up call for European authorities.

Rob Wainwright: It's the first time ever in Europe that we had terrorists rampaging through our streets. First time we had terrorists wearing suicide belts in heavily populated, public areas.

Voiceover: As head of Europol, Rob Wainwright gathers and analyzes information from over 600 law enforcement agencies. He has set up a new counter terrorism center to better coordinate all the intelligence.

Lesley Stahl: How much is encryption a problem generally in these investigations?

Rob Wainwright: In most of them. I mean, across the tens of thousands of investigations that Europol is supporting every year on terrorism and serious crime, at least three quarters of them have encryption at the heart of the challenge that law enforcement face.

Lesley Stahl: Now, what about the November 13th attack specifically?

Rob Wainwright: From what we see, encryption also played a role in that part and that's something that we we're digging into much deeper at the moment.

Lesley Stahl: Why is it still a mystery?

Rob Wainwright: It's not-- not so much of a mystery. It's not that I can share all the details about a very sensitive investigation in public.

Voiceover: We know that the ringleader of the attack, 28-year-old Abdelhamid Abaaoud, was a wanted fugitive who goaded authorities by bragging in this online ISIS magazine how easily he eluded them shuttling between Europe and Syria. He liked taking selfies of his exploits, often posting them online. In this gruesome video, he and his friends tie bodies to the back of a truck, Abaaoud in the driver's seat:

[Abdelhamid Abaaoud (translator): We used to tow jet skis - now we tow the infidels fighting us.]

Lesley Stahl: What is astonishing is that you knew who he was. He was on everybody's radar screen.

Francois Molins (translator): You're right. Abaaoud-- he has been one of the major targets for France and Belgium counterterrorism for many months.

Voiceover: Before Paris, Abaaoud was suspected of guiding European jihadis in attacks in France and Belgium, but the attempts were all foiled. In one of them an iPhone belonging to one of the jihadis was confiscated but it was not useful in finding Abaaoud, because it was encrypted.

Lesley Stahl: We've been told, and I want to confirm it, that the encrypted phone may have prevented you from getting information about the Paris attacks.

Francois Molins (translator): That's a theory that really needs to be looked into, but to do so, we really need to be able to get into that phone. You know, I say, all these smart phones make justice blind because they deprive us of a lot of information that could contribute to our investigations.

Voiceover: Abaaoud was on site in Paris on the night of November 13, coordinating three different teams over his phone: one group, at a soccer stadium, exploded their suicide vests outside. Abaaoud and two others went on a killing spree at bars and cafes... while a third team stormed a rock-concert at the Bataclan theater and started shooting.

Francois Molins (translator): I said to myself: "The thing that we'd been fearing was coming for months, was now happening."

Voiceover: The prosecutor rushed to the scene - first to the cafes where Abaaoud had already sprayed the sites with an assault rifle.

Francois Molins (translator): We know that he participated in the commando attacks at the cafes. Afterwards we see him in a video in the Paris subway. And we do believe that he went maybe just in front of the Bataclan.

Voiceover: The prosecutor also went from the cafes to the Bataclan. What he didn't know was that Abaaoud was outside the theater at the same time, amid throngs of police, standing there in his orange sneakers - apparently talking on the phone to the shooters inside. While police didn't spot him there, he was tracked down to an apartment in a Paris suburb five days later, and killed in a hail of gunfire and

explosions. In a stroke of luck police found a Samsung phone one of the attackers had tossed into a garbage can in front of the Bataclan, and it posed no encryption problems.

Francois Molins (translator): We were able to get information from phone communications that enabled us to retrace the terrorists movements: where they were, where they stayed, their itineraries.

Standard text messages were found on the phone including a final one saying, "Here we go. We're starting!" Also found, the app Telegram. It had been downloaded the day of the attack.

Lesley Stahl: But you personally don't know if the attackers actually communicated via Telegram to plot these coordinated attacks, or even if they used it during the attacks?

Pavel Durov: No, we have no information to prove that.

Lesley Stahl: Is there anything in your mind that says, "Gee, we have to have - to allow law enforcement to get in because what's going on is just unacceptable.

Pavel Durov: You know the interesting thing about encryption is that it cannot be secure just for some people.

Lesley Stahl: ISIS and other terrorist groups, they just push a button on an application like yours, specifically yours, an application... and it's gone around the world, like that.

Pavel Durov: Well again, this is the world of technology and it's impossible to stop them at this point. ISIS could come up with their own messaging solution within a month or so, if they wanted to because the--

Lesley Stahl: You mean create their own Telegram?

Pavel Durov: Exactly.

Voiceover: Since Paris, Durov has been purging ISIS propaganda from Telegram but says, if asked to unlock any private messages, he would tell the authorities that the encryption code makes it mathematically impossible, using a similar argument as Apple.

Lesley Stahl: So you're basically saying that even if you wanted to, your hands are tied.

Pavel Durov: Yes.

Lesley Stahl: You can't do it.

Pavel Durov: We cannot.

Lesley Stahl: So this is one of the great debates of our time. Which is more important? Is it more important to shut down this kind of terrorism or preserve privacy?

Pavel Durov: I'm personally for the privacy side. But one thing that should be clear is that you cannot make just one exception for law enforcement without endangering private communications of hundreds of millions of people because encryption is either secure or not.

Lesley Stahl: The founder of Telegram has told us, he thinks privacy is more important than security issues, and he wouldn't open it up even if you did ask him.

Francois Molins (translator): Fine, that's his personal choice. But I consider that there are limits in all societies. There are limits to freedom and privacy. Freedom doesn't mean you can just do anything and everything you want. And there's a duty of institutions -- police and judicial -- to ensure security. You can't have freedom without security.

Chosun Ilbo
N.Korea 'Using Honeytraps to Steal Cyber Secrets'
Monday, 14 March 2016

North Korea is using honeytraps to steal clandestine information from gullible male South Korean officials on the Internet, the National Intelligence Service said Friday.
The NIS told the National Assembly that the North has set up fake Facebook accounts with pictures of pretty women to hook up with scores of former and incumbent South Korean officials and get hold of classified information.

The NIS said the North is also spreading false rumors about the South Korean government online. "If a beautiful stranger wants to become your friend on Facebook, you should turn them down," an NIS official warned lawmakers.

The NIS said the North Korea succeeded in hacking into the e-mail accounts of 40 South Korean government officials and military officers by sending them e-mails purporting to come from Cheong Wa Dae or other government agencies.

Lee Cheol-woo of the ruling Saenuri Party said after the closed-door session that North Korea is conducting cyber terror aimed at jamming GPS navigation systems. "Terror attacks targeting GPS systems are very dangerous since they can cause aircraft to fly in the wrong direction," he added.

Washington Post
Black Lives Matter group wary of FBI in Apple fight

Saturday, 12 March 2016
Byline: Andrea Peterson

Washington - Black Lives Matter activists are siding with Apple in the company's legal showdown with the FBI over a phone used by one of the San Bernardino, Calif., shooters.
"We urge you to consider the dire implications for free speech and civil liberties if the FBI is permitted to force Apple to create technology to serve its investigatory purposes," a coalition of activists and civil rights organizations wrote in a letter to a California court this week in support of the tech company. "The FBI's historically questionable surveillance procedures do not bode well for setting a precedent that allows the agency universal access to private smartphone data."

Privacy - especially from the spying eyes of the government - is personal for the civil rights community, at least in part because of the movement's history with the FBI.

In the 1950s, the bureau ran an initiative called COINTELPRO. At first, it was aimed at disrupting communist activities, but the program was later expanded to target other domestic groups including the Black Panther Party and the Rev. Martin Luther King Jr.

The FBI started spying directly on the civil rights leader in 1963, not long after the March on Washington, according to historian Beverly Gage. It placed wiretaps on the phones in his home and offices, as well as bugging devices in his hotel rooms, she said, uncovering evidence of King's extramarital affairs, which the bureau unsuccessfully pitched to the news media.

Perhaps frustrated by the lack of interest by the media, FBI Director J. Edgar Hoover in November 1964 denounced King during a news conference as "the most notorious liar in the country." A few days later, one of Hoover's subordinates sent King a disturbing letter, designed to look as if it was from a disenchanted supporter. It referenced audio recordings as evidence of King's infidelity and urged the civil rights leader to kill himself.

The FBI acknowledges the violations of COINTELPRO, noting on its website that the program was "later rightfully criticized by Congress and the American people for abridging first amendment rights and for other reasons."

FBI Director James B. Comey keeps a copy of the letter approving the King wiretap on his desk - and requires all new agents and analysts to study how the FBI treated the civil rights leader. "The reason I do those things is to ensure that we remember our mistakes and that we learn from them," he said in a speech at Georgetown University last year.

But the communities targeted by COINTELPRO remember the FBI's mistakes, too.

That's why the Black Lives Matter activists cited that shameful part of the bureau's history in their letter supporting Apple's challenge of the court order that would force Apple to help investigators access

information on an iPhone belonging to one of the San Bernardino attackers. The iPhone was recovered after the Dec. 2 attack that killed 14 people and injured 22 others. It was given to one of the attackers in his job as a county health inspector, and although the FBI has obtained backups taken from the phone, it has not been able to access the data stored on the device.

"[O]ne need only look to the days of J. Edgar Hoover and wiretapping of Rev. Martin Luther King, Jr. to recognize the FBI has not always respected the right to privacy for groups it did not agree with," the letter said. The activists added, "And many of us, as civil rights advocates, have become targets of government surveillance for no reason beyond our advocacy or provision of social services for the underrepresented."

New York Times
Protecting the Privacy of Internet Users
Saturday, 12 March 2016

Editorial: The chairman of the Federal Communications Commission proposed common-sense privacy rules this week that would limit what broadband companies are allowed to do with the Internet browsing history and other personal information of consumers.
Companies like Comcast and AT&T, which operate wired and wireless networks, know a lot about what Americans do online, like the websites they visit and how long they stay on them. But there are no F.C.C. rules that bar those companies from selling that information to advertisers. The commission can, however, take action against the companies for deceptive and unfair practices.

Under the proposal by the chairman, Tom Wheeler, cable and phone companies would be allowed to use personal data for things like billing and pitching more expensive versions of services that customers are already using. Customers could opt out of marketing for other services provided by their broadband companies. And the companies would have to get permission from their customers before they could do more with the data, like selling it to advertisers. Another rule would require companies to protect the data and notify customers, the commission and law enforcement agencies if the information was stolen.

These are similar to the protections the commission has long imposed on phone companies. Those rules have worked so well that most Americans do not worry that Verizon or T-Mobile is listening to their conversations or using call records to market products and services. People should have similar privacy protections when they use cable or phone lines to get on the Internet.

Companies like AT&T, however, argue that new rules are not needed because a lot of Internet traffic is encrypted and phone and cable companies cannot decipher the data. But even when data is encrypted, companies can still tell what websites people are visiting. And many websites still do not use encryption.

Another criticism is that these rules treat broadband providers differently than Internet businesses like Google and Facebook, which collect huge amounts of personal data about users. But the commission

has no authority to regulate those websites. And it is far easier for consumers to avoid those sites than to avoid their Internet service providers, especially since in many parts of the country people have only one or two choices for broadband.

Mr. Wheeler is able to make this proposal because the commission wisely decided in February 2015 to treat broadband as a telecommunications service rather than as a lightly regulated information service. That decision also made it possible for the commission to forbid cable and phone companies to create fast and slow lanes on the Internet.

The commission will vote on March 31 to open Mr. Wheeler's proposal to public comments before it can be finalized, probably before the end of the year. Cable and phone companies and their Republican supporters in Congress will undoubtedly oppose this regulation. But these rules are necessary because consumers need to have control over their personal information.

Follow The New York Times Opinion section on Facebook and Twitter, and sign up for the Opinion Today newsletter.

Sunday Times (UK)
Police to get phone hacking powers
Sunday, 13 March 2016
Byline: Mark Hookham

London - Police and intelligence agencies will be able to hack into people's mobile phones, tablets and computers using "backdoor" technology, which the government will force firms to install under proposed laws.
According to documents published in the past two weeks, internet service providers and technology giants would be obliged to build secret security flaws into their technology to allow them to be accessed by police and the security services on demand.

This would enable the authorities in Britain to do what the FBI has been unable to do in the US in its attempts to force Apple to give it access to the iPhone of the terrorist Syed Farook, who, with his wife, killed 14 people in California in December.

The FBI won a court order requiring Apple to help it bypass encryption and passcodes on the device but the company is challenging it.

The move threatens to provoke a huge row with the world's biggest tech firms. An executive at one leading company said this weekend: "People shouldn't be in any doubt, the government is pushing for some of the most invasive surveillance legislation out there today.

"The government wants to force companies to build in weaknesses and back doors into security systems when we're seeing the threat of hacking and cyber-crime getting worse.

"Given how much of our personal information is stored online or on phones, people should be worried about it."

The draft code of practice published alongside the government's Investigatory Powers Bill would also gag technology giants such as Apple and Google and broadband providers by banning them from revealing if they had been asked to install the back-door technology.

Ministers are even offering to use taxpayers' cash to help firms such as Apple, Facebook and Google pay for the extra costs of building a back door into messaging systems such as WhatsApp, FaceTime, iMessage or Google Hangouts.

Eric King, the director of Don't Spy On Us, a coalition of human rights groups, said this weekend the scale of the Home Office's proposals were "staggering" and would give security agencies access to "hugely intrusive capabilities".

Details of the measures are outlined in the 83-page draft code that accompanies the government's controversial Investigatory Powers Bill.

The code of practice states that the home secretary will have the power to impose a "technical capability notice" on "communication service providers".

This would force firms to provide the "technical capability" to allow the security services to access communication data as well as to undertake "interception" and "equipment interference".

The bill allows the home secretary to order the removal of "electronic protection", which technology companies claim means encryption.

The notices could be served on any firm with more than 10,000 users that provides a "telecommunication service" to UK customers, which includes phone and internet providers and technology giants that provide messaging services.

In addition, in a power similar to a legal superinjunction, companies served with notices are "under a duty not to disclose the existence and contents of that notice to any person" without the permission of the home secretary.

Failing to comply with a "technical capability notice" would be a breach of civil law.

A judge is not required to serve a technical capability notice, although a firm could force the home secretary to consult the "investigatory powers commissioner" if they oppose the notice. Once imposed, a notice must be reviewed at least once every two years.

The Home Office said the new bill "does not change the current position that companies above a certain size can be required to maintain a permanent interception capability".

Times of India
Pak hacker defaces Raipur AIIMS site, says all Indian governement sites on target
Monday, 14 March 2016
Byline: Rashmi Drolia

Raipur - Pakistani hackers on Saturday defaced the official website of AIIMS Raipur. While AIIMS administration wasn't aware about this till late in the evening, the site was patched till Sunday morning. The homepage of www.aiimsraipur.nic.in was hacked and displayed "Website stamped by Kashmiri Cheeta, Team: Pak Cyber Attackers. We are unbeatable. Mess with the Best, Die like the Rest."

Posting the mirror link on his Facebook wall, the hacker whose handle name is Amir Muzaffar virtually known as 'Kashmiri Cheetah', confirmed that he had hacked the website.

In an exclusive talk with TOI, the Pak hacker warned that "all government sites are on our target and we search sites with '.nic or .gov.in' keywords, and once we find a security lapse, you know what happens. Administrators of government websites are sloppy and rely blindly on white hat hackers whose job is to simply alert them about where the bugs are. They should not forget that there are black hat hackers too who also know where the bugs are and how to spread them to shut the sites down."

The black hat hacker Amir Muzaffar added that if Pak hackers want, they can destroy important files, but that's not in their ethics as of now.

Claiming to have hacked another Indian government's site parallel while talking to TOI he said, "I spotted many vulnerable sites including AIIMS Raipur and defaced it. Though the institute might claim to have recovered it but they have actually redirected it to AIIMS.edu but haven't patched the bugs. It would take five minutes for me to deface it again." he said.

Member of infamous Pak Cyber Attackers group, Amir says he hails from "Kashmir, Pakistan" and does hacking for alerting government about how vulnerable they are to us, if it's 'pk' or India (Pakistani site or Indian) doesn't matter.

Though he doesn't do it for fun he said, "it's for fake fame and a fake Cyber name, otherwise I love India." TOI in its reports had alerted and quoted Pak hacker Faisal Afzal that Pak hackers had launched cyber war against Indian sites. Amir has tagged Afzal in most of his posts on FB.

Earlier, calling it a cyber war against India and mocking at Prime Minister Narendra Modi's newly launched Digital India week, Pak hackers in 2015 had hacked 24 government websites at one go and twice the sites of NIT and PTRSU. Many websites of Kerala government and Gujarat were also hacked by same groups.

Indian hackers in retaliation had hacked around 250 important websites of Pakistan government including Pak telecom authority and others. AIIMS authority has been alerted and they said that the site was now safe.

Hactivist (white hat hacker) Mohit Sahu said that "AIIMS has a clone site to which they have redirected but yes, it's still vulnerable. For PCA boys it's like a game. Amir's Facebook wall shows that he has hacked many Indian sites even emails of government officials whose password he had revealed on the page. They keep challenging each other to hack more."

"Government or any agency before launching unique online schemes/services needs to be alert and 100 percent secure, else future of cyber world could be defeating," Mohit added.

Le Devoir
Un policier de Laval accusé d'utilisation frauduleuse d'une banque de données
Monday, 14 March 2016
Byline: Marie-Michèle Sioui

Montréal - Un nouveau procès concernant le recours frauduleux à une banque de données utilisée par les forces policières s'ouvre ce lundi au palais de justice de Laval et cette fois, c'est l'ex-policier de Laval Yves Smagghe qui est soupçonné d'avoir recherché des informations sur des citoyens pour servir ses fins personnelles.
Le policier de 46 ans, dont le départ a été confirmé le 18 novembre 2015, est of ficiellement accusé d' « utilisation non autorisée d'un ordinateur » , un acte criminel passible d'un emprisonnement maximal de dix ans. On reproche à Yves Smagghe d'avoir consulté le Centre de renseignements policiers du Québec (CRPQ), notamment pour obtenir des informations sur des locataires potentiels, selon ce qu'a appris Le Devoir.

Données confidentielles

Le Directeur des poursuites criminelles et pénales n'a pu donner de détails sur la nature des faits reprochés à l'ex-policier. Mais il a confirmé qu'une utilisation abusive du CRPQ constitue une infraction à l'arti-

cle 342.1 du Code criminel, article qui concerne l' « utilisation non autorisée d'un ordinateur » .

Le CRPQ est une banque de données confidentielles qui regroupe l'ensemble des renseignements informatisés -- à caractère criminel et non criminel -- que les policiers peuvent utiliser dans le cadre de leurs fonctions. Il contiendrait quelques millions de dossiers et sa consultation est strictement limitée au travail policier.

Selon nos sources, Yves

Smagghe en aurait fait une utilisation abusive, et ce, entre novembre 2007 et septembre 2012. Son procès doit commencer ce lundi au palais de justice de Laval et il devrait permettre d'en apprendre davantage sur les motivations de l'ex-policier, qui gère aujourd'hui Oasis Montebello, une vaste propriété située sur le golf du Château Montebello et pouvant être louée par le public.

Exemples récents d'utilisation frauduleuse

Décembre 2015 Le policier de Québec Jean-Bernard Lajoie est mis en accusation pour trafic de cocaïne et, entre autres infractions, pour avoir accédé de manière non autorisée au CRPQ.

Novembre 2015 Philippe Bonenfant, du SPVM, est accusé de trafic de stupéfiants et d'utilisation frauduleuse d'un ordinateur, encore pour consulter le CRPQ.

Novembre 2015 La policière de la Sûreté du Québec MariePierre Tremblay plaide coupable d'abus de confiance, d'entrave à la justice, de possession et de trafic de drogue. Elle aurait consulté le CRPQ pour transmettre des informations à son conjoint, le trafiquant de drogue Keven Harvey-Maltais.

2000 L'inspecteur-chef responsable des enquêtes criminelles à la police de Laval, Ronald Montpetit, quitte ses fonctions après avoir mené illégalement des vérifications dans le CRPQ à propos de personnes ayant postulé pour travailler au complexe Tops, qui appartenait à Tony Accurso.

New York Times
WhatsApp Encryption Said to Stymie Wiretap Order
Sunday, March 13, 2016
Byline: Matt Apuzzo

Washington - While the Justice Department wages a public fight with Apple over access to a locked iPhone, government officials are privately debating how to resolve a prolonged standoff with another technology company, WhatsApp, over access to its popular instant messaging application, officials and others involved in the case said.
No decision has been made, but a court fight with WhatsApp, the world's largest mobile messaging service, would open a new front in the Obama administration's dispute with Silicon Valley over encryption, security and privacy.

WhatsApp, which is owned by Facebook, allows customers to send messages and make phone calls over the Internet. In the last year, the company has been adding encryption to those conversations, making it impossible for the Justice Department to read or eavesdrop, even with a judge's wiretap order.

As recently as this past week, officials said, the Justice Department was discussing how to proceed in a continuing criminal investigation in which a federal judge had approved a wiretap, but investigators were stymied by WhatsApp's encryption.

The Justice Department and WhatsApp declined to comment. The government officials and others who discussed the dispute did so on condition of anonymity because the wiretap order and all the information associated with it were under seal. The nature of the case was not clear, except that officials said it was not a terrorism investigation. The location of the investigation was also unclear.

To understand the battle lines, consider this imperfect analogy from the predigital world: If the Apple dispute is akin to whether the F.B.I. can unlock your front door and search your house, the issue with WhatsApp is whether it can listen to your phone calls. In the era of encryption, neither question has a clear answer.

Some investigators view the WhatsApp issue as even more significant than the one over locked phones because it goes to the heart of the future of wiretapping. They say the Justice Department should ask a judge to force WhatsApp to help the government get information that has been encrypted. Others are reluctant to escalate the dispute, particularly with senators saying they will soon introduce legislation to help the government get data in a format it can read.

Whether the WhatsApp dispute ends in a court fight that sets precedents, many law enforcement officials and security experts say that such a case may be inevitable because the nation's wiretapping laws were last updated a generation ago, when people communicated by landline telephones that were easy to tap.

"The F.B.I. and the Justice Department are just choosing the exact circumstance to pick the fight that looks the best for them," said Peter Eckersley, the chief computer scientist at the Electronic Frontier Foundation, a nonprofit group that focuses on digital rights. "They're waiting for the case that makes the demand look reasonable."

A senior law enforcement official disputed the notion that the government was angling for the perfect case and that a court fight was inevitable.

This is not the first time that the government's wiretaps have been thwarted by encryption. And WhatsApp is not the only company to clash with the government over the issue. But with a billion users and a particularly strong international customer base, it is by far the largest.

Last year, a dispute with Apple over encrypted iMessages in an investigation of guns and drugs, for instance, nearly led to a court showdown in Maryland. In that case, as in others, the company helped the government where it was able to, and the Justice Department backed down.

Jan Koum, WhatsApp's founder, who was born in Ukraine, has talked about his family members' fears that the government was eavesdropping on their phone calls. In the company's early years, WhatsApp had the ability to read messages as they passed through its servers. That meant it could comply with government wiretap orders.

But in late 2014, the company said that it would begin adding sophisticated encoding, known as end-to-end encryption, to its systems. Only the intended recipients would be able to read the messages.

"WhatsApp cannot provide information we do not have," the company said this month when Brazilian police arrested a Facebook executive after the company failed to turn over information about a customer who was the subject of a drug trafficking investigation.

The iPhone case, which revolves around whether Apple can be forced to help the F.B.I. unlock a phone used by one of the killers in last year's San Bernardino, Calif., massacre, has received worldwide attention for the precedent it might set. But to many in law enforcement, disputes like the one with WhatsApp are of far greater concern.

For more than a half-century, the Justice Department has relied on wiretaps as a fundamental crime-fighting tool. To some in law enforcement, if companies like WhatsApp, Signal and Telegram can design unbreakable encryption, then the future of wiretapping is in doubt.

"You're getting useless data," said Joseph DeMarco, a former federal prosecutor who now represents law enforcement agencies that filed briefs supporting the Justice Department in its fight with Apple. "The only way to make this not gibberish is if the company helps."

"As we know from intercepted prisoner wiretaps," he added, "criminals think that advanced encryption is great."

Businesses, customers and the United States government also rely on strong encryption to help protect information from hackers, identity thieves and foreign cyberattacks. That is why, in 2013, a White House report said the government should "not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption."

In a twist, the government helped develop the technology behind WhatsApp's encryption. To promote civil rights in countries with repressive governments, the Open Technology Fund, which promotes open societies by supporting technology that allows people to communicate without the fear of surveillance, provided $2.2 million to help develop Open Whisper Systems, the encryption backbone behind WhatsApp.

Because of such support for encryption, Obama administration officials disagree over how far they should push companies to accommodate the requests of law enforcement. Senior leaders at the Justice Department and the F.B.I. have held out hope that Congress will settle the matter by updating the wiretap laws to address new technology. But the White House has declined to push for such legislation. Josh Earnest, the White House spokesman, said on Friday that he was skeptical "of Congress's ability to handle such a complicated policy area."

James B. Comey, the F.B.I. director, told Congress this month that strong encryption was "vital" and acknowledged that "there are undoubtedly international implications" for the United States to try to break encryption, especially for wiretaps, as in the WhatsApp case. But he has called for technology companies and the government to find a middle ground that allows for strong encryption but accommodates law enforcement efforts. President Obama echoed those remarks on Friday, saying technology executives who were "absolutist" on the issue were wrong.

Those who support digital privacy fear that if the Justice Department succeeds in forcing Apple to help break into the iPhone in the San Bernardino case, the government's next move will be to force companies like WhatsApp to rewrite their software to remove encryption from the accounts of certain customers. "That would be like going to nuclear war with Silicon Valley," said Chris Soghoian, a technology analyst with the American Civil Liberties Union.

That view is one reason government officials have been hesitant to rush to court in the WhatsApp case and others like it. The legal and policy implications are great. While no immediate resolution is in sight, more and more companies offer encryption. And technology analysts say that WhatsApp's yearlong effort to add encryption to all one billion of its customer accounts is nearly complete.

Yonhap English News

Foreign Ministry instructs overseas missions to strengthen cybersecurity

Tuesday, 15 March 2016

Byline: Staff reporter

Section: general

Seoul - South Korea's Foreign Ministry has instructed its overseas missions to strengthen their cybersecurity amid growing threats of online attacks from North Korea, officials said Tuesday. The move came as the South Korean military and government agencies have striven to counter the North's potential attacks in cyberspace by strengthening its readiness posture and interagency cooperation.

"After a cyber crisis alert was issued last month, we have instructed all our missions abroad to enhance their cybersecurity," a ministry official said, declining to be named.

The North recently attempted to hack the smartphones of South Korean military commanders and top government officials responsible for national security, according to the South's National Intelligence Service.

To better cope with the growing threats, the government raised its five-stage cyber alert level to the third highest level of "caution" last month.

On Tuesday, the ministry held a meeting on cybersecurity with its subordinate organizations such as the Korea National Diplomatic Academy, the Korea Foundation and the Korea International Cooperation Agency.

At the meeting, presided over by Kim Hyoung-zhin, the ministry's deputy minister for political affairs, officials discussed joint responses to the threats, the ministry explained.

Toronto Star

Ottawa in Internet dark ages

Tuesday, 15 March 2016

Byline: Alex Boutilier

Section: general

OTTAWA -- The federal government is lagging behind both private sector offerings and Canadians' expectations in online services, internal documents warn.
A full 77 per cent of federal services still cannot be completed over the Internet, documents prepared for Treasury Board President Scott Brison show.

"Government is not doing a good enough job of meeting the needs and expectations of citizens for quality, accessible services," the documents, obtained by the Star under Access to Information law, read.

"Fifteen years ago, Canada placed first worldwide in e-government services; today the UN e-government survey ranks Canada as 11th."

Services such as passport applications, requesting access to government information, or obtaining proof of citizenship all require in-person treks to Service Canada locations or mailed application forms.

A minority of services, like filing taxes or updating pension information, can be done online through government websites.

Canadians grumbling about the provision of government services is, of course, not a new development in the Internet age. However, the documents state that the private sector's online offerings have increased Canadians' expectations on the speed and ease of obtaining services.

In addition to raised expectations, the documents note that it takes a long time for the sprawling federal bureaucracy to implement changes in how it delivers services.

The average time between implementing a budget decision, for instance, is 15 months between the announcement and the execution.

These factors have resulted in a situation where the federal government is failing to "keep pace" with technological developments.

"The private sector is moving toward a digital experience, even within bricks- and-mortar establishments," the documents read.

"(But) the 2013 (auditor general) audit on access to online services found that the (government) had not significantly expanded its online services offerings since 2005."

In an interview Friday, Brison acknowledged that "enterprisewide" tech solutions are difficult - whether for large companies or for governments. But he said the government must get better at offering services online.

"We need to move forward and modernize our services to Canadians, and be able to offer better services in real-time at better value for taxpayers," Brison said in an interview with the Star.

Since assuming his post as Treasury Board president, and responsibility for the federal government's overall service standards and policies, Brison has talked about the need for a culture change in the public service to be more nimble, free with information, and modern.

Brison also recently told the Ottawa Citizen that the federal public service needs an infusion of young blood - more digital-savvy, innovative generation of bureaucrats with fresh ideas.

"It's much easier to build a modern, digital government if you engage the modern, digital generation," Brison said. "This is the generation that has grown up digital. And we are never going to be able to render government digital without their engagement."

But if it were easy to bring the federal government completely online, it probably would have been done already. Brison's briefing materials detail a number of barriers to making more federal services onto the Internet. "Legislative and technological barriers inhibit sharing of information for service innovation ... (and the) potential for dynamic (government-wide) service delivery is unrealized due to untapped business intelligence," the documents read.

Still, some federal agencies have had success moving traditional pen-and-paper services online - for instance, the Canada Revenue Agency's push to get more people filing their taxes online.

The new Liberal government will have to figure out a way to bring about more widespread changes, however, if they plan to make good on their campaign pledge to create a one-stop Internet portal for federal services.

External Pressures on Government 2.0

Disruption: According to Brison's briefing notes, part of the problem is that the way information is transmitted is changing - and old institutions like newspapers, network television and professional experts are being challenged by social media, Netflix, and Google.

Speed: With those changes, information is moving at a much quicker speed - you don't have to wait for the evening news or for expert opinion to form an opinion. "A superabundance of information has led to a scarcity of attention," Brison's briefing notes read.

Authority: The transformation of those traditional pillars, however, brings with it a crisis of authority. Treasury Board notes that citizens are increasingly skeptical - or at least less deferential - to "experts" or those perceived to be "in charge."

Communication: This presents its own challenges for governments to get their message across or market their services. Information, in real-time, is often unfiltered.

The Guardian (London)

Investigatory powers bill not fit for purpose, say 200 senior lawyers

Tuesday, 15 March 2016

Byline: Owen Bowcott

Section: general

London - The investigatory powers bill, which goes before MPs on Tuesday, is not fit for purpose and breaches international standards on surveillance, according to a letter signed by more than 200 senior lawyers.
The legislation acknowledges for the first time the extent of bulk interception and hacking carried out by the government's monitoring agency, GCHQ, and sets out a legal framework with safeguards.

In a letter to the Guardian, however, the complex and controversial bill is condemned by former judges, QCs, law professors and senior lawyers as being fundamentally flawed because it destroys privacy.

Among those who have signed are the chair of the Bar Human Rights Committee Kirsty Brimelow QC, Tom de la Mare QC, who has been a special advocate in security cases, Sir Stephen Sedley, who is a former court of appeal judge, Prof Sir Geoffrey Bindman QC, Hugh Southey QC, Michael Mansfield QC and Philippe Sands QC. Among academic lawyers, there are representatives of nearly 40 law schools in the UK.

One of the key differences between the government and its critics is whether bulk interception of emails and digital records constitutes mass surveillance and breach of privacy.

GCHQ argues that it only carries out targeted searches of data under legal warrants in pursuit of terrorist or criminal activity and that bulk interception is necessary as a first step in that process; other intercepted material, it insists, is never read.

But the United Nations special rapporteur on privacy, Joseph Cannataci, last week criticised the investigatory powers bill saying that authorising bulk interception would legitimise mass surveillance.

The letter coincides with the second reading of the bill. "A law that gives public authorities generalised access to electronic communications contents compromises the essence of the fundamental right to privacy and may be illegal," it declares.

"The investigatory powers bill does this with its 'bulk interception warrants' and 'bulk equipment interference warrants'." The bill also permits "targeted interception warrants" to apply to groups, persons organisations or premises, the letter notes.

The bill also fails to mention "reasonable suspicion" - or even suspects - and there is no need to demonstrate criminal involvement or a threat to national security, the letters adds.

"These are international standards found in the recent opinion of the UN special rapporteur for the right to privacy, and in judgments of the EU court of justice and the European court of human rights," it continues. "At present, the bill fails to meet these standards - the law is unfit for purpose."

James Blessing, chair of the UK Internet Service Providers' Association, said: "[We] support reform of investigatory powers through a new bill, but we are a long way from having a bill that is clear and workable.

"Government needs to address concerns around its intentions, definitions and costs to enable industry to make a proper assessment of the bill and help arliament scrutinise the complex proposals. Getting this right is essential for the UK digital economy and user trust in services."

Eric King, director of Don't Spy On Us, said: "The government's approach to this important reform has been wrong from the very beginning: they've sought to make bad habits lawful, rather that chart a new and legitimate course for the future.

"The fact so many of the bill's key provisions fall short of international standards cannot simply be pushed aside. A full redraft of this flawed bill is needed for it to stand the test of time. Anything less is simply a waste of parliament's time."

Labour has said it will abstain in Tuesday's vote, but the Liberal Democrats and the SNP will oppose the government's bill.

Reuters

Chinese hackers behind U.S. ransomware attacks - security firms

Tuesday, 15 March 2016

Byline: Joseph Menn

Section: general

San Francisco - Hackers using tactics and tools previously associated with Chinese government-supported computer network intrusions have joined the booming cyber crime industry of ransomware, four security firms that investigated attacks on U.S. companies said.
Ransomware, which involves encrypting a target's computer files and then demanding payment to unlock them, has generally been considered the domain of run-of-the-mill cyber criminals.

But executives of the security firms have seen a level of sophistication in at least a half dozen cases over the last three months akin to those used in state-sponsored attacks, including techniques to gain entry and move around the networks, as well as the software used to manage intrusions.

"It is obviously a group of skilled of operators that have some amount of experience conducting intrusions," said Phil Burdette, who heads an incident response team at Dell SecureWorks.

Burdette said his team was called in on three cases in as many months where hackers spread ransomware after exploiting known vulnerabilities in application servers. From there, the hackers tricked more than 100 computers in each of the companies into installing the malicious programs.

The victims included a transportation company and a technology firm that had 30 percent of its machines captured.

Security firms Attack Research, InGuardians and G-C Partners, said they had separately investigated three other similar ransomware attacks since December.

Although they cannot be positive, the companies concluded that all were the work of a known advanced threat group from China, Attack Research Chief Executive Val Smith told Reuters.

The ransomware attacks have not previously been reported. None of the companies that were victims of the hackers agreed to be identified publicly.

The security companies investigating the advanced ransomware intrusions have various theories about what is behind them, but they do not have proof and they have not come to any firm conclusions.

Most of the theories flow from the possibility that the Chinese government has reduced its support for economic espionage, which it pledged to oppose in an agreement with the United States late last year. Some U.S. companies have reported a decline in Chinese hacking since the agreement.

Smith said some government hackers or contractors could be out of work or with reduced work and looking to supplement their income via ransomware.

It is also possible, Burdette said, that companies which had been penetrated for trade secrets or other reasons in the past were now being abandoned as China backs away, and that spies or their associates were taking as much as they could on the way out. In one of Dell's cases, the means of access by the team spreading ransomware was established in 2013.

The cyber security experts could not completely rule out more prosaic explanations, such as the possibility that ordinary criminals had improved their skills and bought tools previously used only by governments.

Dell said that some of the malicious software had been associated by other security firms with a group dubbed Codoso, which has a record of years of attacks of interest to the Chinese government, including those on U.S. defense companies and sites that draw Chinese minorities.

PAYMENT IN BITCOIN

Ransomware has been around for years, spread by some of the same people that previously installed fake antivirus programs on home computers and badgered the victims into paying to remove imaginary threats.

In the past two years, better encryption techniques have often made it impossible for victims to regain access to their files without cooperation from the hackers. Many ransomware payments are made in the virtual currency Bitcoin and remain secret, but institutions including a Los Angeles hospital have gone public about ransomware attacks.

Ransomware operators generally set modest prices that many victims are willing to pay, and they usually do decrypt the files, which ensures that victims will post positively online about the transaction, making the next victims who research their predicament more willing to pay.

Security software companies have warned that because the aggregate payoffs for ransomware gangs are increasing, more criminals will shift to it from credit card theft and other complicated scams.

The involvement of more sophisticated hackers also promises to intensify the threat.

InGuardians CEO Jimmy Alderson said one of the cases his company investigated appeared to have been launched with online credentials stolen six months earlier in a suspected espionage hack of the sort typically called an Advanced Persistent Threat, or APT.

"The tactics of getting access to these networks are APT tactics, but instead of going further in to sit and listen stealthily, they are used for smash-and-grab," Alderson said.

Reuters

Apple fight could escalate with demand for 'source code'

Tuesday, 15 March 2016

Byline: Staff report

Section: general

San Francisco - The latest filing in the legal war between the planet's most powerful government and its most valuable company gave one indication of how the high-stakes confrontation could escalate even further.
In what observers of the case called a carefully calibrated threat, the U.S. Justice Department last week suggested that it would be willing to demand that Apple turn over the "source code" that underlies its products as well as the so-called "signing key" that validates software as coming from Apple.

Together, those two things would give the government the power to develop its own spying software and trick any iPhone into installing it. Eventually, anyone using an Apple device would be unable to tell whether they were using the real thing or a version that had been altered by officials to be used as a spy tool.

Technology and security experts said that if the U.S. government was able to obtain Apple's source code with a conventional court order, other governments would demand equal rights to do the same thing.

"We think that would be pretty terrible," said Joseph Lorenzo Hall, chief technologist at the nonprofit Center for Democracy & Technology.

The battle between Apple and the U.S Justice Department has been raging since the government in February obtained a court order demanding that Apple write new software to help law enforcement officials unlock an iPhone associated with one of the shooters in the December attack in San Bernardino, California that killed 14 people.

Apple is fighting the order, arguing that complying with the request would weaken the security of all iPhones and create an open-ended precedent for judges to make demands of private companies.

The Justice Department's comments about source code and signing keys came in a footnote to a filing last week in which it rejected Apple's arguments. Apple's response to the DOJ brief is expected on Tuesday.

Justice Department lawyers said in the brief that they had refrained from pursuing the iOS source code and signing key because they thought "such a request would be less palatable to Apple. If Apple would prefer that course, however, that may provide an alternative that requires less labor by Apple."

The footnote evoked what some lawyers familiar with the case call a "nuclear option," seeking the power to demand and use the most prized assets of lucrative technology companies.

A person close to the government's side told Reuters that the Justice Department does not intend to press the argument that it could seize the company's code, and someone on Apple's side said the company isn't worried enough to counter the veiled threat in its brief due Tuesday.

But many people expect the iPhone matter to reach the U.S. Supreme Court, and thus even fallback legal strategies are drawing close scrutiny.

ODDS OF SUCCESS UNCLEAR

There is little clarity on whether a government demand for source code would succeed.

Perhaps the closest parallel was in a case filed by federal prosecutors against Lavabit LLC, a privacy-oriented email service used by Edward Snowden. In trying to recover Snowden's unencrypted mail from the company, which did not keep Snowden's cryptographic key, the Justice Department got a court order forcing the company to turn over another key instead, one that would allow officials to impersonate the company's website and intercept all interactions with its users.

"Lavabit must provide any and all information necessary to decrypt the content, including, but not limited to public and private keys and algorithms," the lower court ruled.

Lavabit shut down rather than comply. But company lawyer Jesse Binnall said the Fourth Circuit Court of Appeals, which upheld the lower ruling, did so on procedural grounds, so that the Justice Department's win would not influence much elsewhere.

In any case, full source code would be even more valuable than the traffic key in the Lavabit case, and the industry would go to extreme lengths to fight for it, Binnall said.

"That really is the keys to the kingdom," Binnall said.

Source code is sometimes inspected during lawsuits over intellectual property, and the Justice Department noted that Apple won permission to review some of rival Samsung's (005930.KS) code in one such case. In that case and similar battles, the code is produced with strict rules to prevent copying.

No cases brought by the government have led to that sort of code production, or at least none that have come to light.

But intelligence agencies operate under different rules and have wide latitude overseas. Some advanced espionage programs attributed to the United States used digital certificates that were stolen from Taiwanese companies, though not full programs.

U.S. software code may have been sought in other cases, such as investigations relying on the Patriot Act or the Foreign Intelligence Surveillance Act (FISA), which applies within American borders.

Several people who have argued before the special FISA court or are familiar with some of its cases say they know of no time that the government has sought source code.

Wall Street Journal

Google Faces Challenges in Encrypting Android Phones

Tuesday, 15 March 2016

Byline: Jack Nicas

Section: general

New York - Had San Bernardino shooter Syed Rizwan Farook used an Android phone, investigators would have had a better chance at accessing the data. The reason? Few Android phones are encrypted. Google, Android's maker, doesn't want it that way. The Alphabet Inc. unit has pushed encryption for Android phones and automatically encrypts its own line of Nexus devices.

But other handset makers have resisted because they are concerned that encryption -- scrambling data such as contacts, photos and videos -- hurts a phone's performance. And Google hasn't insisted for fear of driving device makers away from the official Android model, where it makes the most money.

The result: Experts estimate fewer than 10% of the world's 1.4 billion Android phones are encrypted, compared with 95% of Apple Inc.'s iPhones. That includes Mr. Farook's iPhone, now the center of a high-stakes clash between Apple and the U.S. government that raises questions about privacy and security in the digital age.

The disparity between the two dominant mobile-operating systems underscores Google's challenge in corralling the sprawling Android network of more than 400 manufacturers and 4,000 devices.

Google gives away its Android software to attract more users to its services. Google requires device makers to comply with certain requirements to use the Android brand and key Google services such as search and maps. Ultimately, though, device makers are free to use the software as they wish.

Apple, by contrast, controls both the hardware and software on iPhones. It prods users to adopt the latest version of its iOS software, fueling the spread of encryption.

"There is a push and pull with what Google wants to mandate and what the [manufacturers] are going to do," said Andrew Blaich, lead security analyst at Bluebox Security Inc., which helps secure mobile apps. In some ways, Google is "at the mercy of the larger (manufacturers) like Samsung and LG that are driving the ecosystem."

When phones aren't encrypted, law enforcement can more easily view their contents. Authorities use specialized software to crack passcodes on locked -- but unencrypted -- Android devices in about an hour, said an investigator for France's Gendarmerie Nationale. The Manhattan district attorney said in November that investigators can bypass passcodes on some older Android devices, while Google can remotely reset passcodes on others.

Google is pushing harder on device makers. Its latest version of Android -- dubbed 6.0, or Marshmallow -- requires device makers to encrypt phones that contain high-powered processors. As a result, higher-end Android phones released this year and beyond will come encrypted.

Still just 2.3% of Android devices now run Marshmallow, which was released in October. By contrast, 79% of iPhones run Apple's iOS 9, which was released in September, according to company statistics.

Ken Hong, a spokesman for LG Electronics Inc., one of the largest makers of Android phones, said many devices aren't updated to new versions of Android because manufacturers must tweak the software for each phone model, and each wireless carrier. Manufacturers typically update only their more-expensive models.

LG and HTC Corp. said many of their 2016 phones will be encrypted. A spokesman for Samsung Electronics Co., the world's leading maker of Android phones, said its new Galaxy S7 phone is encrypted but declined to comment on other devices.

"If there was encryption that didn't affect usability and performance, then I can't imagine anyone not wanting to include that feature," said Mr. Hong.

Google accelerated its encryption push in September 2014, saying it would require a new phone running the then-latest version of Android, dubbed Lollipop, to be encrypted "from the first time you turn it on." The announcement came days after Apple said it would begin encrypting iPhones.

Before making its pledge, Google said it tested several encrypted phones, and found little impact on performance. But device-makers' tests showed encryption caused seconds-long delays when launching apps on some low-end devices, Google said. In response, Google halted the encryption mandate.

Android security chief Adrian Ludwig said the company aims to eventually mandate encryption on all Android devices as components get less expensive.

Google's ability to push security on handset makers is complicated because it gives Android away free. Some device makers have created their own versions of Android, which don't use Google services such as search, that generate most of the company's revenue. Google doesn't want to drive away other device makers.

For instance, Mr. Ludwig said that when Google announced its plan to require encryption in late 2014, device makers already were manufacturing low-end devices that perform slowly when encrypted. Companies likely would have shifted those devices away from the official version of Android if Google had kept the requirement, he noted.

The Register (UK)

Only 12% of UK thinks Snoopers' Charter is 'adequately explained'

Monday, 14 March 2016

Byline: Alexander J. Martin

Section: general

London - Only 12 per cent of the British public believe the Home Secretary has "adequately explained the impact of the Investigatory Powers Bill to the UK public and presented a balanced argument for its introduction".
A survey on data privacy issues conducted by Open-Xchange has found that the "internet-savvy" public in the UK, Germany and the US are increasingly interested in policies affecting the online realm.

As Rafael Laguna, CEO at Open-Xchange, which conducted the Consumer Openness Index, told The Register: "We see there's an increased sensitivity towards data privacy and data topics, although of course different countries have different hot topics."

Debates regarding the UK's Investigatory Powers Bill, and the conflict between the FBI and Apple in the US, "have influenced people quite a bit, and they have developed stronger opinions."

Forty-six per cent of those surveyed in the UK said they paid somewhat close attention or more to the debate over balancing government surveillance with data privacy. This compares with 56 per cent in the US, and 75 per cent in Germany.

Historical national differences are lessening, however. While Germans were typically the most concerned about privacy issues, considering the partitioning of the country and the legacy of the Nazis and the Stasi, overall public opinion is becoming more similar, suggested Laguna.

In some respects, however, the UK remains more conservative than its left-and-right hand kin, with 33 per cent thinking national security was more important for the government to protect than the right to personal privacy at 11 per cent.

Only 12 per cent of the British public, however, believed the Home Secretary, Theresa May, "has adequately explained the impact of the Investigatory Powers Bill to the UK public and presented a balanced argument for its introduction".

Fifty-three per cent said they did not believe this, while 35 per cent were unsure.

The public is becoming more opinionated and more aware, said Laguna, who said Open-Xchange was hoping to raise that awareness and receive tangible statement from the government.

Fifty per cent of the British public believed that "making personal data easier for government officials to access will also make it easier for criminals to access that data as well", while only six per cent disagreed.

Laguna, who was raised in East Germany under the watch of the Stasi, said: "Everybody in the IT industry understands that there is no such thing as 'weakened encryption', there is either encryption or no encryption. I would wish the government would accept the statements of the experts and say 'We won't try to weaken encryption' and 'Of course, you can't outlaw maths, so we're not trying to do that either'."

Half of respondents said they thought the Investigatory Powers Bill's provisions regarding encryption infringed on the British public's right to privacy. Only 10 per cent thought it would not make investment in the UK less attractive to foreign companies.

"These discussions are raising awareness, and that's always the start of changing opinions," said Laguna.

Le Devoir

Données à la frontière - Plus qu'un enjeu de sécurité

Tuesday, 15 March 2016

Byline: Manon Cornellier

Section: editorial

Editorial - Depuis au moins quatre ans, Ottawa et Washington s'affairent à établir un programme d'échanges de données sur les entrées et sorties de voyageurs. La mise en oeuvre au Canada a pris du retard, mais Ottawa s'est engagé la semaine dernière à terminer le travail dès que possible. Comme toujours, on avance l'argument de la sécurité pour justifier cette coopération, mais les données servent à d'autres fins et les échanges soulèvent des questions en matière de protection de la vie privée.
Les attentats du 11 septembre 2001 ont profondément changé la nature de la relation entre le Canada et les États-Unis. La sécurité est devenue un sujet incontournable, et l'idée d'un périmètre englobant les deux pays s'est imposée. En 2011, les deux pays ont publié une vision commune à ce sujet. Parmi les engagements du plan d'action qui en a découlé en décembre 2011 est apparue une initiative sur les entrées et les sorties des voyageurs.

L'idée est simple. Les deux pays échangent des données sur l'entrée des voyageurs sur leur territoire à la frontière terrestre, ce qui permet à chacun de savoir qui sort du sien. La première étape a permis d'expérimenter le système à quelques points d'entrée terrestres en ne ciblant que les voyageurs n'étant pas citoyens de l'un ou l'autre pays.

La deuxième phase, en vigueur depuis 2013, a étendu l'expérience à tous les points d'entrée terrestres automatisés sans viser les citoyens canadiens ni américains. Ces derniers devaient être ajoutés lors de la troisième phase qui tarde à entrer en vigueur. Quant à la quatrième phase, elle devait étendre les échanges à tous les voyageurs quittant le pays en avion. Les États-Unis récoltent déjà cette information, mais ce n'est toujours pas le cas au Canada.

Ce sont ces deux dernières étapes que le Canada s'engage maintenant à mettre en oeuvre. Ce qui exigera des modifications à des lois et à des règlements. Heureusement, car cela garantira au moins la tenue d'un débat plus que nécessaire au Parlement.

Ces échanges de données soulèvent des inquiétudes depuis le début. Pour s'y opposer, certains évoquent le cas de Maher Arar, bien que ce dernier ait été expulsé en Syrie sur la base d'informations fausses fournies par la GRC. D'autres craignent qu'on fouille dans le passé des gens pour leur interdire l'entrée.

Tel qu'il existe, le programme de suivi des entrées et sorties ne le permettrait pas. La liste des données partagées est limitée : nom, date de naissance, nationalité ou citoyenneté, sexe, information sur le document de voyage (numéro, type et pays de délivrance) et enfin la date, l'heure et le point d'entrée.

Mais que la liste soit courte ou non, des questions persistent au sujet de la protection de la vie privée, de l'échange avec des pays tiers et de l'utilisation des données à d'autres fins que la sécurité. Les gouvernements ne cherchent pas qu'à conjurer une menace terroriste ou à aider les services frontaliers à confirmer le départ de personnes faisant l'objet d'un ordre d'expulsion.

Le gouvernement fédéral envisage d'utiliser ces données pour assurer le respect de certaines lois, comme celles sur la citoyenneté et l'assurance- emploi ou pour vérifier l'admissibilité à certaines prestations. Le hic est qu'à la fin d'avril dernier, les ministères et agences qui prévoient utiliser ces données -- l'Agence des services frontaliers du Canada, l'Agence du revenu, le Service canadien du renseignement de sécurité (SCRS), Citoyenneté et Immigration, Emploi et Développement social et la Gendarmerie royale du Canada -- n'avaient toujours pas remis la nécessaire Évaluation des facteurs relatifs à la vie privée, indique le dernier rapport annuel du Commissaire à la vie privée déposé en décembre.

Le communiqué canadien publié après la visite officielle du premier ministre Justin Trudeau à Washington, la semaine dernière, se limite à dire que la poursuite de cette initiative se fera " en respectant nos cadres constitutionnels et juridiques respectifs et en protégeant le droit des citoyens à la vie privée ". Le communiqué américain ne souffle mot de cette préoccupation.

Un autre problème dont on parle peu est l'échange de données avec des pays tiers. Le Canada ne peut actuellement empêcher les États-Unis de partager celles qu'il leur fournit, même si les autorités américaines sont obligées de l'aviser d'un tel transfert.

Avant d'aller de l'avant, le gouvernement canadien doit mettre cartes sur table au sujet du transfert possible de données à un pays tiers, clarifier la véritable utilisation qu'il compte faire des données et exiger de tous les ministères qu'ils fassent leurs devoirs en matière de protection de la vie privée.

La Tribune (France)

Les élites politiques seraient-elles dépassées par le numérique?

Tuesday, 15 March 2016

Byline: Sylvain Rolland

Section: general

Non identifié - La révolution numérique, caractérisée par l'essor des nouvelles technologies et par la collecte et le traitement des données à grande échelle, bouleverse tous les secteurs. Dans un contexte de chômage de masse, elle pose des défis d'une ampleur inédite au personnel politique. Cette numérisation de la société et de l'économie laisse de côté une élite politique globalement dépassée. Sortis de leur zone de confort, les élus peinent toujours à comprendre et à penser les enjeux de transformation, ils apparaissent en décalage avec les entreprises et les citoyens. Qui s'impatientent. Attention, vous risquez d'y perdre votre latin. « L'algoriSme, c'est un ciblage, mais pas sur des individus : sur des modes de communication »... Mardi 12 mai 2015, palais du Luxembourg. Jean-Yves Le Drian disserte au Sénat sur la très technique loi Renseignement, qui sera adoptée deux mois plus tard. Mais le ministre de la Défense s'emmêle sérieusement les pinceaux. Non seulement l'élu socialiste peine à prononcer correctement le mot « algorithme », mais il patine aussi sur son sens. Car le mot, apparu dès le XIIIe siècle, désigne simplement une méthode de calcul par une suite d'opérations... Évidemment, la bourde ne passe pas inaperçue. Les geeks, les opposants à la loi Renseignement et autres spécialistes des nouvelles technologies se moquent copieusement sur les réseaux sociaux du ministre. Mais ils rient jaune. « Ce lapsus est inquiétant, car il symbolise le déficit de culture numérique d'une grande partie de la classe politique française », déplore un député... de la majorité, qui fait partie de « la trentaine » d'élus nationaux (gouvernement, députés et sénateurs de gauche et de droite) réputés pour leur maîtrise des enjeux numériques.

Depuis l'incident, le mot-dièse #algorisme est devenu une tendance sur Twitter. Il réapparaît à chaque itération d'inculture numérique de la part des élites. Rien n'aurait donc changé depuis 1996? À l'époque, le président Jacques Chirac demandait à quoi servait le « mulot » en désignant une souris d'ordinateur. Fin 2009, le député-maire de Maisons-Laffitte, Jacques Myard (LR), voulait très sérieusement « nationaliser Internet pour mieux le maîtriser » car il serait « pourri par les chevaux de Troie ».

Fort heureusement, la société a fait du chemin. Les politiques aussi. Désormais, beaucoup d'élus pianotent sur leur smartphone et utilisent Facebook et Twitter. En revanche, dès que les sujets se font plus techniques ou nécessitent une maîtrise plus poussée des enjeux, « il n'y a plus grand- monde », déplore Luc Bretones. « Le problème des politiques, c'est qu'ils sont très en retard par rapport aux citoyens et aux entreprises », ajoute le vice-président de l'institut G9+, un cercle de réflexion apolitique consacré à la transformation digitale. Il synthétise le sentiment ambiant : « Comment la France pourrait-elle tirer profit de la révolution numérique quand certains concepts de base, sans même parler de leurs enjeux énormes de transformation, ne sont toujours pas compris par nos responsables politiques? »

« Cette complexité, inédite, paralyse les politiques »

Ce cri du coeur est partagé par tous les experts du numérique, qu'ils soient citoyens, entrepreneurs, intellectuels, et même par les rares élus « éclairés ». Cette frustration se comprend, car le numérique a complètement envahi nos vies, à la fois dans la sphère privée et professionnelle.

Les nouvelles technologies, la collecte et l'analyse de données à grande échelle (le fameux big data), l'informatique en nuages (le cloud) et la généralisation d'Internet pour acheter, vendre et communiquer, transforment profondément la société et l'économie. Si bien que tous les secteurs sont touchés ou vont l'être. De la banque à la santé, en passant par le commerce, l'éducation, les médias, l'administration, la sécurité ou encore les transports, le numérique réinvente les métiers, en crée de nouveaux et impose une réorganisation profonde du travail, de la protection sociale et de la création de valeur. Ces chamboulements se traduisent par un besoin de réformes politiques majeures. De fait, les élus doivent à la fois encadrer cette nouvelle économie et adapter l'ancienne. Favoriser le développement des entreprises numériques tout en protégeant les citoyens, les travailleurs et les consommateurs. Un véritable casse-tête, comme le montre le tollé autour de la loi sur le travail de Myriam El Khomri, ou encore les tensions extrêmes entre Uber et les taxis, symbole de l'impact brutal du numérique sur les secteurs dits « traditionnels ».

Cette urgence de réformer apparaît d'autant plus cruciale dans un contexte de chômage de masse. De la capacité de la France et de l'Europe à saisir la révolution numérique dépendront leur souveraineté économique et politique, et leur croissance dans la décennie à venir, indique un rapport de 2014 des députées Corinne Erhel (PS) et Laure de La Raudière (LR).

« Le numérique est une révolution au sens historique du terme », résume Benoît Thieulin, patron de la société de communication digitale La Netscouade et ancien président du Conseil national du numérique (CNNum).

« Il ne peut plus se penser comme une thématique isolée et secondaire car il irrigue l'ensemble du champ de l'action publique. Cette complexité, inédite, paralyse les politiques, qui sont comme des poissons hors de l'eau », ajoute-t-il. »

Un handicap en partie générationnel

Selon lui, les élus n'ont pas encore pris conscience que désormais, toutes les décisions de politique publique intègrent un volet technologique. Réformer la retraite à points, par exemple, n'implique-t-il pas une question de capacité logicielle pour créer un système d'information capable de gérer le compte personnel d'activité?

On peut en partie expliquer ce décalage entre les élus et la société, théorisé par la journaliste Laure Belot dans son livre La Déconnexion des élites (Les Arènes, 2015) par la sociologie du personnel politique. L'âge moyen des parlementaires frôle les 60 ans.

Seuls 22 députés (sur 577) ont moins de 40 ans. En revanche, 266 dépassent la soixantaine... Une situation beaucoup plus marquée qu'en Allemagne, au Royaume-Uni ou aux États-Unis. S'il n'est pas indispensable d'être jeune pour comprendre le numérique, le manque de renouvellement ralentit la montée en compétence globale sur le sujet.

« Comme ils sont là depuis longtemps, beaucoup de politiques ont bâti leur notoriété et leur légitimité sur d'autres sujets. Ils tendent donc à traiter le numérique à la marge plutôt que de le placer au coeur de la problématique centrale de l'emploi, ce qui est une erreur », analyse Luc Bretones. »

L'homogénéité des profils des élus pose aussi problème. « La classe politique représente très mal la société française. Elle est plus vieille, plus masculine, plus blanche, plus fonctionnaire, peu au contact du monde de l'entreprise et des évolutions sociétales », note Benoît Thieulin. Conséquence : la culture numérique, de plus en plus marquée en entreprise et quasiment instinctive chez les Millennials (ceux qui sont nés entre 1980 et 2000), peine à se diffuser dans les rangs de l'Assemblée, du Sénat et du gouvernement.

« La dernière roue du carrosse gouvernemental »

Pour Élisabeth Grosdhomme-Lulin, inspectrice des finances et directrice générale de la société d'études et de conseil Paradigme et cætera, ce manque de littératie numérique, c'est-à-dire de culture du digital au sens large, est plus grave que l'absence criante d'élus spécialisés. « Dans une démocratie, ce ne sont pas les médecins qui font la politique de santé, ni les agriculteurs qui font la politique agricole, relève-t-elle. Le plus important, c'est que les représentants du peuple soient capables de prendre de la hauteur, ce qui n'est, globalement, pas encore le cas sur le numérique. »

Les élus eux-mêmes partagent ce diagnostic. « On est toujours dans le syndrome Hadopi », déplore la députée Laure de La Raudière (LR), en référence à la loi sur le téléchargement illégal, votée en 2009 et réputée pour son inefficacité. L'élue d'Eure-et-Loir remarque que ses congénères peinent à se départir de leurs « réflexes du XXe siècle ».

« On construit des digues de sable pour protéger l'Ancien Monde en espérant que ça marche, mais ça ne marche jamais », tacle-t-elle. »

L'essor de la French Tech depuis 2013, les moyens importants alloués au financement de l'innovation (création de Bpifrance, essor de Business France et du slogan Creative France...) montrent pourtant que le gouvernement s'applique à développer l'économie numérique. Mais son approche défensive vis-à-vis des nouveaux usages collaboratifs ainsi que sa volonté paradoxale de ne pas froisser les lobbies (taxis, hôtellerie, industrie musicale...) donnent le sentiment d'une politique incohérente et déconnectée des enjeux. Le grand écart entre un axe sécuritaire d'un côté (la loi Renseignement), libéral de l'autre (la promotion de l'entrepreneuriat, les lois Macron et El Khomri), et une approche protectionniste et sociale (la loi Lemaire) brouille le message. Enfin, le statut d'Axelle Lemaire, la secrétaire d'État au numérique, apparaît en décalage avec l'importance de son maroquin. Depuis le remaniement de février

dernier, l'élue des Français d'Amérique du Nord se classe à la 37e place sur 39 dans l'ordre protocolaire. « Le numérique est clairement la dernière roue du carrosse gouvernemental, déplore le directeur général d'une fédération professionnelle d'entreprises du digital. Il faudrait un ministre du Numérique doté d'un vrai poids politique, sous l'autorité directe du Premier ministre, avec un accès à l'Élysée et les moyens de gagner des arbitrages. Axelle Lemaire est extrêmement compétente, mais c'est un poids plume », poursuit-il.

La cocréation de la loi, une méthode plébiscitée

Bonne nouvelle : de plus en plus d'élus prennent conscience de la nécessité de monter en compétence sur ces sujets. À ce titre, la Loi pour une République numérique d'Axelle Lemaire, adoptée en première lecture par l'Assemblée nationale fin janvier, est très révélatrice des progrès effectués depuis quelques années, mais aussi du chemin qu'il reste à parcourir. « Même si elle aurait pu être plus ambitieuse, cette loi est globalement positive sur le fond et une réussite sur la forme », se réjouit Luc Bretones, du cercle de réflexion G9+.

Sur le fond, le texte étend l'ouverture des données publiques à la société civile (l'open data) pour créer une « économie de la donnée ». Elle affirme aussi une série de nouveaux droits pour protéger la vie privée des citoyens/consommateurs (droit à l'oubli, portabilité des données, « mort » numérique...) et développe l'accessibilité au numérique pour les populations les plus fragiles.

« La partie sur l'open data est majeure, car même si de nombreux élus locaux ne s'en rendent pas compte, l'ouverture des données publiques aux citoyens et aux entreprises va profondément toucher leur collectivité », souligne Élisabeth Grosdhomme-Lulin. »

Sur la forme, la loi Lemaire peut être considérée comme le premier texte conçu « dans l'esprit » de la révolution numérique. Sa première version a été rédigée sur la base d'un document de synthèse réalisé par le Conseil national du numérique, à partir des observations de tous les experts du secteur. Puis le texte a été soumis pendant trois semaines à une consultation publique sur Internet. Avec succès : 21.330 contributeurs ont voté plus de 150.000 fois et déposé plus de 8.500 arguments, amendements et propositions de nouveaux articles. Le gouvernement a ensuite revu sa copie pour ajouter cinq nouveaux articles, à l'image de la création d'un cadre légal pour le sport électronique, et effectuer une soixantaine de modifications.

« Cette méthode de cocréation inédite a été longue et éreintante, tout le monde ne peut pas en sortir entièrement satisfait en raison des nécessaires arbitrages, mais elle a créé un dynamisme incroyable », indiquait Axelle Lemaire fin décembre. »

Saluée par la majorité comme par l'opposition, cette méthode devrait être reprise pour de futurs projets de loi, comme celle sur le sport.

Fort de cette légitimité citoyenne, le texte a échappé aux grandes polémiques et aux petites phrases. Davantage de députés ont participé aux débats. Mieux, tous les observateurs ont été « agréablement surpris » par la qualité des interventions parlementaires.

« Malgré quelques propositions incongrues, comme l'interdiction des liens hypertextes [un amendement des députées socialistes Karine Berger et Valérie Rabault, NDLR], le débat a été constructif et salutaire », se réjouit Luc Belot, le rapporteur (PS) du projet de loi. Le député Patrice Martin-Lalande (LR) relativise. « Nous n'étions qu'une quinzaine de parlementaires vraiment investis, mais c'est un indéniable progrès, y compris par rapport à la loi Renseignement ». »

Des sujets cruciaux, jusqu'alors mis sous le tapis, ont enfin été abordés. La question du chiffrement des données, par exemple. L'amendement - rejeté - de Nathalie Kosciusko-Morizet (LR), visant à obliger les constructeurs de matériel informatique à créer des « portes dérobées » pour que les autorités puissent accéder à du contenu chiffré dans le cadre de leurs enquêtes, a forcé le gouvernement à clarifier sa position. À savoir que le chiffrement, garant de la sécurité des données, doit être protégé. Les experts du numérique se réjouissent aussi du débat sur la création d'un « OS souverain » pour concurrencer les géants américains comme Microsoft, Apple et Google. Même s'il a été tourné en ridicule sur Twitter.

« Créer un OS franco- français n'est pas une bonne réponse, car c'est irréalisable, mais il était nécessaire de réfléchir sur la souveraineté numérique de la France », explique Benoît Thieulin, qui y voit le signe d'un « début de prise de conscience ». »

Vers la politisation du numérique ?

En définitive, la loi Lemaire a été adoptée très largement : 356 voix pour, un vote contre. Les députés Les Républicains se sont majoritairement abstenus. Une tactique pour prendre leurs distances avec le gouvernement sans gêner le texte. Certains, à l'image de Patrice Martin-Lalande, ont tout de même apporté leur voix à la majorité. Est-ce à dire que le numérique abolit le clivage gauche/droite traditionnel? « C'est le cas aujourd'hui, et cela révèle le manque de maturité global », estime Laure de La Raudière. Effectivement, on assiste plutôt à une lutte entre les anciens et les modernes, au sein même de chaque parti, plutôt qu'à une bataille idéologique entre la gauche et la droite. Pour beaucoup, le défi des années à venir consiste justement à « politiser le numérique ».

« Il faut qu'on comprenne mieux quel dessein politique se joue derrière des choix d'apparence technologique », précise Benoît Thieulin. »

Veut-on utiliser les outils numériques pour simplifier l'administration et faire des économies d'échelle, ou investir pour mener une révolution de progrès social, d'« empouvoirement » des individus et de solidarité? Souhaite-t-on une société de surveillance grâce aux mégadonnées ou choisit-on de protéger à tout prix la vie privée? À quel échelon - national, franco-allemand, européen - faut-il agir pour faire émerger de nouveaux champions dans les secteurs d'avenir comme l'Internet des objets? Autant de choix stratégiques dotés d'une forte dimension idéologique.

« On aimerait entendre Hollande, Valls et les leaders de l'opposition proposer une trajectoire, des valeurs, et parler de l'avenir comme le fait Obama dans ses discours », résume un entrepreneur de la French Tech. »

En attendant, que faire? La société civile, elle, s'impatiente.

« Quatre-vingt-dix-neuf pour cent des entreprises savent qu'elles auront de gros problèmes dans la décennie à venir si elles ne s'adaptent pas fondamentalement au numérique. Elles ont besoin d'outils », pointe Luc Bretones. »

À l'approche de l'élection présidentielle de 2017, l'institut G9+ s'apprête à dévoiler « 100 idées pour une France numérique ». Il s'agit d'une compilation de propositions par une quarantaine d'experts, issus de toutes les sensibilités politiques et de tous les secteurs. L'objectif : positionner le numérique au coeur de la prochaine campagne électorale en nourrissant la réflexion des futurs candidats.

Au menu : des mesures « concrètes » comme le développement des Moocs dans la formation professionnelle, la création d'un nuage informatique communautaire pour l'administration, d'un carnet de santé en ligne, d'un syndicat national des travailleurs de l'économie collaborative ou d'une fiche de paie dématérialisée.

Le cercle de réflexion espère que les futurs candidats se saisiront de ces propositions ou qu'elles inspireront le gouvernement et les parlementaires.

« Toutes les intelligences sont là, poursuit Luc Bretones. Il y a énormément d'entrepreneurs, d'ingénieurs, d'universitaires, d'experts sur les enjeux actuels qui sont force de proposition et qui aimeraient que les choses bougent. Qu'attendent les politiques pour les écouter et s'emparer de leurs idées? »

Illustration(s) :

DR

Atlantico (site web)

Quand le Pentagone recrute le directeur de Google et s'offre les services de hackers

Tuesday, 15 March 2016

Byline: Fabrice Epelboin

Section: general

Washington - Quand le Pentagone recrute le directeur de Google et s'offre les services de hackers pour pirater son propre réseau
Au début du mois de mars, le Pentagone annonçait le recrutement d'un des dirigeants historiques de Google, ainsi que le lancement d'un Bug Bounty. Deux annonces qui témoignent de la rapide accélération de l'innovation au niveau de l'armée américaine et des enjeux de sécurité criminalité auxquels les gouvernements sont confrontés.

Atlantico : Le Pentagone a annoncé au début du mois l'organisation d'un concours de piratage de ses réseaux ouvert à des hackers. Pourquoi une telle initiative ? Qu'est-ce qui la justifie?

Fabrice Epelboin : Le Pentagone organise ce que l'on appelle un " Bug Bounty ": cela consiste à inviter des hackers à identifier des failles de sécurité dans ses technologies, et à les récompenser quand ils en découvrent. Plus la faille trouvée est critique, plus la récompense est élevée. C'est une pratique assez courante chez les géants des technologies aux Etats-Unis , initiée par Netscape dès 1995. Aujourd'hui, la plupart des grands de la Silicon Valley pratiquent le Bug Bounty afin de sécuriser leurs technologies : Yahoo, Microsoft, Google, Facebook, Paypal, IBM, eBay... Mais des entreprises hors du cadre strict des technologies s'y mettent également, tel United Airlines ou General Motors.

Cette approche de la détection de faille de sécurité connait un boom aux Etats-Unis depuis quelques années, car elle se révèle être un complément indispensable à l'approche traditionnelle, le pentesting, qui consiste à mobiliser un ou deux experts durant quelques semaines en leur confiant la mission de découvrir ces même failles. Avec un Bug Bounty, on peut attirer bien plus de monde, et par là même des compétences et des approches bien plus variées , reflétant la diversité que l'on peut trouver du coté des attaquants. Qui plus est, un Bug Bounty peut être ouvert de façon indéfinie, offrant une attention permanente, là où elle n'était que ponctuelle auparavant avec la précédente approche, le pentesting. Enfin, c'est une approche bien plus rationnelle en termes de ROI : plutôt que d'acheter du temps de recherche d'un ou deux experts, on achète directement auprès des experts le résultat de cette recherche.

Le fait que le Pentagone organise son propre Bug Bounty est en quelque sorte la validation ultime de cette approche de la sécurité informatique, qui fait appel à la foule sur le mode du crowdsourcing et de "l'économie collaborative" .

Aux Etats-Unis, c'est une pratique courante, et l'arrivée du Pentagone n'est que l'aboutissement d'un mouvement entammé depuis des années par tous les géants des technologies, alors qu' en Europe, cette approche de la sécurité informatique est apparue plus récemment. Deux plateformes de Bug Bounty on été lancées cette année en France : Yogosha et BountyFactory.

Le fait de faire appel à des hackers, même si une vérification de sécurité aura lieu, ne présente-t-il pas un risque de sécurité précisément ?

Que ce soit pour le Pentagone ou pour une entreprise, c'est une crainte tout à fait légitime, mais si on l'analyse de près, on s'aperçoit vite qu'il n'y a pas lieu d'appréhender ainsi le Bug Bounty. Les hackers ayant des intentions malveillantes attaquent le Pentagone, qu'il y ait ou non un Bug Bounty en cours, et la situation est la même pour n'importe quelle entreprise qui organise un Bug Bounty. L'idée qu'un Bug Bounty attire des hackers mal intentionnés est fantasque : ces hackers "blackhat" sont déjà en train de scruter les technologies des entreprises qu'elles cherchent à attaquer, ils ne vont pas attendre qu'on leur en donne l'autorisation.

Une autre crainte, qui peut sembler fondée, consiste à imaginer qu'un hacker qui découvre une faille sur une technologie soit tenté de la vendre au plus offrant, et donc pas forcément au propriétaire de la technologie qui a mis en place un Bug Bounty. C'est une crainte plus rationnelle, mais qui ne résiste pas à la réalité du "marché" qu'établit une entreprise ou une institution en mettant en place un Bug Bounty : si vous trouvez un "bug" (une faille de sécurité), vous avez en réalité assez peu de temps devant vous pour le vendre à l'organisateur du Bug Bounty et recevoir une récompense, car d'autres "chasseurs de bug" sont également à l'oeuvre, et chaque faille n'est payée qu'une seule fois, au premier hacker qui la rapporte. Tenter de vendre ailleurs une faille de sécurité, c'est à coup sûr essayer de vendre quelque chose qui n'aura plus la moindre valeur le temps de trouver un acheteur. Entre temps, les chances sont grandes qu'un autre hacker ait rapporté cette même faille au propriétaire de la technologie à travers son programme de Bug Bounty. Ce dernier l'aura corrigé avant que quiconque ne puisse l'exploiter. Ce constat est d'autant plus implacable que les attaques sophistiquées que redoutent les entreprises, comme les institutions, s'appuient la plupart du temps sur l'exploitation d'une série de failles. Il suffit souvent que l'une d'entre elles soit corrigée pour mettre en échec une attaque en cours.

Pour y voir clair, il faut appréhender un Bug Bounty pour ce qu'il est : la mise à prix par une entreprise des failles de sécurité présentes sur ses technologies. Ces failles ont un prix dans l'absolu, en dehors de tout Bug Bounty, du moins aux yeux de ceux qui savent les utiliser pour mettre au point une attaque malveillante. Le but, dans la mise en place d'un Bug Bounty, est d'impacter ce "marché", qui existe, quoi qu'il arrive.

Un Bug Bounty peut impacter ce marché de deux façons. D'une part, en mettant un prix élevé pour les failles les plus critiques, susceptibles de causer des dommages conséquents à l'entreprise qui organise son Bug Bounty : c'est ce que font Facebook ou Google, dont les récompenses pour une faille critique découverte sur leurs technologies peuvent être très élevées , et c'est ce que devrait faire toute entreprise dont le risque en termes d'image ou d'espionnage économique est élevé. D'autre part, le Bug Bounty est un marché ouvert, transparent et rapide, contrairement aux circuits de vente de failles de sécurité du coté de la cybercriminalité. La rapidité de la transaction, conjuguée à des mises à prix suceptibles d'attirer un grand nombre de hackers sur un Bug Bounty, fait que le marché des failles de sécurité au sein de la cybercriminalité est court-circuité. Il faut ajuster les prix de façon à attirer une foule en mesure de noyer le camp adverse, dont les moyens, quels qu'ils soient, ne peuvent se comparer

avec les communautés de hackers réunies autour des différentes plateformes de Bug Bounty, qui se comptent en milliers, voire en dizaine de milliers.

On voit là toute la subtilité dans la façon de mettre en place un Bug Bounty, et surtout dans le choix des mise à prix, car c'est bien l'entreprise qui décide du prix de ses failles de sécurité. Les prix des failles peuvent, par ailleurs, évoluer avec le temps, de façon à attirer des foules différentes, adaptées aux différentes phases d'un processus de sécurisation. La plupart des plateformes de Bug Bounty emploient des experts aguerris qui maitrisent parfaitement ce sujet, et accompagnent les grands comptes dans la mise en place de leurs Bug Bounties. Mais il faut absolument réfléchir en termes de marché, non pas un marché que l'on crée, mais un marché préexistant, sur lequel on cherche à avoir un effet disruptif, et concevoir un Bug Bounty en ayant cet objectif en tête. Il s'agit bel et bien de disrupter le marché de la cybercriminalité en s'appuyant sur de vastes communauté de "hackers éthiques" qui, Dieu merci, sont en bien plus grand nombre que les cybercriminels.

Peut-on envisager la mise en place d'un tel concours en France par le ministère de la Défense ? À quelles conditions et pour quels résultats ?

Traditionnellement, la France a un temps de retard en ce qui concerne l'innovation, et comme le Pentagone vient de s'y mettre... Ceci dit, c'est tout à fait envisageable, et la France est plutôt bien placée pour faire partie des premières nations européennes à mettre ses institutions au Bug Bounty, du fait que les premières plateformes de Bug Bounty européennes ont été créées en France.

Les conditions seraient très certainement similaires au Bug Bounty organisé par le Pentagone : un périmètre limité dans un premier temps, afin de tester le dispositif, et une sélection de hackers préalablement validés par le ministère de la Défense. On peut tout à fait imaginer étendre par la suite de tels Bug Bounty à d'autres institutions, à commencer par les ministères et les administrations, ainsi qu'aux opérateurs d'importance vitale.

Quant aux résultats, ils seraient sans doute similaires à ceux de n'importe quel Bug Bounty : une liste de failles de sécurité à corriger au plus vite - du moins pour les plus critiques. Pour le moment, le ministère de la Défense, comme les autres ministères et administrations françaises, fait appel à des SSII, qui proposent des campagnes de pentesting pour identifier de telles failles de sécurité, mais l'explosion de la cybercriminalité, sans parler de l'espionnage, montre bien que cette approche n'est pas suffisante, et qu'il devient urgent de la compléter par d'autres. Le Bug Bounty est un complément évident.

Dans le même temps, le Pentagone annonçait au début du mois le recrutement du président d'Alphabet (Google) en tant que conseiller en matière d'innovation. Qu'est-ce que cela révèle des liens entre gouvernement et acteurs du numérique (qui plus est dans le contexte actuel tendu entre Apple et le FBI) ? Quel gain pour le Pentagone ?

La porosité entre les GAFAM avec les services de renseignement n'est pas une nouveauté : c'était tout l'objet de l'affaire Prism, le premier volet des révélations d'Edward Snowden. Mais ces derniers temps,

on observe des éléments visibles de première importance. Au moment où Apple occupe le devant de l'actualité avec son bras de fer qui l'oppose au gouvernement américain, Google semble effectuer la démarche inverse, celle de la coopération.

Google possède non seulement un outil de surveillance des populations que le Pentagone et la NSA ne peuvent qu'envier, mais ils sont, qui plus est, la clé de l'accès aux savoirs et à l'information un peu partout dans le monde. En Europe, 95% des recherches sur Internet sont faite à travers Google, ce qui leur donne la possibilité non seulement de contrôler ce à quoi les Européens ont accès en termes d'information, mais également de savoir ce qu'ils cherchent à tout moment.

Si Google venait à être instrumentalisé à des fins politique ou militaires, cela serait un outil d'influence incroyable, et un outil de surveillance omniscient. Il est assez naturel que le Pentagone s'y intéresse, et pas si surprenant que Google réponde à sa demande - après tout, la firme de Mountain View a abandonné récemment son slogan "Don't be Evil". Mais pour le moment, la collaboration de Google avec le Pentagone ne concerne que la gestion de l'innovation, du moins officiellement.

Le Pentagone a tout à gagner à une telle collaboration. Il est évident qu'une personnalité comme Eric Smith a beaucoup à apporter à des militaires en termes de gestion de l'innovation, même si pour ce qui est d'innover, le Pentagone n'est pas en reste.

L'arrivée concomitante de l'un des dirigeants historique de Google au Pentagone et du lancement par ce dernier d'un Bug Bounty montre de façon indiscutable une brusque accélération de l'innovation du coté des institutions américaines, en particulier au sein de l'armée.

D'une manière générale, comment interpréter ces ouvertures de La Défense vers l'extérieur ? Cela ne traduit-il pas un certain aveu de faiblesse ?

Avec une augmentation de +30% au niveau mondial et +50% en France, il est difficile de ne pas dresser un constat d'échec face à l'insécurité sur Internet. D'ailleurs, le CGHQ, l'équivalent anglais de la NSA, a récemment fait des déclarations en ce sens. La cybercriminalité augmente de façon considérable, et ni la NSA, ni le Pentagone ou qui que ce soit, n'ont pu enrayer le phénomène. Il faut dire qu'ils en sont en partie responsables.

La surveillance de masse initiée par les Etats-Unis dès le lendemain du 11 septembre 2001 repose en large partie sur l'introduction volontaire par la NSA et ses alliés, de multiples failles de sécurité dans les technologies utilisées partout dans le monde par les Etats, les entreprises et les particuliers. Cela a créé un territoire d'opportunités pour une multitude d'organisations cyber-criminelles, dont les gains sont désormais comparables, si ce n'est supérieurs, à ceux des trafiquants de drogue. Car le temps où les entreprises et les Etats faisaient face à un hacker "blackhat" isolé est derrière nous. Aujourd'hui, la menace est tout autre: il s'agit de véritables groupes mafieux, très bien organisés, avec de larges équipes aux talents multiples, disposant de beaucoup de temps et de financements.

Ces mafias agissent pour leur propre compte et détroussent les entreprises, ou les espionnent pour le compte de leurs concurrents. Face à une telle menace, le Bug Bounty est une réponse appropriée : faire appel à une foule de hackers éthiques ayant les mêmes compétences que les cyber- mafias, mais à même d'aider les organisateurs de Bug Bounty. Bon nombre d'entreprises l'ont bien compris.

Illustration(s) :

Quand le Pentagone recrute le directeur de Google et s'offre les services de hackers pour pirater son propre réseau

Note(s) :

Mise à jour : 2016-03-15 08:50 UTC +01:00

Jakarta Globe

China's Xi Says Military Must Develop Cutting Edge Technology

Tuesday, 15 March 2016

Section: general

China's military must pour efforts into developing cutting edge defense technology, which has strategic significance, China's President Xi Jinping said on Sunday (13/03), according to state media reports.
Xi also stressed professionalizing the country's military brass, the official China Daily reported on Monday. The armed forces have long been plagued with corruption, which senior officers have cautioned threatens combat capabilities.

Xi, who also chairs the elite Central Military Commission, has targeted corrupt military officials as part of a sprawling campaign against graft that has felled many political foes.

The capability to innovate will determine the future of the Chinese armed forces, he said, briefing lawmakers from the military.

China has poured funds in recent years into developing a high-tech weapons manufacturing industry. It has found buyers among cost-conscious countries that are unable to buy arms from the United States and its allies.

China's military rise has unnerved Asian countries, including Japan, Vietnam and the Philippines, with which Beijing has maritime territorial disputes.

Xi is seeking to drag the People's Liberation Army, the world's largest armed forces, into the modern age, cutting 300,000 jobs and revamping its Cold War-era command structure.

China said earlier this month it would hike military spending by 7.6 percent this year, the lowest increase in six years, amid a slowing economy.

China, the world's second-largest economy, is increasingly exposed to international crises like the Middle East but has little experience at dealing with them, unlike established powers like the United States and Russia.

La Presse canadienne
Publicité ciblée sur le web et les réseaux sociaux Mise en garde pour les consommateurs
Wednesday, 16 March 2016
Byline: Lia Lévesque

Montréal - Le groupe Option consommateurs demande aux entreprises comme Google, Facebook, Microsoft et Yahoo de recueillir moins de renseignements personnels sur les utilisateurs. Et il invite ces derniers à mieux utiliser les outils à leur disposition pour ne pas divulguer ces précieux renseignements. Option consommateurs a dévoilé, mardi, une recherche sur ces entreprises qui offrent des services gratuits aux consommateurs, mais qui, en retour, se servent des renseignements ainsi obtenus pour les pister, connaître leurs goûts, leurs habitudes, et les soumettre à de la publicité ciblée. Or, ces techniques peuvent aller très loin, a affirmé l'auteur de la recherche, Me Alexandre Plourde, au cours d'une rencontre avec la presse. À l'aide d'algorithmes automatisés, elles peuvent même identifier certains mots glissés dans la correspondance des consommateurs, affirme-t-il.

Après avoir fait ces constatations, Option consommateurs ne va pas jusqu'à demander l'adoption de lois et règles plus sévères. L'organisme demande néanmoins que les règles actuelles soient mieux connues des consommateurs et appliquées.

Il faudrait que les agences qui en surveillent le respect, comme le Commissariat à la protection de la vie privée du Canada ou la Commission d'accès à l'information, disposent de plus de moyens, a plaidé Me Plourde. Mais les consommateurs aussi doivent faire une prise de conscience.

« Les consommateurs ont du pouvoir là-dedans. On a déjà vu beaucoup de réseaux sociaux ou des entreprises technologiques qui sont passées, du jour au lendemain, d'être très populaires à perdre presque tous leurs utilisateurs et à disparaître très rapidement du paysage. Nous, ce sur quoi on mise essentiellement, c'est sur l'action des consommateurs. On croit que si les consommateurs savaient ce qu'ils révèlent sur leur vie privée, ils insisteraient davantage sur le respect de leur vie privée », a affirmé Me Plourde.

Il suggère quelques outils, comme le recours au mécanisme « Do not track », qui est censé être inclus dans la plupart des navigateurs.

L'avocat spécialisé en droit de la consommation indique aussi que le consommateur peut aller sur le site de Google pour voir les étiquettes qui lui ont été accolées - comme « aime le jogging » ou « aime le rock » - et retirer les étiquettes qu'il n'aime pas. De même, Me Plourde informe les consommateurs du fait qu'il existe un moteur de recherche appelé duckduckgo, « et c'est justement ça, son avantage comparatif : ne pas recueillir de renseignements personnels sur les consommateurs ».

Me Plourde rappelle qu'ultimement, les consommateurs peuvent aussi se plaindre, d'abord auprès des entreprises visées, ensuite auprès du Commissariat à la protection de la vie privée du Canada et de la Commission d'accès à l'information.

CBC News
Carleton professor fights cyberattacks from Orléans
Wednesday, 16 March 2016
Byline: Kate Porter

Behind locked doors at a municipal building in the Ottawa suburb of Orléans, Tony Bailetti is quietly working on a plan to turn Canada into a global powerhouse for fighting cyberattacks.
The professor is known for nurturing more than 200 companies in his job straddling Carleton University's business and engineering departments.

These days, he jokes that he practically sleeps at VENUS Cybersecurity, a non-profit hub he created in a former town council office.

Bailetti is preoccupied by much more than malicious software nabbing credit card data from retailers like Target.

His eye is on big intrusions -- the idea that cyberattackers could take down power grids and water systems, or remotely take over control of cars from their drivers.

And his goal is to have Canada "playing with the bigger boys and girls" to tacke the global problem of cybersecurity in fewer than five years.

"The people who have investments in critical infrastructure -- we will be the go-to guys," Bailetti said.

'Bell-Northern Research of cybersecurity'

VENUS Cybersecurity was announced to great fanfare at a press conference at Ottawa's City Hall in November 2013.

Politicians boasted that VENUS would create much needed jobs in the eastern suburb -- and Bailetti has done that, though these are no run-of- the-mill jobs.

He has assembled some two dozen bright minds, many who have PhDs or are graduates of Carleton's technology innovation management program. Some do research and development. Others conduct tests offsite.

They're funded partly by grants, and increasingly by contracts they do for companies, government departments and universities.

"I describe VENUS as being the Bell Northern Research of cyber security," Bailetti said, likening thithe venture to the cutting-edge research labs at Nortel Networks' predecessor, almost fabled among Ottawa engineers, where he once worked.

The key for Bailetti, and something he champions in his teaching at Carleton, is that the technology must be practical and solve real problems.

Finding attack brings 'rush'

Alongside a research team, Bailetti gives entrepreneurs space to toil away on cybersecurity startups.

Bailetti may talk about global domination one moment, but the next he's self- deprecating and then directs your attention to entrepreneurs he thinks are doing great things.

Take Sherif Koussa, whose company Software Secured is busy hacking into applications to spot weak computer codes for small businesses.

"When I find an attack and notify a client, I get a kind of rush that I prevented something," Koussa said.

Then, there's Arthur Low, who once designed microchips for Nortel and IBM, and holds patents in cryptography.

Low now thinks he's hit on a way to help computers from being contaminated, especially for companies with employees who travel or work on outside computers.

Low's technology doesn't involve scanning for viruses. Instead, he's created an operating system that he likens to a disposable cup that can be thrown away to prevent the spread of germs.

Low thinks for Canada to become the cybersecurity powerhouse Bailetti predicts, Canada needs more visionaries who will spend money on technology and products like his. And, Low is not banking on government.

"In the end, this has to connect with people with a profit agenda. And the only way that's to happen is you have to help them make money, so our goal is to help other people make money with these solutions,"said Low, who is about to start field trials with an early adopter.

"You just need to have one initial success to prove it works -- and then it's going to catch on like fire."

CBC News
Government tech support putting RCMP, public safety at risk, documents reveal
Wednesday, 16 March 2016

Byline: Alison Crawford

Internal RCMP reports and emails obtained by CBC News show that Shared Services Canada's takeover of the Mounties' tech support has been a costly disaster that has jeopardized court cases and investigations while putting the safety of officers and members of the public at risk.
The documents received through access to information include correspondence from RCMP Commissioner Bob Paulson in which he refused to give SSC any more control over the Mounties' information technologies.

SSC is the federal department created in 2012 to take over the delivery of email, data centre and network services for 43 government agencies, including the RCMP.

By all internal accounts, its work on behalf of the RCMP has been a fiasco.

At a Sept. 25, 2015 meeting between Paulson and SSC president Liseanne Forand, the commissioner highlighted a number of examples where the department's mistakes and oversights have affected policing operations, including:

-On October 22, 2014 while the terrorist attack on Parliament Hill was taking place -- without consulting the RCMP or understanding the risks involved -- SSC increased bandwidth to receive evidence gathered by the public by shutting down the Disaster Recovery site

-Mission B.C.'s phone system is in need of replacement. The concern was originally raised with SSC in January 2015, with no progress to date. The situation has come to the point that there is a public safety risk because the phone line service is unstable, affecting 911 calls and dispatch

-On September 18, 2014 a server failed in a Dorchester, Que. data centre, resulted in some corruption of data needed for an investigative disclosure package. SSC had been advised on Nov. 7, 2012, and through several follow-up inquiries, that the equipment was past the end of its life but did not replace it

-SSC has lapsed contracts concerning security protection of networks and servers

Overall, the documents raise serious concerns about three major areas -- safety and security, loss of service or information, and cost to taxpayers.

Unit compromised

A January 2014 memo to Paulson from the RCMP's civilian IT employees highlighted dozens of concerns.

In December 2013, Mounties reported having to spend almost $1 million to sustain systems critical to two special units, including one that investigates online child sex assaults, because SSC "is neither willing nor able to purchase" the equipment required.

"There is simply no appetite to fix any systems until they have failed. When this happens, it will be too late. RCMP will lose court cases," the group of employees told Paulson.

Another system failure occurred when SSC could not renew Hewlett Packard warranties

"It cost approximately $20,000 to have HP come in to attempt repairs and system recovery ... RCMP was left with a broken system to fix and major data loss which may impact court cases."

Risk to front-line officers

Even more money was wasted when SSC had to pay $10,000 in interest after it didn't pay Northwestel -- the force's phone and internet provider in the territories and northern B.C. -- for months on end.

"Shared Services has not been paying their bills. Vendors have threatened and have cut-off service to various units such as Shaw Cable, disrupting operations to the RCMP. There is risk to the front line," the employees warned Paulson.

Several more egregious examples of ineptitude include how SSC couldn't get the newly opened Berens River RCMP detachment any kind of telecommunications service for two years.

"In desperation a regular member in Berens River ordered satellite service so he could do his work ... and paid for it out of his own pocket on his personal credit card. Shared Services then declined to pay for his out-of-pocket expense," RCMP supervisor Rick Lippens told senior management in an email.

Members of the RCMP repeatedly expressed frustration that SSC treats the Mounties as though they work at a regular government department working 9 a.m. to 5 p.m. in downtown Ottawa.

"They've extended our evergreening cycle from three years to six. That's just asking for trouble. It's one thing if a router goes down in Ottawa and they can walk over and replace it but we need to deal with very remote locations that could be down for days until we can get in there by plane, boat or ice road to deal with a failure," a group of employees wrote in frustration to Paulson.

No one from the RCMP or Shared Services Canada responded to our requests for comment on the documents.

However, in Paulson's Nov. 25, 2014 letter to Forand, the commissioner wrote that the department's proposal to manage even more of the RCMP's information technologies "pose unacceptable risks to public safety, protection of RCMP members and policing across Canada."

Paulson went on to explain how he is compelled to exercise his authority to refuse the Mounties' participation in the next phase of Shared Services Canada.

Toronto Star
Brison envisions one federal online site
Wednesday, 16 March 2016
Byline: Alex Boutilier

OTTAWA -- Treasury Board President Scott Brison says he can see a future where all levels of government provide services to Canadians through a single online portal.
Granted, Brison says, he's thinking in the very long term. But with most Canadians not thinking long and hard about the division of responsibilities between different levels of government, why not give them one-stop shopping?

"When Canadians have an issue with government, they're not necessarily aware of whether the issue is related to federal or provincial government, (or) in some cases municipal," Brison told the Star in an interview last week.

"Long term, we should be thinking not just to work such that all the departments and agencies of the federal government are accessible through a single portal approach . . . but, in time, once we get that right, I think there will be opportunities to work with other levels of government as well."

The new Liberal government has promised to put in place a single point of online access for all federal government services, as well as to create a website where Canadians can securely access all personal information the government has on them.

Brison, who is responsible making those commitments a reality, acknowledged there's work to be done. The Star reported on Tuesday that 77 per cent of all federal government services still require pen and paper forms filled out in person or via snail mail.

But even after getting the federal government fully online, Carleton professor Amanda Clarke said there would be serious barriers to bringing the provinces, territories, and municipalities under one system.

"That would be the dream, for sure. I appreciate his ambition," said Clarke, who studies digital government and public administration.

"(But) how would you brand that website? . . . Every jurisdiction now has created, with higher or lower levels of sophistication, some kind of colour scheme and organization and logos that they use. And these (choices) are also politically powerful, as well."

Clarke said there would be definite advantages to consolidating the services of multiple governments under one roof - such as being able to pool investment in web design and functionality, or scaling responses to policy issues.

The data harvested on such a site would be invaluable, as well. Looking at who is requesting what services in different regions would be a government data geek's dream, and could inform policy responses from all levels of government.

But Clarke said as governments are increasingly "becoming their websites" - that is, moving to a point where the website will be the primary interaction between citizens and government - all the traditional arguments over jurisdiction and responsibility apply.

"All the challenges that are always at play when you talk about cross-jurisdictional collaboration or co-ordination in Canada would come in play when you were dealing with websites," Clarke said.

Despite the challenges, Clarke said Canada is actually starting from a pretty good position.

The federal government's web presence was largely centralized under the previous Conservative government, avoiding the balkanized situation giving countries like the U.K. trouble.

To build from that starting point, Clarke suggested the government could create a team loosely based on the model of large U.S. tech companies to provide a more agile approach to web development.

Wall Street Journal
Apple's Encryption Puzzle
Wednesday, 16 March 2016
Byline: Daisuke Wakabayashi

New York - Apple Inc. has refused federal requests to help unlock the phone of San Bernardino gunman Syed Rizwan Farook. But it turned over data from his phone that Mr. Farook had backed up on the company's iCloud service.
Soon, that might not be so simple. Apple is working to bolster its encryption so that it won't be able to decode user information stored in iCloud, according to people familiar with the matter.

But Apple executives are wrestling with how to strengthen iCloud encryption without inconveniencing users. Apple prides itself on creating intuitive, easy-to- use software, and some in the company worry about adding complexity. If an iCloud user forgets a password, for example, and Apple doesn't have the keys, the user might lose access to photos and other important data.

If Apple keeps a copy of the key, the copy be "can be compromised or the service can be compelled to turn it over," said Window Snyder, a former Apple security and privacy manager who is now chief security officer at Fastly, a content-delivery network.

The issue is similar in the physical world: tighter security means more hurdles, such as more locks or codes for a home alarm system.

As a result, the timing of any move to strengthen encryption is uncertain. The Financial Times earlier reported on Apple's plans to encrypt iCloud backups.

Separately, in a new court filing Tuesday in its iPhone standoff with the government, Apple said it "has never built a backdoor" or "made data stored on the iPhone or iCloud more technically accessible to any country's government."

Apple's iCloud is a set of Internet services that allow users to store and sync data across their devices. A photo taken on an iPhone, for example, can appear automatically on a Mac or iPad with the same iCloud account.

When connected to Wi-Fi, iCloud's backup service automatically takes a daily snapshot of a phone's contents. Customers can use backups to transfer photos, iMessages, health data, and other information from an old iPhone when they buy a new one.

Apple already stores some data that it can't access or read, in a feature called iCloud Keychain, where a user can store passwords and credit- card information.

Another device associated with the same iCloud account can give permission to a new phone to access Keychain. But not everyone has more than one Apple device. A user also could create a security code to regain access, but if the user enters an incorrect code 10 times, Apple removes the Keychain account from its servers.

An Apple spokeswoman pointed to comments by Craig Federighi, the company's senior vice president of software engineering, in a March 6 opinion piece in the Washington Post. "Security is an endless race -- one that you can lead but never decisively win," Mr. Federighi wrote. "Yesterday's best defenses cannot fend off the attacks of today or tomorrow."

To get a sense of the challenge, consider software maker Box Inc., which provides a way for businesses to store data on remote computers in the "cloud." It took Box three years to design a system to encrypt corporate information so that it couldn't access the data, without hindering popular features such as document preview, or forcing users to download additional apps.

Box Keysafe works much like a bank safe- deposit box, with one key held by the owner and one key held by Box. Without both keys, the data can't be decrypted so Box alone can't access the information. Box Chief Executive Aaron Levie said he can foresee consumers seeking similar protection. "The cloud is going more and more in this direction," he said.

Any steps Apple takes to close off access to iCloud backups are likely to further antagonize law-enforcement authorities, for which the backups can be a trove of useful data.

"No doubt it will," said Robert Cattanach, a partner at law firm Dorsey & Whitney LLP and a former Justice Department attorney. "It could present a fairly significant burden to law enforcement."

Apple has fought the Federal Bureau of Investigation's requests to help unlock Mr. Farook's iPhone, which was last backed up on Oct. 19, about six weeks before he and his wife killed 14 people in a Dec. 2 terrorist attack. Apple says the device is encrypted in a way that leaves Apple itself without access to the data, the result of a change it made in its iPhone software in 2014.

In court documents, the FBI has said that the iCloud files revealed that Mr. Farook communicated with some people killed in the attack. In a declaration filed in the case, Christopher Pluhar, an FBI supervisory special agent in the San Bernardino investigation, said iCloud backups could provide "valuable evidence," but offered no specifics of what investigators learned from Mr. Farook's data.

The phone could contain information about Mr. Farook's movements and communications after its last backup.

Washington Free Beacon
China, Russia Planning Space Attacks on U.S. Satellites
Wednesday, 16 March 2016
Byline: Bill Gertz

Washington - China and Russia are preparing to attack and disrupt critical U.S. military and intelligence satellites in a future conflict with crippling space missile, maneuvering satellite, and laser attacks, senior Pentagon and intelligence officials told Congress on Tuesday.
Air Force Gen. John Hyten, commander of the Air Force Space Command, said the threat to U.S. space systems has reached a new tipping point, and after years of post-Cold War stagnation foreign states are focused on curbing U.S. space systems.

"Adversaries are developing kinetic, directed-energy, and cyber tools to deny, degrade, and destroy our space capabilities," Hyten said in a prepared statement for a hearing of the House Armed Service strategic forces subcommittee.

"They understand our reliance on space, and they understand the competitive advantage we derive from space. The need for vigilance has never been greater," the four-star general said.

Hyten said U.S. Global Positioning System satellites remain vulnerable to attack or jamming. The satellites' extremely accurate time-keeping feature is even more critical to U.S. guided weapons than their ability to provide navigation guidance, he said.

Disrupting the satellites time capabilities would degrade the military's ability to conduct precision strike operations used in most weapons systems today.

Hyten said a new joint military-intelligence command center is helping to monitor space threats, such as anti-satellite missile launches, covert killer robot satellites, and ground-fired lasers that can blind or disrupt satellites. The unit is called the Joint Interagency Combined Space Operations Center, located at Schriever Air Force Base, Colorado.

The Space Command also is creating 39 cyber mission teams that will be used for defensive and offensive cyber operations involving space systems.

Lt. Gen. David Buck, commander of Joint Functional Component for Space, a U.S. Strategic Command unit, testified along with Hyten that China and Russia pose the most serious threats to space systems.

"Simply stated, there isn't a single aspect of our space architecture, to include the ground architecture, that isn't at risk," Buck said.

"Russia views U.S. dependency on space as an exploitable vulnerability and they are taking deliberate actions to strengthen their counter-space capabilities," he said.

China in December created its first dedicated space warfare and cyber warfare unit, called the Strategic Support Forces, for concentrating their "space, electronic, and network warfare capabilities," Buck said.

"China is developing, and has demonstrated, a wide range of counter-space technologies to include direct-ascent, kinetic-kill vehicles, co-orbital technologies that can disable or destroy a satellite, terrestrially-based communications jammers, and lasers that can blind or disable satellites," Buck said.

"Moreover, they continue to modernize their space programs to support near-real-time tracking of objects, command and control of deployed forces, and long-range precision strikes capabilities," the three-star general said.

Douglas Loverro, deputy assistant defense secretary for space policy, also warned about growing threats to satellites and outlined U.S. plans to deter future attacks.

Loverro said the United States does not want a war in space. "But let me be clear about our intent--we will be ready," he said.

None of the five Pentagon and intelligence officials who took part in the budget hearing for military space efforts mentioned any U.S. plans or programs to develop anti-satellite missiles and other space weapons for use against Chinese or Russian space systems. The subcommittee, however, held a closed-door session after the public hearing.

A modified U.S. missile defense interceptor, the SM-3, was used in 2008 to shoot down a falling U.S. satellites in a demonstration of the country's undeclared anti-satellite warfare capability.

Loverro suggested U.S. defense and deterrence of space attacks could involve counter attacks, possibly on the ground or in cyber space. But he provided no specifics.

"Today our adversaries perceive that space is a weak-link in our deterrence calculus," Loverro said. "Our strategy is to strengthen that link, to assure it never breaks, and to disabuse our adversaries of the idea that our space capabilities make tempting targets."

Many of the most important navigation, communications, and intelligence satellites were designed during the Cold War for use in nuclear war and thus incorporate hardening against electronic attacks, Loverro said.

For conventional military conflict, however, adversaries today view attacks on U.S. satellites as a way to blunt a conventional military response what Loverro called the "chink in the conventional armor of the United States."

"In this topsy-turvy state, attacks on space forces may even become the opening gambit of an anti-access/area-denial strategy in a regional conflict wherein an adversary seeks to forestall or preclude a U.S. military response," he said. "Chinese military strategists began writing about the targeting of space assets as a 'tempting and most irresistible choice' in the late 1990s, and the People's Liberation Army has been pursuing the necessary capabilities ever since," he said.

Rather than threatening foreign states' satellites, Loverro said deterrence against foreign nations' space attacks is based on defending against missile strikes or other attacks and making sure satellite operations will not be disrupted in war.

That would be carried out through partnering with the growing commercial space sector that is expected to deploy hundreds of new satellites in the coming years that could be used as back up systems for the Pentagon in a conflict.

Deterrence also will be based on increasing foreign partnerships with allied nations in gathering intelligence on space threats and other cooperation.

A space defense "offset" strategy will seek to reduce the advantage of using relatively low cost of missiles, small satellites, or cyber forces to attack U.S. satellites, Loverro said.

"An advanced U.S. satellite might cost upwards of $1 billion; missiles that could destroy such a satellite cost a few percent of that sum; co-orbital microsatellites cost even less; and lasers that might blind or damage satellites have an unlimited magazine with almost zero cost per shot," Loverro said.

Deploying large numbers of low-cost satellites will not offset those advantages, he said.

Instead, Loverro offered vague plans for countering the threat. "A space offset strategy must employ a diverse set of resilience measures that complicate the technical, political, and force structure calculus of our adversaries, by arraying a complex set of responses, with few overlapping vulnerabilities and a combination of known and ambiguous elements," he said.

Frank Calvelli, deputy director of the National Reconnaissance Office, the spy agency that builds and operates strategic intelligence and reconnaissance satellites, said a resurgent Russia and aggressive China are among several current national security threats.

Calvelli revealed that the agency in October launched a new satellite that carried 13 smaller "CubeSats."

"The NRO sponsored nine of the CubeSats while the National Aeronautics and Space Administration sponsored the remaining four," Calvelli said.

Among the missions of the CubeSats are software-defined radios "to provide beyond-line-of-sight communication for disadvantaged users in remote locations, and technology pathfinders to demonstrate tracking technologies, optical communications, and laser communication," he said.

Four advanced intelligence-gathering satellites will be launched this year to support military operations and intelligence analysis and decision-making.

Calvelli also said space threats are prompting the Reconnaissance Office to develop "better and faster" systems in space and on the ground, along with better overall "resiliency"-- a term used by the military to signify an ability to operate during high- intensity warfare.

The agency is investing substantial sums in bolstering defenses for space and ground systems to make them more survivable during space war.

"We are more focused on survivability and resiliency from an enterprise perspective than we have ever been and we have made significant investments to that end," he said.

The agency also is "improving the persistence of our space-based systems, providing greater 'time on target' to observe and characterize activities, and the potential relationship between activities, and to hold even small, mobile targets at risk," Calvelli said.

It also is upgrading its ground stations, which are used to control and communicate with orbiting satellites, including an artificial intelligence system called "Sentient."

"Sentient--a 'thinking' system that allows automated, multi-intelligence tipping and cueing at machine speeds-- is just one of those capabilities," Calvelli said.

New ground stations also are being deployed that will empower "users of all types with the capabilities to receive, process, and generate tailored, timely, highly- assured, and actionable intelligence," he said.

The comments were a rare public discussion of the activities of one of the most secret U.S. intelligence agencies.

Dyke D. Weatherington, director of unmanned warfare and intelligence, surveillance, and reconnaissance at the Pentagon, said eight national security satellites were launched in 2015, including tactical and strategic communications, and navigation, position, and timing satellites.

Weatherington said the United States maintains a strategy advantage in space system but warned that is changing. "The rapid evolution and expansion of threats to our space capabilities in every orbit regime has highlighted the converse: an asymmetric disadvantage due to the inherent susceptibilities and increasing vulnerabilities of these systems," he said.

While space threats are increasing, "our abilities have lagged to protect our own use of space and operate through the effects of adversary threats," Weatherington said.

The Pentagon currently has 19 military- capable GPS satellites on orbit and a new generation of GPS satellites is being developed that will be produce signals three times stronger than current system to be able to overcome electronic jamming, he said.

The officials at the hearing also discussed plans to transition from the sole reliance on the use of Russian-made RD-180 rocket engines to launch national security satellites.

A new U.S. made engine, however, will not be fully developed until 2022 or 2023.

The Hill
DHS cyber threat sharing program review shows privacy risks
Tuesday, 15 March 2016
Byline: Katie Bo Williams

Washington - A Department of Homeland Security review of a cyberthreat information-sharing program has revealed some inadequacies in how the system protects privacy.
Despite safeguards to prevent personally- identifiable information from being transmitted, "residual privacy risk that these processes may not always identify and remove unrelated [personal information], thereby disseminating more [information] than is directly related to the cybersecurity threat," the report reads.

The automated system, required under a major cybersecurity bill signed into law in December, is intended to allow private companies to share threat indicators with the federal government without impacting privacy by stripping personal information out of the shared data.

The so-called Cybersecurity Information Sharing Act placed the system under the umbrella of the Department of Homeland Security, widely seen as the agency with the best privacy protections in the federal government.

The bill requires any personally- identifiable information that is shared through the program -- which is voluntary -- to be directly related to a cybersecurity threat.

But whether the government can be trusted to adequately protect the information it receives and shares was a major sticking point in the passage of the bill.

Some privacy advocates argued vehemently that breaches like the one discovered last summer at the Office of Personnel Management -- which exposed over 20 million people -- demonstrate the risks of providing such information to a federal agency.

The system, known as the Automated Indicator Sharing initiative, is ultimately intended to be fully automated, although right now some data still requires human attention.

If a field contains information that the system doesn't recognize, it will flag it for a human analyst who can determine whether it contains personal information before it is shared.

New York Times
Justice Dept. and Apple Trade Barbs Over Law
Wednesday, 16 March 2016
Byline: Katie Benner, Eric Lichtblau

San Francisco - Apple on Tuesday emphasized its opposition to a court order requiring it to help unlock an iPhone for law enforcement purposes, saying in a new legal brief that the government's "methods for achieving its objectives are contrary to the rule of law, the democratic process and the rights of the American people."
The company's argument quickly drew a response from the Justice Department, which upbraided Apple for trying to stand above the law. "The Constitution and the three branches of the federal government should be entrusted to strike the balance between each citizen's right to privacy," a Justice Department spokeswoman, Emily Pierce, said in a statement. "The Constitution and the laws of the United States do not vest that power in a single corporation."

The latest volleys between Apple and the Justice Department represent a final cementing of positions in a case that has pitted the world's largest company against the government, which wants to extract data

from an iPhone used by a gunman in the San Bernardino, Calif., terrorist attack last December. Apple has refused to comply with the order and its filing on Tuesday was the last before a crucial hearing in the case, which is scheduled for March 22 before Magistrate Judge Sheri Pym of the Federal District Court for the Central District of California.

The case has set off a fierce debate over privacy and security, with heated arguments between Apple and the government. Apple has contended that the court order could have grave consequences for digital security and privacy. The Justice Department has said Apple's inability to get into its smartphones has created a system tailor-made for criminals.

For the last few weeks, the two sides have stumped for their positions before Congress and in the court of public opinion. Each side has asked Congress to decide under what circumstances the government may see private customer data. President Obama said last week that law enforcement authorities must be legally able to collect information from smartphones and other electronic devices.

In its legal filing Tuesday, Apple tried to move the debate from an intense and personal tone and refocus attention on what it said it sees as the matter at hand, a fight over civil liberties and data privacy. The issue cannot be weighed without taking into account the larger national debate over data privacy concerns, Apple said.

"The Justice Department and F.B.I. argue that this court must decide this issue in a vacuum," the company said in its brief. "The court not only can consider this broader context, it must do so."

Apple's filing on Tuesday also reiterated points the company made last month when it asked the court to drop its order, contending that the request would "inflict significant harm -- to civil liberties, society and national security -- and would pre-empt decisions that should be left to the will of the people through laws passed by Congress and signed by the president."

The filing emphasized the constitutional arguments that Apple has made, specifically that the court order violates the company's constitutional right to free speech and subjects it to "arbitrary deprivation" of its liberty by the government.

Apple also repeated its argument that the government was overstepping its bounds by seeking to force the company to break into the iPhone using a statute called the All Writs Act, which dates to 1789. Apple has said the government is interpreting the law too broadly, and re- emphasized that point on Tuesday.

"The All Writs Act cannot be stretched to fit this case," Apple said.

The filing was less fiery than the brief filed in the case last Thursday by the Justice Department, which suggested Apple was refusing to comply with the government while secretly conducting a different,

special relationship with China. Apple's general counsel, Bruce Sewell, has said that the accusations were baseless and cited unnamed sources.

Apple's brief on Tuesday, while less angry in tone, did seek to put to rest what its lawyers called the government's most inflammatory claims about the company's relationship with China and its use of privacy as a marketing tool. To buttress its defense, Apple cited declarations from Craig Federighi, its senior vice president for software engineering, and Robert Ferrini, its senior director for worldwide advertising and planning.

"Apple uses the same security protocols everywhere in the world," Mr. Federighi said in his declaration filed Tuesday. "Apple has never made user data, whether stored on the iPhone or in iCloud, more technologically accessible to any country's government. We believe any such access is too dangerous to allow."

Mr. Ferrini also disputed the government's contention that Apple was using privacy as a marketing tool. Of Apple's approximately 1,793 advertisements worldwide, he said, "not a single one has ever advertised or promoted the ability of Apple's software to block law enforcement requests for access to the contents of Apple devices."

Any decision by Judge Pym is likely to be appealed and could reach the Supreme Court, which has issued a mixed set of rulings in recent years on the scope of the government's powers to collect evidence.

"We look forward to responding to Apple's arguments before the court next week," said Ms. Pierce of the Justice Department.

Washington Post
Conservative group plans to depose seven over Clinton emails
Wednesday, 16 March 2016
Byline: Spencer S. Hsu

Washington - A conservative legal advocacy group submitted plans Tuesday to question under oath seven current and former top State Department officials and aides to Democratic presidential contender Hillary Clinton - but not Clinton herself at this point - about her use of a private email server when she was secretary of state.
Judicial Watch said its deposition plan includes Cheryl D. Mills, who was Clinton's chief of staff at State; Huma Abedin, a top aide who served as Mills's deputy and who now is vice chairman of Clinton's presidential campaign; and Bryan Pagliano, a Clinton staff member during her 2008 presidential campaign who helped set up the private server.

U.S. District Judge Emmet G. Sullivan of Washington granted a request on Feb. 23 for legal discovery by Judicial Watch, which seeks to determine whether Clinton's email arrangement thwarted federal open-

records laws. After his order, Sullivan directed Judicial Watch to file a detailed plan about how it intended to proceed.

The submitted plan can be contested by lawyers from the Justice and State departments and is subject to approval by Sullivan.

Sullivan set an April 12 deadline for filings by the two sides, meaning that questioning of key Clinton aides could take place as she tries to secure the Democratic nomination and turn to the November general election.

"Based on information learned during discovery, the deposition of Mrs. Clinton may be necessary," wrote Michael Bekesha, counsel for Judicial Watch. "If Plaintiff believes Mrs. Clinton's testimony is required, it will request permission from the Court at the appropriate time."

Judicial Watch also said it wants to question Undersecretary for Management Patrick F. Kennedy; Stephen D. Mull, executive secretary from June 2009 to October 2012; Lewis A. Lukens, executive director of the executive secretariat from 2008 to 2011; and Donald R. Reid, senior coordinator for security infrastructure in the bureau of diplomatic security.

A Justice Department spokesman declined to comment.

Clinton campaign spokesman Brian Fallon said, "This is the same right-wing organization that has been repeatedly attacking the Clintons without success since the 1990s, and they are clearly going to pull out all the stops to try to hurt the secretary's presidential campaign."

The Judicial Watch lawsuit came over a May 2013 request for information about Abedin's employment arrangement. For six months in 2012, Abedin was employed simultaneously by the State Department, the Clinton Foundation, Clinton's personal office and a private consulting firm connected to the Clintons.

In his February ruling, Sullivan criticized the government for what he called "a constant drip" of piecemeal disclosures and a "staggering" amount of resources devoted to a situation in which private counsel for former federal employees - Clinton and Abedin - decided what government records to disclose.

Sullivan said there was sufficient basis to show that senior department officials knew of Clinton's server arrangement from the time she took over at State in January 2009, citing an email chain among Kennedy, Lukens, Mills and others regarding setting up a computer in Clinton's office so that she could check her "off network" email.

Sullivan also noted email traffic among Abedin, Mull, Mills, Kennedy and others discussing communication problems, in which Mull suggested that Clinton be issued a State Department BlackBerry that would protect her identity but be subject to public-records requests.

"How on earth can the Court conclude that there's not, at a minimum, a reasonable suspicion of bad faith regarding the State Department's response to this FOIA request?" Sullivan said.

Judicial Watch said it intended to seek answers about department officials' creation, maintenance, support or awareness of Clinton's email system; any instructions given to department workers about communicating by email with Clinton and Abedin; and any inquiries into or discussions about disclosing Clinton's use of the system.

The group also said it would ask the department to identify who handled requests for email records from the secretary's office, inventoried Clinton's and Abedin's information, or used an account on Clinton's email server for official business.

The Register (UK)
Millions menaced as ransomware-smuggling ads pollute top websites
Wednesday, 16 March 2016
Byline: John Leyden

London - Top-flight US online publishers are serving up adverts that attempt to install ransomware and other malware on victims' PCs.
Websites visited by millions of people daily - msn.com, nytimes.com, aol.com, nfl.com, theweathernetwork.com, thehill.com, zerohedge.com and more - are accidentally pushing out booby-trapped adverts via ad networks, warn infosec researchers.

The adverts are built from exploit kits, which as the name suggests, are toolkits of code that exploit security vulnerabilities in browsers and plugins to gain control of computers.

Jérôme Segura, a senior security researcher at Malwarebytes, said that the malvertising campaign began slowly before ratcheting up into top gear on Sunday.

"The first couple of days before this campaign went big, we observed a few hits on smaller publishers that were pushing the RIG exploit kit," Segura blogged. "On Sunday, when the attack really expanded, the Angler exploit kit was then used."

The Angler EK exploits a recently patched Silverlight vulnerability as well as more standard Flash and JavaScript vulnerabilities in order to push malware onto the Windows PCs of surfers served with tainted ads.

Trend Micro reported on the same attack on Monday. The exploit kit downloads a variant of the Bedep backdoor which, in turn, drops a trojan, according to Trend Micro, which reckons "tens of thousands of users" have been affected by the attack.

"It's important to note that while these popular sites are involved in the infection process they are, much like infected clients, victim of malvertising," blogged Trustwave's SpiderLabs Research. "The only 'crime' here is being popular and having high volumes of traffic going through their sites daily."

SpiderLabs has de-obfuscated the malware's code, and found that it checks to see if any antivirus and security products are installed, and if not: it pulls in Angler using a HTML iframe.

Patching regularly, uninstalling Silverlight or setting plugins such as Flash to click-to-play, will defend against attacks from dodgy banner adverts.

London Daily Telegraph
Telecoms bosses falling behind on cyber security, economists say
Tuesday, 15 March 2016
Byline: Kate Palmer

London - Telecoms companies are the most vulnerable businesses in Britain to cyber attacks, yet spend the least on defending themselves against hackers, according to an industry-wide survey.
Mobile and broadband providers were found to be most at risk of being attacked by hackers because they hold highly-prized customer information, according to the study from the Centre for Economic and Business Research (CEBR).

Economists at the CEBR modelled how a real cyber attack would affect a cross-section of the British economy, including the telecoms, utilities, retail, banking and insurance sectors. They found that telecoms companies were the most vulnerable due to the nature of sensitive information stored, the value of this data and low levels of investment in cyber security.

More than half of telecoms bosses who took part in the survey believed their company would experience a "significant breach" within a year's time.

"Britain's boardrooms are struggling to get a handle on cyber security issues," said Andrew Rogoyski, head of cyber security at the CGI, who warned there would be more breaches unless investment increased.

"Bosses know it is a risk but are uncertain in their approach, often failing to prioritise spending on cyber security."

However, three-quarters of telecoms boards said they now planned to increase spending on cyber security experts, compared with just 7pc of boards in the lower-risk retail sector.

And high-profile hacks, including the TalkTalk breach last year, have prompted some 80pc of all businesses surveyed to step up their cyber security, although just half of had crisis management plans in place in the event of a data breach, the report found.

British companies typically hold £52.5m worth of sensitive information, including customers' financial details and commercially- sensitive intellectual property. Banks hold the most valuable details, roughly £65m per financial institution, according to the CEBR.

Economists at the CEBR estimate that the total cost of a serious data breach to a business over one year is £1.2m on average. That figure is roughly in line with recent Government estimates that security breaches would cost companies £1.46m, revised up from £600,000 in 2014.

Vodafone, one of the world's biggest telecoms firms, has set up its own security arm. From today, the UK- based company will begin selling cyber technology developed with BAE systems to business customers, including 80pc of FTSE 100-listed companies.

Vodafone's head of enterprise, Nick Jeffery, said: "Our customers know they face a wide range of cyber threats, many of which could materially impact their operations and brand."

The Guardian (London)
'Snooper's charter': Theresa May faces calls to improve bill to protect privacy
Wednesday, 16 March 2016
Byline: Multiple reporters

London - Theresa May is facing calls from senior Tories and the opposition to improve the investigatory powers bill to allay concerns about privacy.
In a debate for the second reading of the bill, Ken Clarke, the Conservative former home secretary, and Dominic Grieve, the Tory former attorney general, suggested there could be improvements to the new laws that overhaul the state's surveillance powers.

The bill passed easily with 281 for and just 15 against, mostly comprising Liberal Democrats, while Labour and the SNP abstained. However, almost 50 Conservatives were absent, suggesting many may not be happy with the legislation as it currently stands. If the SNP and Labour had voted with the Lib Dems, it would have been comprehensively defeated.

Labour and the SNP abstained as they remain unconvinced about whether privacy is adequately protected, while the Liberal Democrats are going one step further and voting against the bill, which has been nicknamed "snooper's charter".

It will hand law enforcement agencies more access to people's internet connection records but also make sure judges oversee the granting of warrants for interception.

The home secretary said privacy was "hard-wired" into new controversial surveillance powers and they would not give security services generalised access to people's web browsing histories.

But Andy Burnham, the shadow home secretary, said he wanted to see a general presumption in favour of privacy along with at least six other improvements before the party could be persuaded to back the bill.

Clarke twice pressed May on whether judges should be given stronger powers to oversee interception of communications warrants.

As the bill is currently drafted, judges will be able to disagree with the home secretary's granting of a warrant on matters of process but not substance. "Questions of judgment and proportionality are the most important of all, that worry me most," Clarke said.

He said it was necessary to be "vigilant against some future administration abusing" the powers and pointed out that "all kinds of curious public bodies" would be able to get access to huge amounts of extra information. "I doubt the wisdom of that," he added.

Clarke said he was troubled that use of the powers could be justified on the wide-ranging grounds of "economic wellbeing" and "national security".

Grieve said he supported the bill as it was necessary but hoped ministers would accept it was "capable of further improvement" and he trusted that "during its passage, it performs the equally important role of being seen as an upholder of freedom and liberty".

Another to raise concerns was Stella Creasy, the Labour MP for Walthamstow, who said there was a "challenge in separating out contact and content" when people's internet connection records were tracked. "It's not the same as a phone record when you look at somebody's internet correspondence," she said.

However, May insisted there would be no access to people's web browsing histories and the bill would only allow tracing of their connections to the internet.

"It is absolutely possible, and we've been talking at length with the companies, to be able to separate in internet connection records (ICRs) for example, the device or website that a particular device has accessed and not then go into the content of whatever it is that has been looked at in relation to that," she said.

"It's very important that I make that clear because when it comes on to ICRs, we are not talking about looking at people's web browsing history, we are simply looking at that initial point of contact."

Before the debate,concerns about the legislation were raised by a number of groups including the internet provider industry body and a group of 200 lawyers.

The Internet Services Providers' Association said: Our members have significant concerns about the ambitious timetable of the bill. The prime minister himself argued at prime minister's questions that the investigatory powers bill is one of the most important bills this House will discuss.

"We recognise that three parliamentary committees have investigated the bill and made 123 recommendations. However, even our members are not yet fully clear about what the bill will mean for them. It is vital that parliament is provided with a sufficient amount of time to scrutinise the bill."

Renate Samson, chief executive of the civil liberties group Big Brother Watch, has said the drive to get the bill on the statute books by the end of the year was "too fast".

Senior lawyers raised concerns in a letter to the Guardian, saying it was fundamentally flawed because it destroyed privacy.

Among those who have signed the letter are the chair of the Bar Human Rights Committee, Kirsty Brimelow QC, Tom de la Mare QC, who has been a special advocate in security cases, Sir Stephen Sedley, who is a former court of appeal judge, Prof Sir Geoffrey Bindman QC, Hugh Southey QC, Michael Mansfield QC and Philippe Sands QC. Among academic lawyers, there are representatives of nearly 40 law schools in the UK.

Earlier, the Lib Dems called on Labour to do more to kill off the new surveillance laws, calling the decision to abstain from voting on the bill "gutless".

Burnham made it clear that Labour was prepared to vote down the legislation at a later stage and force the government to extend its transitional arrangements unless there were a string of changes.

But he said he was persuaded that the police and security services were losing the ability to catch criminals because of advances in technology and that the law needed to be updated to give a "clear legal framework" for access to some internet records.

The changes suggested by Labour include:

* A guarantee that the political activities of campaigners for justice, trade unionists and bereaved families will not be spied on using the new legislation.

* A clear definition of protecting "national security" and "economic wellbeing", which are the current conditions that justify the use of the new powers.

* A proportionate list of crimes that would justify allowing police and security services to access someone's internet connection record.

* Restrictions on the number of law enforcement agencies that would be allowed to use the legislation.

* Better protections for the confidential communications of "sensitive professions", such as MPs with constituents, lawyers with clients and journalists with sources.

* Approval for interception to be granted by judges on the basis of the evidence rather than merely whether the right process has been followed.

Burnham said: "The bill cannot be supported in its current form, but nor should we just oppose it because there is a deadline where the country needs new legislation.

"What I am saying very clearly to Theresa May is: here are very specific concerns that we have and unless you meet them we will not cooperate with getting this bill on the statute book by the end of the year. That is quite a significant statement."

The Daily Beast
Anti-ISIS-Propaganda Czar's Ninja War Plan: We Were Never Here
Tuesday, 15 March 2016
Byline: Kimberly Dozier

Washington - The Obama administration is launching a stealth anti- Islamic State messaging campaign, delivered by proxies and targeted to individual would-be extremists, the same way Amazon or Google sends you shopping suggestions based on your online browsing history.
At least that's the plan, revealed Monday, of new anti-ISIS message czar Michael Lumpkin, now that the White House has put the ink to the final legal measures establishing the Center for Global Engagement, which replaces previous less- than-successful efforts. The new executive order expands what Lumpkin can spend, who he can hire, and which parts of the U.S. government he can pull into the new campaign.

"I intend to do what we have done in special operations" to hunt ISIS terrorists, Lumpkin told The Daily Beast. "You need a network to defeat a network, so we're going to take a network approach to our messaging."

Those messages won't say "made in the U.S.A."

The new center "is not going to be focused on U.S. messages with a government stamp on them, but rather amplifying moderate credible voices in the region and throughout civil society," said Lisa Monaco, speaking at the Council on Foreign Relations last week. "Recognizing who is going to have the most legitimate voice and doing everything we can to lift that up and not have it be a U.S. message."

The idea is to give local nonprofits, regional leaders, or activists invisible financial support and technical expertise to make their videos or websites or radio programs look and sound professional--and let them own and distribute the message.

The center will also employ data analysts who will work with private industry partners to sift through the public information any user leaves on social media, to determine who might be leaning toward radicalism and message them directly--though how isn't clear yet.

"This is uncharted territory," Lumpkin said. "The U.S. government has not done this type of discrete scalpel-like messaging before."

Lumpkin is a former Navy SEAL who has political capital to spend after running special operations at the Pentagon since December 2013 and managing successful Joint Special Operations Command raids and the occasional drone strike in Syria and Libya, among other tasks.

He has been blunt in his critique of the previous messaging efforts by the much-maligned and now defunct Center for Strategic Counterterrorism Communications.

"Our response to their propaganda has been under-resourced, too slow, and too cautious," Lumpkin said in comments before the Global Special Operations Forces Symposium last month in Palm Harbor, Florida. "In the face of a nimble, adaptive opponent unconstrained by truth or ethics, our people are left swimming in bureaucracy, using outdated technology," he told the audience of current and former special operators.

Lumpkin has fought to double the center's budget from $10 million last year to more than $20 million requested for next year, and he says he'll ask for more after that.

The new center will work a bit like a Hollywood talent agent--finding other, more legitimate voices and making them the star. It will rely on embassies worldwide to reach out to local leaders, media professionals, and others to join the messaging network. The State Department will also help them develop the material.

Frustratingly for journalists and other advocates of government transparency, the center will seldom reveal who it is supporting, just as special operators don't reveal the forces they are training unless that nation chooses to reveal it.

"I don't want to burn our partners," Lumpkin said, while acknowledging that his office is already working with a handful of non-governmental agencies, some of which approached his office for help.

"We're helping guide them, hiring out content to be developed, giving them the contact," Lumpkin said. "They will put their own logos on it and call it their own, which I am very happy with, and then we can

help amplify it and hand it to other people to repurpose it, but they're kind of on their own once they've got it."

The Daily Beast tracked down two of the regional experts working with the State Department, who agreed to describe their cooperation on condition that they were not identified. They said they had approached the State Department for funding, and got a small grant, with the only stipulation being that they make whatever they produced available to the public.

That means these U.S.- funded programs will produce material that may travel the Web and be seen by American citizens--an issue Lumpkin acknowledges.

"Clearly at the State Department, we don't message U.S. citizens," Lumpkin said. That would be done by the new Homeland Security office to counter violent extremism, which is in a similarly embryonic stage.

But if a U.S. citizen comes across the material, it's the same as choosing to follow the State Department's anti- ISIS Twitter account, he added.

Then there's the delivery of the content. That's where the big data analysts come in. Lumpkin will be contracting private companies that crunch the public trail of information Internet users leave behind, just like they do for large retailers looking for new buyers.

His team has also met with social media companies to explore the parameters of their privacy agreements and hear how they police their sites for violent extremism.

It's a touchy subject at social media companies, in an era when so many firms were burned by the revelations of cooperation in the Edward Snowden documents.

Facebook spokesman Jodi Seth said they'd shared research with Lumpkin and other administration officials showing "factors that help make counter-speech more successful," including the format of the content (i.e., generally it is better to share photos and video instead of text) and tone of the content (the most successful forms of counter-speech were constructive, and satire and humor worked better than attacks).

She added that the research shows the speaker is very important and should be directly related to the targeted audience, sometimes a celebrity, sometimes a former extremist or community leader--all advice Lumpkin has obviously incorporated into the new program.

"Twitter is largely a public service and the U.S. government may review public accounts on its own. Government requests for non-public information are reviewed pursuant to our privacy policy and law enforcement guidelines, and disclosed in our transparency report," he wrote.

"They clearly have business equities... and they have privacy arrangements with their customers and we don't want to infringe on that," Lumpkin said. There's plenty that can be learned from "open source" information, i.e., information that anyone with a laptop can find on the Web.

"The big data is there. You just have to figure out how to use it," he said.

When he took charge, he put a stop to tweeting at terrorists--engaging in open rhetorical battles with hardcore ISIS followers on public social media platforms, as previous iterations of the new Global Engagement Center had done. Previous leaders had stopped the tweet battle in English, but continued it in Arabic and other regional languages.

"Those are hardcore followers, so we decided it's not worth our energy to focus on them," one official involved in the program explained.

Lumpkin wants to focus on those who are vulnerable to ISIS's message and emulate how ISIS goes after its followers.

"Usually it starts on Twitter, then it goes to Facebook, then it goes to Instagram, and ultimately, it goes to Telegram or some other encrypted, point-to-point discussion," he said. "They are doing what Amazon does. They are targeting selected information to an individual based on their receptivity. We need to do the same thing."

The office has flip-flopped through different leaders and strategies, with uneven-to-little success. The State Department's Twitter handle Think Again, Turn Away has only 26,000 followers, and much of the anti-ISIS propaganda videos it has released on a dedicated YouTube channel has been widely panned as "gruesome."

Back in 2014, senior State Department officials touted their success in stemming the flow of ISIS recruits. But the numbers released by the U.S. intelligence community soon overturned that assessment, rising from an estimated 7,000 foreign fighters in Syria and Iraq in 2014 to just above 38,000 foreign fighters now, with many of them counted in the ranks of ISIS as well as al Nusra and other rebel groups.

Estimates of the size of ISIS tracked that rise, going from a few thousand to a high of 30,000 last year. An all-source intelligence estimate has since downgraded ISIS's size, to a range of 19,000-25,000 fighters in Iraq and Syria, though a U.S. intelligence official said that was due to "the combined effects of battlefield deaths, desertions, internal disciplinary actions, recruiting shortfalls, and difficulties that foreign fighters face traveling to Syria."

Lumpkin said he'll use sophisticated computer analytic programs to measure if the new messages being sent are resonating with the target population, but the only real measure is if the numbers of ISIS recruits goes down.

"The goal is that you have to stop the recruiting," he said. "You do that through those who are likely to be radicalized and catch them early... to make sure that the true nature of these violent extremist groups is well known so they don't end up joining. It's not what they think it is.

Epoch Times
Michael Chan's Libel Suit: Globe and Mail Files Statement of Defence
Thursday, 17 March 2016
Byline: Omid Ghoreishi

The Globe and Mail's recently filed defence statement in a close to $5 million lawsuit by Ontario Immigration Minister Michael Chan says the paper was acting in the public good by exposing the minister's questionable dealings with China and the concerns they sparked at CSIS.
The Globe's argument centres on the relevance of its reporting on Chan as a public figure, information that the paper made public for the first time regarding interaction between the Canadian Security Intelligence Service and the Ontario government on Chan, and the "very thin investigation" on Chan's conduct by the provincial government.

The Globe reported that Ontario Premier Kathleen Wynne was unaware of CSIS's concerns regarding Chan's relationship with Chinese officials before her decision to promote Chan to the immigration and international trade file.

Chan's statement of claim describes the Globe's stories as old, "ludicrous" allegations and an attempt to boost circulation. The Globe counters that Chan is a public figure who has been placed in a sensitive post even after CSIS took the extraordinary step of approaching the province to have him investigated.

Globe Reports on Chan

Last year, the Globe and Mail published a series of stories about Chan revealing that he was one of the two provincial ministers that then-CSIS director Richard Fadden said in 2010 were feared to be under foreign influence.

Chan has fiercely denied any wrongdoing, calling the Globe stories a "re-hash of ludicrous allegations." He is defended by Wynne.

But the Globe's editor-in-chief David Walmsley, one of the defendants, has said the paper stands by its articles.

The Lawsuit

Filed last August in Ontario's Superior Court of Justice, Chan's lawsuit names Walmsley, the paper's publisher Phillip Crawley, and Craig Offman, the main reporter and author of the articles, as defendants. Offman spent 10 months investigating Chan. Also named is Charles Burton, an associate professor at Brock University who wrote an editorial on the topic in the Globe.

Chan's statement of claim says the Globe's coverage didn't offer anything new, and that the paper published the articles to attract "reader (and paid subscriber) attention and leading to greater revenues" after what it describes as the paper's loss of readership in recent years.

"[The Globe and Mail] had been perceived as not having strength in investigative journalism, and most particularly as having fallen behind the Toronto Star in that area," the statement reads.

It adds that Offman didn't provide Chan with adequate opportunity to comment on the claims in the articles, and that from a "thin and fragile thread," Offman and the Globe proceeded to "weave together a story that would portray for readers the picture that there was a reasonable basis for readers to doubt Michael Chan's loyalty to Canada or for an investigation of that issue."

The Globe's statement says Offman gave opportunities to Chan to respond to issues raised in the articles, including a face-to-face interview and follow-up questions, calling it "disingenuous to suggest that Chan did not have an adequate opportunity to address the concerns of CSIS with Offman."

The Globe's statement also says the story has far from run its course, since "Chan remains a publicly accountable elected representative and cabinet minister in Ontario government."

CSIS's Concerns

In interviews with the CBC in 2010, Fadden, who at the time was the director of CSIS, expressed concerns that two Canadian provincial cabinet ministers are being influenced by foreign governments, without naming any names.

According to the Globe, Fadden had sent a top-secret memo to the federal minister of public safety identifying Chan as one of those cabinet ministers. Following this, the government of Ontario conducted what the Globe describes as "a very thin investigation" of the issue, consisting of a few phone calls.

Concerned by the lack of adequate response by the Ontario government, "CSIS undertook the extraordinary step" of sending a high-level official to ask the provincial government to revisit the issue, the Globe's statement says. Offman's articles were the first to expose those discussions.

Seven issues were raised by CSIS, the Globe says, but the articles only reported on the three that the paper could confirm--two of which centred on Chan's close ties with the Chinese consul-general in Toronto. The third was Chan's possible ownership of two properties in China, which were undisclosed.

Following the CSIS official's visit, the Ontario government engaged the province's integrity commissioner to interview Chan, according to the statement. The matter was disposed of by the commissioner in one to one-and-a-half days, and in October 2014, then-Premier Dalton McGuinty told the public that the matter was closed.

The Globe argues that the integrity commissioner lacks expertise in matters relating to foreign influence.

After Wynne became premier, Chan's cabinet post was changed from minister of tourism and culture to minister of citizenship, immigration, and international trade.

"This elevation in Chan's portfolio placed him in a pivotal position vis-a-vis relations with China, Ontario's second largest trading partner," reads the Globe's statement, adding that Wynne said she had "no information from CSIS, the federal government, or anyone on the matter."

"It is a matter of immense public interest that deserves serious scrutiny," reads the Globe's defence.

Deserving of Consideration'

According to the Globe's statement, Chan's actions while in office are "deserving of consideration."

Chan lobbied to bring the Confucius Institute--controversial Beijing-run institutes intelligence agencies describe as a tool to extend China's soft power--to the Toronto District School Board, even though the institute is not in his riding and education is not within his portfolio.

Among those considerations are: Chan's lobbying efforts to bring the controversial Confucius Institute to the Toronto District School Board; his hiring of Michael Huang, who has a history of taking pro-Beijing causes, as a constituency assistant, as well as Wilson Chan, a former editor with a Toronto Chinese-language newspaper who was fired for censoring anti-Beijing coverage and is now working for Wynne's office in charge of the ethnic media portfolio; and his statements publicly downplaying the importance of Hong Kong's Umbrella Movement.

"Such a stance by Chan flies in the face of Canadian values regarding the proper role of democracy in society," says the Globe's statement, referring to the latter consideration.

The statement also cites an interview, first reported by the Epoch Times, given by Chan to the Chinese state-run Xinhua news agency related to his personal trip to China in 2009 where he attended the 60th anniversary of the founding of the Chinese Communist Party. In the interview, Chan said: "Great is my motherland. Great are the people of my motherland. ... Today seeing the [People's Liberation] army on parade with such precision and the high spirits of the people, I am moved even more by the strength and power of my motherland."

"The Globe and Mail defendants plead that the reporting in the articles was in the public interest in that it provided a detailed examination of the CSIS concerns and the Ontario government's unilateral and opaque decision to declare the matter closed," the Globe's statement says.

Paul Gaboury
Fonction publique fédérale Les critiques sur les réseaux sociaux interdites
Thursday, 17 March 2016
Byline: Paul Gaboury

Ottawa - Les employés fédéraux ne peuvent se servir des médias sociaux pour critiquer les décisions prises par leur employeur.
C'est l'avertissement qu'a lancé le ministère des Services publics et de l'Approvisionnement aux employés fédéraux qui utiliseraient ces jours-ci les médias sociaux pour faire part de leur mécontentement, notamment sur la situation au Bureau de la traduction.

Sous le couvert de l'anonymat, un employé se disant « désespéré » a indiqué au Droit, mardi, qu'une « chasse aux délinquants » était lancée pour trouver les employés qui utilisent les médias sociaux pour commenter les décisions prises par la direction du Bureau de la traduction, notamment sur l'outil de traduction automatique qui est au coeur d'une controverse et de récents débats à la Chambre des communes.

Invité à réagir, le ministère des Services publics et de l'Approvisionnement, responsable du Bureau de la traduction, n'a pas voulu confirmer au Droit si des employés ont été sanctionnés jusqu'à maintenant pour des commentaires émis sur les réseaux sociaux.

Toutefois, le ministère a rappelé aux fonctionnaires que les règles d'éthique en vigueur dans la fonction publique fédérale leur interdisent d'utiliser les réseaux sociaux pour émettre des critiques sur les gestionnaires.

« Le gouvernement du Canada a mis en place plusieurs mécanismes qui permettent aux employés de fournir de la rétroaction directe ou indirecte à ses cadres. L'utilisation des médias sociaux à cette fin contrevient aux règles d'éthique établies dans la fonction publique. Cette politique n'est pas en vigueur uniquement dans la fonction publique, mais aussi auprès de bien d'autres employeurs », a indiqué dans un courriel Jessica Kingsbury, porte- parole de Services publics et Approvisionnement Canada.

Avertissement des syndicats

Dans un avis sur l'utilisation des médias sociaux, en 2012, les principaux syndicats du secteur public fédéral avaient recommandé à leurs membres utilisateurs de Facebook et Twitter de se servir d'un ordinateur domestique et d'une adresse de courriel personnelle, et d'éviter de faire des commentaires visant des particuliers ou des ministères précis. On y indiquait qu'ils n'étaient pas à l'abri de la surveillance de l'employeur simplement parce que leur profil était protégé par des filtres de confidentialité.

L'avis mettait aussi en garde les employés contre les conséquences graves pour les employés qui seraient reconnus coupables de conflits d'intérêts ou de pas avoir suivi les codes et lois. Dans ces cas, l'avis rappelait que les employés risquaient des mesures disciplinaires, pouvant aller « jusqu'à la destitution », et les invitait à faire preuve « d'autant de professionnalisme » en participant à cette campagne que dans leurs fonctions pour l'employeur.

Motherboard (Vice)
'Chilling Effect' of Mass Surveillance Is Silencing Dissent Online, Study Says
Thursday, 17 March 2016
Byline: Nafeez Ahmed

New York - Thanks largely to whistleblower Edward Snowden's revelations in 2013, most Americans now realize that the intelligence community monitors and archives all sorts of online behaviors of both foreign nationals and US citizens.
But did you know that the very fact that you know this could have subliminally stopped you from speaking out online on issues you care about?

Now research suggests that widespread awareness of such mass surveillance could undermine democracy by making citizens fearful of voicing dissenting opinions in public.

A paper published last week in Journalism and Mass Communication Quarterly, the flagship peer-reviewed journal of the Association for Education in Journalism and Mass Communication (AEJMC), found that "the government's online surveillance programs may threaten the disclosure of minority views and contribute to the reinforcement of majority opinion."

The NSA's "ability to surreptitiously monitor the online activities of US citizens may make online opinion climates especially chilly" and "can contribute to the silencing of minority views that provide the bedrock of democratic discourse," the researcher found.

The paper is based on responses to an online questionnaire from a random sample of 255 people, selected to mimic basic demographic distributions across the US population.

Participants were asked to answer questions relating to media use, political attitudes, and personality traits. Different subsets of the sample were exposed to different messaging on US government surveillance to test their responses to the same fictional Facebook post about the US decision to continue airstrikes against the Islamic State of Iraq and Syria (ISIS).

They were then asked about their willingness to express their opinions about this publicly--including how they would respond on Facebook to the post; how strongly they personally supported or opposed continued airstrikes; their perceptions of the views of other Americans; and whether they supported or opposed online surveillance.

The study used a regression model--a statistical method to estimate the relationships between different variables--to test how well a person's decisions to express their opinion could be predicted based on the nature of their opinion, their perceptions of prevailing viewpoints, and their attitude to surveillance.

This sort of model doesn't produce simple percentages, but provides a statistical basis to explain variances in the factors being tested. In this case, the study found that "35% of the variance in an individuals' willingness to self-censor" could be explained by their perceptions of whether surveillance is justified.

For the majority of respondents, the study concluded, being aware of government surveillance "significantly reduced the likelihood of speaking out in hostile opinion climates."

Although more nuanced than a blanket silencing, the study still concluded that "knowing one's online activities are subject to government interception and believing these surveillance practices are necessary for national security play important roles in influencing conformist behavior."

Perhaps unsurprisingly, the most significant conformist effect was from people who supported surveillance. They turned out to be more likely to conceal other dissenting opinions, which they felt strayed from the majority view.

When such individuals "perceive they are being monitored, they readily conform their behavior--expressing opinions when they are in the majority, and suppressing them when they're not," the paper concluded. These findings suggest that a person's "fear of isolation from authority or government" adds new "chilling effects" to public discourse.

"What this research shows is that in the presence of surveillance, our country's most vulnerable voices are unwilling to express their beliefs online," said Elizabeth Stoycheff, associate professor of journalism and new media at the Department of Communication, Wayne State University, and lead author of the paper. "This finding is problematic because it may enable a domineering, majority opinion to take control of online deliberative spaces, thus negating deliberation."

But, she added, the increasing complexity of surveillance, and its use in tandem with private industry, means that more research is essential to understand how surveillance is altering the way people interact online, with content, and with one another.

The study happens to confirm recent comments by Snowden himself last Saturday, during a live video address to a gathering of whistleblowers, journalists and technologists in Berlin.

"It's the minorities who are most at risk" from the impact of mass surveillance, Snowden said. "Without privacy there is only society, only the collective, which makes them all be and think alike. You can't have anything yourself, you can't have your own opinions, unless you have a space that belongs only to you."

The Hill
NSA dismissed Clinton request for 'secure' BlackBerry
Thursday, 17 March 2016
Byline: Julian Hattem

Washington - Federal intelligence officials rebuffed an early effort by Hillary Clinton's top aides to provide her with a "secure 'BlackBerry- like'" device to use while serving as secretary of State, according to new emails released Wednesday.
Emails released as part of an open records lawsuit from conservative legal watchdog Judicial Watch show that the National Security Agency (NSA) rebuffed requests from the State Department in February of 2009 to find a replacement for Clinton's mobile device.

"[T]he current state of the art is not too user friendly, has no infrastructure at State, and is very expensive," Donald Reid, a top security official at the State Department, wrote in a Feb. 13, 2009, email.

"[E]ach time we asked the question, 'What was the solution for [the president]?' we were politely told to shut up and color," he added.

In another email, Reid described Clinton as being "hooked" on her BlackBerry following the 2008 presidential campaign. But she felt "hamstrung" when she had to lock it up before entering secure spaces at the State Department.

Clinton and her aides "are used to having the BB on their hip and staying closely in touch with developments during the day," he wrote.

It's unclear from the emails how the matter was ultimately resolved.

The NSA appears not to have shut the State Department down entirely.

The agency "opened the door for us to establish requirements and they would try to help," Reid wrote in the Feb. 13 message.

In a Feb. 18 email, Reid wrote that he and his staff would "be working with NSA on a set of possible options to meet [Clintons'] and others requirements."

In the same email, Reid noted that a briefing with officials from the NSA and Cheryl Mills, Clinton's then-chief of staff, prompted NSA staffers to raise "a host of related issues" about what Clinton and her staff "have been briefed on with respect to travel and technology vulnerabilities."

Clinton's use of a private email server throughout her tenure as secretary of State has become a nagging political problem for her presidential campaign. Critics contend that it may have skirted federal recordkeeping laws and could also have jeopardized U.S. secrets.

Reid is the security coordinator for security infrastructure in the State Department's diplomatic security bureau. Earlier this week, he and Mills was listed as two of eight people whom Judicial Watch wanted to testify about the setup of Clinton's private email server, as part of a separate case.

FCW.com (US)
Rogers makes his case for a CyberCom budget boos
Thursday, 17 March 2016
Byline: Sean Lyngaas

Washington - U.S. Cyber Command Commander Adm. Michael Rogers on March 16 told appropriators that his command deserves an approximately nine percent budget hike in an increasingly contested cyber environment.
Against a backdrop of sizable nation-state and criminal threats, Cyber Command is right now engaged in a "range of both defensive and offensive real-world operations," Rogers told the House Armed Services Subcommittee on Emerging Threats and Capabilities. One of those operations is hacking the so-called Islamic State after being ordered to do so by Defense Secretary Ash Carter.

Cyber Command is asking for $506 million for fiscal 2017, Rogers advisers said after his testimony. The command's appropriated budget for fiscal 2016 is $466 million, with $207 million of that going to support the command's cyber mission forces, according to Rogers' written testimony.

Over five years since its inception, Cyber Command has reached a "tipping point" in terms of offensive and defensive capabilities, according to Rogers. "We're trying to use some of the real world insights" gleaned from the Office of Personnel Management hack and the campaign against the Islamic State to furnish combatant commands with greater cyber tools, he told lawmakers.

Cyber Command's budget is dwarfed by that of the National Security Agency, which Rogers also heads, but the command has used NSA's technical prowess to grow more adept in cyber operations.

Lawmakers were generally receptive to Rogers' funding requests. However, Rep. Mo Brooks (R- Ala.) sounded a note of caution.

"America's financial condition has taken a fairly stark turn for the worse," Brooks told Rogers.

Rogers replied that part of the reason his command is co-located with NSA is to avoid duplicative funding. Cybersecurity is a field that requires more spending, Rogers argued. "Look at the world around you," he told Brooks, referring to threats in cyberspace.

Rep. Joe Wilson (R-S.C.), the subcommittee's chairman, said the panel was ready to back Rogers' programmatic needs.

"From the intrusion on the Joint Staff networks to the compromise of personal information of millions of government personnel and their families, cyber is proving to be both a domain of warfare on its own, as well as a key enabler for all other domains of war," Wilson said in his opening statement.

The fiscal year 2016 defense policy bill that became law last November granted Cyber Command enhanced acquisition authorities, including the designation of an executive in charge of negotiating agreements with other military departments.

Rogers praised those new acquisition authorities, calling them a "significant augmentation" in the command's ability to hone its mission force.

Cyber Command has a representative at the Pentagon's Silicon Valley outpost, known as the Defense Innovation Unit Experimental, and the admiral was in Northern California earlier this month to push for expanded partnerships with the private sector. The command's next planned "point of presence" for private-sector outreach is Boston, he said at the March 16 hearing.

Baltimore Sun
Cyber Command chief: Foreign governments use criminals to hack U.S. systems
Thursday, 17 March 2016
Byline: Ian Duncan

Washington - Foreign governments are building relationships with criminals and other hackers to hide their attempts to break into American computer systems, the head of U.S. Cyber Command told members of Congress on Wednesday.
"It potentially or theoretically makes it more difficult to go country X and say we see this activity going on, you are doing it, this is unacceptable to us," Adm. Michael S. Rogers said. "And their ability to say it's not us, it's criminal groups."

Rogers, who leads both Cyber Command and the National Security Agency at Fort Meade, said criminals remain the most numerous threat to American networks and people's data, but foreign governments have the patience, skills and resources to carry out the most sophisticated attacks.

In prepared remarks, he focused on how Russia's state-backed hacking efforts sometimes overlap with the work of criminals.

"Russia has very capable cyber operators who can and do work with speed, precision and stealth," he said. "Russia is also home to a substantial segment of the world's most sophisticated cybercriminals, who have found victims all over the world."

The admiral's comments lent weight to those of analysts and lawmakers who have argued that the Russian government relies on criminal groups to carry out hacking attacks.

The U.S. government has not named Russia as the suspect in any particular attack, but the country is believed to be responsible for the breach of the email system of the Joint Chiefs of Staff last year. Officials regularly cite China, Iran and North Korea as other top hacking threats.

Rogers testified before a panel of the House Armed Services Committee on the budget for Cyber Command. The organization recently announced a campaign against the self-declared Islamic State.

It was the first time the United States has acknowledged carrying out a cyber warfare campaign. The details remain mostly secret.

"USCYBERCOM is executing orders to make it more difficult for ISIL to plan or conduct attacks against the U.S. or our allies from their bases in Iraq and Syria to keep our service men and women safer," he said.

Rogers said the command is looking to take on a greater role before conflict breaks out, using cyber power to dissuade adversaries from starting a conflict.

"We at USCYBERCOM are thinking more strategically about shifting our response planning from fighting a war to also providing decision makers with options to deter and forestall a conflict before it begins," he said.

For 2016, the command has a budget of almost $500 million and a staff of some 1,400 troops, civilians and contractors working at Fort Meade. Rogers said he expects the organization to be fully operational by fall of 2018.

Fox News
Clinton tried to change rules to use BlackBerry in secure facility for classified information
Thursday, 17 March 2016
Byline: Catherine Herridge

Washington - Less than a month after becoming secretary of state, and registering the personal email domain that she would use exclusively for government business, Hillary Clinton's team aggressively pursued changes to existing State Department security protocols so she could use her BlackBerry in

secure facilities for classified information, according to new documents released under the Freedom of Information Act.
"Anyone who has any appreciation at all of security, you don't ask a question like that," cybersecurity analyst Morgan Wright told Fox News. "It is contempt for the system, contempt for the rules that are designed to protect the exact kind of information that was exposed through this email set up. "

Current and former intelligence officials grimaced when asked by Fox News about the use of wireless communications devices, such as a BlackBerry, in a SCIF (Sensitive Compartmented Information Facility) emphasizing its use would defeat the purpose of the secure facility, and it is standard practice to leave all electronics outside.

A former State Department employee familiar with the Clinton request emphasized security personnel at the time thought the BlackBerry was only for unclassified material, adding their concerns would have been magnified if they had known Clinton's email account also held classified material.

"When you allow devices like this into a SCIF, you can allow the bad guys to listen in," Wright added.

A February 17, 2009 email marked SECRET and cleared through the NSA says, "Ms. Mills described the requirement as chiefly driven by Secretary Clinton, who does not use standard computer equipment but relies exclusively on her Blackberry for emailing and remaining in contact on her schedule etc. Ideally all members of her suite would be allowed to use Blackberries for communication in the SCIF (Sensitive Compartmented Information Facility)"

Cheryl Mills was Clinton's chief of staff from 2009-13.

The emails, obtained by Judicial Watch as part of a Freedom of Information Act lawsuit also show that a specialized NSA team was brought in to assess the vulnerabilities and feasibility of using wireless communications, including within a secure facility.

The NSA State Department liaison, whose name was withheld, told Mills in a now highly redacted email: "Sometimes the distinction between what can be done and what is, or is not, recommended to be done differ; this is one of those instances. (State Department Diplomatic Security) DS's response illustrates their level of concern based on their extensive professional expertise. "

Another memo from Mar?ch 2009, obtained by Judicial Watch through its FOIA lawsuit, from Assistant Secretary for Diplomatic Security Eric Boswell to Mills explicitly warned, "the vulnerabilities and risks associated with the use of Blackberries in Mahogany Row [seventh floor executive offices] considerably outweigh their convenience." Clinton has claimed she used the personal account and BlackBerry for convenience.

Clinton never used a State Department issued BlackBerry. It is not clear from the documents whether Clinton and her team went ahead and used their BlackBerrys in SCIFs despite the concerns, including

those of the NSA. Though a state department official said "no waiver allowing PDAs within Mahogany Row was granted.".

A February 18 2009 email from the State Department's Senior Coordinator for Security Infrastructure, Donald R. Reid, states "...once she (Clinton) got the hang of it, she was hooked, now every day, she feels hamstrung because she has to lock up her BB up. She does go out several times a day to an office they have crafted for her outside the SCIF and plays email catch-up. Cheryl Mills and others who are dedicated BB addicts are frustrated because they too are not near their desktop very often during the working day..."

The reference to a secondary office for Clinton appears to conflict with a February statement from the State Department that no stand-alone computer was set up outside Clinton's main office on the executive floor, known as Mahogany Row, to check her personal account.

On February 25, Fox News pressed the State Department spokesman about a January 2009 email, also obtained by Judicial Watch, between Under Secretary for Management Patrick Kennedy and then Clinton chief of staff Mills where Kennedy said it was a "great idea" to setup a stand-alone PC for Clinton to check her email.

The State Department said Wednesday no computer was set up but confirmed there was a space created to accommodate Clinton's personal email use. ?"There is an area dedicated to supporting the secretary outside but in the immediate vicinity of the secretary's secure office. Secretary Clinton, as with anyone, could use such non-SCIF spaces to check personal devices.," a State Department official said.

Clinton did not use a government-issued BlackBerry that was certified as secure for government use. Under Secretary for Management Patrick Kennedy recently told the Benghazi Select Committee that he knew about Clinton's personal account from the earliest days, but did not understand the extent of its use, even though he sent State Department business to Clinton via the Clintonemail account.

In January 2009, Clinton signed at least two non-disclosure agreements in which she promised to protect classified information. Since then, more than 2,100 emails containing classified information have been identified, as well as 22 Top Secret that are too damaging to national security to release.

Earlier this week, Judicial Watch presented the federal court in Washington with a list of 7 Clinton aides it wants to question under oath about Clinton's use of a private email sever when she was secretary of state.

Adelaide Advertiser
Spycatcher warns of subs leaks from 'weakest link'
Thursday, 17 March 2016
Byline: Tory Shepherd

One of the world's top spy fighters says he would be "shocked" if Chinese spies were not trying to hack our military capabilities.
Kevin Mandia, a cybersecurity guru, also said it was likely that elements of Australia's Future Submarines would leak out.

Russia "might" target Australia, but China had been "honing their skills" and were the main culprits, he said. Mr Mandia founded the first company dedicated to responding to attacks and is now the president of FireEye, a US-based cybersecurity firm. He is in Canberra this week meeting with MPs and officials.

Mr Mandia said military, defence, industrial capabilities as well as companies doing mergers and acquisitions and any experts on China who advised the Australian Government were among the likely targets.

"I'd be shocked and astonished if the Chinese aren't actively targeting any military capability here," he said.

Asked whether he thought it was possible to keep data related to the submarines safe, he said it would be difficult because of the immense complexity of the project.

"The more companies that work on things, the more suppliers involved in building something and the longer it takes to do it the more (difficult) it becomes to secure. It will become a challenge," he said. "You'll be as secure as the weakest link." The Advertiser revealed last year that France, Germany and Japan - the three countries vying to build the submarines - had all been attacked by Chinese spies.

All three recognise it was a top priority to protect top-secret information and use the best technology possible to protect themselves.

The Defence Department is aware of cyber attacks but say there is no evidence any of Australia's classified information has been compromised to date, while industry is also exposed to constant attempts.

In the recently released Defence White Paper the Government has pledged up to $400 million for cybersecurity capability development over 10 years.

Billions more will be spent on developing electronic warfare to protect Defence assets, modernised intelligence systems, enhanced surveillance and a larger workforce to tackle evolving threats.

"Australia will develop its cyber capabilities to deter and defend against the threat of cyber attack," the White Paper states.Last year a Japanese Government official told The Advertiser that there had been

Chinese cyberattacks on their classified information, while German shipbuilders TKMS said they were fending off up to 40 hacking attempts a day.

Press Trust of India
India's billion-member biometric database raises privacy fears
Thursday, 17 March 2016

New Delhi - India's parliament is set to pass legislation that gives federal agencies access to the world's biggest biometric database in the interests of national security, raising fears the privacy of a billion people could be compromised.
The move comes as the ruling Bharatiya Janata Party (BJP) cracks down on student protests and pushes a Hindu nationalist agenda in state elections, steps that some say erode India's traditions of tolerance and free speech.

It could also usher in surveillance far more intrusive than the US telephone and internet spying revealed by former National Security Agency (NSA) contractor Edward Snowden in 2013, some privacy advocates said.

The Aadhaar database scheme, started seven years ago, was set up to streamline payment of benefits and cut down on massive wastage and fraud, and already nearly a billion people have registered their finger prints and iris signatures.

Now the BJP, which inherited the scheme, wants to pass new provisions including those on national security, using a loophole to bypass the opposition in parliament.

"It has been showcased as a tool exclusively meant for disbursement of subsidies and we do not realise that it can also be used for mass surveillance," said Tathagata Satpathy, a lawmaker from the eastern state of Odisha.

"Can the government ... assure us that this Aadhaar card and the data that will be collected under it -- biometric, biological, iris scan, finger print, everything put together -- will not be misused as has been done by the NSA in the US?" Finance Minister Arun Jaitley has defended the legislation in parliament, saying Aadhaar saved the government an estimated Rs150 billion ($2.2 billion, Dh8 billion) in the 2014-15 financial year alone.

A finance ministry spokesman added that the government had taken steps to ensure citizens' privacy would be respected and the authority to access data was exercised only in rare cases.

According to another government official, the new law is in fact more limited in scope than the decades-old Indian Telegraph Act, which permits national security agencies and tax authorities to intercept telephone conversations of individuals in the interest of public safety.

Those assurances have not satisfied political opponents and people from religious minorities, including India's sizeable Muslim community, who say the database could be used as a tool to silence them. "We are midwifing a police state," said Asaduddin Owaisi, an opposition MP.

Raman Jit Singh Chima, global policy director at Access, an international digital rights organisation, said the proposed Indian law lacked the transparency and oversight safeguards found in Europe or the US, which last year reformed its bulk telephone surveillance programme.

He pointed to the US Foreign Intelligence Surveillance Court, which must approve many surveillance requests made by intelligence agencies, and European data protection authorities as oversight mechanisms not present in the Indian proposal.

The Indian government brought the Aadhaar legislation to the upper house of parliament on Wednesday in a bid to secure passage before lawmakers go into recess.

To get around its lack of a majority there, the BJP is presenting it as a financial bill, which the upper chamber cannot reject. It can return it to the lower house, where the ruling party has a majority.

In its assessment of the measure, New Delhi- based PRS Legislative Research said law enforcement agencies could use someone's Aadhaar number as a link across various data sets such as telephone and air travel records.

That would allow them to recognise patterns of behaviour and detect potential illegal activities. But it could also lead to harassment of individuals who are identified incorrectly as potential security threats, PRS said.

Sunil Abraham, executive director of the Bengaluru-based Centre for Internet and Society, said Aaadhaar created a central repository of biometrics for almost every citizen of the world's most populous democracy that could be compromised.

"Maintaining a central database is akin to getting the keys of every house in Delhi and storing them at a central police station," he said.

"It is very easy to capture iris data of any individual with the use of next generation cameras. Imagine a situation where the police is secretly capturing the iris data of protesters and then identifying them through their biometric records."

Saudi Gazette
GCC paces world in cyber-preparedness
Thursday, 17 March 2016

Abu Dhabi - GCC countries are among the global leaders in cybersecurity preparedness, with the region's network security spend tripling to $1 billion by 2018, industry experts announced Wednesday at Infosecurity Middle East, part of ISNR.
With the region's rapid economic development and connectivity in the Internet of Things era - especially in critical national infrastructure, oil and gas, and financial services - the GCC's network security spend is set to grow from $340 million in 2012 to $1 billion by 2018, according to a new Frost & Sullivan report.

At Infosecurity Middle East's 6th International Cyber Crime Conference, localized from Europe's leading cyber security exhibition, law enforcement, legal, and business and IT experts debated and discussed Smart City, Internet of Things, and financial cyber security, the UAE National Agenda for Information Security, and online safety and privacy for children.

"As cyber-threats grow in complexity and severity, GCC organizations are among the world's most advanced in deploying solutions that proactively protect devices, user information, and corporate data. Infosecurity Middle East is an ideal platform to promote the global Mobile Security Alliance and our enterprise mobility management and end user computing solutions," said Ian Evans, Vice President of End User Computing at VMware, and EMEA Managing Director at AirWatch.

VMware AirWatch joins over 100 leading international exhibiting companies at Infosecurity Middle East, including Bitdefender, Blue Coat, Cyberoam Technologies, Dionach, Elettronica, Exclusive Networks, Huawei, QinetiQ, and Winsted.

"Everyone involved in cybersecurity must always keep in mind that customers have different weak spots and different processes, with risks needing to be managed in different ways. There are exciting opportunities around those cybersecurity solutions that can take the fear factor out of unknown quantities, and make them 'known', but there continues to be significant opportunities around those protection measures that apply the universe of known cyber threat knowledge, to keep us safe every day. Infosecurity Middle East is a major event for driving new business leads for our vendors, and enhancing the region's cybersecurity preparedness," said Nathan Clements, Managing Director, Exclusive Networks Middle East.

Providing hands-on cybersecurity expertise, Infosecurity Middle East, in partnership with (ISC2), the global leader in cyber education, is hosting more than 40 free-to-attend, hands-on workshops, including in risk, governance, and cloud security.

Infosecurity Middle East joins Emergency Response and Disaster Prevention, Fire Fighting Middle East, and Occupational Safety and Health Middle East at ISNR 2016. Organized by the UAE Ministry of Interior and Reed Exhibitions Middle East, ISNR 2016 runs till today (March 17) at the Abu Dhabi National Exhibition Centre.

Naharnet Newsdesk
Illegal Networks: Violating Country's Sovereignty Unacceptable
Thursday, 17 March 2016

Beirut - Telecommunications Minister Butros Harb stated on Wednesday that violations against the country's sovereignty and its national security are unacceptable, assuring that perpetrators behind the illegal internet networks will be punished.
"We will not accept violations against our national sovereignty and security, nor will we accept infringing on the privacy rights of the Lebanese. These crimes will not go unpunished," Harb stated in a press conference.

"The networks belong to suspicious sides and we consider it a crime against our sovereignty," he pointed out, in reference to the possibility that the networks can be breached by Lebanon's long-time foe Israel or any party that wants to spy on the country.

"We are in front of an extensive system with wide expertise. Some of the perpetrators have already been implicated in the Barouk scandal," he added.

Last week and during a meeting of the parliamentary media committee it was unveiled that a "mafia" is taking advantage of internet services by installing internet stations that are not subject to the state control.

The owners of these stations are buying international internet bandwidth with nominal cost from Turkey and Cyprus which they are selling back to Lebanese subscribers at reduced prices.

Harb added: "Some sensitive state departments were victims of illegal internet providers," he said pointing out that they inadvertently subscribed to the services at a nominal cost and sometimes for free.

He stressed that the file was referred to the related judicial and security authorities.

The Minister stressed that the equipment were confiscated, he said: "Our technical teams were able to uncover unlicensed technical equipment in different locations on several mountainous terrains."

Later during the day, Head of the parliamentary media committee MP Hassan Fadlallah said after a weekly meeting of lawmakers with Speaker Nabih Berri: "The parliament will address the illegal internet network. We are faced with a system that works in parallel to that of the state and it is open to Israeli spying."

It has been reported that wireless internet towers and technical equipment were placed lawlessly in some mountainous terrains including Tannourine, al-Dinnieh, Sannine and al- Zaarour.

Smuggled internet services initiate risks namely the possibility of security breach as it lacks the basic control standards exposing Lebanon's security to third parties including Israel.

Adding to the above is the fact that smuggling online services outside legal frameworks is a waste for the state's treasury amounting to over $2 million losses on a monthly basis.

In 2009, a telecommunications station in the Barouk area of the Shouf was uncovered, triggering heated debate on the involvement of Israel in spying operations.

Globe and Mail
We need stronger limits on Apple-style court orders
Saturday, 19 March 2016
Byline: Gerald Chan & Stephen Aylward

Comment: Apple Inc. CEO Tim Cook has recently grabbed headlines for his company's strong stance on digital privacy. The U.S. Federal Bureau of Investigation obtained a court order requiring Apple to bypass the security lock features on an iPhone belonging to one of the shooters in the San Bernardino terrorist attack, and Apple is appealing the order.
Canadian iPhone users following this legal skirmish may not be aware that the same issue has already arisen on this side of the border. The scope of our privacy protections, however, remains uncertain even as police become increasingly reliant on technology companies for assistance. Canada needs clearer and stronger limits on when law enforcement can compel private companies to undermine the digital security of their users.

After rumours surfaced in 2013 of a video showing former mayor Rob Ford smoking crack cocaine, Toronto police began investigating Mr. Ford and his driver, Alexander Lisi. Police obtained a search warrant for Mr. Lisi's iPhone, which they believed would contain evidence linking Mr. Ford or Mr. Lisi to criminal activity.

When they discovered that it was locked with a passcode, they returned to court for an "assistance order" requiring Apple to provide "reasonable technical assistance" to bypass the code. An Ontario judge granted the order.

Because Apple did not contest the order, however, the judge gave no reasons explaining his decision.

Apple has now begun to push back against similar orders in the United States. The Lisi order is virtually identical to an order that Apple successfully opposed in a New York court case decided last month. The San Bernardino order is also similar, although it goes one step further - it requires Apple to create new software to bypass the passcode lock because the iPhone model has more advanced security features.

Until recently, "assistance orders" such as the one in the Lisi case, have played a minor supporting role in criminal investigations. They have been used to allow police access to a building or to make copies of documents.

In a case involving Telus last year, however, assistance orders were given more muscle.

Telus challenged an assistance order requiring it to disclose customer name and address information to police as being overly intrusive. In a setback for technology companies, an Ontario court ruled that assistance orders can go further than connecting wires and flipping switches. They can require a company to do what is necessary to help a warrant "succeed at its intended objective."

Police may also resort to the "production order" power in the Criminal Code, which allows them to require a company to produce data within its control.

This, however, may be a more challenging route. It is arguable that the data in the iPhone is not within Apple's "control" if it has to create new software in order to access it. Even if it is, a company can resist a production order on the basis that it would be "unreasonable in the circumstances" (i.e., too onerous).

Canadian companies have had some success challenging production orders. Earlier this year, Rogers and Telus successfully challenged a set of "tower dump" production orders that would have required them to produce call records of more than 40,000 customers (capturing anyone who happened to be near specified cellular towers). The court found that the requested orders went too far because they were not "minimally intrusive" of customer privacy.

Finally, if neither the "assistance order" or "production order" power suffices, police may try to obtain a "general warrant." This is the residual, catch-all power in the Criminal Code that allows police to "use any device or investigative technique or procedure or do any thing described in the warrant" that is not authorized elsewhere in the code.

Most notably, general warrants have been used to authorize police to do "sneak and peek" searches (covert entries into homes and other properties) in drug cases. Whether the "general warrant" can go so far as to require a company like Apple to create software to bypass its own security features remains to be seen.

In the digital age, the keys to our privacy are held by companies like Telus, Rogers and Apple.

We rely on these companies to protect our data, defend our privacy and guard against hackers.

But until the law catches up with technology, Canadians cannot be sure how their personal information will be protected when law enforcement comes knocking.

This situation does not serve either the privacy or the security of Canadians.

Gerald Chan and Stephen Aylward are lawyers at Stockwoods LLP in Toronto.

Gulf News
Twitter helps connect leaders with people
Monday, 21 March 2016
Byline: Janice Ponce de Leon

Dubai - From announcing new laws to restructuring the cabinet and warning people about accidents and crimes, the UAE government has strengthened its public service by connecting to people in real-time, one tweet at a time.
The micro-blogging site Twitter over its first 10 years of existence has become popular among UAE leaders and government agencies. This comes as no surprise as Twitter has become the social media of choice for world leaders, including His Highness Shaikh Mohammad Bin Rashid Al Maktoum, Vice-President and Prime Minister of the UAE and Ruler of Dubai.

Shaikh Mohammad is one of the world's top 10 most followed world leaders. He ranked fourth in the World Leaders on Twitter ranking report in December 2015, up by two spots in 2014 and with a growth in followers of almost two million. Since joining Twitter in June 2009, Shaikh Mohammad (@HHShkMohd) has garnered 5.85 million followers and made 3,824 tweets.

Shaikh Mohammad has used Twitter to announce government efforts and decisions such as the major restructuring of the federal government in February, and new policies such as mandatory military service in the UAE, among others.

"The significance of these [social media] channels lies in their ability to reach out easily to all members of the society through personal devices," Shaikh Mohammad said at the Social Media Influencer Summit in 2015.

Twiplomacy, a leading global study of world leaders on Twitter, described Shaikh Mohammad's tweets as engaging and have made him "approachable to the masses and his open engagement with audiences on all social platforms demonstrates the UAE government's efforts to be open to dialogue".

To further enhance the dialogue process, Shaikh Mohammad transformed the traditional majlis (Arabic for 'council') into a technology-based citizen engagement platform during the UAE Brainstorming Session last year, according to the Arab Social Media Report 2015.

Thousands of followers proposed more than 82,000 new ideas and innovative solutions through social media, focusing on the challenges in the public health and education sectors.

As a whole, the UAE leads the Gulf countries in terms of social media use and penetration, according to Twiplomacy. After Shaikh Mohammad, Shaikh Abdullah Bin Zayed Al Nahyan, Minister of Foreign Affairs and International Cooperation, has become the second most followed foreign minister on Twitter.

Twitter-friendliness extends to other government entities such as the Ministry of Interior (@moiuae) and Dubai Police that are actively tweeting to their audiences. Both warn people about road accidents, traffic updates, crime prevention, useful hotlines and their latest initiatives.

Dubai's Roads and Transport Authority (@RTA_Dubai) also tweets about opening new bridges and roads, road closures, traffic updates, and many more. Another source of real-time information is the

National Centre of Meteorology and Seismology's Twitter page (@NCMS_media) that contains the latest weather forecasts, live updates and warnings on rain, thunderstorms, and earthquakes.

Washington Post
FBI aids search for culprits in huge cyberheist attempt
Monday, 21 March 2016
Byline: Serajul Quadir

Dhaka, Bangladesh - Police met an FBI official here in the capital of Bangladesh on Sunday to try to track down culprits behind an attempted $951 million cyberheist from the country's central bank.
Initial investigations aim to identify the origin of a transfer order for $81 million that the Federal Reserve Bank of New York paid from Bangladesh Bank's account there to casinos in the Philippines, a senior police official told reporters.

The transfer, one of the largest cyberheists in history, was among 35 requests that unknown hackers made for payments from the bank's New York Fed account in early February.

Other requested transfers from that account, which the country uses for international settlements, apparently were blocked.

Former finance secretary Fazle Kabir took over Sunday as head of the central bank after Atiur Rahman, the former governor, resigned amid complaints from the government that it had learned of the heist only a month later from the media.

Also Sunday, the wife of a cybercrime expert reported that her husband, Tanvir Hassan Zoha, had been abducted early Thursday. He had met with police Tuesday and told the media that he knew three of the user IDs used in the heist.

Senior police official Mirza Abdullahel Baqui said after meeting the FBI official that criminals in six countries apparently were involved in the heist.

"This is the biggest transnational organized crime ever seen in Bangladesh, and so we sought both technical and human assistance" from the FBI, he said.

The officials also discussed how to proceed with their investigation, he added.

A government investigative committee led by former central bank governor Mohammad Farash Uddin began its probe Sunday. "This is a wake-up call," he said of the unprecedented breach in the bank's computer security.

A Senate hearing in the Philippines last week included testimony that $30 million of the total $81 million haul was delivered in cash to an ethnic Chinese casino junket operator in Manila. The rest was transferred to two casinos in the Philippines.

According to his wife, Kamrun Nahar Chowdhury, cybercrime expert Zoha was blindfolded by unknown plainclothes people early Thursday before being taken away in a vehicle.

Chowdhury said that police had refused to investigate her husband's disappearance and that she had appealed to the government for help. Police were unavailable for comment.

"We don't know why he was picked up," she said.

Washington Post
Johns Hopkins researchers poke a hole in Apple's encryption
Monday, 21 March 2016
Byline: Ellen Nakashima

Washington - Apple's growing arsenal of encryption techniques -- shielding data on devices as well as real-time video calls and instant messages -- has spurred the U.S. government to sound the alarm that such tools are putting the communications of terrorists and criminals out of the reach of law enforcement.
But a group of Johns Hopkins University researchers has found a bug in the company's vaunted encryption, one that would enable a skilled attacker to decrypt photos and videos sent as secure instant messages.

This specific flaw in Apple's iMessage platform likely would not have helped the FBI pull data from an iPhone recovered in December's San Bernardino, Calif., terrorist attack, but it shatters the notion that strong commercial encryption has left no opening for law enforcement and hackers, said Matthew D. Green, a computer science professor at Johns Hopkins University who led the research team.

The discovery comes as the U.S. government and Apple are locked in a widely watched legal battle in which the Justice Department is seeking to force the company to write software to help FBI agents peer into the encrypted contents of the iPhone used by Syed Rizwan Farouk, one of two attackers who were killed by police after the shooting rampage that claimed 14 lives.

Cryptographers such as Green say that asking a court to compel a tech company such as Apple to create software to undo a security feature makes no sense -- especially when there may already be bugs that can be exploited.

Apple's growing arsenal of encryption techniques -- shielding data on devices as well as real-time video calls and instant messages -- has spurred the U.S. government to sound the alarm that such tools are putting the communications of terrorists and criminals out of the reach of law enforcement.

But a group of Johns Hopkins University researchers has found a bug in the company's vaunted encryption, one that would enable a skilled attacker to decrypt photos and videos sent as secure instant messages.

This specific flaw in Apple's iMessage platform likely would not have helped the FBI pull data from an iPhone recovered in December's San Bernardino, Calif., terrorist attack, but it shatters the notion that strong commercial encryption has left no opening for law enforcement and hackers, said Matthew D. Green, a computer science professor at Johns Hopkins University who led the research team.

The discovery comes as the U.S. government and Apple are locked in a widely watched legal battle in which the Justice Department is seeking to force the company to write software to help FBI agents peer into the encrypted contents of the iPhone used by Syed Rizwan Farouk, one of two attackers who were killed by police after the shooting rampage that claimed 14 lives.

Cryptographers such as Green say that asking a court to compel a tech company such as Apple to create software to undo a security feature makes no sense -- especially when there may already be bugs that can be exploited.

Naharnet Newsdesk
Internet Cut at Defense Ministry to Dismantle Illegal Network
Monday, 21 March 2016

Beirut - The internet connection at the Defense Ministry at Yarzeh was severed over the weekend in order to dismantle the illegal network that was recently uncovered in the country, reported the daily al-Mustaqbal on Sunday.
The development was a product of a parliamentary decision to remove illegal internet stations. The Defense Ministry has since been "returned to the fold of the state" and the legal internet network.

A decision was also taken to implement future projects aimed at developing the army's communication capabilities through a fiber-optic network that connects various military stations.

Media reports said there are four illegal "communication crossings" with a tremendous ability of 40GB per second WiFi network speed, which is equivalent to a third of the international capacities set by the Ministry of Telecommunications in service (150GB per second).

Anonymous parties described as a "mafia" are taking advantage of internet services by installing internet stations that are not subject to state control.

It has been reported that wireless internet towers and technical equipment were placed illegally in some mountainous terrains, including Tannourine, al-Dinnieh, Sannine and al- Zaarour.

Smuggled internet services could cause possible security breaches as they lack the basic control standards, exposing Lebanon to third parties, including Israel.

In addition, smuggling online services outside legal frameworks is a waste for the state's treasury amounting to over $2 million losses on a monthly basis.

The National (UAE)
Commentary: Technology is not always twinned with progress
Monday, 21 March 2016
Byline: Justin Thomas

If nations can be classed as underdeveloped, developing, and developed, can they also be considered overdeveloped? We have a fascination with technology and progress. Perhaps this is hard-wired into the human psyche? The most creative and destructive force in nature is the human mind. Our latest technological tools take the form of thinking machines, artificially intelligent devices that save us time and effort. We now have an app for almost everything. But at what cost?
Carl Jung, the Swiss psychologist, once suggested that: "Our progressiveness, though it may result in a great many delights, piles up an equally gigantic debt, which has to be paid off from time to time in the form of hideous catastrophes". Today's computers can rapidly manage large amounts of data. Most of the time they do this without a hitch. But when they do mess up, they mess up spectacularly.

Banking, for example, was an industry quick to embrace the digital revolution and here we can find examples of potentially catastrophic malfunction. In 2013, Reggie Theus, a restaurant manager from Texas, became an accidental trillionaire when a banking error left him looking at a balance of $4 trillion (Dh 14tn). In 2015, Deutsche Bank misdirected $6 billion to one of its customers. In the same year, an Indian woman became one of the richest women on earth when a banking error resulted in her account being credited with the rupee equivalent of around $1.5bn.

There are many other cases of banking mishaps, and invariably these errors are apologetically attributed to IT failures. The quoted examples are the cases that make the news. I wonder about the errors that go undetected or unreported?

It is not only in industry. Our technological advancements impact our social lives too. As the old joke goes: do you know who really loves smart phones? Divorce lawyers. A survey by the American Academy of Matrimonial Lawyers found that evidence pulled from our digital devices is increasingly featuring in divorce proceedings: from text messages to GPS data. Information technology undoubtedly helps us connect with one and other. However, the ease with which we can now connect has, some argue, made

it easier for people to be unfaithful, also ushering in new ways to cheat on each other. It would be tragically ironic if the devices that were meant to connect us, actually lead to an increase in disconnection in the form of divorce.

However, for every tragic tale that implicates technology, there are many more that point the finger at human frailty. After the German Wings disaster, when a co-pilot allegedly crashed a commercial passenger plane into a French mountainside, one of the debates that arose was: human pilot vs autopilot. Developments in artificial intelligence and sensor technology are now raising serious questions about the need for human pilots, lines of inquiry that may resurface following Saturday's FlyDubai plane crash in Russia.

Also, when there is an app that can do what you do - only faster and cheaper - how will you feel? Technology and unemployment is an old Luddite concern. However, it is becoming more relevant as the rate of our labour-saving technological progress increases in the context of a growing global population.

I'm not against technology at all, but we do need to look critically at what our technology actually helps us achieve. To paraphrase a British politician: if the cannibal now orders his meals online and eats them with titanium cutlery, rather than his hands, is that progress?

Technology is not always synonymous with progress, and progress is best when it's at the right pace and in the right direction.

For Carl Jung, and many other psychologists, the direction of progress now needs to turn inwards. We need to focus more effort on conquering cruelty, greed, despair and selfishness. We already have lots of apps for the external stuff.

Dr Justin Thomas is an associate professor of psychology at Zayed University and author of Psychological Well-Being in the Gulf States.

The Local.se
Swedish newspaper websites shut down in hacker attack
Sunday, 20 March 2016

Stockholm - The online editions of Sweden's main newspapers were knocked out for several hours by unidentified hackers at the weekend, police said on Sunday as they launched an investigation.
The attack was "extremely dangerous and serious," the head of the Swedish Media Publishers' Association, Jeanette Gustafsdotter, told Swedish news agency, TT.

"To threaten access to news coverage is a threat to democracy," she said.

No one has claimed responsibility for the attacks, which either partially or totally shut down the sites of Dagens Nyheter, Svenska Dagbladet, Expressen, Aftonbladet, Dagens Industri, Sydsvenskan and Helsingborgs Dagblad on Saturday evening from about 8:00 pm (1900 GMT) until about 11:00 pm (2200 GMT).

Several experts quoted in the media suggested the sites were subjected to distributed denial-of-services (DDoS) attacks, in which hackers hijack multiple computers to send a flood of data to the target, crippling its computer system.

Police said in a statement they had launched an investigation, and Swedish intelligence was also being kept abreast of developments.

An anonymous threat was issued on a Twitter account shortly before the attack. The account was attributed to J@_notJ.

Washington Post
America's cyber-insecurity
Sunday, 20 March 2016
Byline: Fred Kaplan

OpEd: When the widely respected national security mandarin Robert Gates was appointed secretary of defense in late 2006, his daily intelligence reports on the cascade of cyberattacks directed against the United States left him incredulous. As author and Slate columnist Fred Kaplan recounts, Gates was "so stunned by the volume of attempted intrusions into American military networks - his briefings listed dozens, sometimes hundreds every day - that he wrote a memo to the Pentagon's deputy general counsel. At what point, he asked, did a cyber attack constitute an act of war under international law?" When the defense secretary finally received a response - vague and evasive, in his estimation - almost two full years had passed.
The episode illustrates an enduring challenge for the United States in the digital age. While some bureaucratic actors within its government are not capable of operating at Internet speed, America's adversaries - hostile sovereign powers, transnational criminal enterprises, hacker and terrorist collectives - continue to attack with all the relentless intensity and innovation afforded by a constantly evolving arsenal of modern cyberweapons, penetration technologies and tactics.

"Dark Territory" captures the troubling but engrossing narrative of America's struggle to both exploit the opportunities and defend against the risks of a new era of global cyber- insecurity. Assiduously and industriously reported, Kaplan's history underscores a double irony in American cyber-strategy. The severity and scope of cyberthreats against the United States have been consistently predicted and demonstrated for decades and have never meaningfully abated. The most extreme threats, such as "decapitation" strikes against U.S. military networks and critical infrastructure, have been effectively countered for more than 20 years, however, while the most pervasive and common penetrations

against American business and corporate interests have been growing exponentially, with no plausible strategy in sight to engineer effective deterrence or a reliable defense.

America's vulnerabilities have been clear for decades. In 1997, a secret National Security Agency "Red Team" was instructed to test the defenses protecting the Pentagon's computer networks. The National Military Command Center was hacked in a day. The Defense Department's intelligence directorate was then penetrated with stunning simplicity: A member of the Red Team called, claiming to be from the Pentagon IT department, and explained that the directorate's password would need to be changed. "The person answering the phone gave him the existing password without hesitation," Kaplan discovered. "The Red Team broke in."

The following year, the computers at Andrews Air Force Base outside Washington were penetrated, a hack that swiftly spread to a dozen military locations. The breach, code-named Solar Sunrise, was initially traced by investigators to an Internet service provider in the United Arab Emirates, triggering speculation that the operation had originated from Iraq. Yet within days, a less dramatic explanation emerged. The culprits were a pair of 16-year-old boys in the San Francisco suburbs operating under the aliases Makaveli and Stimpy.

Kaplan recapitulates one hack after another, building a portrait of bewildering systemic insecurity in the cyber domain. Appointed director of national intelligence in 2007, Mike McConnell was by then a self-appointed proselytizer on the burgeoning cyberthreat. He lobbied the government's national security agencies - as well as the Treasury, Energy and Commerce departments - seeking to impart a greater sense of awareness and urgency. "He would bring the cabinet secretary a copy of a memo," Kaplan writes. " 'Here,' McConnell would say, handing it over. 'You wrote this memo last week. The Chinese hacked it from your computer. We hacked it back from their computer.' "

The cyberthreat posed by China is among the most acute, Kaplan observes, because it is driven by a diverse spectrum of incentives. China executed the most spectacular breach ever of U.S. government data, hacking the Office of Personnel Management (an event that followed the completion of Kaplan's manuscript). According to a Senate briefing provided by FBI Director James Comey, the personal information of up to 18 million Americans was stolen. In addition to conventional spying and penetration operations, Kaplan explains, China engages in highly organized commercial cyberespionage and intellectual property theft. In March 2013, national security adviser Tom Donilon confronted Beijing over its attacks against American corporations and the "sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale."

The principal Chinese antagonist of American business, according to Kaplan, was well known across the senior ranks of the Obama administration. It was the Second Bureau of the Third Department of the People's Liberation Army's General Staff, also known as Unit 61398, headquartered in a 12-story building outside Shanghai. It is but one cadre of a cyber-force estimated to be in the tens of thousands.

Kaplan alludes to the scope of the cybersecurity crisis for American businesses and corporations, citing a report by telecommunications giant Verizon that there were 79,790 verified security breaches in the United States in 2014, with approximately 25 percent more penetrations and 55 percent more data losses than the year before. As arresting as this statistic may be, it does not convey the ultimate economic costs at stake. According to some cybersecurity industry estimates, more than $750 billion in economic value is stolen through global cybercrime and commercial cyberespionage operations annually.

One of the deep insights of "Dark Territory" is the historical understanding by both theorists and practitioners that cybersecurity is a dynamic game of offense and defense, each function oscillating in perpetual competition. The United States, Kaplan demonstrates, has excelled in offense.

Tailored Access Operations, an elite unit within the NSA, developed an arsenal of technologies enabling penetration across the communications network. "Obscure points of entry were discovered in servers, routers, workstations, handsets, phone switches, even firewalls (which, ironically, were supposed to keep hackers out), as well as in the software that programmed, and the networks that connected, this equipment," Kaplan notes, ticking off now- ubiquitous hacking technologies. "LoudAuto activated a laptop's microphone and monitored the conversation of anyone in its vicinity. HowlerMonkey extracted and transmitted files via radio signals," even when a computer was not connected to the Internet. "MonkeyCalendar tracked a cell phone's physical location and conveyed the information through a text message. NightStand was a portable wireless system that loaded a computer with malware from several miles away."

During the Iraq War, NSA equipment and analysts were deployed on the ground in a heavily fortified concrete bunker north of Baghdad to assist with the "surge" in American operations to crush insurgent militias and terrorist groups. Captured laptops yielded e-mails, passwords, phone numbers, usernames and the identities of al-Qaeda leaders, all of which were used to launch entrapment and assassination operations that in 2007 alone resulted in the deaths of 4,000 Iraqi insurgents.

In 2009, Defense Secretary Gates created a dedicated Cyber Command. In the first three years the command's budget tripled from $2.7 billion to $7 billion, and cyberattack teams grew from 900 specialists to 4,000, with 14,000 anticipated by the end of the decade. The most ingenious and resourceful operation that has spilled into the public domain is code-named Olympic Games, a joint initiative by the NSA, the CIA and Israel's cyberwar bureau, Unit 8200, to inject the now-famous "Stuxnet" malware program into the industrial computer systems at Iran's nuclear facility in Natanz, disabling thousands of uranium centrifuges.

Today the United States - its defense complex, intelligence community, government agencies, and broad array of economic and corporate interests - is utterly engulfed in what appears to be a ceaseless cycle of offensive incursions and breached defenses. As the Defense Science Board stated in 2013 in a now grimly familiar conclusion, "The network connectivity that the United States has used to tremendous advantage, economically and militarily, over the past twenty years has made the country more

vulnerable than ever to cyber attacks." It is an unsettling thesis that "Dark Territory" indisputably substantiates.

Gordon M. Goldstein is a managing director at the global technology investment firm Silver Lake Partners and an adjunct senior fellow at the Council on Foreign Relations.

Vice News Canada
Chelsea Manning Revealed How the US 'Insider Threat' Program Tries to Catch Whistleblowers
Sunday, 20 March 2016
Byline: Tess Owen

Washington - Do you work with an egomaniac? Does your colleague seem disgruntled? Are they worried about money? Are they greedy? Or a pushover?
If so, they might be a whistleblower, according to the US government's handbook for its "Insider Threat" program. The program surveils the internal communications of the government's military and civilian contractors, combing them for evidence of particular personality traits and flagging would-be whistleblowers -- like US soldier Chelsea Manning and former NSA staffer Edward Snowden -- to prevent future intelligence leaks.

Manning, who is serving a 35-year sentence for leaking classified information to Wikileaks in 2010, obtained documents about the program after she submitted a Freedom of Information Act request from behind bars in Fort Leavenworth, Kansas. The documents show how officials used Manning to establish a prototype of a whistleblower. Her character and personality are dissected and presented as being symptomatic of the kind of person who would reveal state secrets.

The document, which was first published by the Guardian, lists broad categories at the beginning of the soldier's 31-page file. The main categories are listed as "greed or financial difficulties," "disgruntled or wants revenge," "ideology," "divided loyalties," "vulnerable to blackmail," "ego/self image," "ingratiation," and "family/personal issues."

Related: Chelsea Manning Is Suing the Government to Get Her FBI File

Manning contends that those purported "motives" are overly broad and subjective, and essentially give US officials the green light to spy on whoever they want. "The broad sweep of the program means officials have been given a blank check for surveillance," Manning said.

"This lack of focus has already led to the program becoming industrialized," Manning said, referring to a document from 2015 in which the US Department of Defense revealed the existence of "continuing evaluations" of 100,000 personnel on and off the job.

In the aftermath of the Wikileaks revelations in 2010, where Manning downloaded and distributed thousands of classified documents, the Obama administration formed the National Insider Threat Task Force. The task force was comprised of a number of government agencies, including the Office of the Director of National Intelligence and the Department of Justice. That initiative was applicable to anyone who worked for a federal agency.

Some civil rights groups have found the way Manning's gender dysphoria is cast in the document to be particularly egregious. US officials imply that Manning's gender identity had a significant part to play in her decision to leak the documents. The version of the document using Manning as a case study was drawn up in 2014, 10 days before she legally changed her gender from male to female. As a result, the document uses male pronouns to describe Manning.

"During PVT Manning's service in the US army, he struggled with his self-image as a man when he wanted to be an openly accepted female in the US army."

"The program alleges that I am 'disgruntled' based on my perceived sexual orientation and gender identity," Manning wrote in response to the documents. "It describes me as an 'advocate for homosexuals openly serving' in the military, and my concern and advocacy of queer and trans rights as being expressed 'obsessively.'"

Related: Edward Snowden Calls 'Bullshit' on FBI's Claim That It Can't Unlock iPhone

The ideology Manning espoused, according to the document, was that of a hacker who deemed "all information (government in particular) should be public knowledge."

That Manning had reportedly broken up with her boyfriend before being deployed to Iraq, that she worked the late shift, and that she researched gay rights "obsessively," were also red flags, according to the document.

There are no federal statutes that limit a private employer from surveilling their staff. However, the Federal Privacy Act does limit the amount of information a federal employer can collect on their employees. As a way of getting around those restrictions, the "Insider Threat" initiative basically provides all federal employers with a warrant.

The program also fosters a "if you see something, say something" mentality in the workplace - - effectively encouraging people to keep tabs on their co-workers. "In past espionage cases, we find people saw things that may have helped identify a spy, but never reported it," Gene Barlow, a spokesman for the Office of the National Counterintelligence Executive said in 2013. "That is why the awareness effort of the program is to teach people not only what types of activity to report, but how to report it and why it is so important to report it."

New York Times
Building a Better Anonymouse Trap
Sunday, 20 March 2016
Byline: Margaret M. Sullivan

The Times has a new way to handle information supplied by people who don't want to be identified by name -- also known as anonymous sources, or jocularly, because they are omnipresent and hard to control, as "anonymice."
After I wrote about the new guidelines last week in a blog post, many readers wrote me to share their reactions. I want to use this column to give voice to those reactions, which ranged from skepticism to gratitude, sometimes with a healthy dose of caution thrown in.

But first, some background. The new policy has been in the works ever since The Times published (and then had to recant major parts of) two articles within six months that were based on anonymous sources: One reported that the Justice Department had been asked to do a criminal investigation of Hillary Clinton's email practices; another described the supposedly out-in-the-open social media support for jihad by one of the San Bernardino killers.

After the articles were fixed, and hefty corrections or editors' notes attached, the executive editor, Dean Baquet, told me that he thought current practices needed strengthening. He assigned a team of senior newsroom managers, led by the standards editor, Philip Corbett, to work on it; and they in turn sought the opinion of some of The Times's most experienced reporters and editors.

The result is a sensible, wise and much-needed approach to a problem that readers have long complained about. It's one of the concerns I've heard the most about during my time as public editor.

Under the new guidelines, articles in which the main point hinges on an anonymous source or sources must get special scrutiny; they have to be flagged for review and approval by Mr. Baquet, or by one of two deputy executive editors, Matt Purdy and Susan Chira. Mr. Purdy, in an interview last week, described these kinds of stories to me as potential "journalistic I.E.D.s" because they may explode and do great harm to The Times's credibility.

Any other use of anonymous sources must be approved by a "desk head" -- for example, the top culture, metro or international editor -- or that person's deputy. And the guidelines reinforce a longstanding policy that an editor must know the identity of each anonymous source.

Finally, the guidelines state that the use of direct quotations from unnamed individuals should be rare. Mr. Purdy told me that too often, these quotes allow sources to express "their impression, their spin, their agenda" without accountability and without allowing readers to evaluate their motives. After all, readers don't know who's behind the quoted words.

Many readers were appreciative that The Times has taken their concerns seriously. "Outstanding!" wrote Steven Hillyard of Carmel, Calif., who said he had almost given up on this issue. He added: "Keep it up; it's important for us to get the real news, not just spin."

And Jim Poling, managing editor of The Hamilton Spectator, a daily newspaper in Ontario, Canada, praised The Times for what he called an important step and for emphasizing the importance of credibility. He distributed the guidelines to his own staff for consideration.

Still, perhaps the most common reaction was a kind of world-weary skepticism, along the lines of "I'll believe it when I see it."

Philip Kalikman of New York said that editors' assurances that the guidelines would indeed be followed, "rest on a lot of wishful thinking and good intentions." He proposed a reader-driven policing of the guidelines: "How about a requirement that whenever a reader writes to the public editor to question or object to the use of an anonymous source, and the public editor deems the objection valid, the news editors must respond to the specific incident with more information." I've passed the idea along to Mr. Corbett.

Another reaction -- less common but certainly worth thinking about -- was concern that the policy might hurt enterprise journalism. Some readers realize that sometimes anonymous sources are the only way important stories can come to light.

Steven M. Gorelick of Westfield, New Jersey wrote: "It seems I'm in the minority, but I hope The Times will do everything possible to make sure that the use of anonymous sources remains a vital, effective part of the reporter's tool kit."

Tightening the rules is fine, Mr. Gorelick said, but the paper should not go too far. "The last thing I want is a news product limited to stories provided and confirmed by named sources," he wrote. "I don't want genuinely intimidated whistle-blowers to ever be reluctant to get on the phone. I don't want powerful people who are uniquely situated to know painful truths to ever have to fear exposure if they contact a reporter."

Mr. Gorelick depends, he said, on Times journalists' "best judgment and careful scrutiny of who these sources are and the truth of what they are claiming."

His comments are astute. Whenever I've written on this subject, mostly to urge The Times to follow its own guidelines on using anonymous sources only as "a last resort," I've acknowledged that confidential sources are indispensable to a lot of great journalism.

These new guidelines certainly don't ban anonymous sources, nor should they. But they will probably make them less common and more carefully scrutinized; that was evident already in the pages of The

Times last week. The guidelines are a commendable development. It will be important to adhere to them conscientiously, not just in this initial phase but in the long run.

The opening words of Mr. Baquet's memo announcing the changes put it well: "The use of anonymous sources is sometimes crucial to our journalistic mission. But it also puts a strain on our most valuable and delicate asset: our trust with readers."

Sometimes it takes a crisis to create change. But no matter what prompted it, newsroom leadership has listened to readers' concerns and taken firm action. That's heartening -- and crucially important for the future of The Times.

A post in last week's Public Editor's Journal took up reader concerns about the post-publication editing of an article on Bernie Sanders' legislative accomplishments, which changed its tenor without notification or explanation to readers.

Follow the public editor on Twitter at twitter.com/sulliview and read her blog at publiceditor.blogs.nytimes.com. The public editor can also be reached by e- mail: public@nytimes.com.

New York Times
ZTE Document Raises Questions About Huawei and Sanctions
Saturday, 19 March 2016
Byline: Paul Mozur

Hong Kong - When the United States government punished ZTE of China this month, saying it had done business with Iran, it released internal company documents that it said detailed how the electronic equipment maker had done it -- and that also suggested the problem might not be limited to one Chinese company.
One document described how ZTE would set up seemingly independent companies -- called "cut-off companies" -- that would sign the deals in other countries. That could enable it to continue to do business in Iran, North Korea and other countries placed under American restrictions.

In describing the effort, the document cited as a model -- and at times a cautionary tale -- a rival company it called F7. ZTE said F7 had done something similar, though its business in restricted companies ended up hurting its American ambitions.

The document does not give F7's real name. But the description offered by ZTE matches a company far larger and more politically sensitive: Huawei Technologies, its chief rival and a major force in the technology world.

The ZTE document, dated August 2011, suggests that other Chinese companies could have potential exposure to American export limits. Given the recent sanctions against ZTE, it also suggests that the issue could be a continuing one between Chinese and American government officials.

ZTE on Thursday said that it had delayed the release of its annual financial results because of the sanctions, which limit the ability of American companies to sell equipment to it.

ZTE officials declined to comment on the identity of F7, and Huawei declined to comment. ZTE has said it is cooperating with investigators and is committed to complying with the law.

The United States Commerce Department, which last week restricted sales of American telecommunications equipment to ZTE, accusing it of violating embargoes, did not respond to requests for comment.

It is rare for the Commerce Department to publicly provide evidence for an addition to its blacklist of restricted companies, especially full disclosure of internal documents.

It is not clear how accurate ZTE's version of the events might be. The document says some information about F7 was gathered by ZTE's legal department, without offering details.

F7, the document says, tried in 2010 to buy an American company called 3Leaf but met with opposition from American officials. That same year, Huawei agreed to buy major assets from 3Leaf, but it dropped the bid in February 2011 because of opposition from American officials.

F7 also has a joint venture with the American digital security company Symantec, the 2011 document says. Huawei had a joint venture with Symantec before the American company dissolved it in 2012.

Like ZTE, Huawei makes telecommunications equipment for corporate networks and for big telecommunications systems such as phone companies. American officials have long suspected it has Chinese government ties, and United States intelligence officials have tried to tap into the company's network. Both companies are effectively barred from selling equipment for American networks.

Huawei says that it is privately owned and that accusations of government ties are an excuse to hurt the company for protectionist purposes.

Huawei is much larger than ZTE. In 2014, it reported revenue of about $60 billion, about four times that of ZTE. Depending on the measure, it ranks with Sweden's Ericsson as the world's largest supplier of the base stations and other equipment that make mobile telecom networks run. Huawei equipment supports networks in countries across the world, including many European markets.

While both Huawei and ZTE are given privileged status as high-tech innovators by China's leadership, Huawei is more prominent.

Huawei has also had greater success selling its smartphones in America, and indeed across the world. The company was the third-largest smartphone vendor by units sold in the fourth quarter of 2015 according to IDC, with an 8.1 percent share of the global market, compared with the 21.4 percent share of Samsung, the company in first place.

Despite the trouble in the United States, Huawei has not shied away from potentially controversial deals. In September, Huawei signed a deal with Syria's Communications and Technology Ministry to help the country develop its communications networks.

The ZTE document details how F7 recruited compliance experts and placed them in its joint ventures as part of efforts to mitigate its risks. It says that the company recruited one "senior export control compliance specialist from Texas Instruments" and a "Chinese- American attorney who is familiar with the related laws in the U.S."

It also describes how F7 found partners that it could say were independent companies and that could work on its behalf in countries under embargo. F7, it said, found a big information technology company that was "serving as its agent to sign contracts for projects in embargoed countries."

"This cut-off company's capital credit and capability are relatively strong compared to our company; it can cut off risks more effectively," the document said.

But ZTE came to believe that F7's activities in embargoed countries hurt its American expansion efforts.

It said it believed that F7's efforts to acquire companies in the United States were in part blocked because of its "ongoing projects in embargoed countries."

Pakistan Dawn
The threat of cyberterrorism
Monday, 21 March 2016
Byline: Uzair M. Younus

Islamabad - Over three billion users access the internet today, compared to a measly 400 million in 2000. As the internet creates new opportunities for countries across the world, it also creates a whole host of challenges in the cyber realm. The anonymity offered by the internet, and its disregard for national boundaries, a revolutionary trait, is now becoming a military challenge. To ensure long-term security of its military and civilian infrastructure, Pakistan must implement a forward-looking strategy to deal with these cyber threats.
When US director of National Intelligence, James Clapper, was asked about the threats faced by the United States, he placed cyber at the top. "Cyber threats," he said, "to US national and economic security are increasing in frequency, scale, sophistication and severity of impact; [and] the ranges of

cyber threat actors, methods of attack, targeted systems and victims are also expanding." The United States is not the only country facing this challenge; all leading economies of the world are wary of the real danger they face in cyberspace.

Starting with the Stuxnet attack on Iran in January 2009, the scale and damage caused by cyberattacks has grown tremendously. Russia, China, North Korea, Iran, the United States and Israel all have robust and indigenous cyber warfare capabilities. Under the Modi government, India has also started work on developing its own cyber capabilities. Pakistan has been lagging behind and has so far failed to develop and implement any robust policy framework directed at emerging cyber challenges.

Cyberterrorism poses an immediate and short-term threat to the country's national security. This could consist of cyberattacks and the use of the internet by terrorists to plan, recruit, and communicate with other terrorists inside and outside the country. While terrorists probably do not have the sophisticated skills to target critical infrastructure, they have used the dark corners of the internet to communicate, recruit, and plan terrorist attacks. As ongoing counterterrorism operations squeeze the physical space for militants in Pakistan, they will increasingly withdraw deep into the internet to plan and communicate with each other. Unable to carry out large terrorist attacks in public, they could also begin to learn new and more dangerous cyber warfare capabilities.

The government, military and private sector must develop a framework for securing the country's critical infrastructure from cyberattacks.

A more serious and long-term threat emanates from cyber warfare carried out by other nation states, in particular India. After the Mumbai terrorist attacks of November 2008, plans to carry out quick military strikes against Pakistan were developed. Future terrorist attacks, like Mumbai, could lead to a quick military response from India and punish Pakistan for its alleged involvement in terrorist strikes on Indian soil. In response, Pakistan began developing tactical nuclear weapons at a rapid pace. These weapons have lowered the nuclear threshold and act as a deterrent against such measures.

The introduction of offensive cyber capabilities, however, would upend this strategic balance. Armed with offensive cyber weapons, and confident that Pakistan does not have similar capabilities, India could wreck Pakistan's critical military infrastructure. It could then conduct quick offensive strikes against Pakistan, or be satisfied with the damaging effect of cyberattacks. The development of such weapons would undermine the balance of power in the region and allow India to conduct punitive strikes against Pakistan with relative ease.

A three- pronged approach is needed to deal with cyber threats emanating from state and non-state actors.

Firstly, the government must pass well-articulated legislation that provides a legal framework for law enforcement and intelligence agencies to operate under. The draft cybercrime bill developed by the government has raised a number of issues. This bill needs a lot more work and must be amended before

being passed as law. Furthermore, a transparent process, with input from the private sector, needs to be developed for accessing communications data when national security is at risk. Such regulatory measures should not trample on freedom of speech and the user's right to privacy, and should have oversight measures to ensure that the powers granted to the intelligence agencies are not abused.

Secondly, Pakistan must develop a centralised command that serves as the central organisation responsible for the development of military capabilities in the cyber realm. This cyber command should be tasked with modernising Pakistan's cyber defences, both in the military and civilian domain, and for developing and demonstrating offensive cyber capabilities. The goal of the cyber command must be to ensure that Pakistan achieves and maintains a strategic cyber deterrent. China's People's Liberation Army (PLA) is beginning to develop a similar cyber command, and Pakistan can leverage its deep defensive ties with China to collaborate with the PLA in this domain.

Finally, the government, military, and the private sector must come together to develop a framework for securing the country's critical infrastructure from cyberattacks. Financial markets, the electric grid, nuclear weapons, and other physical assets must be secured in a consistent manner. Scenario planning and war games must be conducted to harden critical assets, and exercises must be carried out to simulate cyberattacks and flush out measures that must be taken during such events.

Cyber threats will continue to grow exponentially in the coming years and the costs of not investing in a full spectrum of cyber capabilities will continue to escalate. While the Senate Committee on Defence and Defence Production, along with other experts have raised this issue, no significant headway has yet been made. Emerging cyber threats can no longer be ignored, and a continued failure to plan and execute today will cause long-term damage to the security of the country.

Indo-Asian News Service
English unsafe language to communicate crucial data
Monday, 21 March 2016

New Delhi - English language was the highest spam sending language in 2015, with 84.1 per cent of all spammers using it for cyberattacks, followed by Chinese (2.6 per cent) and German (1.7 per cent) in second and third spots, respectively, a report by Trend Micro Incorporated said.
Japan-based firm Trend Micro Incorporated released its annual security round-up report, which dissected the most significant security incidents from 2015.

It said that people need to constantly update their systems to protect against new attacks. "The first quarter of 2016 clearly showed we need to also watch out for older threats, and how no industry or system should feel exempt. After all, who would have thought that language is also something to worry about from cyber threats perspective?" the report said.

The research confirms cyber criminals are now bolder, smarter and more daring than ever before.

The Trend Micro Smart Protection Network blocked more than 52 billion threats in 2015 -- a 25 per cent decrease from 2014.

This decrease is consistent with the downward trend of system infections since 2012, caused by attackers who have become more selective of their targets as well as the shift in technologies they use.

Le Progrès (Lyon)
Robin du web, un Anonymous résisterait dans le Mâconnais
Monday, 21 March 2016
Byline: Jérôme Morin

Mâcon, France - Il a 36 ans, vit dans la région mâconnaise et ferait partie du mouvement des Anonymous. Un homme, qui travaille dans le domaine paramédical, lève le voile sur ce groupe né sur internet. Pas besoin d'être hacker, assure-t-il, pour devenir un Anonymous.
Nous ne commettons ni vol de données, ni destruction. » Un homme de 36 ans, né à Mâcon et qui vit aujourd'hui dans les environs, ferait partie du mouvement des Anonymous, né sur internet, et qui fonctionne sans leader. « Je ne suis qu'un membre, pas le représentant », prévient l'activiste, qui s'est engagé il y a deux ans dans ce réseau « totalement apolitique. On voit souvent les Anonymous comme un groupe de hackers. En fait, seulement 10 % sont capables de pirater n'importe quoi. Chacun peut être Anonymous. »

Pour preuve, l'homme, performant, dit-il, en informatique, participerait également chaque mois à des maraudes à Lyon auprès de sans-abri avec d'autres Anonymous. Il aurait aussi placardé des affiches du type "Je ne veux pas que tu penses comme moi. Je veux simplement que tu penses", dans les rues du Mâconnais.

« Nous sommes pacifiques et nous le resterons. Certains mouvements d'extrême droite notamment utilisent malheureusement notre symbole » : le fameux masque blanc à moustache.

Un hacking en cours de la banque centrale des banques centrales ?

Un masque qui, selon le trentenaire, est « le symbole de ceux qui ont choisi de se battre pour la justice et la liberté. Nous protégeons l'anonymat car il ne fait pas bon de nos jours de dire la vérité. » Comme lui, des habitants de Chalon, Montceau ou encore Lyon auraient rejoint le mouvement international.Avec « ses frères et soeurs » Anonymous, il assure dénoncer.

Régulièrement les propos pédophiles tenus sur Facebook et Twitter - et « ils sont nombreux ».Après les attentats du 13 novembre, les Anonymous ont notamment bloqué des sites internet de Daesh. Actuellement, ils se concentreraient, selon le jeune homme, sur une grosse opération de hacking de la banque centrale des banques centrales, la Bank for International Settlements, basée en Suisse.

National Post
A Right to Privacy?
Wednesday, 30 March 2016
Byline: Marni Soupcoff
Section: oped

If there's one thing we know about politics, it's that you should never expect the players to be consistent. Before last fall's federal election, several prominent Liberal MPs expressed strong misgivings about Canada's agreement to turn over the personal financial information of "U.S. persons" residing in Canada to the U.S. government. It was a deal reached to comply with the U.S.'s new Foreign Account Tax Compliance Act (FATCA). At the Americans' behest, Canada began sharing tax information about Canadians, some of whom have never lived in the United States, never worked in the United States and never owed the Internal Revenue Service (IRS) a single penny.
No one was clearer about his qualms about this agreement than now- Prime Minister Justin Trudeau, who wrote in a pre-election letter, "The Government of Canada has a responsibility to stand up for its citizens when foreign governments are encroaching on their rights. We believe that the deal reached between Canada and the U.S. is insufficient to protect affected Canadians."

In 2014, MP Marc Garneau, now the transport minister, also voiced his disapproval of the agreement by pointing out that the IRS was trying to get the Canada Revenue Agency (CRA) to "do its dirty work." Yet now he says he supports the deal.

The current revenue minister, Diane Lebouthillier, has repeatedly defended the agreement and sought to reassure Canadians that it does not violate their rights. According to iPolitics reporter Elizabeth

Thompson, a request from that news outlet for an interview with Lebouthillier elicited an email reply from her office that said: "The CRA ensures that tax cooperation with its foreign partners is done in a manner fully consistent with privacy rights in Canada. It is important to note that Canada and the United States have a long history of exchanging tax information in a fair and responsible manner, going back to 1942."

It is, of course, every policymaker's prerogative to change his mind, and there's no doubt that the U.S. has made the penalties for not acceding to its demands with regard to FACTA exceptionally harsh. It is, however, still disappointing that we appear to be no further ahead in addressing the constitutional problems with the FATCA-related agreement than we were when the previous government passed it two years ago.

Indeed, the unfair ramifications of the deal remain: for Canadians, merely having dual U.S. citizenship - for example, because one's parents were Americans or one was born on U.S. soil to Canadian parents - is enough to trigger the mandatory sharing of private financial details. This is why two Ontario women launched a lawsuit against the Canadian government in August 2014 for agreeing to the information sharing.

That suit is still before the courts, but the feelings of one of the plaintiffs, Gwen Deegan, expressed around the time the constitutional challenge was launched, remain as relevant as ever: "This is an infringement on Canadians of U.S. origin by our Canadian government. It's literally a betrayal and I feel we can't just sit idly by and let it happen."

Deegan is a graphic designer from Toronto who was born in the United States, but has not lived there since she was five years old; she has never held a U.S. passport, nor has she ever worked in the United States. This tenuous connection with the United States still qualifies her as a "U.S. person" whose financial details the CRA will now be turning over to the IRS, if it hasn't already. Her fellow plaintiff, Ginny Hillis, a retired lawyer from Windsor, Ont., has also not lived in the United States since she was five years old; that's when she moved to Canada with her Canadian parents. Like Deegan, Hillis has never held a U.S. passport.

As I noted in a column in 2014, the interesting thing about Deegan and Hillis's circumstances is that both women happen to be married to Canadians with whom they hold several joint financial accounts. Why should these women's husbands - who are not "U.S. persons," even under the most expansive definition of that term - also be subject to having the details of their financial savings turned over to a foreign government? Do Canada's constitutional guarantees of liberty, security of the person and freedom from unreasonable search and seizure not apply as forcefully to these men, as well?

At the heart of this debate is the question of whether the agreement with the U.S. is in violation of the Canadian Constitution, as Deegan, Hillis and others have argued convincingly during this case.

If it is, all the American bullying in the world is not enough reason to sacrifice Canadians' rights.

Marni Soupcoff is executive director of the Canadian Constitution Foundation (theccf.ca).

National Post
Cracking the Apple case
Wednesday, 30 March 2016
Section: editorial

The stare-down between Apple Inc. and the U.S. government over the sanctity of the company's encryption techniques has ended with the Federal Bureau of Investigation hacking into an iPhone 5C on its own. But the underlying issue remains. Despite valid public concern about protection of personal privacy, the FBI was right to do so.
The key question was whether Apple was obliged to help the government break into a device suspected of containing information relevant to the investigation into the terrorist attack in San Bernardino, Calif., last year. The company declined to assist, professing a duty to protect the privacy of its customers.

It's natural to sympathize.

People don't want strangers - whether criminals, governments or the merely prurient - rummaging around in their online financial transactions, medical communications or love letters. And the Obama administration has shown a cavalier disregard for certain civil liberties, especially the Fourth Amendment guarantee against "unreasonable searches and seizures." Some of the more notorious examples that have come to light include the Department of Justice secretly obtaining journalists' phone records, the FBI and National Security Agency tapping into Internet servers and misleading Congress about their activities, and the Central Intelligence Agency hacking into Senate Intelligence Committee computers while the committee was investigating its detention and interrogation policies.

No wonder people are worried. And no wonder companies like Apple feel compelled to respond to their concerns. But the technological aspect of the San Bernardino iPhone case should not obscure the underlying issues, which are legal rather than technical.

The reason governments, in Canada as well as the U.S., can't kick down your door and strip-search you in your bedroom isn't because it doesn't know how. It's because it would need a warrant to do so. The same is true should it wish to seize your phone and rifle through your text messages.

Suppose police were aware that crucial evidence had been hidden in a safe. They can't just blow it open at will. But they can apply for a warrant and make their case to a judge. If the police then asked the manufacturer for details enabling them to open it without damaging the contents, would the company be defending liberty to refuse? Or obstructing justice?

The manufacturer would be correct to point out that aiding the police might increase their technical ability to open any such safe with or without a warrant. Yet having that knowledge would not necessarily lead to a rash of lawless break-ins. Because what stops the police from safe-cracking at random isn't lack of tools or technical knowledge. It's the absence of a warrant.

The same applies to data stored in private phones. Users have every right to protect their privacy, including through encryption, just as they have every right to lock their doors. And the state has no right to ask companies to weaken their encryption, as the U.S. government was accused of doing in asking Apple to create a modified operating system to bypass the iPhone's password security. But that does not imply absolute protection for information related to unlawful activities, or give the company the right to refuse cooperation in lawfully obtaining access.

The FBI found a way into this iPhone anyway, and hence others like it. In doing so, it may dent confidence in Apple's boasts about the quality of its encryption. Indeed, one possible side benefit of this case may to help cure people's outsized faith in the ability of technology to guard privacy, especially those curiously convinced that Apple products have flawless encryption and are immune to viruses.

The key to protection against the state breaking into your phone is the same one protecting the sanctity of your home. Without a warrant, such activity is itself criminal.

It's important that judges remain skeptical when warrants are sought for digital devices. But if appropriate conditions are met, there is no more right to refuse to unlock your phone to the police than to refuse to unlock your door. And phone companies have no more right than safe manufacturers to refuse to explain how the thing works.

Eternal vigilance is the price of freedom. Not strong encryption.

BNN.ca
BlackBerry could stand to benefit after U.S. authorities hack iPhone
Wednesday, 30 March 2016
Byline: Jeff Lagerquist

BlackBerry Inc. could benefit from the U.S. Federal Bureau of Investigation's successful unlocking of the San Bernadino gunman's iPhone as major smartphone makers look to shore up security on their devices. But technology analyst Carmi Levy says it will mean Blackberry drawing a "line in the sand" on government access, like rival Apple Inc.
"If BlackBerry wants to maintain its brand going forward . . . it's all about security. It needs to be perceived the same way," said Levy in an interview with BNN.

Privacy software has been a key focus for BlackBerry for several years as the Waterloo, Ontario-based company shifts its focus away from building phones.

"Security is what we do. Privacy is what you get. We have the most trusted networks outside of the carriers themselves. It is what we offer, and how we think about our business," said CEO John Chen in a Feb. 11 blog post.

Both BlackBerry and Apple have denied government requests for so- called backdoor software that would allow investigators to access a phone's data without company assistance. But Chen has said that BlackBerry's privacy commitment "does not extend to criminals."

The successful hack of the iPhone 5C used by Syed Farook avoids a courtroom battle between the U.S. Justice Department and Apple Inc. that could have set a precedent on privacy issues between governments and technology companies.

Apple is now faced with selling a product that has a proven security vulnerability. The FBI and U.S. Justice Department have no obligation to reveal how the phone's security features were hacked. Speculation online points to third party assistance from the private sector - including Israeli data extraction specialists Cellebrite Mobile Synchronization Ltd.

"Apple has got a problem now. Apple is no longer the one controlling the agenda of who gets into its phones. Some third party is," said Levy. "Next time the FBI, CSIS, or any other law enforcement agency [is] not even going to bother with a warrant for Apple. They are going to go to that third party and ask for their help."

Meanwhile, BlackBerry has showcased its ability to combine its core security competencies with Google's Android platform with the release of its PRIV smartphone last year.

"This could turn out to be a potential win for BlackBerry if they are able to secure contracts with those operating software makers, that would be Google or Apple," said BNN's Amber Kanwar.

The potential boon for BlackBerry's software business comes at a time when some analysts are predicting the company will cease its hardware offerings. Daniel Chan of TD Securities said in a recent note to clients the absence of a cheap BlackBerry handset at the Mobile World Congress in Barcelona a few weeks ago was a telltale sign that the company would focus solely on software.

BlackBerry has been on a buying spree to boost its security capabilities over the last 18 months, acquiring AtHoc, Secusmart, WatchDox, and Good Technology. The company hopes to extend its security services beyond smartphones into Internet of Things-based machine-to-machine communication.

BlackBerry reports its fiscal fourth-quarter earnings on Friday.

China Daily
Manufacturing of 'spy' story to stain China's reputation
Wednesday, 30 March 2016

Chinese businessman Su Bin, according to some media reports, pleaded guilty to "cyber espionage" charges almost at the same time that China's Foreign Ministry announced President Xi Jinping's participation in the fourth Nuclear Security Summit in Washington on Thursday and Friday.
No wonder some media outlets and US officials are trying to cast a shadow over Beijing-Washington ties before Xi's meeting with US President Barack Obama on the sidelines of the nuclear summit. With vivid descriptions and seemingly "credible evidence", the reports have painted the picture of a plot in Su's case which resembles those in James Bond movies and some Hollywood blockbusters to catch eyeballs.

According to US Assistant Attorney General for National Security John Carlin, the admission of guilt by Su sends a strong signal that a heavy price has to be paid for stealing intelligence from the US and its enterprises, and Washington will - and has the capability to - capture those who do so and hold them accountable. An official from the Federal Bureau of Investigation's cyber section said the US should be on high alert against cyber threats because its adversaries are continuously raising their capabilities.

The reports also said that following Su's confession, the US is doubling its efforts to prevent "cyber espionage" by China.

That Washington chose to announce the "details" of Su's case on the very day that Beijing released the agenda for Xi's visit to the US suggests it is aimed at pressuring China into conceding some serious demands on cybersecurity. The making of "China's cyber espionage" story and its dissemination across the media and the international community are apparently aimed at spoiling China's reputation.

By doing so, the US can use the excuse of "judicial independence" to shirk its responsibility in such a case whenever China raises questions over Washington's cyberespionage activities.

The timing of the announcement is also a breach of basic international practice and diplomatic protocol, and exposes the US' hegemony mentality.

Despite appearing to be an accidental incident, the Su case shows the effects of the US' meticulous planning if seen in the context of the recent developments in Sino-US ties. Over the past year, the US' policy toward China has witnessed certain changes, making it increasingly likely that Washington would find faults with Beijing. This is not only related to the increasing anti-China rhetoric in the year of the US presidential election, but also to the growing "sense of anxiety" in the US' strategy toward China.

The intensifying strategic competition between the two sides because of China's steady rise has prompted some in the US to seek a strong response to China. It has also made them push for a "China-containment" policy by raising topics such as "cyber espionage" and "freedom of navigation" in the South China Sea to disturb the peaceful environment China needs for its development.

Considering that the expected meeting between Xi and Obama in Washington is likely to further advance Sino-US relations, Washington should reduce the media hype over the Su case and prevent it from disturbing the smooth development of bilateral ties, damaging mutual interests and endangering the US' strategic interests.

China and the US both should adhere to the agreements they reached at a high-level dialogue in December on fighting cyber crimes, for they are meant to guide them to seek common grounds, expand cooperation and avoid confrontation in the field of cybersecurity. More importantly, the US should discard its Cold War mentality and work with China to keep Sino-US ties on track in order to develop a new pattern of bilateral relations, which both have vowed to build.

The author is director of the center for crisis management studies, China Institutes of Contemporary International Relations.

Philippine Star

Comelec seeks NBI help vs hackers
Wednesday, 30 March 2016

The Commission on Elections yesterday asked the National Bureau of Investigation (NBI) to look into the hacking of the Comelec's website last Sunday.
Comelec spokesman James Jimenez said they have referred the case to the NBI's cybercrime division as a group identifying itself as "LulzSec" has claimed uploading parts of the Comelec's database to its Facebook account.

"That matter has actually been referred to the NBI cybercrimes. So right now, the first step really is to validate whether or not the data they posted are authentic... At this point, I really don't know if it's the real deal and that's the first thing that we want to find out," Jimenez said.

The NBI, however, said it has yet to receive the request from the Comelec.

"None yet," said Victor Lorenzo, executive officer of the NBI's cybercrime division.

However, Lorenzo stressed the communication between the NBI and the Comelec should be established and secured before the hacking incident is investigated.

"We have to check if the logs on the website have been restored. Comelec may have kept some of them while restoring the website for security," Lorenzo said.

In its Facebook account, LulzSec posted "A great lol (laugh out loud) to the Commission on Elections, here's your whoooole database."

LulzSec, reportedly affiliated with hacker group Anonymous Philippines, hacked the Comelec's website, leaked the voter database and demanded that the poll body make the May 9 elections credible.

The website is still accessible but the precinct finder search engine, which publishes assigned precincts of registered voters based on their names and birthdays, is still "under maintenance."

Jimenez said the Comelec has not restored the website as it is undertaking a cleanup.

"But it's not been hacked again," Jimenez said. "I think that's the most important thing. We're just undergoing maintenance right now. It's not yet 100 percent back to normal but we're working on it."

Jimenez said the election website would be highly secured in time for the upcoming polls.

Khaleej Times
DarkMatter to boost regional cyber security solutions

Wednesday, 30 March 2016
Byline: Sandhya D'Mello

Dubai - UAE-headquartered DarkMatter -- exclusive cyber security partner to the UAE government -- an international cyber security firm, is planning to boost its cyber security solutions in UAE and in the region, said Dr Najwa Aaraj, vice-president of special projects at DarkMatter on the sidelines of the Future Technology Week which opened on Tuesday and will conclude on March 31, 2016 at Dubai World Trade Centre, or DWTC.
Dr Aaraj gave a presentation based on the theme, 'Security solutions for the mobile embedded world'. The company helps transforming the cyber security landscape by providing a complete range of state-of-the-art services and solutions to government and commercial clients.

"We have observed that UAE market is one of the biggest adapters of the smartphone embedded devices, IoT devices and embedded systems with people wanting to adopt latest technology and latest operating systems and apps are installed there. However, there is no real control and poor device management over what applications are being downloaded. Societies need to understand the mobile and cyber threats are on rise with almost five billion attacks in 2015 alone were recorded on general infrastructure in addition to half a million new threats coming every year."

The first edition of Future Technology Week opened at DWTC on Tuesday, with thousands of technology industry professionals flocking to the opening salvo of the two-day Internet of Things Expo (IoTX) and the one-day Gulf Enterprise Mobility Exhibition & Conference, or Gemec.

The Gemec discussions focussed on how heightened enterprise mobility will transform companies' customer engagement strategies and how forensics, access controls and authentication can limit mobile security threats in a mobile embedded world. Ashi Sheth, manager Enterprise Platforms of Netflix, delivered the keynote address.

A new umbrella identity collecting Gulf Information Security Expo & Conference (GISEC), IoTX, The Big Data Show and GEMEC, the exhibition element of Future Technology Week collects more than 180 exhibitors displaying innovative solutions and products on the show floor.

Jerusalem Post
Knesset approves extension of biometric database pilot
Wednesday, 30 March 2016
Byline: Yonah Jeremy Bob

Jerusalem - The Knesset on Tuesday voted 41-32 in favor of a nine- month extension of the current biometric database pilot program despite signs that support for the initiative, even within the coalition, has eroded somewhat.

The vote ratified a request by Interior Minister Arye Deri on Sunday for an extension until December 31, 2016 to better learn the issues since he is relatively new in the job.

The reduced support is a result of a representative of the program admitting last week that the database is not leak-proof, an issue coalition chairman Tzachi Hanegbi (Likud) noted bothered him as well and could lead him to eventually vote down the program.

Last week, the Movement for Digital Rights slammed the admission by Naama Ben Zvi Riblis, a lawyer for the Biometric Database Authority, as proof that validated its attack on the entire new biometric database idea as exposing citizens to a new level of invasion of their privacy rights.

The NGO's lawyer, Yehonatan Kleigar, stated, "At this meeting they put the truth on the table for the first time" as the authority "said on the record that the working assumption was that the entire biometric database would be hacked... and now we are not the only ones who are saying this... so why do we need this? Why take the risk?" Asked about the admission of how easily the database could be hacked, Knesset Constitution, Law and Justice Committee chairman Nissan Slomiansky's spokesman said he did not remember the authority saying that, but, surprisingly, if they did say that, the chairman still "had no position" on whether this should impact moving forward.

Committee spokesman Shimon Malka said the authority making the admission of "no one will sign an insurance form that the database will never be hacked" was correct, while suggesting that the NGO had taken the statement a little bit further than what was said.

The initial pilot program started in June 2013 and expired in June 2015, but former interior minister Silvan Shalom had already extended the program nine months, with that extension due to expire soon.

Slomiansky summarized the views at the hearing as mostly agreeing that the biometric cards were positive developments, but with a debate about whether to continue the database.

Ben Zvi Riblis, in contrast, said the database should be continued, but that possibly it would only contain facial recognition data and not fingerprint data.

The phenomenon of forging false identity cards led the Knesset to authorize the pilot for new identity cards in 2009 and to authorize managing the database in August 2011.

Arab News
KACST chief calls for upgrade in cyber security technology
Wednesday, 30 March 2016
Byline: Mohammed Rasooldeen

Riyadh - There is a strong need to develop scientific research in the field of information security through transfer and localization of technology in the Kingdom, said Prince Turki bin Saud bin Mohammed, president of the King Abdulaziz City for Science and Technology (KACST), here on Tuesday.
He was speaking during the inauguration of the third Saudi international conference on information technology entitled "Cyber Security" at the KACST headquarters.

Organized by KACST under the patronage of Custodian of the Two Holy Mosques King Salman, the event was attended by Communications and IT Minister Mohammed Al-Suwaiyel.

The theme of the two-day conference was "Information security and protection to ensure a secure electronic culture."

Prince Turki said the annual losses accruing from cybertattacks are estimated at $445 billion globally, and the volume of damage of such attacks is expected to rise in the future as a result of the expansion of electronic services and the entry of new technology concepts. "We have to build our own national capabilities through innovation to protect data."

Moreover, he said, the KACST has been working in cooperation with the relevant authorities on the transfer and localization of latest technologies in the Kingdom through the establishment of a sophisticated infrastructure and national capability building in many scientific fields. "They include the transfer of information technology in general and cyber security technology in particular, in accordance with the vision of the leadership to pave the way for scientific research and technical development in various fields for sustainability."

International experts are discussing cutting-edge technology on cyber security at the event. Also, the conference is addressing a number of key themes, notably: "The next ten years of the Internet: Threats and opportunities;" "Bridging the cyber security skills gap: UK experience;" "Malware Download Path Forensics and Mitigation" and "Toward Deployment of a Next-generation Secure Internet Architecture."

The conference has targeted staff and students from higher education institutions, and encourages attendance of managers and officials of public and private sectors within and outside the Kingdom who are interested in electronic security management, the authors of the regulations and policies for information security and its innovation within and outside the Kingdom besides local and international experts and researchers in the field of information security technology.

The event will feature 11 lecturers who are specialized in the field of information security, such as Professor Taher Elgamal, Professor Radha Poovendran, Professor Mustaque Ahamad and Professor Bart Preneel.

The winners of the cyber security competition entitled "Capture the Flag Competition" were also honored on the occasion, with Dia Mohammed Diab, from the Dia to Diab Team, winning the first prize carrying a cash award of SR25,000.

Le Monde
Le FBI abandonne ses poursuites contre Apple
Wednesday, 30 March 2016
Byline: Zeliha Chaffin

San Bernardino, Californie - L'agence annonce avoir déverrouillé l'iPhone de l'un des terroristes de San Bernardino
C'est un coup dur pour la firme à la pomme. Le FBI a annoncé, lundi 28 mars, avoir réussi à débloquer l'iPhone d'un des auteurs de l'attentat de San Bernardino (Californie), sans avoir eu recours à l'aide d'Apple. Dans un document transmis à la justice par les autorités américaines, le FBI précise avoir " accédé avec succès aux données stockées sur l'iPhone de - Syed - Farook et n'a donc plus besoin de l'assistance d'Apple ". Cet épilogue met fin au feuilleton qui oppose la firme à la pomme au gouvernement américain depuis le 16 février.

Conséquence de ce rebondissement : l'injonction judiciaire à l'encontre d'Apple est annulée. " Notre décision de mettre fin à la procédure est basée seulement sur le fait qu'avec l'assistance récente d'un tiers nous sommes maintenant capables de débloquer cet iPhone sans compromettre les informations dans le téléphone ", a précisé la procureure fédérale du centre de la Californie, Eileen Decker, dans un communiqué.

Depuis mi-février, la marque à la pomme était au coeur d'une violente polémique, car elle refusait de se plier aux injonctions du FBI. L'agence fédérale américaine l'exhortait à lui fournir un logiciel permettant de contourner les protections dont sont dotés les iPhone pour déverrouiller un téléphone chiffré ayant appartenu à l'un des terroristes présumés de l'attentat de San Bernardino, qui avait fait 14 morts le 2 décembre 2015.

La firme de Cupertino se refusait à satisfaire cette demande, arguant que celle-ci allait " au-delà de l'affaire concernée " et risquait de créer un précédent dangereux pour garantir la sécurité des données privées de ses clients. Le PDG d'Apple, Tim Cook, s'était même autorisé à commenter ce duel judiciaire, lundi 21 mars, lors de la keynote de présentation du nouvel iPhone SE. " L'iPhone est un objet extrêmement personnel. C'est une extension de nous-mêmes. Nous avons une responsabilité envers nos utilisateurs et envers notre pays. Nous ne la fuirons pas ", avait-il précisé. Apple avait notamment reçu le soutien d'autres géants du secteur, à l'instar de Google ou Facebook.

Un débat ouvert en FranceLe FBI se sera finalement passé de son aide. " Dès le début, nous nous sommes opposés à la demande du FBI (...) parce que nous pensions que c'était mal et que cela aurait constitué un dangereux précédent. Ce procès n'aurait jamais dû être intenté ", a déclaré Apple dans un

communiqué lundi soir. Si le déblocage de l'iPhone, qui met en avant une faille, pourrait lui nuire, Apple garde la satisfaction d'être resté ferme sur ses positions.

Le mystère qui entoure le déblocage du smartphone par le FBI reste, lui, entier. Le 21 mars, l'agence fédérale américaine avait indiqué qu'une " tierce partie " avait fait aux enquêteurs la démonstration d'une " autre méthode pour déverrouiller l'iPhone ". Le nom d'une entreprise israélienne, Cellebrite, spécialisée dans l'extraction de données sur mobiles, comme possible partenaire du FBI pour hacker l'iPhone, avait été évoqué par la presse, sans qu'il y ait confirmation.

En France, le débat sur la protection des données privées est également ouvert. Dans le cadre du projet de loi contre le crime organisé et le terrorisme, l'Assemblée nationale a adopté en mars un amendement du député Philippe Goujon (LR) contraignant les fabricants de téléphone à déchiffrer leurs appareils sur demande de la justice et punissant de cinq ans de prison et 350 000 euros d'amende ceux qui s'y refuseraient. Le Sénat devrait l'examiner cette semaine.

Los Angeles Times
Apple seeks FBI hacking method
Wednesday, 30 March 2016
Byline: Paresh Dave

Los Angeles - Apple Inc. refused to give the FBI software the agency desperately wanted. Now Apple is the one that needs the FBI's assistance.
The FBI announced Monday that it managed to unlock an iPhone 5c belonging to one of the San Bernardino shooters without the help of Apple. And the agency has shown no interest in telling Apple how it skirted the phone's security features, leaving the tech giant guessing about a vulnerability that could compromise millions of devices.

"One way or another, Apple needs to figure out the details," said Justin Olsson, product counsel at security software maker AVG Technologies. "The responsible thing for the government to do is privately disclose the vulnerability to Apple so they can continue hardening security on their devices."

But that's not how it's playing out so far. The situation illuminates a process that usually takes place in secret: Governments regularly develop or purchase hacking techniques for law enforcement and counterterrorism efforts, and put them to use without telling affected companies.

What's different in this case is that the world has been watching from the start. After Syed Rizwan Farook and his wife killed 14 people in December, the government publicly sought a court order to compel Apple to unlock Farook's work phone. Apple opposed that order, heightening long-standing tensions between Silicon Valley and law enforcement.

Now that the FBI has dropped its case against Apple, there's a new ethical dilemma: Should tech companies be made aware of flaws in their products, or should law enforcement be able to deploy those bugs as crime-fighting tools?

It's unclear whether the FBI's hacking technique will work on other versions of the iPhone, though a law enforcement official who spoke on the condition of anonymity said its applications were limited.

Some news outlets citing anonymous sources have identified Israeli police technology maker Cellebrite as the undisclosed third party helping the government, but neither the company nor the FBI has confirmed those reports.

A source who is unauthorized to discuss the case told The Times that the FBI was provided with the ability to incorrectly guess more than 10 passwords without permanently rendering the phone's data inaccessible. That allowed the agency to use software to run through potential pass codes until it landed on the correct one. It is not clear what info, if any, was gleaned from the phone.

Attorneys for Apple are researching legal tactics to compel the government to turn over the specifics, but the company had no update on its progress Tuesday.

The FBI could argue that the most crucial information is part of a nondisclosure agreement, solely in the hands of the outside party that assisted the agency, or cannot be released until the investigation is complete.

Many experts agree that the government faces no obvious legal obligation to provide information to Apple. But authorities, like professional security researchers, have recognized that a world in which computers are crucial in commerce and communications shouldn't be riddled with security flaws.

Even the White House's cybersecurity coordinator has acknowledged there are times when more people could be harmed by an unfixed security issue than helped by the government covertly using the loophole as part of an investigation.

A secretive White House-led procedure governs whether companies get notified of potential flaws.

Officials involved in the multi-agency deliberations -- called the Vulnerabilities Equities Process -- consider the risks and rewards of keeping flaws secret, according to federal records. They weigh whether the government could get the information in some other way and how likely it is someone else will discover the same vulnerability.

Federal officials have maintained that they lean toward private disclosure of a newly discovered vulnerability in most cases. But in some cases, federal agents have apparently benefited from previously unknown technical slip-ups by software developers.

The National Security Agency, though it denies the claim, reportedly took advantage of a flaw in the way websites transmit sensitive data for two years before private researchers uncovered the issue in 2014. Attorneys in two other cases have accused the FBI of using bugs in the Tor Internet browser to identify suspected criminals.

Apple's anxiety is understandable. No tech company wants a major security gap in its products - - and most are given months of warning to fix issues before they are made public by the researchers who discover them.

That's why Apple sees the government holding a moral obligation to disclose details of its hacking technique.

"Apple's best chance is to make a compelling case that the disclosure of this exploit is in the interest of national security, as in, if it remains undisclosed and undiscovered, it potentially puts innocent users at risk of data breach," AVG's Olsson said.

Apple stated in court filings that part of the reason its executives feared developing software to circumvent iPhone security features was that once created, it could end up in the wrong hands. That same argument could come into play with the disclosure issue if Apple makes a public plea that the government and the outside group can't properly safeguard the technique. Last year, an Italian company that bought and sold bugs saw its entire database leaked onto the Internet. The security issue could explain why the FBI and the outside party are being so secretive about the process.

There's also the concern that now that an iPhone can be hacked, others will try. The iPhone has been seen as "a tiny little Fort Knox that from the outside has shown very hard to get into," said Kevin Bocek, vice president of security strategy and threat intelligence at Venafi.

The San Bernardino situation changes the dynamics, providing a reason for "cybercriminals and amateur hackers to come out of the woodwork," said Peter Tran, a general manager at RSA's advanced cyber defense group.

Although someone helped the FBI crack the iPhone, probably in exchange for money, other people who stumble upon the same hacking technique could choose to sell to cyberthieves or other governments. An extensive underground online network, concentrated in Eastern Europe, does just that every day, Bocek said.

Apple generally doesn't reward bug-finders with cash. But given the publicity in this instance, experts said Apple could turn to the black market too.

"It proves once again that what you don't know, you can buy," said Nikias Bassen, principal mobile security researcher at Zimperium.

Wall Street Journal
Broader Fight Is Brewing Over Tech Privacy
Wednesday, 30 March 2016
Byline: Daisuke Wakabayashi, Devlin Barrett

New York - The sudden halt in the legal battle over a dead terrorist's phone may only intensify the broader fight about privacy and encryption, as tech companies race to better secure their hardware and software, while law-enforcement authorities fight to maintain access.
The Justice Department decided Monday to drop its lawsuit against Apple Inc., saying that the Federal Bureau of Investigation, aided by a third party, had unlocked the iPhone belonging to Syed Rizwan Farook, one of two gunmen in the San Bernardino, Calif., attack, and no longer needed the company's help.

The government didn't disclose how it got into the phone, or whether that vulnerability remains open for others to exploit in the future.

It isn't clear whether the government will share the information with Apple, but officials said Tuesday that there are good reasons to keep the company in the dark -- at least for now. Chief among those, they said, was Apple's resistance to helping investigators unlock its phones.

Meanwhile, the FBI is working to determine whether the method used to crack Mr. Farook's iPhone 5C might work on other models of the phone, according to people familiar with the matter.

The Justice Department's decision to drop the case leaves both the government and the company in awkward positions. Apple avoids being compelled to build a back door into its software that it argued could be exploited by hackers, but now faces an undefined threat to iPhone security.

The government gains a tool to unlock Apple devices that it says could help fight crime and terrorism, but risks losing credibility with Silicon Valley and the public, after first saying it couldn't open the phone, and then declaring that it could but refusing to reveal how. And, if it doesn't share the information with Apple, it risks leaving criminals an opening to exploit the same weakness.

The outcome is likely to intensify the mistrust between technology companies and law-enforcement authorities. Technology firms may now feel the need to make their security as impenetrable as possible to ease the public's concerns about privacy, industry officials said.

Meanwhile, without a decisive court victory, law- enforcement agencies have more incentive to find and exploit technological vulnerabilities and keep their methods secret.

"It deepens both sides in their respective positions," said Casey Ellis, chief executive of cybersecurity firm Bugcrowd. Government agencies have kept vulnerabilities to themselves before, but the FBI doing "this publicly and in front of so many people is a new thing," he said.

The legal fight between the government and Apple was viewed as a pivotal showdown over how to balance security and privacy in the smartphone era, with both sides prepared to go to the Supreme Court. But, federal prosecutors in the case asked the judge to vacate her earlier order compelling Apple to cooperate, leaving the central issue unresolved. Late Tuesday, the judge granted the prosecutors' request.

Apple has made clear that it will keep fortifying its devices. It said Monday it would "continue to increase the security of our products as the threats and attacks on our data become more frequent and more sophisticated."

As reported, Apple is working to beef up its encryption so that it won't be able to access some user information stored by its iCloud service.

Other companies are expected to follow suit.

Mark Bartholomew, a law professor at the University of Buffalo who specializes in privacy and cybersecurity, said technology firms will now "go full-speed ahead on full encryption and fuller encryption."

Decisions on whether government computer experts should tell tech firms or the public about security flaws are handled through what White House officials call a vulnerabilities equity review process, in which intelligence and law-enforcement agencies weigh the pros and cons of revealing the glitch so it can be fixed.

The Office of the Director of National Intelligence has said it leans toward disclosing security flaws.

There are other considerations that can weigh in favor of not disclosing them, including whether criminal hackers or foreign governments are likely to exploit the vulnerability, and whether revealing itcould curtail government access to critical intelligence.

On Tuesday, prosecutors made a new court filing in another closely watched phone case in federal court in Brooklyn, N.Y., where a magistrate judge has ruled in favor of Apple, saying current law doesn't allow the Justice Department to force the company to help investigators open a locked phone in a drug case. Federal prosecutors have asked a higher judge to review that decision.

With the San Bernardino phone now accessed by investigators, the Brooklyn case could become the next big legal fight involving the issue.

USA Today
1,000 devices in limbo after FBI drops iPhone case

Wednesday, 30 March 2016
Byline: Kevin Johnson, Elizabeth Weise

Washington - The government's surprise decision to withdraw its case against Apple over the San Bernardino, Calif., killer's iPhone adds uncertainty to criminal cases in which state and local authorities are confronted with more than 1,000 locked smartphones and other devices, blocking access to potential evidence, according to a survey of more than a dozen jurisdictions.
These locked devices are separate from the most high- profile one: the iPhone used by Syed Farook, who with his wife, Tashfeen Malik, carried out the shooting in San Bernardino that left 14 dead in December. In mid-February, a California court ordered Apple to aid the FBI in unlocking that iPhone.

On Monday, the FBI said it had been able to unlock the phone without Apple's aid. Left unanswered is what the Justice Department's abandoned legal action means for other law enforcement agencies seeking help from manufacturers in unlocking devices.

"We were hoping this decision, which could have gone to the Supreme Court, would have been a road map, and now it's not," said Stewart Baker of Steptoe & Johnson. State and local investigators have been blocked from accessing contents of more than 1,000 devices because of their inability to bypass security functions similar to those encountered by the FBI in the San Bernardino case.

"The overwhelming majority of criminal investigations stalled by default device encryption will remain so until Congress intervenes," Manhattan District Attorney Cyrus Vance said in a statement Tuesday.

According to some attorneys, the government's actions have weakened its credibility if it tries to argue for compelling companies to help it in future cases. Justice spent a month saying Apple's assistance was the only way it could get into the phone, then suddenly said it wasn't, said Scott Vernick, head of data security at Fox Rothschild in Philadelphia.

"Now any other court is going to ask, 'Really? Are you sure you need their help? That's what you asked for last time, and apparently you didn't,'" Vernick said.

Washington Post
FBI, Apple in 'arms race,' experts say
Wednesday, 30 March 2016
Byline: Matt Zapotosky, Elizabeth Dwoskin

Washington - The U.S. government's revelation that it had accessed the San Bernardino shooter's iPhone without the help from Apple that it had so desperately sought indicates that the FBI was either disguising its technical capabilities or its agents and employees remain outmatched by tech workers in the private sector, according to current and former bureau officials and legal scholars.

The bureau in recent years has launched a recruiting blitz to attract employees with cyber expertise, and the National Science Foundation has even made scholarship money available to students who study cybersecurity and later work in government. But former FBI officials said the bureau will always face an uphill battle against private firms, which can offer much more money, a less-rigorous code of conduct and more opportunities to do creative work.

Ernest Hilbert, a former FBI special agent focusing on cybercrimes, said the bureau had lost tech talent in recent years. "The most an agent can make is 180K," he said. "That's like a starting salary in the private sector. You have a big push by private industry to pull out these individuals."

That bureau officials were able to access Syed Rizwan Farook's phone allows the government to avoid - at least for now - a showdown with Apple over the extent U.S. law compels the company to help in a criminal investigation.

But the high-profile fight over the San Bernardino terrorist's phone also exposes that Apple's phone has vulnerability, further motivating it and other companies to strengthen the security of their devices and forcing the government to keep up with new security measures, technology executives and security analysts said.

"They're in an arms race," said Matthew Blaze, a cryptography researcher and professor at the University of Pennsylvania. "The FBI is trying to find new ways in, and Apple is trying to find new ways to defend against that."

In interviews, engineers across Silicon Valley said they thought the case would affect the way products are built going forward at both start-ups and large companies.

The case "will reinforce people's arguments" for tougher encryption, said Cameron Walters, an engineer who was an early engineer at payments start-up Square. "It might push them to do it - if it was a question of effort versus return."

The cloud-computing company Box, which filed a legal brief supporting Apple in the San Bernardino case, is one of the many tech firms rushing to offer new encryption-related security features. It recently launched a product, KeySafe, that allows corporate customers to hold on to their own encryption keys - a move co-founder and chief executive Aaron Levie said was as much about fighting off hackers as about fending off government surveillance. The implementation of KeySafe means the company cannot collect and hand over a customer's private information even when the authorities have a warrant.

Lawyers and people in the tech industry say that the FBI's sudden arrival at a solution - a month ago it was claiming it could not get into Farook's phone without Apple's help - raises questions about law enforcement's handling of the matter. FBI officials have offered their version of what happened in court documents and sworn affidavits, and have disputed any insinuation that they did wrong.

On this much, many agree: The case shows that the FBI is lagging behind when it comes to some technical capabilities.

"I think the bureau is absolutely in an uphill battle, desperately trying to keep up pace, and they are not," said Ronald T. Hosko, a former assistant director in charge of the FBI's criminal division who is now president of the Law Enforcement Legal Defense Fund.

The FBI devotes significant resources to cybersecurity investigations and its operational- technology division. The bureau's fiscal 2017 budget proposal asked for $85.1 million more for cybersecurity and an additional $38.3 million for an initiative meant to help investigators beat encryption when appropriate.

Farook and his wife, Tashfeen Malik, were killed in a shootout with police in December after they launched an attack that killed 14 people at the Inland Regional Center in San Bernardino, Calif.

The bid to access the phone used by Farook was meant to further the FBI's investigation. The Justice Department obtained a court order compelling Apple's assistance under the All Writs Act, a centuries-old law that gives courts the power to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."

Federal prosecutors initially said they had no way into the phone without Apple's help. Apple resisted, arguing that complying with the government's request would infringe customers' privacy.

Last week, on the eve of a hearing in the case, prosecutors for the first time suggested there might be a way in without Apple, writing in a court filing that "an outside party demonstrated to the FBI a possible method for unlocking Farook's iPhone." The method apparently worked; prosecutors wrote in another court filing Monday that they had "successfully accessed the data stored on Farook's iPhone," and a judge formally vacated an order compelling Apple's assistance Tuesday.

The FBI has not disclosed how it got in, other than to say it no longer needed Apple's help. An official familiar with the matter, while declining to discuss the San Bernardino case in particular, said, "Whether a solution comes ultimately from our own personnel, from another federal agency or other entity is less important than whether the solution addresses the requirements to investigate major crimes and terrorist attacks." The official spoke on the condition of anonymity to discuss internal bureau operations.

Alex Abdo, a staff attorney with the American Civil Liberties Union, said that "the speed with which they were able to verify this new technique is a reason to be skeptical" of officials' previous claims.

"The FBI sat on this phone for two months, then made a deliberate decision to very publicly fight with Apple over the unlocking mechanism, and then made very strong statements about their inability to get in without Apple's help. And, on a dime, that all changed," Abdo said.

FBI and Justice Department officials have bristled at the notion that they misled the public or that agents were not working hard to access the phone. Deputy Attorney General Sally Q. Yates said at a recent news conference that FBI agents had "been working hard all along" and that officials at the Justice Department were "a little surprised" to learn there might be another solution.

FBI Director James B. Comey wrote in a letter to the Wall Street Journal that he was "not embarrassed to admit that all technical creativity does not reside in government."

That the FBI got in without Apple's help leaves unresolved a critical question: Can the government use the All Writs Act to compel others to take the steps it wanted Apple to take? That matter, legal experts said, will be left for Congress or another court case.

Wall Street Journal
Hackers Breach Law Firms, Including Cravath, Weil Gotshal
Wednesday, 30 March 2016
Byline: Nicole Hong, Robin Sidel

New York - Hackers broke into the computer networks at some of the country's most prestigious law firms, and federal investigators are exploring whether they stole confidential information for the purpose of insider trading, according to people familiar with the matter.
The firms include Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP, which represent Wall Street banks and Fortune 500 companies in everything from lawsuits to multibillion-dollar merger negotiations.

Other law firms also were breached, the people said, and hackers, in postings on the Internet, are threatening to attack more.

It isn't clear what information the hackers stole, if any, but the focus of the investigation is on whether confidential data were taken for the purpose of insider trading, according to a person familiar with the matter.

The Manhattan U.S. attorney's office and Federal Bureau of Investigation are conducting the probe, which began in the past year and is in its early stages, the people said. Representatives for both declined to comment.

Cravath said the incident, which occurred last summer, involved a "limited breach" of its systems and that the firm is "not aware that any of the information that may have been accessed has been used improperly." The firm said its client confidentiality is sacrosanct and that it is working with law enforcement as well as outside consultants to assess its security.

A spokeswoman for Weil Gotshal declined to comment.

The cyberattacks show what law-enforcement officials have been warning companies about for years. As hacking tools and hackers for hire proliferate in certain corners of the Internet, it has become easier for criminals to breach computer networks as a way to further a range of crimes, from insider trading to identity theft.

In recent years, a number of major retailers have been breached, as was J.P. Morgan Chase & Co., the country's biggest bank by assets. In those cases, hackers stole data such as credit-card numbers and email addresses that they could use to make fraudulent purchases or entice customers into scams.

The attacks on law firms appear to show thieves scouring the digital landscape for more sophisticated types of information. Law firms are attractive targets because they hold trade secrets and other sensitive information about corporate clients, including details about undisclosed mergers and acquisitions that could be stolen for insider trading.

Hackers often steal large amounts of information indiscriminately and then analyze it later to see how it could be useful, making it difficult to determine early on in these types of investigations whether any information was actually used for insider trading, observers said.

The potential vulnerability of law firms is raising concerns among their clients, who are conducting their own assessments of the firms they hire, according to senior lawyers at a number of firms.

A case last year shows that hackers have gone after sensitive material to fuel illegal trading. In that case, brought by federal prosecutors in New Jersey and Brooklyn, N.Y., hackers in Ukraine allegedly breached newswires companies in the U.S. and stole news releases about corporate earnings before they became public. Stock traders then made lucrative bets based on the releases, prosecutors said. At least three of the defendants have pleaded guilty, and the case is pending.

The federal investigation into the law firms is one of several recent cyber-related incidents that have affected the legal industry.

In February, a posting appeared on an underground Russian website called DarkMoney.cc, in which the person offered to sell his phishing services to other would-be cyberthieves and identified specific law firms as potential targets. In phishing attacks, criminals send emails to employees, masked as legitimate messages, in an effort to learn sensitive information like passwords or account information.

Security firm Flashpoint issued alerts to law firms in January and February about the threats and has acquired a copy of a phishing email that is aimed at law firms, according to a person familiar with the alerts. "It has definitely picked up steam," this person said.

The FBI also issued an alert in recent weeks that warned law firms about potential attacks, according to people familiar with the alert. The FBI declined to comment.

Law firms said they have double-checked their cybersecurity defenses in response to the posting and raised more awareness about the issue internally. It isn't clear if the hacker's efforts have resulted in any breaches. A Flashpoint spokeswoman declined to comment on the alerts.

One senior partner at a top law firm said he often receives suspicious emails from people who pretend to be seeking legal representation. "Law firms are being deluged with attempts to crack their systems," he said.

Law firms last year formed an information-sharing group to disseminate information about cyberthreats and other vulnerabilities. It is modeled after a similar organization for financial institutions.

So far, 75 law firms have joined the group, said Bill Nelson, chief executive officer of the Financial Services Information Sharing and Analysis Center, which oversees the legal group and similar entities that focus on other industries, such as retail.

One of the trickiest questions for law firms is when they are required to publicly disclose a data breach. Forty-seven U.S. states have their own breach-notification laws, forcing law firms and other companies to navigate a patchwork of different rules.

New York Times
Beijing May Pull Reins Tighter on Websites in Country
Wednesday, 30 March 2016
Byline: Paul Mozur

Hong Kong - China's government said on Monday that it would take steps to more strictly manage websites in the country, its latest push to set boundaries in the wider Internet.
A draft law posted by one of China's technology regulators said that websites in the country would have to register domain names with local service providers and with the authorities.

It was not clear whether the rule would apply to all websites or only to those hosted on servers in China. Chinese laws can be haphazardly enforced and are usually vague, and because the new rule is only a draft, analysts said they expected the regulator, the Chinese Ministry of Industry and Information Technology, to specify later to whom the law would apply.

If the rule applies to all websites, it will have major implications and will effectively cut China out of the global Internet. By creating a domestic registry for websites, the rule would create a system of censorship in which only websites that have specifically registered with the Chinese government would be reachable from within the country.

Zhu Wei, deputy director of the Communications Law Research Center at the China University of Political Science and Law in Beijing, said he believed that under the current wording, the law would block foreign websites not registered with China.

"I think the draft mostly tries to address Internet security and the large amount of pornographic websites and other websites that violate Chinese laws," he said. "Most of those domains are registered abroad. It is not easy to tackle them."

Other experts, however, said the law would probably apply only to websites hosted in China.

"I think these regulations are about content hosted in China," said Rogier Creemers, a lecturer on Chinese politics at Oxford University. "It can be that they expand in the future." He pointed out that if the rules applied to all websites, they would eliminate access overnight to a huge chunk of the Internet.

If the law applies only to sites hosted in China, it would still represent a consolidation of power by Beijing. Forcing registration with Chinese entities is likely to create a new boom in domain-name service registrars. At the moment, Alibaba operates China's primary domain-name service provider, called Wan Wang.

The new rule would also enable the Chinese government to keep closer tabs on the real identities of website operators. It would also help Beijing assemble a registry of important websites if China wants to break away from the global registry that unifies the Internet, Mr. Creemers said.

The Ministry of Industry and Information Technology, which said violators of the rule would face fines of 10,000 renminbi to 30,000 renminbi, or about $1,500 to $4,500, will hear comments on the regulation until April 25.

The new rules are the latest in a string of measures taken by the Chinese government under President Xi Jinping to assert control over the Internet. This year, regulators created rules to block foreign companies from publishing online content in China without the government's consent. Regulators also shut down the social media accounts of the sharp-tongued tycoon Ren Zhiqiang.

In recent years, Mr. Xi has presided over a special committee to strengthen the government's oversight of the Internet domestically, and more broadly to influence how the Internet is governed abroad.

He has also presided over the creation of the Cyberspace Administration of China, a regulatory body that has pushed censorship and worked on an annual conference intended to trumpet China's belief that each country should be allowed to impose rules on the Internet within its borders.

Lokman Tsui, a professor at the School of Journalism and Communication at the Chinese University of Hong Kong, said the latest move was "in line with the developments that have been going on for a while

now, where the government is trying to exercise more supervision and control over the Internet, and on the domain name system in China."

Washington Post
Judge allows questioning in Clinton email case
Wednesday, 30 March 2016
Byline: Spencer S. Hsu

Washington - A second federal judge in Washington ruled Tuesday that a conservative legal watchdog group may question the State Department and potentially several top aides to Democratic presidential contender Hillary Clinton about her use of a private email server while she was secretary of state.
In a three-page order, U.S. District Senior Judge Royce C. Lamberth granted a request from Judicial Watch, which has sought public records of talking points used by Susan E. Rice, then the U.S. ambassador to the United Nations, in television appearances after the deadly Sept. 11, 2012, attacks on U.S. facilities in Benghazi, Libya.

Appearing five days later on Sunday- morning talk shows, Rice, now President Obama's national security adviser, said the assaults appeared to have stemmed from a spontaneous protest over an anti-Islam video. U.S. investigators later concluded that the attacks were carried out by terrorist groups.

"Where there is evidence of government wrong-doing and bad faith, as here, limited discovery is appropriate, even though it is exceedingly rare in FOIA [Freedom of Information Act] cases," Lamberth wrote.

His decision came about five weeks after another federal judge in Washington, U.S. District Judge Emmet G. Sullivan, ruled that current and former top State Department and Clinton aides could be questioned under oath about her email arrangement in a separate Judicial Watch FOIA case. The group has questioned whether officials intentionally thwarted federal open-records laws by using or allowing the use of a private email server during Clinton's tenure at State from 2009 to 2013.

In both cases, the judges said sufficient doubt had been raised about whether department searches of public records were adequate.

The department faced dozens of FOIA lawsuits after disclosures that Clinton exclusively used a personal server for government business while at State and that several aides also used the server or personal email addresses. Clinton and others have since returned tens of thousands of pages that they or their attorneys have designated as work-related for government FOIA review and potential release.

However, Sullivan and Lamberth criticized what Lamberth called the "constantly shifting admissions by the government and former government officials" about the arrangement. Sullivan said the server

arrangement allowed former federal employees to decide what government records to disclose, apparently without ensuring that State records were secured within the department's own systems.

Calling Clinton's personal server use "extraordinary," Lamberth wrote, "An understanding of the facts and circumstances . . . is required before the Court can determine whether the search conducted here reasonably produced all responsive documents."

Sullivan, in the earlier case, set an April 12 deadline for Judicial Watch and the government's lawyers to lay out a plan for how they want to proceed, subject to court approval.

Lamberth said in his order that after Sullivan decides how to proceed in that case, Judicial Watch should submit a proposed discovery plan within 10 days to him in the Rice matter, and the government can respond in another 10 days.

The case before Sullivan concerns public records sought by Judicial Watch about the employment arrangement of Huma Abedin, a longtime confidante who served as Clinton's deputy chief of staff.

Judicial Watch has proposed questioning seven current and former officials, including Cheryl D. Mills, who was Clinton's chief of staff at State; Abedin, who now is vice chairman of Clinton's presidential campaign; and Bryan Pagliano, a Clinton staff member during her 2008 presidential campaign who helped set up the private server.

Others designated for deposition are Undersecretary for Management Patrick F. Kennedy; Stephen D. Mull, executive secretary at State from June 2009 to October 2012; Lewis A. Lukens, executive director of the executive secretariat from 2008 to 2011; and Donald R. Reid, senior coordinator for security infrastructure in the Bureau of Diplomatic Security.

Judicial Watch said it intends to seek answers about department officials' creation, maintenance, support or awareness of Clinton's email system; any instructions given to department workers about communicating by email with Clinton and Abedin; and any inquiries into or discussions about disclosing Clinton's use of the system.

Sullivan noted in his ruling that senior department officials appeared to know about Clinton's set-up from her swearing-in at State in January 2009, citing an email chain among Kennedy, Lukens, Mills and others regarding setting up a computer in Clinton's office so she could check her "off network" email.

Sullivan also noted email traffic among Abedin, Mull, Mills, Kennedy and others discussing communication problems, in which Mull suggested that Clinton be issued a State Department BlackBerry that would protect her identity but be subject to public-records requests.

Politico

Official: FBI team on Clinton email probe not near 150
Monday, 28 March 2016
Byline: Josh Gerstein

Washington - The FBI does not have close to 150 agents working the investigation into former Secretary of State Hillary Clinton's email server, a source familiar with the matter told POLITICO Monday.
The official, who spoke on condition of anonymity, commented after the Washington Post reported that FBI Director James Comey told an unnamed member of Congress that 147 agents were working the Clinton investigation.

Asked about the Post report, the source said: "That number is greatly exaggerated."

The source and other officials declined to provide any further details about FBI staffing or the status of the inquiry.

The Post report followed similar but slightly different reports in other media outlets. In January, Fox News reported that 100 FBI agents were working regularly on the Clinton case with as many as 50 more on temporary assignment. At about the same time, the Washington Examiner reported that a former U.S. Attorney for Washington, D.C., Joseph DiGenova, indicated a similar scope to the FBI probe.

"There are now, I am told, 150 agents working on this case," DiGenova said, calling that "a very unusually high number."

Both the Fox and Washington Examiner reports focused on an expansion of the Clinton email probe to cover possible public corruption involving the Clinton Foundation. The FBI has declined to confirm that any such probe is underway, although Comey has confirmed publicly that the FBI is looking into issues involving classified material on the Clinton server.

In a court filing Friday, an FBI records official called that investigation "active" and "ongoing."

New York Times
Apple's Newest Challenge: Learning How Government Cracked Its iPhone
Wednesday, 30 March 2016
Byline: Multiple reporters

San Francisco - Now that the United States government has cracked open an iPhone that belonged to a gunman in the San Bernardino, Calif., mass shooting without Apple's help, the tech company is under pressure to find and fix the flaw.
But unlike other cases where security vulnerabilities have cropped up, Apple may face a higher set of hurdles in ferreting out and repairing the particular iPhone hole that the government hacked.

The challenges start with the lack of information about the method that the law enforcement authorities, with the aid of a third party, used to break into the iPhone of Syed Rizwan Farook, an attacker in the San Bernardino rampage last year. Federal officials have refused to identify the person, or organization, who helped crack the device, and have declined to specify the procedure used to open the iPhone. Apple also cannot obtain the device to reverse-engineer the problem, the way it would in other hacking situations.

Making matters trickier, Apple's security operation has been in flux. The operation was reorganized late last year. A manager who had been responsible for handling most of the government's data extraction requests left the team to work in a different part of the company, according to four current and former Apple employees, who spoke on the condition of anonymity because they were not authorized to speak publicly about the changes. Other employees, among them one whose tasks included trying to hack Apple's own products, left the company over the last few months, they said, while new people have joined.

The situation is in many ways a continuation of the cat-and-mouse game Apple is constantly engaged in with hackers, but the unusually prominent nature of this hacking -- and the fact that the hacker was the United States government -- creates a predicament for the company.

"Apple is a business, and it has to earn the trust of its customers," said Jay Kaplan, chief executive of the tech security company Synack and a former National Security Agency analyst. "It needs to be perceived as having something that can fix this vulnerability as soon as possible."

Apple referred to a statement it made on Monday when the government filed to drop its case demanding that the company help it open Mr. Farook's iPhone. "We will continue to increase the security of our products as the threats and attacks on our data become more frequent and more sophisticated," Apple said.

Apple has been making many long-term moves to increase the security of its devices. The company's chief executive, Timothy D. Cook, has told colleagues that he stands by Apple's road map to encrypt everything stored on its devices and services, as well as information stored in Apple's cloud service iCloud, which customers use to back up the data on their mobile devices. Apple engineers have also begun developing new security measures that would make it tougher for the government to open a locked iPhone.

For now, with the dearth of information about the flaw in Mr. Farook's iPhone 5C, which runs Apple's iOS 9 operating system, security experts could only guess at how the government broke into the smartphone.

Forensics experts said the government might have attacked Apple's system using a widely discussed method to extract information from a protected area in the phone by removing a chip and fooling a mechanism that blocks password guessing, in order to find the user's password and unlock the data.

The authorities may have used a procedure that mirrors the phone's storage chip, called a NAND chip, and then copied it onto another chip. Often referred to as "NAND-mirroring," this would allow the F.B.I. to replace the original NAND chip with one that has a copy of that content. If the F.B.I. tried 10 passcodes to unlock the phone and failed, it could then generate a new copy of the phone's content and try another password guess.

"It's like trying to play the same level on Super Mario Brothers over and over again and just restoring from your saved game every time you kill Mario," said Jonathan Zdziarski, an iOS forensics expert.

Newer iPhone models may be less susceptible to NAND-mirroring because they have an upgraded chip known as the A7, with a security processor called the Secure Enclave that has a unique numerical key not known to the company and which is essential to the securing of information stored in the phone.

Security vulnerabilities in Apple products have become increasingly prized by hackers in recent years, given the ubiquity of the company's mobile devices. Yet as interest has grown in attacking Apple's hardware and software, the company's own security teams have been in flux.

Apple previously had two main security teams -- a group called Core OS Security Engineering and a product security team. The product security team included a privacy group that examined whether data was properly encrypted and anonymized, among other functions, according to three former Apple employees. The product security team also had people who reacted to vulnerabilities found by people outside Apple, as well as a proactive team, called RedTeam, which worked to actively hack Apple products.

Last year, the product security team was broken up and the privacy group began reporting to a new manager, the former employees said. The rest of product security -- the proactive and reactive pieces -- was absorbed by the Core OS Security Engineering team, which itself experienced shifts.

The leader of the Core OS Security Engineering team, Dallas DeAtley, left the security division last year to work in a different part of Apple. Mr. DeAtley was one of the few employees who over the years had taken care of government requests to extract data from iPhones. Mr. DeAtley did not respond to requests for comment.

A few other members of the team also departed. Others joined Apple as the company acquired a handful of security outfits last year, including LegbaCore, which previously found and fixed flaws for Apple.

Some of the departures had more to do with market forces, the former Apple employees said. Security professionals are some of the most sought-after engineers in the technology sector.

Whether Apple's security operation will ever obtain information about how the government hacked into Mr. Farook's iPhone remains unclear.

It's possible that the government won't say how it opened the iPhone because the method is "proprietary to the company that helped the F.B.I.," said Stewart A. Baker, a lawyer at Steptoe & Johnson and the Department of Homeland Security's first assistant secretary for policy.

Within the security community, researchers and professionals said they were incensed that they - - and Apple -- may not find out how the F.B.I. was able to crack Mr. Farook's iPhone.

"There is very little debate that it is in everyone's best interest that Apple find out about this vulnerability and everyone should be asking why that is not the case," said Alex Rice, the chief technology officer at HackerOne, a security company in San Francisco that helps coordinate vulnerability disclosure for corporations.

The Hill
Obama extends cyber sanctions power
Wednesday, 30 March 2016
Byline: Cory Bennett

Washington - President Barack Obama on Tuesday expanded upon his statement that the rising number of cyberattacks on the U.S. constitutes a national emergency.
"These significant malicious cyber-enabled activities continue to pose an unusual and extraordinary threat to the national security, foreign policy and economy of the United States," Obama wrote in a notice.

The president initially made the declaration on April 1, 2015, as part of an executive order that empowered the Treasury Department to levy sanctions on individuals or entities behind cyberattacks and cyber espionage.

The move was an attempt to impose costs on foreign hackers who have peppered the U.S. with cyberattacks for years with few repercussions.

The sanctions would effectively freeze targets's assets when they pass through the U.S. financial system and prohibit them from transacting with American companies.

Obama said Treasury would retain these powers for at least another year, given the pervasive cyber threat that remains.

"The measures adopted on that date to deal with that emergency, must continue in effect beyond April 1, 2016," he said.

The White House has yet to exercise these powers, although some believe the administration may follow up the recent indictment of seven Iranian hackers with targeted sanctions.

Prior to the executive action, the White House did slap North Korea with a round of economic sanctions after blaming the reclusive East Asian country for orchestrating a digital assault on the movie studio Sony Pictures Entertainment.

Reuters
Spy chiefs tell U.S. lawmakers plan to share raw data protects privacy
Wednesday, 30 March 2016
Byline: Mark Hosenball

Washington - American spy chiefs have told congressmen that a plan to allow the National Security Agency (NSA) to share more raw eavesdropping reports with other agencies will not be unlawful and will protect the privacy rights of U.S. citizens.
In a letter sent on Monday to two members of Congress and reviewed by Reuters, Director of National Intelligence James Clapper said the NSA's proposal to give other spy agencies access to "unevaluated signals intelligence" will ensure data is used only for intelligence activities directed at foreigners.

Last week, U.S. Representatives Ted Lieu and Blake Farenthold of the House Oversight Committee asked the NSA to halt the sharing plan, suggesting it would be "unconstitutional and dangerous." The specifics of the proposal are still secret.

Lieu, a Democrat from California and Farenthold, a Republican from Texas, wrote in a March 21 letter to NSA Director Michael Rogers that the proposal would violate Fourth Amendment privacy protections because the collected data would not require a warrant before being searched for domestic law enforcement purposes.

Monday's reply from the intelligence chief's office said the plan would not allow the use of communications data for domestic law enforcement.

Instead, the proposed rules would limit access to raw NSA data to spy agencies, "and only for authorized foreign intelligence and counterintelligence purposes," said the letter. It said it would also not authorize any new collection of private communications.

Civil liberties advocates have interpreted the proposed change as potentially allowing NSA foreign intelligence data, which sometimes can include collection of communications to, from or about Americans, to be used for domestic policing purposes.

Under current procedures, NSA analysts are supposed to scrub or black out certain personal information, particularly related to American citizens or residents, before handing any communications data over to other agencies.

Congress last year passed a law curtailing certain aspects of the NSA's spying authority, most notably ending its bulk collection of domestic phone records exposed by former NSA contractor Edward Snowden in 2013. NSA began that program after the Sept. 11, 2001 attacks on the United States by Islamist militants.

The NSA has presented the plan to a government advisory committee, the Privacy and Civil Liberties Oversight Board, for review.

London Daily Telegraph
Trident upgraded to protect against cyber attack
Tuesday, 29 March 2016
Byline: Ben Farmer

London - Britain's Trident nuclear deterrent is to be updated to protect it from cyber attack. Software in the nuclear missile system will be upgraded as defence officials admitted there was "legitimate concern" about threats from cyber hackers.

The Trident missiles, which are shared with America, will be updated amid growing worries defence computers and systems could be vulnerable to cyber attacks from Russia, China, groups such as Islamic State or organised crime gangs.

A former Defence Secretary last year warned that the deterrent was unreliable unless the Government could ensure it was free of cyber weak spots that might be targeted.

Lord Browne of Ladyton warned: "If they are unable to do that then there is no guarantee that we will have a reliable deterrent or the Prime Minister will be able to use this system when he needs to reach for it."

The US Navy has now announced American and British Trident missiles will be upgraded as both nations pour billions into cyber security.

John Daniels, a spokesman for the US Navy's nuclear deterrent programme, told Bloomberg: "Now that cyber has become even more important in our national security, there will be even more requirements. In our modern era, cybersecurity threats are a legitimate concern."

The software security work will be carried out by BAE Systems, which carries out maintenance of the missiles. The company declined to comment on the work.

Britain's 58 missiles, which are carried by the Royal Navy's four Vanguard class nuclear submarines, are sent back to America for upgrades and maintenance. Each boat carries eight missiles, and each one can be fitted with up to 12 warheads that can strike different targets with a range of 7,500 miles.

Andrew Futter, a nuclear strategy expert at Leicester University, said until recently commanders had been "fairly complacent" about the cyber threat to the nuclear deterrent.

He said defence officials had stressed that because the UK's nuclear submarines were not connected to the Internet on secret deterrent missions they were largely protected from hackers by an "air gap" between the deterrent and the rest of the online world.

But he said there were still potential weak spots and there was a greater risk when the boats came in to port to receive upgrades and maintenance. Malicious programs to sabotage or damage the deterrent could also be secretly hidden in nuclear systems when new parts are being designed and made.

Dr Futter said a scenario where someone hacks into the deterrent to try to fire a missile or hold a country to ransom was "very, very slim".

A more likely risk would be hackers stealing design or operational secrets from the deterrent that would make it vulnerable.

He said: "It's information security that could be more important in the cyber realm."

A Ministry of Defence spokesman said: "The deterrent remains safe and secure. We take our responsibility to maintain a credible nuclear deterrent extremely seriously and continually assess the security of the whole deterrent programme and its operational effectiveness, including against threats from cyber."

London Times
Internet spy system could cost over £1bn
Wednesday, 30 March 2016
Byline: James Dean

London - The cost of creating a new surveillance system to collect the internet browsing records of British citizens has been drastically underestimated by the Home Office, MPs have been told.
The government would have to spend about £1.2 billion, more than seven times the Home Office's upper estimate, an analysis has suggested.

The authorities want internet companies to collect internet connection records (ICRs) of every British citizen and store them for up to 12 months using a new provision in the Investigatory Powers Bill. These

records, which are time-stamped histories of all the websites that people have visited, are to be used to help the police and security services with investigations.

The Danish government is attempting to put a similar record system in place but suspended its plans earlier this month after an official study found that the set-up costs would be far higher than envisioned. The Commons public bill committee on the Investigatory Powers Bill was told last week that the Danish study cast doubt on the Home Office's estimates.

The government has estimated that it would need to reimburse internet companies between £130.6 million and £164.4 million to set up computer systems that are capable of gathering and storing ICRs. Annual running costs would be a further £4.4 million to £5.6 million over ten years.

However, a study by EY, commissioned by the Danish government, found that the country's internet providers would need to spend 1 billion Danish kroner (£105 million) on computer systems capable of collecting and storing ICRs. The figure is equivalent to about £19 per person and would add up to £1.2 billion if that cost is applied to the UK's population of 64.6 million.

The IT-Political Association of Denmark, a digital rights group, said in written evidence: "Based on the new cost information from Denmark, it seems unlikely that the Home Office budget can cover a sufficiently effective ICR implementation, unless only a small part of the British population is subjected to [ICRs]."

The Home Office did not respond to requests for comment.

Globe and Mail
Six guilty pleas to murder conspiracy end risk of revealing police-surveillance secrets
Thursday, 31 March 2016
Byline: Colin Freeze

Six accused mobsters were acquitted of first-degree murder charges in Laval on Wednesday as they agreed to plead guilty to a lesser charge of murder conspiracy, scuttling a separate hearing that risked revealing sensitive information about police surveillance technology.
In the second case the same day in Montreal, Canada's national police force learned there would be no binding Quebec Court of Appeal hearing related to "mobile device identifier" technology that the RCMP had used to keep tabs on the alleged Mafia members.

These two decisions on the same landmark police- surveillance case came Wednesday morning after five years of being stuck in neutral as lawyers debated disclosure issues.

The outcome benefited both prosecution and defence, but it meant none of those convicted of murder conspiracy in the shooting death of a man in the streets of Montreal five years ago are still facing actual murder charges.

"This is a matter of prosecutorial discretion and I will not comment further," Quebec prosecutor Robert Rouleau said, after The Globe asked him why the Crown did not pursue the firstdegree murder charges.

The case appears to show just how far police and prosecutors will go to safeguard investigative techniques considered secret.

Speaking outside the appeal court Wednesday, Mr. Rouleau pointed out that the guilty pleas effectively meant there would be no more disclosure about the police devices.

"Since the case becomes moot, there's no reason to pursue a production order if there is no disclosure to be made."

The Globe first reported on filings related to the case earlier this month, revealing that Crown prosecutors had taken to publicly calling the RCMP device a "mobile device identifier" in an apparent bid to escape some of the criticisms surrounding devices more commonly known as "IMSI- catchers."

It turns out that MDI is simply an RCMP term. "The MDI is a device that may be described as and is commonly referred to as an 'IMSI catcher,' " reads one Crown exhibit in the case, viewed by The Globe and Mail on Wednesday.

The roots of the case trace back to Nov. 24, 2011, when a New Yorker named Salvatore (Sal the Ironworker) Montagna was shot dead on the outskirts of Montreal. Fearing more bloodletting was

imminent, an RCMP- led team divulged its organized-crime surveillance operation to local police so they could make arrests in that gangland slaying.

For five years, six suspects faced first-degree murder charges - a conviction would mean 25 years in prison with no chance of parole. On Wednesday, the same six pleaded guilty to the lesser charge of conspiracy to commit murder. Sentencing hasn't been settled yet, but it likely means that - at the most - they will get a few years on top of the time they've spent in jail awaiting trial.

(A seventh man also pleaded guilty Wednesday to being an accessory after the fact of a murder.)

The case amounts to the first acknowledged used by Canadian police of IMSI catchers.

The portable devices, packed by police surveillance teams, can impersonate a cellphone tower, capturing the digital signatures of all the phones within a given radius (IMSI stands for "international mobile subscriber identity"). From there, police can try to identify suspects' phones by a process of elimination and try to get wiretaps on those specific phones.

In pretrial motions police argued all this was a privileged investigative technique, while defence lawyers argued they were entitled to detailed information about the device. Toronto-based defence lawyers Frank Addario and Michael Lacy raised a litany of detailed questions - such as asking for the IMSI catcher's make and model, its range and the reliability of its evidence. A national-security specialist, Toronto lawyer Anil Kapoor, was brought in as a friend of the court to help settle some of the questions.

While prosecutors argued the defence was on a "fishing trip" that would essentially hand the police playbook to alleged mobsters, Quebec Superior Court Judge Michael Stober sided with the defence last December. "The Court concludes that the accused have a legitimate interest in receiving disclosure of information that goes to the heart of this prosecution," he ruled.

The Crown immediately appealed - setting the stage for Wednesday's appeal court hearing. Had it happened, it would have had the effect of creating a binding ruling about how police are to use and disclose such devices in Quebec.

Instead, Wednesday morning's hearing in Montreal lasted only long enough for the judges to learn that the scheduled hearing was no longer necessary, due to the guilty pleas that had just been uttered in Laval. The effect is that Justice Stober ruling is an outlier's opinion from the lone judge in Canada who got a chance to explore the legal questions raised by RCMP IMSI catchers.

"It's not going to bind any other courts," said Mr. Kapoor, who had been on hand to Montreal to make arguments at the appellate court.

Sputnik (Russia)
US 'Political Chatter' Prevents Snowden's Defense
Thursday, 31 March 2016

Moscow - Former US National Security Agency (NSA) contractor Edward Snowden accused of espionage by the United States cannot prove his innocence, as long as US authorities only make cunning statements about him and do not announce the subject of his charges, one of Snowden's lawyers said Thursday.
"From the first day Edward Snowden has been on the territory of Russia, sweeping accusations against him began to appear, without submitting any specific charges of committing any crime. A person must understand the subject of the charges to defend himself, and there is no such thing, there is a political chatter," Anatoly Kucherena told RIA Novosti.

The lawyer also called Washington's claims of providing Snowden with a fair trial in the United States "cunning."

"We are well aware that such chatter, sweeping accusations, insults, him being used for political purposes by US presidential hopefuls - leave a just, fair trial of Edward Snowden out of the question," Kucherena added.

Snowden started making revelations about widespread US global surveillance in 2013. The same year, Russia granted the whistleblower temporary asylum for one year. In August 2014, Snowden received a three-year residence permit to live in Russia.

In the United States, he faces up to 30 years in prison on charges of espionage and theft of government property.

The US Espionage Act was never intended to prosecute journalistic sources used for public good and prevents Snowden from defending himself in an open court before a jury, according to the whistleblower.

Wall Street Journal
Google Was Also Ordered To Unlock Phones
Thursday, 31 March 2016
Byline: Devlin Barrett

Washington - Alphabet Inc.'s Google has been repeatedly ordered to help federal agents open cellphones, according to court records in seven states that show Apple Inc. isn't the only company facing government demands at the center of a fierce debate over privacy and security.

The American Civil Liberties Union found 63 instances where the government sought a court order under a 1789 law called the All Writs Act to compel Apple and Google to help in accessing data on locked phones.

The outcomes aren't clear. However, federal prosecutors have said until late last year, when Apple began resisting such efforts, it was routine for judges to approve such requests. And those requests aren't new -- the cases stretch back to 2008.

Details of the cases come days after the Justice Department said it cracked into a terrorist's cellphone, ending a court battle over whether Apple can be forced by a court to help the Federal Bureau of Investigation bypass the phone's passcode security system.

The overall numbers aren't surprising, since prosecutors have previously said Apple provided assistance in such cases more than 70 times. Most, but not all, of the 63 cases identified by the ACLU involve Apple.

But the figures offer the first accounting of how the government has also sought such orders for Google to help investigators pull data off locked smartphones, typically by having the company reset the devices' passwords.

"We carefully scrutinize subpoenas and court orders to make sure they meet both the letter and spirit of the law," a Google spokesman said. "However, we've never received an All Writs Act order like the one Apple recently fought that demands we buildnew tools that actively compromise our products' security. . .We would strongly object to such an order."

The language of the All Writs Act is expansive, allowing federal courts broad authority to compel others to do what they say. But the government has most often looked to it for help in cases involving technology beyond its control.

The Justice Department has defended the practice of getting court orders to compel assistance from technology companies as a routine and necessary part of law-enforcement work when there is no other way for agents to access a suspect's phone that might hold important criminal evidence. Privacy groups argue the government is misusing an outdated law to claim authority not granted by Congress.

A court filing last month from Apple indicated there were at least a dozen active cases in which the Justice Department was pursuing similar orders involving Apple.

In one of the Google cases, a 2015 drug investigation in California, prosecutors got a court order compelling Google to provide assistance in getting data from an Alcatel cellphone and a Kyocera cellphone, both of which were using Google's Android operating system, according to court records.

The ACLU found Google was also the subject of All Writs Act cases in Alabama, New Mexico, North Carolina, North Dakota, Oregon and South Dakota.

Some records show judges signed court orders compelling Google to help investigators, though the records don't indicate whether Google complied. In one such case, a 2015 child pornography investigation in Sacramento, Calif., Google was ordered to reset the password of a Samsung telephone so investigators could search its contents. Other court dockets are unclear as to the outcome of the prosecutors' request.

The technical issues are different for Alphabet Inc.'s Google than for Apple, partly because Google makes the Android cellphone operating system, but that system runs on phones manufactured by others, while Apple makes both phones and their operating software.

The Google cases involve investigations by the FBI, Secret Service, Homeland Security Department, Drug Enforcement Administration and Bureau of Land Management.

Apple's dispute with the Justice Department in the terrorism case centered on the work phone of Syed Rizwan Farook, who along with his wife killed 14 people and injured 22 others in a Dec. 2 attack on a holiday party of San Bernardino, Calif., county employees.

Just as the two sides were due to face off in court last week, federal officials said they found a new potential technique to get data from the phone without Apple's help. On Monday, the Justice Department said the method worked and it was dropping the case against Apple.

Los Angeles Times
FBI keeping hack tools under wraps
Thursday, 31 March 2016
Byline: Paresh Dave, David Pierson

Los Angeles - Even when courts compel law enforcement agencies to reveal the ways they hack into technology products, it's criminal suspects - - not the makers of hardware or software -- who are most likely to learn the details.
As Apple Inc. considers legal tactics that could force the FBI to share how it unlocked an iPhone belonging to one of the San Bernardino shooters, a federal court case in Washington illuminates how the judicial process can leave the tech world in the dark.

The case involves the Tor browser, which is popular among activists, dissidents, journalists -- and those who want to mask their identities when surfing online. The FBI hacked the browser as part of a sweeping child pornography investigation that led to 1,300 suspects.

In one of the cases, a judge has ordered that the FBI give defense attorneys details about the software flaw that allowed the FBI to identify suspect Jay Michaud of Vancouver, Wash., whose prosecution has

been at the forefront of the investigation. But prosecutors on Tuesday opposed the ruling in a heavily redacted document.

They say the defense already has enough information to analyze the operation. And former federal prosecutors say disclosing the vulnerability takes away the ability to use the technique to nab more offenders.

But technology developers and privacy activists fear that consumers' safety could be put at risk if the Tor issue turns out to be an unpatched bug.

The tension will manifest in "much more litigation to understand the techniques used to capture individuals," said Michael Zweiback, an attorney at Alston & Bird and former chief of the Justice Department's cybercrimes section.

The issue will not go away as the FBI's growing interest in probing the Internet for criminal activity will require using "techniques that are more proactive -- that are recognized exploits -- to get access to information," Zweiback said.

In the Washington case, federal agents briefly seized control of Playpen, a secretive online forum, accessible through Tor, where more than 214,000 members traded what authorities describe as sexually explicit photos and videos, including of children. The FBI learned the Internet protocol addresses of Playpen visitors by using a software bug linked to Tor to defeat the browser's security measures.

Public defenders for Michaud, who is charged with possession of child pornography, say they can't fully vet the legality of the FBI's investigation without knowing how the agency hacked Tor. While the government has turned over details about the software that identified his address, it hasn't shared information about how that tracking tool was introduced.

Prosecutors and experts say what matters is that the hack didn't tamper with Michaud's data.

"Getting through the lock doesn't matter, as long as the information on the other side of the door isn't affected," Zweiback said, comparing digital searches with physical ones.

Colin Fieman, an attorney for Michaud, told a judge in his case last month that the government's objections to revealing the vulnerability were "puzzling." The information wasn't classified or confidential, he said, according to a court transcript.

Law enforcement generally seeks to protect its hacking methods as long as possible because the techniques' usefulness shrinks when the public or manufacturers are aware, Zweiback said.

Fieman said only his technological expert would examine the hacking tool.

"We are not looking to circulate this stuff," he told the court. "We just need to look at it."

Last month, U.S. District Judge Robert Bryan ruled in Fieman and Michaud's favor. But prosecutors this week asked Bryan to reconsider, saying that the additional information wouldn't address the defense's concerns. Justice and FBI officials didn't have immediate comment.

Fieman in an email Wednesday said he disagreed with the government's assertion that law enforcement privilege "should trump a defendant's constitutional rights to an effective defense and fair trial."

Though his team may eventually gain access to details of the FBI method, Tor has little recourse. Suing the government to get the same information is unlikely to end well, legal experts said.

Kate Krauss, director of communications and public policy for the Cambridge, Mass.-based nonprofit that develops and operates the browser, said her colleagues suspect that the issue exploited by the FBI has been fixed, but they want to confirm that.

"We're watching with interest," Krauss said over a voice call on the encrypted chat app Signal. "We're the gold standard for online anonymity software, and we're committed to keeping the security stronger."

It's a desire shared by Apple too. Attorneys for the Cupertino, Calif., company say they plan to insist that the government explain how, with the help of an undisclosed outside group, investigators bypassed an iPhone 5c's security -- the same device authorities had maintained couldn't be opened without Apple's assistance.

Krauss said Tor, just like the tech industry at large, prefers that people who find vulnerabilities in products privately report them so they can be fixed before they are turned against users. But law enforcement and counter- terrorism agencies maintain a narrow set of bugs are better left untouched for investigative purposes.

Apple and Tor may never confirm the FBI's tactics. But the publicity around the two incidents could lead judges overseeing similar cases to ask more questions, said Robert Cattanach, a former Justice Department attorney who specializes in cybersecurity for the law firm Dorsey & Whitney.

"You have skeptical judges and criminal defense lawyers using San Bernardino to exploit ways to get under the FBI's skin if nothing else," Cattanach said. "Even the most neutral federal judge is going to give pause when the FBI makes representations."

Michael Vatis, a former official with the Justice Department and FBI, now a partner at Steptoe & Johnson, said any time that the FBI uses a technical vulnerability in a case, details of it are kept under seal. But Cattanach said there were instances, though rare, when the FBI revoked cases because it was

asked to share hacking methods, even just to defendants and their attorneys. He declined to provide details.

Attorneys said the question of when authorities must bare all is set to explode in significance. The FBI and police will need to rely increasingly on taking advantage of technical flaws to ferret out cybercriminals as tech companies introduce stronger security protections.

"There's been some frustration at the FBI that they're operating with one hand tied behind their back," Cattanach said. "They've since realized that if you're going to beat the bad guys at their own game, you've got to play the game."

But in improving capabilities, the FBI has turned into yet another security research group that tech firms want to learn from.

"There is a great deal of irony ... that the FBI is being asked to reveal their work now" in the Michaud case, Vatis said.

Los Angeles Times
FBI may keep its hacking secret
Thursday, 31 March 2016
Byline: Richard Winton, James Queally

Los Angeles - The successful hack of a phone linked to the San Bernardino terror attacks is unlikely to help police win greater access to encrypted data in thousands of smartphones sitting in evidence lockers nationwide, legal experts and law enforcement officials say.
The process used to gain access to Syed Rizwan Farook's iPhone 5c might not work on other devices, according to an FBI official with knowledge of the investigation.

Though the FBI might want to use the new tool to help solve other criminal cases, doing so would also make the process subject to discovery during criminal trials and place the information in the public domain, according to the official, who was not authorized to discuss the case and spoke on the condition of anonymity.

Any application of the method used to access Farook's phone would probably be limited to investigations that are unlikely to result in criminal cases, the official said.

"A technical option developed for a particular computing device may not work on other devices," the FBI official said. "The effectiveness of these lawful methods may be limited by time and resources, and may lack the scalability to be a viable option for most investigations."

On Wednesday, an Arkansas prosecutor said the FBI has agreed to help his office gain access to an iPhone 6 and an iPod that might hold evidence in a murder trial. It was not clear if the FBI would employ the method it used to access Farook's phone.

News that the FBI found a way into Farook's phone Monday thrilled police, who have long complained that encrypted data represents a major roadblock to routine police investigations. Thousands of smartphones sit in police evidence lockers across the country. At least 400 locked devices are in the possession of the Los Angeles Police Department and the L.A. County Sheriff's Department.

But as it became clear that the FBI's success in the San Bernardino case wouldn't translate to broader access for law enforcement, officials once again called on Congress to settle the issue.

"We cannot ask crime victims across 3,000 local jurisdictions to stake their hope for justice on an unending technological arms race between the government and Apple," Manhattan Dist. Atty. Cyrus Vance Jr., one of the leading national voices decrying encryption, said in a statement issued Tuesday. "The ongoing public safety challenge posed by warrant-proof encryption demands a comprehensive, legislative solution."

Terrence Cunningham, the police chief in Wellesley, Mass., and president of the International Assn. of Chiefs of Police, said he respects the FBI's position but warned that criminals will continue to use encryption to deflect police investigations until a legislative solution is presented.

"The concern is that today's technology provides criminals with powerful new tools that keep police from protecting the public," he said. "Data that rests in emails, text messages, photos and videos stored on mobile devices can help to locate a suspect or a victim, and in some cases, save lives. Law enforcement's mission is to keep the public safe and to protect communities, and collecting digital evidence from criminals and terrorists will help us do that."

Federal investigators have offered few details about how they gained access to Farook's phone. The iPhone 5c was at the center of a court battle between the FBI and Apple, which led to a court order that Apple create software that would allow the FBI to access encrypted data on the device.

Farook disabled the phone's iCloud backup feature six weeks before the Dec. 2 attack, according to court filings. He had also enabled an auto- erase feature that would permanently destroy all data on the phone after 10 consecutive failed attempts to enter the device's password.

A third party provided the FBI with a way to disable the password entry limit, according to another law enforcement official with knowledge of the investigation who was not authorized to discuss the case and spoke on the condition of anonymity.

Internal government policy might limit what, if anything, the FBI could share about the method used to hack Farook's phone, said Andrew Crocker, a staff attorney with the Electronic Frontier Foundation, a digital rights advocacy group.

If the government exploited a flaw in Apple's security measures, it could be required to disclose that information to Apple under the Vulnerabilities Equities Process, Crocker said. The policy is weighted toward disclosure, but the government has successfully fought to keep such details secret before.

Government agencies are allowed to share information about digital security flaws with one another, he said. But if the government chose not to share that information with Apple, it could also conceivably be barred from telling police agencies about the process used to unlock Farook's phone.

"They certainly can share it within the federal government without disclosing it to Apple," Crocker said. "The way I read the policy, sharing it with local police would be a dissemination outside the government."

In the Arkansas case, Cody Hiland, prosecuting attorney for the state's 20th Judicial District, said the FBI's Little Rock field office had agreed to help prosecutors gain access to a pair of locked devices linked to suspects in the slayings of Robert and Patricia Cogdell.

Calls to the FBI's Little Rock field office were not immediately returned. An FBI spokesman in Washington, D.C., declined to comment.

Attorneys for Apple are researching legal tactics to compel the government to tell the company what, if any, flaws it exploited in gaining access to Farook's phone. But most experts believe the FBI has no obligation to comply. The FBI could also argue that the most crucial information is part of a nondisclosure agreement, solely in the hands of the outside party that assisted the agency, or cannot be released until the investigation is complete.

Though the debate over Farook's phone did not land in criminal court, the fight between law enforcement and Silicon Valley over access to encrypted data is far from over. The FBI may have claimed a victory this week, but some police leaders fear it won't take long for Apple or another company to build tougher encryption methods.

"If the FBI did in fact find some type of a flaw that they were able to exploit, clearly the industry is going to say, 'We've got to find a way to plug that hole,'" Cunningham said.

Jerusalem Post
Twitter diplomacy conference opens in Tel Aviv
Thursday, 31 March 2016
Byline: Herb Keinon

Tel Aviv - Tweeting diplomatic messages and using Facebook as a communications tool during crisis situations are among the topics being discussed in Tel Aviv at a two-day first-of-itskind conference on digital diplomacy.
The conference, which opened Wednesday, is jointly hosted by the Foreign Ministry and the Partner Institute for Internet Studies at Tel Aviv University.

It is bringing together some 50 diplomats and scholars from 25 countries to look at how states are using digital platforms as a diplomatic tool.

The conference is dealing with a number of issues that are arising as a result of the use of social media by foreign ministries around the world, including the need to train diplomats in social media engagement, ways to evaluate the impact, and the intersect between digital diplomacy, public diplomacy and nation branding.

Noam Katz, head of the ministry's public diplomacy division, is scheduled to deliver a talk Thursday on how Israel engages with the Arab world through social media.

According to the ministry, governments are increasingly using social media as a diplomatic tool, with some 400 heads of states and governments active on Twitter.

Foreign Ministry spokesman Alon Lavi said that the ministry sees digital diplomacy as an important diplomatic tool, "certainly in light of the challenges we face." He said that Israel is able through social media to expose many people to its messages whom Jerusalem would otherwise be unable to reach.

Khaleej Times
'50% of GCC organisations can't predict, prevent cyber attacks'
Thursday, 31 March 2016
Byline: Sandhya D'Mello

Dubai - Gulf Business Machines, or GBM, the region's number one provider of IT solutions, has revealed that nearly 50 per cent of GCC executives lack confidence in their organisations in having the right tools to predict and prevent cyber attacks.
The statistic is part of GBM's latest security survey, which was unveiled at Gulf Information Security Expo and Conference (GISEC) 2016. The annual GBM Security Study, now in its fifth year, polled over 700 executives and IT professionals based in the UAE, Qatar, Oman, Bahrain and Kuwait.

Corporate investment in IT security is a major focus of the GBM survey, and despite internal and external threats to organisations, 71 per cent of executives confirmed that their IT security budgets will either stay the same or decrease in 2016.

In response to whether their organisations hire external consultants to help guard against cyber threats, 48 per cent of respondents said that their organisations conduct regular third-party security assessments, while 40 per cent of organisations have a dedicated IT governance, risk and compliance function.

Discussing the security survey at GISEC, Hani Nofal, Vice President of Networks, Security and Mobility said: "Security is no longer strictly an IT function but companies across the region increasingly understand that this is a boardroom and organizational conversation."

Asharq Al-Awsat
Saudi Censorship to Monitor Cyber-Attacks on Government Bodies
Thursday, 31 March 2016
Byline: Fatah Al-Rahman Youssef

Riyadh - A Saudi official has revealed that there is a continuous censorship and follow up to track any attempt for cyber attacking government and private installations, including terrorist actions and money laundering.
The official explained that there are specialized committees in the country to review these cases and protect information security in the Kingdom.

Prince Dr Turki bin Saud bin Mohammed, President of King Abdulaziz City for Science and Technology (KACST) talked during a press conference following the inauguration of the Third Saudi International Conference on Information Technology entitled "Cyber Security", which was organized by KACST at its headquarters in Riyadh, under the patronage of the Custodian of the Two Holy Mosques King Salman bin Abdulaziz Al Saud.

Dr Turki bin Saud explained that his country is fully alert to save its security information from hackers and pointed out that Saudi Arabia has assigned specialized bodies to watch suspicious activities, including terrorist acts and money laundering.

The prince called the private sector to invest in the fields of information and electronic securities, be updated, and submit challenges, problems and review solutions to solve them and contribute to developing the information security field.

Dr Turki said that the cost of losses due to cyber- attacks per year was estimated at $ 445 billion globally, and the damage bill of such attacks is expected to rise in the future as a result of the expansion of electronic services and the entry of new technology concepts.

He also reinforced the need to develop scientific research efforts in the field of information security in support of national interests through the transfer and localization of technology, building capabilities and innovation of national algorithms that can be used safely to protect data.

Moreover, the KACST President said that the City has worked and is still working in cooperation with the relevant authorities on the transfer and localization of the latest technologies of the Kingdom through the establishment of a sophisticated infrastructure and national capability-building in many scientific fields.

These fields include the transfer of those related to information technology in general and cyber security technology in particular, emanating from the leadership's interest in scientific research and technical development in various fields for their important role in development and its sustainability.

Moreover, Dr Turki pointed out that KACST has built a supportive integrated environment for the transfer and development of technologies related to information security through the establishment of the National Center for Information Security Technology and implementation of applied research in the field of information security in partnership with a number of distinguished universities and research centers around the world, as well as the preparation of qualified and national capabilities on research and development in this area.

The conference targeted staff and students from higher education institutions and encouraged attendance of managers and officials of public and private sectors within and outside the Kingdom, who are interested in electronic security management, the authors of the regulations and policies for information security and its innovation, besides local and international experts and researchers in the field of information security technology.

The National (UAE)
Online 'activists' a threat to Middle East security
Thursday, 31 March 2016
Byline: Caline Malek

Dubai - The most prevalent cyber criminals in the Middle East are not online thieves out to pilfer your bank account, but "activists", according to a new report by a UK-based defence, security and aerospace company.
These individuals and groups take their political, religious or social causes to the internet, setting out to harm reputations, steal data or target infrastructure, said Dr Adrian Nish, head of threat intelligence at BAE Systems Applied Intelligence.

"There are many tensions in the Middle East, many communities who are very active, scoring political blows against each other," he said.

"And to some extent, it does not seem like such a significant threat but then you do get nation state-backed actors using those personas to steal information and maybe publish it, and pretend to be an activist. "We've seen many cases of this happening in the Middle East."

While these crimes, he said, were much more at the nation-state angle than corporate, there were also cyber criminals targeting Middle Eastern businesses, "trying to defraud people out of large sums of money as well", Dr Nish said during a meeting on demystifying cybercriminals at the Fairmont Hotel in Dubai on Wednesday. Cyber crime is a massive industry with so many ways for criminals to cause havoc, he said.

There are those who run phone support scams, those who write software for other cyber criminals or launder the ill-gotten gains or help prop up the cybercrime supply chain in other ways. There are also non-state actors who work for governments to steal valuable data or intelligence to create international incidents.

Cyber crime was the second most-reported economic crime, and one that affected 30 per cent of organisations, in the Middle East, the report said.

"Threats are evolving, and governments and businesses have an urgent requirement to comply with increasing regulation," said Bulent Teksoz, global cyber security strategist at BAE Systems Applied Intelligence. Warfare, he said, does not look like it used to.

"Battles would take place in the air, on land or in the sea but the battlefield has now extended to cyber space," he said. "Borders mean nothing.

"This interconnected world leaves organisations vulnerable to threats. "You have to know your enemy to defend yourself."

He said that Middle East governments did recognise the scale of the threat and were taking precautions to defend their countries. "Governments are doing well on educating end-users," he said.

Matthew Cochran, chairman of the Defence Services Marketing Council in Abu Dhabi, said 'hacktivism' was dangerous if not controlled and approved by the government.

"If a 'hacktivist' is not appropriately audited by cyber security supervisors and cleared by the respective government cyber command authorities then a slippery slope of private individuals with an enormous amount of sensitive documents and data can endanger both the public and government alike globally," he said.

Reuters
FBI's secret method of unlocking iPhone may never reach Apple
Thursday, 31 March 2016
Byline: Staff report

Washington - The FBI may be allowed to withhold information about how it broke into an iPhone belonging to a gunman in the December San Bernardino shootings, despite a U.S. government policy of disclosing technology security flaws discovered by federal agencies.
Under the U.S. vulnerabilities equities process, the government is supposed to err in favor of disclosing security issues so companies can devise fixes to protect data. The policy has exceptions for law enforcement, and there are no hard rules about when and how it must be applied.

Apple Inc has said it would like the government to share how it cracked the iPhone security protections. But the Federal Bureau of Investigation, which has been frustrated by its inability to access data on encrypted phones belonging to criminal suspects, might prefer to keep secret the technique it used to gain access to gunman Syed Farook's phone.

The referee is likely to be a White House group formed during the Obama administration to review computer security flaws discovered by federal agencies and decide whether they should be disclosed.

Experts said government policy on such reviews was not clear-cut, so it was hard to predict whether a review would be required. "There are no hard and fast rules," said White House cybersecurity coordinator Michael Daniel, in a 2014 blog post about the process.

If a review is conducted, many security researchers expect that the White House group will not require the FBI to disclose the vulnerability it exploited.

Some experts said the FBI might be able to avoid a review entirely if, for instance, it got past the phone's encryption using a contractor's proprietary technology.

Explaining the policy in 2014, the Office of the Director of National Security said the government should disclose vulnerabilities "unless there is a clear national security or law enforcement need."

The interagency review process also considers whether others are likely to find the vulnerability. It tends to focus on flaws in major networks and software, rather than individual devices.

During a press call, a senior Justice Department official declined to disclose whether the method used on Farook's phone would work on other phones or would be shared with state and local law enforcement.

Apple declined to comment beyond saying it would like the government to provide information about the technique used.

PROTECTING "CRUCIAL INTELLIGENCE"

The government reorganized the review process roughly two years ago and has not disclosed which agencies regularly participate other than the Department of Homeland Security and at least one

intelligence agency. A National Security Council spokesman did not respond to a request for comment about agency participation.

In his April 2014 blog post, White House cybersecurity coordinator Daniel, who chairs the review group, said secrecy was sometimes justified.

"Disclosing a vulnerability can mean that we forego an opportunity to collect crucial intelligence that could thwart a terrorist attack stop the theft of our nation's intellectual property," Daniel wrote.

On Tuesday, a senior administration official said the vulnerability review process generally applies to flaws detected by any federal agency.

Paul Rosenzweig, a former deputy assistant secretary at the Department of Homeland Security, said he would be "shocked" if the Apple vulnerability is not considered by the group.

"I can't imagine that on one of this significance that the FBI, even if it tried to, would succeed in avoiding the review process," said Rosenzweig, founder of Red Branch Consulting, a homeland security consulting firm.

He predicted the FBI would not be forced to disclose the vulnerability because it appears to require physical possession of a targeted phone and therefore poses minimal threat to Internet security more broadly.

Many security researchers have suggested that the phone's content was probably retrieved after mirroring the device's storage chip to allow data duplication onto other chips, effectively bypassing limitations on the number of passcode guesses.

Kevin Bankston, director of the think tank Open Technology Institute, said there is no public documentation of how the review process has worked in recent years. He said Congress should consider legislation to codify and clarify the rules.

Stewart Baker, former general counsel of the NSA and now a lawyer with Steptoe & Johnson, said the review process could be complicated if the cracking method is considered proprietary by the third party that assisted the FBI.

Several security researchers have pointed to the Israel-based mobile forensics firm Cellebrite as the likely third party that helped the FBI. That company has repeatedly declined comment.

If the FBI is not required to disclose information about the vulnerability, Apple might still have a way to pursue details about the iPhone hack.

The Justice Department has asked a New York court to force Apple to unlock an iPhone related to a drug investigation. If the government continues to pursue that case, the technology company could potentially use legal discovery to force the FBI to reveal what technique it used, a source familiar with the situation told Reuters.

At least one expert thinks a government review could require disclosure. Peter Swire, a professor of law at the Georgia Institute of Technology who served on the presidential intelligence review group that recommended the administration disclose most flaws, said there is "a strong case" for informing Apple about the vulnerability under the announced guidelines.

"The process emphasizes the importance of defense for widely used, commercial software," he said.

The Register (UK)
Former FBI spy hunter: Don't trust China on 'no hack' pact
Wednesday, 30 March 2016
Byline: John Leyden

London - A former FBI investigator who helped expose Soviet double agent Robert Hanssen warns that enterprises should give up worrying about hackers, "who are now the good guys", and be more worried about spies.
Veteran spy hunter turned infosec exec Eric O'Neill said that espionage has evolved and become increasingly digital as hackers have become key in exposing security bugs through bug bounties and the like. The evolution of the threat landscape has happened without corporate security mindsets catching up, he says.

Too many enterprises continue to think that they aren't important enough to become a target for cyber-espionage from so- called APT groups but this mindset is wrong and needs to change, according to O'Neill, who argues that reconnaissance followed by spear-phishing or other social engineering attacks has become the go-to spying method of the 21st century. Much of this is targeted towards industrial espionage with China and (to a much smaller extent) Russia primarily to blame, he says.

O'Neill, the national security strategist for endpoint security firm Carbon Black, described last year's China-US "no hack pact" as a "joke".

"I don't believe there's anyone in the US government [who] thought China would stop spying," O'Neill said.

"Chinese firms don't invest in research and development. They're not interested in innovation themselves," he claimed.

O'Neill claims China is playing the long game with hacks against American health insurer Anthem and the US government's Office of Personnel Management last year. China has said the attacks were carried out by China- based criminals rather than state-sponsored hackers. But O'Neill insists that both breaches were about long-term intelligence gathering and perhaps ultimately aimed towards cultivating insiders as assets rather than the theft of trade secrets. Real world examples of the latter are not hard to find.

O'Neill cited the case of a Chinese spy convicted of stealing trade secrets from Motorola as well as the recent case of a Chinese man convicted of stealing military aircraft secrets from Boeing.

The attack against US retailer Target, which relied on breaching its systems and stealing credit card data after first hacking into its heating and ventilation contractor, is also more a case of espionage rather than a "conventional" hack, according to O'Neill.

"You need the right mindset and extraordinary efforts to prevent loss," O'Neill said. "Attackers are spending more time and energy on more sophisticated attacks."

The bad guys are not playing by the rules. This is a particular problem because security as a whole is too reactive and slow to adapt. "We need to do a better job at protecting ourselves," O'Neil concluded.

O'Neil served five years in the FBI prior to leaving just before 9/11 ("I'd probably still be at the agency if I hadn't left beforehand," he said) to work as a lawyer before moving to a security consultancy. In his new role at Carbon Black, O'Neil will be focusing on raising awareness of cybersecurity within governments, helping to shape policies around national security.

Yonhap News Agency
S. Korea restarts project to launch 5 military satellites
Thursday, 31 March 2016

South Korea plans to kick start a program to send five satellites into orbit by 2022 which will allow the military to keep close tabs on North Korea, defense officials said Thursday.
The project, dubbed "425 project," has been stalled for a year amid budget limitations, with the National Assembly allocating only 2 billion won (US$1.7 million) in the 2016 budget out of 64.3 billion won requested by the defense ministry.

"The ministry has set its sights on reaching a contract within the latter half of this year," a defense official said. "The timing of the project's kickoff has been delayed by one year ... but we will follow through with the goal to complete the project within the target date," he noted.

Under the project, the military plans to launch five reconnaissance satellites by 2022 that have onboard cameras capable of taking clear images of an object on the Earth's surface with a diameter of 0.3-0.5 meters.

Four of satellites will also be equipped with all-weather synthetic aperture radar, while one will carry electronic optics and infrared surveillance equipment.

With the new satellites, South Korea would be able to detect all launch preparations or other military activities by North Korea, including those involving mobile transport erector launchers, within two to three hours.

Globe and Mail
Ottawa's big IT project still struggling
Monday, 04 April 2016
Byline: Barrie Mckenna

It was a seductively simple idea.
Take the maze of federal government databases, e-mail systems and computer networks, and put them under one departmental roof. More than 60 e-mail systems would become one, 500plus databases would be merged into seven, and thousands of tech workers from dozens of departments would go to work for a single agency, Shared Services Canada.

The two Conservative ministers in charge at the time - former public works minister Rona Ambrose (now interim Conservative leader) and treasury board president Tony Clement - were bursting with optimism when they announced the project five years ago. They promised the consolidation would save piles of money (up to $400-million a year), wipe out duplication and enhance cybersecurity.

"This is a whole new way of doing business for the government," Mr. Clement vowed.

Not so much. It's turned into an old and very familiar story of how Ottawa works. Years and billions of dollars later, virtually none of the wondrous benefits have come to pass.

And in last week's budget, the new Liberal government quietly gave Shared Services a $384-million infusion over two years to its roughly $1.9-billion annual budget - apparently, to keep creaky old government computer systems from crashing. The agency will get another $75-million to strengthen security.

But this isn't just an inside-Ottawa tale of serial bungling. There are disturbing real-world consequences of the government's failure to fix chronic information technology (IT) problems. Websites periodically crash and go offline, sometimes for days, because of continuing database problems.

A 2014 cyberattack by Chinese hackers on the National Research Council's network paralyzed much of its research work for nearly a year. Also in 2014, emergency workers in Saskatchewan lost voice communications for nearly an hour owing to a mix-up between Shared Services and the RCMP.

Not only is Ottawa not saving money, it's spending more and getting less than it needs in the way of IT. Much of the promised consolidation remains a work in progress, with no clear end-date in sight.

The merging of e-mail systems, outsourced to Bell Canada and CGI Group, is already more than a year behind schedule. Fewer than one in five government workers is using new Canada.ca addresses.

Efforts to move more than 15,000 computer applications onto three new centralized databases in Gatineau, Que., Barrie, Ont., and at Canadian Forces Base Borden, north of Toronto, are running late.

Fewer than 10 per cent of government apps have been shifted over to Shared Services. And an $18-million project aimed at making it easier for users to sort through Statistics Canada data is also badly behind schedule.

Auditor-General Michael Ferguson issued a scathing report in February, outlining Shared Services' mounting problems and its inability to deliver results. "They have big problems ahead of themselves," Mr. Ferguson told reporters bluntly.

The view of the new Liberal government is that Shared Services was set up to fail by the Conservatives. The agency was hit with severe budget cuts soon after its creation, leaving it starved of the resources it needed.

The question now is can the new government make it right? A key issue is sorting out what information technology the government should develop in-house, and what it should buy off the shelf. In a postbudget brief, Canadian Advanced Technology Alliance president John Reid lamented that "despite longstanding good intentions, the [government's] procurement model has not modernized to keep up with industry changes and standards. It is not fully aligned with the digital era."

It's a missed opportunity to spur innovation, according to CATA. Too often, Ottawa winds up overpaying for inferior IT, while crowding out the private sector by building custom systems rather than buying commercial offerings and spurring the emergence of promising technology exports.

The government "has no export sales. ... No intellectual property gets created that is patentable," the group laments.

Of course, CATA, which speaks for Canadian tech companies, has an interest in seeing some of that business flow to its members.

But given recent experience, it's hard to imagine Ottawa could do worse. Surely there is a better way for Ottawa to acquire the technology it needs to do its work.

La Presse
La surveillance demasse menacerait la diversité d'opinions
Saturday, 02 April 2016
Byline: Marc Thibodeau

La surveillance de masse des communications en ligne pousse nombre d'internautes à s'autocensurer, y compris ceux qui affirment «n'avoir rien à cacher», et limite la diversité d'opinions à un degré préoccupant.

Le constat figure dans une nouvelle étude parue dans la revue Journalism & Mass Communication Quartely qui sonne l'alarme quant à l'impact potentiellement néfaste sur la liberté d'expression de pratiques mises en lumière aux États- Unis par Edward Snowden.

L'ancien consultant de la National Security Agency (NSA) avait notamment affirmé en 2013, documents à l'appui, que l'influent service de renseignements était en mesure d'accéder au contenu des serveurs de géants de la Silicon Valley comme Google, Facebook et Yahoo!.

Les firmes désignées ont démenti toute collaboration sans pour autant convaincre la population américaine, qui demeure très partagée quant à l'utilisation de programmes de surveillance à grande échelle par le gouvernement pour lutter contre le terrorisme.

Étude

Pour évaluer leur impact sur le comportement des internautes, une chercheuse de la Wayne State University, au Michigan, a demandé à un groupe de 250 personnes de réagir à une nouvelle fictive portant sur l'engagement des États-Unis contre le groupe armé État islamique.

Les répondants devaient préciser à quel point ils étaient à l'aise avec l'idée de commenter publiquement la nouvelle sur Facebook, dire ce qu'ils estiment être la position de la majorité des Américains à ce sujet et donner leur appréciation des programmes de surveillance de masse.

La moitié des personnes recrutées pour l'exercice se voyaient rappeler qu'il était important de garder en tête que la NSA «surveille les activités en ligne de citoyens».

Dans la vaste majorité des cas, écrit la chercheuse responsable, Elizabeth Stoycheff, les participants ayant été sensibilisés par le message sur la NSA se montraient beaucoup moins disposés à exprimer leur opinion s'ils avaient l'impression qu'elle n'était pas conforme à celle de la majorité.

Ceux qui étaient les plus susceptibles d'adopter un comportement conformiste sont ceux qui soutenaient le plus les programmes de surveillance.

«Ces individus prétendent que la surveillance est nécessaire pour assurer la sécurité nationale et qu'ils n'ont rien à cacher. Toutefois, quand ces individus ont l'impression qu'ils sont surveillés, ils modifient volontairement leur comportement - exprimant leurs opinions quand ils sont en phase avec la majorité et les taisant dans le cas contraire», relève l'auteur.

Seules les personnes qui étaient très critiques à l'endroit des programmes de surveillance semblaient disposées à exprimer leur opinion sans réserve, qu'ils soient ou non en phase avec la majorité.

Des études antérieures ont démontré que les usagers des réseaux sociaux sont moins susceptibles de s'exprimer librement sur un sujet s'ils ont l'impression d'être minoritaires, en partie de crainte de se retrouver isolés.

L'effet «modérateur» découlant de la crainte d'un programme de surveillance constitue un autre facteur que les autorités devraient examiner attentivement alors qu'ils statuent sur l'utilité et la légitimité de programmes de surveillance de masse, souligne Mme Stoycheff.

Programme révisé

La polémique suscitée par les révélations d'Edward Snowden a notamment poussé le Congrès américain à réviser un programme de collecte de métadonnées qui permettait à la NSA d'accumuler des renseignements sur l'ensemble des clients de Verizon.

Les élus ont cependant «traîné les pieds» avant d'interrompre cette pratique et tardent à adopter les réformes requises pour protéger adéquatement les données des internautes contre des intrusions abusives, juge l'Electronic Frontier Foundation (EFF) dans un récent rapport.

L'organisation de défense des droits des internautes salue parallèlement les efforts des géants de l'internet, relevant qu'ils ont, dans la majorité des cas, adopté des politiques beaucoup plus restrictives à ce sujet au cours des dernières années.

Les normes de l'industrie en la matière ont sensiblement évolué, mais il reste encore beaucoup à faire, prévient l'EFF.

Washington Post
Hackers find soft spot in hospitals
Sunday, 03 April 2016
Byline: Carolyn Y. Johnson and Matt Zapotosky

The cyberattack on MedStar Health - one of the biggest health-care systems in the Washington region - is a foreboding sign that an industry racing to digitize patient records and services faces a new kind of security threat that it is ill-prepared to handle, security experts and hospital officials say.
For years, hospitals and the health-care industry have focused on keeping patient data from falling into the wrong hands. But the recent attacks on MedStar's network and other hospitals across the country highlight an even more frightening downside of security breaches: As hospitals have become dependent on electronic systems to coordinate care, communicate critical health data and avoid medication errors, patients' well-being may also be at stake when hackers strike.

Hospitals are used to chasing the latest medical innovations, but they are rapidly learning that caring for sick people also means protecting medical records and technology systems from hackers. An industry

that has traditionally spent a small fraction of its budget on cyberdefense is finding that it also must teach doctors and nurses not to click on suspicious online links and shore up its technical systems against hackers armed with an ever-evolving set of tools.

In some ways, health care is an easy target: Its security systems tend to be less mature than those of other industries, such as banking and tech, and its doctors and nurses depend on data to perform time-sensitive, lifesaving work. Where a financial-services firm might spend a third of its budget on information technology, hospitals spend only about 2 to 3 percent, said John Halamka, the chief information officer of Beth Israel Deaconess Medical Center in Boston.

"If you're a hacker . . . would you go to Fidelity or an underfunded hospital?" Halamka said. "You're going to go where the money is and the safe is easiest to open."

The stakes are extraordinarily high. Hospitals' electronic systems are often in place to help prevent errors. Without computer systems, pharmacists cannot easily review patients' lab results, look up what other medications the patients are on or figure out what allergies they might have before dispensing medications. And nurses administering drugs cannot scan the medicines and the patients' wristbands as a last check that they are giving the correct treatments. When lab results exist only on a piece of paper in a patient's file, it is possible they could be accidentally removed by a busy doctor or nurse - and critical information could simply disappear.

In MedStar's case, a virus early this week infiltrated its computer systems, forcing the health-care giant to shut down its entire network, turn away patients, postpone surgeries and resort to paper records.

"One thing I think is becoming clear, especially over the last few weeks or months, is that health care is rapidly becoming a target for this," said Daniel Nigrin, chief information officer of Boston Children's Hospital, whose network came under attack by the hacker collective Anonymous in April 2014. "What struck us at that point was, you know what? These attacks can do a lot more than get your data; they can really disrupt the day-to-day operations of your facilities."

Although a handful of hospitals nationwide have been victims of cyberattacks in recent weeks, the MedStar security breach shows hackers' increasing boldness and sophistication. The chain is one of biggest employers in the Baltimore-Washington region and runs 10 hospitals as well as 250 clinics and other sites. MedStar spokeswoman Ann Nickels declined to elaborate on what sort of software attack the hospital suffered, but several employees have said they saw a pop-up message suggesting that it was "ransomware" - software that can lock people out of systems until they make a bitcoin payment. According to a photo of the pop-up message provided by a MedStar Southern Maryland Hospital Center employee, the hackers were demanding 45 bitcoins - equivalent to about $19,000 - to restore access to MedStar's system.

"You just have 10 days to send us the Bitcoin," the note read. "After 10 days we will remove your private key and it's impossible to recover your files."

Nickels said MedStar saw "no indication that data has left our system" or that patient privacy had been compromised. In a statement, the health-care system said it had not paid any type of ransom. A Friday-afternoon update from the hospital said MedStar was "approaching 90 percent functionality" of its systems.

Ransomware is not new, but cybersecurity experts and FBI data say its use is on the rise. Hospitals, of course, are not the only institutions facing such attacks. In nine months in 2014, the FBI received 1,838 complaints about ransomware, and it estimates that victims lost more than $23.7 million. The next year, the bureau received 2,453 complaints, and victims lost $24.1 million. The FBI does not condone the paying of ransoms, but its agents acknowledge that businesses are often left with a tough choice.

Hospitals, in particular, are vulnerable. In the weeks before the attack on MedStar, hackers hit Hollywood Presbyterian Medical Center in Los Angeles, extorting $17,000 in bitcoins, and Kentucky-based Methodist Hospital, which declared a state of emergency after an attack. Two Southern California hospitals, part of Prime Healthcare Services, were attacked in March.

Justin Harvey, the chief security officer of Fidelis Cybersecurity, said the hackers' success is likely to make them bolder, and he worries about critical infrastructure in the United States.

"I can't comment on whether the [Federal Aviation Administration] and all the power grids are up to snuff," he said. "If they're not, it can create a big problem."

Craig Williams, security outreach manager at Talos, the cybersecurity research group of Cisco, said the use of ransomware has exploded because it yields good profit margins. He estimated that it is a $100 million-a-year business.

"The malware industry is making giant steps toward ransomware, and really, the reason behind this is ransomware's profit margin simply exceeds that of other types of criminal activity," Williams said.

The way hackers get into a system is generally through a phishing attack - persuading an unsuspecting employee to click on a link or an attachment in an email - or by finding a network vulnerability.

That leaves hospitals with two challenges: designing systems that can resist attack and training employees.

On the network side, Williams said health-care companies - or any companies - that do not have full-time security specialists may not be keeping up with the latest problems and patches. He noted that one strain of ransomware exploits a well-known vulnerability in networks, and when his team did a scan of the Internet this week, it found 2.1 million servers that would be susceptible to such an attack.

The cultural problem may be even harder to solve.

"You're as vulnerable as your most gullible employee," Halamka said.

At Beth Israel, the hospital has printed up stickers that appear on salad containers and cookie packaging in the cafeteria so that people are reminded, even when eating lunch, not to click on links in emails they did not expect to receive. The hospital also has conducted internal phishing campaigns - sending fake emails to employees to assess where risks exist and to see whether extra cybersecurity training is needed.

Experts said the recent attacks seem to be based in Eastern Europe, although it is hard to tell whether one group alone is responsible. The hacks have similarities, to be sure, but hackers trade tools and information. One concern is that as the attacks gain coverage, they will inspire more copycats who will use the same technique to target other vulnerable networks.

"This thing is an industry, the black market that does this type of activity," said Chris Ensey, chief operating officer at Dunbar Security Solutions.

The details of MedStar's particular case - including what particular version of ransomware might have been used and how it got into the system - remain murky. An FBI spokesman declined to provide any details - including on the type of possible ransomware - other than to say the bureau was "aware of the incident and is looking into the nature and scope of the matter."

The Sun (UK)
Google removes Taliban propaganda app from its stores after it was used to spread hate speech
Monday, 04 April 2016
Byline: Fionn Hargreaves

AN app developed by the Taliban has been taken down from Google's Play Store for breaking the tech giant's rules on hate speech. The hate- filled app, "Pashto Afghan News - alemarah" ran news and videos from the extremist group.
Pashto is one of the two official languages of Afghanistan and Alemarah is the name of the Taliban's propaganda arm.

US group SITE Intel, who moniter jihadist activity online, discovered the app on Friday.

It was taken down on Saturday.

The app is thought to have been removed for inciting hate speech.

Google's rules state: "We don't allow apps that advocate against groups of people based on their race or ethnic origin, religion, disability, gender, age, nationality, veteran status, sexual orientation, or gender identity".

A Google spokesman said: "While we don't comment on specific apps, our policies are designed to provide a great experience for users and developers. That's why we remove apps from Google Play that violate those policies."

READ MORE:

'My kids can't even see your face. Are you a man or a woman?' Muslim in a veil posts footage of furious row with 'Islamophobic shopper' who called her 'Batman'

'A contrived set- up': Peru Two drugs mule under fire for having 'X Factor look' and being insincere in first TV interview since release

NHS nurse blackmailed female colleague in sick revenge porn plot after she dumped him

The terrorist group aim to reconquer Afghanistan after being removed from power in 2001.

They want to bring back Sharia law, a conservative Islamic law, to the country.

Taliban spokesman Zabihullah Mujahed told Boomberg the app "is part of our advanced technological efforts to make more global audience"

But Mr Mujahed said that they were having technical difficulty with the app.

This is just one of many ways in which extremist groups are using the internet to spread their messages of hate.

The Taliban already run a website in five different languages as well as maintaining a Facebook and Twitter account.

Twitter are trying to fight ISIS's large presence on their social media site as staff have been suspending extremists' accounts.

It was estimated in 2015 that ISIS are running more than 46,000 Twitter accounts.

Wall Street Journal
Why iPhone Breach Is Good for Users

Monday, 04 April 2016
Byline: Christopher Mims
Section: column

There was only one way for the court battle between the Federal Bureau of Investigation and Apple Inc. over access to the data on a killer's phone could end well for everyday Americans. Luckily, the FBI achieved it.
With the help of outside hackers, whose identity remains a mystery, the FBI successfully circumvented Apple's much-touted security. In the process, the agency did exactly what defenders of encryption and digital privacy have advocated for some time. It is called "lawful hacking," which is another way to describe law enforcement exploiting weaknesses in a security process.

Advocates say lawful hacking is an alternative to, and preferable to, creating a new "backdoor" into the system. An author of a recent paper on the subject, Columbia University professor and cybersecurity expert Steven Bellovin, says "I don't have any problem with what the FBI did. The whole premise of lawful hacking is there are vulnerabilities."

Here is why that is a good thing: It makes software more secure. Bugs are often discovered by "white hat" hackers who share them with the software's creator so they can be patched, typically before the flaw is even disclosed. This isn't a purely benevolent system; it works because these hackers, or their employers at universities or cybersecurity companies, want the money from bug "bounties," or the publicity that comes with finding an exploit, and because everyone, including hackers, is vulnerable to undisclosed exploits.

This dynamic is so well-established that it played out quietly in the background as the FBI-Apple dispute raged. Researchers at Johns Hopkins University last month revealed a flaw in Apple's iMessage texting program that could have allowed law-enforcement agents or hackers to decrypt photos or videos attached to messages as they moved over the Internet. The researchers disclosed the bug to Apple, which devised a patch.

We also saw the process at work in 2014 with a bug called Heartbleed, which jeopardized the encryption scheme used on much of the Internet. The flaw was first reported by a researcher at Google; a fix was quickly devised and deployed by those responsible for the open-source code in which it was found.

In that case, the White House made an unprecedented disclosure about how the federal government decides whether or not to share a vulnerability with the companies responsible for fixing them. The National Security Agency, for example, has said it discloses 91% of the vulnerabilities it discovers, but probably only after it has used them for its own purposes. Officials said they decide whether to disclose a flaw by weighing factors including whether the vulnerability poses a threat to national security, the likelihood that someone else has found it, the value of the intelligence that could be gathered if it is used, and whether it can be patched.

Given the publicity around the iPhone dispute, Shane McGee, chief privacy officer of cybersecurity firm FireEye Inc., says it is now open season on Apple's iOS operating system among hackers, who are often driven by ego as much as lucre.

There is a big caveat in the Apple case, however. For now, at least, the FBI won't disclose the bug to Apple, which means Apple can't fix it. That is bad for Apple's privacy-focused brand and could be bad for users, since others who learn of the flaw could exploit it for nefarious purposes. We don't know how likely that is, because we don't know how the FBI gained access to the phone; its method could require physical access to a device, plus a lot of time and money, making other exploits less likely.

The FBI and Apple declined to comment.

Whatever happens with this bug, and this phone, the struggle between breaking into software and securing software will only intensify. As FireEye's Mr. McGee points out, Apple is already working to make the next version of iOS even more impenetrable by the government and Apple itself.

The possibility that Apple could create a device that it would be unable to breach even if ordered by a court must keep those in law enforcement awake at night. And yet we seem headed to a world in which even the most draconian edict couldn't force Apple to unravel the laws of mathematics at the heart of its own encryption.

In a world of ever-multiplying threats -- including multimillion-dollar bank heists carried out from a keyboard -- increased security is an unqualified win for all Apple users.

It won't necessarily come easily, however. Absent action from Congress -- which lawmakers have said is unlikely in a polarizing election year -- the battle between Apple and the FBI seems destined to continue ad infinitum. Which, paradoxically, is evidence that the system is working.

It may be in the nature of this dispute that it can never end. And that may be the only satisfactory "resolution" we can hope for.

New York Times
Technology Upgrades Get White House Out of the 20th Century
Monday, 04 April 2016
Byline: Michael D. Shear

Can you run the country with spotty Wi-Fi, computers that power on and off randomly and desktop speakerphones from Radio Shack, circa 1985?
It turns out you can. But it is not ideal, as President Obama's staff has discovered during the past seven years. Now, as Mr. Obama prepares to leave the White House early next year, one of his legacies will be the office information technology upgrade that his staff has finally begun.

Until very recently, West Wing aides were stuck in a sad and stunning state of technological inferiority: desktop computers from the last decade, black- and-white printers that could not do double-sided copies, aging BlackBerries (no iPhones), weak wireless Internet and desktop phones so old that few staff members knew how to program the speed-dial buttons.

On Air Force One, administration officials sent emails over an air-to-ground Internet connection that was often no better than dial-up modems from the mid- 1990s.

"We can't do this," recalled Anita Decker Breckenridge, the deputy chief of staff for operations at the White House, who has since worked with the Air Force to upgrade the president's plane to broadband speeds. "This is the Oval Office in the sky. Talk about a network that didn't work."

Part of the problem? Responsibility for White House technology has long been divvied up between four agencies, each with their own chief information officer: the National Security Council, the Executive Office of the President, the Secret Service and the White House Communications Agency. That led to a series of Band-Aid solutions over the years, as one agency or another has attempted piecemeal upgrades to White House gear.

It also led to comical moments. In 2014, when White House aides accompanying Mr. Obama on his summer vacation in Martha's Vineyard struggled with balky laptops as they tried to revise a presidential statement, they could not get on-the- road tech support from the White House Communications Agency because the agency's staff members were not authorized to log in to computers issued by the Executive Office of the President.

Ms. Breckenridge was inspired by Mr. Obama's development in 2015 of the United States Digital Service and its mission to upgrade the federal government beyond the White House. She was determined after her frustrations in Martha's Vineyard to fix the mess, and by March 2015 had hired David Recordon, who designed and maintained the office technology for Mark Zuckerberg and the other employees at Facebook, as the information technology guy for the White House complex.

"It was an interesting challenge and world for me," Mr. Recordon said.

One of his first tasks was trying to map the miles of Ethernet cables and phone wires inside the walls of 1600 Pennsylvania Avenue. The team of technicians eventually discovered and removed 13,000 pounds of abandoned cables that no longer served any purpose.

"They had been installed over the decades by different organizations using different standards, different techniques, from different eras," Mr. Recordon said. "They were finding these pipes that just had bundles of cable that had been cut off over the years, no longer used. So we just started pulling it out."

With the wiring fixed, Mr. Recordon started replacing computers (the new ones have fast, solid- state drives and modern processors) and color printers. The new phone system -- the first since the Clinton years -- is all digital, with built-in speakerphones and speed-dial buttons that can be changed online. Many White House aides now carry the most recent iPhones. Mr. Obama, however, still carries a specially modified, highly secure BlackBerry.

The Wi-Fi in the Roosevelt Room is finally strong enough to live-stream an event on Facebook, like White House aides did last week when Mr. Obama surprised former federal inmates whose sentences had been commuted. Forgotten passwords are no longer an irritant now that the White House has started requiring users to log on with a chip-enabled smart card and a pin code.

Mr. Recordon's team also designed a new web-based system for admitting visitors to the West Wing that can be managed securely from any computer, including ones outside the White House complex.

To be sure, some important West Wing technology was upgraded by the George W. Bush administration, which overhauled the Situation Room for the first time since the Kennedy administration and added modern communications gear. Joe Hagin, the deputy chief of staff for Mr. Bush, recalled having to replace the phones in the presidential limousine after Mr. Bush complained that he had not been able to make a single phone call from his motorcade over an entire weekend.

"He said to me, 'What the heck would happen if there were a true national emergency?' " Mr. Hagin recalled. That fear came true months later on Sept. 11, 2001, when communications glitches plagued the government and led to new equipment in Air Force One and the first BlackBerries in the White House.

Mr. Hagin's team also upgraded the Intel 486 computers and got rid of the slow and cumbersome Lotus Notes email system. But the speed of technological advancement has once again left the current White House behind.

"I'm very sympathetic to them," said Mr. Hagin, who commiserated with Ms. Breckenridge last year about the sorry state of White House technology.

Ms. Breckenridge said the White House has not had to request any additional money for the new upgrades, which have been paid for out of the existing technology budgets for the various agencies involved. In some cases, she said, they have saved money by eliminating duplications. The four agencies no longer negotiate their own contracts with cellphone companies and no longer buy duplicate copies of software licenses.

Ms. Breckenridge said she was hopeful that Mr. Obama will leave to his successor's staff a building that is more useful in the Facebook and Twitter era, or whatever comes next.

Mr. Hagin said he wished them well, but predicted it will not be easy. He recalled once discovering a basement room in the West Wing filled with telephone switching gear that technicians said could be replaced with a unit the size of a dorm-room refrigerator. But everyone was nervous about cutting the wires because no schematics or design guides existed anymore, he said.

Replacing the equipment took a full two years.

Jerusalem Post
Wikimedia Foundation holds its 'Hackathon' in Jerusalem
Sunday, 03 April 2016

The Start-Up Nation earned yet another colorful feather in its already well-ornamented cap on Sunday, after hosting the annual Wikimedia Foundation's Hackathon in Jerusalem.
The four-day event, which brought together more than 150 computer developers from 17 countries to enhance Wikipedia's user experience and ensure reliable data, concluded at the capital's Hansen House, a former leper hospital converted into a bustling hub for artists.

There, at least 40 programmers from around the globe presented proposals to improve the highly popular online encyclopedia frequented by millions of users every day.

Quim Gil, an engineering community manager for the Wikimedia Foundation, emceed the forum's final event, where programmers presented solutions to improve the technological infrastructure of Wikipedia, particularly the MediaWiki platform on which it is based, and the Wikimedia code development.

"We celebrate this event every year," said Gil in a cavernous third-floor Jerusalem Stone-lined room in the historic former hospital, located in the Talbiyeh neighborhood, near the Jerusalem Theater.

"It's our biggest technical event of the Wikimedia movement, which is held in a different city every year."

According to Gil, Wikimedia chose Jerusalem after deeming the Wikimedia Israel chapter to be the best candidate for prospective host cities around the world.

"The Wikimedia movement has different chapters and organizations, so we opened a call for different participants, and in this case we felt that Wikimedia Israel was what we felt was the most appropriate candidate for this year," he said.

The Wikimedia Foundation, Gil explained, is the organization in charge of hosting Wikipedia, as well as the foundation's numerous other ancillary projects.

"Our mission is to bring free knowledge for all the world, for everybody, for free," he said. "And this is a gathering of developers working to improve Wikipedia system projects, and developer tools that allow us to create, promote and distribute content in a better way."

As a case in point, Gil cited one solution presented at the forum developed to assist users with poor vision.

"One of the projects we demonstrated here is a gadget that will allow people with impaired vision to be able to read pages with increased font and with higher contrast than regular Wikipedia," he said.

Another development featured an editing app for Android, which allows users to make edits and add citations from their smart phones.

"Using a tiny mobile interface to review a huge document will allow people to select a word or sentence and then be given an option just to edit that one sentence," he said. "For us this is critical, because Wikipedia wouldn't be what it is if readers didn't become editors at some point."

Indeed, Gil emphasized that ensuring that users are capable of adding and correcting content in real time, from any mobile device, is instrumental to the nonprofit company's ongoing success.

"Users are welcome to use Wikipedia, but if a percentage of those users see a typo or a missing date, them being able to fix it is what makes Wikipedia what it is," he said.

Asked about the dangers of users who post false or libelous content on the platform, Gil responded that another project developed at the conference addressed that issue by applying artificial intelligence to prevent such abuses.

And despite the event's steep competition, Gil noted that a prize is not presented to the most industrious developer.

"We had 40 projects demonstrated that didn't exist three days ago," he said. "We are not really into number ones', we are a community of collaboration and longtime relationships. This is how we work."

Yuri Astrakhan, a senior software engineer for Wikimedia Foundation, who was born and Russia and has lived in New York for 25 years, said he presented a solution for storing more data on Wikipedia.

"I worked on a way to store structured data so that when you make an interactive graph or chart or a map, you can store the data in a structured way and reuse it for multiple articles," he said.

Aaron Halfaker, a senior research scientist for the foundation, said the major attraction for participants is the concept of "open knowledge."

"This is a lot of people who are really interested in the idea of open knowledge, and the way that they can contribute to it most effectively," he said.

Gil said next year's Wikimedia Foundation's Hackathon will be hosted in Austria.

Associated Press
State Dept. delays Clinton email review amid FBI probe
Saturday, 02 April 2016
Byline: Matthew Lee

The State Department has suspended its internal review into whether former Secretary of State Hillary Clinton or her top aides mishandled emails containing information now deemed "top secret." Spokeswoman Elizabeth Trudeau said Friday the department had paused the review to avoid interfering with an ongoing FBI investigation into Clinton's use of a private server while she was America's top diplomat.

She said the decision was made after the department sought the FBI's advice on how to proceed with the review and received word that it should follow its standard practice.

Trudeau said the department's standard practice is to place internal reviews "on hold while there is an ongoing law enforcement investigation underway."

"Of course, we do not want our internal review to complicate or impede the progress of their ongoing law enforcement investigation," Trudeau said.

Trudeau said the department would "reassess next steps" in the internal review process when the FBI completes its probe.

The department began the internal review in January when it announced that it had classified 22 emails that Clinton sent or received as top secret.

None of the emails was marked classified at the time it was sent.

One aspect of the internal review, conducted by the bureaus of Diplomatic Security and Intelligence and Research, was to investigate whether any of the information in the emails was classified at the time of transmission.

The review could result in counseling, warnings or other action against employees if it finds the information was mishandled.

Wall Street Journal
FBI Offers Help to Agencies On Phones
Saturday, 02 April 2016
Byline: Devlin Barrett

WASHINGTON -- The Federal Bureau of Investigation told law enforcement agencies around the country Friday it would try to help them open locked phones or other devices as much as "legal and policy constraints" allow.
The unusual guidance from the nation's premier law- enforcement agency is in response to a surge of interest from state and local authorities in how the agency was able to open a locked iPhone seized in the probe of a terror attack in San Bernardino, Calif., in December.

The FBI advisory seems to be aimed at reassuring police and prosecutors that while they don't have much to tell them now, they hope to provide more information and possibly help in the near future.

For months, the FBI had been unable to open the phone -- a 5C model -- and was engaged in a high stakes legal battle with Apple Inc. trying to force the company to help open the device. The Justice Department ended that legal battle this week, when it announced a third party outside the U.S. government had shown them a new means of cracking the phone.

"That method for unlocking that specific iPhone proved successful," the FBI missive said, adding that the agency is aware the difficulty of accessing locked data in criminal probes "is a substantial state and local law enforcement challenge that you face daily."

The FBI is now testing to see whether the method used in the San Bernardino case may work against over types of iPhones, say people familiar with the matter.

While the government says it needs to be able to look inside such devices when it has a warrant, Apple and other tech companies argue that even with a warrant it is wrong to force them to create new weaknesses in their systems that could expose millions of customers to hacking or snooping.

The FBI letter goes on to pledge an "open dialogue" with local officials, ending: "We are in this together."

Washington Post
FBI weighs if it can share hacking tool with local law enforcement
Saturday, 02 April 2016
Byline: Ellen Nakashima and Adam Goldman

The FBI and Justice Department are debating whether the hacking tool that helped the bureau unlock the iPhone of one of the San Bernardino, Calif., terrorists can be used to help state and local law enforcement, officials said Friday.
That will be a challenge because the bureau has classified the tool, making it difficult to use in state and local criminal prosecutions requiring disclosure of evidence to defendants, officials said.

"There's a desire to be forward-leaning to help state and local law enforcement," said a senior law enforcement official, who, like others, spoke on the condition of anonymity to discuss an ongoing investigation. "But no one knows quite what the answer is."

Moreover, the tool itself likely will have a shelf life of only a few months, as tech companies may find and fix the vulnerabilities that the tool exploits, and they periodically update the under-lying software.

The firm that helped the bureau -- not the Israeli company Cellebrite, as had been widely rumored -- charged a one-time flat fee, officials said.

The bureau is not releasing the company's name and has declined to discuss details of the solution. Officials last week said the approach was aimed at dismantling security features on the iPhone 5C to permit investigators to make many attempts to crack the passcode without wiping data from the device.

Since its announcement, the bureau has been peppered with inquiries from state and local law enforcement officials seeking to know whether the solution might be useful for their cases.

Manhattan District Attorney Cyrus R. Vance Jr. was among those who called. But, he said, he recognized that the solution itself may not be applicable to the more than 200 iPhones that he has sitting in a crime lab and his technicians cannot unlock.

None is a 5C running iOS 9, which is the model and operating system of the phone used by Syed Rizwan Farook, who was killed by police in December after a shooting attack that claimed 14 lives.

"The overwhelming majority of criminal investigations stalled by default device encryption will remain so until Congress intervenes," Vance said.

One-off technical solutions will result in a "cat-and-mouse cyber arms race" between the government and industry, he said in an interview. "I don't think that's the smart way to approach public safety or privacy policy."

The classification of the method highlights a tension between criminal and national security cases in which the most sophisticated tools are not always available to law enforcement. Unlike state and local courts, federal courts have procedures to protect classified information.

"It's been a challenge for law enforcement for a while," said Austin Berglas, a former assistant special agent in charge of the FBI's New York cyber branch and now head of cyber investigations at K2 Intelligence, a consultancy firm.

Berglas has worked cases on both sides of the divide, including one federal cybercrime investigation in which he was not given permission to use a classified tool because intelligence officials feared it would be disclosed in court.

"The FBI is very prudent when deploying the technologies," Berglas said. "The question is: Is it going to help the greater good by using this? Knowing that we may never have the ability to use this capability against the adversary again, are we willing to take that risk and use it?"

To referee the issue, the government has an interagency process headed by the attorney general to decide which capabilities should be classified. This is separate from the "vulnerabilities equities process" managed by the White House, which decides which software flaws should be disclosed to the software maker.

Now that the bureau owns the solution, it could conceivably have a local agency submit a phone to be unlocked to see if the solution works on it. But there would be constraints. For instance, the FBI likely would not testify about the tool in court, and the local agency would likely have to avoid using data retrieved from the phone as evidence in a criminal prosecution.

"So it would depend on how heavily that evidence weighs in that case. If it's a small part, maybe they can build a case around it," the senior official said. If not, he said, the tool is not for them.

Peter Modafferi, chief of detectives of New York's Rockland County, said he does not fault federal authorities for keeping some of their tools on a high shelf. "That's life," he said. "The bureau goes out of its way to help us when they can, but there's a difference between national security and local law enforcement."

Sunday Times (UK)
Threats spur Djibouti to sue Facebook (Canada)
Sunday, 03 April 2016
Byline: Mark Tighe

The president of Djibouti wants an Irish High Court judge to order Facebook to delete three accounts he alleges have been used to make death threats and threats of violence against him and his family. Ismail Omar Guelleh, known as IOG in the small East African country he has led since 1999, has applied for a High Court injunction against Facebook Ireland. The case is due for mention on April 11 in the chancery list, where business disputes are decided. Maki Omar Abdoulkadar, Djibouti's director of public prosecutions, has filed an affidavit in the case in support of his president's application.

Facebook Ireland is designated as the data processor for all account holders not resident in America or Canada. Guelleh's case is the first time a foreign individual has brought a legal action in Ireland seeking to compel Facebook to take action about material hosted by the social network. The Sunday Times has established that last year Guelleh brought an action against Facebook France and Facebook Inc in Paris in a bid to have the same three accounts suspended and the individual behind them identified.

Facebook appealed against a Paris judge's finding in Guelleh's favour in the French Court of Appeal, where it lost on most grounds. The company paid a fine rather than disclose the identity of the account holder.

The accounts use variations of the username Ainan Ainan, an anti-Guelleh activist who claims to live in Brussels.

One of Ainan Ainan's posts quoted in the French judgment spoke about Guelleh "losing a leg or two" or "an eye or two".

The post described the president as a "pirate". "Soon he will be punished , even if he fled ... he will be captured or die. [in English] Dead or alive".

Another post, partly in English and French, referred to Guelleh and said: "we'll be everywhere. To kill you." The post called on people to stop their pacifism and march against Guelleh's regime.

In its appeal in the French case, Facebook argued that the French judges had exceeded their power and complained that their actions in ordering the closure of accounts was disproportionate with respect for freedom of expression.

It also argued that although the accounts were in the French language and Djibouti is a former French colony, the proper jurisdiction was in Ireland where Facebook Ireland was subject to Irish data protection laws.

Guelleh's complaint sought damages of 85,000 from Facebook including a 20,000 fine for not taking down the accounts. He said that the accounts defamed him, and threatened his life and the physical safety of his family. Despite his efforts Facebook had refused to close the "illegal" accounts, he said.

The Court of Appeal fined Facebook 5,000 and 1,000 a day for three months for failing to close the accounts.

Djibouti is strategically important because of its location on the Horn of Africa near shipping lanes and areas where Islamist terrorists are active on the Arabian peninsula.

Reporters Without Borders ranks Djibouti 170 out of 180 countries in its annual world press freedom index. Guelleh, is campaigning to be re-elected president in an election this Friday. He is expected to be returned for a fourth term.

Reporters Without Borders said that this year, Mohamed Ibrahim Waiss, who works for La Voix de Djibouti, an opposition online radio station outside the country, was beaten by police and made to surrender his Facebook usernames and passwords so his account could be used to post images insulting the opposition. A US State Department report of 2013 noted that government forces monitor social media and police visit those who post antigovernment messages.

Maydaneh Abdallah Okieh, a journalist and activist, was sentenced to 45 days in prison and fined 1,000 after he posted photographs on Facebook of police breaking up a demonstration. On appeal, the court increased his sentence to five months.

This year, a London judge ruling on a case brought by Djibouti called Guelleh's regime "capricious", "cavalier" and on occasions "reprehensible".

Reuters
FBI trick for breaking into iPhone likely to leak, limiting its use
Sunday, 03 April 2016
Byline: Staff reporter

SAN FRANCISCO - The FBI's method for breaking into a locked iPhone 5c is unlikely to stay secret for long, according to senior Apple Inc engineers and outside experts.
Once it is exposed, Apple should be able to plug the encryption hole, comforting iPhone users worried that losing physical possession of their devices will leave them vulnerable to hackers.

When Apple does fix the flaw, it is expected to announce it to customers and thereby extend the rare public battle over security holes, a debate that typically rages out of public view.

The Federal Bureau of Investigation last week dropped its courtroom quest to force Apple to hack into the iPhone of one of the San Bernardino shooters, saying an unidentified party provided a method for getting around the deceased killer's unknown passcode.

If the government pursues a similar case seeking Apple's help in New York, the court could make the FBI disclose its new trick.

But even if the government walks away from that battle, the growing number of state and local authorities seeking the FBI's help with locked phones in criminal probes increases the likelihood that the FBI will have to provide it. When that happens, defense attorneys will cross-examine the experts involved.

Although each lawyer would mainly be interested in whether evidence-tampering may have occurred, the process would likely reveal enough about the method for Apple to block it in future versions of its phones, an Apple employee said.

"The FBI would need to resign itself to the fact that such an exploit would only be viable for a few months, if released to other departments," said Jonathan Zdziarski, an independent forensics expert who has helped police get into many devices. "It would be a temporary Vegas jackpot that would quickly get squandered on the case backlog."

In a memo to police obtained by Reuters on Friday, the FBI said it would share the tool "consistent with our legal and policy constraints."

Even if the FBI hoards the information - despite a White House policy that tilts toward disclosure to manufacturers - if it is not revealed to Apple, there are other ways the method could come to light or be rendered ineffective over time, according to Zdziarski and senior Apple engineers who spoke on condition of anonymity.

The FBI may use the same method on phones in cases in which the suspects are still alive, presenting the same opportunity for defense lawyers to pry.

In addition, the contractor who sold the FBI the technique might sell it to another agency or country. The more widely it circulates, the more likely it will be leaked.

"Flaws of this nature have a pretty short life cycle," one senior Apple engineer said. "Most of these things do come to light."

The temporary nature of flaws is borne out in the pricing of tools for exploiting security holes in the government-dominated market for "zero-days," called that because the companies whose products are targets have had zero days' warning of the flaw.

Many of the attack programs that are sold to defense and intelligence contractors and then to government buyers are purchased over six months, with payments spaced apart in case the flaw is discovered or the hole is patched incidentally with an update from the manufacturer, market participants told Reuters.

Although Apple is concerned about consumer perception, employees said the company had made no major recent changes in policy. Instead, its engineers take pride in the fact that a program for breaking into an iPhone via the web was recently purchased by a defense contractor for $1 million, and that even that program is likely to be short- lived.

They said most iPhone users have more to fear from criminals than from countries, and few crooks can afford anything like what it costs to break into a fully up-to-date iPhone.

Wall Street Journal
China's ZTE to Replace Three Senior Executives
Sunday, 03 April 2016
Byline: Juro Osawa

HONG KONG--ZTE Corp.'s board will meet early next week to replace three of its most senior executives, including its chief executive, people familiar with the matter said, as the Chinese telecommunications-equipment maker tries to rebuild its reputation after being accused of violating of U.S. trade rules. Chief Executive Shi Lirong, who has been in the role since 2010, as well as executive vice presidents Tian Wenguo and Qiu Weizhao, will step down pending board approval, the people said. Chief Technology Officer Zhao Xianming is expected to assume the role of CEO and chairman, they said.

On Tuesday and Wednesday, the board plans to discuss and approve the management changes as well as ZTE's 2015 financial results, which were delayed after the U.S. Commerce Department slapped trade sanctions on the company last month, alleging it violated rules by exporting American technological goods to Iran and other nations.

As part of a recent agreement between the U.S. Commerce Department and ZTE to temporarily remove the sanctions, the Chinese company's executives who have been involved in the alleged violation must be removed from management roles, the people said.

In a 2011 ZTE internal document obtained and disclosed last month by the U.S. government, Mr. Tian and Mr. Qiu were named as executives who were in charge of ZTE's plans for allegedly circumventing U.S. export rules. The document detailed the Chinese firm's elaborate plans to set up shell companies to ship goods to Iran without getting caught by U.S. authorities.

ZTE didn't make the executives available for comment.

The shake-up in ZTE's top management comes after the U.S. Commerce Department recently agreed to lift the sanctions on a temporary basis as long as the company stays true to the commitments it has made with the U.S. government. The sanctions, which blocked ZTE's access to supplies of U.S. components and software, threw the Chinese firm's business into doubt and created a new source of tension between Washington and Beijing. China's commerce minister responded by expressing "strong dissatisfaction" with the situation.

ZTE, which has roughly 80,000 employees globally, is a major global supplier of telecom networking-equipment such as wireless base stations and antennas. Over the past few years, its smartphone business has also gained a substantial presence in the U.S., where it was ranked fourth with a 7.2%

market share last year, behind Apple Inc., Samsung Electronics Co. and LG Electronics Inc., according to research firm Canalys.

ZTE is renewing its management as it scrambles to keep its business moving. ZTE will release its full-year earnings Wednesday after postponing the announcement last month, the people said. Trading in ZTE's Hong Kong-listed shares, suspended since March 7, is expected to resume Thursday, the people said.

Some of the company's component suppliers that had temporarily halted shipments with the company last month are resuming their shipments, according to people familiar with the matter.

ZTE is also planning to release its new flagship smartphone called the Axon 2 in mid-May, after delaying its previous plans to launch the phone in April, people familiar with the matter said.

In January, ZTE said it expects to report a 44% increase in 2015 net profit to 3.78 billion yuan ($583 million) and revenue to rise 24% to 100.8 billion yuan, based on preliminary unaudited results.

Had the sanctions stayed in place longer, the impact would have been disastrous for ZTE, analysts said.

In a letter sent to ZTE employees March 8, when the U.S. sanctions took effect, Mr. Shi described the situation as a "crisis" and said the company had set up a special team of executives to handle the issue. The U.S. restrictions hindered ZTE's ability to procure not only components manufactured in the U.S., but also those manufactured overseas based on U.S. technology, according to lawyers specializing in U.S. export control laws.

The Mirror
RAF's new 'GCHQ in the sky' spy planes which can hack enemy emails and phone calls
Sunday, 03 April 2016
Byline: Nigel Nelson

The MoD has bought nine Boeing P-8 Poseidon aircraft to replace the Nimrod spy planes contrioversially scrapped in 2010
Air chiefs have bought nine spy planes, each one like a flying GCHQ .

The Boeing P-8 Poseidon is as effective at information -gathering as the Government's eavesdropping headquarters.

It can hack terrorists' mobile calls and emails, track and -monitor enemy movements and direct our fighter jet response.

The RAF is believed to be spending £2.6billion on buying and maintaining the P-8s, -regarded as the world's most -hi-tech spy planes.

The fleet will also guard Britain's shipping lanes, protect the Navy's aircraft carrier and nuclear submarines.

Britain has had no maritime spy plane since the controversial 2010 scrapping of the Nimrod MR4A by the Government.

Since then Russian combat jets and nuclear-powered subs have encroached into British air and waters almost weekly.

The P-8 is so advanced it can identify an enemy sub's -periscope from several thousand feet.

Read more: Tories order spy planes that don't work with RAF's in-flight refuelling system

Its sensors and radars are so precise it will detect, classify and identify ships and small -vessels. It can also track subs.

And it is sophisticated enough to direct our jets and -surveillance drones on to targets approaching the UK.

The spy-in-the-sky is also one of the most deadly planes in the air as it can carry a lethal -battery of missiles, anti-submarine -torpedoes, bombs, depth charges and mines.

The aircraft, with two pilots and seven intelligence experts, has a range of about 1,200 miles with a 500mph cruising speed. It can also hover 200ft over a target for up to four hours during -sub-hunting operations.

The P-8, already used by the Australian, US, Indian and New Zealand air forces, will be -delivered to the RAF by 2020.

Defence chiefs scrapped a new generation of Nimrods in 2010 as part of MoD cuts.

Over £3.8billion of taxpayers money had been spent on the programme, which was £789million over budget and was nine years late.

When the Nimrod costs are added to the £250million per P-8, the cost of each plane rises to over £650million.

A defence source told the Sunday People : "The cancellation of the Nimrod -programme had effectively given Russian subs and aircraft a "free pass" to enter UK waters.

"Barely a week passes without some Russian ship, aircraft or sub trying to enter British -shipping lanes or airspace."

An MoD spokesman said: "We are committed to buying P-8 aircraft, which will be based at RAF Lossiemouth.

"The full cost of programme is yet to be determined."

Weapons: Freefall bombs, Harpoon anti-ship missiles, supersonic low-altitude -missiles (SLAM), land attack missiles, depth charges, sonar buoy torpedoes.

Range: 1,200 miles

Speed: Max 564mph

Cruising: 506mph

Dimensions: Length 129ft Wingspan: 117ft Weight: 62.7tons

Crew: Pilot and co-pilot plus seven console operators

Engines: 2 x CFM56-7B -turbofans.

Radar/surveillance: Electro- optical infrared -sensor can ID, track and -engage several targets - from land vehicles, aircraft, and ships. Can hack mobiles, emails and encrypted -communications. Advanced magnetic anomaly detection system for sub tracking.

Globe and Mail
Ottawa's big IT project still struggling
Monday, 04 April 2016
Byline: Barrie Mckenna

It was a seductively simple idea.
Take the maze of federal government databases, e-mail systems and computer networks, and put them under one departmental roof. More than 60 e-mail systems would become one, 500plus databases would be merged into seven, and thousands of tech workers from dozens of departments would go to work for a single agency, Shared Services Canada.

The two Conservative ministers in charge at the time - former public works minister Rona Ambrose (now interim Conservative leader) and treasury board president Tony Clement - were bursting with optimism when they announced the project five years ago. They promised the consolidation would save piles of money (up to $400-million a year), wipe out duplication and enhance cybersecurity.

"This is a whole new way of doing business for the government," Mr. Clement vowed.

Not so much. It's turned into an old and very familiar story of how Ottawa works. Years and billions of dollars later, virtually none of the wondrous benefits have come to pass.

And in last week's budget, the new Liberal government quietly gave Shared Services a $384-million infusion over two years to its roughly $1.9-billion annual budget - apparently, to keep creaky old government computer systems from crashing. The agency will get another $75-million to strengthen security.

But this isn't just an inside-Ottawa tale of serial bungling. There are disturbing real-world consequences of the government's failure to fix chronic information technology (IT) problems. Websites periodically crash and go offline, sometimes for days, because of continuing database problems.

A 2014 cyberattack by Chinese hackers on the National Research Council's network paralyzed much of its research work for nearly a year. Also in 2014, emergency workers in Saskatchewan lost voice communications for nearly an hour owing to a mix-up between Shared Services and the RCMP.

Not only is Ottawa not saving money, it's spending more and getting less than it needs in the way of IT. Much of the promised consolidation remains a work in progress, with no clear end-date in sight.

The merging of e-mail systems, outsourced to Bell Canada and CGI Group, is already more than a year behind schedule. Fewer than one in five government workers is using new Canada.ca addresses.

Efforts to move more than 15,000 computer applications onto three new centralized databases in Gatineau, Que., Barrie, Ont., and at Canadian Forces Base Borden, north of Toronto, are running late.

Fewer than 10 per cent of government apps have been shifted over to Shared Services. And an $18-million project aimed at making it easier for users to sort through Statistics Canada data is also badly behind schedule.

Auditor-General Michael Ferguson issued a scathing report in February, outlining Shared Services' mounting problems and its inability to deliver results. "They have big problems ahead of themselves," Mr. Ferguson told reporters bluntly.

The view of the new Liberal government is that Shared Services was set up to fail by the Conservatives. The agency was hit with severe budget cuts soon after its creation, leaving it starved of the resources it needed.

The question now is can the new government make it right? A key issue is sorting out what information technology the government should develop in-house, and what it should buy off the shelf. In a postbudget brief, Canadian Advanced Technology Alliance president John Reid lamented that "despite longstanding good intentions, the [government's] procurement model has not modernized to keep up with industry changes and standards. It is not fully aligned with the digital era."

It's a missed opportunity to spur innovation, according to CATA. Too often, Ottawa winds up overpaying for inferior IT, while crowding out the private sector by building custom systems rather than buying commercial offerings and spurring the emergence of promising technology exports.

The government "has no export sales. ... No intellectual property gets created that is patentable," the group laments.

Of course, CATA, which speaks for Canadian tech companies, has an interest in seeing some of that business flow to its members.

But given recent experience, it's hard to imagine Ottawa could do worse. Surely there is a better way for Ottawa to acquire the technology it needs to do its work.

La Presse
La surveillance demasse menacerait la diversité d'opinions
Saturday, 02 April 2016
Byline: Marc Thibodeau

La surveillance de masse des communications en ligne pousse nombre d'internautes à s'autocensurer, y compris ceux qui affirment «n'avoir rien à cacher», et limite la diversité d'opinions à un degré préoccupant.

Le constat figure dans une nouvelle étude parue dans la revue Journalism & Mass Communication Quartely qui sonne l'alarme quant à l'impact potentiellement néfaste sur la liberté d'expression de pratiques mises en lumière aux États- Unis par Edward Snowden.

L'ancien consultant de la National Security Agency (NSA) avait notamment affirmé en 2013, documents à l'appui, que l'influent service de renseignements était en mesure d'accéder au contenu des serveurs de géants de la Silicon Valley comme Google, Facebook et Yahoo!.

Les firmes désignées ont démenti toute collaboration sans pour autant convaincre la population américaine, qui demeure très partagée quant à l'utilisation de programmes de surveillance à grande échelle par le gouvernement pour lutter contre le terrorisme.

Étude

Pour évaluer leur impact sur le comportement des internautes, une chercheuse de la Wayne State University, au Michigan, a demandé à un groupe de 250 personnes de réagir à une nouvelle fictive portant sur l'engagement des États-Unis contre le groupe armé État islamique.

Les répondants devaient préciser à quel point ils étaient à l'aise avec l'idée de commenter publiquement la nouvelle sur Facebook, dire ce qu'ils estiment être la position de la majorité des Américains à ce sujet et donner leur appréciation des programmes de surveillance de masse.

La moitié des personnes recrutées pour l'exercice se voyaient rappeler qu'il était important de garder en tête que la NSA «surveille les activités en ligne de citoyens».

Dans la vaste majorité des cas, écrit la chercheuse responsable, Elizabeth Stoycheff, les participants ayant été sensibilisés par le message sur la NSA se montraient beaucoup moins disposés à exprimer leur opinion s'ils avaient l'impression qu'elle n'était pas conforme à celle de la majorité.

Ceux qui étaient les plus susceptibles d'adopter un comportement conformiste sont ceux qui soutenaient le plus les programmes de surveillance.

«Ces individus prétendent que la surveillance est nécessaire pour assurer la sécurité nationale et qu'ils n'ont rien à cacher. Toutefois, quand ces individus ont l'impression qu'ils sont surveillés, ils modifient volontairement leur comportement - exprimant leurs opinions quand ils sont en phase avec la majorité et les taisant dans le cas contraire», relève l'auteur.

Seules les personnes qui étaient très critiques à l'endroit des programmes de surveillance semblaient disposées à exprimer leur opinion sans réserve, qu'ils soient ou non en phase avec la majorité.

Des études antérieures ont démontré que les usagers des réseaux sociaux sont moins susceptibles de s'exprimer librement sur un sujet s'ils ont l'impression d'être minoritaires, en partie de crainte de se retrouver isolés.

L'effet «modérateur» découlant de la crainte d'un programme de surveillance constitue un autre facteur que les autorités devraient examiner attentivement alors qu'ils statuent sur l'utilité et la légitimité de programmes de surveillance de masse, souligne Mme Stoycheff.

Programme révisé

La polémique suscitée par les révélations d'Edward Snowden a notamment poussé le Congrès américain à réviser un programme de collecte de métadonnées qui permettait à la NSA d'accumuler des renseignements sur l'ensemble des clients de Verizon.

Les élus ont cependant «traîné les pieds» avant d'interrompre cette pratique et tardent à adopter les réformes requises pour protéger adéquatement les données des internautes contre des intrusions abusives, juge l'Electronic Frontier Foundation (EFF) dans un récent rapport.

L'organisation de défense des droits des internautes salue parallèlement les efforts des géants de l'internet, relevant qu'ils ont, dans la majorité des cas, adopté des politiques beaucoup plus restrictives à ce sujet au cours des dernières années.

Les normes de l'industrie en la matière ont sensiblement évolué, mais il reste encore beaucoup à faire, prévient l'EFF.

Washington Post
Hackers find soft spot in hospitals
Sunday, 03 April 2016
Byline: Carolyn Y. Johnson and Matt Zapotosky

The cyberattack on MedStar Health - one of the biggest health-care systems in the Washington region - is a foreboding sign that an industry racing to digitize patient records and services faces a new kind of security threat that it is ill-prepared to handle, security experts and hospital officials say.
For years, hospitals and the health-care industry have focused on keeping patient data from falling into the wrong hands. But the recent attacks on MedStar's network and other hospitals across the country highlight an even more frightening downside of security breaches: As hospitals have become dependent on electronic systems to coordinate care, communicate critical health data and avoid medication errors, patients' well-being may also be at stake when hackers strike.

Hospitals are used to chasing the latest medical innovations, but they are rapidly learning that caring for sick people also means protecting medical records and technology systems from hackers. An industry

that has traditionally spent a small fraction of its budget on cyberdefense is finding that it also must teach doctors and nurses not to click on suspicious online links and shore up its technical systems against hackers armed with an ever-evolving set of tools.

In some ways, health care is an easy target: Its security systems tend to be less mature than those of other industries, such as banking and tech, and its doctors and nurses depend on data to perform time-sensitive, lifesaving work. Where a financial-services firm might spend a third of its budget on information technology, hospitals spend only about 2 to 3 percent, said John Halamka, the chief information officer of Beth Israel Deaconess Medical Center in Boston.

"If you're a hacker . . . would you go to Fidelity or an underfunded hospital?" Halamka said. "You're going to go where the money is and the safe is easiest to open."

The stakes are extraordinarily high. Hospitals' electronic systems are often in place to help prevent errors. Without computer systems, pharmacists cannot easily review patients' lab results, look up what other medications the patients are on or figure out what allergies they might have before dispensing medications. And nurses administering drugs cannot scan the medicines and the patients' wristbands as a last check that they are giving the correct treatments. When lab results exist only on a piece of paper in a patient's file, it is possible they could be accidentally removed by a busy doctor or nurse - and critical information could simply disappear.

In MedStar's case, a virus early this week infiltrated its computer systems, forcing the health-care giant to shut down its entire network, turn away patients, postpone surgeries and resort to paper records.

"One thing I think is becoming clear, especially over the last few weeks or months, is that health care is rapidly becoming a target for this," said Daniel Nigrin, chief information officer of Boston Children's Hospital, whose network came under attack by the hacker collective Anonymous in April 2014. "What struck us at that point was, you know what? These attacks can do a lot more than get your data; they can really disrupt the day-to-day operations of your facilities."

Although a handful of hospitals nationwide have been victims of cyberattacks in recent weeks, the MedStar security breach shows hackers' increasing boldness and sophistication. The chain is one of biggest employers in the Baltimore-Washington region and runs 10 hospitals as well as 250 clinics and other sites. MedStar spokeswoman Ann Nickels declined to elaborate on what sort of software attack the hospital suffered, but several employees have said they saw a pop-up message suggesting that it was "ransomware" - software that can lock people out of systems until they make a bitcoin payment. According to a photo of the pop-up message provided by a MedStar Southern Maryland Hospital Center employee, the hackers were demanding 45 bitcoins - equivalent to about $19,000 - to restore access to MedStar's system.

"You just have 10 days to send us the Bitcoin," the note read. "After 10 days we will remove your private key and it's impossible to recover your files."

Nickels said MedStar saw "no indication that data has left our system" or that patient privacy had been compromised. In a statement, the health-care system said it had not paid any type of ransom. A Friday-afternoon update from the hospital said MedStar was "approaching 90 percent functionality" of its systems.

Ransomware is not new, but cybersecurity experts and FBI data say its use is on the rise. Hospitals, of course, are not the only institutions facing such attacks. In nine months in 2014, the FBI received 1,838 complaints about ransomware, and it estimates that victims lost more than $23.7 million. The next year, the bureau received 2,453 complaints, and victims lost $24.1 million. The FBI does not condone the paying of ransoms, but its agents acknowledge that businesses are often left with a tough choice.

Hospitals, in particular, are vulnerable. In the weeks before the attack on MedStar, hackers hit Hollywood Presbyterian Medical Center in Los Angeles, extorting $17,000 in bitcoins, and Kentucky-based Methodist Hospital, which declared a state of emergency after an attack. Two Southern California hospitals, part of Prime Healthcare Services, were attacked in March.

Justin Harvey, the chief security officer of Fidelis Cybersecurity, said the hackers' success is likely to make them bolder, and he worries about critical infrastructure in the United States.

"I can't comment on whether the [Federal Aviation Administration] and all the power grids are up to snuff," he said. "If they're not, it can create a big problem."

Craig Williams, security outreach manager at Talos, the cybersecurity research group of Cisco, said the use of ransomware has exploded because it yields good profit margins. He estimated that it is a $100 million-a-year business.

"The malware industry is making giant steps toward ransomware, and really, the reason behind this is ransomware's profit margin simply exceeds that of other types of criminal activity," Williams said.

The way hackers get into a system is generally through a phishing attack - persuading an unsuspecting employee to click on a link or an attachment in an email - or by finding a network vulnerability.

That leaves hospitals with two challenges: designing systems that can resist attack and training employees.

On the network side, Williams said health-care companies - or any companies - that do not have full-time security specialists may not be keeping up with the latest problems and patches. He noted that one strain of ransomware exploits a well-known vulnerability in networks, and when his team did a scan of the Internet this week, it found 2.1 million servers that would be susceptible to such an attack.

The cultural problem may be even harder to solve.

"You're as vulnerable as your most gullible employee," Halamka said.

At Beth Israel, the hospital has printed up stickers that appear on salad containers and cookie packaging in the cafeteria so that people are reminded, even when eating lunch, not to click on links in emails they did not expect to receive. The hospital also has conducted internal phishing campaigns - sending fake emails to employees to assess where risks exist and to see whether extra cybersecurity training is needed.

Experts said the recent attacks seem to be based in Eastern Europe, although it is hard to tell whether one group alone is responsible. The hacks have similarities, to be sure, but hackers trade tools and information. One concern is that as the attacks gain coverage, they will inspire more copycats who will use the same technique to target other vulnerable networks.

"This thing is an industry, the black market that does this type of activity," said Chris Ensey, chief operating officer at Dunbar Security Solutions.

The details of MedStar's particular case - including what particular version of ransomware might have been used and how it got into the system - remain murky. An FBI spokesman declined to provide any details - including on the type of possible ransomware - other than to say the bureau was "aware of the incident and is looking into the nature and scope of the matter."

The Sun (UK)
Google removes Taliban propaganda app from its stores after it was used to spread hate speech
Monday, 04 April 2016
Byline: Fionn Hargreaves

AN app developed by the Taliban has been taken down from Google's Play Store for breaking the tech giant's rules on hate speech. The hate- filled app, "Pashto Afghan News - alemarah" ran news and videos from the extremist group.
Pashto is one of the two official languages of Afghanistan and Alemarah is the name of the Taliban's propaganda arm.

US group SITE Intel, who moniter jihadist activity online, discovered the app on Friday.

It was taken down on Saturday.

The app is thought to have been removed for inciting hate speech.

Google's rules state: "We don't allow apps that advocate against groups of people based on their race or ethnic origin, religion, disability, gender, age, nationality, veteran status, sexual orientation, or gender identity".

A Google spokesman said: "While we don't comment on specific apps, our policies are designed to provide a great experience for users and developers. That's why we remove apps from Google Play that violate those policies."

READ MORE:

'My kids can't even see your face. Are you a man or a woman?' Muslim in a veil posts footage of furious row with 'Islamophobic shopper' who called her 'Batman'

'A contrived set- up': Peru Two drugs mule under fire for having 'X Factor look' and being insincere in first TV interview since release

NHS nurse blackmailed female colleague in sick revenge porn plot after she dumped him

The terrorist group aim to reconquer Afghanistan after being removed from power in 2001.

They want to bring back Sharia law, a conservative Islamic law, to the country.

Taliban spokesman Zabihullah Mujahed told Boomberg the app "is part of our advanced technological efforts to make more global audience"

But Mr Mujahed said that they were having technical difficulty with the app.

This is just one of many ways in which extremist groups are using the internet to spread their messages of hate.

The Taliban already run a website in five different languages as well as maintaining a Facebook and Twitter account.

Twitter are trying to fight ISIS's large presence on their social media site as staff have been suspending extremists' accounts.

It was estimated in 2015 that ISIS are running more than 46,000 Twitter accounts.

Wall Street Journal
Why iPhone Breach Is Good for Users

Monday, 04 April 2016
Byline: Christopher Mims
Section: column

There was only one way for the court battle between the Federal Bureau of Investigation and Apple Inc. over access to the data on a killer's phone could end well for everyday Americans. Luckily, the FBI achieved it.
With the help of outside hackers, whose identity remains a mystery, the FBI successfully circumvented Apple's much-touted security. In the process, the agency did exactly what defenders of encryption and digital privacy have advocated for some time. It is called "lawful hacking," which is another way to describe law enforcement exploiting weaknesses in a security process.

Advocates say lawful hacking is an alternative to, and preferable to, creating a new "backdoor" into the system. An author of a recent paper on the subject, Columbia University professor and cybersecurity expert Steven Bellovin, says "I don't have any problem with what the FBI did. The whole premise of lawful hacking is there are vulnerabilities."

Here is why that is a good thing: It makes software more secure. Bugs are often discovered by "white hat" hackers who share them with the software's creator so they can be patched, typically before the flaw is even disclosed. This isn't a purely benevolent system; it works because these hackers, or their employers at universities or cybersecurity companies, want the money from bug "bounties," or the publicity that comes with finding an exploit, and because everyone, including hackers, is vulnerable to undisclosed exploits.

This dynamic is so well-established that it played out quietly in the background as the FBI-Apple dispute raged. Researchers at Johns Hopkins University last month revealed a flaw in Apple's iMessage texting program that could have allowed law-enforcement agents or hackers to decrypt photos or videos attached to messages as they moved over the Internet. The researchers disclosed the bug to Apple, which devised a patch.

We also saw the process at work in 2014 with a bug called Heartbleed, which jeopardized the encryption scheme used on much of the Internet. The flaw was first reported by a researcher at Google; a fix was quickly devised and deployed by those responsible for the open-source code in which it was found.

In that case, the White House made an unprecedented disclosure about how the federal government decides whether or not to share a vulnerability with the companies responsible for fixing them. The National Security Agency, for example, has said it discloses 91% of the vulnerabilities it discovers, but probably only after it has used them for its own purposes. Officials said they decide whether to disclose a flaw by weighing factors including whether the vulnerability poses a threat to national security, the likelihood that someone else has found it, the value of the intelligence that could be gathered if it is used, and whether it can be patched.

Given the publicity around the iPhone dispute, Shane McGee, chief privacy officer of cybersecurity firm FireEye Inc., says it is now open season on Apple's iOS operating system among hackers, who are often driven by ego as much as lucre.

There is a big caveat in the Apple case, however. For now, at least, the FBI won't disclose the bug to Apple, which means Apple can't fix it. That is bad for Apple's privacy-focused brand and could be bad for users, since others who learn of the flaw could exploit it for nefarious purposes. We don't know how likely that is, because we don't know how the FBI gained access to the phone; its method could require physical access to a device, plus a lot of time and money, making other exploits less likely.

The FBI and Apple declined to comment.

Whatever happens with this bug, and this phone, the struggle between breaking into software and securing software will only intensify. As FireEye's Mr. McGee points out, Apple is already working to make the next version of iOS even more impenetrable by the government and Apple itself.

The possibility that Apple could create a device that it would be unable to breach even if ordered by a court must keep those in law enforcement awake at night. And yet we seem headed to a world in which even the most draconian edict couldn't force Apple to unravel the laws of mathematics at the heart of its own encryption.

In a world of ever-multiplying threats -- including multimillion-dollar bank heists carried out from a keyboard -- increased security is an unqualified win for all Apple users.

It won't necessarily come easily, however. Absent action from Congress -- which lawmakers have said is unlikely in a polarizing election year -- the battle between Apple and the FBI seems destined to continue ad infinitum. Which, paradoxically, is evidence that the system is working.

It may be in the nature of this dispute that it can never end. And that may be the only satisfactory "resolution" we can hope for.

New York Times
Technology Upgrades Get White House Out of the 20th Century
Monday, 04 April 2016
Byline: Michael D. Shear

Can you run the country with spotty Wi-Fi, computers that power on and off randomly and desktop speakerphones from Radio Shack, circa 1985?
It turns out you can. But it is not ideal, as President Obama's staff has discovered during the past seven years. Now, as Mr. Obama prepares to leave the White House early next year, one of his legacies will be the office information technology upgrade that his staff has finally begun.

Until very recently, West Wing aides were stuck in a sad and stunning state of technological inferiority: desktop computers from the last decade, black- and-white printers that could not do double-sided copies, aging BlackBerries (no iPhones), weak wireless Internet and desktop phones so old that few staff members knew how to program the speed-dial buttons.

On Air Force One, administration officials sent emails over an air-to-ground Internet connection that was often no better than dial-up modems from the mid- 1990s.

"We can't do this," recalled Anita Decker Breckenridge, the deputy chief of staff for operations at the White House, who has since worked with the Air Force to upgrade the president's plane to broadband speeds. "This is the Oval Office in the sky. Talk about a network that didn't work."

Part of the problem? Responsibility for White House technology has long been divvied up between four agencies, each with their own chief information officer: the National Security Council, the Executive Office of the President, the Secret Service and the White House Communications Agency. That led to a series of Band-Aid solutions over the years, as one agency or another has attempted piecemeal upgrades to White House gear.

It also led to comical moments. In 2014, when White House aides accompanying Mr. Obama on his summer vacation in Martha's Vineyard struggled with balky laptops as they tried to revise a presidential statement, they could not get on-the- road tech support from the White House Communications Agency because the agency's staff members were not authorized to log in to computers issued by the Executive Office of the President.

Ms. Breckenridge was inspired by Mr. Obama's development in 2015 of the United States Digital Service and its mission to upgrade the federal government beyond the White House. She was determined after her frustrations in Martha's Vineyard to fix the mess, and by March 2015 had hired David Recordon, who designed and maintained the office technology for Mark Zuckerberg and the other employees at Facebook, as the information technology guy for the White House complex.

"It was an interesting challenge and world for me," Mr. Recordon said.

One of his first tasks was trying to map the miles of Ethernet cables and phone wires inside the walls of 1600 Pennsylvania Avenue. The team of technicians eventually discovered and removed 13,000 pounds of abandoned cables that no longer served any purpose.

"They had been installed over the decades by different organizations using different standards, different techniques, from different eras," Mr. Recordon said. "They were finding these pipes that just had bundles of cable that had been cut off over the years, no longer used. So we just started pulling it out."

With the wiring fixed, Mr. Recordon started replacing computers (the new ones have fast, solid- state drives and modern processors) and color printers. The new phone system -- the first since the Clinton years -- is all digital, with built-in speakerphones and speed-dial buttons that can be changed online. Many White House aides now carry the most recent iPhones. Mr. Obama, however, still carries a specially modified, highly secure BlackBerry.

The Wi-Fi in the Roosevelt Room is finally strong enough to live-stream an event on Facebook, like White House aides did last week when Mr. Obama surprised former federal inmates whose sentences had been commuted. Forgotten passwords are no longer an irritant now that the White House has started requiring users to log on with a chip-enabled smart card and a pin code.

Mr. Recordon's team also designed a new web-based system for admitting visitors to the West Wing that can be managed securely from any computer, including ones outside the White House complex.

To be sure, some important West Wing technology was upgraded by the George W. Bush administration, which overhauled the Situation Room for the first time since the Kennedy administration and added modern communications gear. Joe Hagin, the deputy chief of staff for Mr. Bush, recalled having to replace the phones in the presidential limousine after Mr. Bush complained that he had not been able to make a single phone call from his motorcade over an entire weekend.

"He said to me, 'What the heck would happen if there were a true national emergency?' " Mr. Hagin recalled. That fear came true months later on Sept. 11, 2001, when communications glitches plagued the government and led to new equipment in Air Force One and the first BlackBerries in the White House.

Mr. Hagin's team also upgraded the Intel 486 computers and got rid of the slow and cumbersome Lotus Notes email system. But the speed of technological advancement has once again left the current White House behind.

"I'm very sympathetic to them," said Mr. Hagin, who commiserated with Ms. Breckenridge last year about the sorry state of White House technology.

Ms. Breckenridge said the White House has not had to request any additional money for the new upgrades, which have been paid for out of the existing technology budgets for the various agencies involved. In some cases, she said, they have saved money by eliminating duplications. The four agencies no longer negotiate their own contracts with cellphone companies and no longer buy duplicate copies of software licenses.

Ms. Breckenridge said she was hopeful that Mr. Obama will leave to his successor's staff a building that is more useful in the Facebook and Twitter era, or whatever comes next.

Mr. Hagin said he wished them well, but predicted it will not be easy. He recalled once discovering a basement room in the West Wing filled with telephone switching gear that technicians said could be replaced with a unit the size of a dorm-room refrigerator. But everyone was nervous about cutting the wires because no schematics or design guides existed anymore, he said.

Replacing the equipment took a full two years.

Jerusalem Post
Wikimedia Foundation holds its 'Hackathon' in Jerusalem
Sunday, 03 April 2016

The Start-Up Nation earned yet another colorful feather in its already well-ornamented cap on Sunday, after hosting the annual Wikimedia Foundation's Hackathon in Jerusalem.
The four-day event, which brought together more than 150 computer developers from 17 countries to enhance Wikipedia's user experience and ensure reliable data, concluded at the capital's Hansen House, a former leper hospital converted into a bustling hub for artists.

There, at least 40 programmers from around the globe presented proposals to improve the highly popular online encyclopedia frequented by millions of users every day.

Quim Gil, an engineering community manager for the Wikimedia Foundation, emceed the forum's final event, where programmers presented solutions to improve the technological infrastructure of Wikipedia, particularly the MediaWiki platform on which it is based, and the Wikimedia code development.

"We celebrate this event every year," said Gil in a cavernous third-floor Jerusalem Stone-lined room in the historic former hospital, located in the Talbiyeh neighborhood, near the Jerusalem Theater.

"It's our biggest technical event of the Wikimedia movement, which is held in a different city every year."

According to Gil, Wikimedia chose Jerusalem after deeming the Wikimedia Israel chapter to be the best candidate for prospective host cities around the world.

"The Wikimedia movement has different chapters and organizations, so we opened a call for different participants, and in this case we felt that Wikimedia Israel was what we felt was the most appropriate candidate for this year," he said.

The Wikimedia Foundation, Gil explained, is the organization in charge of hosting Wikipedia, as well as the foundation's numerous other ancillary projects.

"Our mission is to bring free knowledge for all the world, for everybody, for free," he said. "And this is a gathering of developers working to improve Wikipedia system projects, and developer tools that allow us to create, promote and distribute content in a better way."

As a case in point, Gil cited one solution presented at the forum developed to assist users with poor vision.

"One of the projects we demonstrated here is a gadget that will allow people with impaired vision to be able to read pages with increased font and with higher contrast than regular Wikipedia," he said.

Another development featured an editing app for Android, which allows users to make edits and add citations from their smart phones.

"Using a tiny mobile interface to review a huge document will allow people to select a word or sentence and then be given an option just to edit that one sentence," he said. "For us this is critical, because Wikipedia wouldn't be what it is if readers didn't become editors at some point."

Indeed, Gil emphasized that ensuring that users are capable of adding and correcting content in real time, from any mobile device, is instrumental to the nonprofit company's ongoing success.

"Users are welcome to use Wikipedia, but if a percentage of those users see a typo or a missing date, them being able to fix it is what makes Wikipedia what it is," he said.

Asked about the dangers of users who post false or libelous content on the platform, Gil responded that another project developed at the conference addressed that issue by applying artificial intelligence to prevent such abuses.

And despite the event's steep competition, Gil noted that a prize is not presented to the most industrious developer.

"We had 40 projects demonstrated that didn't exist three days ago," he said. "We are not really into number ones', we are a community of collaboration and longtime relationships. This is how we work."

Yuri Astrakhan, a senior software engineer for Wikimedia Foundation, who was born and Russia and has lived in New York for 25 years, said he presented a solution for storing more data on Wikipedia.

"I worked on a way to store structured data so that when you make an interactive graph or chart or a map, you can store the data in a structured way and reuse it for multiple articles," he said.

Aaron Halfaker, a senior research scientist for the foundation, said the major attraction for participants is the concept of "open knowledge."

"This is a lot of people who are really interested in the idea of open knowledge, and the way that they can contribute to it most effectively," he said.

Gil said next year's Wikimedia Foundation's Hackathon will be hosted in Austria.

Associated Press
State Dept. delays Clinton email review amid FBI probe
Saturday, 02 April 2016
Byline: Matthew Lee

The State Department has suspended its internal review into whether former Secretary of State Hillary Clinton or her top aides mishandled emails containing information now deemed "top secret." Spokeswoman Elizabeth Trudeau said Friday the department had paused the review to avoid interfering with an ongoing FBI investigation into Clinton's use of a private server while she was America's top diplomat.

She said the decision was made after the department sought the FBI's advice on how to proceed with the review and received word that it should follow its standard practice.

Trudeau said the department's standard practice is to place internal reviews "on hold while there is an ongoing law enforcement investigation underway."

"Of course, we do not want our internal review to complicate or impede the progress of their ongoing law enforcement investigation," Trudeau said.

Trudeau said the department would "reassess next steps" in the internal review process when the FBI completes its probe.

The department began the internal review in January when it announced that it had classified 22 emails that Clinton sent or received as top secret.

None of the emails was marked classified at the time it was sent.

One aspect of the internal review, conducted by the bureaus of Diplomatic Security and Intelligence and Research, was to investigate whether any of the information in the emails was classified at the time of transmission.

The review could result in counseling, warnings or other action against employees if it finds the information was mishandled.

Wall Street Journal
FBI Offers Help to Agencies On Phones
Saturday, 02 April 2016
Byline: Devlin Barrett

WASHINGTON -- The Federal Bureau of Investigation told law enforcement agencies around the country Friday it would try to help them open locked phones or other devices as much as "legal and policy constraints" allow.
The unusual guidance from the nation's premier law- enforcement agency is in response to a surge of interest from state and local authorities in how the agency was able to open a locked iPhone seized in the probe of a terror attack in San Bernardino, Calif., in December.

The FBI advisory seems to be aimed at reassuring police and prosecutors that while they don't have much to tell them now, they hope to provide more information and possibly help in the near future.

For months, the FBI had been unable to open the phone -- a 5C model -- and was engaged in a high stakes legal battle with Apple Inc. trying to force the company to help open the device. The Justice Department ended that legal battle this week, when it announced a third party outside the U.S. government had shown them a new means of cracking the phone.

"That method for unlocking that specific iPhone proved successful," the FBI missive said, adding that the agency is aware the difficulty of accessing locked data in criminal probes "is a substantial state and local law enforcement challenge that you face daily."

The FBI is now testing to see whether the method used in the San Bernardino case may work against over types of iPhones, say people familiar with the matter.

While the government says it needs to be able to look inside such devices when it has a warrant, Apple and other tech companies argue that even with a warrant it is wrong to force them to create new weaknesses in their systems that could expose millions of customers to hacking or snooping.

The FBI letter goes on to pledge an "open dialogue" with local officials, ending: "We are in this together."

Washington Post
FBI weighs if it can share hacking tool with local law enforcement
Saturday, 02 April 2016
Byline: Ellen Nakashima and Adam Goldman

The FBI and Justice Department are debating whether the hacking tool that helped the bureau unlock the iPhone of one of the San Bernardino, Calif., terrorists can be used to help state and local law enforcement, officials said Friday.
That will be a challenge because the bureau has classified the tool, making it difficult to use in state and local criminal prosecutions requiring disclosure of evidence to defendants, officials said.

"There's a desire to be forward-leaning to help state and local law enforcement," said a senior law enforcement official, who, like others, spoke on the condition of anonymity to discuss an ongoing investigation. "But no one knows quite what the answer is."

Moreover, the tool itself likely will have a shelf life of only a few months, as tech companies may find and fix the vulnerabilities that the tool exploits, and they periodically update the under-lying software.

The firm that helped the bureau -- not the Israeli company Cellebrite, as had been widely rumored -- charged a one-time flat fee, officials said.

The bureau is not releasing the company's name and has declined to discuss details of the solution. Officials last week said the approach was aimed at dismantling security features on the iPhone 5C to permit investigators to make many attempts to crack the passcode without wiping data from the device.

Since its announcement, the bureau has been peppered with inquiries from state and local law enforcement officials seeking to know whether the solution might be useful for their cases.

Manhattan District Attorney Cyrus R. Vance Jr. was among those who called. But, he said, he recognized that the solution itself may not be applicable to the more than 200 iPhones that he has sitting in a crime lab and his technicians cannot unlock.

None is a 5C running iOS 9, which is the model and operating system of the phone used by Syed Rizwan Farook, who was killed by police in December after a shooting attack that claimed 14 lives.

"The overwhelming majority of criminal investigations stalled by default device encryption will remain so until Congress intervenes," Vance said.

One-off technical solutions will result in a "cat-and-mouse cyber arms race" between the government and industry, he said in an interview. "I don't think that's the smart way to approach public safety or privacy policy."

The classification of the method highlights a tension between criminal and national security cases in which the most sophisticated tools are not always available to law enforcement. Unlike state and local courts, federal courts have procedures to protect classified information.

"It's been a challenge for law enforcement for a while," said Austin Berglas, a former assistant special agent in charge of the FBI's New York cyber branch and now head of cyber investigations at K2 Intelligence, a consultancy firm.

Berglas has worked cases on both sides of the divide, including one federal cybercrime investigation in which he was not given permission to use a classified tool because intelligence officials feared it would be disclosed in court.

"The FBI is very prudent when deploying the technologies," Berglas said. "The question is: Is it going to help the greater good by using this? Knowing that we may never have the ability to use this capability against the adversary again, are we willing to take that risk and use it?"

To referee the issue, the government has an interagency process headed by the attorney general to decide which capabilities should be classified. This is separate from the "vulnerabilities equities process" managed by the White House, which decides which software flaws should be disclosed to the software maker.

Now that the bureau owns the solution, it could conceivably have a local agency submit a phone to be unlocked to see if the solution works on it. But there would be constraints. For instance, the FBI likely would not testify about the tool in court, and the local agency would likely have to avoid using data retrieved from the phone as evidence in a criminal prosecution.

"So it would depend on how heavily that evidence weighs in that case. If it's a small part, maybe they can build a case around it," the senior official said. If not, he said, the tool is not for them.

Peter Modafferi, chief of detectives of New York's Rockland County, said he does not fault federal authorities for keeping some of their tools on a high shelf. "That's life," he said. "The bureau goes out of its way to help us when they can, but there's a difference between national security and local law enforcement."

Sunday Times (UK)
Threats spur Djibouti to sue Facebook (Canada)
Sunday, 03 April 2016
Byline: Mark Tighe

The president of Djibouti wants an Irish High Court judge to order Facebook to delete three accounts he alleges have been used to make death threats and threats of violence against him and his family. Ismail Omar Guelleh, known as IOG in the small East African country he has led since 1999, has applied for a High Court injunction against Facebook Ireland. The case is due for mention on April 11 in the chancery list, where business disputes are decided. Maki Omar Abdoulkadar, Djibouti's director of public prosecutions, has filed an affidavit in the case in support of his president's application.

Facebook Ireland is designated as the data processor for all account holders not resident in America or Canada. Guelleh's case is the first time a foreign individual has brought a legal action in Ireland seeking to compel Facebook to take action about material hosted by the social network. The Sunday Times has established that last year Guelleh brought an action against Facebook France and Facebook Inc in Paris in a bid to have the same three accounts suspended and the individual behind them identified.

Facebook appealed against a Paris judge's finding in Guelleh's favour in the French Court of Appeal, where it lost on most grounds. The company paid a fine rather than disclose the identity of the account holder.

The accounts use variations of the username Ainan Ainan, an anti-Guelleh activist who claims to live in Brussels.

One of Ainan Ainan's posts quoted in the French judgment spoke about Guelleh "losing a leg or two" or "an eye or two".

The post described the president as a "pirate". "Soon he will be punished , even if he fled ... he will be captured or die. [in English] Dead or alive".

Another post, partly in English and French, referred to Guelleh and said: "we'll be everywhere. To kill you." The post called on people to stop their pacifism and march against Guelleh's regime.

In its appeal in the French case, Facebook argued that the French judges had exceeded their power and complained that their actions in ordering the closure of accounts was disproportionate with respect for freedom of expression.

It also argued that although the accounts were in the French language and Djibouti is a former French colony, the proper jurisdiction was in Ireland where Facebook Ireland was subject to Irish data protection laws.

Guelleh's complaint sought damages of 85,000 from Facebook including a 20,000 fine for not taking down the accounts. He said that the accounts defamed him, and threatened his life and the physical safety of his family. Despite his efforts Facebook had refused to close the "illegal" accounts, he said.

The Court of Appeal fined Facebook 5,000 and 1,000 a day for three months for failing to close the accounts.

Djibouti is strategically important because of its location on the Horn of Africa near shipping lanes and areas where Islamist terrorists are active on the Arabian peninsula.

Reporters Without Borders ranks Djibouti 170 out of 180 countries in its annual world press freedom index. Guelleh, is campaigning to be re-elected president in an election this Friday. He is expected to be returned for a fourth term.

Reporters Without Borders said that this year, Mohamed Ibrahim Waiss, who works for La Voix de Djibouti, an opposition online radio station outside the country, was beaten by police and made to surrender his Facebook usernames and passwords so his account could be used to post images insulting the opposition. A US State Department report of 2013 noted that government forces monitor social media and police visit those who post antigovernment messages.

Maydaneh Abdallah Okieh, a journalist and activist, was sentenced to 45 days in prison and fined 1,000 after he posted photographs on Facebook of police breaking up a demonstration. On appeal, the court increased his sentence to five months.

This year, a London judge ruling on a case brought by Djibouti called Guelleh's regime "capricious", "cavalier" and on occasions "reprehensible".

Reuters
FBI trick for breaking into iPhone likely to leak, limiting its use
Sunday, 03 April 2016
Byline: Staff reporter

SAN FRANCISCO - The FBI's method for breaking into a locked iPhone 5c is unlikely to stay secret for long, according to senior Apple Inc engineers and outside experts.
Once it is exposed, Apple should be able to plug the encryption hole, comforting iPhone users worried that losing physical possession of their devices will leave them vulnerable to hackers.

When Apple does fix the flaw, it is expected to announce it to customers and thereby extend the rare public battle over security holes, a debate that typically rages out of public view.

The Federal Bureau of Investigation last week dropped its courtroom quest to force Apple to hack into the iPhone of one of the San Bernardino shooters, saying an unidentified party provided a method for getting around the deceased killer's unknown passcode.

If the government pursues a similar case seeking Apple's help in New York, the court could make the FBI disclose its new trick.

But even if the government walks away from that battle, the growing number of state and local authorities seeking the FBI's help with locked phones in criminal probes increases the likelihood that the FBI will have to provide it. When that happens, defense attorneys will cross-examine the experts involved.

Although each lawyer would mainly be interested in whether evidence-tampering may have occurred, the process would likely reveal enough about the method for Apple to block it in future versions of its phones, an Apple employee said.

"The FBI would need to resign itself to the fact that such an exploit would only be viable for a few months, if released to other departments," said Jonathan Zdziarski, an independent forensics expert who has helped police get into many devices. "It would be a temporary Vegas jackpot that would quickly get squandered on the case backlog."

In a memo to police obtained by Reuters on Friday, the FBI said it would share the tool "consistent with our legal and policy constraints."

Even if the FBI hoards the information - despite a White House policy that tilts toward disclosure to manufacturers - if it is not revealed to Apple, there are other ways the method could come to light or be rendered ineffective over time, according to Zdziarski and senior Apple engineers who spoke on condition of anonymity.

The FBI may use the same method on phones in cases in which the suspects are still alive, presenting the same opportunity for defense lawyers to pry.

In addition, the contractor who sold the FBI the technique might sell it to another agency or country. The more widely it circulates, the more likely it will be leaked.

"Flaws of this nature have a pretty short life cycle," one senior Apple engineer said. "Most of these things do come to light."

The temporary nature of flaws is borne out in the pricing of tools for exploiting security holes in the government-dominated market for "zero-days," called that because the companies whose products are targets have had zero days' warning of the flaw.

Many of the attack programs that are sold to defense and intelligence contractors and then to government buyers are purchased over six months, with payments spaced apart in case the flaw is discovered or the hole is patched incidentally with an update from the manufacturer, market participants told Reuters.

Although Apple is concerned about consumer perception, employees said the company had made no major recent changes in policy. Instead, its engineers take pride in the fact that a program for breaking into an iPhone via the web was recently purchased by a defense contractor for $1 million, and that even that program is likely to be short- lived.

They said most iPhone users have more to fear from criminals than from countries, and few crooks can afford anything like what it costs to break into a fully up-to-date iPhone.

Wall Street Journal
China's ZTE to Replace Three Senior Executives
Sunday, 03 April 2016
Byline: Juro Osawa

HONG KONG--ZTE Corp.'s board will meet early next week to replace three of its most senior executives, including its chief executive, people familiar with the matter said, as the Chinese telecommunications-equipment maker tries to rebuild its reputation after being accused of violating of U.S. trade rules. Chief Executive Shi Lirong, who has been in the role since 2010, as well as executive vice presidents Tian Wenguo and Qiu Weizhao, will step down pending board approval, the people said. Chief Technology Officer Zhao Xianming is expected to assume the role of CEO and chairman, they said.

On Tuesday and Wednesday, the board plans to discuss and approve the management changes as well as ZTE's 2015 financial results, which were delayed after the U.S. Commerce Department slapped trade sanctions on the company last month, alleging it violated rules by exporting American technological goods to Iran and other nations.

As part of a recent agreement between the U.S. Commerce Department and ZTE to temporarily remove the sanctions, the Chinese company's executives who have been involved in the alleged violation must be removed from management roles, the people said.

In a 2011 ZTE internal document obtained and disclosed last month by the U.S. government, Mr. Tian and Mr. Qiu were named as executives who were in charge of ZTE's plans for allegedly circumventing U.S. export rules. The document detailed the Chinese firm's elaborate plans to set up shell companies to ship goods to Iran without getting caught by U.S. authorities.

ZTE didn't make the executives available for comment.

The shake-up in ZTE's top management comes after the U.S. Commerce Department recently agreed to lift the sanctions on a temporary basis as long as the company stays true to the commitments it has made with the U.S. government. The sanctions, which blocked ZTE's access to supplies of U.S. components and software, threw the Chinese firm's business into doubt and created a new source of tension between Washington and Beijing. China's commerce minister responded by expressing "strong dissatisfaction" with the situation.

ZTE, which has roughly 80,000 employees globally, is a major global supplier of telecom networking-equipment such as wireless base stations and antennas. Over the past few years, its smartphone business has also gained a substantial presence in the U.S., where it was ranked fourth with a 7.2%

market share last year, behind Apple Inc., Samsung Electronics Co. and LG Electronics Inc., according to research firm Canalys.

ZTE is renewing its management as it scrambles to keep its business moving. ZTE will release its full-year earnings Wednesday after postponing the announcement last month, the people said. Trading in ZTE's Hong Kong-listed shares, suspended since March 7, is expected to resume Thursday, the people said.

Some of the company's component suppliers that had temporarily halted shipments with the company last month are resuming their shipments, according to people familiar with the matter.

ZTE is also planning to release its new flagship smartphone called the Axon 2 in mid-May, after delaying its previous plans to launch the phone in April, people familiar with the matter said.

In January, ZTE said it expects to report a 44% increase in 2015 net profit to 3.78 billion yuan ($583 million) and revenue to rise 24% to 100.8 billion yuan, based on preliminary unaudited results.

Had the sanctions stayed in place longer, the impact would have been disastrous for ZTE, analysts said.

In a letter sent to ZTE employees March 8, when the U.S. sanctions took effect, Mr. Shi described the situation as a "crisis" and said the company had set up a special team of executives to handle the issue. The U.S. restrictions hindered ZTE's ability to procure not only components manufactured in the U.S., but also those manufactured overseas based on U.S. technology, according to lawyers specializing in U.S. export control laws.

The Mirror
RAF's new 'GCHQ in the sky' spy planes which can hack enemy emails and phone calls
Sunday, 03 April 2016
Byline: Nigel Nelson

The MoD has bought nine Boeing P-8 Poseidon aircraft to replace the Nimrod spy planes contrioversially scrapped in 2010
Air chiefs have bought nine spy planes, each one like a flying GCHQ .

The Boeing P-8 Poseidon is as effective at information -gathering as the Government's eavesdropping headquarters.

It can hack terrorists' mobile calls and emails, track and -monitor enemy movements and direct our fighter jet response.

The RAF is believed to be spending £2.6billion on buying and maintaining the P-8s, -regarded as the world's most -hi-tech spy planes.

The fleet will also guard Britain's shipping lanes, protect the Navy's aircraft carrier and nuclear submarines.

Britain has had no maritime spy plane since the controversial 2010 scrapping of the Nimrod MR4A by the Government.

Since then Russian combat jets and nuclear-powered subs have encroached into British air and waters almost weekly.

The P-8 is so advanced it can identify an enemy sub's -periscope from several thousand feet.

Read more: Tories order spy planes that don't work with RAF's in-flight refuelling system

Its sensors and radars are so precise it will detect, classify and identify ships and small -vessels. It can also track subs.

And it is sophisticated enough to direct our jets and -surveillance drones on to targets approaching the UK.

The spy-in-the-sky is also one of the most deadly planes in the air as it can carry a lethal -battery of missiles, anti-submarine -torpedoes, bombs, depth charges and mines.

The aircraft, with two pilots and seven intelligence experts, has a range of about 1,200 miles with a 500mph cruising speed. It can also hover 200ft over a target for up to four hours during -sub-hunting operations.

The P-8, already used by the Australian, US, Indian and New Zealand air forces, will be -delivered to the RAF by 2020.

Defence chiefs scrapped a new generation of Nimrods in 2010 as part of MoD cuts.

Over £3.8billion of taxpayers money had been spent on the programme, which was £789million over budget and was nine years late.

When the Nimrod costs are added to the £250million per P-8, the cost of each plane rises to over £650million.

A defence source told the Sunday People : "The cancellation of the Nimrod -programme had effectively given Russian subs and aircraft a "free pass" to enter UK waters.

"Barely a week passes without some Russian ship, aircraft or sub trying to enter British -shipping lanes or airspace."

An MoD spokesman said: "We are committed to buying P-8 aircraft, which will be based at RAF Lossiemouth.

"The full cost of programme is yet to be determined."

Weapons: Freefall bombs, Harpoon anti-ship missiles, supersonic low-altitude -missiles (SLAM), land attack missiles, depth charges, sonar buoy torpedoes.

Range: 1,200 miles

Speed: Max 564mph

Cruising: 506mph

Dimensions: Length 129ft Wingspan: 117ft Weight: 62.7tons

Crew: Pilot and co-pilot plus seven console operators

Engines: 2 x CFM56-7B -turbofans.

Radar/surveillance: Electro- optical infrared -sensor can ID, track and -engage several targets - from land vehicles, aircraft, and ships. Can hack mobiles, emails and encrypted -communications. Advanced magnetic anomaly detection system for sub tracking.

USA Today
Pentagon to Panama Papers, a history of leaked data
Tuesday, 05 April 2016
Byline: Elizabeth Weise

The 11.5 million leaked documents from the Panamanian law firm Mossack Fonseca are providing a treasure trove of data on a hidden world of offshore accounts and murky dealings.
Expect more such leaks in the future.

"It's becoming much easier than it used to be to store and move very large amounts of data. I would expect this to continue," said John King, a professor of information at the University of Michigan in Ann Arbor.

The history of such leaks shows a steady increase in their depth and breadth, as information technology has become more sophisticated and allowed more data to be captured and revealed by leakers.

In 1948, spy Whittaker Chambers famously hid two rolls of microfilm in a hollowed-out pumpkin in a pumpkin patch. The film contained just 58 images of State and Navy Department documents.

By 1969, anti-war activist Daniel Ellsberg spent multiple nights laboriously making photocopies of the so-called Pentagon Papers, a 700-page report by the Department of Defense covering U.S. decision- making in Vietnam. Excerpts were eventually published in The New York Times and the Washington Post.

WikiLeaks has published nearly 500,000 documents leaked by hackers who attacked Sony Pictures Entertainment on Thanksgiving of 2014.

In 2013 Edward Snowden leaked more than 1.5 million documents from the National Security Agency to the press. What are being called "the Panama Papers" contain 10 times that amount.

The documents are estimated to contain about 2.6 terabytes of data, according to the Suddeutsche Zeitung, the German newspaper that first obtained them. It's not that much data. Ten terabytes would be about 260 HD movies. Today, big-box stores routinely sell solid-state drives that hold 3 terabytes of data and are just a little thicker than a smartphone.

Moving that much data surreptitiously out of a network also isn't that hard. "If you have the time, you can remove an enormous amount of data in not very much elapsed time because you can take it in chunks," King said.

According to a report by cyber security firm Mandiant, the median number of days hackers spend inside a system before they're discovered was 205 in 2015. Of course, that depends on the network, whether the people who own it are watching and what kinds of movement they are used to seeing.

"Transferring 11 terabytes of data wouldn't even be noticed on the Netflix or Amazon networks, but would stand out pretty quickly most other places," said Jonathan Sander, vice president of Lieberman Software, a cyber security firm based in Los Angeles.

The Intercept
A Key Similarity Between Snowden Leak and Panama Papers: Scandal Is What's Been Legalized
Tuesday, 05 April 2016
Byline: Glenn Greenwald
Section: column

FROM THE START of the reporting based on Edward Snowden's leaked document archive, government defenders insisted that no illegal behavior was revealed. That was always false: Multiple courts have now found the domestic metadata spying program in violation of the Constitution and relevant statutes and have issued similar rulings for other mass surveillance programs; numerous articles on NSA and GCHQ documented the targeting of people and groups for blatantly political or legally impermissible purposes; and the leak revealed that President Obama's top national security official (still), James Clapper, blatantly lied when testifying before Congress about the NSA's activities -- a felony.
But illegality was never the crux of the scandal triggered by those NSA revelations. Instead, what was most shocking was what had been legalized: the secret construction of the largest system of suspicionless spying in human history. What was scandalous was not that most of this spying was against the law, but rather that the law -- at least as applied and interpreted by the Justice Department and secret, one-sided FISA "courts" -- now permitted the U.S. government and its partners to engage in mass surveillance of entire populations, including their own. As the ACLU's Jameel Jaffer put it after the Washington Post's publication of documents showing NSA analysts engaged in illegal spying: "The 'non-compliance' angle is important, but don't get carried away. The deeper scandal is what's legal, not what's not."

Yesterday, dozens of newspapers around the world reported on what they are calling the Panama Papers: a gargantuan leak of documents from a Panama-based law firm that specializes in creating offshore shell companies. The documents reveal billions of dollars being funneled to offshore tax havens by leading governmental and corporate officials in numerous countries (the U.S. was oddly missing from the initial reporting, though journalists vow that will change shortly).

Some of these documents undoubtedly reveal criminality: either monies that were illegally obtained (and are being hidden for that reason) or assets being concealed in order to criminally evade tax debts. But the crux of this activity -- placing assets offshore in order to avoid incurring tax liability -- has been legalized. That's because Western democracies, along with overt tyrannies, are typically controlled by societies' wealthiest, and laws are enacted to serve their interests. Vox's Matt Yglesias this morning published a very good explainer of various aspects of this leak and he makes that point clear:

Even as the world's wealthiest and most powerful nations have engaged in increasingly complex and intensive efforts at international cooperation to smooth the wheels of global commerce, they have willfully chosen to allow the wealthiest members of Western society to shield their financial assets from taxation (and in many cases divorce or bankruptcy settlement) by taking advantage of shell companies and tax havens.

If Panama or the Cayman Islands were acting to undermine the integrity of the global pharmaceutical patent system, the United States would stop them. But the political elite of powerful Western nations have not acted to stop relatively puny Caribbean nations from undermining the integrity of the global tax system -- largely because Western economic elites don't want them to. ...

... But even though various criminal money-laundering schemes are the sexiest possible use of shell companies, the day-to-day tax dodging is what really pays the bills. As a manager of offshore bank accounts told me years ago, "People think of banking secrecy as all about terrorists and drug smugglers, but the truth is there are a lot of rich people who don't want to pay taxes." And the system persists because there are a lot of politicians in the West who don't particularly want to make them. ...

... Incorporating your hedge fund in a country with no corporate income tax even though all your fund's employees and investors live in the United States is perfectly legal. So is, in most cases, setting up a Panamanian shell company to own and manage most of your family's fortune.

Tax avoidance is an inevitable feature of any tax system, but the reason this particular form of avoidance grows and grows without bounds is that powerful politicians in powerful countries have chosen to let it happen. As the global economy has become more and more deeply integrated, powerful countries have created economic "rules of the road" that foreign countries and multinational corporations must follow in order to gain lucrative market access.

Proving that certain behavior is "legal" does not prove that it is ethical or just. That's because corrupted political systems, by definition, often protect and legalize exactly the behavior that is most unjust. Vital journalism does not only expose law breaking. It also highlights how corrupted political and legal systems can be co-opted by the most powerful in order to legally sanction atrocious and destructive behavior that serves their interests, typically with little or no public awareness that it's been done.

In such cases, as Jaffer put it, "The deeper scandal is what's legal, not what's not." The key revelation is not the illegality of the specific behavior in question but rather the light shined on how our political systems function and for whose benefit they work. That was true of the Snowden leak, and it's true of the Panama Papers as well.

Le Figaro
La sécurité aérienne à l'épreuve de la technologie
Tuesday, 05 April 2016

Byline: Véronique Guillermard

Quinze ans après sa création, l'Agence européenne de la sécurité aérienne (EASA) veut élargir son champ d'intervention. Elle a déposé une demande en ce sens auprès de sa tutelle, l'Union européenne. « Le monde a beaucoup changé depuis 2002, les technologies évoluent très vite et de nouveaux sujets de sécurité et de sûreté aériennes sont apparus. Nos missions doivent évoluer » , a expliqué Patrick Ky, directeur exécutif de l'EASA, lors d'un débat organisé par le magazine Air & Cosmos .
Drones, big data, cybersécurité... sont quelques-uns des nouveaux domaines dans lesquels l'EASA aura des responsabilités à partir de 2017. Elles s'ajouteront à ses missions historiques de certification des appareils européens, d'écriture du règlement européen de sécurité aérienne et au contrôle de son application.

Des avions « hackés »

Bruxelles a demandé à l'agence de travailler sur les drones civils. L'EASA a été chargée d'écrire « une opinion technique » qui doit servir de base à un futur règlement européen. Les incidents entre drones et avions de ligne se multiplient, comme l'a démontré la collision évitée de justesse entre un drone et un Airbus A 320 à l'approche de Roissy début mars. Aux États-Unis, les incidents sont quasi quotidiens. Le 19 mars, un drone a frôlé un A 380 de la Lufthansa à l'aéroport de Los Angeles. « Pour le moment, la compétence de l'EASA est circonscrite aux drones de plus de 150 kg mais elle sera étendue en 2017. À côté de la mise en place de règles communes en Europe, nous discutons avec les avionneurs et les motoristes. Nous pourrions demander des tests d'ingestion de drone par un avion de ligne et des mesures d'impact de drone sur la verrière d'un cockpit par exemple » , développe Patrick Ky.

Autre chantier auquel s'est attelé l'EASA, la construction « d'une compétence big data » . L'idée est de réunir toutes les données des vols européens, recensant notamment les incidents, et de les analyser afin de modéliser les zones à risque pour les avions commerciaux. Ils sont de plus en plus nombreux - comme le vol MH17 détruit par un missile au-dessus de l'Ukraine en juillet 2014 - à survoler des régions en crise (guerre, terrorisme...). L'EASA doit rattraper son retard sur la FAA, son homologue américaine, qui s'est dotée d'un système de big data, baptisé « Asias » . « Les Américains nous ont proposé de gérer et traiter nos données dans leur centre. Mais comme Asias dépend du ministère de la Défense américain, nous avons décliné. Il est stratégique pour l'Europe de construire son propre système de big data » , insiste le directeur exécutif. Pourtant, la Commission n'est pas disposée à débloquer les 50 millions d'euros nécessaires. Du coup, Patrick Ky envisage de faire appel à l'industrie dans le cadre d'un partenariat public-privé.

L'EASA avance aussi en matière de cybersécurité. Elle a mené « des études de vulnérabilité » édifiantes. Elles démontrent que les avions peuvent être piratés au sol ou en vol. Un expert de l'agence doué en informatique et titulaire d'une licence de pilote est parvenu à pénétrer, en quelques minutes, dans le système de messagerie (Acars) d'un avion. Et il ne lui a fallu que deux ou trois jours pour entrer dans son système de contrôle au sol.

Yonhap News Agency
N. Korea's GPS jamming targeted at aircraft navigation system: official
Tuesday, 05 April 2016

Seoul - North Korea's continuing attempts to jam South Korea' Global Positioning System (GPS) may be aimed at disrupting the navigation systems of aircraft, government officials said as the communist country continued to send jamming signals on Tuesday.
In a provocative operation that started in late March, North Korea has been sending GPS-jamming signals across the border. The signals began last Thursday and continued on and off into Tuesday, according to military and information and communication technology (ICT) sector officials.

"An assessment showed that North Korea's near daily GPS-jamming activity seems to be targeting aircraft's navigation equipment," an intelligence source said, asking not to be named.

But the North Korean operation has not yet resulted in any trouble with South Korea's aircraft because they use both GPS and an inertial navigation system that is immune to jamming attacks, the official said.

In the GPS disruption campaign so far, the North has sent jamming signals on a total of 100 occasions and their maximum output reached more than 45 decibels, the official said.

The strength of the signals are constantly lessening or increasing in what appears to be a new type of assault operation, according to the official.

The country's ICT ministry said the jamming attack has not led to any major GPS disruption locally as of Tuesday, although a total of 962 airplanes have been exposed to the malicious signals.

Nearly 700 fishing ships have been subject to the signals as well, while a total of 1,786 mobile telecommunication base stations have been exposed.

Officials said North Korea had previously launched similar jamming assaults three times between 2010 and 2012, which partly disrupted the GPS-guided navigation of some 1,000 passenger jets as well as of the military's unmanned aerial vehicles.

Korea Herald
New dilemma on digital privacy
Tuesday, 05 April 2016
Byline: Lee Jae-min
Section: oped

We all know how devastating it is to lose a cellphone or tablet PC, as our daily life is entirely disrupted.

With so much personal information digitized and stored in one single device, the handheld gadget means the entire world for the owner. So, from the perspective of users, nothing would be more sensitive to their privacy than the information contained in this device.

On the contrary, for the law enforcement agencies a cell phone is an information bonanza. Make-or-break materials are stored on the device. Naturally, nothing provides sharper confrontation between national security and privacy than digital devices and cloud technologies. The digitalization cuts both ways.

As one of the most wired countries in the world, this issue is not new to Korea either. For almost two years now, law enforcement agencies and KakaoTalk, a South Korean messaging app, have been wrangling over the agencies' access to some of the tech company's messaging data. Knowing that almost 90 percent of South Koreans use the app for daily communication, the agencies have come to appreciate the value of digital information to be mined. In the company's eyes, however, such cooperation runs the risk of compromising consumers' privacy and causing a major dent to its business image.

When the FBI retrieved an iPhone used by a terrorist in San Bernardino last December, the agency knew that the smartphone would yield critical information about the events leading to the attack. But the device was encrypted and protected by a password and someone needed to break the code to get to the information inside.

The problem was, 10 incorrect password entries would cause the phone to destroy all the information stored on it. A strong safety feature indeed.

In order to retrieve the information safely, the agency asked Apple to decrypt the iPhone, but the company refused to cooperate, citing the risk of such technologies leading to the invasion of privacy of its consumers. Apple's continued rejection led to a seminal legal battle over national security versus privacy in the digital age. The legal confrontation has just ended, for better or worse, as the FBI succeeded in breaking the code with the help of hired experts.

These recent examples tell us that the cat-and-mouse games between law enforcement agencies and digital companies will continue, as new technologies will immediately emerge to deal with new vulnerabilities. Companies will continue to develop and apply stronger protection systems for the information of their consumers. With that, the demand from law enforcement agencies for help and cooperation to break down security walls will equally escalate. So this issue stands to intensify over time.

Yet, reliable guidelines are yet to come that balance the state's interest for national security and individuals' interest for privacy in the new landscape of the digital age.

What applies now in this field is simply the rules developed from the days of papers and documents collected and stored by corporations, or the days of getting cooperation from phone companies for wiretapping. These conventional rules do not necessarily fit with cyber networks and devices connecting people participating in the networks. Rapid advances in technology are raising new issues in this field as well.

When confronted with this issue, people tend to have a mixed feeling. On the one hand, they release a sigh of relief because the key information has been retrieved to preserve national security. On the other, they raise their eyebrows as their messages and conversations deep inside the smartphones can be broken into and retrieved by outsiders.

We are playing both sides of this fence. Notably, to deal with this new dilemma some countries have initiated a constructive discussion between law enforcement agencies and tech companies in order to explore a new legislation. This is a new development that we need to pay attention to.

Lee Jae-min is a professor of law at Seoul National University. -- Ed.

Associated Press
Data of nearly 50 million Turks allegedly leaked online
Tuesday, 05 April 2016

Hackers have posted a database online that seems to contain the personal information of nearly 50 million Turkish citizens in what is one of the largest public leaks of its kind.
The leaked database contains 49,611,709 entries and divulged considerable private information, putting people at risk of identity theft and fraud. Entries include data such as national ID numbers, addresses, birthdates and parents' names.

The hackers spotlighted the information for Turkish President Recep Tayyip Erdogan, his predecessor Abdullah Gül, and Prime Minister Ahmet Davuto?lu.

The leak came with the message: "Who would have imagined that backwards ideologies, cronyism and rising religious extremism in Turkey would lead to a crumbling and vulnerable technical infrastructure?"

In a message on the lessons to be learned by Turkey, the hackers said, "Bit shifting isn't encryption."

The hackers also dedicated their stunt to the U.S,. saying: "We really shouldn't elect [Donald] Trump, that guy sounds like he knows even less about running a country than Erdo?an does."

The site appears to be hosted by an Icelandic group that specializes in divulging leaks, using servers in Romania.

The Associated Press on April 4 was able to partially verify the authenticity of the leak by running 10 non-public Turkish ID numbers against names contained in the dump. Eight were a match.

In an era where hackers frequently gain access to sensitive information, the Turkish government is not alone in facing a major breach.

Among the most serious recent incidents, the U.S. government's Office of Personnel Management revealed in April 2015 that hackers gained access to the personal information of more than 22 million U.S. federal employees, retirees, contractors and others, and millions of sensitive and classified documents.

U.S. officials believe a Chinese espionage operation infiltrated OPM's records.

This Day
ICAO Moves to Avert Attacks in Nigeria, Cameroun, Egypt, Others (Canada)
Tuesday, 05 April 2016
Byline: Dele Ogbodo

Abuja - The President in Council of the International Civil Aviation Organisation (ICAO), Mr. Bernard Olumuyiwa Aliyu, has said the body is strategising with the Ministers of Aviation of Nigeria, Cameroun, Niger, Somali, Egypt and countries within the continent to stem any terrorist attack on their airports. One of the strategies, Aliyu said, would be the adoption of biometric passport or the e-passport to monitor closely the movement of passengers within and outside the region.

He admitted that ICAO had been having very close relationship with the Ministers of Aviation on aviation security challenges in Mali, Somali, Egypt and Nigeria, adding that aviation security was a very sensitive issue which ICAO cannot put in public domain.

The ICAO boss, who is seeking re-election bid for a second term, made the disclosure at a get-together dinner organised Sunday night in Abuja for him by the Minister of State for Aviation, Mr. Hadi Sirika.

He stated that ICAO was working hard to make the airports safe across Africa, adding that "bombing at airports is one of the critical issues that we are discussing at the moment," as he said ICAO and Nigeria would have to collaborate very closely on the matter.

He said: "Few months ago, I sent ICAO team to Nigeria and the neighbouring countries of Chad, Niger and Cameroun to do an assessment, and arising from that, we will strategies on new measures that we are going to implement.

"As I leave Nigeria, I will be going for aviation security and facilitation on Africa where they will all gather together at a meeting with ICAO and the African Civil Aviation Commission (ACAC) to chart the way forward.

"We shall raise the level of aviation security on the continent as well as the issues of facilitation and biometrics passport which we call the e-passport in order to monitor closely the movement of people and passengers in the region."

Aliyu alleged that corruption had impacted on the national economy and retarded the growth of the civil aviation, adding however that there was light at the end of the tunnel because of the present posture of President Muhammadu Buhari and his current fight against corruption.

"I'm hopeful for our country because of the posture and the determination of Buhari regarding his fight against corruption. This is the bane of our society that has impacted all aspects of the national economy including the civil aviation.

"I'm very hopeful now with the determination of the minister and the support that he is receiving from government, when he visited me in Montreal, Canada, I told him that we cannot afford to miss this opportunity.

"With me being at ICAO and he being the minister for aviation, we will put ICAO resources at the disposal of Nigeria in all its efforts to move the sector forward."

In his remark, Sirika, said government is committed to making sure that Aliu is re-elected as president of the council before the end of the year based on his experience and achievements that he has recorded in his first term.

He said: "We began his campaign for a second term and it was huge success and welcomed by every country and nation so far. When I spoke to the delegates of the United States and Canada about the representation of Aliu they told me that you cannot do any better."

Canadian Press
Panama Papers leaks show change doesn't happen by itself, says Edward Snowden
Wednesday, 06 April 2016
Byline: Tamsyn Burgmann

VANCOUVER _ A trove of leaked data about offshore tax havens in Panama highlights more than ever the vital role of the whistleblower in a free society, says one of the tech era's most prominent figures to expose state secrets, Edward Snowden.
The former U.S. intelligence contractor said Tuesday that the so-called Panama Papers, which were given to journalists by an anonymous source, demonstrate that "change doesn't happen by itself."

"The media cannot operate in a vacuum and ... the participation of the public is absolutely necessary to achieving change," the ex-National Security Agency analyst said during a video conference from Moscow.

Snowden was speaking from exile on a panel organized by Simon Fraser University examining the opportunities and dangers of online data gathering.

The 32- year-old remains wanted by the U.S. government on charges of espionage after leaking classified documents in 2013 as evidence that government spy agencies were monitoring citizens' telecommunication.

The 11.5 million documents taken from the Panamanian law firm Mossack Fonseca reportedly reveal the offshore dealings of more than 100 politicians and public figures from multiple countries.

Snowden told more than 2,700 people at the Vancouver event that the 2.6 terabytes of data contained in the papers demonstrate the most privileged and powerful people in the world are operating by a different set of rules.

"It happens without our knowledge, without our awareness, without our consent," he said. "They don't even pay the same taxes as we do."

Reporters for a German newspaper obtained the volumes of data after they were approached by an unnamed individual about one year ago. The team sought help from the International Consortium of Investigative Journalists in Washington, D.C., which assembled 400 reporters in 80 countries to decipher the contents. The first reports were published on Sunday.

The moderator of the event asked Snowden whether the confidential source had reached out to him asking for advice on how to conduct the leak.

"If they had, I could not say one way or another, because that would be inappropriate," he replied, before adding with a laugh: "But, for they record, no, they have not."

Snowden joked throughout the one-and- a-half hour session, speaking in an animated style and often adjusting his glasses. He told the crowd it was 5 a.m. for him and he hadn't actually slept.

Within days of the Panama Papers' publication, Iceland's Prime Minister resigned. Sigmundur Gunnlaugsson stepped down earlier Tuesday following mass protests over revelations he had owned an offshore company with his wife.

Snowden lauded the "fruits of the investigation" but emphasized that global reform won't come in one night or as a result of a single protest.

"By developing a culture of transparency and accountability where we not only know what government is doing, but recognize that we have not just the right but the responsibility to actually act in changing the nature of government ... directly holds these individuals to account," he said.

"We can achieve change. And ultimately whether we do or not is a decision that falls to us."

Snowden has been livestreamed into Canada before. He made a surprise appearance at the 2014 TED Conference in Vancouver and spoke to high school students at Upper Canada College in Toronto in February 2015.

Globe and Mail
Snowden says Panama Papers show whistleblowers 'vital' to society
Wednesday, 06 April 2016
Byline: Sunny Dhillon

Vancouver - Edward Snowden, the former U.S. National Security Agency contractor responsible for the release of thousands of classified documents detailing the American government's use of mass surveillance, says the Panama Papers show the role of the whistleblower in a free society has become "vital."
Mr. Snowden, who is living in Russia under political asylum, made the comments via video link during a sold-out event hosted by Simon Fraser University on Tuesday night.

Mr. Snowden said the Panama Papers reveal "the most privileged and the most powerful members of society are operating by a different set of rules."

"I think that this shows, more than ever, the role of the whistleblower in a free society has become not only desirable but vital," he said.

The Panama Papers are a cache of 11.5- million records leaked from Mossack Fonseca, a Panamanian law firm that has been retained by politicians and business leaders around the world to channel money beyond their countries' borders and into tax havens through the use of offshore accounts.

The Prime Minister of Iceland stepped down Tuesday after he and his wife were said to have had an offshore account.

The International Consortium of Investigative Journalists has said the records reveal the offshore holdings of 140 politicians and public officials, and more than 200,000 shell companies in all.

Simply setting up offshore entities is not illegal and companies, as well as rich individuals, often do so to take advantage of perfectly legal tax loopholes or for other legitimate purposes. But offshore entities can also be used to illegally evade taxes or to launder or hide money.

Mr. Snowden, when asked by the event moderator if he had had any contact with the person who leaked the Panama Papers, said he had not.

He accused public officials of increasingly "creating a new paradigm."

"They're increasingly guarding knowledge of their operations, of their assets, of their interests," he said. "At the same time, through programs of mass surveillance revealed in recent years, we, the private citizens, are increasingly transparent to government. The relationship between the governing and the governed has become inverted. And rather than those who represent us in our government being accountable to us, we are now accountable to them."

Mr. Snowden, when asked about Canada's new anti-terror legislation, cited its connection to the United States and the Five Eyes intelligence alliance.

"You put everything in one big, giant bucket. I would suspect this is what C-51 is really about," he said. "It's about broadening that bucket and making sure we put more Canadian information in that sharing bucket, so that it's more easily shared. Now I don't want to say that it's absolutely what's happening, but ... this is how it works, this is what we do for every other country."

Mr. Snowden received a standing ovation at the end of the 90-minute event.

Tuesday's event, held at the Queen Elizabeth Theatre, was part of the SFU President's Dream Colloquium, which brings leading thinkers to the university. The event was also live-streamed online.

This was not the first time Mr. Snowden directly addressed a Canadian audience. He also spoke via web link to a crowd of more than 1,000 students at Toronto's Upper Canada College in February of last year.

Washington Times
ISIS Internet operation impossible to stop: U.S. commander
Wednesday, 06 April 2016
Byline: Rowan Scarborough

The nation's top military officer in charge of cyber warfare said on Tuesday that the U.S. is powerless to shut down the vast information network operated on the Internet by the Islamic State terror army. Like no other terrorist group, the Islamic State has embraced cyber space, and its associated messaging apps and platforms, to spread propaganda, recruit foreign killers and plan massacres, such as the March 22 attacks in Brussels.

At a Senate Armed Services Committee hearing, Sen. Joe Manchin asked Navy Adm. Michael S. Rogers, chief of U.S. Cyber Command, "why can't be shut down the part of the Internet. Why can't we interrupt ISIS's ability to go on social media and attract? Why aren't we able to infiltrate that more?"

"The idea you are going to shut down the Internet, given its construction and complexity, is just not [doable]," answered Adm. Rogers, who also directs the National Security Agency, which works to intercept ISIL's communications.

"I've had people ask me can't you just stop it in that area of the world where all the problems are coming from?" Mr. Manchin, West Virginia Democrat, asked, referring to ISIL's home turf of Iraq and Syria.

"It's just not that simple," Adm. Rogers said. "I wish I could say there is a part of the Internet that is only used by a specific set of users."

Adm. Rogers' public answer does not mean his agencies are not attacking ISIL in cyber space.

Defense Secretary Ashton Carter said in February that the U.S. is targeting various ISIL networks to disrupt activities. He said one tactic is to overload a network to force a crash, in what is Cyber Command's first publicly acknowledged war.

"We're trying to both physically and virtually isolate ISIL, limit their ability to conduct command and control, limit their ability to communicate with each other, limit their ability to conduct operations locally and tactically," said Mr. Carter.

The U.S., in an operation never publicly disclosed, developed malware that caused damage to Iran's nuclear weapons program.

ISIL uses not only the seeable public Internet, but also encrypted apps readily downloadable on the commercial market to link up with killers and potential recruits.

Adm. Rogers said the Internet is clearly a boon to ISIL.

"They've harnessed the power of the information arena to promulgate their ideology on a global basis to recruit on a global basis, to generate revenue, and to move money as well as to coordinate some level of activity on a larger dispersed basis," he testified.

"The challenge I look for, what concerns me when I look at the future, what happens if a non-state actor, ISIL being one example, starts to use cyber as a weapons system? That would really be a troubling development," the admiral said.

Washington Post
World's top messaging app now fully encrypted
Wednesday, 06 April 2016
Byline: Ellen Nakashima

WhatsApp, the world's most popular instant-message app with more than 1 billion users, is now fully encrypted on all platforms: Android, iPhone, BlackBerry and others.
That's good news for users who care about security and privacy, including journalists and dissidents. At the same time, it represents the intensification of a trend toward ubiquitous encryption that has posed challenges for law enforcement in the United States and around the world.

"The idea is simple: when you send a message, the only person who can read it is the person or group chat that you send that message to. No one can see inside that message. Not cybercriminals. Not hackers. Not oppressive regimes. Not even us," WhatsApp co-founders Jan Koum and Brian Acton wrote in a blog post Tuesday.

Such encryption, in which only the sender and receiver can decrypt messages, makes it virtually impossible for foreign governments and U.S. agencies to intercept instant messages and voice calls, even with a warrant.

WhatsApp, which is owned by Facebook, has frustrated federal investigators in criminal investigations, but the Justice Department has not taken the matter to court publicly in the way it did recently with Apple.

The Apple case involved data stored on an iPhone used by one of the terrorists in San Bernardino, Calif. By contrast, WhatsApp provides chat, group chat and voice call services to users - or "data in motion."

WhatsApp and Facebook are "great American companies," FBI General Counsel James A. Baker said Tuesday in a moderated discussion at a conference of the International Association of Privacy Professionals. But "this presents us with a significant problem."

If the trend continues, he said, "encryption like that will continue to roll out in a variety of different ways across the technological landscape," adding that the "genie's out of the bottle."

Some of it is good, Baker said, noting that his own data has been stolen by hackers a number of times and he wished that the data had been encrypted. "But the key thing is that it has costs."

His boss, FBI Director James B. Comey, has often said that the Islamic State is using encrypted apps to direct people to kill "innocent people" in the United States. And it is hindering investigations of murder, child pornography, organized crime and a range of other crimes, law enforcement officials said.

Still, Comey said at a congressional hearing last month: "It is not our job to tell the American people how to resolve that problem. . . . Our job is simply to tell people there is a problem."

But for WhatsApp and Open Whisper Systems, a group of software developers that has helped the company integrate the "end-to-end" encryption into its platform, the issues are security and privacy. "What we're doing is trying to make private communications simple," not thwart criminal investigations, said Moxie Marlinspike, founder of Open Whisper Systems.

Criminals and terrorists will use encryption regardless of what commercial firms do, he said. Some al-Qaeda-linked groups have released their own encryption platforms.

Koum and Acton said in their blog post: "While we recognize the important work of law enforcement in keeping people safe, efforts to weaken encryption risk exposing people's information to abuse from cybercriminals, hackers, and rogue states."

Koum, who is WhatsApp chief executive, said he has a personal stake in privacy. "I grew up in the USSR during communist rule and the fact that people couldn't speak freely is one of the reasons my family moved to the United States."

Open Whisper Systems developed the encryption protocol for WhatsApp - the same protocol used for an Open Whisper messaging app called Signal, which has millions of users. Over the next year, Open Whisper Systems will continue to work with additional messaging platforms to incorporate strong encryption, the group said.

Wall Street Journal
Facebook's WhatsApp Bolsters Encryption
Wednesday, 06 April 2016
Byline: Robert McMillan

Facebook Inc.'s WhatsApp texting service said it had strengthened its encryption so that only the sender and receiver are able to read the contents of messages.
WhatsApp has been working for more than a year to ensure the encryption works on different phone platforms and for different types of messages. On Tuesday, a spokesman said the more secure encryption is now available for all of the service's one billion users.

Facebook's move comes as the nation debates the uses and limits of encryption technology. Over the past month, Apple Inc. and the Federal Bureau of Investigation have been locked in a bitter struggle over the FBI's demands that Apple help unlock its mobile phones.

The FBI argues that it will be less effective without ways to tap into the communications of terrorists and criminals. Apple and other technology companies argue that encryption is essential to protecting consumer privacy.

The Justice Department suspended one case against Apple after saying it found another way to extract data from the phone of San Bernardino shooter Syed Rizwan Farook.

But roughly a dozen other cases are pending in federal court, and local prosecutors say they have hundreds of encrypted phones that are stymying investigations.

"We're sympathetic with Apple," Facebook Chief Executive Mark Zuckerberg said during a technology conference in February. "I don't think requiring back doors into encryption is either going to be an effective way to increase security or is really the right thing to do."

WhatsApp has been working on the project since late 2014, using encryption software built by Open Whisper Systems, a not-for-profit security-development group. In 2014, text messages were encrypted, but WhatsApp group messages and messages containing media, such as photos or videos, weren't encrypted.

Many Internet companies encrypt messages before they are stored on their servers, but they are typically able to decrypt them when necessary -- for example, in the case of a court order. With Open Whisper's technology, WhatsApp won't be able to read its customers' messages under any circumstances, a feature known as "end-to-end" encryption.

That will make it much harder for anyone -- including criminals, intelligence agencies and law enforcement -- to read WhatsApp messages without permission, said Moxie Marlinspike, founder of Open Whisper Systems.

USA Today
Chinese censors curb Panama Papers coverage
Wednesday, 06 April 2016

Byline: Roger Yu

China moved swiftly in reacting to reports and online chats about the Panama Papers leak, largely banning the topic and related search terms at news organizations and social media channels in the country.
A group of over 100 news organizations worldwide -- coordinated by the International Consortium of Investigative Journalists -- published stories Sunday about the inner workings of Panamanian law firm Mossack Fonseca, which helps politicians, businessmen, athletes and celebrities create offshore accounts for untraceable funds.

The political fallout from the consortium's investigative stories, based on 11.5million documents that were leaked anonymously, continued this week as Iceland's Prime Minister Sigmundur David Gunnlaugsson stepped aside Tuesday amid pressure.

Several prominent Chinese names appear in the documents, according to the ICIJ's report.

"The files reveal offshore companies linked to the family of China's top leader, Xi Jinping," the report said. "Family members of at least eight current or former members of China's Politburo Standing Committee, the country's main ruling body, have offshore companies arranged though Mossack Fonseca. They include President Xi's brother-in-law, who set up two British Virgin Islands companies in 2009."

The revelation will not be easy to find online for Chinese readers, though. Internet censors also blocked the stories by the ICIJ's and several of its publishing partners, including Spain's El Pas, France's Le Monde, Sddeutsche Zeitung in Germany, the Canadian Broadcasting Corp., and the United Kingdom and U.S. editions of The Guardian, according to ICIJ, citing reports from news organizations and analytics by GreatFire.org, which monitors Web censorship in China.

The People's Daily, an official daily newspaper of the Chinese Communist Party, and state broadcaster China Central Television have not reported on the affair, according to The Wall Street Journal.

A search for "Panama" on the website of the China Daily, an English daily in China, renders one wire story -- written by Agence France-Presse -- related to the investigation. Five stories related to the Panama Papers appeared on Xinhua's English website, but they referred to the scandals in Iceland, Spain and New Zealand.

Mossack says it "does not foster or promote illegal acts."

Washington Post
Spy probe morphed into child porn case

Wednesday, 06 April 2016
Byline: Ellen Nakashima

FBI agents entered Keith Gartenlaub's home in Southern California while he and his wife were visiting her relatives in Shanghai. Agents wearing gloves went through boxes, snapped pictures of documents and made copies of three computer hard drives before leaving as quietly as they had entered. The bureau suspected that Gartenlaub was a spy for China.

The FBI had obtained a secret search warrant to enter the house, citing national security grounds. The agents were searching for evidence that Gartenlaub, an information technology manager at Boeing, had leaked computer information about the defense contractor's C-17 military transport plane to people acting on behalf of China.

But since the search in January 2014, no spy or hacking charges have been brought against him.

Instead, seven months later, he was charged with the possession and receipt of child pornography. He has denied the charges, but a jury convicted him in December.

Gartenlaub's case highlights how exceptional powers given to the government in recent years to gather information about suspected terrorist or espionage threats without some of the traditional safeguards for a defendant's rights are now leading to charges in more routine criminal cases.

Over the past 15 years or so, the wall between U.S. intelligence officials and criminal prosecutors has fallen, making it easier for them to share information, especially to fight terrorism. And under the Foreign Intelligence Surveillance Act (FISA), defendants are generally unable to effectively challenge the warrants that authorized the search or surveillance because they are not permitted to see them or the underlying application on national security grounds.

Gartenlaub's attorneys are troubled that what began as an espionage case - one that resulted two weeks ago in a guilty plea by a Chinese businessman with no connection to their client - morphed into a child pornography prosecution.

In Gartenlaub's case, the government made sealed filings, so neither the defense nor the public was able to see them. Based on the secret filings, the judge held that the government had shown probable cause that the house to be searched belonged to "an agent of a foreign power" or a spy.

"There has, over the last decade-plus, been an erosion of the formerly bright line between foreign intelligence surveillance and investigation for criminal prosecution," said Jennifer Daskal, a former official in the Justice Department's national security division who teaches law at American University.

In criminal cases, by contrast, a defendant and his attorneys are generally entitled to see an affidavit for a warrant and challenge the grounds for its issuance before a judge. Gartenlaub wants to see the warrant in his case so he can challenge it as based on false information and therefore invalid.

"The government is increasingly using national security tools to investigate domestic criminal cases, bypassing key constitutional protections," said Patrick Toomey, a staff lawyer with the American Civil Liberties Union. "This problem is only compounded in the digital age, where the FBI is collecting vast amounts of our data for intelligence purposes but then goes sifting through all that information in unrelated criminal investigations."

In a case in Philadelphia last year, for instance, the government used a FISA order to obtain evidence on a Temple University professor who they apparently suspected was sharing technology with China, but they indicted him on garden-variety wire fraud charges before eventually dropping the case. In an Iowa case, the government used a FISA order to gather information about a Chinese businessman suspected of stealing patented corn seeds from farm fields. In 2013, he was indicted on charges of theft of trade secrets. He pleaded guilty this year to one count of conspiracy to steal trade secrets.

Federal prosecutors in Gartenlaub's case insist that they followed the law.

"The issue of the FISA warrant was the subject of an extensive pretrial briefing and an order from the judge finding that the orders were lawfully issued and did not violate the defendant's due process rights," said Thom Mrozek, a spokesman for the U.S. attorney's office in Los Angeles.

The judge specifically found that the pornography material "obtained pursuant to FISA was lawfully acquired" and did not violate the defendant's Fourth Amendment rights, he said. The court also found that "there is no indication of any false statements having been included in the FISA materials."

Mrozek said the fact that the child pornography case began as a national security investigation does not lessen its severity.

"When law enforcement lawfully obtains evidence of a serious crime, in this case a crime against children, we will pursue further investigation of that crime," he said.

Justice Department officials added that Congress has always intended that information obtained through intelligence authorities could be used in criminal prosecutions. "It would be irresponsible for the government to ignore evidence of criminal wrongdoing when such evidence is lawfully collected," said Justice Department spokesman Marc Raimondi.

In Gartenlaub's case, the defense unsuccessfully argued that he could not be linked to identical copies of child pornography videos found on four hard drives in his house. Two of the hard drives had been in a computer that was kept at a beach house where numerous people had access to it, Gartenlaub said.

"They claim I'm a spy and a pervert, and I'm neither one," Gartenlaub said in an interview from his home in Riverside County, a house he may not leave without permission while awaiting sentencing.

Jeff Fischbach, a forensic technologist for the defense, said there is no evidence that the child pornography was ever seen by anyone who used the computer, much less Gartenlaub.

The government's own forensic expert, Bruce W. Pixley, said he could not find any evidence of the material being downloaded onto any of the computers, the defense noted. That means it had to have been copied onto the computer - but by whom is unknown.

Prosecutors are seeking a 10-year prison term for Gartenlaub, who has asked Judge Christina A. Snyder of the U.S. District Court for the Central District of California to overturn the verdict or order a new trial. A hearing is scheduled for this month.

Gartenlaub, 47, was fired in August 2014 and has been unemployed since. His attorney said his defense was hampered by an inability to obtain basic information about how the evidence was obtained and on what specific grounds the warrant was issued.

"We've always cherished the right to confront and cross-examine our accusers and examine the evidence that's used as the basis for a search of our homes," said Mark J. Werksman, Gartenlaub's attorney. "And to be told, 'We went in. We had good reasons. We're not going to tell you why. Trust us,' is alarming. Especially when the case becomes a run-of-the-mill criminal case."

In February 2013, the FBI emailed Gartenlaub that it was investigating a data breach and wanted to talk to him. Over two days at Boeing's facility in Long Beach, Calif., and a third day at its Huntington Beach facility, agents interviewed Gartenlaub about the C-17 program; his team of engineers was also questioned. Two agents showed him a copy of an intercepted email. The communication described information on the C-17 that was apparently being sought by the Chinese.

Gartenlaub told them that he had no idea who wrote it or why.

The next time he heard about the C-17 was more than a year later, in June 2014, when he saw the news about the arrest of the Chinese businessman, Su Bin. When he reviewed Su's arrest warrant, he realized that the email excerpt he had been shown 16 months earlier had been sent by Su.

Still, Gartenlaub had no sense that he was a target. "Why would I think I would be under suspicion?" he said.

The only thing he could think was that his wife, who was born in China and became a U.S. citizen and was a member of an Orange County Chinese business association, somehow made the FBI suspicious.

In an affidavit for a warrant for the couple's emails, separate from the national security warrant, agent Wesley Harris stated that Gartenlaub was the "nationwide Unix military administrator for Boeing," suggesting that that position would allow him to log into C-17 data, Gartenlaub said.

According to two Boeing colleagues, who spoke on the condition of anonymity because they were not authorized to talk to the media, there is no such job at the company. And Gartenlaub was, in any case, an IT manager. Moreover, they said, the breached files were accessible through servers in the field, such as at Air Force bases. These were not servers that Gartenlaub or his team of engineers who supported the plane's designers had access to, they said.

Then on a Monday in late August, two FBI agents came to speak to Gartenlaub at the Huntington Beach facility. They showed him pictures of himself and his wife with some of her acquaintances whom Gartenlaub couldn't remember.

Two days later, the agents returned. This time they handcuffed him.

During his initial appearance in a federal courthouse in Santa Ana, Calif., the prosecutors indicated a willingness to reduce or drop the child pornography charges if he would tell them about the C-17, said Sara Naheedy, Gartenlaub's attorney at the time.

"They said what they really wanted was information about the C-17 Chinese hacking situation," Naheedy recalled.

All along, Werksman said, the government suspected Gartenlaub was working with Su. "They triangulated Keith as the guy at Boeing who would have been Su Bin's inside source," he said.

That suspicion is "ridiculous," Gartenlaub said.

"I've been a good Boeing employee for years. Just because I married somebody from China doesn't mean I'm going to betray my country," he said. "If they think I'm a spy, then charge me with it."

Associated Press
Russia, China are greatest cyberthreats, but Iran is growing
Wednesday, 06 April 2016
Byline: Lolita C. Baldor

Russia and China present the greatest cyber security threat to the U.S., but Iran is trying to increase and spend more on its capabilities, the Navy admiral in charge of the military's Cyber Command told Congress Tuesday.
Adm. Michael Rogers told the Senate Armed Services Committee that while the U.S. has more overall military power than the three countries, the gaps are narrower when it comes to cyber warfare.

He said U.S. Cyber Command is making progress building cyber mission teams, and will have 133 fully operational by September 2018. He said that nearly 100 teams are already conducting cyberspace operations.

Defence Secretary Ash Carter has beefed up the use of offensive cyber warfare in Iraq and Syria and made increasing the department's cyber capabilities a key goal.

As part of that, he is considering elevating Cyber Command to a full, independent military command. Currently U.S. Cyber Command is a sub-unit of the military's Strategic Command.

During testimony on Tuesday, Rogers told senators that being designated a full command would allow his units to "be faster, which would generate better mission outcomes."

He added that it also would give him more input into the budget process and how to prioritize spending.

A senior U.S. official said Tuesday that Carter believes that making Cyber Command a full command would be worthwhile. The official said that while discussions with the White House are ongoing, Carter has not yet sent his final recommendation to the president. Congress would also need to approve such a change.

The official was not authorized to discuss the matter publicly and spoke on condition of anonymity.

During the hearing, Rogers said that his major cybersecurity concerns include attacks against critical infrastructure in the U.S. and the possibility that cyber hackers may begin breaching networks and changing data, rather than just reading it or stealing it. As a result, he said, officials would no longer be able to "believe what we're seeing," including in data that the military needs for critical operations.

In addition, he said that there are increasing worries that extremist groups and others may begin to view cyber as a weapons system and "want to use it as a vehicle to inflict pain against the United States and others."

New York Times
China Censors Mentions of 'Panama Papers' Leaks
Wednesday, 06 April 2016
Byline: Michael Forsythe and Austin Ramzy

The release of the "Panama Papers" is setting off a political firestorm the world over, prompting protests calling for the resignation of Iceland's prime minister and drawing stern replies from the Kremlin.

But in China, where the names of relatives of several top leaders have been found in the leak of millions of pages of documents from a Panamanian law firm that expose the murky world of offshore companies, most citizens will never hear of the news, which the International Consortium of Investigative Journalists released on Sunday.

Censors have been working hard to ensure that news of the leaks does not penetrate China's "Great Firewall" of Internet controls. Searches using the Chinese characters for "Panama" early on Tuesday on Weibo, China's equivalent to Twitter, turned up information on regulations for importing fruit, including some from Panama. But by the afternoon in Beijing, queries resulted in the following terse message: "Sorry, searches for 'Panama' came up with no relevant results."

A censorship notice sent by a Chinese provincial Internet office told editors to delete reports on the leaks, according to China Digital Times, a website affiliated with the University of California, Berkeley, that monitors the Chinese Internet.

"If material from foreign media attacking China is found on any website, it will be dealt with severely," the notice said. China Digital Times said it did not name the body issuing the notice to protect its source.

The top censored phrases monitored on Monday on Weibo by the University of Hong Kong's Weiboscope all appeared to be related to the Panama Papers: tax evasion, file, leaked, Putin and company.

The leaks, from the Panamanian law firm Mossack Fonseca, show that relatives or business partners of several current and former members of China's ruling Politburo were tied to offshore companies that had the effect of obscuring their ownership interests.

Surely the most politically sensitive leak, for China's censors, was the revelation that Deng Jiagui, the brother-in-law of President Xi Jinping, had set up two British Virgin Islands-registered companies through Mossack Fonseca in 2009, when Mr. Xi was vice president but already marked as the heir apparent for the country's top position.

The consortium did not find what the two companies -- Best Effect Enterprises and Wealth Ming International -- were used for, and by the time Mr. Xi became China's top leader in late 2012, the companies were dormant, reported the group, based in Washington.

The new revelations add to previous exposés of Mr. Deng, who is married to Mr. Xi's older sister, Qi Qiaoqiao. In 2012, Bloomberg News reported on the vast business empire built by Mr. Deng and Ms. Qi both inside China and through offshore companies that amounted to hundreds of millions of dollars. In early 2014, the consortium's first report from leaked offshore accounts also turned up information on an offshore company where Mr. Deng was an owner.

Another politically powerful Chinese couple that had been the subject of previous revelations by the consortium was Li Xiaolin, the daughter of the former premier Li Peng, and Ms. Li's husband, Liu Zhiyuan. The Panama Papers leaks showed that Ms. Li and Mr. Liu were the owners of a foundation based in Liechtenstein that in turn owned a company in the British Virgin Islands, Cofic Investments. A lawyer for Cofic told Mossack Fonseca that the company's profits came from helping the law firm's other clients export heavy machinery from Europe to China, the consortium reported.

Ms. Li's name has turned up in each of the three exposés by the consortium on leaked offshore accounts and Swiss bank accounts that have been published in the past two years. Last year, she and Mr. Liu were listed as the owners of a Swiss bank account that held as much as $2.5 million.

Another relative of a top leader revealed to have offshore accounts is Jasmine Li Zidan, the granddaughter of Jia Qinglin, a former member of the Politburo Standing Committee. Ms. Li's father, Li Botan, was a central figure in a report last year by The New York Times on the political ties of the Dalian Wanda Group chairman, Wang Jianlin. Companies linked to Mr. Li made hundreds of millions of dollars in capital gains from their holdings in Wanda property and entertainment enterprises.

One of the few mainland news outlets to mention the Panama Papers was Global Times, a newspaper run by the Chinese Communist Party.

In a commentary published on Tuesday, the newspaper questioned the lack of a named source for the documents, and the Chinese version of the article suggested that Western intelligence agencies could easily slip fake information into such a large trove of records.

The article accused the Western news media of using the leaks for ideological purposes by attacking President Vladimir V. Putin of Russia. It said that Iceland's prime minister, who is under fire after the leaks disclosed that he and the woman who is now his wife set up a British Virgin Islands company in 2007, was an insignificant figure by comparison.

"The Western media has taken control of the interpretation each time there has been such a document dump, and Washington has demonstrated particular influence in it," Global Times wrote. "Information that is negative to the U.S. can always be minimized, while exposure of non- Western leaders, such as Putin, can get extra spin."

The Global Times article omitted any information about the leaks pertaining to Chinese leaders.

New York Times
WhatsApp Encryption Now Covers All Messages
Wednesday, 06 April 2016
Byline: Mike Issac

WhatsApp, the messaging app owned by Facebook and used by more than one billion people, on Tuesday introduced full encryption for its service, a way to ensure that only the sender and recipient can read messages sent using the app.
Known as "end-to-end encryption," it will be applied to photos, videos and group text messages sent among people in more than 50 languages across the world, including India, Brazil and Europe. Previously, only one-to-one text messages were fully encrypted.

"Every day we see stories about sensitive records being improperly accessed or stolen," WhatsApp said in a blog post. "And if nothing is done, more of people's digital information and communication will be vulnerable to attack in the years to come."

"Fortunately, end-to-end encryption protects us from these vulnerabilities," the company said.

The move thrusts WhatsApp further into a standoff between tech companies and law enforcement officials over access to digital data, one that pits Silicon Valley's civil libertarian ideals against the federal government's concerns over national security. Increased encryption will make it more difficult, if not impossible, for the authorities to intercept WhatsApp communications for investigations.

The government has faced similar issues with companies like Telegram, Signal and Wickr Me, messaging services that also offer encrypted communications.

The debate over access to digital data erupted in February when a federal court in California ordered Apple to help crack open an iPhone used by a gunman in the San Bernardino, Calif., rampage last year. Apple's chief executive, Timothy D. Cook, resisted the order, saying that the company needed to protect individuals' privacy. Law enforcement officials, including the F.B.I. director, James B. Comey, have criticized encryption as a hindrance to investigations, including in terrorism cases.

Last month, President Obama said in a speech that he opposed the stance on encryption taken by technology companies. The Justice Department later dropped its demand that Apple help open the iPhone of the San Bernardino killer after saying that it had found another, undisclosed, way into the device.

End-to-end encryption for WhatsApp is of particular concern to the F.B.I., considering the service's huge subscriber base and large international footprint. With increasing amounts of communications now sent across messaging services, encrypted texts, video, photos and the like may end up being more problematic for law enforcement than locked devices. The encryption on WhatsApp will be turned on by default, so users will not be required to enable it themselves.

WhatsApp has previously clashed with law enforcement over its digital data. Last month, the federal police in Brazil arrested a Facebook executive for not turning over information from a WhatsApp account in a drug trafficking case. The executive was released.

In the United States, the Justice Department has been discussing how to proceed in a continuing criminal investigation in which a federal judge approved a wiretap, but investigators were stymied by WhatsApp's encryption.

London Times
WhatsApp locks out terror police
Wednesday, 06 April 2016
Byline: James Dean

Terrorism investigators are to be completely locked out of WhatsApp after the company re-engineered its systems to make it powerless to comply with warrants to hand over suspicious communications. A security upgrade to the world's most popular messaging service means that its engineers can no longer unscramble encrypted communications sent by its one billion users.

WhatsApp's decision will further antagonise GCHQ, MI5 and MI6, which believe that American technology companies fail to provide adequate assistance to terrorism investigations. The companies argue that strong encryption is essential as more private communications take place through digital channels.

French officials investigating the Paris attacks last November named WhatsApp as being among several messaging services allegedly used by Isis to plot the massacres.

WhatsApp said yesterday that it had switched on "end-to-end" encryption by default for text, video, picture and audio messages and voice calls transmitted over its network. It therefore no longer holds the digital "keys" needed to unscramble encrypted communications. The company previously had enabled such encryption for some users and some communications.

WhatsApp's move comes shortly after a spat over encryption between Apple and the FBI. The FBI wanted to force Apple to break into an encrypted iPhone used by a suspected terrorist in the San Bernardino massacre in California last year, but dropped its case last week.

Dow Jones News Service
Underground Hacker Market is Booming, Says New Report
Wednesday, 06 April 2016
Byline: Nicole Hong

Intelligence analysts found that business is booming in underground markets for Russian and other hackers, according to a report released Tuesday by security firm Dell SecureWorks Inc.

Malware, which includes viruses and other software intended to disrupt computer users, is becoming "much cheaper and continues to offer a low barrier to entry for cybercriminals looking to steal information," wrote the analysts, who scoured dozens of websites on the dark web over the past eight months.

Among the findings: Hackers are offering to steal personal emails from Gmail or Yahoo accounts for $129. The report, which didn't detail the extent to which the online hackers delivered on their promises, said one illicit service boasted that emails could be snatched without the victim noticing any suspicious activity.

Offers to hack into corporate email accounts cost more: $500 per mailbox, the security firm said.

The findings come amid growing concerns among law-enforcement officials about the burgeoning hacker-for-hire market, which allows anyone with Internet access and a bit of money to potentially wreak havoc on computer networks. Hacking has become a way to facilitate all sorts of crimes, from illegal gambling to insider trading.

Tutorials for new hackers, such as how to send phishing emails, can be purchased online for $20 to $40, the report said. Remote access "trojans, " which allow cybercriminals to secretly control other people's computers from a distance, can go for as little as $5 to $10.

The report suggests that hackers are operating more like regular businesses, with many Russian hackers touting 24/7 customer service. Analysts found hackers hawking their goods like a typical startup company. One ad offered "free-trial attacks" and "huge abilities."

Standard goods for identity theft like credit card numbers, bank account credentials and passports are still popular on the dark web. Dell SecureWorks also found that hackers are now selling frequent flyer accounts and hotel points accounts, a trend previously reported by The Wall Street Journal. These points can be exchanged on legitimate websites for gift cards.

Sputnik News Service
Russian Hackers Extend Working Hours to Please Customers
Wednesday, 06 April 2016

Underground hackers throughout the world, particularly in Russia, have started to expand working hours and offer transaction guarantees in order to provide excellent service to customers, Dell's SecureWorks said in a report.
"That trend [of improving services] has not died out, but rather increased, especially on the Russian Underground forums, where we saw many of the hackers expand their working hours to include weekends and even promising to be available 24/7," the report stated on Tuesday.

Dell's SecureWorks, which provides intelligence-driven security solutions to counter cyberattacks, noted that "like any other market in a capitalist system, the business of cybercrime is guided by the supply and demand for various goods and services waxes and wanes."

The company added that many hackers are now providing customers with the ability to work through so- called "guarantors."

"A guarantor for a legitimate transaction typically ensures that the exchange of data and payment takes place fairly by holding money and the product before distributing it to both parties involved in the transaction," the report explained.

The services offered by hackers include accessing Gmail and Yahoo accounts, and hacking into popular Russian and Ukrainian email providers such as Mail.Ru, Yandex, Rambler and Ukr.net.

An email hack costs anywhere from $65 to $129, according to the report.

The hackers also offer to access US and Russian socials media accounts, corporate emails and sell credit card credentials from around the world. Providing DDoS, or distributed denial-of-service attacks, is another popular service hackers offer.

In addition, Russian hackers are ready to provide full business dossiers on Russian companies.

"The hackers are selling information and documents from Russian organizations, including all of the credentials associated with a company's various bank accounts (account numbers, logins, passwords, tokens)," the report pointed out.

Yet another hackers' service includes selling identities, passports, social security cards and other documents.

"The price for an actual US passport ranges from $3,000 to as high as $10,000," the report said. "Templates for US passports sell anywhere from $100 to $300, and the buyer must find their own printer."

Dell SecureWorks urged individuals and companies to implement protective measures to address the threat of potential cyberattack. The company advised building strong technology defenses, using encrypted email and employing vulnerability scanning, among other measures to guard against hacks.

Daily Sabah
Turkish hacker group's attacks shut down Armenian government websites
Wednesday, 06 April 2016

Amid renewed fighting between Armenia and Azerbaijan since the weekend, a Turkish hacker group launched attacks on Armenian government websites on Tuesday, causing long shutdowns.
The attacks by the hacker team named "Aslan Neferler Tim" (which can roughly be translated as Lion Privates Team) caused blackouts on government websites including defense, energy, agriculture ministries' sites, in addition to various other government agencies.

In a Facebook post, the group claimed that their attacks will increase.

The group had earlier claimed responsibility for the attacks on the websites of Belgian government agencies, Dutch right-wing politician Geert Wilders, the Armenian Central Bank, and the main webpage of renowned hacker movement Anonymous.

Yonhap News Agency
N.K. cyber capabilities pose serious challenges to U.S.: cyber command chief
Wednesday, 06 April 2016
Byline: Staff reporter

Washington - North Korea's cyber capabilities pose serious challenges to the United States, the U.S. cyber commander said Tuesday, emphasizing the communist nation has steadily been bolstering its capabilities and has been "quite active" in the cyber domain.
Adm. Michael S. Rogers made the assessment in a statement submitted for a Senate Armed Services Committee hearing, saying the North is one of the countries that his command is watching "most closely," along with Russia, China and Iran.

"Iran and North Korea represent lesser but still serious challenges to U.S. interests. Although both states have been more restrained in this last year in terms of cyber activity directed against us, they remain quite active and are steadily improving their capabilities," Rogers said. "Both of these nations have encouraged malicious cyber activity against the United States and their neighbors, but they currently devote the bulk of their resources and effort to working against their neighbors."

The North's cyber capabilities have been a greater focus of attention since a massive hacking attack on Sony Pictures in late 2014, which Pyongyang is believed to have carried out in retaliation for Sony's release of a comedy film ridiculing North Korean leader Kim Jong-un.

"A year ago I mentioned North Korea's brazen cyber operations to impair and intimidate Sony Pictures Entertainment. We have seen no repetition of such destructive assaults against targets in the United States," Rogers said.

The Intercept
Documents reveal secretive UK surveillance policies
Thursday, 21 April 2016
Byline: Ryan Gallagher

Washington - Newly disclosed documents offer a rare insight into the secretive legal regime underpinning the British government's controversial mass surveillance programs.
London-based group Privacy International obtained the previously confidential files as part of an ongoing legal case challenging the scope of British spies' covert collection of huge troves of private data.

Millie Graham Wood, Legal Officer at Privacy International, said in a statement Wednesday that the documents show "the staggering extent to which the intelligence agencies hoover up our data. This can be anything from your private medical records, your correspondence with your doctor or lawyer, even what petitions you have signed, your financial data, and commercial activities."

She added: "The agencies themselves admit that the majority of data collected relates to individuals who are not a threat to national security or suspected of a crime. This highly sensitive information about us is vulnerable to attack from hackers, foreign governments, and criminals."

The documents, published online Wednesday, primarily relate to the opaque rules regulating British spy agencies' use of so-called bulk personal datasets, which are obtained without any judicial authorization and contain "personal data about a wide range of individuals, the majority of whom are not of direct intelligence interest," according to the agencies' own definition of them.

The datasets could cover a wide variety of information, the documents suggest, potentially revealing details deemed particularly "sensitive," such as people's political opinions, religious beliefs, union affiliation, physical or mental health status, sexual preferences, biometric data, and financial records. They may also contain data revealing legally privileged information, journalists' confidential sources, and "details about individuals who are dead," one document says.

The documents include internal guidance codes for spies who have access to the surveillance systems. One memo, dated June 2014, warns employees of MI6, the U.K.'s equivalent of the CIA, against performing a "self-search" for data on themselves, offering a bizarre example that serves to illustrate the scope of what some of the repositories contain.

"An example of an inappropriate 'self search' would be to use the database to remind yourself where you have travelled so you can update your records," the memo says. "This is not a proportionate use of the system, as you could find this information by another means (i.e. check the stamps in your passport or keep a running record of your travel) that would avoid collateral intrusion into other people's data."

Another document warns MI6's employees that they must not trawl the surveillance databases "for information about other members of staff, neighbors, friends, acquaintances, family members and

public figures." That is, it adds, "unless it is necessary to do so as part of your official duties." The agency says that it has monitoring systems in place to catch any abuses, but it is unclear whether the checks that are in place are sufficient. One 2010 policy paper from MI6 states there is "no external oversight" of it or its partners' "bulk data operations," though adds that this was subject to review.

Elsewhere in the documents, eavesdropping agency Government Communications Headquarters (GCHQ) and domestic intelligence agency MI5 admit that they have obtained the bulk datasets on several occasions dating back more than a decade - GCHQ beginning in 1998, and MI5 in 2005 - under Section 94 of the 1984 Telecommunications Act. The agencies argue that the data has thwarted terror plots and is needed "to identify subjects of interest, or unknown individuals who surface in the course of investigations; to establish links between individuals and groups, or otherwise improve understanding of a target's behavior and connections; to validate intelligence obtained through other sources; or to ensure the security of operations or staff."

Last year, The Intercept exposed how GCHQ has in recent years attempted to create what it described as the world's largest surveillance system, covertly harvesting in excess of 50 billion records every day about people's emails, phone calls, and Web browsing habits. In one program code-named KARMA POLICE, the agency said it was seeking to obtain "a web browsing profile for every visible user on the internet."

The Guardian (London)
UK spy agencies have collected bulk personal data since 1990s, files show (Canada)
Thursday, 21 April 2016
Byline: Owen Bowcott, Richard Norton-Taylor

London - Britain's intelligence agencies have been secretly collecting bulk personal data since the late 1990s and privately admit they have gathered information on people who are "unlikely to be of intelligence or security interest".
Disclosure of internal MI5, MI6 and GCHQ documents reveals the agencies' growing reliance on amassing data as a prime source of intelligence even as they concede that such "intrusive" practices can invade the privacy of individuals.

A cache of more than 100 memorandums, forms and policy papers, obtained by Privacy International during a legal challenge over the lawfulness of surveillance, demonstrates that collection of bulk data has been going on for longer than previously disclosed while public knowledge of the process was suppressed for more than 15 years.

The files show that GCHQ, the government's electronic eavesdropping centre based in Cheltenham, was collecting and developing bulk data sets as early as 1998 under powers granted by section 94 of the 1984 Telecommunications Act.

The documents offer a unique insight into the way MI5, MI6, and GCHQ go about collecting and storing bulk data on individuals, as well as authorising discovery of journalists' sources.

Bulk personal data includes information extracted from passports, travel records, financial data, telephone calls, emails and many other open or covert sources. Often they are "fused" together to help pinpoint suspects.

The frequency of warnings to intelligence agency staff about the dangers of trespassing on private records is at odds with ministers' repeated public reassurances that only terrorists and serious criminals are having their personal details compromised.

For example, a newsletter circulated in September 2011 by the Secret Intelligence Agency (SIS), better known as MI6, cautioned against staff misuse. "We've seen a few instances recently of individuals crossing the line with their database use ... looking up addresses in order to send birthday cards, checking passport details to organise personal travel, checking details of family members for personal convenience," it says.

"Another area of concern is the use of the database as a 'convenient way' to check the personal details of colleagues when filling out service forms on their behalf. Please remember that every search has the potential to invade the privacy of individuals, including individuals who are not the main subject of your search, so please make sure you always have a business need to conduct that search and that the search is proportionate to the level of intrusion involved." Better where possible to use "less intrusive" means, it adds.

There has been disciplinary action. Between 2014 and 2016, two MI5 and three MI6 officers were disciplined for mishandling bulk personal data. Last year, it was reported that a member of GCHQ's staff had been sacked for making unauthorised searches.

The papers show that data handling errors remain a problem. Government lawyers have admitted in responses to Privacy International that between 1 June 2014 and 9 February this year, "47 instances of non-compliance either with the MI5 closed section 94 handling arrangements or internal guidance or the communications data code of practice were detected." Four errors involved "necessity and proportionality" issues; 43 related to mistransposed digits, material that did not relate to the subject of investigation or duplicated requests.

Another MI5 file notes that datasets "contain personal data about individuals, the majority of whom are unlikely to be of intelligence or security interest".

The documents have been disclosed before a trial due later this summer at the investigatory powers tribunal, which hears complaints about state-authorised surveillance and the intelligence agencies. IPT sessions hear secret evidence behind closed doors.

Release of these internal records follows admissions by David Cameron and by parliament's intelligence and security committee (ISC) last year in the wake of revelations by the US whistleblower Edward Snowden.

The most recent documents refer to a "more onerous authorisation process" after the prime minister's avowal of the "use of bulk personal data". They provide fresh detail of what is happening in the intelligence agencies.

Web and phone companies are required to retain data for official access for 12 months, but the intelligence agency documents make clear that acquired bulk data sets can be held far longer.

An MI5 memorandum says retention of "low intrusion" material needs to be reviewed only every two years. Some key words are missing from the memo, but it adds: "In MI5, a maximum retention period [redaction] is applied to [bulk personal data]. This can be increased in exceptional circumstances via a policy waiver. This waiver must be authorised by a senior MI5 official and agreed by the BPDRP [bulk data retention review panel] but shall be subject to a detailed review."

Bulk personal data is exchanged with "foreign agencies", presumably mainly those from other countries in the UK's traditional "Five Eyes" alliance - the USA, Canada, Australia and New Zealand.

The documents do not specify every type of information exploited but give examples and broad categories: population data and passports, travel records, financial data and communications information. "Some of this data is publicly available, some of it is purchased and some of it is acquired covertly in accordance with SIS statutory functions," according to an MI6 note.

Monetary information is held. "The fact that [MI5] holds bulk financial, albeit anonymised data is assessed to be a high corporate risk since there is no public expectation that the service will hold or have access to this data in bulk. Were it to become widely known that the service held this data, the media response would most likely be unfavourable and probably inaccurate.

"In some cases, it may be necessary for the relevant team to approach the data provider to examine whether any unnecessary/extraneous parts of the dataset can be removed prior to acquisition. Such extraneous data might include large numbers of minors, details of earnings or medical information."

Death provides no escape. "Policy and processes in relation to bulk personal data is the same for both the living and the dead," a combined agencies memo records.

Each intelligence service has its own database, it appears from the documents. For MI5, storage of bulk data is at their London HQ, Thames House. "In order to ensure the security and integrity of the datasets that the service relies upon for its enhanced analytical capabilities and to reassure data providers that their data will be handled securely, it is essential that the necessary physical controls are in place to

mitigate unauthorised access to, or loss of, this information during transportation to and subsequent storage in Thames House."

The justification for assembling such sophisticated databases, according to an MI5 document, is that it speeds up the process of detecting suspects. "By integrating bulk data [redaction] with information about individual subjects of interest from other sources of intelligence (liaison relationships, agent reporting, intercept, eavesdropping, surveillance) and from 'fusing' different data- sets in order to identify common links, we can better understand target networks, locations and behaviours, enabling a greater depth and breadth of target coverage.

"The fragmentary nature of many intelligence leads and the magnitude of the threat all mean that there is currently no effective method of resolving identities in a timely fashion without using bulk data."

The standard MI5 form for acquisition of bulk data requires agency staff to a tick box if it holds sensitive personal data such as "biometric, financial, medical, racial or ethnic origin, religious, journalistic, political, legal, sexual or criminal activity" and membership of a trade union. MI5 officers also need to explain why acquisition is "necessary and proportionate".

The documents show how alert the agencies are to their legal obligations. They refer to the agencies' "ethics team", the need for "proportionality" and "necessity". One note stresses that GCHQ employees' conditions of employment state that "unauthorised entry to computer records may constitute gross misconduct".

But the papers also reveal how much latitude the law - notably Ripa, the Telecommunications Act, and the Data Protection Act - in practice gives them.

The documents include for the first time certificates under section 28 of the Data Protection Act - signed by David Blunkett and Jack Straw in 2001 when they were home and foreign secretary respectively - which provided secrecy about authorised bulk data interceptions under section 94 of the Telecommunications Act. The existence of such directions were not disclosed until last year.

The quantity of information the agencies have been forced to release suggests their long-established position of "neither confirming nor denying" any operational details may be crumbling at the edges.

In parliamentary debate over the investigatory powers bill, the government has argued that the security services only conduct targeted searches of data under legal warrants in pursuit of terrorist or criminal activity and that bulk interception is necessary as a first step in that process.

Millie Graham Wood, a legal officer at Privacy International, said: "The information revealed by this disclosure shows the staggering extent to which the intelligence agencies hoover up our data.

"This highly sensitive information about us is vulnerable to attack from hackers, foreign governments and criminals. The agencies have been doing this for 15 years in secret and are now quietly trying to put these powers on the statute book for the first time in the investigatory powers bill, which is currently being debated in parliament. These documents reveal a lack of openness and transparency with the public about these staggering powers and a failure to subject them to effective parliamentary scrutiny."

A Home Office spokesman said: "Bulk powers have been essential to the security and intelligence agencies over the last decade and will be increasingly important in the future.

"The acquisition and use of bulk provides vital and unique intelligence that the security and intelligence agencies cannot obtain by any other means. The security and intelligence agencies use the same techniques that modern businesses increasingly rely on to analyse data in order to overcome the most significant national security challenges."

BBC News
Spies' 'staggering' data requests revealed
Thursday, 21 April 2016
Byline: Chris Vallance

London - Since 2005 successive Home Secretaries have authorised the collection of vast amounts of telecommunications data, documents reveal.
The documents also show that MI5 secretly collected large amounts of "anonymised" financial data.

Campaign group Privacy International said the documents show "the staggering extent of UK government surveillance".

The Home Office said the data acquisition had "been essential to the security and intelligence agencies".

It added that the data had provided "vital and unique intelligence".

The disclosure of the documents was made to Privacy International as it prepares for an Investigatory Powers Tribunal hearing in July.

The tribunal handles complaints against UK intelligence agencies MI5, MI6 and GCHQ.

The campaign group is challenging the agencies use and acquisition of "bulk personal datasets" - very large amounts of personal data collected from public and private organisations.

The Home Office has repeatedly refused to list the datasets the agencies hold, but the documents show the agencies could request a range of sensitive information, including medical information, financial information, and information about telephone and internet communications.

The documents reveal that among other things this data is vital in identifying "foreign fighters", possibly a reference to jihadists involved in the conflict in Syria and Iraq.

Privacy International said: "The intelligence agencies have secretly given themselves access to potentially any and all recorded information about us".

But the Home Office told the BBC: "The acquisition and use of bulk [data] provides vital and unique intelligence", adding: "The security and intelligence agencies use the same techniques that modern businesses increasingly rely on to analyse data in order to overcome the most significant national security challenges".

Bad press

In several documents the risk that the public might become aware of the powers is discussed.

An MI5 policy issued in 2010 says the agency's access to "anonymised" financial data would be against "public expectations".

It says that if the data is revealed the media response could be "unfavourable and probably inaccurate".

David Davis MP, a former Conservative Shadow Home Secretary, told the BBC: "It's clear the agencies and the government have been keeping information secret about what they've been doing not just for security reasons, as is normally claimed, but to avoid both embarrassment and public opposition."

Every six months since 21 July 2005, Home Secretaries have authorised MI5 to collect in a database, information from communication network providers, the documents reveal.

This could include telephone data and internet data. It does not include the content of communications.

The documents say the data is anonymous as it does not contain "subscriber information", but privacy campaigners argue it would be possible work out the identity of an individual from the data.

MI5 says the data is deleted every 12 months. In the documents the data is said to be of "significant security value."

The data is obtained under Section 94 of the Telecommunications Act 1984. The government's independent reviewer of terrorism legislation, David Anderson QC, has previously told the BBC the legislation was "so vague that anything could be done under it".

But requests to use the database, the documents say, require a separate authorisation under the Regulation of Investigatory Powers Act.

Misuse detailed

The documents set out detailed procedures required to authorise the collection and use of the data.

But they reveal that misuse has occurred.

One document produced by MI6 gives examples of "individual users crossing the line" for example, "looking up addresses in order to send birthday cards" and "checking details of family members for personal reasons"

The revelations will add to the controversy surrounding the Investigatory Powers Bill currently working its way through parliament.

Millie Graham Wood of Privacy International said: "The agencies have been doing this for 15 years in secret and are now quietly trying to put these powers on the statute book for the first time."

But the Home Office said the new law is necessary and will strengthen safeguards, telling the BBC that the Bill "will also establish the Investigatory Powers Commissioner who will keep under review the use of bulk personal datasets by the intelligence agencies."

That is currently done by the Intelligence Services Commissioner, who confirmed in his 2014 report that "the case for holding BPD has been established in each service" and "agencies all have strict procedures in place in relation to handling, retention and deletion."

New York Times
Chinese Maker of Drones Says It May Share Data
Thursday, 21 April 2016
Byline: Paul Mozur

Shenzhen - DJI is the Chinese company that took drone technology -- long the purview of major military forces -- and made it cheap and accessible enough for ordinary people.
But as the technology is put into the hands of consumers, it raises new questions for DJI and others in the industry: What should be done with the information those drones gather? The little pilotless flying machines typically carry cameras, GPS sensors and other devices that can tell interested parties where they have been and what they have seen. How much of that information should be shared with local governments?

That question is especially important in China, where regulators have looked askance at drones while tightening their hold over civil society.

In a briefing for Chinese and foreign journalists at DJI's headquarters in Shenzhen on Wednesday, Zhang Fanxi, a spokesman for the company, said it was still working out how to deal with the data it collects in China. But for now, he said, DJI is complying with requests from the Chinese government to hand over data.

Adam Najberg, another DJI spokesman, said DJI evaluated each request and complied if it decided that request was legitimate.

DJI could also give the government data from flights in Hong Kong, Mr. Zhang said. That could raise eyebrows among drone users in the city, a semiautonomous Chinese territory with its own laws that guarantee freedom of expression and its own independent judicial system. Protests in Hong Kong that shut down parts of the city in late 2014 were prompted in part by concerns that Beijing was interfering in local affairs.

For the moment, Mr. Zhang said, DJI was uncertain what the industry would decide to do with the data. "This data, exactly how we use it, when we use it and which government departments we give it to" is a continuing discussion, he said.

DJI also sells drones in the United States. Mr. Najberg said DJI did not have a way to see video or images from drones beyond those that users upload themselves via a company social-media app. He also said that the company's phone app uploads flight data to its servers, though consumers can use third-party apps that do not.

DJI is not alone in cooperating with Chinese authorities when they request data, which is required of all companies doing business there. In its most recent report on government requests for information, Apple said it received about 1,000 requests for data in the second half of last year from Chinese authorities and supplied data about two-thirds of the time. Apple said this week that it had never handed encryption keys over to the Chinese authorities, which would give Beijing direct and broad access to communications on Apple's products.

(Over the same period, Apple received about 4,000 requests from the United States authorities and handed over data four-fifths of the time, according to its report. Access to encrypted communications on Apple devices has become the subject of a fierce American political debate.)

But China has been seeking more ways to tap into electronic communications. Two years ago, it proposed a law that would require foreign companies to turn over encryption keys for security reasons, though the final version dropped that language. Officials have cited rising online crime in China, worries about terrorist attacks and disclosures by Edward J. Snowden, the former United States government contractor who revealed that American intelligence agencies sometimes used American technology products to gather information.

Mr. Zhang said DJI did not give Chinese authorities direct access to drones unless requested. "If the government says it wants this data, we will tell the user," he said. "We communicate all of this."

Still, China has not formalized rules over drones, so the industry's obligations are unclear.

Already, DJI's user agreement flags the possibility that whoever flies a drone may not be flying it alone. It reads: "Please note that if you conduct your flight in certain countries, your flight data might be monitored and provided to the government authorities according to local regulatory laws."

In other areas, relations with Beijing remain untested. The company has had numerous requests from local governments in China to work with and train the military police and other security forces to use its drones for surveillance and to track criminals, Mr. Zhang said.

Still, drones face a skeptical audience here. In 2013, Chinese forces shot down a drone over a Beijing suburb. Several months later, a foreigner who took breathtaking shots of central Beijing with a DJI drone earned a brief detention and a stern talking-to.

Drones have raised security concerns in the United States as well, after one crashed on the White House lawn last year. At the briefing, DJI said that it continued to expand a system that ensured the drones could not fly in sensitive areas, an arrangement known as geofencing.

Sydney Morning Herald
Australia ready to hit back at foreign attackers
Thursday, 21 April 2016
Byline: Heath Aston

Sydney - Australia has acknowledged for the first time that it is prepared to strike back against foreign cyber attacks and take "offensive" action to protect the nation's interests.
The message that the government is ready to "deter and respond to malicious cyber activities", comes before a $230 million cyber security strategy to be announced by Prime Minister Malcolm Turnbull on Thursday.

The first update to the nation's cyber attack plan since 2009 will largely involve recruiting 100 more police and cyber specialists to boost the fight against "foreign adversaries", both state- sponsored and those linked to organised crime, and also widen information sharing between business and government.

China, Russia, North Korea and Iran are among the nations suspected to be the most active in launching daily "cyber crime intrusions" against government, business and people in Australia.

In the past six months, systems at the Bureau of Meteorology experienced a "massive breach", believed to have originated in China, and it was reported 97 federal agencies were told to encrypt more data amid "hundreds" of attempted intrusions a month.

The extra resources come on top of $400 million over a decade in the Defence white paper to pay for cyber defence, including experts with hacking experience working for the Australian Signals Directorate whose motto is "Reveal their secrets, protect our own".

Mr Turnbull will characterise the security strategy as a way to protect and enshrine the personal freedoms associated with the online world rather than the creeping reach of Big Brother.

"The maintenance of our security online and the protection of freedom online are not only compatible but reinforce each other," he said. "Australia and Australians are targets for malicious actors - including serious and organised criminal syndicates and foreign adversaries - who are all using cyberspace to further their aims and attack our interests.

"The scale and reach of malicious cyber activity affecting Australian public and private sector organisations and individuals is unprecedented."

Mr Turnbull will appoint a new minister assisting the prime minister on cyber security and a new special adviser on cyber security in his department. Foreign Minister Julie Bishop will appoint Australia's first cyber ambassador.

The Australian Cyber Security Centre, housed inside the headquarters of the Australian Security Intelligence Organisation in Canberra, will be moved to encourage more interaction with business.

A "joint threat-sharing centre" will be established in a capital city, with plans for one in each state capital over time.

The strategy document confirms resources have already gone into "offensive cyber capabilities".

The United States has long used offensive cyber powers. In 2010 its "Stuxnet" worm reportedly infected control systems and disabled Iranian nuclear centrifuges.

China Daily
Nation's drones are in demand
Thursday, 21 April 2016
Byline: Zhao Lei

Beijing - Foreign countries seek 'powerful, affordable' CH military series for reconnaissance, combat, anti-terrorist uses

A number of foreign nations are awaiting delivery of China's CH series military drones, one of the country's most popular products on the international arms market.

The drone family, bearing the name Cai Hong, which means rainbow in Chinese, is considered by experts to be among the most lethal drones on the planet. The newest and largest capacity combat drone in the series, the CH-5, is awaiting government approval for export.

"The total value of contracts we signed in 2015 could definitely be one of the highest in terms of armed drone deals made last year on the international market," Shi Wen, chief drone designer at the China Academy of Aerospace Aerodynamics in Beijing, told China Daily in an exclusive interview. He did not provide a figure.

The academy, part of China Aerospace Science and Technology Corp, is one of China's largest military drone developers. Its CH series drones have been sold to 20 military users from more than 10 foreign countries and are the largest military drone family that China has exported, Shi said.

The early models, CH-1 and CH-2, are small, unarmed reconnaissance craft that have a proven record in locating and monitoring targets. The larger ones - the CH-3 midrange combat and reconnaissance drone and CH-4 mid-altitude, high-endurance armed drone - immediately attracted buyers seeking a powerful, affordable unmanned combat aircraft.

"Our best-selling type so far is the CH-3, while the CH-4 has also received many orders," Shi said, adding that many more countries have expressed a "strong desire" to buy CH drones, but have yet to do so because of their sluggish economies.

The Australian
Firepower boosted to battle cyber hits
Thursday, 21 April 2016
Byline: Brendan Nicholson

Sydney - The government will spend -another $230 million to fight the more than 1000 major cyber -attacks in Australia each year.
The new strategy does not identify nations or criminal gangs responsible for hits on Australia's computer systems but it says they are sophisticated enough to find and target the weakest link in -robust defences.

"Cyber adversaries are aggressive and persistent in their efforts to compromise Australian networks and information," says the cyber security strategy to be -released by Malcolm Turnbull today.

"They are constantly improving their methods in an attempt to defeat our network defences and exploit new technologies." China has been blamed for cyber intrusions around the world and one of its agencies is believed to have penetrated the computer system of Australia's Bureau of Meteorology.

That was of particular concern because of fears it could have provided the intruders with a back door into many more sensitive public service areas, including -Defence's Canberra headquarters.

China strongly denied any involvement in the breach.

Plugging the gap in the public service system and upgrading -security is believed to have cost Australia millions of dollars.

The report concludes that the way the internet is governed, with the private sector and the community as equal partners with governments, is the most effective model to ensure it is open, free and secure.

The new money, to be spent over four years, will cover the cost of additional infrastructure and pay for an additional 101 cyber -security specialists. The Australian Signals Directorate will assess the vulnerability of government agencies and advise them how to deal with emerging technology and threats.

A cyber ambassador will be -appointed to liaise with other -nations on cyber threats.

The Australian Cyber Security Centre will be pulled out of the high-security ASIO building to make it more accessible to Aus-tralian businesses and institutions.

The fresh resources complement a massive investment in cyber activity announced in the defence white paper, with an -additional 900 uniformed ADF personnel and 800 Defence civilians to work in the intelligence processing and broader cyber protection areas.

The Turnbull government says Australia is ahead of most countries in the cyber security area.

The Australian Signals Directorate has the ability to defend the nation against a major cyber -attack or to launch an attack of its own on a -nation or criminal gang penetrating Australia's computer systems.

The strategy says it is important to track down those responsible for malicious cyber activity and bring them to justice.

"Due to the global nature of malicious online activities, tackling cyber crime will involve both increasing the numbers and improving the criminal intelligence capacity and skill sets of law -enforcement officers at home as well as partnering with law enforcement and other agencies abroad," the strategy says."Any measure used by Aus-tralia in deterring and responding to malicious cyber activities would be consistent with our support for the international rules-based order and our obligations under international law."

Australian Associated Press
Govt gears up for cyberattack combat
Thursday, 21 April 2016
Byline: Elise Scott

Canberra - Prime Minister Malcolm Turnbull has declared war on cyberinvasion, confirming the government could launch offensive attacks to deter foreign online espionage.
He did so in unveiling Australia's $230 million cybersecurity strategy, which focuses on closer collaboration with business.

The move comes as the government confirmed reports the Bureau of Meteorology and Department of Parliamentary Services have been targets of malicious cyberattacks in recent years.

Foreign Minister Julie Bishop told reporters on the NSW South Coast the BOM attack was under investigation.

Mr Turnbull said an offensive cybercapability provided an option for the government to respond, but would be subject to "stringent" legal oversight.

"Some intrusions are the work of foreign adversaries, others involve malicious software," he said at the strategy launch in Sydney on Thursday.

"The scale and rate of compromise is increasing."

The government would work with other nations to shut down safe havens for criminal and terrorist organisations.

Unexplained cyberattacks could escalate into war between countries, Mr Turnbull said.

The Australian Crime Commission estimated the cost to the economy of cybercrime was about $1 billion each year, while other assessments put it closer to $17 billion.

Many people would have no idea they'd been targeted by cybercriminals.

"Now as your prime minister, my highest duty and that of my government is to keep Australians safe," Mr Turnbull said.

"It is no different in cyberspace."

The strategy's centrepiece involves sharing threat information between business and government, using the existing Australian Cyber Security Centre and new portals in capital cities.

The centre will be relocated from Australia's spy building in Canberra to a more accessible venue.

The prime minister will convene annual meetings with business leaders.

The strategy, the first since 2009, took 18 months to develop and will create about 100 jobs - most of which will be highly specialised.

Mr Turnbull announced the new role of cyberambassador and will appoint a minister assisting him on cybersecurity.

The strategy sits alongside $400 million outlined in the Defence blueprint for cyberactivities.

While agencies don't believe there's yet been a serious cyberattack - which is defined as compromising national security - there are thousands of intrusions every year.

They range from theft of intellectual property to illegally modifying data to seeking ransom to unlock a computer affected by malicious software.

"We must safeguard against criminality, espionage, sabotage and unfair competition online," Mr Turnbull said.

About $190 million allocated to the strategy was new money, with the remaining funds coming from the Innovation and Science Agenda.

It included an education program to raise awareness of cyberintrusions.

Associated Press
Forum to focus on cybersecurity needs in US and Canada
Thursday, 21 April 2016
Byline: Staff report

Boston - Cybersecurity experts are planning to hold a forum on ways the United States and Canada can toughen their online defenses.
The discussion will focus on the growing number of lone wolf and foreign government-sponsored cyber-attacks that harm national security and commerce in both countries.

Thursday's event is sponsored by The New England-Canada Business Council and will include a discussion of strategies needed to stem the tide of cyber-attacks -- particularly those by crime syndicates, rogue nations, terrorist groups and individual hackers.

Organizers of the forum say the attacks disrupt the free exchange of information on the Internet and undermine business transactions.

One of the biggest cyber thefts on record was by an Eastern European crime organization that investigators say raked in $300 million from stolen credit card numbers.

Le Figaro avec l'Agence France-Presse
L'Australie confirme avoir essuyé une cyberattaque en 2015
Thursday, 21 April 2016
Byline: Journaliste maison

Canberra - L'Australie a reconnu aujourd'hui qu'une de ses administrations sensibles avait été la cible en 2015 d'un piratage informatique d'envergure, et débloqué des centaines de millions de dollars australiens pour lutter contre la cybercriminalité.
Le premier ministre australien Malcolm Turnbull s'est refusé à accuser la Chine de cette attaque, concédant seulement que "des efforts étaient fournis par des acteurs étrangers, gouvernementaux ou non, pour pénétrer" dans les systèmes informatiques des agences gouvernementales australiennes. "Je suis en mesure de confirmer que le Bureau de météorologie a été victime d'une intrusion informatique d'envergure qui a été découverte au début de l'année dernière, et le département des services parlementaires a été la victime d'une intrusion similaire ces dernières années", a déclaré le premier ministre lors d'une conférence de presse à Sydney.

"Je n'ai rien à ajouter", a-t-il balayé devant les journalistes qui l'interrogeaient sur l'éventuelle origine chinoise de l'attaque contre le Bureau de météorologie (BOM). En décembre, l'Australian Broadcasting Corporation l'avait imputée à Pékin en s'appuyant sur les déclarations d'un responsable non identifié.

Le BOM, qui a des liens avec le ministère de la Défense, est doté d'un des plus puissants superordinateurs du pays. M. Turnbull a annoncé une enveloppe de 230 millions de dollars australiens (159 millions d'euros) pour lutter contre la cybercriminalité. Celle-ci vient s'ajouter à l'allocation de 400 millions prévue dans ce domaine pour les 10 ans qui viennent.

Les autorités estiment le coût annuel direct des cyberattaques en Australie à un milliard de dollars australiens, selon M. Turnbull. "Mais certaines estimations en chiffrent le coup réel à 1% du PIB, soit 17 milliards de dollars australiens", a ajouté le Premier ministre. Des médias avaient déjà attribué en 2013 à des pirates informatiques chinois le vol des plans secrets du nouveau siège des renseignements australiens. En 2011, les ordinateurs des premier ministre, ministres des Affaires étrangères et de la

Défense avaient été piratés. La presse affirmait que les agences du renseignement chinois étaient soupçonnées, une information que Canberra n'avait là encore pas voulu commenter.

Globe and Mail
Disclosure issues linger over police surveillance techniques
Tuesday, 26 April 2016
Byline: Colin Freeze

Canadian detectives cannot keep secret their advanced spying devices or their relationships with telecommunications corporations because claims of police privilege carry little or no weight in criminal courts.
So ruled Quebec Superior Court Justice Michael Stober as he ordered several modern police surveillance techniques disclosed to lawyers representing six accused mobsters in Montreal.

Finding that police arguments for secrecy rely at times upon "selfserving and weak" legal logic, his decisions have laid bare RCMP tactics.

From the Stober disclosure rulings flowed the recent revelation that the Mounties use a device that mimics a cellphone tower.

The fact that Canadian federal agents also have access to a version of a virtual skeleton key, one that can crack coded BlackBerry communications, has also been exposed.

Police had fought for years to protect such methods from becoming broadly known, until a cat-and-mouse criminal case pitting the RCMP against the Montreal six forced Justice Stober to consider 21st-century techniques.

A publication ban was imposed on his rulings about pretrial disclosure when they were issued last fall, but redacted versions were filed in a higher court this spring. On March 30, the Quebec Court of Appeal in Montreal was to revisit the Stober decisions.

But on the morning that matter was to be heard, the Crown lawyers who appealed the rulings walked away from the underlying first- degree-murder case.

Across town in Laval, the six people arrested in 2011 were acquitted of that charge and pleaded guilty to the lesser charge of conspiracy to murder.

That outcome freed the Crown of its obligation to make increasingly uncomfortable amounts of disclosure and left the appellate judges with no case to consider.

Court decision or no court decision, however, important disclosure issues remain for police, lawyers and judges across Canada.

Here's the question: If police want to borrow from the playbooks of modern spies and advance their investigations with secret surveillance techniques or the help of telecommunications corporations, can they prevent those methods from being revealed during prosecutions?

The court of Justice Stober, which has had a unique exposure to those issues, ruled that the answer is a resounding no. "The interests of the accused in having a fair trial where the accused is able to make full answer and defence outweighs the public interest in protecting police-investigative techniques," he ruled.

The case was extraordinary in several ways. The judge heard police pleas for secrecy in several closed pretrial proceedings from which the accused and their defence lawyers were barred. To balance the scales, the court took the extraordinary step of allowing Toronto lawyer Anil Kapoor, who has national-security clearance, to make arguments on the defence's behalf.

What emerged as a result of these hearings is that, while police in Canada may have plenty of protections to keep human informants anonymous, they have no analogous legal safeguards for surveillance technology or corporate relationships.

Yet, federal agents remain loath to reveal their techniques because they feel they are in an arms race with savvy adversaries.

In the Montreal case, each suspect had multiple unregistered BlackBerrys, and they talked to each other through the company's proprietary encoded "PINto-PIN" texts. Detectives within the RCMP's technological units saw a murder conspiracy take shape in those messages, but it came into focus only through painstaking work.

First, the Mounties had to use a portable cellphone-tower simulator (often known as a "IMSI catcher") to draw data that revealed which handsets in a certain area were controlled by the suspects.

Then, police served assistance orders on BlackBerry directing the Waterloo company to help facilitate interception of the suspects' messages - which were cracked with a version of the company's "global encryption key" that RCMP had somehow acquired.

In more mundane crimes, defence lawyers challenge the accuracy of police breathalyzers and radar guns. In the case at hand, lawyers Frank Addario and Mike Lacy pushed for increasing amounts of detail about police techniques. At one point, they even persuaded Justice Stober to order police to hand over their version of the BlackBerry key so that the defence lawyers for the accused could test it.

Prosecutors and police pushed back hard on that front, saying that would be like letting go of a skeleton key that could open tens of millions of houses. A BlackBerry executive swore a last-minute affidavit saying such a move could undermine customers' trust. In the end, Justice Stober withheld the key, even as he ordered other surveillance techniques disclosed.

At one point, an RCMP inspector testified that a degree of secrecy is needed because being seen to help police is "not good marketing" for tech companies. But Justice Stober characterized such arguments as "weak and self-serving." As a Canadian judge, he said, he had no legal basis to consider any "adverse impact on [Blackberry's] business interests."

The bottom line for the Crown was that Justice Stober's disclosure orders could yield "a new and thorough body of information that would educate the criminal element," or even provide it with "a user guide on how to circumvent a level of secrecy the State is entitled to protect." This, at least, is what the Crown appeal had put forward, until the surprise plea arrangement between the Crown and defence scuttled the hearing.

The Australian
Cybersphere globe's new battlefront
Tuesday, 26 April 2016
Byline: Alan Dupont
Section: oped

If the ambitious goals of Malcolm Turnbull's just released cyber security strategy are achieved, the document could turn out to be the most important and innovative government strategy yet written. Its great strength is that it provides a clear plan for harnessing Australia's transitioning economy to the enabling technology of the internet, while recognising that a secure cyber space is critical to exploiting the benefits of the digital age and to protecting our interests online.

Turnbull's aim is to make Australia a cyber smart nation. This is a formidable undertaking requiring sustained investment in cyber architecture and intellectual capital, major cultural change and a genuine cyber partnership between government, business and the wider community that has yet to materialise.

His starting point is that the internet is the most transformational technological development in human history and therefore central to Australia's future prosperity and security. It's hard to argue with this proposition. Australia is already a wired economy. Nearly 90 per cent of Australians are online, including 84 per cent of small and medium businesses. The internet-based economy contributed $79 billion, or 5.1 per cent of GDP, in 2014 which could grow to $139bn, or 7.3 per cent of GDP, by 2020. By 2019, the average Australian household will have 24 devices connected online.

But it's not just humans who are connecting to the internet. Machines are, too, in ever increasing numbers. Cars, fridges, power plants -- just about every device we use has the capacity to communicate autonomously with other machines. By 2020, the government estimates there may be 50 billion devices connected to the internet globally. Cybersecurity pioneer John McAfee believes the figure is likely to be 212 billion. The Internet of Things is increasingly the Internet of Everything.

Australia has been slow off the mark to understand and capitalise on the enormous economic -potential of this cyber revolution. We have too few cyber entrepreneurs; business still regards cyber security as a technological, rather than a strategic issue; and there is an educational and vocational mismatch between what the digital economy needs and what our schools and universities provide. We are a long way from being a cyber smart nation.

By contrast, a small country like Israel has embraced the cyber revolution, attracting 20 per cent of global private sector investment in the burgeoning cyber security industry and joining the US, Russia, China and Britain as an emerging cyber power. Israel is nurturing a new generation of cyber-literate young people in its universities and schools, right down to primary school level.

The good news is that the cyber security strategy puts Australia on a path to addressing our digital deficiencies by fostering a new network of cyber research and innovation.

At its hub will be a cyber security growth centre that will define and prioritise cyber challenges. Cyber security centres of excellence in universities will be established to help address the serious shortage of cyber security professionals. They will be linked to previous STEM initiatives designed to boost our dwindling stocks of scientists, technologists, engineers and mathematicians.

However, these commendable steps and the accompanying four-year commitment of $230 million are insufficient to realise Turnbull's vision, which requires nothing less than a cradle-to-grave investment of a kind rarely seen in Australia, starting with primary school education. Cyber literacy has to become an intuitive and foundational skill for all Australians.

A second impediment to realising the full potential of the internet is malicious cyber attacks, which have grown exponentially in number and sophistication over the past decade.

An estimated one million Australians were victims of online identity fraud in 2014 and cyber crime may be costing the economy as much as $17bn annually. One in three Australian businesses have experienced some form of cyber crime.

Professional services firm Deloitte ranks Australia as one of the five most vulnerable economies to cyber attacks in the Asia Pacific region.

The loss of intellectual property and state secrets in electronic smash and grab burglaries is an even more serious issue, because they are the crown jewels that determine a country's competitive position and capacity to defend -itself. Malicious actors inhabit the cyber world's dark side and include criminals, terrorists, spies and hostile states. They undermine trust in the reliability and security of the internet. So improving our cyber defences and sensitising Australians to the risk is central to the strategy's success.

The core problem is finding the right balance between protecting users through better security and regulation, and maintaining an open and free system. In Turnbull's words, "we must ensure that the

administration of the internet continues to be governed by those who use it -- not dominated by governments. Equally, cyberspace cannot be allowed to become a lawless domain".

Unfortunately, there are daily reminders that the bad guys are winning. These headlines, taken from a representative selection of international news stories, give a sense of what a lawless internet could mean. "Two teenage hackers crack Brinks smart safe in less than 30 minutes"; "Pirates hack into shipping company servers to identify booty"; "Islamic State brainwashes youth online"; "Electricity grid at risk, says spy boss".

Despite the increasing coverage of dark side stories, most Australians do not see cyber threats as first order security issues because of the reluctance of governments, and business, to openly discuss the challenge.

Governments worry about revealing sensitive intelligence methods. Companies fear a loss of reputation, or business to competitors in publicly revealing the loss of IP, personal data or money, from a successful hack.

Another reason, according to Alastair MacGibbon, Turnbull's new special adviser on cyber security, is that "we seem to think that cyber attacks have no offline or kinetic effects", unlike a highly visible and obviously destructive terrorist bomb, conventional war or natural disaster. Not being able to see the perpetrator, or vicariously share the anguish of victims, diminishes the emotional impact of a cyber attack.

Regrettably, cyber wars with real kinetic effects are already a reality since it is possible to destroy a power generator with only 21 lines of malicious code, as Russian hackers demonstrated in December, last year, with a devastating attack on Ukraine that left 230,000 Ukrainians in the dark and was the first confirmed hack to take down a power grid.

In championing the virtues of an open, free but secure internet network the national security strategy has struck the right balance between advancing and protecting our economic and security interests in the digital age. But the jury is still out on the ultimate measure of success -- the creation of a dynamic digital economy supported by a resilient cyber network.

Alan Dupont is adjunct professor of international security at the University of NSW and a non-resident fellow at the Lowy Institute.

Tech City News (UK)
Tech: A double-edged sword for national security
Tuesday, 26 April 2016
Byline: Emily Spavin

London - "I remember my first day at Mi6. I thought it was probably going to be nothing like the James Bond books and films. 'It'll just be a desk job', I told myself. I was wrong."
Matthew Dunn now lives in Gloucestershire and writes spy novels for a living - an interesting enough way to earn a crust, but his previous career is much more fascinating.

He served as a British intelligence officer and Mi6 field officer, taking part in around 70 missions that saw him travel the world, moving undercover from one hostile environment to another.

"I was tasked with targeting senior echelons, people who had access to secrets in rogue states that offered significant threats in terms of things like regional conflicts, nuclear conflicts and hostile threats against the West in the guise of intelligence attacks or military attacks," Dunn explained.

He used his training in all aspects of intelligence collection and direct action, including explosives, military unarmed combat, surveillance, advanced driving, infiltration techniques and covert communications, with one particular mission earning him a rare personal commendation from the Secretary of State for Foreign and Commonwealth Affairs.

Gadgetry

As for the role technology played in Dunn's Mi6 career, he explained James Bond-esque gadgetry did exist to some capacity, but not quite to the extent it plays in the Hollywood films.

"Mi6 does have a whole department totally devoted to creating weird and wacky gadgets and other technical equipment. It is actually called the Q department, but I still don't know whether Q in James Bond or Q in Mi6 came first."

Dunn said he was provided with technology such as recording briefcases, surveillance equipment and special weaponry, but explained it was something of a running joke due to its temperamental nature: "The gadgets all worked absolutely perfectly when tested in the head office, but it was often a different story when you tried to use them overseas."

"I'm sure things have come a long way since then, though," he conceded.

The internet has dramatically changed the way the Secret Intelligence Service operates and

the threats faced by the service have certainly developed and mutated, meaning nerds at laptops now often do work previously carried out by men with guns and sharp suits.

In the words of Q in the James Bond epic SkyFall: "I'll hazard I can do more damage on my laptop sitting in my pyjamas before my first cup of Earl Grey than you can do in a year in the field."

Internet

Technology is becoming ever more vital in the protection of national security, particularly within the sphere of counter terrorism. Tech enabled the government to prevent at least seven potentially deadly attacks in the UK last year, however, much more needs to be done to limit the freedom terrorists have in using these same tools to further their plights, promote propaganda and recruit new members.

This January, Baroness Shields, the Minister for Internet Safety, delivered a speech on challenging online extremism. She said the internet is becoming an "echo chamber of hate, fear mongering and intolerance", with terrorist groups like Isis/Daesh being quick to realise and exploit the power of the web. They are running modern and effective global brand marketing campaigns thanks to the borderless and boundary-free nature of social platforms.

"Unlike in the physical world where national governments can take clear and firm actions to keep people safe; there are no such obvious solutions available in the virtual world," she said.

In 2015, the UK's Counter Terrorism Internet Referral unit worked with industry players to remove over 55,000 pieces of terrorist and extremist content. Also last year, YouTube removed 14 million videos in just one instance and, since the middle of 2015, Twitter suspended over 125,000 accounts for threatening or promoting terrorist acts, primarily related to Daesh.

While this is all very positive, it's worth bearing in mind an average of 200,000 Daesh-supporting messages are posted every day on Twitter alone.

Communication

Social media aside, the way in which terrorists communicate has changed significantly, particularly over the past three years. In June 2014, NSA director US Navy Admiral Michael S Rogers said whistleblower Edward Snowden's revelation of government surveillance techniques had lead to some terrorist groups altering their methods of communication.

Among Snowden's revelations was information that the NSA was secretly tapping into Yahoo and Google data centers to collect data from hundreds of millions of account holders across the globe. He also revealed the UK's Government Communications Headquarters (GCHQ) had spied on users of Second Life, Xbox Live and World of Warcraft, and planned to infect millions of computers with malware using a program called Turbine.

While some lauded Snowden a hero, others labelled him a traitor and said revealing government collections partners tipped off terrorists and enabled them to drop those carriers and email addresses. Many have since switched to alternative platforms with encryption.

Last September, head of MI5 Andrew Parker explained that developments in encryption are making Mi5's job harder. Parker told the BBC that encrypted communication services are outpacing the laws required to govern access to data: "Shifts in technology, particularly internet technology, and the use of encryption and so on are creating a situation where law enforcement agencies and security agencies can no longer obtain, under proper legal warrant, the content of communications between people they have reason to believe are terrorists."

Privacy vs protection

Tech giants now, more than ever, have governments knocking on their doors, demanding access to records of users' communications. Thus these companies face, on a daily basis, the struggle of creating a suitable balance between privacy and protection.

In the first six months of 2010, Google received almost 15,000 government requests for user data. By 2014, that number had risen to just under 35,000. The tech giant provided information in over 65% of these cases, but is adamant it will not give in to all government demands.

"The solution, we believe, lies in a principled yet practical approach: one that restricts indiscriminate surveillance and supports valid law enforcement efforts while also protecting people's privacy and security," said Rachel Whetstone, former senior vice president of communications and public policy at Google.

In the UK specifically, parliament is scrutinising the Draft Investigatory Powers Bill - the largest overhaul for 15 years of laws surrounding surveillance. It wants to provide new powers to security services, enabling them to collect tens of thousands of personal records online without ministerial authorisation or oversight.

The Intelligence and Security Committee recently published a report labelling parts of the Bill "inconsistent and largely incomprehensible" and said it lacks clarity on fundamental issues, such as encryption and equipment interference.

Counter-extremism

Whatever the eventual reach of the Bill, is severe surveillance really the answer? Perhaps what is required to boost national security is a bigger drive to turn potential terrorist converts away from the darkened path they're being led down.

Jonathan Russell is head of policy at counter-extremism think tank Quilliam and his organisation focuses on spreading a counter narrative to that proffered by terrorists.

"Counter-extremism has existed for about a decade offline, but in the last three or four years, we have had to shift our focus online," he explained.

Russell said Quilliam's research into how extremists exploit people online has found they "create echo chambers for themselves". They use platforms like Facebook and Twitter, firstly because of the sheer volume of people using those services, but also because the algorithms in use mean they can focus their message without being interrupted by counter-arguments.

"YouTube is the clearest example of that," he said. Watch a Miley Cyrus video, then you'll be presented with related content - another Miley Cyrus video or something similar.

"Exactly the same is true for extremists, except that's worrying because you can just get pushed further and further down a rabbit hole and turn around after an hour or two and have only heard one point of view," explained Russell.

The extremists don't necessarily say anything on social media platforms that promotes violence, because they know that would be taken down, instead they stoke the victimhood narrative, driving opposition to the establishment and painting an overarching picture that the West is at war with Islam.

Most of the messages they produce are about utopia, not brutality, as brutality turns many people off, said Russell.

"They're essentially selling a dream," he added, "and it's up to us to come up with alternative messages and sell a different dream."

Russell stressed that, while Daesh may look like a "medieval death cult", they're using 21st century tools in their plight, so the response needs to be in line with this - they need to be dealt with as if they're a modern brand - a corporation.

"The tools we have available to us with which to respond are not national security tools, they're not related to surveillance, most of them are from the strategic communications and marketing worlds."

Russell said the social media giants have been very good at working with Quilliam and other groups to set up networks and give people in communities the skills to spread counter-extremism messages themselves.

What he'd really like to see, though, is the government doing more to support this kind of approach and for private companies to see this work as part of their corporate and social responsibilities.

"This is the answer, not surveillance. We need to win the war of words and work together to fight the great evil of our time," he concluded.

Vital role

Whatever the specifics, tech has undoubtedly played a vital role in national security over, at least, the past 70 years, and as technology develops, the more integral it becomes.

On a daily basis, it helps the government intercept threats and protect its citizens, but conversely, it enables terrorists to communicate, enemies to intercept confidential information and extremists to recruit.

The war on terror is nowhere near over and both threats and counterterrorism practices will continue to evolve. We now have to rely on the masses, the smartest and the most talented to join the right side of the battle.

NBC News
Ransomware Hackers Blackmail U.S. Police Departments
Tuesday, 26 April 2016
Byline: Chris Francescani

New York - Cyber criminals who have forced U.S. hospitals, schools and cities to pay hundreds of millions in blackmail or see their computer files destroyed are now targeting the unlikeliest group of victims -- local police departments.
Eastern European hackers are hitting law enforcement agencies nationwide with so-called "ransomware" viruses that seize control of a computer system's files and encrypt them. The hackers then hold the files hostage if the victims don't pay a ransom online with untraceable digital currency known as Bitcoins. They try to maximize panic with the elements of a real-life hostage crisis, including ransom notes and countdown clocks.

If a ransom is paid, the victim gets an emailed "decryption key" that unlocks the system. If the victim won't pay, the hackers threaten to delete the files, which they did last year to departments in Alabama and New Hampshire. That means evidence from open cases could be lost or altered, and violent criminals could go free.

Since 2013, hackers have hit departments in at least seven states. Last year, five police and sheriff's departments in Maine were locked out of their records management systems by hackers demanding ransoms.

Ransomware crimes on all U.S. targets are soaring. In just the first three months of 2016, attacks increased tenfold over the total entire previous year, costing victims more than $200 million. Authorities stress that this number only represents known attacks. One federal law enforcement official told NBC News that the "large majority" of attacks go unreported.

The viruses - most of which come from Russia and Eastern Europe -- are typically so impenetrable that even FBI agents have at times advised victims to just pay up and get their data back.

Police computers, however, are especially vulnerable to ransomware, because many small departments have ancient systems.

One chief acknowledged to NBC News that when his department's computers were attacked last year, they were running on DOS, an outdated disc-operating system that dates back to the early 1980s.

"Think about it," said Robert Siciliano, an online safety expert for Intel Security. "You have local law enforcement [which is] provided grants for all kinds of advanced technologies that often revolve around weaponry, but then when it comes to upgrading their desktops laptops -- they may not be up to speed."

Said Siciliano, "It's not unheard of to see a Windows XP or Vista still in action in a law enforcement environment."

'We Are Cops. We Generally Don't Pay Ransoms'

An attack commonly begins when a person opens a piece of malware disguised as a recognizable, sometime personalized e-mail attachment. Once opened, it freezes data block by block until everything is locked.

Then, a ticking countdown clock will often appear on a victim's screen, experts said, with a ransom demand and deadline. Hackers nearly always demand Bitcoins.

Some digital ransom notes include user-friendly instructions on how to buy Bitcoins online, and direct targets to websites that broker anonymous, peer- to-peer financial exchanges.

The attacks are increasingly forcing police chiefs into frustrated deliberations over whether or not -- against all their training and instincts -- to reward extortionists whose identity they may never know.

"My initial reaction was 'No way!" said Sheriff Todd Brackett of Lincoln County, Maine, whose system was frozen last spring. After "48 long hours," Brackett reluctantly paid.

"We are cops," he said with a sigh. "We generally don't pay ransoms."

Last year, the police chief in Durham, New Hampshire, refused to pay, and his files were deleted. He was able to recover most of them from a backup system.

When the Collinsville, Alabama, police department was hit in 2014, the chief refused to pay. He never saw the files again.

What makes the ransoms so maddeningly tempting for cops to pay is that most attacks that have disabled police department computers have sought just a few hundred dollars.

"It's much easier to ask for smaller amounts that you are actually going to get," said Alabama criminal justice professor Diana Dolliver.

Local law enforcement agencies' computer systems can contain plenty of vital -- sometimes even deeply personal -- information, ranging from rape and other violent crime reports to 911 call records, case files of ongoing investigations, personnel records and access to law enforcement databases like the National Crime Information Center (NCIC), which contains criminal case information on federal, state and local investigations.

While authorities say they are not aware of attacks on local law enforcement networks that have resulted in compromised evidence, they believe it is only a matter of time.

Business Is Booming

The attacks on U.S. police are an improbable part of what experts describe as a ransomware epidemic. One new study warns that 2016 "is the year ransomware will wreak havoc on America's critical infrastructure community ...'To Pay or Not to Pay,' will be the question fueling heated debate in boardrooms across the nation."

The business of high-tech extortion is growing exponentially. Last year, the FBI received nearly 2,500 ransomware attack complaints that cost victims $24 million. In the first three months of 2016, ransomware attacks cost Americans another $209 million.

Yet security experts and law enforcement officials agree that the actual figures are likely much, much higher.

"There are a lot of other law enforcement agencies out there that have been affected by this...that don't want their names out there," said Jeff McCliss, a Dickson County, Tennessee- -based detective whose department paid a $622 ransom in Bitcoins.

Many known intrusions have focused on health care facilities, school systems and even small cities -- targets with critical infrastructure, limited security and a constant need for access to their records.

In February, California's Hollywood Presbyterian Medical Center paid a ransom of about $17,000 in Bitcoins, one of at least six major health care systems victimized so far this year. Last month, the city of Plainfield, New Jersey, faced a demand for about $700 in Bitcoins to unfreeze their municipal servers.

Federal investigators say that a majority of the attacks are launched by Eastern European cyber gangs, but there have been few high-profile arrests to date because it's so hard to identify and locate the culprits.

And while early versions of ransomware had to be executed individually, by a human, experts said that today's viruses are fully automated. They are commonly disbursed like spam by the thousands, allowing hackers to execute hundreds of shakedowns simultaneously.

Vulnerabilities 'So Easy to Mitigate'

Ransomware viruses have put federal law enforcement officials in a nearly impossible position. In most cases they can't thwart the attack, apprehend the culprit or retrieve the locked data -- and they know from experience that most victims who pay get their files back.

Yet they're all- too-aware that each payout encourages more extortion.

For several years, multiple federal agencies have issued warning after warning to the public and private sectors urging proper "cyber-hygiene" and stressing the simplicity of the fix -- keep your software up to date and your system regularly backed up.

"This is so easy to mitigate," the federal official said.

While the FBI now explicitly advises against paying ransoms, individual agents have been known to nudge victims in that direction.

"To be honest, we often advise people to just pay the ransom," Joseph Bonavolonta, a Boston FBI cyber and counterintelligence specialist, told a security conference last fall. "The ransomware is that good."

Those comments drew headlines in the tech industry press, and prompted a clarifying statement from the FBI.

"The FBI doesn't make recommendations to companies," the agency told Naked Security last October. "[I]nstead the Bureau explains what the options are ... and how it's up to individual companies to decide for themselves the best way to proceed ... either revert to back up systems, contact a security professional, or pay."

Earlier this month, an FBI spokeswoman issued a statement to NBC News which said, in part, that "The FBI does not condone payment of ransom, as payment of extortion monies may encourage continued criminal activity, lead to other victimizations, or be used to facilitate serious crimes."

Bonavolonta could not immediately be reached for comment.

The Department of Homeland Security offers cyber-safety training to state and local governments and conducts "red team" tests on municipal systems to determine how secure they are. The FBI offers similar training in the private sector.

"It's really important for people to know [that] we can help," said Dr. Andy Ozmant, DHS assistant secretary for cybersecurity and communications. "We have a lot of resources available."

Compromised Evidence?

Experts said that ransomware attacks can have a potentially devastating impact on a municipality's criminal justice system.

"A good defense attorney is going to raise a question about whether or not evidence had been tampered with," said Dolliver. "That's the part I've actually been really watching for, but have not seen it come up in court cases."

Lincoln County law enforcement officials brought the same concerns to their local prosecutors, who concluded that none of the recovered data was ever actually breached.

So far at least, legal experts said, most ransomware cases have not necessarily tainted evidence.

"If the computer is simply held hostage but there is no evidence that any files have been altered, there will be no problem," said Steven Saltzburg, a George Washington University law professor who co-authored the 2013 Federal Criminal Procedures Litigation Manual. "If there is evidence that files have been altered, that is a problem."

'Last Laugh'

The ransomware attacks on U.S. police have left more than a few chiefs privately fuming, including Sheriff Brackett.

In a last-ditch bid to strike at least a tiny blow on behalf of U.S. law enforcement against ransomware extortionists, Brackett and his IT team paid the Bitcoin ransom, received the decryption key, cancelled the payment, and unlocked their system.

"We got the last laugh," Brackett thought to himself at the time.

Two days after his bait-and-switch scheme, hackers struck again.

This time the ransom was about $500.

This time Brackett paid and walked away.

The Register (UK)

Hackers so far ahead of defenders it's not even a game
Tuesday, 26 April 2016
Byline: John Leyden

London - Cybercriminals are way ahead of the game against defenders without having to try anything new, according to the latest edition of Verizon's benchmark survey of security breaches.
The study shows that miscreants have no need to switch up, because the same old tactics are still working fine. Security defenders are still performing poorly in their attempts to defend against hacking or malware-based attacks. This isn't for a lack of trying or skills on their part, but almost completely down to the fact that the game is rigged against them.

Verizon's ninth annual Data Breach Investigations Report (DBIR) provides an analysis of over 100,000 security incidents and 3,141 confirmed data breaches last year, drawing on real-world data breach caseloads handled by either Verizon or around 50 other contributing organisations.

Those involved include the US Secret Service, the European Cyber Crime Center (EC3), UK CERT and the Irish Reporting and Information Security Service (IRISS CERT), amongst others.

Hackers are getting faster whilst defenders are treading water. Over 99 per cent of attacks compromise systems within days (four out of five do it within minutes), and two-thirds of those siphon off data within days (a fifth do it in minutes). Whilst there was an improvement in the number of breaches detected in 'days or less' noted in the last DBIR, that turned out to be a temporary blip. This year, less than a quarter of breaches were detected within the same timeframe - meaning attackers have almost always gotten away with the goods before anyone notices.

Worse yet, it's usually not the victim that notices the breach, but a third party (normally either a security researcher or law enforcement).

Nearly two-thirds of all breaches are still traced back to weak or stolen passwords - a basic security failure.

"People are not sitting in front of consoles, looking for SQL Injections before running a manual attack," Dave Ostertag, global investigation manager at Verizon told El Reg. "They are stealing credentials, planting malware, pivoting and exfiltrating data."

Hackers have begun using multiple exfiltration points to avoid detection, Ostertag added.

Phishing lures

Phishing (which "is efficient and works really well," according to Ostertag) remains a huge problem and a major factor in most breaches. The DBIR found that nearly a third of phishing emails get opened, and more than one in ten recipients open the attachments, a significant rise from last year. The main

perpetrators of these attacks are organised crime syndicates, but nearly one in ten can be attributed to a state-affiliated actor. China accounts for more than half of all cyber- espionage attacks by volume last year, according to Ostertag, who nonetheless welcomed the recent US/China no hack pact as a positive development.

Public sector, manufacturing and professional services firms top the hit list of targets for cyber-espionage. Attackers are using phishing scams and pilfered passwords to open up a backdoor onto enterprise networks. This foothold is used to smuggle malware into targeted networks. Corporate networks would be far harder to attack - even with access credentials - in cases where enterprises had applied two-factor authentication. However, failure in this area was yet another security shortcoming identified during Verizon's study.

"Many victims have single- factor access into parts of their network even if they think otherwise," according to Ostertag.

On the cybercrime-for-profit front, ransomware is a problem across the board in manufacturing, the public sector and healthcare, Verizon reports. Cybercrooks, like cyber-spies, often rely on phishing.

"Hackers do their homework using social media like LinkedIn and other sources to know who to target, and what sort of content is likely to be opened," Ostertag explained.

"Cybercrooks are going after people who initiate or manage financial transactions."

Older threats such as phishing, malware and weak passwords predominate in breaches. By contrast, the much- discussed security risks from the Internet of Things and mobile phones barely register in Verizon's breach study.

Wall Street Journal
The Encryption Farce
Tuesday, 26 April 2016
Byline: Editorial Board

Editorial - If history repeats itself first as tragedy and then as farce, what does the FBI have in store next for its encryption war with Apple? After withdrawing its demands in San Bernardino and then reopening hostilities with a drug prosecution in Brooklyn, the G-men abruptly dumped the second case over the weekend too. Is anyone in charge at the Justice Department, or are junior prosecutors running the joint? The FBI claimed for weeks in a California court that it couldn't unlock the iPhone of terrorist Syed Farook unless Apple was compelled to create a new operating system, but then reported at the 11th hour that an unspecified outside party had engineered a solution that didn't require Apple's help. Justice lawyers also insisted the purpose of the litigation wasn't to create a legal precedent, but that such extraordinary commandeering was an exception for "one phone" related to terrorism.

This claim never stood up to scrutiny, given the nationwide profusion of such cases. But the Brooklyn flame-out is especially instructive about the FBI-Justice method without the crutch of invoking the fast-moving terror exigencies or uncovering potential domestic cells.

The iPhone in question was seized when the feds arrested a methamphetamine dealer called Jun Feng in 2014. Feng isn't dead, like Farook; he merely said he couldn't remember his password. Justice waited more than a year to try to force Apple to break the device, and shortly after these proceedings were initiated Feng and his codefendants copped guilty pleas.

Justice said the case wasn't moot because the device's data could yield evidence of other drug trafficking. FBI Director James Comey has suggested that the San Bernardino software exploit is no use on other iPhone models.

Yet while Justice argued in Brooklyn that Apple's help was essential, it also argued the FBI had no obligation to pursue a non-Apple work-around. The remarkable claim was that prosecutors need not exhaust all possible alternatives before conscripting a private company, such as consulting with other U.S. agencies, hiring an outside digital forensics outfit or even interrogating Feng again.

Such assertions were as false in Brooklyn as in San Bernardino. Two hours and a half before a deadline on Friday night, the government withdrew the case after "an individual provided the passcode to the iPhone," according to legal filings. This second immaculate conception in as many months further undermines the FBI's credibility about its technological capabilities. Judges ought to exercise far more scrutiny in future decryption cases even as Mr. Comey continues to pose as helpless.

The FBI Director recently said at Kenyon College that the end of the San Bernardino affair was "a very good thing," because "litigation is a terrible place to have any discussion about a complicated policy issue, especially one that touches on our values, on the things we care about most, on technology, on trade-offs, and balance." He added that "it will be bad thing if the conversation ended."

Yet forgive us if this "conversation" now seems more like a Jim Comey monologue. The debate might start to be productive if the FBI Director would stop trying to use the courts as an ad hoc policy tool and promised not to bring any more cases like the one in Brooklyn.

Meanwhile, the White House has taken the profile- in-courage stand of refusing to endorse or oppose any encryption bill that Congress may propose. If the Obama team won't start adjusting to the technological realities of strong and legal encryption, they could at least exercise some adult supervision at Main Justice.

New York Times
Obama Stresses Data in Terrorism Fight

Tuesday, 26 April 2016
Byline: Mark Scott

Berlin - The trans-Atlantic debate over digital privacy rights versus the surveillance needs of intelligence agencies was put under a spotlight on Monday, as President Obama called for continued access by law enforcement officials to thwart terrorism, while some European privacy advocates urged greater restraint.
"I want to say this to young people who value their privacy and spend a lot of time on their phones: The threat of terrorism is real," Mr. Obama said, speaking at a trade show in Hanover, Germany.

"I've worked to reform our surveillance programs to ensure that they're consistent with the rule of law and upholding our values, like privacy -- and, by the way, we include the privacy of people outside of the United States," he added.

Mr. Obama's message comes at a sensitive time, as cities like Brussels and Paris are still recovering from recent terrorist attacks. But his words are unlikely to slow down European efforts to expand people's control over their digital lives.

Europe is at the heart of a global debate over the way companies like Google and Facebook, as well as national intelligence agencies, handle people's digital data. Some regulators in the 28-member bloc have called on companies and governments, particularly that of the United States, to comply with the region's tough privacy regulations.

"Those who want to play in our backyard must play by our rules," Viviane Reding, a member of the European Parliament from Luxembourg and a former top European Union official, said on Monday at a privacy conference in Berlin. "Protection of our personal data shouldn't have a national barrier."

Ms. Reding is an author of a European Union privacy law that will go into force in 2018. It will be able to impose fines of up to 4 percent of a company's global revenue for the most serious breaches of European data protection rules. Those penalties would apply to any company -- even if it has no physical presence in Europe -- that has customers within the European Union.

At issue are communications via cellphones, as well as data generated in social media, online searches and e-commerce purchases.

The protections pursued in the European Union include the so-called right to be forgotten, detailed by the bloc's highest court, which requires search giants like Google to remove links to online information in some cases.

And Europe's national privacy regulators have vowed to take a tough line against a new pact between the United States and the European Union that is intended to ensure the relatively unimpeded flow of

personal data across the Atlantic. The national regulators are wary of the ability of American law enforcement and intelligence agencies to monitor data to fight crime or terrorism.

But American agencies, including the Commerce Department and the Federal Trade Commission, argue that they actively monitor companies' access to individuals' digital data. They say that American privacy safeguards -- including the United States Constitution -- often provide better protection than the rules in other jurisdictions, including those in Europe.

"We care about Europeans' privacy," Mr. Obama said in Hanover, "not just Americans' privacy."

Many European officials acknowledge that the region's privacy laws share many similarities with those in the United States. But they also highlight important differences, including the lack of overarching federal privacy legislation. The differences, they say, must be bridged if Europe and the United States are to effectively supervise the way companies like Facebook and Google gain access to data worldwide.

"The digital world is globalized," Giovanni Buttarelli, the European Union's data protection supervisor, said at the Berlin conference on Monday. "So data protection should also be globalized."

The Intercept
Spy Chief Complains That Edward Snowden Sped Up Spread of Encryption by 7 Years
Monday, 25 April 2016
Byline: Jenna McLaughlin

Washington - The Director of National Intelligence on Monday blamed NSA whistleblower Edward Snowden for advancing the development of user- friendly, widely available strong encryption.
"As a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years," James Clapper said during a breakfast for journalists hosted by the Christian Science Monitor.

The shortened timeline has had "a profound effect on our ability to collect, particularly against terrorists," he said.

When pressed by The Intercept to explain his figure, Clapper said it came from the National Security Agency. "The projected growth maturation and installation of commercially available encryption -- what they had forecasted for seven years ahead, three years ago, was accelerated to now, because of the revelation of the leaks."

Asked if that was a good thing, leading to better protection for American consumers from the arms race of hackers constantly trying to penetrate software worldwide, Clapper answered no.

"From our standpoint, it's not ... it's not a good thing," he said.

Technologists have been tirelessly working to strengthen encryption for decades, not just the past few years. But Snowden's revelations about the pervasiveness of mass surveillance clearly accelerated its more widespread availability.

And technologists say the threat of law enforcement "going dark" has been overhyped. For instance, there are almost always ways to hack around encryption, even if you can't break it.

Clapper acknowledged that there is no such thing as unbreakable encryption from his perspective. "In the history of mankind, since we've been doing signals intelligence, there's really no such thing, given proper time, and proper application of technology."

Christian Science Monitor
Encryption hindering efforts to stop Islamic State, intelligence director says
Monday, 25 April 2016
Byline: Anna Mulrine

Washington - The Edward Snowden leaks have accelerated the sophistication of encryption technologies by "about seven years," Director of National Intelligence James Clapper told reporters this morning. And that is not a development to be celebrated, he added in remarks at a breakfast hosted by The Christian Science Monitor.

"From our standpoint, it's not a good thing."

New, commercially available encryption software "had and is having major, profound effects on our ability" to collect intelligence, "particularly against terrorists," he warned.

That's in large part because the Islamic State is "the most sophisticated user by far of the Internet." They privately purchase software that "to ensure end-to-end encryption" of their communications.

"And so that is a major inhibitor to discerning plotting, principally by ISIL and others," Mr. Clapper said, using one acronym for the Islamic State.

The seven year estimation comes from the National Security Agency, he said.

It raises the issue of the tension between the need for security against cyber attacks - which as recently as February Clapper cited as a greater threat than terrorism - and the opposition to law enforcement against so-called unbreakable encryption software that, they say, could hinder their search for terrorists.

Clapper for his part echoed President Obama's warning against "absolutist positions" on the topic. "Somehow, we need to find a balance here," he said. "I don't know the technicalities of how we might

arrive here, how we thread the needle" between how to "ensure privacy and security on an individual basis, as well as security in the context of what's best for the collective good."

At the moment, he added, that goal "is an elusive holy grail that we're pursuing."

That said, he warned that the development of unbreakable encryption, which he likened to the possibility that that it could, in essence, "give the terrorists a pass."

Clapper warned Monday that the group has clandestine cells that are plotting more terrorist attacks in Germany, Italy, and England.

To this end, the United States is stepping up efforts to promote more intelligence sharing. In the meantime, since the recent IS attacks on Paris and Brussels, US intelligence officials have learned some things about the terrorist group, he said.

For starters, they are "very op-sec conscious," Clapper said. A former Air Force lieutenant general, he was using military parlance for "operational security."

It is clear that IS is also taking advantage of the migrant crisis in Europe, he added.

And that poses a formidable challenge for Europe. There is a "fundamental conflict" between European Union incentives and drives to promote openness and free movement of people and goods with privacy, "which is in some ways in conflict with the responsibilities that each country has as a nation-state to protect the borders and securities of their nations and peoples," Clapper said.

Times of Israel
The programming school that keeps the IDF running
Tuesday, 26 April 2016
Byline: David Shamah

Jerusalem - You can't shake a stick in Israel's technology scene without hitting a graduate of the IDF's famous Unit 8200, which has produced CEOs and CTOs of some of the world's most successful tech and cyber-security firms. All of those soldiers passed through the IDF Computing and Cyber Defense Academy, which runs dozens of courses for the many tech needs of the modern Israeli army.
"The Israeli army faces challenges large and small, from the sakin to the gar'in" -- threats ranging from stabbing attacks to nuclear weapons, according to Major Dor Cohen, head of the programming section of the Academy.

There is today one common denominator that powers all of the army's defensive efforts, he said. "It's fair to say that technology is the basic building block of any defense effort these days, large or small," said Cohen.

"Programming, cyber-defense tactics, app development, and other technology are the backbone of all parts of the IDF today, from systems like Iron Dome and David's Sling that defend against missile attacks to programs that can quickly issue deployment orders and ensure that soldiers and reservists get where they need to be quickly to ensuring that supplies, parts, personnel, and everything else arrives where it is supposed to. I'm proud to say that the academy is ground zero for the training of the personnel needed to master the technology to do this."

Part of the C4i Computer Services Directorate, the academy hosts dozens of courses at its campus, including, for example, Shahar, the tech-oriented "little brother" of the much more well-known Nahal Hareidi program, which deploys ultra-Orthodox soldiers in the field, on patrols and in combat duty.

The Programming division teaches students basic and advanced knowledge in computer languages, app development, cyber-security, firewalls, hacking projects - anything needed to navigate the world of programming and networks, with the objective to quickly, neatly, and effectively deploy systems that help protect Israel.

Speed of response is one of the important skills taught, said Cohen. "We learned this all too well in 2014's Operation Protective Edge, when things changed minute to minute. In most organizations you have levels of administration and approval that require supervisors to sign off on projects, and the process could take weeks. Cyber-threats and other matters came up throughout the war, and we needed to respond within hours."

In addition, apps are becoming increasingly important in the IDF, said Cohen. "Everyone today carries around in their pocket a super-sophisticated computer that can be used to provide directions, information, warnings, and other vital information. There is no reason not to use these devices and their capabilities in defending Israelis. Of course, the apps and the system have to be secure."

In February, the Academy sponsored a hackathon in which hundreds of soldiers developed apps and technologies that could respond to the issues faced by soldiers in the field. "Our courses teach programmers to develop apps using secure technologies the IDF has developed," said Cohen. "There is a great demand throughout the various forces for these apps, and we get many requests for solutions using these devices."

One of the greatest challenges Cohen faces is finding the personnel to fill the growing number of programming jobs throughout the IDF. "As everyone knows, there are not enough kids studying math and science in high schools, and we are part of the effort to encourage more students to take on those subjects," said Cohen. "But we don't strictly rely on the educational system to produce the candidates

we need. We review the records of IDF recruits and check their aptitudes, and if we find a likely candidate we lobby them to join our program."

According to Cohen, his program can take recruits who know almost nothing about computers or programming and turn them into programmers with very good to excellent skills.

Of course, a lot of hard work goes into creating programmers "from scratch" - both on the part of the candidates themselves and on the part of Cohen's staff. Fortunately, they are up to the task, he said.

"Many of the teachers in the program are themselves graduates, very highly motivated - enough to remain in the army and to help develop the new generation of programmers instead of going into private enterprise."

And although many highly motivated young Israelis prefer service in combat units, there's plenty of action - and prestige - in the army's programming and cyber units, said Cohen. "Our soldiers don't fight in the field in the same way Golani and Givati unit soldiers fight, but they are engaged in extremely important defense projects.Tech is now the basis of warfare. Without our people, the army cannot move an inch."

Fox News
Did anti-Israel bias keep France from getting terror tech before Paris attacks?
Tuesday, 26 April 2016
Byline: Hollie McKay

Washington - Shortly after the Charlie Hebdo attack in Paris, and nearly a year before terrorists killed 130 in coordinated strikes that rocked the City of Light, French security officials rejected an Israeli company's offer of terrorist-tracking software that could have helped them flag the deadly terror cell, a security expert said.
The offer of data- mining technology that would allow French authorities to "connect all the dots" in the Islamist extremist community was made to the Directorate- General for Internal Security, France's main intelligence agency. It is used to analyze and match up fragmented intelligence reports from several national and international databases, giving counter-terrorism agents the most up-to-date information on potential terrorists available.

The overture was rejected.

"French authorities liked it, but the official came back and said there was a higher-level instruction not to buy Israeli technology," a well-placed Israeli counter-terror specialist familiar with the technology and the company behind it told FoxNews.com. "The discussion just stopped."

The Israeli source declined to name the company or detail the technology, which has been shared with the U.S. and other nations on good terms with Israel, other than to say it scans databases from multiple agencies and Interpol and pinpoints "high-risk" people. But he believes it could have given French authorities a chance at stopping the Nov. 13, 2015, attacks in Paris, and possibly the coordinated bombings in Brussels that killed 32 on March 22.

"Government agencies struggling to foil terror attacks need access to technologies that allow them to connect their data fragments, making it possible to handle daily data challenges," the source said. "With this system, all data can then be easily navigated, processed and represented by employing a set of powerful analytic tools and unique algorithms."

The offer followed Israeli Prime Minister Benjamin Netanyahu's pledge to work closely with Europe on enhancing security in the wake of the Brussels attacks, taken in Israel as a call for intelligence and technology sharing.

"In Paris or Brussels or San Bernardino or Tel Aviv or Jerusalem, terror must be condemned equally and it must be fought equally," Netanyahu said. "Israel stands ready to cooperate with all the nations in this great struggle."

No official reason was given for France's rejection of the offer, and the source acknowledged it could have been triggered by legitimate concerns about hacking vulnerability. Yet many suspect politics was to blame.

"The European Union has blamed Israel for everything that is happening in the Middle East and stopped cooperation in regards to military, law enforcement and intelligence training and banning university cooperation which [generates] much of the technology to fight terrorism," said Itamar Gelbman, a former IDF Special Forces and who is now a counter-terrorism consultant.

DGSI did not respond to requests for comment and a European Union official told FoxNews.com that there is no formal French, or wider EU ban, on purchasing technology products made in Israel. However, tensions between the European Union and Israel have heightened in recent years, primarily over claims the Jewish State illegally occupies Palestinian territories.

The Israeli-Palestinian conflict has long divided the international community. Human rights groups routinely condemn Israel for repressing and harshly retaliating against Palestinian aggression, while Israel remains staunch that it acts in self-defense and to protect its people.

Kamal Nawash, an American attorney and president of the Free Muslims Coalition, noted that Europe's tough stance against Israel and hesitation in making technology purchases is an "example of the global community sending a message to Israel that its treatment of the Palestinians is unacceptable."

"Israel would be wise to change its treatment of Palestinians by providing them with civil and human rights and pursuing a desegregation policy in general," Nawash said. "Otherwise, Israel may experience the same fate as South Africa during the apartheid era with all the countries of the world boycotting Israel."

The recent spate of terror attacks on European soil could bring about a resurgence in investment with Israeli tech and intelligence companies, given its undisputed status as a global leader in the field.

"Israel has been facing terror threats since its inception in 1948," said Gilles Perez, manager of HLS & Aerospace Unit at the Israel Export Institute. "In the 1970s, it was Israel's national airline that pioneered the concept of an undercover security officer on every commercial flight long before it was adopted by other countries after September 11, almost 40 years later."

Security at airports, such as Zaventem Airport in Brussels, where last month's bombing occurred, has long been an area of Israeli expertise. But intelligence, such as the system offered to French officials, could be even more crucial, said Col. Eran Lerman, former deputy chief of Israel's National Security Council and senior IDF Military Intelligence division director.

"However, the key to successful security has to be intelligence, in the broader sense of the word," Lerman told Homeland Security Today. "For too many years, for very good reasons, Europeans have neglected the need for effective intelligence measures."

Israel-based security training expert Daniel Sharon said that since the Brussels attacks last month there has been particular interest in airport and aviation security prevention concepts, interest that transcends popular protest.

"The goods are boycotted in European supermarkets," Sharon said. "But when they are in trouble they run to Israel for help."

Less than a week after the attacks in Brussels, Belgian law enforcement bought advanced surveillance and rapid view technology from Israeli company BriefCam. The technology is already in use at the Statue of Liberty and various U.S. airports, said President and CEO Dror Irani.

Israel's tech and security sector has long been an incubator for anti-terror solutions, say experts. The more France and Europe in general are threatened, the more willing they may be to work with companies based in the Jewish state.

"Israel is leading the field in counter-terrorism technology, but it's not a popular country," said Ari Zoldan, CEO of technology and e-commerce firm Quantum Network. "It is unlikely that Israel will suddenly become popular, but the need for better national security will force people to work with Israeli solutions."

Reuters

Bangladesh Bank hackers compromised SWIFT software, warning to be issued

Tuesday, 26 April 2016

Dhaka - The attackers who stole $81 million from the Bangladesh central bank probably hacked into software from the SWIFT financial platform that is at the heart of the global financial system, said security researchers at British defense contractor BAE Systems.
SWIFT, a cooperative owned by 3,000 financial institutions, confirmed to Reuters that it was aware of malware targeting its client software. Its spokeswoman Natasha Deteran said SWIFT would release on Monday a software update to thwart the malware, along with a special warning for financial institutions to scrutinize their security procedures.

The new developments now coming to light in the unprecedented cyber-heist suggest that an essential lynchpin of the global financial system could be more vulnerable than previously understood to hacking attacks, due to the vulnerabilities that enabled attackers to modify SWIFT's client software.

Deteran told Reuters on Sunday that it was issuing the software update "to assist customers in enhancing their security and to spot inconsistencies in their local database records."

The software update and warning from Brussels-based SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, come after researchers at BAE, which has a large cyber-security business, told Reuters they believe they discovered malware that the Bangladesh Bank attackers used to manipulate SWIFT client software known as Alliance Access.

BAE said it plans to go public on Monday with a blog post about its findings concerning the malware, which the thieves used to cover their tracks and delay discovery of the heist.

The cyber criminals tried to make fraudulent transfers totaling $951 million from the Bangladesh central bank's account at the Federal Reserve Bank of New York in February.

Most of the payments were blocked, but $81 million was routed to accounts in the Philippines and diverted to casinos there. Most of those funds remain missing.

Investigators probing the heist had previously said the still-unidentified hackers had broken into Bangladesh Bank computers and taken control of credentials that were used to log into the SWIFT system. But the BAE research shows that the SWIFT software on the bank computers was probably compromised in order to erase records of illicit transfers.

Deteran reiterated on Sunday that "the malware has no impact on SWIFT's network or core messaging services."

The SWIFT messaging platform is used by 11,000 banks and other institutions around the world, though only some use the Alliance Access software, Deteran said.

SWIFT may release additional updates as it learns more about the attack in Bangladesh and other potential threats, Deteran said. SWIFT is also reiterating a warning to banks that they should review internal security.

"Whilst we keep all our interface products under continual review and recommend that other vendors do the same, the key defense against such attack scenarios is that users implement appropriate security measures in their local environments to safeguard their systems," Deteran said.

Adrian Nish, BAE's head of threat intelligence, said he had never seen such an elaborate scheme from criminal hackers.

"I can't think of a case where we have seen a criminal go to the level of effort to customize it for the environment they were operating in," he said. "I guess it was the realization that the potential payoff made that effort worthwhile."

A Bangladesh Bank spokesman declined comment on BAE's findings. A senior official with the Bangladesh Police's Criminal Investigation Department said that investigators had not found the specific malware described by BAE, but that forensics experts had not finished their probe.

Bangladesh police investigators said last week that the bank's computer security measures were seriously deficient, lacking even basic precautions like firewalls and relying on used, $10 switches in its local networks.

Still, police investigators told Reuters in an interview that both the bank and SWIFT should take the blame for the problems.

"It was their responsibility to point it out but we haven't found any evidence that they advised before the heist," said Mohammad Shah Alam, head of the Forensic Training Institute of the Bangladesh police's criminal investigation department, referring to SWIFT.

The BAE alert to be published on Monday includes some technical indicators that the firm said it hopes banks could use to thwart similar attacks. Those indicators include the IP address of a server in Egypt the attackers used to monitor use of the SWIFT system by Bangladesh Bank staff.

The malware, named evtdiag.exe, was designed to hide the hacker's tracks by changing information on a SWIFT database at Bangladesh Bank that tracks information about transfer requests, according to BAE.

BAE said that evtdiag.exe was likely part of a broader attack toolkit that was installed after the attackers obtained administrator credentials. It is still not clear exactly how the hackers ordered the money transfers.

Nish said that BAE found evtdiag.exe on a malware repository and had not directly analyzed the infected servers. Such repositories collect millions of new samples a day from researchers, businesses, government agencies and members of the public who upload files to see if they are recognized as malicious and help thwart future attacks.

Nish said he was highly confident the malware was used in the attack because it was compiled close to the date of the heist, contained detailed information about the bank's operations and was uploaded from Bangladesh.

While that malware was specifically written to attack Bangladesh Bank, "the general tools, techniques and procedures used in the attack may allow the gang to strike again," according to a draft of the warning that BAE shared with Reuters.

The malware was designed to make a slight change to code of the Access Alliance software installed at Bangladesh Bank, giving attackers the ability to modify a database that logged the bank's activity over the SWIFT network, Nish said.

Once it had established a foothold, the malware could delete records of outgoing transfer requests altogether from the database and also intercept incoming messages confirming transfers ordered by the hackers, Nish said.

It was able to then manipulate account balances on logs to prevent the heist from being discovered until after the funds had been laundered.

It also manipulated a printer that produced hard copies of transfer requests so that the bank would not identify the attack through those printouts, he said.

Globe and Mail
Disclosure issues linger over police surveillance techniques
Tuesday, 26 April 2016
Byline: Colin Freeze

Canadian detectives cannot keep secret their advanced spying devices or their relationships with telecommunications corporations because claims of police privilege carry little or no weight in criminal courts.
So ruled Quebec Superior Court Justice Michael Stober as he ordered several modern police surveillance techniques disclosed to lawyers representing six accused mobsters in Montreal.

Finding that police arguments for secrecy rely at times upon "selfserving and weak" legal logic, his decisions have laid bare RCMP tactics.

From the Stober disclosure rulings flowed the recent revelation that the Mounties use a device that mimics a cellphone tower.

The fact that Canadian federal agents also have access to a version of a virtual skeleton key, one that can crack coded BlackBerry communications, has also been exposed.

Police had fought for years to protect such methods from becoming broadly known, until a cat-and-mouse criminal case pitting the RCMP against the Montreal six forced Justice Stober to consider 21st-century techniques.

A publication ban was imposed on his rulings about pretrial disclosure when they were issued last fall, but redacted versions were filed in a higher court this spring. On March 30, the Quebec Court of Appeal in Montreal was to revisit the Stober decisions.

But on the morning that matter was to be heard, the Crown lawyers who appealed the rulings walked away from the underlying first- degree-murder case.

Across town in Laval, the six people arrested in 2011 were acquitted of that charge and pleaded guilty to the lesser charge of conspiracy to murder.

That outcome freed the Crown of its obligation to make increasingly uncomfortable amounts of disclosure and left the appellate judges with no case to consider.

Court decision or no court decision, however, important disclosure issues remain for police, lawyers and judges across Canada.

Here's the question: If police want to borrow from the playbooks of modern spies and advance their investigations with secret surveillance techniques or the help of telecommunications corporations, can they prevent those methods from being revealed during prosecutions?

The court of Justice Stober, which has had a unique exposure to those issues, ruled that the answer is a resounding no. "The interests of the accused in having a fair trial where the accused is able to make full answer and defence outweighs the public interest in protecting police-investigative techniques," he ruled.

The case was extraordinary in several ways. The judge heard police pleas for secrecy in several closed pretrial proceedings from which the accused and their defence lawyers were barred. To balance the scales, the court took the extraordinary step of allowing Toronto lawyer Anil Kapoor, who has national-security clearance, to make arguments on the defence's behalf.

What emerged as a result of these hearings is that, while police in Canada may have plenty of protections to keep human informants anonymous, they have no analogous legal safeguards for surveillance technology or corporate relationships.

Yet, federal agents remain loath to reveal their techniques because they feel they are in an arms race with savvy adversaries.

In the Montreal case, each suspect had multiple unregistered BlackBerrys, and they talked to each other through the company's proprietary encoded "PINto-PIN" texts. Detectives within the RCMP's technological units saw a murder conspiracy take shape in those messages, but it came into focus only through painstaking work.

First, the Mounties had to use a portable cellphone-tower simulator (often known as a "IMSI catcher") to draw data that revealed which handsets in a certain area were controlled by the suspects.

Then, police served assistance orders on BlackBerry directing the Waterloo company to help facilitate interception of the suspects' messages - which were cracked with a version of the company's "global encryption key" that RCMP had somehow acquired.

In more mundane crimes, defence lawyers challenge the accuracy of police breathalyzers and radar guns. In the case at hand, lawyers Frank Addario and Mike Lacy pushed for increasing amounts of detail about police techniques. At one point, they even persuaded Justice Stober to order police to hand over their version of the BlackBerry key so that the defence lawyers for the accused could test it.

Prosecutors and police pushed back hard on that front, saying that would be like letting go of a skeleton key that could open tens of millions of houses. A BlackBerry executive swore a last-minute affidavit saying such a move could undermine customers' trust. In the end, Justice Stober withheld the key, even as he ordered other surveillance techniques disclosed.

At one point, an RCMP inspector testified that a degree of secrecy is needed because being seen to help police is "not good marketing" for tech companies. But Justice Stober characterized such arguments as "weak and self-serving." As a Canadian judge, he said, he had no legal basis to consider any "adverse impact on [Blackberry's] business interests."

The bottom line for the Crown was that Justice Stober's disclosure orders could yield "a new and thorough body of information that would educate the criminal element," or even provide it with "a user guide on how to circumvent a level of secrecy the State is entitled to protect." This, at least, is what the Crown appeal had put forward, until the surprise plea arrangement between the Crown and defence scuttled the hearing.

The Australian
Cybersphere globe's new battlefront
Tuesday, 26 April 2016
Byline: Alan Dupont
Section: oped

If the ambitious goals of Malcolm Turnbull's just released cyber security strategy are achieved, the document could turn out to be the most important and innovative government strategy yet written. Its great strength is that it provides a clear plan for harnessing Australia's transitioning economy to the enabling technology of the internet, while recognising that a secure cyber space is critical to exploiting the benefits of the digital age and to protecting our interests online.

Turnbull's aim is to make Australia a cyber smart nation. This is a formidable undertaking requiring sustained investment in cyber architecture and intellectual capital, major cultural change and a genuine cyber partnership between government, business and the wider community that has yet to materialise.

His starting point is that the internet is the most transformational technological development in human history and therefore central to Australia's future prosperity and security. It's hard to argue with this proposition. Australia is already a wired economy. Nearly 90 per cent of Australians are online, including 84 per cent of small and medium businesses. The internet-based economy contributed $79 billion, or 5.1 per cent of GDP, in 2014 which could grow to $139bn, or 7.3 per cent of GDP, by 2020. By 2019, the average Australian household will have 24 devices connected online.

But it's not just humans who are connecting to the internet. Machines are, too, in ever increasing numbers. Cars, fridges, power plants -- just about every device we use has the capacity to communicate autonomously with other machines. By 2020, the government estimates there may be 50 billion devices connected to the internet globally. Cybersecurity pioneer John McAfee believes the figure is likely to be 212 billion. The Internet of Things is increasingly the Internet of Everything.

Australia has been slow off the mark to understand and capitalise on the enormous economic -potential of this cyber revolution. We have too few cyber entrepreneurs; business still regards cyber security as a technological, rather than a strategic issue; and there is an educational and vocational mismatch between what the digital economy needs and what our schools and universities provide. We are a long way from being a cyber smart nation.

By contrast, a small country like Israel has embraced the cyber revolution, attracting 20 per cent of global private sector investment in the burgeoning cyber security industry and joining the US, Russia, China and Britain as an emerging cyber power. Israel is nurturing a new generation of cyber-literate young people in its universities and schools, right down to primary school level.

The good news is that the cyber security strategy puts Australia on a path to addressing our digital deficiencies by fostering a new network of cyber research and innovation.

At its hub will be a cyber security growth centre that will define and prioritise cyber challenges. Cyber security centres of excellence in universities will be established to help address the serious shortage of cyber security professionals. They will be linked to previous STEM initiatives designed to boost our dwindling stocks of scientists, technologists, engineers and mathematicians.

However, these commendable steps and the accompanying four-year commitment of $230 million are insufficient to realise Turnbull's vision, which requires nothing less than a cradle-to-grave investment of a kind rarely seen in Australia, starting with primary school education. Cyber literacy has to become an intuitive and foundational skill for all Australians.

A second impediment to realising the full potential of the internet is malicious cyber attacks, which have grown exponentially in number and sophistication over the past decade.

An estimated one million Australians were victims of online identity fraud in 2014 and cyber crime may be costing the economy as much as $17bn annually. One in three Australian businesses have experienced some form of cyber crime.

Professional services firm Deloitte ranks Australia as one of the five most vulnerable economies to cyber attacks in the Asia Pacific region.

The loss of intellectual property and state secrets in electronic smash and grab burglaries is an even more serious issue, because they are the crown jewels that determine a country's competitive position and capacity to defend -itself. Malicious actors inhabit the cyber world's dark side and include criminals, terrorists, spies and hostile states. They undermine trust in the reliability and security of the internet. So improving our cyber defences and sensitising Australians to the risk is central to the strategy's success.

The core problem is finding the right balance between protecting users through better security and regulation, and maintaining an open and free system. In Turnbull's words, "we must ensure that the

administration of the internet continues to be governed by those who use it -- not dominated by governments. Equally, cyberspace cannot be allowed to become a lawless domain".

Unfortunately, there are daily reminders that the bad guys are winning. These headlines, taken from a representative selection of international news stories, give a sense of what a lawless internet could mean. "Two teenage hackers crack Brinks smart safe in less than 30 minutes"; "Pirates hack into shipping company servers to identify booty"; "Islamic State brainwashes youth online"; "Electricity grid at risk, says spy boss".

Despite the increasing coverage of dark side stories, most Australians do not see cyber threats as first order security issues because of the reluctance of governments, and business, to openly discuss the challenge.

Governments worry about revealing sensitive intelligence methods. Companies fear a loss of reputation, or business to competitors in publicly revealing the loss of IP, personal data or money, from a successful hack.

Another reason, according to Alastair MacGibbon, Turnbull's new special adviser on cyber security, is that "we seem to think that cyber attacks have no offline or kinetic effects", unlike a highly visible and obviously destructive terrorist bomb, conventional war or natural disaster. Not being able to see the perpetrator, or vicariously share the anguish of victims, diminishes the emotional impact of a cyber attack.

Regrettably, cyber wars with real kinetic effects are already a reality since it is possible to destroy a power generator with only 21 lines of malicious code, as Russian hackers demonstrated in December, last year, with a devastating attack on Ukraine that left 230,000 Ukrainians in the dark and was the first confirmed hack to take down a power grid.

In championing the virtues of an open, free but secure internet network the national security strategy has struck the right balance between advancing and protecting our economic and security interests in the digital age. But the jury is still out on the ultimate measure of success -- the creation of a dynamic digital economy supported by a resilient cyber network.

Alan Dupont is adjunct professor of international security at the University of NSW and a non-resident fellow at the Lowy Institute.

Tech City News (UK)
Tech: A double-edged sword for national security
Tuesday, 26 April 2016
Byline: Emily Spavin

London - "I remember my first day at Mi6. I thought it was probably going to be nothing like the James Bond books and films. 'It'll just be a desk job', I told myself. I was wrong."
Matthew Dunn now lives in Gloucestershire and writes spy novels for a living - an interesting enough way to earn a crust, but his previous career is much more fascinating.

He served as a British intelligence officer and Mi6 field officer, taking part in around 70 missions that saw him travel the world, moving undercover from one hostile environment to another.

"I was tasked with targeting senior echelons, people who had access to secrets in rogue states that offered significant threats in terms of things like regional conflicts, nuclear conflicts and hostile threats against the West in the guise of intelligence attacks or military attacks," Dunn explained.

He used his training in all aspects of intelligence collection and direct action, including explosives, military unarmed combat, surveillance, advanced driving, infiltration techniques and covert communications, with one particular mission earning him a rare personal commendation from the Secretary of State for Foreign and Commonwealth Affairs.

Gadgetry

As for the role technology played in Dunn's Mi6 career, he explained James Bond-esque gadgetry did exist to some capacity, but not quite to the extent it plays in the Hollywood films.

"Mi6 does have a whole department totally devoted to creating weird and wacky gadgets and other technical equipment. It is actually called the Q department, but I still don't know whether Q in James Bond or Q in Mi6 came first."

Dunn said he was provided with technology such as recording briefcases, surveillance equipment and special weaponry, but explained it was something of a running joke due to its temperamental nature: "The gadgets all worked absolutely perfectly when tested in the head office, but it was often a different story when you tried to use them overseas."

"I'm sure things have come a long way since then, though," he conceded.

The internet has dramatically changed the way the Secret Intelligence Service operates and

the threats faced by the service have certainly developed and mutated, meaning nerds at laptops now often do work previously carried out by men with guns and sharp suits.

In the words of Q in the James Bond epic SkyFall: "I'll hazard I can do more damage on my laptop sitting in my pyjamas before my first cup of Earl Grey than you can do in a year in the field."

Internet

Technology is becoming ever more vital in the protection of national security, particularly within the sphere of counter terrorism. Tech enabled the government to prevent at least seven potentially deadly attacks in the UK last year, however, much more needs to be done to limit the freedom terrorists have in using these same tools to further their plights, promote propaganda and recruit new members.

This January, Baroness Shields, the Minister for Internet Safety, delivered a speech on challenging online extremism. She said the internet is becoming an "echo chamber of hate, fear mongering and intolerance", with terrorist groups like Isis/Daesh being quick to realise and exploit the power of the web. They are running modern and effective global brand marketing campaigns thanks to the borderless and boundary-free nature of social platforms.

"Unlike in the physical world where national governments can take clear and firm actions to keep people safe; there are no such obvious solutions available in the virtual world," she said.

In 2015, the UK's Counter Terrorism Internet Referral unit worked with industry players to remove over 55,000 pieces of terrorist and extremist content. Also last year, YouTube removed 14 million videos in just one instance and, since the middle of 2015, Twitter suspended over 125,000 accounts for threatening or promoting terrorist acts, primarily related to Daesh.

While this is all very positive, it's worth bearing in mind an average of 200,000 Daesh-supporting messages are posted every day on Twitter alone.

Communication

Social media aside, the way in which terrorists communicate has changed significantly, particularly over the past three years. In June 2014, NSA director US Navy Admiral Michael S Rogers said whistleblower Edward Snowden's revelation of government surveillance techniques had lead to some terrorist groups altering their methods of communication.

Among Snowden's revelations was information that the NSA was secretly tapping into Yahoo and Google data centers to collect data from hundreds of millions of account holders across the globe. He also revealed the UK's Government Communications Headquarters (GCHQ) had spied on users of Second Life, Xbox Live and World of Warcraft, and planned to infect millions of computers with malware using a program called Turbine.

While some lauded Snowden a hero, others labelled him a traitor and said revealing government collections partners tipped off terrorists and enabled them to drop those carriers and email addresses. Many have since switched to alternative platforms with encryption.

Last September, head of MI5 Andrew Parker explained that developments in encryption are making Mi5's job harder. Parker told the BBC that encrypted communication services are outpacing the laws required to govern access to data: "Shifts in technology, particularly internet technology, and the use of encryption and so on are creating a situation where law enforcement agencies and security agencies can no longer obtain, under proper legal warrant, the content of communications between people they have reason to believe are terrorists."

Privacy vs protection

Tech giants now, more than ever, have governments knocking on their doors, demanding access to records of users' communications. Thus these companies face, on a daily basis, the struggle of creating a suitable balance between privacy and protection.

In the first six months of 2010, Google received almost 15,000 government requests for user data. By 2014, that number had risen to just under 35,000. The tech giant provided information in over 65% of these cases, but is adamant it will not give in to all government demands.

"The solution, we believe, lies in a principled yet practical approach: one that restricts indiscriminate surveillance and supports valid law enforcement efforts while also protecting people's privacy and security," said Rachel Whetstone, former senior vice president of communications and public policy at Google.

In the UK specifically, parliament is scrutinising the Draft Investigatory Powers Bill - the largest overhaul for 15 years of laws surrounding surveillance. It wants to provide new powers to security services, enabling them to collect tens of thousands of personal records online without ministerial authorisation or oversight.

The Intelligence and Security Committee recently published a report labelling parts of the Bill "inconsistent and largely incomprehensible" and said it lacks clarity on fundamental issues, such as encryption and equipment interference.

Counter-extremism

Whatever the eventual reach of the Bill, is severe surveillance really the answer? Perhaps what is required to boost national security is a bigger drive to turn potential terrorist converts away from the darkened path they're being led down.

Jonathan Russell is head of policy at counter-extremism think tank Quilliam and his organisation focuses on spreading a counter narrative to that proffered by terrorists.

"Counter-extremism has existed for about a decade offline, but in the last three or four years, we have had to shift our focus online," he explained.

Russell said Quilliam's research into how extremists exploit people online has found they "create echo chambers for themselves". They use platforms like Facebook and Twitter, firstly because of the sheer volume of people using those services, but also because the algorithms in use mean they can focus their message without being interrupted by counter-arguments.

"YouTube is the clearest example of that," he said. Watch a Miley Cyrus video, then you'll be presented with related content - another Miley Cyrus video or something similar.

"Exactly the same is true for extremists, except that's worrying because you can just get pushed further and further down a rabbit hole and turn around after an hour or two and have only heard one point of view," explained Russell.

The extremists don't necessarily say anything on social media platforms that promotes violence, because they know that would be taken down, instead they stoke the victimhood narrative, driving opposition to the establishment and painting an overarching picture that the West is at war with Islam.

Most of the messages they produce are about utopia, not brutality, as brutality turns many people off, said Russell.

"They're essentially selling a dream," he added, "and it's up to us to come up with alternative messages and sell a different dream."

Russell stressed that, while Daesh may look like a "medieval death cult", they're using 21st century tools in their plight, so the response needs to be in line with this - they need to be dealt with as if they're a modern brand - a corporation.

"The tools we have available to us with which to respond are not national security tools, they're not related to surveillance, most of them are from the strategic communications and marketing worlds."

Russell said the social media giants have been very good at working with Quilliam and other groups to set up networks and give people in communities the skills to spread counter-extremism messages themselves.

What he'd really like to see, though, is the government doing more to support this kind of approach and for private companies to see this work as part of their corporate and social responsibilities.

"This is the answer, not surveillance. We need to win the war of words and work together to fight the great evil of our time," he concluded.

Vital role

Whatever the specifics, tech has undoubtedly played a vital role in national security over, at least, the past 70 years, and as technology develops, the more integral it becomes.

On a daily basis, it helps the government intercept threats and protect its citizens, but conversely, it enables terrorists to communicate, enemies to intercept confidential information and extremists to recruit.

The war on terror is nowhere near over and both threats and counterterrorism practices will continue to evolve. We now have to rely on the masses, the smartest and the most talented to join the right side of the battle.

NBC News
Ransomware Hackers Blackmail U.S. Police Departments
Tuesday, 26 April 2016
Byline: Chris Francescani

New York - Cyber criminals who have forced U.S. hospitals, schools and cities to pay hundreds of millions in blackmail or see their computer files destroyed are now targeting the unlikeliest group of victims -- local police departments.
Eastern European hackers are hitting law enforcement agencies nationwide with so-called "ransomware" viruses that seize control of a computer system's files and encrypt them. The hackers then hold the files hostage if the victims don't pay a ransom online with untraceable digital currency known as Bitcoins. They try to maximize panic with the elements of a real-life hostage crisis, including ransom notes and countdown clocks.

If a ransom is paid, the victim gets an emailed "decryption key" that unlocks the system. If the victim won't pay, the hackers threaten to delete the files, which they did last year to departments in Alabama and New Hampshire. That means evidence from open cases could be lost or altered, and violent criminals could go free.

Since 2013, hackers have hit departments in at least seven states. Last year, five police and sheriff's departments in Maine were locked out of their records management systems by hackers demanding ransoms.

Ransomware crimes on all U.S. targets are soaring. In just the first three months of 2016, attacks increased tenfold over the total entire previous year, costing victims more than $200 million. Authorities stress that this number only represents known attacks. One federal law enforcement official told NBC News that the "large majority" of attacks go unreported.

The viruses - most of which come from Russia and Eastern Europe -- are typically so impenetrable that even FBI agents have at times advised victims to just pay up and get their data back.

Police computers, however, are especially vulnerable to ransomware, because many small departments have ancient systems.

One chief acknowledged to NBC News that when his department's computers were attacked last year, they were running on DOS, an outdated disc-operating system that dates back to the early 1980s.

"Think about it," said Robert Siciliano, an online safety expert for Intel Security. "You have local law enforcement [which is] provided grants for all kinds of advanced technologies that often revolve around weaponry, but then when it comes to upgrading their desktops laptops -- they may not be up to speed."

Said Siciliano, "It's not unheard of to see a Windows XP or Vista still in action in a law enforcement environment."

'We Are Cops. We Generally Don't Pay Ransoms'

An attack commonly begins when a person opens a piece of malware disguised as a recognizable, sometime personalized e-mail attachment. Once opened, it freezes data block by block until everything is locked.

Then, a ticking countdown clock will often appear on a victim's screen, experts said, with a ransom demand and deadline. Hackers nearly always demand Bitcoins.

Some digital ransom notes include user-friendly instructions on how to buy Bitcoins online, and direct targets to websites that broker anonymous, peer- to-peer financial exchanges.

The attacks are increasingly forcing police chiefs into frustrated deliberations over whether or not -- against all their training and instincts -- to reward extortionists whose identity they may never know.

"My initial reaction was 'No way!" said Sheriff Todd Brackett of Lincoln County, Maine, whose system was frozen last spring. After "48 long hours," Brackett reluctantly paid.

"We are cops," he said with a sigh. "We generally don't pay ransoms."

Last year, the police chief in Durham, New Hampshire, refused to pay, and his files were deleted. He was able to recover most of them from a backup system.

When the Collinsville, Alabama, police department was hit in 2014, the chief refused to pay. He never saw the files again.

What makes the ransoms so maddeningly tempting for cops to pay is that most attacks that have disabled police department computers have sought just a few hundred dollars.

"It's much easier to ask for smaller amounts that you are actually going to get," said Alabama criminal justice professor Diana Dolliver.

Local law enforcement agencies' computer systems can contain plenty of vital -- sometimes even deeply personal -- information, ranging from rape and other violent crime reports to 911 call records, case files of ongoing investigations, personnel records and access to law enforcement databases like the National Crime Information Center (NCIC), which contains criminal case information on federal, state and local investigations.

While authorities say they are not aware of attacks on local law enforcement networks that have resulted in compromised evidence, they believe it is only a matter of time.

Business Is Booming

The attacks on U.S. police are an improbable part of what experts describe as a ransomware epidemic. One new study warns that 2016 "is the year ransomware will wreak havoc on America's critical infrastructure community ...'To Pay or Not to Pay,' will be the question fueling heated debate in boardrooms across the nation."

The business of high-tech extortion is growing exponentially. Last year, the FBI received nearly 2,500 ransomware attack complaints that cost victims $24 million. In the first three months of 2016, ransomware attacks cost Americans another $209 million.

Yet security experts and law enforcement officials agree that the actual figures are likely much, much higher.

"There are a lot of other law enforcement agencies out there that have been affected by this...that don't want their names out there," said Jeff McCliss, a Dickson County, Tennessee- -based detective whose department paid a $622 ransom in Bitcoins.

Many known intrusions have focused on health care facilities, school systems and even small cities -- targets with critical infrastructure, limited security and a constant need for access to their records.

In February, California's Hollywood Presbyterian Medical Center paid a ransom of about $17,000 in Bitcoins, one of at least six major health care systems victimized so far this year. Last month, the city of Plainfield, New Jersey, faced a demand for about $700 in Bitcoins to unfreeze their municipal servers.

Federal investigators say that a majority of the attacks are launched by Eastern European cyber gangs, but there have been few high-profile arrests to date because it's so hard to identify and locate the culprits.

And while early versions of ransomware had to be executed individually, by a human, experts said that today's viruses are fully automated. They are commonly disbursed like spam by the thousands, allowing hackers to execute hundreds of shakedowns simultaneously.

Vulnerabilities 'So Easy to Mitigate'

Ransomware viruses have put federal law enforcement officials in a nearly impossible position. In most cases they can't thwart the attack, apprehend the culprit or retrieve the locked data -- and they know from experience that most victims who pay get their files back.

Yet they're all- too-aware that each payout encourages more extortion.

For several years, multiple federal agencies have issued warning after warning to the public and private sectors urging proper "cyber-hygiene" and stressing the simplicity of the fix -- keep your software up to date and your system regularly backed up.

"This is so easy to mitigate," the federal official said.

While the FBI now explicitly advises against paying ransoms, individual agents have been known to nudge victims in that direction.

"To be honest, we often advise people to just pay the ransom," Joseph Bonavolonta, a Boston FBI cyber and counterintelligence specialist, told a security conference last fall. "The ransomware is that good."

Those comments drew headlines in the tech industry press, and prompted a clarifying statement from the FBI.

"The FBI doesn't make recommendations to companies," the agency told Naked Security last October. "[I]nstead the Bureau explains what the options are ... and how it's up to individual companies to decide for themselves the best way to proceed ... either revert to back up systems, contact a security professional, or pay."

Earlier this month, an FBI spokeswoman issued a statement to NBC News which said, in part, that "The FBI does not condone payment of ransom, as payment of extortion monies may encourage continued criminal activity, lead to other victimizations, or be used to facilitate serious crimes."

Bonavolonta could not immediately be reached for comment.

The Department of Homeland Security offers cyber-safety training to state and local governments and conducts "red team" tests on municipal systems to determine how secure they are. The FBI offers similar training in the private sector.

"It's really important for people to know [that] we can help," said Dr. Andy Ozmant, DHS assistant secretary for cybersecurity and communications. "We have a lot of resources available."

Compromised Evidence?

Experts said that ransomware attacks can have a potentially devastating impact on a municipality's criminal justice system.

"A good defense attorney is going to raise a question about whether or not evidence had been tampered with," said Dolliver. "That's the part I've actually been really watching for, but have not seen it come up in court cases."

Lincoln County law enforcement officials brought the same concerns to their local prosecutors, who concluded that none of the recovered data was ever actually breached.

So far at least, legal experts said, most ransomware cases have not necessarily tainted evidence.

"If the computer is simply held hostage but there is no evidence that any files have been altered, there will be no problem," said Steven Saltzburg, a George Washington University law professor who co-authored the 2013 Federal Criminal Procedures Litigation Manual. "If there is evidence that files have been altered, that is a problem."

'Last Laugh'

The ransomware attacks on U.S. police have left more than a few chiefs privately fuming, including Sheriff Brackett.

In a last-ditch bid to strike at least a tiny blow on behalf of U.S. law enforcement against ransomware extortionists, Brackett and his IT team paid the Bitcoin ransom, received the decryption key, cancelled the payment, and unlocked their system.

"We got the last laugh," Brackett thought to himself at the time.

Two days after his bait-and-switch scheme, hackers struck again.

This time the ransom was about $500.

This time Brackett paid and walked away.

The Register (UK)

Hackers so far ahead of defenders it's not even a game
Tuesday, 26 April 2016
Byline: John Leyden

London - Cybercriminals are way ahead of the game against defenders without having to try anything new, according to the latest edition of Verizon's benchmark survey of security breaches.
The study shows that miscreants have no need to switch up, because the same old tactics are still working fine. Security defenders are still performing poorly in their attempts to defend against hacking or malware-based attacks. This isn't for a lack of trying or skills on their part, but almost completely down to the fact that the game is rigged against them.

Verizon's ninth annual Data Breach Investigations Report (DBIR) provides an analysis of over 100,000 security incidents and 3,141 confirmed data breaches last year, drawing on real-world data breach caseloads handled by either Verizon or around 50 other contributing organisations.

Those involved include the US Secret Service, the European Cyber Crime Center (EC3), UK CERT and the Irish Reporting and Information Security Service (IRISS CERT), amongst others.

Hackers are getting faster whilst defenders are treading water. Over 99 per cent of attacks compromise systems within days (four out of five do it within minutes), and two-thirds of those siphon off data within days (a fifth do it in minutes). Whilst there was an improvement in the number of breaches detected in 'days or less' noted in the last DBIR, that turned out to be a temporary blip. This year, less than a quarter of breaches were detected within the same timeframe - meaning attackers have almost always gotten away with the goods before anyone notices.

Worse yet, it's usually not the victim that notices the breach, but a third party (normally either a security researcher or law enforcement).

Nearly two-thirds of all breaches are still traced back to weak or stolen passwords - a basic security failure.

"People are not sitting in front of consoles, looking for SQL Injections before running a manual attack," Dave Ostertag, global investigation manager at Verizon told El Reg. "They are stealing credentials, planting malware, pivoting and exfiltrating data."

Hackers have begun using multiple exfiltration points to avoid detection, Ostertag added.

Phishing lures

Phishing (which "is efficient and works really well," according to Ostertag) remains a huge problem and a major factor in most breaches. The DBIR found that nearly a third of phishing emails get opened, and more than one in ten recipients open the attachments, a significant rise from last year. The main

perpetrators of these attacks are organised crime syndicates, but nearly one in ten can be attributed to a state-affiliated actor. China accounts for more than half of all cyber- espionage attacks by volume last year, according to Ostertag, who nonetheless welcomed the recent US/China no hack pact as a positive development.

Public sector, manufacturing and professional services firms top the hit list of targets for cyber-espionage. Attackers are using phishing scams and pilfered passwords to open up a backdoor onto enterprise networks. This foothold is used to smuggle malware into targeted networks. Corporate networks would be far harder to attack - even with access credentials - in cases where enterprises had applied two-factor authentication. However, failure in this area was yet another security shortcoming identified during Verizon's study.

"Many victims have single- factor access into parts of their network even if they think otherwise," according to Ostertag.

On the cybercrime-for-profit front, ransomware is a problem across the board in manufacturing, the public sector and healthcare, Verizon reports. Cybercrooks, like cyber-spies, often rely on phishing.

"Hackers do their homework using social media like LinkedIn and other sources to know who to target, and what sort of content is likely to be opened," Ostertag explained.

"Cybercrooks are going after people who initiate or manage financial transactions."

Older threats such as phishing, malware and weak passwords predominate in breaches. By contrast, the much- discussed security risks from the Internet of Things and mobile phones barely register in Verizon's breach study.

Wall Street Journal
The Encryption Farce
Tuesday, 26 April 2016
Byline: Editorial Board

Editorial - If history repeats itself first as tragedy and then as farce, what does the FBI have in store next for its encryption war with Apple? After withdrawing its demands in San Bernardino and then reopening hostilities with a drug prosecution in Brooklyn, the G-men abruptly dumped the second case over the weekend too. Is anyone in charge at the Justice Department, or are junior prosecutors running the joint? The FBI claimed for weeks in a California court that it couldn't unlock the iPhone of terrorist Syed Farook unless Apple was compelled to create a new operating system, but then reported at the 11th hour that an unspecified outside party had engineered a solution that didn't require Apple's help. Justice lawyers also insisted the purpose of the litigation wasn't to create a legal precedent, but that such extraordinary commandeering was an exception for "one phone" related to terrorism.

This claim never stood up to scrutiny, given the nationwide profusion of such cases. But the Brooklyn flame-out is especially instructive about the FBI-Justice method without the crutch of invoking the fast-moving terror exigencies or uncovering potential domestic cells.

The iPhone in question was seized when the feds arrested a methamphetamine dealer called Jun Feng in 2014. Feng isn't dead, like Farook; he merely said he couldn't remember his password. Justice waited more than a year to try to force Apple to break the device, and shortly after these proceedings were initiated Feng and his codefendants copped guilty pleas.

Justice said the case wasn't moot because the device's data could yield evidence of other drug trafficking. FBI Director James Comey has suggested that the San Bernardino software exploit is no use on other iPhone models.

Yet while Justice argued in Brooklyn that Apple's help was essential, it also argued the FBI had no obligation to pursue a non-Apple work-around. The remarkable claim was that prosecutors need not exhaust all possible alternatives before conscripting a private company, such as consulting with other U.S. agencies, hiring an outside digital forensics outfit or even interrogating Feng again.

Such assertions were as false in Brooklyn as in San Bernardino. Two hours and a half before a deadline on Friday night, the government withdrew the case after "an individual provided the passcode to the iPhone," according to legal filings. This second immaculate conception in as many months further undermines the FBI's credibility about its technological capabilities. Judges ought to exercise far more scrutiny in future decryption cases even as Mr. Comey continues to pose as helpless.

The FBI Director recently said at Kenyon College that the end of the San Bernardino affair was "a very good thing," because "litigation is a terrible place to have any discussion about a complicated policy issue, especially one that touches on our values, on the things we care about most, on technology, on trade-offs, and balance." He added that "it will be bad thing if the conversation ended."

Yet forgive us if this "conversation" now seems more like a Jim Comey monologue. The debate might start to be productive if the FBI Director would stop trying to use the courts as an ad hoc policy tool and promised not to bring any more cases like the one in Brooklyn.

Meanwhile, the White House has taken the profile- in-courage stand of refusing to endorse or oppose any encryption bill that Congress may propose. If the Obama team won't start adjusting to the technological realities of strong and legal encryption, they could at least exercise some adult supervision at Main Justice.

New York Times
Obama Stresses Data in Terrorism Fight

Tuesday, 26 April 2016
Byline: Mark Scott

Berlin - The trans-Atlantic debate over digital privacy rights versus the surveillance needs of intelligence agencies was put under a spotlight on Monday, as President Obama called for continued access by law enforcement officials to thwart terrorism, while some European privacy advocates urged greater restraint.
"I want to say this to young people who value their privacy and spend a lot of time on their phones: The threat of terrorism is real," Mr. Obama said, speaking at a trade show in Hanover, Germany.

"I've worked to reform our surveillance programs to ensure that they're consistent with the rule of law and upholding our values, like privacy -- and, by the way, we include the privacy of people outside of the United States," he added.

Mr. Obama's message comes at a sensitive time, as cities like Brussels and Paris are still recovering from recent terrorist attacks. But his words are unlikely to slow down European efforts to expand people's control over their digital lives.

Europe is at the heart of a global debate over the way companies like Google and Facebook, as well as national intelligence agencies, handle people's digital data. Some regulators in the 28-member bloc have called on companies and governments, particularly that of the United States, to comply with the region's tough privacy regulations.

"Those who want to play in our backyard must play by our rules," Viviane Reding, a member of the European Parliament from Luxembourg and a former top European Union official, said on Monday at a privacy conference in Berlin. "Protection of our personal data shouldn't have a national barrier."

Ms. Reding is an author of a European Union privacy law that will go into force in 2018. It will be able to impose fines of up to 4 percent of a company's global revenue for the most serious breaches of European data protection rules. Those penalties would apply to any company -- even if it has no physical presence in Europe -- that has customers within the European Union.

At issue are communications via cellphones, as well as data generated in social media, online searches and e-commerce purchases.

The protections pursued in the European Union include the so-called right to be forgotten, detailed by the bloc's highest court, which requires search giants like Google to remove links to online information in some cases.

And Europe's national privacy regulators have vowed to take a tough line against a new pact between the United States and the European Union that is intended to ensure the relatively unimpeded flow of

personal data across the Atlantic. The national regulators are wary of the ability of American law enforcement and intelligence agencies to monitor data to fight crime or terrorism.

But American agencies, including the Commerce Department and the Federal Trade Commission, argue that they actively monitor companies' access to individuals' digital data. They say that American privacy safeguards -- including the United States Constitution -- often provide better protection than the rules in other jurisdictions, including those in Europe.

"We care about Europeans' privacy," Mr. Obama said in Hanover, "not just Americans' privacy."

Many European officials acknowledge that the region's privacy laws share many similarities with those in the United States. But they also highlight important differences, including the lack of overarching federal privacy legislation. The differences, they say, must be bridged if Europe and the United States are to effectively supervise the way companies like Facebook and Google gain access to data worldwide.

"The digital world is globalized," Giovanni Buttarelli, the European Union's data protection supervisor, said at the Berlin conference on Monday. "So data protection should also be globalized."

The Intercept
Spy Chief Complains That Edward Snowden Sped Up Spread of Encryption by 7 Years
Monday, 25 April 2016
Byline: Jenna McLaughlin

Washington - The Director of National Intelligence on Monday blamed NSA whistleblower Edward Snowden for advancing the development of user- friendly, widely available strong encryption.
"As a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years," James Clapper said during a breakfast for journalists hosted by the Christian Science Monitor.

The shortened timeline has had "a profound effect on our ability to collect, particularly against terrorists," he said.

When pressed by The Intercept to explain his figure, Clapper said it came from the National Security Agency. "The projected growth maturation and installation of commercially available encryption -- what they had forecasted for seven years ahead, three years ago, was accelerated to now, because of the revelation of the leaks."

Asked if that was a good thing, leading to better protection for American consumers from the arms race of hackers constantly trying to penetrate software worldwide, Clapper answered no.

"From our standpoint, it's not ... it's not a good thing," he said.

Technologists have been tirelessly working to strengthen encryption for decades, not just the past few years. But Snowden's revelations about the pervasiveness of mass surveillance clearly accelerated its more widespread availability.

And technologists say the threat of law enforcement "going dark" has been overhyped. For instance, there are almost always ways to hack around encryption, even if you can't break it.

Clapper acknowledged that there is no such thing as unbreakable encryption from his perspective. "In the history of mankind, since we've been doing signals intelligence, there's really no such thing, given proper time, and proper application of technology."

Christian Science Monitor
Encryption hindering efforts to stop Islamic State, intelligence director says
Monday, 25 April 2016
Byline: Anna Mulrine

Washington - The Edward Snowden leaks have accelerated the sophistication of encryption technologies by "about seven years," Director of National Intelligence James Clapper told reporters this morning. And that is not a development to be celebrated, he added in remarks at a breakfast hosted by The Christian Science Monitor.

"From our standpoint, it's not a good thing."

New, commercially available encryption software "had and is having major, profound effects on our ability" to collect intelligence, "particularly against terrorists," he warned.

That's in large part because the Islamic State is "the most sophisticated user by far of the Internet." They privately purchase software that "to ensure end-to-end encryption" of their communications.

"And so that is a major inhibitor to discerning plotting, principally by ISIL and others," Mr. Clapper said, using one acronym for the Islamic State.

The seven year estimation comes from the National Security Agency, he said.

It raises the issue of the tension between the need for security against cyber attacks - which as recently as February Clapper cited as a greater threat than terrorism - and the opposition to law enforcement against so-called unbreakable encryption software that, they say, could hinder their search for terrorists.

Clapper for his part echoed President Obama's warning against "absolutist positions" on the topic. "Somehow, we need to find a balance here," he said. "I don't know the technicalities of how we might

arrive here, how we thread the needle" between how to "ensure privacy and security on an individual basis, as well as security in the context of what's best for the collective good."

At the moment, he added, that goal "is an elusive holy grail that we're pursuing."

That said, he warned that the development of unbreakable encryption, which he likened to the possibility that that it could, in essence, "give the terrorists a pass."

Clapper warned Monday that the group has clandestine cells that are plotting more terrorist attacks in Germany, Italy, and England.

To this end, the United States is stepping up efforts to promote more intelligence sharing. In the meantime, since the recent IS attacks on Paris and Brussels, US intelligence officials have learned some things about the terrorist group, he said.

For starters, they are "very op-sec conscious," Clapper said. A former Air Force lieutenant general, he was using military parlance for "operational security."

It is clear that IS is also taking advantage of the migrant crisis in Europe, he added.

And that poses a formidable challenge for Europe. There is a "fundamental conflict" between European Union incentives and drives to promote openness and free movement of people and goods with privacy, "which is in some ways in conflict with the responsibilities that each country has as a nation-state to protect the borders and securities of their nations and peoples," Clapper said.

Times of Israel
The programming school that keeps the IDF running
Tuesday, 26 April 2016
Byline: David Shamah

Jerusalem - You can't shake a stick in Israel's technology scene without hitting a graduate of the IDF's famous Unit 8200, which has produced CEOs and CTOs of some of the world's most successful tech and cyber-security firms. All of those soldiers passed through the IDF Computing and Cyber Defense Academy, which runs dozens of courses for the many tech needs of the modern Israeli army.
"The Israeli army faces challenges large and small, from the sakin to the gar'in" -- threats ranging from stabbing attacks to nuclear weapons, according to Major Dor Cohen, head of the programming section of the Academy.

There is today one common denominator that powers all of the army's defensive efforts, he said. "It's fair to say that technology is the basic building block of any defense effort these days, large or small," said Cohen.

"Programming, cyber-defense tactics, app development, and other technology are the backbone of all parts of the IDF today, from systems like Iron Dome and David's Sling that defend against missile attacks to programs that can quickly issue deployment orders and ensure that soldiers and reservists get where they need to be quickly to ensuring that supplies, parts, personnel, and everything else arrives where it is supposed to. I'm proud to say that the academy is ground zero for the training of the personnel needed to master the technology to do this."

Part of the C4i Computer Services Directorate, the academy hosts dozens of courses at its campus, including, for example, Shahar, the tech-oriented "little brother" of the much more well-known Nahal Hareidi program, which deploys ultra-Orthodox soldiers in the field, on patrols and in combat duty.

The Programming division teaches students basic and advanced knowledge in computer languages, app development, cyber-security, firewalls, hacking projects - anything needed to navigate the world of programming and networks, with the objective to quickly, neatly, and effectively deploy systems that help protect Israel.

Speed of response is one of the important skills taught, said Cohen. "We learned this all too well in 2014's Operation Protective Edge, when things changed minute to minute. In most organizations you have levels of administration and approval that require supervisors to sign off on projects, and the process could take weeks. Cyber-threats and other matters came up throughout the war, and we needed to respond within hours."

In addition, apps are becoming increasingly important in the IDF, said Cohen. "Everyone today carries around in their pocket a super-sophisticated computer that can be used to provide directions, information, warnings, and other vital information. There is no reason not to use these devices and their capabilities in defending Israelis. Of course, the apps and the system have to be secure."

In February, the Academy sponsored a hackathon in which hundreds of soldiers developed apps and technologies that could respond to the issues faced by soldiers in the field. "Our courses teach programmers to develop apps using secure technologies the IDF has developed," said Cohen. "There is a great demand throughout the various forces for these apps, and we get many requests for solutions using these devices."

One of the greatest challenges Cohen faces is finding the personnel to fill the growing number of programming jobs throughout the IDF. "As everyone knows, there are not enough kids studying math and science in high schools, and we are part of the effort to encourage more students to take on those subjects," said Cohen. "But we don't strictly rely on the educational system to produce the candidates

we need. We review the records of IDF recruits and check their aptitudes, and if we find a likely candidate we lobby them to join our program."

According to Cohen, his program can take recruits who know almost nothing about computers or programming and turn them into programmers with very good to excellent skills.

Of course, a lot of hard work goes into creating programmers "from scratch" - both on the part of the candidates themselves and on the part of Cohen's staff. Fortunately, they are up to the task, he said.

"Many of the teachers in the program are themselves graduates, very highly motivated - enough to remain in the army and to help develop the new generation of programmers instead of going into private enterprise."

And although many highly motivated young Israelis prefer service in combat units, there's plenty of action - and prestige - in the army's programming and cyber units, said Cohen. "Our soldiers don't fight in the field in the same way Golani and Givati unit soldiers fight, but they are engaged in extremely important defense projects.Tech is now the basis of warfare. Without our people, the army cannot move an inch."

Fox News
Did anti-Israel bias keep France from getting terror tech before Paris attacks?
Tuesday, 26 April 2016
Byline: Hollie McKay

Washington - Shortly after the Charlie Hebdo attack in Paris, and nearly a year before terrorists killed 130 in coordinated strikes that rocked the City of Light, French security officials rejected an Israeli company's offer of terrorist-tracking software that could have helped them flag the deadly terror cell, a security expert said.
The offer of data- mining technology that would allow French authorities to "connect all the dots" in the Islamist extremist community was made to the Directorate- General for Internal Security, France's main intelligence agency. It is used to analyze and match up fragmented intelligence reports from several national and international databases, giving counter-terrorism agents the most up-to-date information on potential terrorists available.

The overture was rejected.

"French authorities liked it, but the official came back and said there was a higher-level instruction not to buy Israeli technology," a well-placed Israeli counter-terror specialist familiar with the technology and the company behind it told FoxNews.com. "The discussion just stopped."

The Israeli source declined to name the company or detail the technology, which has been shared with the U.S. and other nations on good terms with Israel, other than to say it scans databases from multiple agencies and Interpol and pinpoints "high-risk" people. But he believes it could have given French authorities a chance at stopping the Nov. 13, 2015, attacks in Paris, and possibly the coordinated bombings in Brussels that killed 32 on March 22.

"Government agencies struggling to foil terror attacks need access to technologies that allow them to connect their data fragments, making it possible to handle daily data challenges," the source said. "With this system, all data can then be easily navigated, processed and represented by employing a set of powerful analytic tools and unique algorithms."

The offer followed Israeli Prime Minister Benjamin Netanyahu's pledge to work closely with Europe on enhancing security in the wake of the Brussels attacks, taken in Israel as a call for intelligence and technology sharing.

"In Paris or Brussels or San Bernardino or Tel Aviv or Jerusalem, terror must be condemned equally and it must be fought equally," Netanyahu said. "Israel stands ready to cooperate with all the nations in this great struggle."

No official reason was given for France's rejection of the offer, and the source acknowledged it could have been triggered by legitimate concerns about hacking vulnerability. Yet many suspect politics was to blame.

"The European Union has blamed Israel for everything that is happening in the Middle East and stopped cooperation in regards to military, law enforcement and intelligence training and banning university cooperation which [generates] much of the technology to fight terrorism," said Itamar Gelbman, a former IDF Special Forces and who is now a counter-terrorism consultant.

DGSI did not respond to requests for comment and a European Union official told FoxNews.com that there is no formal French, or wider EU ban, on purchasing technology products made in Israel. However, tensions between the European Union and Israel have heightened in recent years, primarily over claims the Jewish State illegally occupies Palestinian territories.

The Israeli-Palestinian conflict has long divided the international community. Human rights groups routinely condemn Israel for repressing and harshly retaliating against Palestinian aggression, while Israel remains staunch that it acts in self-defense and to protect its people.

Kamal Nawash, an American attorney and president of the Free Muslims Coalition, noted that Europe's tough stance against Israel and hesitation in making technology purchases is an "example of the global community sending a message to Israel that its treatment of the Palestinians is unacceptable."

"Israel would be wise to change its treatment of Palestinians by providing them with civil and human rights and pursuing a desegregation policy in general," Nawash said. "Otherwise, Israel may experience the same fate as South Africa during the apartheid era with all the countries of the world boycotting Israel."

The recent spate of terror attacks on European soil could bring about a resurgence in investment with Israeli tech and intelligence companies, given its undisputed status as a global leader in the field.

"Israel has been facing terror threats since its inception in 1948," said Gilles Perez, manager of HLS & Aerospace Unit at the Israel Export Institute. "In the 1970s, it was Israel's national airline that pioneered the concept of an undercover security officer on every commercial flight long before it was adopted by other countries after September 11, almost 40 years later."

Security at airports, such as Zaventem Airport in Brussels, where last month's bombing occurred, has long been an area of Israeli expertise. But intelligence, such as the system offered to French officials, could be even more crucial, said Col. Eran Lerman, former deputy chief of Israel's National Security Council and senior IDF Military Intelligence division director.

"However, the key to successful security has to be intelligence, in the broader sense of the word," Lerman told Homeland Security Today. "For too many years, for very good reasons, Europeans have neglected the need for effective intelligence measures."

Israel-based security training expert Daniel Sharon said that since the Brussels attacks last month there has been particular interest in airport and aviation security prevention concepts, interest that transcends popular protest.

"The goods are boycotted in European supermarkets," Sharon said. "But when they are in trouble they run to Israel for help."

Less than a week after the attacks in Brussels, Belgian law enforcement bought advanced surveillance and rapid view technology from Israeli company BriefCam. The technology is already in use at the Statue of Liberty and various U.S. airports, said President and CEO Dror Irani.

Israel's tech and security sector has long been an incubator for anti-terror solutions, say experts. The more France and Europe in general are threatened, the more willing they may be to work with companies based in the Jewish state.

"Israel is leading the field in counter-terrorism technology, but it's not a popular country," said Ari Zoldan, CEO of technology and e-commerce firm Quantum Network. "It is unlikely that Israel will suddenly become popular, but the need for better national security will force people to work with Israeli solutions."

Reuters

Bangladesh Bank hackers compromised SWIFT software, warning to be issued

Tuesday, 26 April 2016

Dhaka - The attackers who stole $81 million from the Bangladesh central bank probably hacked into software from the SWIFT financial platform that is at the heart of the global financial system, said security researchers at British defense contractor BAE Systems.
SWIFT, a cooperative owned by 3,000 financial institutions, confirmed to Reuters that it was aware of malware targeting its client software. Its spokeswoman Natasha Deteran said SWIFT would release on Monday a software update to thwart the malware, along with a special warning for financial institutions to scrutinize their security procedures.

The new developments now coming to light in the unprecedented cyber-heist suggest that an essential lynchpin of the global financial system could be more vulnerable than previously understood to hacking attacks, due to the vulnerabilities that enabled attackers to modify SWIFT's client software.

Deteran told Reuters on Sunday that it was issuing the software update "to assist customers in enhancing their security and to spot inconsistencies in their local database records."

The software update and warning from Brussels-based SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, come after researchers at BAE, which has a large cyber-security business, told Reuters they believe they discovered malware that the Bangladesh Bank attackers used to manipulate SWIFT client software known as Alliance Access.

BAE said it plans to go public on Monday with a blog post about its findings concerning the malware, which the thieves used to cover their tracks and delay discovery of the heist.

The cyber criminals tried to make fraudulent transfers totaling $951 million from the Bangladesh central bank's account at the Federal Reserve Bank of New York in February.

Most of the payments were blocked, but $81 million was routed to accounts in the Philippines and diverted to casinos there. Most of those funds remain missing.

Investigators probing the heist had previously said the still-unidentified hackers had broken into Bangladesh Bank computers and taken control of credentials that were used to log into the SWIFT system. But the BAE research shows that the SWIFT software on the bank computers was probably compromised in order to erase records of illicit transfers.

Deteran reiterated on Sunday that "the malware has no impact on SWIFT's network or core messaging services."

The SWIFT messaging platform is used by 11,000 banks and other institutions around the world, though only some use the Alliance Access software, Deteran said.

SWIFT may release additional updates as it learns more about the attack in Bangladesh and other potential threats, Deteran said. SWIFT is also reiterating a warning to banks that they should review internal security.

"Whilst we keep all our interface products under continual review and recommend that other vendors do the same, the key defense against such attack scenarios is that users implement appropriate security measures in their local environments to safeguard their systems," Deteran said.

Adrian Nish, BAE's head of threat intelligence, said he had never seen such an elaborate scheme from criminal hackers.

"I can't think of a case where we have seen a criminal go to the level of effort to customize it for the environment they were operating in," he said. "I guess it was the realization that the potential payoff made that effort worthwhile."

A Bangladesh Bank spokesman declined comment on BAE's findings. A senior official with the Bangladesh Police's Criminal Investigation Department said that investigators had not found the specific malware described by BAE, but that forensics experts had not finished their probe.

Bangladesh police investigators said last week that the bank's computer security measures were seriously deficient, lacking even basic precautions like firewalls and relying on used, $10 switches in its local networks.

Still, police investigators told Reuters in an interview that both the bank and SWIFT should take the blame for the problems.

"It was their responsibility to point it out but we haven't found any evidence that they advised before the heist," said Mohammad Shah Alam, head of the Forensic Training Institute of the Bangladesh police's criminal investigation department, referring to SWIFT.

The BAE alert to be published on Monday includes some technical indicators that the firm said it hopes banks could use to thwart similar attacks. Those indicators include the IP address of a server in Egypt the attackers used to monitor use of the SWIFT system by Bangladesh Bank staff.

The malware, named evtdiag.exe, was designed to hide the hacker's tracks by changing information on a SWIFT database at Bangladesh Bank that tracks information about transfer requests, according to BAE.

BAE said that evtdiag.exe was likely part of a broader attack toolkit that was installed after the attackers obtained administrator credentials. It is still not clear exactly how the hackers ordered the money transfers.

Nish said that BAE found evtdiag.exe on a malware repository and had not directly analyzed the infected servers. Such repositories collect millions of new samples a day from researchers, businesses, government agencies and members of the public who upload files to see if they are recognized as malicious and help thwart future attacks.

Nish said he was highly confident the malware was used in the attack because it was compiled close to the date of the heist, contained detailed information about the bank's operations and was uploaded from Bangladesh.

While that malware was specifically written to attack Bangladesh Bank, "the general tools, techniques and procedures used in the attack may allow the gang to strike again," according to a draft of the warning that BAE shared with Reuters.

The malware was designed to make a slight change to code of the Access Alliance software installed at Bangladesh Bank, giving attackers the ability to modify a database that logged the bank's activity over the SWIFT network, Nish said.

Once it had established a foothold, the malware could delete records of outgoing transfer requests altogether from the database and also intercept incoming messages confirming transfers ordered by the hackers, Nish said.

It was able to then manipulate account balances on logs to prevent the heist from being discovered until after the funds had been laundered.

It also manipulated a printer that produced hard copies of transfer requests so that the bank would not identify the attack through those printouts, he said.

Motherboard Blog

Canada Is Considering Spying on Kids to Stop Cyberbullying

Wednesday, 27 April 2016

Byline: Jordan Pearson

Section: general

Toronto - Cyberbullying is simply awful, and its consequences can be utterly horrific. Canadians have known this all too well since 17-year-old Rehtaeh Parsons' suicide in 2013, after photos of her alleged rape circulated online.
It's only human to want to put a stop to it. But is it worth spying on kids?

To wit, the Canadian government is looking for a person or organization to "conduct an evaluation of an innovative cyberbullying prevention or intervention initiative" in a "sample of school- aged children and youth," according to a tender notice published by Public Safety Canada last week.

Although nothing has been finalized, the government will consider letting the organization spy on kids' digital communications to do it, Barry McKenna, the Public Safety procurement consultant in charge of the tender, told me.

"The tender doesn't preclude or necessarily require digital monitoring," said McKenna. "But there are certainly products on the market that do that, and I would guess that that kind of intervention would be one of interest."

The school board overseeing the school used in the study would have to sign off on digital surveillance of kids, McKenna said, and so would Public Safety. McKenna would not disclose whether any person or organization has responded to the tender yet. The government has budgeted $60,000 for the program, the notice states.

"Cyberbullying isn't a technological problem"

"Any use by government of technology to scan the internet and read somebody's communications obviously raises privacy issues," said David Fraser, a Canadian privacy lawyer consulting on a new cyberbullying law for Nova Scotia. "Fewer privacy issues if it's following an intervention and it's targeted," he continued, "way more if they're trying to single out kids in Canada and assess what they're saying."

"What we've seen come out of Public Safety and most law enforcement agencies is a pretty un-nuanced, heavy- handed, over the top model," Fraser added. Nova Scotia's previous cyberbullying law, passed in the wake of Parsons' suicide, was ruled unconstitutional and struck down for being too broad and infringing on people's civil rights.

If the Public Safety study ends up taking a more blanket approach to monitoring kids instead of targeting surveillance after an incident, it could also risk undermining communication between kids and their teachers or parents, according to US Cyberbullying Research Center co- director Sameer Hinduja.

"Installing tracking apps undermines any sort of open-minded communication [that] youth-serving adults might have with these kids, because you're tracking them surreptitiously," said Hinduja. "Kids, as they get older, want more privacy and freedom. It's natural--you want it, and I want it."

This isn't the first time somebody has considered surveillance as a solution to the complex social issue of kids being absolutely horrific to each other, and it likely won't be the last. In 2013, The LA Times noted that the Glendale Unified School District in Southern California reportedly paid a firm $40,000 to monitor kids' social media accounts to combat bullying. The move raised the ire of privacy advocates in the US then, too.

The point, according to Hinduja, is that bullying isn't a uniquely digital problem. You don't solve bullying forever by putting a teacher in every hallway, and you don't fix crime by putting a cop on every corner.

"Cyberbullying isn't a technological problem," said Hinduja. "You can't blame the apps, the smartphones, or the internet. Instead, cyberbullying is rooted in other issues that everyone has been dealing with since the beginning of time: adolescent development, kids learning to manage their problems, and dealing with stress."

Motherboad Blog

Needs to Revive the Encryption Debate It Had in the 1990s

Wednesday, 27 April 2016

Byline: Matthew Braga

Section: Comment

Comment: In the wake of a court battle between Apple and the FBI, American lawmakers have been considering a new policy on encryption, on the basis that strong technological protections are making it difficult for law enforcement and intelligence agencies to solve crime.
Such a policy, which would mandate a so-called backdoor in encryption software, would inevitably compromise the security of all communications, privacy advocates have argued. And yet, given the gravity of the situation, in Canada there has been no similar debate. At least, not recently.

Though largely forgotten today, the Canadian federal government actually did have an encryption debate of its own in the late 1990s. It brought law enforcement together with experts to discuss encryption's role in a then-early internet, and the potential impacts on national security and public safety that might arise from encryption's use.

What's most fascinating is how closely the arguments from two decades prior mirror those that are being made today. Though technology has come a long way since then, looking back at Canada's own debate shows that some of the arguments being made today by politicians and law enforcement in the US are still stuck in the past.

"We all came to the conclusion that [legislation] would be the death-knell for [...] secure communications online," said Ann Cavoukian, who served as the Information and Privacy Commissioner of Ontario from 1997 to 2014. "We thought it had died, and here it is again."

18 law enforcement agencies, including the RCMP and CSIS, even called for "mandatory access" to encryption keys

US lawmakers and experts previously engaged in a pair of fierce cryptographic fights that came to a head in 1994: the first, over the passing of the Communications Assistance for Law Enforcement Act, or CALEA, an American wiretapping law that dictates when and how telecommunications companies have to assist law enforcement and intelligence agencies engage in electronic surveillance; and the second, over a US-government backed encryption scheme called Clipper, a special computer chip that, when installed in a phone, would give the National Security Agency backdoor access to otherwise encrypted communications.

Ultimately, CALEA passed--with compromises--and the Clipper chip was scrapped. It was in this context, the aftermath of the Crypto Wars to the south, that the Canadian government decided to have its own debate.

In January 1999, a Senate Special Committee on Terrorism and Public Safety released a report on threats to public safety and national security, and listed encryption as an emerging issue. Based on interviews with law enforcement, academics, telecommunications companies and members of the financial community, the committee reiterated many of the same arguments that can still be heard today: that encryption is making law enforcement's job harder; that backdoors built into encryption mechanisms for

government use could just as easily be used by criminals; and that undermining encryption would compromise the security of financial systems too.

18 law enforcement agencies, including the RCMP and CSIS, even called for "mandatory access" to encryption keys used to protect stored data and data in transit. In what has become an oft-used turn-of-phrase, police argued that "they do not seek increased investigative capabilities through mandatory key access or otherwise, but instead seek only to restore and maintain their existing investigative capabilities."

In the end, no cryptography policy was proposed, and the committee recommended law enforcement and intelligence agencies seek other methods to overcome the obstacle of encryption. However, the committee did recommend amending the Criminal Code "to provide lawful access to encryption keys by law enforcement and security intelligence organizations and to criminalize encryption when used in the commission of a crime."

These recommendations were never adopted. It's not clear why, but it's likely that the government chose to follow the lead of countries such as the US, which had backed down from similar schemes.

As the RCMP previously told Motherboard, there is no power in the Criminal Code specific to encryption. According to Scott Bardsley, press secretary for Public Safety Minister Ralph Goodale's office, police can either compel a third party to decrypt data with judicial authorization, or they may attempt to decrypt the data themselves.

When asked if the Canadian government was planning on revisiting the encryption debate, Barsdley would only tell Motherboard that "broad public consultations on national security issues" are planned in the "medium term." But Cavoukian would be happy if there was no debate at all.

"I would prefer no discussion, because if there's no discussion, you're not resurrecting the discussion of the 90s," she said. "To me, we put the issue to bed."

Globe and Mail

Ransomware poses complex legal and reputational risks

Wednesday, 27 April 2016

Byline: Brent Arnold & Christopher Oates

Section: Comment

Comment: As businesses and public institutions increasingly become the targets of ransomware - malware that blocks access to computer systems or the information they contain until the user performs actions demanded by hackers - legal risks surrounding such headlinemaking attacks have come to the fore in Canadian corporate consciousness.
A January report by the Online Trust Alliance reveals that ransomware attacks aimed at companies are not only growing more prevalent, but they are also becoming more sophisticated. Today's hackers can custom tailor their demands according to the size and market value of their corporate mark. Making matters worse, last month Apple's iOS operating system was infected with ransomware for the first time.

Ransomware typically gains access to a computer system when a user clicks on unfamiliar links or strange attachments (although a growing number of programs are infecting computers via the download of ostensibly legitimate applications).

In its most benign form, an infection could force employees to complete a survey; at its most malignant, it has strongarmed companies into paying actual ransoms (typically in the nationless and virtually untraceable currency of bitcoin).

Businesses that fail to comply face the destruction of client and proprietary data, and intellectual property - not to mention sustaining significant reputational damage and exposure to third-party lawsuits from clients and consumers (and there is never any guarantee that meeting hackers' demands will result in computers or data being unlocked).

Despite this growing threat, legal recourses for ransomware victims are slim. The activity is, of course, illegal and should be immediately reported to police (the RCMP also suggest reporting to the Canadian Anti-Fraud Centre). But despite the fact that such attacks have been reported for more than a decade, there are no documented cases of ransomware perpetrators ever having been prosecuted in Canada.

Given the often remote nature of the crime (the few attacks that have been successfully traced typically come from foreign countries), criminal and civil remedies may be unlikely to succeed.

In the rare event a cybercriminal is identified, civil proceedings against foreign nationals are most likely to result in default judgments that are difficult if not impossible to collect on.

While cybercriminals frequently avoid prosecution, their corporate victims may find themselves in the legal spotlight. Recent amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) will soon require companies subject to PIPEDA to alert the federal privacy commissioner, affected individuals and relevant organizations or government institutions following a breach of security safeguards that "creates a real risk of significant harm to the individual."

This can include risk of economic loss by the person whose personal information is subject to the breach, as well as potential reputational harms.

While reporting obligations provide an important consumer protection and will be a legal necessity in certain cases (companies that fail to report where required by PIPEDA may be subject to fines of up to $100,000), they are nonetheless problematic for businesses - particularly those for whom data security is a critical component of their brand identity. Recent hacks have shaken consumer and shareholder confidence and resulted in both significant disruption for targeted businesses and resignations by top executives.

All indicators suggest ransomware will only become more vicious and prevalent in the foreseeable future. With added reporting pressure looming on the horizon, companies that fall prey may soon find themselves facing complex legal and reputational risks.

Brent Arnold and Christopher Oates are lawyers at Gowling WLG, whose practices focus heavily on technology- and privacy-related matters.

Washington Post

FBI says it can't explain how iPhone was hacked

Wednesday, 27 April 2016

Byline: Ellen Nakashima

Section: general

Washington - The FBI intends to tell the White House this week that its understanding of how a third party hacked the iPhone of a shooter in San Bernardino, Calif., is so limited that there's no point in undertaking a government review of whether the tool should be shared with Apple, officials said. The decision, said officials familiar with the discussion who spoke on the condition of anonymity, ends several weeks of internal debate by bureau lawyers and technical experts about the FBI's obligation to disclose the method.

Last month, the FBI paid more than $1 million for a tool to crack an iPhone used by one of the shooters in California. But the contract did not include rights to the software flaws that went into the tool, officials said.

As a result, the bureau has a limited technical understanding of how the method worked, officials said.

On Tuesday, FBI Director James B. Comey acknowledged the internal debate.

"The threshold is: Are we aware of the vulnerability, or did we just buy a tool and don't have sufficient knowledge of the vulnerability that would implicate the process?" he said at a cyber conference at Georgetown University.

Comey was referring to a process, led by the White House, in which agencies such as the FBI, National Security Agency (NSA) and Homeland Security Department debate whether to disclose a computer software flaw discovered by the government to the software maker so the company can fix it.

Most flaws are disclosed, the White House has said. But some are kept secret so that the law enforcement or intelligence agency can use them in intelligence- gathering or criminal investigations.

The FBI's decision to not submit to a review of the method used in the San Bernardino case was first reported by the Wall Street Journal.

Some security experts said the bureau or the NSA could reverse-engineer the tool to gain information about the flaws. But the bureau was not likely to do so, several officials said.

"If what we have bought is a tool, and we've said that we won't reverse-engineer the tool such that you can figure out what vulnerability is used to make the tool work, then even if we wanted to disclose something, there's nothing we can disclose," one senior administration official said.

The FBI recovered the iPhone of Syed Rizwan Farook, one of the shooters in the December terrorist attack in San Bernardino, but could not access the data on it because it did not know Farook's passcode. In February, the Justice Department obtained a court order to force Apple to write software that would disable several phone security features so the FBI could try to crack the code.

Apple challenged the order, arguing that the court had no basis to issue it and that it would set a dangerous precedent. In late March, the FBI disclosed that a third party had come forward with a tool to help it gain access to the phone and so it no longer needed the court order to force Apple's assistance.

Security and privacy advocates then began to push the bureau to disclose to Apple the flaws on which the tool was based so the tech giant could repair them.

Last month, professional hackers or vulnerabilities researchers brought flaws they had found to a company whose name the FBI has not disclosed.

Apple has said it will not press for the vulnerabilities to be disclosed.

"We're confident that the vulnerability the government alleges to have found will have a short shelf life," a lawyer for Apple told reporters earlier this month. "In our normal process . . . we'll continue to improve the phones and at some point this fix will get implemented."

Times of Israel

Operational Cyber Intelligence

Wednesday, 27 April 2016

Section: general

Jerusalem - Visitors to the CyberTech 2016 exhibition had the impression that every single exhibitor boasted a cyber intelligence capability. Indeed, cyber intelligence (or threat intelligence) has evolved into one of the hottest trends of the cyber technology industry in the last few years. Even the relatively small Israeli market generates massive demand for intelligence services and some ten product and service companies are involved in this activity, competing one another.
The regulator has not remained idle either. According to Directive #361 of the Banking Supervisor at the Bank of Israel, financial institutions must use intelligence in addition to the other security mechanisms they employ. So, apparently everyone is talking about cyber intelligence and many people would like to know how to consume it, but what, in fact, is cyber intelligence and how does it help users to defend themselves against threats?

Cyber intelligence produces operational insights by looking outside the organization and issuing alerts of imminent and future threats to the organization. The type of intelligence may be categorized according to the manner in which the information is collected and analyzed and the manner in which the final product is used. Roughly, the world of cyber intelligence is divided into three categories: technical intelligence, tactical intelligence and operational intelligence.

Technical Intelligence Technical intelligence constitutes the overwhelming majority of intelligence sold around the world. This intelligence category is based on a method adopted from military intelligence, known as Signals Intelligence (SigInt), which consists of the interception of electronic signals and deriving information from those signals. In the Internet world, this refers to the characteristics of web traffic (IP address, server locations and so forth), as well as to malware indicators. Combining these data makes it possible to identify suspicious traffic to and from the organization, and to block it.

Organizations and suppliers that collect intelligence of this category deploy networks of sensors to identify suspicious traffic and IP addresses suspected of disseminating malware and junk mail. This information is delivered in a digital format directly to the security systems (Firewalls, Anti-Virus

software) and enables them to block undesirable elements. The primary disadvantage of this intelligence category is the fact that it is essentially responsive, namely - it identifies and handles attacks that have already taken place somewhere in the digital space. It cannot effectively identify new attacks that have not been documented, analyzed and translated into 'signatures'.

The various approaches that attempt to solve this problem through mathematical/statistical analysis of behavior patterns are plagued by a high percentage of false positive 'noise' messages. Additionally, these technical intelligence models do not normally produce insights regarding potential attacks, and no conclusions may be derived from them for the purpose of making tactical or strategic security decisions. Additionally, the widespread use of robotic networks (botnets) for offensive purposes makes spotting and prevention extremely difficult.

Tactical Intelligence The second intelligence category is tactical intelligence. This category is about spotting and identifying preparations for an attack, identifying information that leaked from the organization and analyzing the technological capabilities and motivation of the attackers, as well as their development methods and attack vectors, with the intention of providing early warning prior to the attack. This intelligence category relies on Human Intelligence (HumInt) or the translation thereof to the web world - WebInt - plus complementary technical intelligence.

This intelligence activity is similar to the ages-old methodology of operating agents who collect information directly and pass it on to their operators for analysis, processing and subsequent action, combined with field intelligence specialists who analyze the 'combat doctrines' of the various opponents, their possible attack objectives, methods for extensive cyber warfare operations and so forth.

HumInt in the cyber world includes the creation of virtual personae, or 'Avatars', planting them in attacker groups or in organized crime forums, passively 'monitoring' their discussions and reporting the information to the operator. The product of this intelligence- gathering effort is normally a report that concludes the activity and offers recommended courses of action, or in more uncommon cases - a concrete early warning of an intended attack.

This intelligence category suffers from a dual disadvantage - as it involves entities operated by humans, the coverage span of the intelligence being collected is limited. A good cyber analyst can operate 2-5 entities simultaneously, but there are dozens of forums in which he should operate. After the intelligence has been produced, it is submitted to the end user as a report that he should read, analyze and then make decisions regarding possible courses of action. Naturally, this burdens the end user (normally the Chief Information Security Officer - CISO) who suffers from substantial manpower gaps to begin with.

"Most of the Intelligence being produced is not utilized" The objective of intelligence is to support the security layout. Without such a layout, intelligence is of no significance. For this reason, only mature organizations seek intelligence after they had already deployed the standard solutions and as they now

wish to enhance their security. For these organizations, the intelligence should provide a sort of early warning against attacks. In reality, however, technical intelligence does not produce such alerts and tactical intelligence produces generalized alerts.

This is the reason why most of the intelligence being produced for cyberspace is not utilized - it does not pertain to the organization directly. Clients who gain experience using cyber intelligence services stop consuming those services after a while, as they find no direct value in them and as they do not have available, skilled personnel for assimilating and implementing the intelligence they are provided with. Consequently, the world is becoming disillusioned with cyber intelligence as a sub-activity of the cyber technology world. In a very short period of time, numerous companies were acquired or stricken off the market (Sight Partners and IID were acquired by FireEye and Norse has ceased to operate recently). Apparently, the market is maturing and now seeks tactical solutions with a high degree of automation.

Operational Intelligence The third category of cyber intelligence, which begins to stand out as a separate activity, is operational intelligence. It derives from the change in the security concept. Instead of securing the peripheral boundaries of the organization, which means primarily deploying security assets for the purpose of identifying and stopping the attack or the attacker - developing prompt capabilities for identifying an attack and neutralizing the damage it attempts to inflict. This approach is an adaptation to the cyber threats of the active routine security concept used in the field of national security.

One of the companies that offers an operational intelligence solution is the Sixgill Company of Yokne'am, Israel. This company develops a platform capable of producing intelligence effectively as it allows a small number of analysts to 'dominate' an extensive pool of sources in the Darknet - forums, 'stores' that sell credit cards and 'Dumps' (websites that publish large amounts of data stolen from various elements).

As the system produces alerts automatically, it directs the analysts to analyze the information and derive operational insights. The CEO of Sixgill, Avi Kashtan, told us that the system was developed in cooperation with one of the world's leading banks that uses it daily to spot preparations for attacks, employee and customer data that leaked or was stolen and more general information about future trends.

The operational intelligence approach calls for information that consists primarily of methods, processes and combat and active defense doctrines. It empowers the doctrinal and technical elements cyber intelligence can extract from the space where the opponents organize and conduct their administrative activities. Instead of searching for information regarding a specific attack against the organization, operational cyber intelligence focuses on analyzing the opponents' combat doctrines, weapon systems and attack and operational scenarios. This approach shifts the center of gravity from advance identification and blocking - which were proven to be ineffective, to the ability to respond and block the outcome of the attack within the organizational environment or in its immediate vicinity.

Reuters

FBI decides provisionally not to share iPhone unlock: sources

Wednesday, 27 April 2016

Byline: Mark Hosenball, Dustin Volz

Section: general

Washington - The FBI has provisionally decided not to share an iPhone unlocking mechanism used by a contractor to open the phone of one of the San Bernardino shooters because the agency does not own the mechanism, two U.S. government sources said on Tuesday.
The FBI is expected within days to write to the White House explaining why the agency cannot share the unlocking mechanism with other government agencies, Apple or other third parties, said the sources, who asked to remain anonymous.

Several U.S. government sources said the FBI contractor that unlocked the shooter's phone was a foreign entity and did not give U.S. authorities details of the mechanism. Without that, the FBI could not share it even if it wanted to, sources said.

Reuters reported on April 13 that the unnamed contractor had sole ownership of the method it used, making it unlikely that the government could share it.

A day later, the FBI warned Apple of a separate flaw in its iPhone and Mac software, the company told Reuters on Tuesday.

It was the first time the government had alerted Apple to a vulnerability under a White House interagency procedure, known as the Vulnerabilities Equities Process, for reviewing technology security flaws and deciding which ones should be made public, the company said.

The FBI's provisional decision means that the unlocking mechanism used on the San Bernardino iPhone will not be referred to the interagency procedure for review.

Earlier on Tuesday, FBI Director James Comey said his agency was assessing whether the mechanism would go through the review.

"We are in the midst of trying to sort that out," Comey said.

Officials have said that the interagency review process leans toward disclosure of technological flaws. But it is not set up to handle or reveal flaws which are discovered and owned by private companies, sources have told Reuters.

Comey's comments appeared to confirm the FBI did not own the method used to crack the county-owned work phone belonging to Syed Farook, who with his wife opened fire in December on a San Bernardino, Calif., holiday party, killing 14 and wounding 22.

The method instead belongs to a still-unidentified third party that the FBI said came forward due to the attention received from its public pursuit of a court order to compel Apple's assistance in unlocking the phone.

Apple's refusal to comply prompted a high-profile standoff and fueled a long-simmering debate over security, privacy and law enforcement access to encrypted technology.

The government withdrew its case after it said the hacking method worked. Comey has said the method works on a "narrow slice" of iPhone 5c devices running iOS 9.

An Apple senior executive told reporters earlier this month that it was confident the flaw used by the third party would have a "short shelf life" and be patched through the firm's ongoing efforts to improve the security of its devices.

Reuters

After the Snowden NSA leaks, fewer people are searching for info on terror groups online (Canada)

Wednesday, 27 April 2016

Byline: Joseph Menn

Section: general

San Francisco - nternet traffic to Wikipedia pages summarizing knowledge about terror groups and their tools plunged nearly 30 percent after revelations of widespread Web monitoring by the U.S. National Security Agency, suggesting that concerns about government snooping are hurting the ordinary pursuit of information.
A forthcoming paper in the Berkeley Technology Law Journal analyzes the fall in traffic, arguing that it provides the most direct evidence to date of a so-called "chilling effect," or negative impact on legal conduct, from the intelligence practices disclosed by fugitive former NSA contractor Edward Snowden.

Author Jonathon Penney, a fellow at the University of Toronto's interdisciplinary Citizen Lab, examined monthly views of Wikipedia articles on 48 topics identified by the U.S. Department of Homeland Security as subjects that they track on social media, including Al Qaeda, dirty bombs and jihad.

In the 16 months prior to the first major Snowden stories in June 2013, the articles drew a variable but an increasing audience, with a low point of about 2.2 million per month rising to 3.0 million just before disclosures of the NSA's Internet spying programs. Views of the sensitive pages rapidly fell back to 2.2 million a month in the next two months and later dipped under 2.0 million before stabilizing below 2.5 million 14 months later, Penney found.

The traffic dropped even more to topics that survey respondents deemed especially privacy-sensitive. Viewership of a presumably "safer" group of articles about U.S. government security forces decreased much less in the same period.

Penney's results, subjected to peer-review, offer a deeper dive into an issue investigated by previous researchers, including some who found a 5.0 percent drop in Google searches for sensitive terms immediately after June 2013. Other surveys have found sharply increased use of privacy-protecting Web browsers and communications tools.

Penney's work may provide fodder for technology companies and others arguing for greater restraint and disclosure about intelligence-gathering. Chilling effects are notoriously difficult to document and so have limited impact on laws and court rulings.

More immediately, the research could aid a lawsuit filed by the American Civil Liberties Union on behalf of Wikipedia's nonprofit parent organization and other groups against the NSA and the Justice Department.

The year-old suit argues that intelligence collection from backbone Internet traffic carriers violated the Fourth Amendment ban on unreasonable searches.

Wall Street Journal

Pentagon Won't Give Islamic State Clues on Cyber Strategy

Wednesday, 27 April 2016

Byline: Damian Paletta

Section: general

Washington - The Pentagon is being careful not to reveal the precise ways it is targeting Islamic State through the use of expanded cyber weaponry, concerned that any clues could help the terror network avoid future attacks.
Adm. Mike Rogers, head of U.S. Cyber Command and the National Security Agency, said Tuesday that the Pentagon's use of computer tactics to confront Islamic State is part of its broader campaign to defeat the group. Speaking at Georgetown University, however, he wouldn't say what those tactics are or what the impact has been.

"I'm not going to go into specifics of what we're doing," Adm. Rogers said. "We are working against an adaptive, agile opponent. I'm not interested in giving them any advantage."

In February, the White House and Pentagon began speaking more openly about the government's use of cyberweapons to confront Islamic State, saying it was meant to complement military strikes that have killed a number of the terror network's senior officials in recent months. The public mentions of these computer tools marked a first for the Pentagon, which is usually much more secretive about its use of cyberattacks against foreign groups.

Officials have said the tactics include actions like disrupting Islamic State's ability to communicate, sowing confusion among its members, and steering militants toward certain tools that are easier for the U.S. government to intercept or track.

The true impact of these cyberattacks, however, is unclear. Some people who follow Islamic State's use of social media, for example, say they have seen some change in how militants communicate, but that the group hasn't abandoned traditional methods altogether.

The government's use of these tactics has fed a long-standing tension between intelligence agencies and the military. Intelligence agencies generally want to use any access to an adversary's computer networks to monitor information, while military leaders often see benefit in destroying those networks.

Military and intelligence officials have had numerous discussions about the best way to address this dilemma when confronting Islamic State, people familiar with the matter said. Those discussions are expected to continue.

Presidential front-runners Hillary Clinton and Donald Trump have both expressed frustration that Islamic State continues to use computers and software encryption tools to communicate, recruit and plan attacks. They have proposed taking steps that limit or eliminate Islamic State's access to computers in places like Raqqa, Syria, and Mosul, Iraq.

As recently as several months ago, there were four active Internet cafes in Raqqa, people familiar with the matter said, and Islamic State was careful about monitoring who logged onto Internet devices there and how those devices were used.

Intelligence officials have known about these Internet cafes for months, and it is unclear if the new tactics by Cyber Command are aimed at targeting such locations or pursuing militants and leaders on the battlefield.

The U.S. government has launched a separate effort to work with tech companies including Facebook Inc. and Twitter Inc., hoping to make it harder for violent extremists to use those social media tools.

Financial Times

Iran opens a new front in cyber warfare

Tuesday, 26 April 2016

Byline: Sam Jones

Section: general

London - The first neighbourhood they unplugged was Olaya, Riyadh's wealthiest and gaudiest central district. By the time they had finished their rampage through the computer systems behind the power grid, the infiltrators believed they had left millions without electricity, crippling hospitals and military facilities.
What the hackers, whose use of Farsi and bespoke malware gave away their Iranian origins, did not realise was that the critical computer networks they had compromised were fake.

The network, complete with Arabic scripting and precise names of individual substations and pylons, was the work of MalCrawler, a cyber security group specialising in protecting industrial computer systems. It was just one of a set of intricate digital honeytraps designed to gauge the intentions of the attackers who routinely tried to crack into the systems owned by MalCrawler's clients. Equally intricate models were made of European, American and Israeli power systems.

The evidence from the models aligned. The Chinese hungrily scooped up anything that looked like novel technical information. The Russians permeated deep into systems, mapping them and implanting hard-to-find backdoor access for potential future use. But neither dared do damage -- unlike Iran.

Among the world's big five cyber superpowers -- the US, UK, Israel, Russia and China -- MalCrawler concluded there was a digital equilibrium in military cyber offence based on assumptions over deterrence and reprisal.

"But in the Middle East, that's not the case at all," says Dewan Chowdhury, MalCrawler's chief executive. "The mindset just seemed completely different -- it wasn't espionage or some kind of targeted operation necessarily, it was just to do as much damage as possible."

The model MalCrawler designed to replicate the Israeli power grid was hit just as hard as the Saudi one. The hackers, again displaying tell-tale signs of Iranian origin, fatally compromised the safety systems of what they thought was one of Israel's nuclear power stations.

Iran is rapidly emerging as the sixth member of the cyber superpower club. Denuded of its nuclear ambitions by the landmark deal struck last year to limit uranium and plutonium enrichment, some fear Tehran will wield its cyber arsenal as an equally long-range weapon with which to menace its adversaries.

"Before the [nuclear] deal, cyber was just one option they used for leverage, but now, post deal, it is even more central to their toolkit," says one senior Middle Eastern intelligence official. "Iran is poised to do something in cyber that will change the way the world looks at it?...?the US knows this. [The US] saw what they [Iran] did during the agreement and they know what they are doing after it."

Industrial sabotage

While high-tech espionage is rife -- for strategic state advantage and commercial and criminal gain -- destructive acts of cyber attack remain rare.

Iran is the only country that has both been on the receiving end of a major act of physical cyber-sabotage and the perpetrator of such an attack. In 2008, the Stuxnet computer worm, created by the US and Israel was unleashed on Iran's nuclear programme.

In 2012, Iranian hackers struck Saudi Arabia's national oil company, Saudi Aramco, nearly obliterating its corporate IT infrastructure, and bringing the company close to collapse.

Aramco was a wake-up call for Iran's adversaries. Nearly four years on, just how strong are Iran's cyber capabilities and what, if anything, will Tehran seek to do with them?

"Their abilities are growing fast and they are diversifying. They're getting harder and harder to track," says one senior intelligence official from within the five-eyes alliance -- the digital intelligence-sharing group comprising Australia, Canada, New Zealand, the UK and US. "There is certainly a big move towards having more destructive capability. They want to be able to do more Aramcos. Right now they are researching, practising." Tehran says it spends $1bn a year on cyber programmes.

While its industrial oil production systems were unaffected, Aramco was nearly fatally compromised because so much of its corporate infrastructure was destroyed. Company officials had to use typewriters and faxes to try and keep billions of dollars of oil trades from falling through. Domestically, the company gave oil away for several days following the attack because it could not process transactions.

Christina Kubecka, a cyber security expert who worked for the oil company, told CNN last year that company officials flew to Southeast Asia to acquire as many computer hard drives as they could straight off factory floors.

But the Aramco incident was also a relatively unsophisticated hack. One senior security consultant who worked for the Saudi government in 2012 told the Financial Times that during the very early stages of the operation, the Iranian infiltrators -- who dubbed themselves the Cutting Sword of Justice - - stumbled on a Word document saved on an IT department hard drive, entitled: "Administrator passwords".

Iran's other big cyber operation at that time was Operation Ababil, attributed to a hacking group known as the Cyber Fighters of Izz ad-Din al-Qassam. It launched crude, but sustained attacks to try to overwhelm the websites of some of the US's largest banks. The group claimed no allegiance, but two senior western intelligence officials and other independent cyber security experts say it was an Iranian proxy.

In March this year, the US justice department brought charges against seven Iranians who it said were responsible for the attacks. All worked for Iranian companies -- fronts, said prosecutors, for Tehran's Islamic Revolutionary Guards Corps.

The attacks were "the first shot across the bow", says John Hultquist, director of cyber espionage analysis at iSight. "Since Aramco [and Ababil], we have seen significant development from Iran in terms of their operations and capabilities. I wouldn't call them top tier in sophistication yet, but if I were to list off the most important threats globally -- I would put them [in] there. The [importance] of what they are going after, and their sheer aggression, that's the issue."

Lethal kittens and cleavers

Two hacking groups in particular highlight the development of Iran's cyber capabilities. The first, known as Rocket Kitten, has been closely tracked by many in the cyber security industry since 2014.

FireEye, a US digital security company, first identified it as "Ajax security team", noting its use of a spear-phishing campaign -- the use of legitimate-looking emails to snare targeted victims into opening malicious attachments or following links -- to target Iranian dissidents and Israeli organisations. By 2015, however, other cyber security groups realised that Rocket Kitten, as it was rechristened, was using its own customised malware, not just off-the-shelf code, and was broadening its reach.

Last November, lapses in the Rocket Kitten security procedures allowed the US firm Check Point to access the hackers' own software platform, called "Oyun". Check Point discovered a sophisticated user-friendly application and within it a list of more than 1,842 "projects" -- individuals targeted by hackers. When they ran through the list, they came up with a comprehensive breakdown of Rocket Kitten's targets: 18 per cent were Saudi, 17 per cent from the US, 16 per cent Iranian and 5 per cent Israeli. They ranged from defence officials and contractors, to dissidents, journalists and politicians.

Two intelligence officials, one from Europe and the other from the Middle East, separately told the FT that Rocket Kitten was linked to the IRGC, which, they both added, dominates Tehran's cyber warfare agenda.

It is a second IRGC-backed group, however, that is of even more interest to western defence and security experts.

In December 2014, Cylance, a US cyber security firm, informed its clients of the activities of Iranian hackers engaged in a project it called Operation Cleaver. Based on a forensic analysis of the hackers' activities, Cylance pointed to a group that dubbed itself "Tarh Andishan" -- "the thinkers" in Farsi -- as being behind the action. The research pointed to government- backed organisations as being ultimately responsible.

Cylance declared Iran "the new China" for its aggressive actions in cyber space. Its report detailed a sophisticated online campaign, tracked over two years, that was using custom-built malware to deliberately infect and gain access to sensitive industrial control systems and critical infrastructure in companies across the globe.

The hackers behind Cleaver successfully infected the computers of hundreds of companies and sensitive organisations, from military systems, to oil and gas production controls, to airport and airline security databases. The countries hit hardest were not just the regional and traditional foes of Iran. They included places such as South Korea and Canada.

"What Cleaver really brought to the surface was that these guys were aggressive, compromising critical infrastructure in missions that did not have any classic espionage outcome?...?the Iranians aren't getting into airports and oil and gas companies for intelligence collection?...?these are systems to compromise in order to do harm," says Mr Hultquist. "What was really eye-opening is that they were doing it globally."

Complex picture

Knowing what Iran is technically capable of is only part of the picture. Since 2012, when Ayatollah Ali Khamenei, the Islamic republic's supreme leader, established the supreme cyber council, it has been hardliners that have dominated control of it.

"[Cyber] is folded into the larger context of political and military relationships that the [Iranian] leadership has to sit down and calculate, 'When do I want to do this?'," says Jim Lewis, director of technology and public policy at the Washington-based Center for Strategic and International Studies.

Much of Iran's capability in cyber space stems from its efforts to control dissent and monitor émigrés in the wake of protests triggered by the flawed 2009 election and emergence of the Green movement. The Basij militias -- the paramilitary, pro-regime forces under the direction of the IRGC -- that were crucial in suppressing those protests are now a critical part of Iran's cyber force.

A second, more sophisticated and highly trained group within the guards is responsible for activities such as those seen in operation Cleaver, says one senior British security official.

Iran's proxy cyber forces form a third component with Tehran accused of being one of the world's most active cyber "proliferators", providing damaging malware to groups such as Hizbollah, the Lebanese Shia militants. Such arrangements do raise questions over command and control -- and just what is being done in Iran's name without explicit sanction from Tehran.

In the months since the nuclear deal, MalCrawler, whose digital honeytraps are still in use, collecting data, has noticed a tail-off in Iranian activity. "We're in a period of reorganisation in cyber space," says Mr Chowdhury.

But few expect that to remain the case. "In the short term, as sanctions come off, they want stability," says one Israeli official, "so they are rethinking their attacks. But people need to understand that they are developing capabilities for use years from now."

Cyber, he says, is as core to Iran's strategy as its ballistic missile programme.

"Before cyber they were powerless," says CSIS's Mr Lewis. "They had to sit there and take it. We had sanctions, we had aircraft carriers off their coast. Now with cyber they can strike back."

La Tribune (France)

Sous-marins : les cinq clés du succès de DCNS en Australie

Wednesday, 27 April 2016

Byline: Michel Cabirol

Section: general

Paris - Le succès de DCNS en Australie est à la fois surprenant et logique. Surprenant parce que gagner chez les Wallabies pour un groupe français de défense est une véritable gageure tant ce pays partage des intérêts stratégiques intimes avec les États-Unis, puis dans un second temps avec les pays du Pacifique comme le Japon. Logique également car l'offre de DCNS était imbattable sur le plan technologique et industrielle. N'en déplaise à tous les adeptes du french-bashing, le groupe naval avait le meilleur sous-marin de la compétition en Australie, loin devant le sous- marin japonais et celui proposé sur le papier par l'allemand ThyssenKrupp Marine Systems (TKMS).
Encore fallait-il en convaincre les Australiens ainsi que les Américains, qui n'étaient pas franchement pro-DCNS selon les médias australiens, et, surtout, être capable de le démontrer au sein d'une équipe de France soudée. Sur ce dernier point, ce ne fût pas toujours le cas en coulisse... mais le succès effacera tout. En dépit de ces parasites, la France a toutefois montré officiellement à l'Australie une équipe oeuvrant sur la même longueur d'ondes. Comme savent le faire les Allemands à chaque compétition.

Le réalisme à la française a donc payé dans une compétition qui était imperdable sur le plan technique pour DCNS mais que le groupe naval aurait pu perdre. Car l'histoire des négociations de très grands contrats d'armement montre que très souvent la balance a penché plus sur des critères politiques qu'opérationnels. C'est donc tout à l'honneur de l'Australie, qui s'engage pour 50 ans avec DCNS, d'avoir choisi le meilleur sous-marin pour ces marins dans le cadre d'une consultation qui a été "menée de façon très rigoureuse" , indique-t-on dans l'entourage du ministre de la Défense, Jean-Yves Le Drian.

"L'offre française présentait les meilleures capacités pour répondre aux besoins uniques de l'Australie", a assuré le Premier ministre australien Malcolm Turnbull à Adélaïde, où les sous-marins seront construits. Les 12 sous-marins, a-t-il expliqué, seront "les vaisseaux les plus sophistiqués construits dans le monde".

1/ Le Shortfin Barracuda, le nec plus ultra de la compétition

Face à ses deux rivaux japonais et allemand, DCNS a mis en compétition un sous-marin océanique de plus de 95 mètres de long pour plus de 4.000 tonnes de déplacement en plongée, un navire dérivé du sous-marin nucléaire d'attaque (SNA) Barracuda, le Shortfin Barracuda Block 1A qui dispose d'une propulsion hybride (diesel et électrique). Dans sa version nucléarisée, le Barracuda existe bel et bien. Les premiers essais à la mer sont d'ailleurs programmés en 2017. C'est la première fois que DCNS proposait de partager avec un pays étranger les technologies mises au point pour le Barracuda, qualifiées de joyaux de la couronne par la direction générale de l'armement (DGA).

Selon le gouvernement australien, le sous-marin proposé par DCNS offre "des performances supérieures en matière de senseurs et de furtivité, ainsi que des capacités de projection et d'endurance similaires à celles des sous- marins de la classe Collins", les sous-marins actuellement en service dans la marine australienne.

Le bâtiment est doté d'un système de propulsion avec des pompes-hélices plutôt que d'hélices classiques afin de réduire son empreinte sonore. En outre, selon la directrice générale en charge du développement de DCNS, Marie-Pierre de Bailliencourt, le Shortfin Barracuda offre les "meilleures capacités opérationnelles" en termes d'architecture et de technologies. Notamment il offre une "supériorité acoustique, la meilleure discrétion et va garantir aux Australiens la meilleure autonomie et la meilleure endurance à la mer, c'est-à-dire sa capacité à mener de longues patrouilles" , a-t-elle précisé.

Du côté de ses rivaux, TKMS n'avait aucun sous-marin à proposer de la taille des 4.000 tonnes, le plus gros qu'il ait construit étant le sous-marin d'attaque de 2.200 tonnes, le Dolphins II en service en Israël. Dans ce cadre, TKMS, qui a par ailleurs déjà deux ans de retard dans le programme de sous-marins singapouriens, proposait pour satisfaire au cahier des charges du programme "SEA 1000" le programme Type 216, un bâtiment basé sur les sous-marins 212/214. Avec l'AIP, il aurait eu un rayon d'action de 4.815 km (2.600 nautiques). Mais ce n'était encore qu'un projet contrairement au Shortfin Barracuda. "TKMS a promis la lune en sur-vendant leurs technologies et ont été très bruyants surt la partie industrielle" , analyse une source proche du dossier.

Le consortium, composé de l'État, de Mitsubishi Heavy Industries et de Kawasaki Heavy Industries proposait quant à lui à la marine australienne le sous- marins de type Soryu, long de 84 mètres et déplaçant 4.200 tonnes en plongée. Toutefois, il était moins performant en plongée en eau très profonde, le Barracuda allant beaucoup plus profondément. Le Soryu avait également des problèmes techniques sur la double-coque. Enfin, les industriels japonais, qui sont engagés dans un important programme de renouvellement des sous-marins de la marine japonaise, n'avaient pas non plus les forces nécessaires pour réaliser les bâtiments australiens.

2/ Une équipe de France soudée officiellement

En dépit des sourires qui illuminent aujourd'hui le visage des industriels et des étatiques français, cela n'a pas été facile de mener une équipe de France soudée au succès en Australie. Très clairement, de nombreuses questions se sont posées dans le milieu de la défense sur la façon dont DCNS menait les discussions avec l'Australie. Ces critiques sont restées dans "la famille" de la défense ou presque...Le dossier français a été amélioré au fur et à mesure des discussions qu'a eu le groupe naval avec les Australiens dans le cadre du dialogue compétitif. Notamment le volet industriel a bien été renforcé de façon à réduire l'écart avec les Allemands dont ce volet était le point fort.

Pour autant, le PDG de DCNS, Hervé Guillou, avec sa foi de charbonnier, a cru très tôt à un possible succès dès son arrivée à l'été 2014 à la barre du groupe naval. A l'issue de sa visite le 1er novembre 2014 à Albany en Australie pour le centenaire en hommage des soldats australiens et néo-zélandais (ANZAC) morts en Europe au cours de la Première Guerre Mondiale, Jean-Yves Le Drian y croit aussi. Tant mieux. Car personne n'imagine alors un succès de DCNS en Australie tant les Japonais sont archi- favoris. Ils sont déjà quasi-choisis par le gouvernement précédent.

Pour Jean-Yves Le Drian, DCNS doit arriver au moins en deuxième position derrière les Japonais, qui, juge-t-on en France, ont fait une offre incertaine. Ce qui a été in fine le cas. Canberra a estimé selon la presse que l'offre japonaise posait "un risque considérable" compte tenu du manque d'expérience de Tokyo dans la construction navale à l'étranger. Le ministère de la Défense se met alors en ordre de marche de la même manière que pour les campagnes Rafale. Tous les quinze jours, il organise dès la fin de l'année 2014 une réunion de suivi très détaillée de la campagne en présence d'Hervé Guillou, de responsables de Thales, de la DGA, de l'état-major des armées et du chef d'état-major de la marine ainsi que d'un représentant du ministère des Affaires étrangères. "Il y a eu une très forte intégration des équipes étatiques et industrielles autour de Jean-Yves Le Drian" , assure-t-on dans l'entourage du ministre.

Des entreprises telles que Total, Schneider Electric, Vivendi, Technip et même Airbus... donnent de temps en temps des coups de main à l'équipe France. Bref, la fibre patriotique française joue à fonds. En tant que représentant spécial pour les relations avec l'Australie, le franco-australien Ross McInness, président du conseil d'administration de Safran, a également oeuvré pour le dossier français. Parallèlement, des délégations australiennes viennent à plusieurs reprises à Cherbourg en toute discrétion pour mieux comprendre l'offre française. "Il a fallu leur expliquer comment nous avions construit le coût du programme, quel était le niveau de risques, comment nous comptions gérer les approvisionnements... , précise-t-on à la Tribune. Il a également fallu leur expliquer les écarts de prix selon le lieu de fabrication des sous-marins : en France, en Australie ou un mixte" .

Jean-Yves Le Drian continue de son côté à se démener discrètement pour DCNS. Lors d'un voyage à Washington le 6 juillet, il interroge le ministre de la Défense Ashton Carter, sur la position des États-Unis sur ce dossier. On lui assure alors la neutralité des Américains. En février 2016, le ministre de la Défense retourne en Australie à Sydney, Canberra et Adélaïde, où seront fabriqués les sous-marins australiens dans le chantier navals publics australiens ASC. Il présente à nouveau au Premier ministre australien les arguments de l'offre française. Courant avril, la France apprend que le dossier s'accélère. La semaine dernière, François Hollande écrit à Malcolm Turnbull pour lui rappeler la volonté de la France d'entretenir une coopération stratégique sur le long terme avec l'Australie.

3/ Une relation stratégique de haut niveau

"Nous n'avons pas fait une offre sur un produit mais une offre sur un partenariat sur 50 ans avec l'Australie" , explique-t-on chez DCNS à La Tribune. Car au vu du fiasco de la coopération sur les Collins entre le chantier naval suédois Kockums et l'Australie, qui a traumatisé Canberra, les Australiens ne souhaitaient pas se tromper une nouvelle fois. "Ils cherchaient un allié fiable" , explique- t-on chez DCNS. Ainsi, l'accord de gouvernement à gouvernement (G to G) a fait partie intégrante des 21 points de l'offre française. L'Australie a pu être rassurée également par la capacité de la France à garder une industrie sous-marinière sur une très longue durée pour fournir à la Marine nationale - notamment des sous-marins nucléaires lanceurs d'engins (SNLE) jusqu'en 2085 - et à accompagner et qualifier des programmes complexes grâce à la DGA. "Il ont été rassurés par la stabilité et la pérennité du partenariat qu'on leur proposai t", affirme-t-on dans l'entourage du ministre.

"Notre capacité opérationnelle est sans comparaison avec les deux autres pays , assure-t-on en outre dans l'entourage du ministre. A l'image de l'Australie, nous avons une marine océanique capable de mener des missions de longue durée à travers tous les océans" . Ce qui n'est pas le cas de l'Allemagne, qui reste essentiellement en mer Baltique et en Mer du Nord, et du Japon, dont la zone de navigation est également restreinte que celle de la France. "Les Australiens ont beaucoup insisté sur ce volet" , précise-t-on au ministère. C'est dans ce cadre que la marine française a apporté son soutien au projet de DCNS. Le groupe aéronaval (GAN) français parti en fin d'année dernière dans le golfe persique pour lutter contre Daech a accueilli dans son escorte la frégate australienne HMAS Melbourne.

Au-delà du soutien de Canberra à la France dans le cadre de la lutte contre le djihadisme international (escorte du porte-avions Charles-de-Gaulle et ravitaillement des avions de combat français par des tankers australiens dans le cadre de l'opération Chammal en Irak), la France et l'Australie partagent "une grande proximité d'analyse" dans leurs réflexions stratégiques au regard de leur livre blanc sur la défense, observe-t-on dans l'entourage du ministre. Tout comme la France, l'Australie a identifié trois grandes menaces : un pays qui menace la souveraineté (Chine), la menace du terrorisme transnational (combattants australiens au sein de Daech) et, enfin, le risque de déstabilisation d'une région par des Etats faillis comme les Fidji après le putsch de décembre 2006 .

Par ailleurs, la non-livraison des Mistral à la Russie en 2014 a permis à la France de présenter une offre, assure-t-on dans l'entourage du ministre. L'Australie a été l'un des pays qui a le plus interrogé la France sur le dossier des Mistral. Enfin, Paris aurait continué son partenariat stratégique avec Canberra même en cas d'échec.

4/ Une proposition industrielle attractive

Face à la soi-disant " Deutsche Qualität" de l'Allemagne, la France a mis les bouchées doubles pour présenter une offre industrielle attractive et séduisante pour l'Australie. La France a très vite compris qu'elle devait aider Canberra à développer des capacités industrielles de souveraineté nationale pour compenser une dépense de plus de 34 milliards d'euros. Les transferts de technologies (ToT) étaient donc l'une des clés majeures de la compétition. D'autant plus que les Australiens, très déçus par les faibles retours industriels du programme Collins, ont toute la capacité à absorber les ToT.

DCNS possède une longue expérience de coopération au niveau international avec les succès du Scorpène au Brésil, en Malaisie et en Inde où à chaque fois le groupe naval a transféré de la technologie. En revanche, TKMS voulait industrialiser l'Australie en emmenant dans ses bagages sa supply chain et les Japonais n'avaient aucune expérience en ToT pour un programme de cette envergure. Contrairement à DCNS et ses partenaires, qui ont préféré s'appuyer sur l'industrie australienne pour développer cette fameuse industrie de souveraineté nationale. DCNS a signé des accords d'exclusivité avec les huit principales universités australiennes, dont l'hydrodynamisme (dynamisme des fluides), les matériaux composites, les fluides anti-corrosion... En outre, DCNS a audité 250 entreprises australiennes pour expertiser leur solidité sur le long terme.

Thales, un atout pour DCNS en Australie

"Thales est un industriel de confiance en Australie , a résumé le PDG de Thales, Patrice Caine. Cela a aidé DCNS a faire le break face aux Allemands" . En tant que sous-systémier du groupe américain qui sera retenu pour le cerveau des sous- marins (CMS ou systèmes de gestion de combat) -Lockheed Martin ou Raytheon - , le groupe d'électronique vise "potentiellement" 1 milliard de prises de commandes comme la fourniture de sonars et d'équipements de communications, de guerre électronique et d'optronique pour les sous-marins que doit fournir DCNS à l'Australie. Thales, qui emploie quelque 3.200 personnes en Australie, a déjà fourni au pays les sonars et des équipements d'optronique et de communications pour ses sous-marins, a-t-il rappelé.

Note(s) :

Straits Times

Don't be a victim of cyber attacks

Wednesday, 27 April 2016

Section: general

Singapore - It all started with my business card. It was all the hacker needed to start a chain of events that ended with me clicking on a dubious link on a website.
Earlier this month, I had approached security firm Trend Micro to conduct an experiment: they would attempt to hack me and my colleague, Lisabel Ting.

Cybercrime is on the rise; the number of such incidents almost doubled in 2015 from the previous year, according to crime statistics released by the Singapore Police Force in February.

Earlier this month, the Government announced in Parliament that a new cyber security Bill will be introduced in 2017 to strengthen measures against online crime.

The purpose of the Trend Micro experiment was to find out how easy - or difficult - it is for cyber attacks to succeed. Trend Micro's senior research manager Ryan Flores crafted a spear-phishing e-mail that impersonated my former boss, someone I know and trust. For Lisabel, Mr Flores had created a fake Facebook profile of her friend in order to get close to her.

Spear-phishing starts with the cyber criminal researching the target to create e-mails that appear to come from trusted sources. They could be a colleague or business partner. These e-mails may include content relevant to the target's interests or industry. Because these e-mails appear authentic, the target is more likely to download an attachment or open a link in them, which are openings for malware to be installed on your device.

For instance, cyber criminals could install a keylogger that records your key strokes to find out your passwords.

Ransomware is another form of malware used in cyber scams. "The hacker would lock the user out of his device and demand a ransom to unlock it. Personal information could also be used to blackmail the user," explained Mr Flores.

Spear-phishing is not new, but it is increasingly easy to use because of the vast amount of personal information available on social media such as Facebook and LinkedIn. These days, anything from a person's movie preferences to the home address can be found in an online search. Photos can reveal a person's social circles and travel information will show a person's location, said Intel Security's vice-president David Freer.

In fact, Singapore was ranked third globally in terms of spear-phishing attacks, according to Symantec's annual Internet Security Threats 2015 report.

The high number of spear-phishing attempts in Singapore could be because of its status as a regional financial hub, with many potential targets for cyber criminals, said Symantec's senior director Peter Sparkes.

In other words, these cyber hits could be targeted at employees in order to compromise their organisations. A high-profile example is a 2011 incident that occurred at RSA, the American security firm known for its two-factor authentication product. An RSA employee fell victim to a spear-phishing e-mail that contained malware giving the criminals remote access to his computer and company network. As a result, sensitive company data was stolen.

To prevent yourself from becoming a victim of cyber attacks, here are five tips compiled from security experts at Symantec, Intel Security and Trend Micro:

Keep your browser, operating system and security software updated to prevent malware from affecting your computer, in the event that you open a malicious attachment or link. But note that there are often new vulnerabilities that may not have been patched in time.

Be cautious about sharing the details of your life on social media. Personal information, such as the name of your primary school or pet nickname may be used in security questions asked by online accounts to verify users during password recovery.

If an online deal sounds too good to be true, it probably is. Avoid clicking on such links. Hover the mouse over the link to check if it leads to a reputable website.

Vary the names of your e-mail accounts - do not use the same alias for multiple accounts. Each account should have its own unique and strong password (mix of alpha-numeric characters).

Use the incognito or private browsing modes offered by browsers, especially when accessing the Internet at a public location.

Iran Daily

US, Canada to join Iranian crude customers

Wednesday, 27 April 2016

Section: general

Tehran - Iran has begun negotiations with American and Canadian oil companies on petrochemical sales, technology purchase as well as investment in the country's oil and gas projects.
Following the removal of nuclear- related sanctions, new oil agreements were to be inked with major European firms like Shell, BP, Eni, Total and Repsol though North American companies seem to have overtaken them in launching oil talks with Iran, Mehr News Agency reported.

Accordingly, over the past few months several American and Canadian companies have initiated talks on implementing projects in upstream and midstream sections of Iranian oil, gas and petrochemical industries aiming to make investments, sell goods and equipment, offer drilling services as well as to purchase oil products of Iran.

Iran's Minister of Oil Bijan Zanganeh had previously pointed to negotiations with several American companies like General Electric, stressing "the talks have been constructive."

In addition, Managing Director of National Iranian Oil Company Rokneddin Javadi has rejected the existence of legal restrictions or prohibitions on making oil deals or joint investments with North American companies especially American ones; "Iran is ready to sell oil to all world countries except for the Zionist regime."

In time with the return of General Electric to the negotiations table, Halliburton Company of the US has also conducted talks with the National Iranian Drilling Company on offering certain technical services as

the likelihood of signing oil agreements with the American firm has increased for launching new drilling projects with Iranian private and state companies.

Managing Director of the National Petrochemical Company (NPC) Marzieh Shah-Daei touched upon certain talks with a number of American companies on running new cooperation in petrochemical industries maintaining "no direct talks has been conducted with American oil giants"

Shah-Daei said the axis of talks with the American-European company has been purchase of technical knowledge asserting "direct investment in Iranian petrochemical industries on the part of American companies is not currently at stake."

Meanwhile, some managers of Iranian petrochemical firms have reported on receiving proposals from American companies on exports of certain petrochemical and polymer products like different grades of PVC powder.

Also, Head of Technology and Research at Iranian Offshore Oil Company (IOOC) Javad Rostami had noted "the project to examine economic justification and feasibility of Binaloud oilfield has been handed over to a Canadian company; "currently, we are looking forward to receiving the final report by the company," he had asserted.

Head of Oil Industry Equipment Producing Association Reza Khiamian also reported on talks with Canadian oil equipment producers adding "in addition to the North American country, some negotiations have been held with European countries like France and Germany."

Khiamian further enumerated main axes of talks between Iranian and Canadian companies including "knowledge and technology transfer, establishment of a production line for manufacturing advanced industrial equipment as well as investment attraction."

On Monday, Director of DMC Process Project at Research Institute of Petroleum Industry (RIPI) Mansur Bazmi also reported on collaborations with a Canadian company on construction of an oil desalination plant; "Iran and Canada will both participate in the construction the facilities."

Gulf News

Is your fleet hacker-proof?

Wednesday, 27 April 2016

Byline: Stephen Brennan

Section: general

Dubai - Traffic accidents killed 675 people in the UAE last year and injured a further 6,863. The advent of driverless cars holds the promise to cut this to a fraction.
The full societal potential of the technology goes far further -- from providing a lifeline to the old, to cutting down on traffic congestion and freeing up family time.

What's vital is that government and motor industry executives take the necessary steps to ensure that driverless cars are protected from malicious hackers, learning from other industries research and experience, so that the public can profit from this transformative technology.

It's important to get things into perspective before indulging in science fiction fantasies of runaway cars causing havoc on our roads. Much of the technology already exists. For example, autopilot controls most of the routine portion of aircraft flights.

Airlines increasingly mandate computer control for extreme weather conditions, where computers can react swiftly, predictably and without panic.

Nonetheless, the autonomy and connectivity of driverless cars does leave them open to attacks from malicious cybercriminals or terrorists. The principal threats are three-fold:

First, hackers could gain control of an individual car, either to cause mischief, or at the extreme end turn it into a missile.

Second, they could use the car's systems to intrude on the privacy of individuals, by tracking their movements and access personal or otherwise sensitive data (although considering most of us carry around a smartphone this is hardly a unique threat).

Third, and potentially most damaging, hackers could use the inherent connectivity of driverless vehicles to disrupt an entire city. It's not hard to imagine thousands of cars parked motionless on Shaikh Zayed road.

It happens most rush hours, but if these fleets were being controlled to produce maximum disruption over days, this would have serious implications for emergency services and the economy of Dubai.

There are clear steps that carmakers, and their governmental regulators, can take to ensure that any risk from cyberattack is minimised. The airline industry has already led the way with its focus and enhancements on deterministic ethernet.

Carmakers need to ensure that control systems are managed in an organised and systematic manner rather than simply bolted on to the general internet connectivity of the vehicle.

It's vital to look after three 'A's of computer security: authentication, authorisation and accounting. Authentication provides a way of identifying a user with advanced cryptography. This ensures that the car's central processing unit knows exactly who or what it's receiving information from and giving commands to at all times.

Authorisation ensures that each part of the system gives appropriate commands; it's perfectly acceptable for the neighbouring car to be providing its positional data to avoid a crash; it's not for the car to cause your engine to stop.

Third, all the information needs to be accounted for. It's inevitable some accidents will happen, and it's vital that a record is kept of all events for subsequent analysis just like a plane's black box.

Cybersecurity concerns should not stop a revolution, which according to tech entrepreneur Elon Musk may be only a few years away, but security does need to be built in at a foundational level to ensure the world gains the benefits and minimises the risks.

Fars News Agency

International Bank Transfer System Hacked

Wednesday, 27 April 2016

Section: general

Tehran - Swift, the global financial network that banks use to transfer billions of dollars every day, has warned its customers it is aware of "a number of recent cyber incidents" where attackers had sent fraudulent messages over its system.
The disclosure came as law enforcement authorities in Bangladesh and elsewhere investigated the cyber theft of US$81m (£55.9m) from the Bangladesh central bank account at the New York Federal Reserve. Swift has acknowledged the scheme involved altering Swift software on Bangladesh Bank's computers to hide evidence of fraudulent transfers, Guardian reported.

Monday's statement from Swift marked the first acknowledgement that the Bangladesh Bank attack was not an isolated incident but one of several recent criminal schemes that aimed to take advantage of the global messaging platform used by some 11,000 financial institutions.

"Swift is aware of a number of recent cyber incidents in which malicious insiders or external attackers have managed to submit Swift messages from financial institutions' back offices, PCs or workstations connected to their local interface to the Swift network," the group warned customers.

The warning, which Swift issued in a confidential alert sent over its network, did not name any victims or disclose the value of any losses from the previously undisclosed attacks. Swift confirmed to Reuters the authenticity of the notice.

Swift, or the Society for Worldwide Interbank Financial Telecommunication, is a cooperative owned by 3,000 financial institutions.

Also on Monday, Swift released a security update to the software that banks use to access its network to thwart malware that security researchers with British defence contractor BAE Systems said was probably used by hackers in the Bangladesh Bank heist.

BAE's evidence suggested that hackers manipulated Swift's Alliance Access server software, which banks use to interface with Swift's messaging platform, to cover their tracks. BAE said it could not explain how the fraudulent orders were created and pushed through the system.

But Swift provided some evidence about how that happened in its note to customers, saying that in most cases the attackers obtained valid credentials for operators authorised to create and approve Swift messages, then submitted fraudulent messages by impersonating those people.

Cyber security experts said more attacks could surface as Swift banking clients look to see if their access had been compromised.

Shane Shook, a banking security consultant, said hackers were turning to Swift and other private financial messaging platforms because they could steal larger amounts. "These hacks specifically target financial institutions because smaller efforts result in much larger thefts," he said. "It's much more efficient than stealing from consumers."

Justin Harvey, chief security officer with Fidelis Cybersecurity, said hackers followed the money and would be drawn into such schemes in hopes of emulating a big heist like the one on Bangladesh Bank. "After the Bangladesh Bank heist became public, every other attacker out there is looking to see if they can do the same," he said.

Swift spokeswoman Natasha Deteran told Reuters that the commonality in these cases was that internal or external attackers compromised the banks' own environments to obtain valid operator credentials. "Customers should do their utmost to protect against this," she said in an email to Reuters.

Swift told customers that the security update must be installed by 12 May. "We have made the Alliance interface software update mandatory as it is designed to help banks identify situations in which

attackers have attempted to hide their traces - whether these actions have been executed manually or through malware," she said.

Motherboard Blog

Canada Is Considering Spying on Kids to Stop Cyberbullying

Wednesday, 27 April 2016

Byline: Jordan Pearson

Section: general

Toronto - Cyberbullying is simply awful, and its consequences can be utterly horrific. Canadians have known this all too well since 17-year-old Rehtaeh Parsons' suicide in 2013, after photos of her alleged rape circulated online.
It's only human to want to put a stop to it. But is it worth spying on kids?

To wit, the Canadian government is looking for a person or organization to "conduct an evaluation of an innovative cyberbullying prevention or intervention initiative" in a "sample of school- aged children and youth," according to a tender notice published by Public Safety Canada last week.

Although nothing has been finalized, the government will consider letting the organization spy on kids' digital communications to do it, Barry McKenna, the Public Safety procurement consultant in charge of the tender, told me.

"The tender doesn't preclude or necessarily require digital monitoring," said McKenna. "But there are certainly products on the market that do that, and I would guess that that kind of intervention would be one of interest."

The school board overseeing the school used in the study would have to sign off on digital surveillance of kids, McKenna said, and so would Public Safety. McKenna would not disclose whether any person or organization has responded to the tender yet. The government has budgeted $60,000 for the program, the notice states.

"Cyberbullying isn't a technological problem"

"Any use by government of technology to scan the internet and read somebody's communications obviously raises privacy issues," said David Fraser, a Canadian privacy lawyer consulting on a new cyberbullying law for Nova Scotia. "Fewer privacy issues if it's following an intervention and it's targeted," he continued, "way more if they're trying to single out kids in Canada and assess what they're saying."

"What we've seen come out of Public Safety and most law enforcement agencies is a pretty un-nuanced, heavy- handed, over the top model," Fraser added. Nova Scotia's previous cyberbullying law, passed in the wake of Parsons' suicide, was ruled unconstitutional and struck down for being too broad and infringing on people's civil rights.

If the Public Safety study ends up taking a more blanket approach to monitoring kids instead of targeting surveillance after an incident, it could also risk undermining communication between kids and their teachers or parents, according to US Cyberbullying Research Center co- director Sameer Hinduja.

"Installing tracking apps undermines any sort of open-minded communication [that] youth-serving adults might have with these kids, because you're tracking them surreptitiously," said Hinduja. "Kids, as they get older, want more privacy and freedom. It's natural--you want it, and I want it."

This isn't the first time somebody has considered surveillance as a solution to the complex social issue of kids being absolutely horrific to each other, and it likely won't be the last. In 2013, The LA Times noted that the Glendale Unified School District in Southern California reportedly paid a firm $40,000 to monitor kids' social media accounts to combat bullying. The move raised the ire of privacy advocates in the US then, too.

The point, according to Hinduja, is that bullying isn't a uniquely digital problem. You don't solve bullying forever by putting a teacher in every hallway, and you don't fix crime by putting a cop on every corner.

"Cyberbullying isn't a technological problem," said Hinduja. "You can't blame the apps, the smartphones, or the internet. Instead, cyberbullying is rooted in other issues that everyone has been dealing with since the beginning of time: adolescent development, kids learning to manage their problems, and dealing with stress."

Motherboad Blog

Needs to Revive the Encryption Debate It Had in the 1990s

Wednesday, 27 April 2016

Byline: Matthew Braga

Section: Comment

Comment: In the wake of a court battle between Apple and the FBI, American lawmakers have been considering a new policy on encryption, on the basis that strong technological protections are making it difficult for law enforcement and intelligence agencies to solve crime.
Such a policy, which would mandate a so-called backdoor in encryption software, would inevitably compromise the security of all communications, privacy advocates have argued. And yet, given the gravity of the situation, in Canada there has been no similar debate. At least, not recently.

Though largely forgotten today, the Canadian federal government actually did have an encryption debate of its own in the late 1990s. It brought law enforcement together with experts to discuss encryption's role in a then-early internet, and the potential impacts on national security and public safety that might arise from encryption's use.

What's most fascinating is how closely the arguments from two decades prior mirror those that are being made today. Though technology has come a long way since then, looking back at Canada's own debate shows that some of the arguments being made today by politicians and law enforcement in the US are still stuck in the past.

"We all came to the conclusion that [legislation] would be the death-knell for [...] secure communications online," said Ann Cavoukian, who served as the Information and Privacy Commissioner of Ontario from 1997 to 2014. "We thought it had died, and here it is again."

18 law enforcement agencies, including the RCMP and CSIS, even called for "mandatory access" to encryption keys

US lawmakers and experts previously engaged in a pair of fierce cryptographic fights that came to a head in 1994: the first, over the passing of the Communications Assistance for Law Enforcement Act, or CALEA, an American wiretapping law that dictates when and how telecommunications companies have to assist law enforcement and intelligence agencies engage in electronic surveillance; and the second, over a US-government backed encryption scheme called Clipper, a special computer chip that, when installed in a phone, would give the National Security Agency backdoor access to otherwise encrypted communications.

Ultimately, CALEA passed--with compromises--and the Clipper chip was scrapped. It was in this context, the aftermath of the Crypto Wars to the south, that the Canadian government decided to have its own debate.

In January 1999, a Senate Special Committee on Terrorism and Public Safety released a report on threats to public safety and national security, and listed encryption as an emerging issue. Based on interviews with law enforcement, academics, telecommunications companies and members of the financial community, the committee reiterated many of the same arguments that can still be heard today: that encryption is making law enforcement's job harder; that backdoors built into encryption mechanisms for

government use could just as easily be used by criminals; and that undermining encryption would compromise the security of financial systems too.

18 law enforcement agencies, including the RCMP and CSIS, even called for "mandatory access" to encryption keys used to protect stored data and data in transit. In what has become an oft-used turn-of-phrase, police argued that "they do not seek increased investigative capabilities through mandatory key access or otherwise, but instead seek only to restore and maintain their existing investigative capabilities."

In the end, no cryptography policy was proposed, and the committee recommended law enforcement and intelligence agencies seek other methods to overcome the obstacle of encryption. However, the committee did recommend amending the Criminal Code "to provide lawful access to encryption keys by law enforcement and security intelligence organizations and to criminalize encryption when used in the commission of a crime."

These recommendations were never adopted. It's not clear why, but it's likely that the government chose to follow the lead of countries such as the US, which had backed down from similar schemes.

As the RCMP previously told Motherboard, there is no power in the Criminal Code specific to encryption. According to Scott Bardsley, press secretary for Public Safety Minister Ralph Goodale's office, police can either compel a third party to decrypt data with judicial authorization, or they may attempt to decrypt the data themselves.

When asked if the Canadian government was planning on revisiting the encryption debate, Barsdley would only tell Motherboard that "broad public consultations on national security issues" are planned in the "medium term." But Cavoukian would be happy if there was no debate at all.

"I would prefer no discussion, because if there's no discussion, you're not resurrecting the discussion of the 90s," she said. "To me, we put the issue to bed."

Globe and Mail

Ransomware poses complex legal and reputational risks

Wednesday, 27 April 2016

Byline: Brent Arnold & Christopher Oates

Section: Comment

Comment: As businesses and public institutions increasingly become the targets of ransomware - malware that blocks access to computer systems or the information they contain until the user performs actions demanded by hackers - legal risks surrounding such headlinemaking attacks have come to the fore in Canadian corporate consciousness.
A January report by the Online Trust Alliance reveals that ransomware attacks aimed at companies are not only growing more prevalent, but they are also becoming more sophisticated. Today's hackers can custom tailor their demands according to the size and market value of their corporate mark. Making matters worse, last month Apple's iOS operating system was infected with ransomware for the first time.

Ransomware typically gains access to a computer system when a user clicks on unfamiliar links or strange attachments (although a growing number of programs are infecting computers via the download of ostensibly legitimate applications).

In its most benign form, an infection could force employees to complete a survey; at its most malignant, it has strongarmed companies into paying actual ransoms (typically in the nationless and virtually untraceable currency of bitcoin).

Businesses that fail to comply face the destruction of client and proprietary data, and intellectual property - not to mention sustaining significant reputational damage and exposure to third-party lawsuits from clients and consumers (and there is never any guarantee that meeting hackers' demands will result in computers or data being unlocked).

Despite this growing threat, legal recourses for ransomware victims are slim. The activity is, of course, illegal and should be immediately reported to police (the RCMP also suggest reporting to the Canadian Anti-Fraud Centre). But despite the fact that such attacks have been reported for more than a decade, there are no documented cases of ransomware perpetrators ever having been prosecuted in Canada.

Given the often remote nature of the crime (the few attacks that have been successfully traced typically come from foreign countries), criminal and civil remedies may be unlikely to succeed.

In the rare event a cybercriminal is identified, civil proceedings against foreign nationals are most likely to result in default judgments that are difficult if not impossible to collect on.

While cybercriminals frequently avoid prosecution, their corporate victims may find themselves in the legal spotlight. Recent amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) will soon require companies subject to PIPEDA to alert the federal privacy commissioner, affected individuals and relevant organizations or government institutions following a breach of security safeguards that "creates a real risk of significant harm to the individual."

This can include risk of economic loss by the person whose personal information is subject to the breach, as well as potential reputational harms.

While reporting obligations provide an important consumer protection and will be a legal necessity in certain cases (companies that fail to report where required by PIPEDA may be subject to fines of up to $100,000), they are nonetheless problematic for businesses - particularly those for whom data security is a critical component of their brand identity. Recent hacks have shaken consumer and shareholder confidence and resulted in both significant disruption for targeted businesses and resignations by top executives.

All indicators suggest ransomware will only become more vicious and prevalent in the foreseeable future. With added reporting pressure looming on the horizon, companies that fall prey may soon find themselves facing complex legal and reputational risks.

Brent Arnold and Christopher Oates are lawyers at Gowling WLG, whose practices focus heavily on technology- and privacy-related matters.

Washington Post

FBI says it can't explain how iPhone was hacked

Wednesday, 27 April 2016

Byline: Ellen Nakashima

Section: general

Washington - The FBI intends to tell the White House this week that its understanding of how a third party hacked the iPhone of a shooter in San Bernardino, Calif., is so limited that there's no point in undertaking a government review of whether the tool should be shared with Apple, officials said. The decision, said officials familiar with the discussion who spoke on the condition of anonymity, ends several weeks of internal debate by bureau lawyers and technical experts about the FBI's obligation to disclose the method.

Last month, the FBI paid more than $1 million for a tool to crack an iPhone used by one of the shooters in California. But the contract did not include rights to the software flaws that went into the tool, officials said.

As a result, the bureau has a limited technical understanding of how the method worked, officials said.

On Tuesday, FBI Director James B. Comey acknowledged the internal debate.

"The threshold is: Are we aware of the vulnerability, or did we just buy a tool and don't have sufficient knowledge of the vulnerability that would implicate the process?" he said at a cyber conference at Georgetown University.

Comey was referring to a process, led by the White House, in which agencies such as the FBI, National Security Agency (NSA) and Homeland Security Department debate whether to disclose a computer software flaw discovered by the government to the software maker so the company can fix it.

Most flaws are disclosed, the White House has said. But some are kept secret so that the law enforcement or intelligence agency can use them in intelligence- gathering or criminal investigations.

The FBI's decision to not submit to a review of the method used in the San Bernardino case was first reported by the Wall Street Journal.

Some security experts said the bureau or the NSA could reverse-engineer the tool to gain information about the flaws. But the bureau was not likely to do so, several officials said.

"If what we have bought is a tool, and we've said that we won't reverse-engineer the tool such that you can figure out what vulnerability is used to make the tool work, then even if we wanted to disclose something, there's nothing we can disclose," one senior administration official said.

The FBI recovered the iPhone of Syed Rizwan Farook, one of the shooters in the December terrorist attack in San Bernardino, but could not access the data on it because it did not know Farook's passcode. In February, the Justice Department obtained a court order to force Apple to write software that would disable several phone security features so the FBI could try to crack the code.

Apple challenged the order, arguing that the court had no basis to issue it and that it would set a dangerous precedent. In late March, the FBI disclosed that a third party had come forward with a tool to help it gain access to the phone and so it no longer needed the court order to force Apple's assistance.

Security and privacy advocates then began to push the bureau to disclose to Apple the flaws on which the tool was based so the tech giant could repair them.

Last month, professional hackers or vulnerabilities researchers brought flaws they had found to a company whose name the FBI has not disclosed.

Apple has said it will not press for the vulnerabilities to be disclosed.

"We're confident that the vulnerability the government alleges to have found will have a short shelf life," a lawyer for Apple told reporters earlier this month. "In our normal process . . . we'll continue to improve the phones and at some point this fix will get implemented."

Times of Israel

Operational Cyber Intelligence

Wednesday, 27 April 2016

Section: general

Jerusalem - Visitors to the CyberTech 2016 exhibition had the impression that every single exhibitor boasted a cyber intelligence capability. Indeed, cyber intelligence (or threat intelligence) has evolved into one of the hottest trends of the cyber technology industry in the last few years. Even the relatively small Israeli market generates massive demand for intelligence services and some ten product and service companies are involved in this activity, competing one another.
The regulator has not remained idle either. According to Directive #361 of the Banking Supervisor at the Bank of Israel, financial institutions must use intelligence in addition to the other security mechanisms they employ. So, apparently everyone is talking about cyber intelligence and many people would like to know how to consume it, but what, in fact, is cyber intelligence and how does it help users to defend themselves against threats?

Cyber intelligence produces operational insights by looking outside the organization and issuing alerts of imminent and future threats to the organization. The type of intelligence may be categorized according to the manner in which the information is collected and analyzed and the manner in which the final product is used. Roughly, the world of cyber intelligence is divided into three categories: technical intelligence, tactical intelligence and operational intelligence.

Technical Intelligence Technical intelligence constitutes the overwhelming majority of intelligence sold around the world. This intelligence category is based on a method adopted from military intelligence, known as Signals Intelligence (SigInt), which consists of the interception of electronic signals and deriving information from those signals. In the Internet world, this refers to the characteristics of web traffic (IP address, server locations and so forth), as well as to malware indicators. Combining these data makes it possible to identify suspicious traffic to and from the organization, and to block it.

Organizations and suppliers that collect intelligence of this category deploy networks of sensors to identify suspicious traffic and IP addresses suspected of disseminating malware and junk mail. This information is delivered in a digital format directly to the security systems (Firewalls, Anti-Virus

software) and enables them to block undesirable elements. The primary disadvantage of this intelligence category is the fact that it is essentially responsive, namely - it identifies and handles attacks that have already taken place somewhere in the digital space. It cannot effectively identify new attacks that have not been documented, analyzed and translated into 'signatures'.

The various approaches that attempt to solve this problem through mathematical/statistical analysis of behavior patterns are plagued by a high percentage of false positive 'noise' messages. Additionally, these technical intelligence models do not normally produce insights regarding potential attacks, and no conclusions may be derived from them for the purpose of making tactical or strategic security decisions. Additionally, the widespread use of robotic networks (botnets) for offensive purposes makes spotting and prevention extremely difficult.

Tactical Intelligence The second intelligence category is tactical intelligence. This category is about spotting and identifying preparations for an attack, identifying information that leaked from the organization and analyzing the technological capabilities and motivation of the attackers, as well as their development methods and attack vectors, with the intention of providing early warning prior to the attack. This intelligence category relies on Human Intelligence (HumInt) or the translation thereof to the web world - WebInt - plus complementary technical intelligence.

This intelligence activity is similar to the ages-old methodology of operating agents who collect information directly and pass it on to their operators for analysis, processing and subsequent action, combined with field intelligence specialists who analyze the 'combat doctrines' of the various opponents, their possible attack objectives, methods for extensive cyber warfare operations and so forth.

HumInt in the cyber world includes the creation of virtual personae, or 'Avatars', planting them in attacker groups or in organized crime forums, passively 'monitoring' their discussions and reporting the information to the operator. The product of this intelligence- gathering effort is normally a report that concludes the activity and offers recommended courses of action, or in more uncommon cases - a concrete early warning of an intended attack.

This intelligence category suffers from a dual disadvantage - as it involves entities operated by humans, the coverage span of the intelligence being collected is limited. A good cyber analyst can operate 2-5 entities simultaneously, but there are dozens of forums in which he should operate. After the intelligence has been produced, it is submitted to the end user as a report that he should read, analyze and then make decisions regarding possible courses of action. Naturally, this burdens the end user (normally the Chief Information Security Officer - CISO) who suffers from substantial manpower gaps to begin with.

"Most of the Intelligence being produced is not utilized" The objective of intelligence is to support the security layout. Without such a layout, intelligence is of no significance. For this reason, only mature organizations seek intelligence after they had already deployed the standard solutions and as they now

wish to enhance their security. For these organizations, the intelligence should provide a sort of early warning against attacks. In reality, however, technical intelligence does not produce such alerts and tactical intelligence produces generalized alerts.

This is the reason why most of the intelligence being produced for cyberspace is not utilized - it does not pertain to the organization directly. Clients who gain experience using cyber intelligence services stop consuming those services after a while, as they find no direct value in them and as they do not have available, skilled personnel for assimilating and implementing the intelligence they are provided with. Consequently, the world is becoming disillusioned with cyber intelligence as a sub-activity of the cyber technology world. In a very short period of time, numerous companies were acquired or stricken off the market (Sight Partners and IID were acquired by FireEye and Norse has ceased to operate recently). Apparently, the market is maturing and now seeks tactical solutions with a high degree of automation.

Operational Intelligence The third category of cyber intelligence, which begins to stand out as a separate activity, is operational intelligence. It derives from the change in the security concept. Instead of securing the peripheral boundaries of the organization, which means primarily deploying security assets for the purpose of identifying and stopping the attack or the attacker - developing prompt capabilities for identifying an attack and neutralizing the damage it attempts to inflict. This approach is an adaptation to the cyber threats of the active routine security concept used in the field of national security.

One of the companies that offers an operational intelligence solution is the Sixgill Company of Yokne'am, Israel. This company develops a platform capable of producing intelligence effectively as it allows a small number of analysts to 'dominate' an extensive pool of sources in the Darknet - forums, 'stores' that sell credit cards and 'Dumps' (websites that publish large amounts of data stolen from various elements).

As the system produces alerts automatically, it directs the analysts to analyze the information and derive operational insights. The CEO of Sixgill, Avi Kashtan, told us that the system was developed in cooperation with one of the world's leading banks that uses it daily to spot preparations for attacks, employee and customer data that leaked or was stolen and more general information about future trends.

The operational intelligence approach calls for information that consists primarily of methods, processes and combat and active defense doctrines. It empowers the doctrinal and technical elements cyber intelligence can extract from the space where the opponents organize and conduct their administrative activities. Instead of searching for information regarding a specific attack against the organization, operational cyber intelligence focuses on analyzing the opponents' combat doctrines, weapon systems and attack and operational scenarios. This approach shifts the center of gravity from advance identification and blocking - which were proven to be ineffective, to the ability to respond and block the outcome of the attack within the organizational environment or in its immediate vicinity.

Reuters

FBI decides provisionally not to share iPhone unlock: sources

Wednesday, 27 April 2016

Byline: Mark Hosenball, Dustin Volz

Section: general

Washington - The FBI has provisionally decided not to share an iPhone unlocking mechanism used by a contractor to open the phone of one of the San Bernardino shooters because the agency does not own the mechanism, two U.S. government sources said on Tuesday.
The FBI is expected within days to write to the White House explaining why the agency cannot share the unlocking mechanism with other government agencies, Apple or other third parties, said the sources, who asked to remain anonymous.

Several U.S. government sources said the FBI contractor that unlocked the shooter's phone was a foreign entity and did not give U.S. authorities details of the mechanism. Without that, the FBI could not share it even if it wanted to, sources said.

Reuters reported on April 13 that the unnamed contractor had sole ownership of the method it used, making it unlikely that the government could share it.

A day later, the FBI warned Apple of a separate flaw in its iPhone and Mac software, the company told Reuters on Tuesday.

It was the first time the government had alerted Apple to a vulnerability under a White House interagency procedure, known as the Vulnerabilities Equities Process, for reviewing technology security flaws and deciding which ones should be made public, the company said.

The FBI's provisional decision means that the unlocking mechanism used on the San Bernardino iPhone will not be referred to the interagency procedure for review.

Earlier on Tuesday, FBI Director James Comey said his agency was assessing whether the mechanism would go through the review.

"We are in the midst of trying to sort that out," Comey said.

Officials have said that the interagency review process leans toward disclosure of technological flaws. But it is not set up to handle or reveal flaws which are discovered and owned by private companies, sources have told Reuters.

Comey's comments appeared to confirm the FBI did not own the method used to crack the county-owned work phone belonging to Syed Farook, who with his wife opened fire in December on a San Bernardino, Calif., holiday party, killing 14 and wounding 22.

The method instead belongs to a still-unidentified third party that the FBI said came forward due to the attention received from its public pursuit of a court order to compel Apple's assistance in unlocking the phone.

Apple's refusal to comply prompted a high-profile standoff and fueled a long-simmering debate over security, privacy and law enforcement access to encrypted technology.

The government withdrew its case after it said the hacking method worked. Comey has said the method works on a "narrow slice" of iPhone 5c devices running iOS 9.

An Apple senior executive told reporters earlier this month that it was confident the flaw used by the third party would have a "short shelf life" and be patched through the firm's ongoing efforts to improve the security of its devices.

Reuters

After the Snowden NSA leaks, fewer people are searching for info on terror groups online (Canada)

Wednesday, 27 April 2016

Byline: Joseph Menn

Section: general

San Francisco - nternet traffic to Wikipedia pages summarizing knowledge about terror groups and their tools plunged nearly 30 percent after revelations of widespread Web monitoring by the U.S. National Security Agency, suggesting that concerns about government snooping are hurting the ordinary pursuit of information.
A forthcoming paper in the Berkeley Technology Law Journal analyzes the fall in traffic, arguing that it provides the most direct evidence to date of a so-called "chilling effect," or negative impact on legal conduct, from the intelligence practices disclosed by fugitive former NSA contractor Edward Snowden.

Author Jonathon Penney, a fellow at the University of Toronto's interdisciplinary Citizen Lab, examined monthly views of Wikipedia articles on 48 topics identified by the U.S. Department of Homeland Security as subjects that they track on social media, including Al Qaeda, dirty bombs and jihad.

In the 16 months prior to the first major Snowden stories in June 2013, the articles drew a variable but an increasing audience, with a low point of about 2.2 million per month rising to 3.0 million just before disclosures of the NSA's Internet spying programs. Views of the sensitive pages rapidly fell back to 2.2 million a month in the next two months and later dipped under 2.0 million before stabilizing below 2.5 million 14 months later, Penney found.

The traffic dropped even more to topics that survey respondents deemed especially privacy-sensitive. Viewership of a presumably "safer" group of articles about U.S. government security forces decreased much less in the same period.

Penney's results, subjected to peer-review, offer a deeper dive into an issue investigated by previous researchers, including some who found a 5.0 percent drop in Google searches for sensitive terms immediately after June 2013. Other surveys have found sharply increased use of privacy-protecting Web browsers and communications tools.

Penney's work may provide fodder for technology companies and others arguing for greater restraint and disclosure about intelligence-gathering. Chilling effects are notoriously difficult to document and so have limited impact on laws and court rulings.

More immediately, the research could aid a lawsuit filed by the American Civil Liberties Union on behalf of Wikipedia's nonprofit parent organization and other groups against the NSA and the Justice Department.

The year-old suit argues that intelligence collection from backbone Internet traffic carriers violated the Fourth Amendment ban on unreasonable searches.

Wall Street Journal

Pentagon Won't Give Islamic State Clues on Cyber Strategy

Wednesday, 27 April 2016

Byline: Damian Paletta

Section: general

Washington - The Pentagon is being careful not to reveal the precise ways it is targeting Islamic State through the use of expanded cyber weaponry, concerned that any clues could help the terror network avoid future attacks.
Adm. Mike Rogers, head of U.S. Cyber Command and the National Security Agency, said Tuesday that the Pentagon's use of computer tactics to confront Islamic State is part of its broader campaign to defeat the group. Speaking at Georgetown University, however, he wouldn't say what those tactics are or what the impact has been.

"I'm not going to go into specifics of what we're doing," Adm. Rogers said. "We are working against an adaptive, agile opponent. I'm not interested in giving them any advantage."

In February, the White House and Pentagon began speaking more openly about the government's use of cyberweapons to confront Islamic State, saying it was meant to complement military strikes that have killed a number of the terror network's senior officials in recent months. The public mentions of these computer tools marked a first for the Pentagon, which is usually much more secretive about its use of cyberattacks against foreign groups.

Officials have said the tactics include actions like disrupting Islamic State's ability to communicate, sowing confusion among its members, and steering militants toward certain tools that are easier for the U.S. government to intercept or track.

The true impact of these cyberattacks, however, is unclear. Some people who follow Islamic State's use of social media, for example, say they have seen some change in how militants communicate, but that the group hasn't abandoned traditional methods altogether.

The government's use of these tactics has fed a long-standing tension between intelligence agencies and the military. Intelligence agencies generally want to use any access to an adversary's computer networks to monitor information, while military leaders often see benefit in destroying those networks.

Military and intelligence officials have had numerous discussions about the best way to address this dilemma when confronting Islamic State, people familiar with the matter said. Those discussions are expected to continue.

Presidential front-runners Hillary Clinton and Donald Trump have both expressed frustration that Islamic State continues to use computers and software encryption tools to communicate, recruit and plan attacks. They have proposed taking steps that limit or eliminate Islamic State's access to computers in places like Raqqa, Syria, and Mosul, Iraq.

As recently as several months ago, there were four active Internet cafes in Raqqa, people familiar with the matter said, and Islamic State was careful about monitoring who logged onto Internet devices there and how those devices were used.

Intelligence officials have known about these Internet cafes for months, and it is unclear if the new tactics by Cyber Command are aimed at targeting such locations or pursuing militants and leaders on the battlefield.

The U.S. government has launched a separate effort to work with tech companies including Facebook Inc. and Twitter Inc., hoping to make it harder for violent extremists to use those social media tools.

Financial Times

Iran opens a new front in cyber warfare

Tuesday, 26 April 2016

Byline: Sam Jones

Section: general

London - The first neighbourhood they unplugged was Olaya, Riyadh's wealthiest and gaudiest central district. By the time they had finished their rampage through the computer systems behind the power grid, the infiltrators believed they had left millions without electricity, crippling hospitals and military facilities.
What the hackers, whose use of Farsi and bespoke malware gave away their Iranian origins, did not realise was that the critical computer networks they had compromised were fake.

The network, complete with Arabic scripting and precise names of individual substations and pylons, was the work of MalCrawler, a cyber security group specialising in protecting industrial computer systems. It was just one of a set of intricate digital honeytraps designed to gauge the intentions of the attackers who routinely tried to crack into the systems owned by MalCrawler's clients. Equally intricate models were made of European, American and Israeli power systems.

The evidence from the models aligned. The Chinese hungrily scooped up anything that looked like novel technical information. The Russians permeated deep into systems, mapping them and implanting hard-to-find backdoor access for potential future use. But neither dared do damage -- unlike Iran.

Among the world's big five cyber superpowers -- the US, UK, Israel, Russia and China -- MalCrawler concluded there was a digital equilibrium in military cyber offence based on assumptions over deterrence and reprisal.

"But in the Middle East, that's not the case at all," says Dewan Chowdhury, MalCrawler's chief executive. "The mindset just seemed completely different -- it wasn't espionage or some kind of targeted operation necessarily, it was just to do as much damage as possible."

The model MalCrawler designed to replicate the Israeli power grid was hit just as hard as the Saudi one. The hackers, again displaying tell-tale signs of Iranian origin, fatally compromised the safety systems of what they thought was one of Israel's nuclear power stations.

Iran is rapidly emerging as the sixth member of the cyber superpower club. Denuded of its nuclear ambitions by the landmark deal struck last year to limit uranium and plutonium enrichment, some fear Tehran will wield its cyber arsenal as an equally long-range weapon with which to menace its adversaries.

"Before the [nuclear] deal, cyber was just one option they used for leverage, but now, post deal, it is even more central to their toolkit," says one senior Middle Eastern intelligence official. "Iran is poised to do something in cyber that will change the way the world looks at it?...?the US knows this. [The US] saw what they [Iran] did during the agreement and they know what they are doing after it."

Industrial sabotage

While high-tech espionage is rife -- for strategic state advantage and commercial and criminal gain -- destructive acts of cyber attack remain rare.

Iran is the only country that has both been on the receiving end of a major act of physical cyber-sabotage and the perpetrator of such an attack. In 2008, the Stuxnet computer worm, created by the US and Israel was unleashed on Iran's nuclear programme.

In 2012, Iranian hackers struck Saudi Arabia's national oil company, Saudi Aramco, nearly obliterating its corporate IT infrastructure, and bringing the company close to collapse.

Aramco was a wake-up call for Iran's adversaries. Nearly four years on, just how strong are Iran's cyber capabilities and what, if anything, will Tehran seek to do with them?

"Their abilities are growing fast and they are diversifying. They're getting harder and harder to track," says one senior intelligence official from within the five-eyes alliance -- the digital intelligence-sharing group comprising Australia, Canada, New Zealand, the UK and US. "There is certainly a big move towards having more destructive capability. They want to be able to do more Aramcos. Right now they are researching, practising." Tehran says it spends $1bn a year on cyber programmes.

While its industrial oil production systems were unaffected, Aramco was nearly fatally compromised because so much of its corporate infrastructure was destroyed. Company officials had to use typewriters and faxes to try and keep billions of dollars of oil trades from falling through. Domestically, the company gave oil away for several days following the attack because it could not process transactions.

Christina Kubecka, a cyber security expert who worked for the oil company, told CNN last year that company officials flew to Southeast Asia to acquire as many computer hard drives as they could straight off factory floors.

But the Aramco incident was also a relatively unsophisticated hack. One senior security consultant who worked for the Saudi government in 2012 told the Financial Times that during the very early stages of the operation, the Iranian infiltrators -- who dubbed themselves the Cutting Sword of Justice - - stumbled on a Word document saved on an IT department hard drive, entitled: "Administrator passwords".

Iran's other big cyber operation at that time was Operation Ababil, attributed to a hacking group known as the Cyber Fighters of Izz ad-Din al-Qassam. It launched crude, but sustained attacks to try to overwhelm the websites of some of the US's largest banks. The group claimed no allegiance, but two senior western intelligence officials and other independent cyber security experts say it was an Iranian proxy.

In March this year, the US justice department brought charges against seven Iranians who it said were responsible for the attacks. All worked for Iranian companies -- fronts, said prosecutors, for Tehran's Islamic Revolutionary Guards Corps.

The attacks were "the first shot across the bow", says John Hultquist, director of cyber espionage analysis at iSight. "Since Aramco [and Ababil], we have seen significant development from Iran in terms of their operations and capabilities. I wouldn't call them top tier in sophistication yet, but if I were to list off the most important threats globally -- I would put them [in] there. The [importance] of what they are going after, and their sheer aggression, that's the issue."

Lethal kittens and cleavers

Two hacking groups in particular highlight the development of Iran's cyber capabilities. The first, known as Rocket Kitten, has been closely tracked by many in the cyber security industry since 2014.

FireEye, a US digital security company, first identified it as "Ajax security team", noting its use of a spear-phishing campaign -- the use of legitimate-looking emails to snare targeted victims into opening malicious attachments or following links -- to target Iranian dissidents and Israeli organisations. By 2015, however, other cyber security groups realised that Rocket Kitten, as it was rechristened, was using its own customised malware, not just off-the-shelf code, and was broadening its reach.

Last November, lapses in the Rocket Kitten security procedures allowed the US firm Check Point to access the hackers' own software platform, called "Oyun". Check Point discovered a sophisticated user-friendly application and within it a list of more than 1,842 "projects" -- individuals targeted by hackers. When they ran through the list, they came up with a comprehensive breakdown of Rocket Kitten's targets: 18 per cent were Saudi, 17 per cent from the US, 16 per cent Iranian and 5 per cent Israeli. They ranged from defence officials and contractors, to dissidents, journalists and politicians.

Two intelligence officials, one from Europe and the other from the Middle East, separately told the FT that Rocket Kitten was linked to the IRGC, which, they both added, dominates Tehran's cyber warfare agenda.

It is a second IRGC-backed group, however, that is of even more interest to western defence and security experts.

In December 2014, Cylance, a US cyber security firm, informed its clients of the activities of Iranian hackers engaged in a project it called Operation Cleaver. Based on a forensic analysis of the hackers' activities, Cylance pointed to a group that dubbed itself "Tarh Andishan" -- "the thinkers" in Farsi -- as being behind the action. The research pointed to government- backed organisations as being ultimately responsible.

Cylance declared Iran "the new China" for its aggressive actions in cyber space. Its report detailed a sophisticated online campaign, tracked over two years, that was using custom-built malware to deliberately infect and gain access to sensitive industrial control systems and critical infrastructure in companies across the globe.

The hackers behind Cleaver successfully infected the computers of hundreds of companies and sensitive organisations, from military systems, to oil and gas production controls, to airport and airline security databases. The countries hit hardest were not just the regional and traditional foes of Iran. They included places such as South Korea and Canada.

"What Cleaver really brought to the surface was that these guys were aggressive, compromising critical infrastructure in missions that did not have any classic espionage outcome?...?the Iranians aren't getting into airports and oil and gas companies for intelligence collection?...?these are systems to compromise in order to do harm," says Mr Hultquist. "What was really eye-opening is that they were doing it globally."

Complex picture

Knowing what Iran is technically capable of is only part of the picture. Since 2012, when Ayatollah Ali Khamenei, the Islamic republic's supreme leader, established the supreme cyber council, it has been hardliners that have dominated control of it.

"[Cyber] is folded into the larger context of political and military relationships that the [Iranian] leadership has to sit down and calculate, 'When do I want to do this?'," says Jim Lewis, director of technology and public policy at the Washington-based Center for Strategic and International Studies.

Much of Iran's capability in cyber space stems from its efforts to control dissent and monitor émigrés in the wake of protests triggered by the flawed 2009 election and emergence of the Green movement. The Basij militias -- the paramilitary, pro-regime forces under the direction of the IRGC -- that were crucial in suppressing those protests are now a critical part of Iran's cyber force.

A second, more sophisticated and highly trained group within the guards is responsible for activities such as those seen in operation Cleaver, says one senior British security official.

Iran's proxy cyber forces form a third component with Tehran accused of being one of the world's most active cyber "proliferators", providing damaging malware to groups such as Hizbollah, the Lebanese Shia militants. Such arrangements do raise questions over command and control -- and just what is being done in Iran's name without explicit sanction from Tehran.

In the months since the nuclear deal, MalCrawler, whose digital honeytraps are still in use, collecting data, has noticed a tail-off in Iranian activity. "We're in a period of reorganisation in cyber space," says Mr Chowdhury.

But few expect that to remain the case. "In the short term, as sanctions come off, they want stability," says one Israeli official, "so they are rethinking their attacks. But people need to understand that they are developing capabilities for use years from now."

Cyber, he says, is as core to Iran's strategy as its ballistic missile programme.

"Before cyber they were powerless," says CSIS's Mr Lewis. "They had to sit there and take it. We had sanctions, we had aircraft carriers off their coast. Now with cyber they can strike back."

La Tribune (France)

Sous-marins : les cinq clés du succès de DCNS en Australie

Wednesday, 27 April 2016

Byline: Michel Cabirol

Section: general

Paris - Le succès de DCNS en Australie est à la fois surprenant et logique. Surprenant parce que gagner chez les Wallabies pour un groupe français de défense est une véritable gageure tant ce pays partage des intérêts stratégiques intimes avec les États-Unis, puis dans un second temps avec les pays du Pacifique comme le Japon. Logique également car l'offre de DCNS était imbattable sur le plan technologique et industrielle. N'en déplaise à tous les adeptes du french-bashing, le groupe naval avait le meilleur sous-marin de la compétition en Australie, loin devant le sous- marin japonais et celui proposé sur le papier par l'allemand ThyssenKrupp Marine Systems (TKMS).
Encore fallait-il en convaincre les Australiens ainsi que les Américains, qui n'étaient pas franchement pro-DCNS selon les médias australiens, et, surtout, être capable de le démontrer au sein d'une équipe de France soudée. Sur ce dernier point, ce ne fût pas toujours le cas en coulisse... mais le succès effacera tout. En dépit de ces parasites, la France a toutefois montré officiellement à l'Australie une équipe oeuvrant sur la même longueur d'ondes. Comme savent le faire les Allemands à chaque compétition.

Le réalisme à la française a donc payé dans une compétition qui était imperdable sur le plan technique pour DCNS mais que le groupe naval aurait pu perdre. Car l'histoire des négociations de très grands contrats d'armement montre que très souvent la balance a penché plus sur des critères politiques qu'opérationnels. C'est donc tout à l'honneur de l'Australie, qui s'engage pour 50 ans avec DCNS, d'avoir choisi le meilleur sous-marin pour ces marins dans le cadre d'une consultation qui a été "menée de façon très rigoureuse" , indique-t-on dans l'entourage du ministre de la Défense, Jean-Yves Le Drian.

"L'offre française présentait les meilleures capacités pour répondre aux besoins uniques de l'Australie", a assuré le Premier ministre australien Malcolm Turnbull à Adélaïde, où les sous-marins seront construits. Les 12 sous-marins, a-t-il expliqué, seront "les vaisseaux les plus sophistiqués construits dans le monde".

1/ Le Shortfin Barracuda, le nec plus ultra de la compétition

Face à ses deux rivaux japonais et allemand, DCNS a mis en compétition un sous-marin océanique de plus de 95 mètres de long pour plus de 4.000 tonnes de déplacement en plongée, un navire dérivé du sous-marin nucléaire d'attaque (SNA) Barracuda, le Shortfin Barracuda Block 1A qui dispose d'une propulsion hybride (diesel et électrique). Dans sa version nucléarisée, le Barracuda existe bel et bien. Les premiers essais à la mer sont d'ailleurs programmés en 2017. C'est la première fois que DCNS proposait de partager avec un pays étranger les technologies mises au point pour le Barracuda, qualifiées de joyaux de la couronne par la direction générale de l'armement (DGA).

Selon le gouvernement australien, le sous-marin proposé par DCNS offre "des performances supérieures en matière de senseurs et de furtivité, ainsi que des capacités de projection et d'endurance similaires à celles des sous- marins de la classe Collins", les sous-marins actuellement en service dans la marine australienne.

Le bâtiment est doté d'un système de propulsion avec des pompes-hélices plutôt que d'hélices classiques afin de réduire son empreinte sonore. En outre, selon la directrice générale en charge du développement de DCNS, Marie-Pierre de Bailliencourt, le Shortfin Barracuda offre les "meilleures capacités opérationnelles" en termes d'architecture et de technologies. Notamment il offre une "supériorité acoustique, la meilleure discrétion et va garantir aux Australiens la meilleure autonomie et la meilleure endurance à la mer, c'est-à-dire sa capacité à mener de longues patrouilles" , a-t-elle précisé.

Du côté de ses rivaux, TKMS n'avait aucun sous-marin à proposer de la taille des 4.000 tonnes, le plus gros qu'il ait construit étant le sous-marin d'attaque de 2.200 tonnes, le Dolphins II en service en Israël. Dans ce cadre, TKMS, qui a par ailleurs déjà deux ans de retard dans le programme de sous-marins singapouriens, proposait pour satisfaire au cahier des charges du programme "SEA 1000" le programme Type 216, un bâtiment basé sur les sous-marins 212/214. Avec l'AIP, il aurait eu un rayon d'action de 4.815 km (2.600 nautiques). Mais ce n'était encore qu'un projet contrairement au Shortfin Barracuda. "TKMS a promis la lune en sur-vendant leurs technologies et ont été très bruyants surt la partie industrielle" , analyse une source proche du dossier.

Le consortium, composé de l'État, de Mitsubishi Heavy Industries et de Kawasaki Heavy Industries proposait quant à lui à la marine australienne le sous- marins de type Soryu, long de 84 mètres et déplaçant 4.200 tonnes en plongée. Toutefois, il était moins performant en plongée en eau très profonde, le Barracuda allant beaucoup plus profondément. Le Soryu avait également des problèmes techniques sur la double-coque. Enfin, les industriels japonais, qui sont engagés dans un important programme de renouvellement des sous-marins de la marine japonaise, n'avaient pas non plus les forces nécessaires pour réaliser les bâtiments australiens.

2/ Une équipe de France soudée officiellement

En dépit des sourires qui illuminent aujourd'hui le visage des industriels et des étatiques français, cela n'a pas été facile de mener une équipe de France soudée au succès en Australie. Très clairement, de nombreuses questions se sont posées dans le milieu de la défense sur la façon dont DCNS menait les discussions avec l'Australie. Ces critiques sont restées dans "la famille" de la défense ou presque...Le dossier français a été amélioré au fur et à mesure des discussions qu'a eu le groupe naval avec les Australiens dans le cadre du dialogue compétitif. Notamment le volet industriel a bien été renforcé de façon à réduire l'écart avec les Allemands dont ce volet était le point fort.

Pour autant, le PDG de DCNS, Hervé Guillou, avec sa foi de charbonnier, a cru très tôt à un possible succès dès son arrivée à l'été 2014 à la barre du groupe naval. A l'issue de sa visite le 1er novembre 2014 à Albany en Australie pour le centenaire en hommage des soldats australiens et néo-zélandais (ANZAC) morts en Europe au cours de la Première Guerre Mondiale, Jean-Yves Le Drian y croit aussi. Tant mieux. Car personne n'imagine alors un succès de DCNS en Australie tant les Japonais sont archi- favoris. Ils sont déjà quasi-choisis par le gouvernement précédent.

Pour Jean-Yves Le Drian, DCNS doit arriver au moins en deuxième position derrière les Japonais, qui, juge-t-on en France, ont fait une offre incertaine. Ce qui a été in fine le cas. Canberra a estimé selon la presse que l'offre japonaise posait "un risque considérable" compte tenu du manque d'expérience de Tokyo dans la construction navale à l'étranger. Le ministère de la Défense se met alors en ordre de marche de la même manière que pour les campagnes Rafale. Tous les quinze jours, il organise dès la fin de l'année 2014 une réunion de suivi très détaillée de la campagne en présence d'Hervé Guillou, de responsables de Thales, de la DGA, de l'état-major des armées et du chef d'état-major de la marine ainsi que d'un représentant du ministère des Affaires étrangères. "Il y a eu une très forte intégration des équipes étatiques et industrielles autour de Jean-Yves Le Drian" , assure-t-on dans l'entourage du ministre.

Des entreprises telles que Total, Schneider Electric, Vivendi, Technip et même Airbus... donnent de temps en temps des coups de main à l'équipe France. Bref, la fibre patriotique française joue à fonds. En tant que représentant spécial pour les relations avec l'Australie, le franco-australien Ross McInness, président du conseil d'administration de Safran, a également oeuvré pour le dossier français. Parallèlement, des délégations australiennes viennent à plusieurs reprises à Cherbourg en toute discrétion pour mieux comprendre l'offre française. "Il a fallu leur expliquer comment nous avions construit le coût du programme, quel était le niveau de risques, comment nous comptions gérer les approvisionnements... , précise-t-on à la Tribune. Il a également fallu leur expliquer les écarts de prix selon le lieu de fabrication des sous-marins : en France, en Australie ou un mixte" .

Jean-Yves Le Drian continue de son côté à se démener discrètement pour DCNS. Lors d'un voyage à Washington le 6 juillet, il interroge le ministre de la Défense Ashton Carter, sur la position des États-Unis sur ce dossier. On lui assure alors la neutralité des Américains. En février 2016, le ministre de la Défense retourne en Australie à Sydney, Canberra et Adélaïde, où seront fabriqués les sous-marins australiens dans le chantier navals publics australiens ASC. Il présente à nouveau au Premier ministre australien les arguments de l'offre française. Courant avril, la France apprend que le dossier s'accélère. La semaine dernière, François Hollande écrit à Malcolm Turnbull pour lui rappeler la volonté de la France d'entretenir une coopération stratégique sur le long terme avec l'Australie.

3/ Une relation stratégique de haut niveau

"Nous n'avons pas fait une offre sur un produit mais une offre sur un partenariat sur 50 ans avec l'Australie" , explique-t-on chez DCNS à La Tribune. Car au vu du fiasco de la coopération sur les Collins entre le chantier naval suédois Kockums et l'Australie, qui a traumatisé Canberra, les Australiens ne souhaitaient pas se tromper une nouvelle fois. "Ils cherchaient un allié fiable" , explique- t-on chez DCNS. Ainsi, l'accord de gouvernement à gouvernement (G to G) a fait partie intégrante des 21 points de l'offre française. L'Australie a pu être rassurée également par la capacité de la France à garder une industrie sous-marinière sur une très longue durée pour fournir à la Marine nationale - notamment des sous-marins nucléaires lanceurs d'engins (SNLE) jusqu'en 2085 - et à accompagner et qualifier des programmes complexes grâce à la DGA. "Il ont été rassurés par la stabilité et la pérennité du partenariat qu'on leur proposai t", affirme-t-on dans l'entourage du ministre.

"Notre capacité opérationnelle est sans comparaison avec les deux autres pays , assure-t-on en outre dans l'entourage du ministre. A l'image de l'Australie, nous avons une marine océanique capable de mener des missions de longue durée à travers tous les océans" . Ce qui n'est pas le cas de l'Allemagne, qui reste essentiellement en mer Baltique et en Mer du Nord, et du Japon, dont la zone de navigation est également restreinte que celle de la France. "Les Australiens ont beaucoup insisté sur ce volet" , précise-t-on au ministère. C'est dans ce cadre que la marine française a apporté son soutien au projet de DCNS. Le groupe aéronaval (GAN) français parti en fin d'année dernière dans le golfe persique pour lutter contre Daech a accueilli dans son escorte la frégate australienne HMAS Melbourne.

Au-delà du soutien de Canberra à la France dans le cadre de la lutte contre le djihadisme international (escorte du porte-avions Charles-de-Gaulle et ravitaillement des avions de combat français par des tankers australiens dans le cadre de l'opération Chammal en Irak), la France et l'Australie partagent "une grande proximité d'analyse" dans leurs réflexions stratégiques au regard de leur livre blanc sur la défense, observe-t-on dans l'entourage du ministre. Tout comme la France, l'Australie a identifié trois grandes menaces : un pays qui menace la souveraineté (Chine), la menace du terrorisme transnational (combattants australiens au sein de Daech) et, enfin, le risque de déstabilisation d'une région par des Etats faillis comme les Fidji après le putsch de décembre 2006 .

Par ailleurs, la non-livraison des Mistral à la Russie en 2014 a permis à la France de présenter une offre, assure-t-on dans l'entourage du ministre. L'Australie a été l'un des pays qui a le plus interrogé la France sur le dossier des Mistral. Enfin, Paris aurait continué son partenariat stratégique avec Canberra même en cas d'échec.

4/ Une proposition industrielle attractive

Face à la soi-disant " Deutsche Qualität" de l'Allemagne, la France a mis les bouchées doubles pour présenter une offre industrielle attractive et séduisante pour l'Australie. La France a très vite compris qu'elle devait aider Canberra à développer des capacités industrielles de souveraineté nationale pour compenser une dépense de plus de 34 milliards d'euros. Les transferts de technologies (ToT) étaient donc l'une des clés majeures de la compétition. D'autant plus que les Australiens, très déçus par les faibles retours industriels du programme Collins, ont toute la capacité à absorber les ToT.

DCNS possède une longue expérience de coopération au niveau international avec les succès du Scorpène au Brésil, en Malaisie et en Inde où à chaque fois le groupe naval a transféré de la technologie. En revanche, TKMS voulait industrialiser l'Australie en emmenant dans ses bagages sa supply chain et les Japonais n'avaient aucune expérience en ToT pour un programme de cette envergure. Contrairement à DCNS et ses partenaires, qui ont préféré s'appuyer sur l'industrie australienne pour développer cette fameuse industrie de souveraineté nationale. DCNS a signé des accords d'exclusivité avec les huit principales universités australiennes, dont l'hydrodynamisme (dynamisme des fluides), les matériaux composites, les fluides anti-corrosion... En outre, DCNS a audité 250 entreprises australiennes pour expertiser leur solidité sur le long terme.

Thales, un atout pour DCNS en Australie

"Thales est un industriel de confiance en Australie , a résumé le PDG de Thales, Patrice Caine. Cela a aidé DCNS a faire le break face aux Allemands" . En tant que sous-systémier du groupe américain qui sera retenu pour le cerveau des sous- marins (CMS ou systèmes de gestion de combat) -Lockheed Martin ou Raytheon - , le groupe d'électronique vise "potentiellement" 1 milliard de prises de commandes comme la fourniture de sonars et d'équipements de communications, de guerre électronique et d'optronique pour les sous-marins que doit fournir DCNS à l'Australie. Thales, qui emploie quelque 3.200 personnes en Australie, a déjà fourni au pays les sonars et des équipements d'optronique et de communications pour ses sous-marins, a-t-il rappelé.

Note(s) :

Straits Times

Don't be a victim of cyber attacks

Wednesday, 27 April 2016

Section: general

Singapore - It all started with my business card. It was all the hacker needed to start a chain of events that ended with me clicking on a dubious link on a website.
Earlier this month, I had approached security firm Trend Micro to conduct an experiment: they would attempt to hack me and my colleague, Lisabel Ting.

Cybercrime is on the rise; the number of such incidents almost doubled in 2015 from the previous year, according to crime statistics released by the Singapore Police Force in February.

Earlier this month, the Government announced in Parliament that a new cyber security Bill will be introduced in 2017 to strengthen measures against online crime.

The purpose of the Trend Micro experiment was to find out how easy - or difficult - it is for cyber attacks to succeed. Trend Micro's senior research manager Ryan Flores crafted a spear-phishing e-mail that impersonated my former boss, someone I know and trust. For Lisabel, Mr Flores had created a fake Facebook profile of her friend in order to get close to her.

Spear-phishing starts with the cyber criminal researching the target to create e-mails that appear to come from trusted sources. They could be a colleague or business partner. These e-mails may include content relevant to the target's interests or industry. Because these e-mails appear authentic, the target is more likely to download an attachment or open a link in them, which are openings for malware to be installed on your device.

For instance, cyber criminals could install a keylogger that records your key strokes to find out your passwords.

Ransomware is another form of malware used in cyber scams. "The hacker would lock the user out of his device and demand a ransom to unlock it. Personal information could also be used to blackmail the user," explained Mr Flores.

Spear-phishing is not new, but it is increasingly easy to use because of the vast amount of personal information available on social media such as Facebook and LinkedIn. These days, anything from a person's movie preferences to the home address can be found in an online search. Photos can reveal a person's social circles and travel information will show a person's location, said Intel Security's vice-president David Freer.

In fact, Singapore was ranked third globally in terms of spear-phishing attacks, according to Symantec's annual Internet Security Threats 2015 report.

The high number of spear-phishing attempts in Singapore could be because of its status as a regional financial hub, with many potential targets for cyber criminals, said Symantec's senior director Peter Sparkes.

In other words, these cyber hits could be targeted at employees in order to compromise their organisations. A high-profile example is a 2011 incident that occurred at RSA, the American security firm known for its two-factor authentication product. An RSA employee fell victim to a spear-phishing e-mail that contained malware giving the criminals remote access to his computer and company network. As a result, sensitive company data was stolen.

To prevent yourself from becoming a victim of cyber attacks, here are five tips compiled from security experts at Symantec, Intel Security and Trend Micro:

Keep your browser, operating system and security software updated to prevent malware from affecting your computer, in the event that you open a malicious attachment or link. But note that there are often new vulnerabilities that may not have been patched in time.

Be cautious about sharing the details of your life on social media. Personal information, such as the name of your primary school or pet nickname may be used in security questions asked by online accounts to verify users during password recovery.

If an online deal sounds too good to be true, it probably is. Avoid clicking on such links. Hover the mouse over the link to check if it leads to a reputable website.

Vary the names of your e-mail accounts - do not use the same alias for multiple accounts. Each account should have its own unique and strong password (mix of alpha-numeric characters).

Use the incognito or private browsing modes offered by browsers, especially when accessing the Internet at a public location.

Iran Daily

US, Canada to join Iranian crude customers

Wednesday, 27 April 2016

Section: general

Tehran - Iran has begun negotiations with American and Canadian oil companies on petrochemical sales, technology purchase as well as investment in the country's oil and gas projects.
Following the removal of nuclear- related sanctions, new oil agreements were to be inked with major European firms like Shell, BP, Eni, Total and Repsol though North American companies seem to have overtaken them in launching oil talks with Iran, Mehr News Agency reported.

Accordingly, over the past few months several American and Canadian companies have initiated talks on implementing projects in upstream and midstream sections of Iranian oil, gas and petrochemical industries aiming to make investments, sell goods and equipment, offer drilling services as well as to purchase oil products of Iran.

Iran's Minister of Oil Bijan Zanganeh had previously pointed to negotiations with several American companies like General Electric, stressing "the talks have been constructive."

In addition, Managing Director of National Iranian Oil Company Rokneddin Javadi has rejected the existence of legal restrictions or prohibitions on making oil deals or joint investments with North American companies especially American ones; "Iran is ready to sell oil to all world countries except for the Zionist regime."

In time with the return of General Electric to the negotiations table, Halliburton Company of the US has also conducted talks with the National Iranian Drilling Company on offering certain technical services as

the likelihood of signing oil agreements with the American firm has increased for launching new drilling projects with Iranian private and state companies.

Managing Director of the National Petrochemical Company (NPC) Marzieh Shah-Daei touched upon certain talks with a number of American companies on running new cooperation in petrochemical industries maintaining "no direct talks has been conducted with American oil giants"

Shah-Daei said the axis of talks with the American-European company has been purchase of technical knowledge asserting "direct investment in Iranian petrochemical industries on the part of American companies is not currently at stake."

Meanwhile, some managers of Iranian petrochemical firms have reported on receiving proposals from American companies on exports of certain petrochemical and polymer products like different grades of PVC powder.

Also, Head of Technology and Research at Iranian Offshore Oil Company (IOOC) Javad Rostami had noted "the project to examine economic justification and feasibility of Binaloud oilfield has been handed over to a Canadian company; "currently, we are looking forward to receiving the final report by the company," he had asserted.

Head of Oil Industry Equipment Producing Association Reza Khiamian also reported on talks with Canadian oil equipment producers adding "in addition to the North American country, some negotiations have been held with European countries like France and Germany."

Khiamian further enumerated main axes of talks between Iranian and Canadian companies including "knowledge and technology transfer, establishment of a production line for manufacturing advanced industrial equipment as well as investment attraction."

On Monday, Director of DMC Process Project at Research Institute of Petroleum Industry (RIPI) Mansur Bazmi also reported on collaborations with a Canadian company on construction of an oil desalination plant; "Iran and Canada will both participate in the construction the facilities."

Gulf News

Is your fleet hacker-proof?

Wednesday, 27 April 2016

Byline: Stephen Brennan

Section: general

Dubai - Traffic accidents killed 675 people in the UAE last year and injured a further 6,863. The advent of driverless cars holds the promise to cut this to a fraction.
The full societal potential of the technology goes far further -- from providing a lifeline to the old, to cutting down on traffic congestion and freeing up family time.

What's vital is that government and motor industry executives take the necessary steps to ensure that driverless cars are protected from malicious hackers, learning from other industries research and experience, so that the public can profit from this transformative technology.

It's important to get things into perspective before indulging in science fiction fantasies of runaway cars causing havoc on our roads. Much of the technology already exists. For example, autopilot controls most of the routine portion of aircraft flights.

Airlines increasingly mandate computer control for extreme weather conditions, where computers can react swiftly, predictably and without panic.

Nonetheless, the autonomy and connectivity of driverless cars does leave them open to attacks from malicious cybercriminals or terrorists. The principal threats are three-fold:

First, hackers could gain control of an individual car, either to cause mischief, or at the extreme end turn it into a missile.

Second, they could use the car's systems to intrude on the privacy of individuals, by tracking their movements and access personal or otherwise sensitive data (although considering most of us carry around a smartphone this is hardly a unique threat).

Third, and potentially most damaging, hackers could use the inherent connectivity of driverless vehicles to disrupt an entire city. It's not hard to imagine thousands of cars parked motionless on Shaikh Zayed road.

It happens most rush hours, but if these fleets were being controlled to produce maximum disruption over days, this would have serious implications for emergency services and the economy of Dubai.

There are clear steps that carmakers, and their governmental regulators, can take to ensure that any risk from cyberattack is minimised. The airline industry has already led the way with its focus and enhancements on deterministic ethernet.

Carmakers need to ensure that control systems are managed in an organised and systematic manner rather than simply bolted on to the general internet connectivity of the vehicle.

It's vital to look after three 'A's of computer security: authentication, authorisation and accounting. Authentication provides a way of identifying a user with advanced cryptography. This ensures that the car's central processing unit knows exactly who or what it's receiving information from and giving commands to at all times.

Authorisation ensures that each part of the system gives appropriate commands; it's perfectly acceptable for the neighbouring car to be providing its positional data to avoid a crash; it's not for the car to cause your engine to stop.

Third, all the information needs to be accounted for. It's inevitable some accidents will happen, and it's vital that a record is kept of all events for subsequent analysis just like a plane's black box.

Cybersecurity concerns should not stop a revolution, which according to tech entrepreneur Elon Musk may be only a few years away, but security does need to be built in at a foundational level to ensure the world gains the benefits and minimises the risks.

Fars News Agency

International Bank Transfer System Hacked

Wednesday, 27 April 2016

Section: general

Tehran - Swift, the global financial network that banks use to transfer billions of dollars every day, has warned its customers it is aware of "a number of recent cyber incidents" where attackers had sent fraudulent messages over its system.
The disclosure came as law enforcement authorities in Bangladesh and elsewhere investigated the cyber theft of US$81m (£55.9m) from the Bangladesh central bank account at the New York Federal Reserve. Swift has acknowledged the scheme involved altering Swift software on Bangladesh Bank's computers to hide evidence of fraudulent transfers, Guardian reported.

Monday's statement from Swift marked the first acknowledgement that the Bangladesh Bank attack was not an isolated incident but one of several recent criminal schemes that aimed to take advantage of the global messaging platform used by some 11,000 financial institutions.

"Swift is aware of a number of recent cyber incidents in which malicious insiders or external attackers have managed to submit Swift messages from financial institutions' back offices, PCs or workstations connected to their local interface to the Swift network," the group warned customers.

The warning, which Swift issued in a confidential alert sent over its network, did not name any victims or disclose the value of any losses from the previously undisclosed attacks. Swift confirmed to Reuters the authenticity of the notice.

Swift, or the Society for Worldwide Interbank Financial Telecommunication, is a cooperative owned by 3,000 financial institutions.

Also on Monday, Swift released a security update to the software that banks use to access its network to thwart malware that security researchers with British defence contractor BAE Systems said was probably used by hackers in the Bangladesh Bank heist.

BAE's evidence suggested that hackers manipulated Swift's Alliance Access server software, which banks use to interface with Swift's messaging platform, to cover their tracks. BAE said it could not explain how the fraudulent orders were created and pushed through the system.

But Swift provided some evidence about how that happened in its note to customers, saying that in most cases the attackers obtained valid credentials for operators authorised to create and approve Swift messages, then submitted fraudulent messages by impersonating those people.

Cyber security experts said more attacks could surface as Swift banking clients look to see if their access had been compromised.

Shane Shook, a banking security consultant, said hackers were turning to Swift and other private financial messaging platforms because they could steal larger amounts. "These hacks specifically target financial institutions because smaller efforts result in much larger thefts," he said. "It's much more efficient than stealing from consumers."

Justin Harvey, chief security officer with Fidelis Cybersecurity, said hackers followed the money and would be drawn into such schemes in hopes of emulating a big heist like the one on Bangladesh Bank. "After the Bangladesh Bank heist became public, every other attacker out there is looking to see if they can do the same," he said.

Swift spokeswoman Natasha Deteran told Reuters that the commonality in these cases was that internal or external attackers compromised the banks' own environments to obtain valid operator credentials. "Customers should do their utmost to protect against this," she said in an email to Reuters.

Swift told customers that the security update must be installed by 12 May. "We have made the Alliance interface software update mandatory as it is designed to help banks identify situations in which

attackers have attempted to hide their traces - whether these actions have been executed manually or through malware," she said.

New York Times
F.B.I. Opts Not to Share iPhone-Unlocking Method
Thursday, 28 April 2016
Byline: Eric Lichtblau, Katie Benner

Washington - The F.B.I. closed the door Wednesday to the possibility of giving Apple the technical solution that the government bought to unlock the iPhone used by one of the attackers in the mass shooting in San Bernardino, Calif.
The decision leaves Apple in the dark about the technical details of how the F.B.I. -- with help from an unknown outside group that was apparently paid at least $1.3 million -- managed to bypass the company's vaunted encryption.

After two months of tense sparring over the San Bernardino iPhone, the government's decision was a clear rebuke to Apple. Its chief executive, Timothy D. Cook, has declared publicly that the company should not have to develop new software so the F.B.I. can unlock its phones. The F.B.I. on Wednesday appeared eager to return the favor by refusing to divulge how it finally broke in.

The decision upset some technology industry executives, who said it appeared to run counter to the Obama administration's promises to promote security and transparency in the nation's technology operations.

Apple declined to comment on Wednesday.

F.B.I. officials maintained that what they bought from the outside company amounted only to a tool for getting into the phone, and not a blueprint exposing the actual security flaws in the device.

As a result, F.B.I. officials decided not to send the issue on to a special White House panel that reviews the question of whether software vulnerabilities discovered by American intelligence officials should be shared with the software designer to enhance security.

That review panel could have determined that the technical fix bought by the F.B.I. should be shared with Apple.

"The F.B.I. purchased the method from an outside party so that we could unlock the San Bernardino device," said Amy S. Hess, executive assistant director for science and technology.

"We did not, however, purchase the rights to technical details about how the method functions, or the nature and extent of any vulnerability upon which the method may rely in order to operate. As a result, currently we do not have enough technical information about any vulnerability that would permit any meaningful review" by the White House examiners, she said.

Soon after the government said that a third party had successfully gotten data from the phone, after giving the F.B.I. a demonstration of its method in February, many security professionals were hopeful that the method would be made public.

"It's the position of Obama administration that security flaws should be disclosed to the parties that can fix them," said Denelle Dixon-Thayer, chief legal and business officer at Mozilla. She added that the fact that the F.B.I. did not take the necessary steps to understand how the outside group opened the phone shows that the review process over all needs to be more transparent.

The government's decision simply to hire the locksmith and ignore how that lock was opened "creates a gap in the review process" that is "not transparent and has not been set in legislation," she said.

The F.B.I.'s carefully worded statement reveals that law enforcement authorities have found a loophole in the vulnerability review process created by the administration-- hire the hacker to extract the data, but be careful to not know how he got the job done.

"The F.B.I. is intentionally exploiting a known vulnerability and enabling people to profit off of it," said Alex Rice, the chief technology officer at HackerOne, a security company in San Francisco that helps coordinate vulnerability disclosure for corporations. "The collateral damage done by this lack of transparency and the possible ongoing existence of the flaw is serious."

The government's claim that it does not have enough details to provide any information to the review process is not unusual. "Over the last 10 years as cellphones became more important to criminal investigations, law enforcement would hire digital forensics teams, would extract data for investigators without necessarily buying the capability to do it themselves," said Ben Johnson, the co- founder of the security start-up Carbon Black.

The F.B.I. decided not to send the issue to the White House to review under a classified and little- known system known as the Vulnerabilities Equities Process.

There are often "legitimate pros and cons" in deciding whether a flaw should be disclosed to the designer, a senior official said in a 2014 White House blog post -- one of the few times the review process has been publicly discussed.

Because the government relies on Internet security, wrote Michael Daniel, special assistant to the president on cybersecurity, "disclosing vulnerabilities usually makes sense. We need these systems to be secure as much as, if not more so, than anyone else."

But Mr. Daniel acknowledged that the United States government could sometimes exploit the security flaws itself if it does not disclose them.

"Disclosing a vulnerability can mean that we forgo an opportunity to collect crucial intelligence that could thwart a terrorist attack, stop the theft of our nation's intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks," he said.

Wall Street Journal
Encryption Without Tears
Thursday, 28 April 2016
Byline: Senators Richard Burr and Dianne Feinstein

Op-ed - In an increasingly digital world, strong encryption of devices is needed to prevent criminal misuse of data. But technological innovation must not mean placing individuals or companies above the law.
Over the past year the two of us have explored the challenges associated with criminal and terrorist use of encrypted communications. Two examples illustrate why the status quo is unacceptable.

The first is the Islamic State-inspired terrorist attack last year in Garland, Texas. FBI Director Jim Comey said the attackers "exchanged 109 messages with an overseas terrorist" the morning of the shooting, but the FBI cannot access those messages to determine the exact role of Islamic State in the shooting and how to help prevent future attacks.

Another case involves the murder of Brittney Mills, eight months pregnant when she was shot to death last year on her front porch in Baton Rouge, La. Her unborn son was delivered at the hospital but died a week later.

Even though police found Brittney's smartphone next to her body, the murder remains unsolved and law enforcement cannot access any information on her encrypted phone, including an electronic diary Brittney kept.

These are two of the many cases where law enforcement is unable to fully investigate terrorism or criminal activities. In fact, today the FBI is unable to gain access to data on many of the mobile devices they obtain that are password protected.

In response to these cases, we are circulating a proposal in the Senate to ensure that technology does not undermine the justice system.

The draft proposal requires a person or a company -- when served with a court order -- to provide law enforcement with information (in readable form) or appropriate technical assistance that is responsive to the judicial request. This will enable law enforcement to conduct investigations using the communications involved in criminal and terrorist activities.

Our draft bill wouldn't impose a one-size-fits-all solution on all covered entities, which include device manufacturers, software developers and electronic-communications services. The proposal doesn't define the technological solutions or tell businesses how to solve the problem. It provides compensation for reasonable costs that businesses may incur when complying with a court order.

We want to provide businesses with full discretion to decide how best to design and build systems that maintain data security while at the same time complying with court orders.

Critics in the industry suggest that providing access to encrypted data will weaken their systems. But these same companies, for business purposes, already maintain and have access to vast amounts of encrypted personal information, such as credit-card numbers, bank-account information and purchase histories.

We are not asking companies to provide law enforcement with unfettered access to encrypted data. We aren't even asking companies to tell the government how they gain access to this encrypted data. All we are doing is asking companies to find a way to keep their data secure while also cooperating with law enforcement in terrorism and criminal investigations.

President Obama said earlier this year, "You cannot take an absolutist view on this." We agree -- and believe that strong data security and compliance with the justice system don't have to be mutually exclusive. American technology companies have done some amazing things that are the envy of the world. We think that finding a way to achieve both goals simultaneously is not beyond their capabilities.

Note: Sen. Burr (R., N.C.) is the chairman, and Sen. Feinstein (D., Calif.) the vice chairman, of the Senate Select Committee on Intelligence.

Washington Post
Three TSA managers say 'bullies' punish whistleblowers
Thursday, 28 April 2016
Byline: Ashley Halsey III

Washington - The Transportation Security Administration on Wednesday was caught in a crossfire by three of its executives who said the agency's managers punish employees when they point out security lapses at the nation's airports.
"These leaders are some of the biggest bullies in government," Jay Brainard, a TSA security director in Kansas, told the House Committee on Oversight and Government Reform. "While the new administrator of TSA has made security a much-needed priority once again, make no mistake about it, we remain an agency in crisis."

As airports anticipate what may be a record crush of passengers this summer, the three men testified that morale was near rock bottom among TSA security workers.

"Many airports are complaining that TSA is getting worse, not better," said Oversight Committee Chairman Jason Chaffetz (R-Utah). He said that 103 of the TSA's 48,000 airport screeners quit each week.

"They really don't like working there," Chaffetz said. "That's a management problem there."

Chaffetz set the stage for Wednesday's hearing in a series of letters sent in February and March to TSA Administrator Peter V. Neffenger. They demanded to know all disciplinary actions taken against TSA employees, bonus payments made to TSA staff and an explanation for a policy under which workers can be forced to relocate.

Since his Senate confirmation in June 2015, Neffenger has centralized training of TSA employees in Georgia, restricted executive bonuses, ended forced relocations and taken steps to increase airport security.

Brainard told the committee that Neffenger had "done his best to get his arms around the situation, but he hasn't resolved it." He said a group of about 20 senior supervisors whom he blames for the TSA's mismanagement were "waiting [Neffenger] out."

"The refusal to address or to hold senior leaders accountable is paralyzing this agency," Mark Livingston, a program manager in the TSA's Office of the Chief Risk Officer, testified. "TSA employees are less likely to report operational security or threat- relevant issues out of fear of retaliation from supervisors who fear further retaliation from their chain of command. No one who reports issues is safe at TSA."

When he raised concerns, Livingston said, his supervisors ignored them and punished him instead.

"They reduced me two pay grades," he said. "This action was intended to publicly humiliate me. They sought to make an example of me."

The men have run afoul with their supervisors. Livingston has filed a discrimination lawsuit against the agency. Brainard and Andrew Rhoades, an assistant director in the Office of Security Operations, reportedly are under internal review by the TSA.

Rhoades said he was asked to run the names of Somali Americans with whom he met in Minneapolis through a terrorist database, a directive he considered to be racial profiling.

"The Transportation Security Administration takes seriously all allegations of inappropriate behavior by its employees at all levels and does not tolerate illegal, unethical or immoral conduct," the TSA said in a statement after the hearing. "Due to ongoing litigation and open investigations, we are unable to comment on many of the specific allegations brought up during today's hearing."

The hearing came 10 months after an inspector general's report that said his undercover operatives were able to slip through airport security with weapons and phony bombs more than 95 percent of the time. They were able to carry weapons or bomb-like material through airport-security checkpoints in 67 of 70 attempts last year.

Then- acting TSA administrator Melvin Carraway was forced from the job in June 2015 after reports of the airport-security issues became public.

"I appreciate that the TSA has taken steps to address the inspector general's concerns," Chaffetz said.

Rhoades's trouble with the TSA dates to autumn 2014, when a local TV news station began reporting on security lapses at the Minneapolis-St. Paul International Airport.

Rhoades already was on record with his supervisors for objecting to the way TSA screeners were handling confiscated weapons and a failure to put stickers on some checked bags that had been cleared by the agency. He said he played no role in the leaks.

In the aftermath of the news reports, one of Rhoades's supervisors set out to determine whether TSA employees provided information to reporters, according to an investigation by the U.S. Office of Special Counsel (OSC). Early last year, the OSC said, the same supervisor issued Rhoades a forced transfer to Florida.

The OSC stepped in to investigate whether it was a retaliatory move against a whistleblower, and the TSA later rescinded the transfer.

CBS News
Ransomware's next target: Anything that's connected
Thursday, 28 April 2016
Byline: Anne Picci

New York - "Ransomware" has turned into a lucrative business for scammers, but it could jump from a troubling annoyance to life-threatening attacks.
The hack is typically targeted at computers, with scammers encrypting files on unwitting victims' machines. They then demand a ransom - - typically about $500, payable in untraceable Bitcoin -- in exchange for a key that will decrypt the files. One new type of scam convinces consumers to download the malicious encryption software with the message "Your package has been delivered."

Already this year, the pace of ransomware attacks has quickened. Security firm Endgame noted that a dozen new variations have been identified so far, compared with about 10 for all of 2015. Security experts say the frequency and type of ransomware attacks are only going to pick up, given that hackers are profiting from it.

One think tank is predicting that the types of attacks will eventually expand to the "Internet of things," or Internet-connected devices such as cars and medical devices like pacemakers.

"Everything is connected now. It's the Internet of everything," said James Scott, senior fellow at the Institute for Critical Infrastructure Technology, which published the report on connected devices. "There are so many vulnerabilities that you can exploit."

While most people think of ransomware as targeting their computers, it has already spread to mobile phones. Last year, a version emerged called "Porn Droid" that changes an Android phone's PIN and then flashes a warning to the user that appears to come from the FBI. The warning tells the user that the phone has been locked because "suspicious files have been found" including pornography. The fee to get out of the "charges"? $500.

If a mobile phone is infected with ransomware, it's best to restore it to its factory settings, Scott noted.

When it comes to other Internet-connected devices, many "lack any form of security," according to the report.

"How much do you predict someone would pay to remove ransomware from a pacemaker?" the report asked. "The scenario is not too far-fetched; in fact, it is much more deadly. Many medical devices, such as pacemakers, insulin pumps, and other medication dispersion systems are Internet or Bluetooth enabled."

Still, the scammers face drawbacks in that it's tougher to deliver a message demanding a ransom through a pacemaker, for instance. In that case, it's likely the scammer would still use email or texting to communicate with the victim.

Scott said consumers should take several steps to avoid a ransomware or malware attack. First, back up your computer to an external hard drive, and make sure to unplug the hard drive between backups. The latter step will keep the it clear of malware or ransomware in case of an attack on the computer.

Second, maximize your privacy settings on your social media accounts, which will stop scammers (as well as anyone you don't know) from sending you texts or messages with malicious links or programs. Third, limit the personal information you disclose on sites such as Facebook (FB) or LinkedIn (LNKD).

"Guys put where they went to high school, their hobbies," Scott said. "I'm a social engineer. So, LinkedIn was the always the first place I would look when a company wanted us to penetrate their network."

Hackers can use that personal information to engineer an email campaign that looks as if it's from a company's CEO or another executive.

Browser add-ons such as self-destructing cookies and HTTPS Everywhere can help protect consumers, Scott noted. If your ISP offers antivirus or antispam services, sign up. It's also important to understand how hackers target consumers, such as through "spearphishing," which is when criminals create emails that are designed to look as though they come from a trusted source.

Consumers should also "stop filling out every form they see on the Internet," Scott added. "You don't have to put your real name in if you want to download an e-book."

London Daily Telegraph
Revealed: Britain's borders left exposed as screening system crashed twice in 48 hours
Thursday, 28 April 2016
Byline: Ben Riley Smith

London - Britain's borders were left exposed to terrorists last year after a Home Office computer system which screens passengers crashed twice in 48 hours, The Telegraph can reveal.
The eBorders system, which was put in place after the 9/11 terror attacks to protect the country from jihadists, ground to a halt in June last year.

The incident, which this newspaper has seen details of, was deemed so serious that Theresa May, the Home Secretary, was alerted by officials close to midnight.

The Home Office refused to reveal how often the system has crashed or whether there have been any outages since the incident.

Technicians worked through the night to fix the system amid fears from border officials that hundreds of extremists, convicts and illegal immigrants were arriving in the UK undetected.

The disclosure that a vital part of Britain's border security stopped working during a time of "severe" threat from terrorism will raise serious questions about whether it is fit for purpose.

Mrs May is likely to come under pressure to explain why the public were kept in the dark despite tens of thousands of people likely to be traveling into the UK at the time.

Flights were not grounded despite the system being down and border officials unable to check in advance passenger details against terrorism watch lists.

Sources familiar with the situation told the Daily Telegraph that they would normally expect to see the names of hundreds of potential suspect passengers being 'flagged' each day.

During the outages just one individual was 'flagged' suggesting others could have gone under the radar.

A Home Office spokesman said that all passengers would still have had to cross passport control after arriving in the UK.

Officials at the border have access to lists of "dangerous" people, which the Home Office insists would have been cross-checked to ensure there was no breach.

However the warnings index - which dates back to 1995 - was deemed inadequate on its own after the 9/11 attacks and was recently found to be breaking down twice a week.

But terrorists or criminals could still have boarded aircraft without being detected by British security services.

The Telegraph has launched a new Border Security campaign, which has seen former counter terrorism figures call for a review in the wake of terror attacks on the Continent.

At the heart of Britain's ability to stop dangerous people entering the country is Semaphore, a system which checks passenger data against watch lists of suspect individuals.

Every day Semaphore scans information on passengers traveling to and from Britain on planes, trains and ferries against lists of those flagged up by government agencies.

The system - unlike its predecessor - helps alert the border agencies to suspect passengers bound for the UK before they board planes.

Matches are passed to the National Border Targeting Centre (NBTC) which decides whether to stop the passenger from boarding, intercept them at passport control or let them enter the UK.

This newspaper has learnt that on Sunday, June 14, and Monday, June 15, the Sempahore system suffered two national outages after being overwhelmed by requests.

The first crash happened when a fault saw tens of thousands or error messages flood the system which froze under the pressure.

Both Mrs May and James Brokenshire, the immigration minister, were alerted shortly before midnight as technicians worked through the night, updating the government every hour.

The system appeared to stabilise before another malfunction saw hundreds of thousands of passenger details flood the system and trigger another outage on Monday night. Mrs May was notified again.

Officers at the NBTC warned that instead of seeing hundreds of matches they had received just one - meaning potential criminals and jihadists heading to Britain were not being flagged up.

Specialists worked through the night again trying to locate the source of the problem before finally stabilising the system on Wednesday.

They occurred just months after the Charlie Hebdo shooting that saw jihadists kill 11 people in Paris and while Britain's threat level was set at "severe", meaning a terrorist attack is "highly likely".

The Age
Cyber security check-up
Thursday, 28 April 2016
Byline: Georgia Wilkins

Canberra - The federal government will foot the bill for cyber security "health checks" at some of Australia's biggest companies.
The top 100 ASX-listed companies will be have the chance to get their voluntary check under the government's new $230 million cyber security package.

The government has declined to say how much it will spend on the scheme but said it hoped to eventually roll out the service to all public and private companies. It would not say whether the checks would be done by a government regulator or private consultants.

Industry experts said on Monday that large companies should have to shoulder the burden of data protection themselves.

"If the ASX100 are not competent enough to govern their own cyber security issues, those boards are not doing their jobs," said Dr Robert Merkel, a lecturer in software engineering at Monash University.

Prime Minister Malcolm Turnbull last week announced the government's cyber security strategy, which will focus on closer collaboration of government and business.

It is the result of a year-long review of the industry. The strategy will see the Australian Cyber Security Centre moved away from the Australian Security Intelligence Organisation in Canberra to allow for greater ties with business.

The government said cyber security health checks would "enable boards and senior management to better understand their cyber security status".

Ty Miller, director of security firm Threat Intelligence, said health checks were becoming popular in the industry.

"There's an increasing amount of cyber insurance being purchased, because there are so many more breaches happening these days," he said.

"When you sign up to a cyber insurance policy, you have to have a certain level of security in the organisation, and you can check that through a health check."

Associated Press
Police in dark over Haider Facebook posts
Thursday, 28 April 2016
Byline: Numan Haider

Canberra - Police say they might not have met a radicalised Melbourne teen who was shot dead after stabbing two officers if they been aware of ASIO'S concerns about his escalating Facebook posts. Numan Haider, 18, was shot in the head outside the Endeavour Hills police station after he stabbed a Victoria Police officer and an Australian Federal Police officer attached to the Joint Counter Terror Team on September 23, 2014.

Officers from ASIO, AFP and Victoria Police had met before then to share information on Haider.

Two ASIO officers told an inquest into Haider's death on Thursday that at a meeting on September 19, Haider's escalating online activity - including Facebook posts - was discussed.

They said "erratic" behaviour by Haider at Dandenong Plaza on September 18 - where the teen unfurled a flag linked to Islamic State - was also discussed.

However, three Victoria Police also giving evidence on Thursday had no memory of ASIO sharing Facebook posts with them.

They said they would have reconsidered meeting the teen had they seen the posts, which included a picture of Haider wearing a balaclava and holding the Shahada flag, with derogatory comments about ASIO and the AFP.

The first Victoria Police officer also contradicted the ASIO witnesses' recollection that the interagency meeting knew about the incident at Dandenong Plaza.

He said he had returned from leave on September 22 when he saw the report on Haider at Dandenong Plaza, and then passed it on to another Victoria Police officer to inform ASIO and AFP.

Another police officer told the inquest that during the September 19 meeting all the agencies agreed Haider was not an immediate threat and police would make contact with him.

Earlier this week a senior ASIO officer gave evidence that in the weeks before he was killed, Numan Haider had conducted internet searches for information on Tony Abbott's upcoming visits to Victoria, a military base and AFL football.

She said she would not allow ASIO officers to interview Haider again because she believed he had at least one knife.

The inquest continues before Coroner John Olle.

Xinhua News Agency
New Zealand government seeking business help in cybercrime fight
Thursday, 28 April 2016
Byline: John Macdonald

Wellington - Leading international cyber security specialists will discuss how New Zealand businesses can help fight cybercrime at the first government-backed Cyber Security Summit in Auckland next week, Communications Minister Amy Adams said Thursday.
"Cyber-attacks can and do damage our economy. Businesses are acutely aware of the 257 million NZ dollars (178.2 million U.S. dollars) lost to cybercrime last year," Adams said in a statement.

"The challenge cyber security presents can't be met by the public sector alone. What's clear is that we need a joined up response -- the private and public sectors working together to share information and expertise," she said.

"The summit is an opportunity for chairs and chief executives from across New Zealand to continue the conversation around how as a country we tackle the threat of cybercrime, and improve our resilience and security in this increasingly digital age."

International keynote speakers at the May 5 summit would include Jim Lewis from the U.S. Center for Strategic and International Studies in Washington, and Matt Thomlinson, vice president of security of Microsoft.

Times of Israel
Security breach in Israeli-made Waze lets hackers stalk users
Thursday, 28 April 2016
Byline: Stuart Winer

Jerusalem - Computer researchers in the US have demonstrated a way of breaching the globally popular Waze road navigation application that allows hackers to track users' movements or even create fake traffic jams.

Ben Zhao, professor of computer science at University of California-Santa Barbara, was along with his research team able to use the method to create thousands of "ghost cars" in Waze's system, which could then be used to monitor genuine users, the Fusion website reported Tuesday. "Anyone could be doing this [tracking of Waze users] right now," Zhao said. "It's really hard to detect."

Created in Israel in 2008 and sold to Google in 2013 for $1.1 billion, Waze provides navigation instructions to drivers that include traffic conditions and road hazards, and has an estimated 50 million users around the world.

The researchers began their hack by intercepting the transmission that Waze servers use to communicate with users. The Waze servers employ an SSL encryption to communicate with cellphones -- a security precaution intended to verify that the servers are communicating with a real phone. By diverting a cellphone running Waze and making it communicate directly with their own computers, researchers were able to reverse-engineer the coding Waze uses to communicate with users' phones.

Armed with the code, Zhao and his team wrote software that could send instructions to the Waze servers filling the system with virtual "ghost cars" which could be used to create a fake traffic jam -- or monitor real drivers located around the virtual vehicles.

As a social networking app, Waze relies on users sharing information such as location and username with other drivers to build up a picture of traffic conditions. The ghost cars were used to gather data from real users enabling tracking of their movements.

Researchers demonstrated the tracking method on one of their own team as well as on a Fusion reporter. They also created a fake traffic jam on a quiet Texas back road in the dead of night, to prove that it could be done but without interfering with users.

"You could scale up to real- time tracking of millions of users with just a handful of servers," Zhao noted. "If I wanted to, I could easily crawl all of the US in real time. I have 50-100 servers, and could get more from [Amazon Web Services] and then I could track all of the drivers."

The team, which began testing their theory in the spring of 2014, warned Waze later that year and published their findings in 2015. In January, Waze issued an update of the application which included new cloaking measures but the researchers found they were still able to track users. Nonetheless, Waze users who choose the option of going "invisible" are not vulnerable to the hack. "It's such a massive privacy problem," Zhao said.

The hack is similar to one carried out by a pair of Israeli students two years ago when they managed to create fake traffic jams, but gave researchers much more powerful options for manipulating the Waze system.

Fusion speculated that hackers could use the breach to download the activity of drivers who use the app and then make the information public, revealing who had been where and when. "We needed to get this information out there," Zhao said. "Sitting around and not telling the public and the users isn't an option. They could be tracked right now and never know it."

Zhao warned that the same method could also be used on other social networking apps, and expressed the opinion that plugging the breach would not be a simple task. "Not being able to separate a real device from a [hacking] program is a larger problem," said Zhao. "It's not cheap and it's not easy to solve."

A Waze spokesperson told Fusion that, "The company is examining the new issue raised by the researchers and will continue to take the necessary steps to protect the privacy of our users." The company is "examining the new issue raised by the researchers and will continue to take the necessary steps to protect the privacy of our users," the spokesperson added.

In 2014 Israeli students Shir Yadid and Meital Ben-Sinai from the Technion, Israel's Institute of Technology, demonstrated a method of hacking into Waze and tricking the system to show fake traffic jams. The Israeli researchers also notified Waze of the method at the time.

Naharnet Newsdesk
Lebanon's security agencies to get telecoms data
Thursday, 28 April 2016

Beirut - The cabinet held a regular session on Wednesday to address various issues and approved providing the telecommunications data to all security apparatuses while leaving the decision of giving it to the State Security in the hands of PM Tammam Salam.
"We have requested that all security apparatuses have access to the data including the State Security and Salam has assured us that this will be the case," said Education Minister Elias Bou Saab after the cabinet session.

On the H5N1 bird flu virus that was detected in poultry farms in Baalbek last week, Information Minister Ramzi Jreij said: "The government gave an initial approval to compensate the farmers whose poultry was affected by the virus."

As for the waste management file, Jreij said: "The cabinet approved the formation of a committee, chaired by the Premier, to address waste incinerators."

Ahead the meeting, Environment Minister Mohammed al-Mashnouq replied to complaints about the waste odor filling the air saying: "The odor is the result of the removal of 550 tons of accumulated trash."

The session that kicked off at the Grand Serail in a bid to tackle several pressing issues excluded the thorny file of the State Security which officials said is being followed up by Salam.

Before the session convened, Tourism Minister Michel Pharaon emphasized that "the solution for the State Security file is an administrative one."

The National (UAE)
UAE aims to be world hub for technology
Thursday, 28 April 2016

Dubai - The UAE on Wednesday launched the latest component of its strategy to become an ideas hothouse and a world-leading hub for technology.
Sheikh Mohammed bin Rashid, the Vice President and Prime Minister and Ruler of Dubai, announced ambitious plans to develop and exploit 3-D printing, a process that the consultants McKinsey estimate will have a $550 billion impact on the global economy in the next 10 years.

The new plans follow a target set this week for a quarter of journeys in Dubai to be driverless by 2030. Like 3-D printing, autonomous transport is viewed as a "disruptive" technology with worldwide implications. Companies as diverse as Google, Mercedez-Benz, Audi and the German industrial comglomerate Bosch are investing heavily in its future.

Sheikh Mohammed made it clear on Wednesday that the UAE would continue its quest to achieve global leadership in driving innovation that had benefits for all mankind.

"Our vision for development is driven by a deep understanding of future needs, and built on proactive ideas because we want to be in first place globally," he said.

"Our methodology for development is based on initiatives that can be applied anywhere in the world, creating a model not only for our economy but also for the global economy.

"The future does not wait for those who hesitate and slow down. The next stage requires us to act fast and utilise the opportunities. A few days ago we launched the Dubai Future Agenda and we have started to implement it in a way that adds value to humanity and our national economy.

"The UAE is presenting to the world today the first integrated and comprehensive strategy to exploit 3-D technology to serve humanity."

Sheikh Mohammed said the first impact of 3-D technology would be on the construction industry, and he set a target of 25 per cent of buildings in Dubai to be constructed using 3-D printing by 2030.

The technology would transform the industry by saving time, cutting construction waste and reducing the need for unskilled labour, with an estimated economic benefit of Dh3bn by 2025, Sheikh Mohammed said.

He expects the use of 3-D in construction to increase by about 2 per cent a year from 2019, depending on how the technology and its reliability develop.

Sheikh Mohammed also targeted medical and consumer products for manufacture using 3-D printing.

In the medical products sector, the focus will be on 3-D printed teeth, bones, artificial organs, medical and surgical devices and hearing aids, with a projected value of Dh1.7bn by 2025.

Consumer products made using using 3-D printing will include household items, optics, fashion jewellery, children's games and fast food, with an estimated value of Dh2.8bn by 2025.

Sheikh Mohammed has directed organisations including Dubai Municipality, Dubai Holding and Dubai Health Authority, under the umbrella of the Dubai Future Foundation, to implement the overall strategy.

They will set up the infrastructure to develop 3-D printing technology, propose a legislative framework to regulate it, find sources of funding, recruit the necessary scientific talent and determine market demand.

There will also be an international forum in Dubai for 3-D printing designers, manufacturers and developers, to discuss developments in the technology.

"The future will depend on 3-D printing technologies in all aspects of our life, starting from the houses we live in, the streets we use, the cars we drive, the clothes we wear and the food we eat," Sheikh Mohammed said,

"This technology will create added economic value and benefits worth billions of dollars. We should have a share in this growing global market."

All Africa
Pour la création d'une association algérienne de cryptographie
Wednesday, 27 April 2016
Byline: Journaliste maison

Oran, Algérie - La création d'une société savante dédiée à la cryptographie figure parmi les ambitions affichées mardi à Oran par des participants à un un premier workshop international consacré à cette spécialité scientifique portant sur le développement des techniques de protection des données informatiques.

"La réflexion est engagée en vue de la création d'une association algérienne de cryptographie", a indiqué Pr Adda Ali Pacha, président de la rencontre réunissant deux jours durant une cinquantaine de participants algériens et étrangers à l'Université des sciences et de la technologie Mohamed Boudiaf (USTO-MB).

Le regroupement de compétences nationales au sein d'une société savante a pour objectif de "répondre avec efficience aux attentes du secteur économique et industriel", a expliqué Pr Pacha, également directeur du Laboratoire de codage et de la sécurité de l'information (Lacosi).

Illustrant la contribution de la communauté universitaire en la matière, ce responsable a fait savoir que cinq projets de recherche sont actuellement menés par les équipes de son laboratoire relevant de l'USTO-MB.

Le workshop s'est ouvert en présence de la rectrice, Nacéra Benharrat qui s'est félicitée de la tenue de cet événement dans la mesure où "il met en lumière les capacités des chercheurs nationaux à apporter des solutions technologiques à même de protéger les intérêts de l'industrie et des institutions du pays".

La responsable de l'USTO-MB a en outre insisté sur la feuille de route mise en oeuvre au sein de son établissement, axée essentiellement sur "l'enrichissement des cursus pédagogiques au profit des étudiants, la diversification des parcours de formation et le développement de la recherche scientifique".

La conférence plénière de ce workshop a été donnée par le Pr René Lozi de l'Université de Nice "Sophia Antipolis" (France) qui a évoqué les étapes historiques du développement de la cryptographie avant de mettre en relief son importance aujourd'hui dans nombre de domaines comme la lutte contre le terrorisme et la lutte contre l'espionnage industriel.

La rencontre est mise à profit par les participants algériens, issus de différentes universités du pays, pour présenter les résultats de leurs travaux de recherche portant notamment sur la création de nouveaux algorithmes utiles pour le chiffrage des données.

Ce workshop est organisé avec le soutien d'organismes partenaires, à l'instar de la Direction générale de la recherche scientifique et du développement technologique (DG-RSDT) et de l'Autorité de régulation de la poste et des télécommunications (ARPT).

La Presse+
Sécurité informatique 5 millions pour une solution signée Immunio
Wednesday, 27 April 2016
Byline: Jean-François Codère

Montréal - Automatiser la sécurité des applications web, c'est le défi que s'est donné la jeune entreprise montréalaise Immunio, qui vient de conclure un nouveau cycle de financement de 5 millions US mené par White Star Capital, un fonds d'origine québécoise.
White Star rejoint le fonds britannique Hoxton Ventures, la BDC et Real Ventures au sein du capital d'Immunio, qui avait déjà fait l'objet d'un placement de 3,3 millions US depuis sa fondation, en 2013.

Immunio a été cofondée par Zaid Al Hamami et Mike Milner, qui se sont rencontrés à Montréal alors qu'ils travaillaient pour Canonical. Le premier terminait une maîtrise en administration des affaires du MIT, le deuxième avait bossé pendant une dizaine d'années pour le Centre de la sécurité des télécommunications (CST) au Canada et chez son équivalent britannique.

Les deux hommes cherchaient une façon de se lancer dans le domaine de la cybersécurité.

« C'est un marché qui a toujours été très axé sur les grandes entreprises, observe M. Al Hamami. En 2000, la seule demande venait des banques, alors les entreprises technologiques ont produit des solutions très complexes, dispendieuses, qui nécessitent des consultants. Moi, je me demandais qui étaient les entreprises qui faisaient des choses cool, qui s'adressaient vraiment aux ingénieurs parce que, ultimement, c'est eux qui décident ce qui marche ou non, et la réponse était : personne. Alors nous nous sommes lancés. »

Après deux ans de développement, Immunio a lancé sa solution récemment. Il s'agit d'un module qui s'intègre aux applications web et surveille leur sécurité en temps réel.

« On surveille constamment pour déterminer ce qui constitue une activité normale pour cette application et nous détectons ce qui n'est pas normal », résume M. Al Hamami.

L'accès à des fichiers inhabituels, un utilisateur qui se branche à partir d'une région inattendue ou une ligne de code qui envoie de drôles de requêtes à la base de données sont autant d'éléments qu'Immunio peut d'abord détecter, puis bloquer.

« On peut pointer à notre client la ligne de code exacte que les pirates ont ciblée et leur indiquer comment ils s'en servent. »

Selon Jean-François Marcoux, cofondateur de White Star Capital, Immunio dispose d'une technologie « très unique, qui rend accessible la sécurité des applications à tous les développeurs ». Son cycle de vente assez court, comparativement à des solutions plus complexes et conçues sur mesure, est aussi cité comme un avantage qui pourrait lui permettre de croître rapidement.

Immunio compte actuellement 22 employés, dont la moitié à Montréal, où elle compte embaucher « agressivement » au cours de la prochaine année.

International Business Times (UK)
Qatar National Bank: Database leak gives data on al-Jazeera journalists and British 'spies'
Thursday, 28 April 2016
Byline: Jason Murdock

London - A 1.4GB trove of internal documents, files and sensitive financial data purporting to be from the Qatar National Bank (QNB) has been leaked online.
The massive data dump appears to contain hundreds of thousands of records including customer transaction logs, personal identification numbers and credit card data. Additionally, dozens of separate folders consist of information on everything from Al Jazeera journalists to what appears to be the Al-Thani Qatar Royal Family.

However, it is a folder listed as "SPY, Intelligence" that quickly catches the eye. Upon analysis, it contains a slew of records listed as Ministry of Defence, MI6 (the UK foreign intelligence service) and Qatar's State Security Bureau, also known as "Mukhabarat".

The MI6 file, which sits alongside similar documents reportedly holding information on Polish and French intelligence, opens up an in-depth report on an alleged agent. This includes names of close relations, phone numbers, social media accounts and credit card data. Furthermore, in one instance, a file marked "wife", opens a photo showing a woman and two children.

There are roughly a dozen of these intelligence dossiers included in the Qatar data dump. However, this data is not likely to have been collated by the bank and remains unverified by IBTimes UK.

The alleged banking leak also openly lists a folder marked "Al Jazeera" that stores nearly 30 separate profiles alongside a Microsoft Excel file that holds more than 1,200 records - including national ID numbers, telephone numbers and home addresses. Much like the intelligence files, the Al Jazeera disclosure contains a number of entries labelled "SPY" and also includes images of the person alongside social accounts, banking data and passwords.

When contacted, multiple sources confirmed to IBTimes UK the data is legitimate.

On the customer-facing side, the data dump contains a number of folders that are likely to concern users. Some of the listed database spreadsheets are labelled: "Account Master", "User Profile" and "Transactions" however, much like the rest of the contents, IBTimes UK is still in the process of verifying the entire leak. It remains unknown how current the data is - and how or when it made its way into the public domain.

The massive leak was initially uploaded at Global-Files.net however was quickly removed without explanation. Then, a separate well-known whistle-blowing website mirrored the entire data dump in an easily- accessible format.

In response to questions from IBTimes UK, Maha Mubarak, QNB media relations officer said: "It is QNB Group policy not to comment on reports circulated via social media. QNB would like to take this opportunity to assure all concerned that there is no financial impact on our clients or the bank. QNB Group places the highest priority on data security and deploying the strongest measures possible to ensure the integrity of our customers' information. QNB is further investigating this matter in coordination with all concerned parties."

The same statement has since been posted online.

After analysing the data Simon Edwards, cybersecurity expert with Trend Micro, said: "The breach seems to be a classic attack on a bank, with the majority of data leaked online exposing customers' bank account details, such as account numbers, credit cards and addresses.

"There's also a lot of information on banking transactions, suggesting that the perpetrators were trying to expose specific transactions. This theory can be further strengthened by the hacker's attempts to profile the bank's customers into different categories, mostly focusing on Qatar's TV network along with other foreign agencies, some of which are categorised as 'spies'."

He added: "Interestingly, there is also additional data about mainly foreign bank account holders, which includes information such as their Facebook and LinkedIn profiles, along with 'friends' associated through those social networks. This data doesn't appear to have come directly from the bank itself, rather the perpetrator used the data held by the bank to then build up profiles of further targets."

Reuters
German nuclear plant infected with computer viruses, operator says
Thursday, 28 April 2016
Byline: Staff report

Frankfurt - A nuclear power plant in Germany has been found to be infected with computer viruses, but they appear not to have posed a threat to the facility's operations because it is isolated from the Internet, the station's operator said on Tuesday.
The Gundremmingen plant, located about 120 km (75 miles) northwest of Munich, is run by the German utility RWE.

The viruses, which include "W32.Ramnit" and "Conficker", were discovered at Gundremmingen's B unit in a computer system retrofitted in 2008 with data visualization software associated with equipment for moving nuclear fuel rods, RWE said.

Malware was also found on 18 removable data drives, mainly USB sticks, in office computers maintained separately from the plant's operating systems. RWE said it had increased cyber-security measures as a result.

W32.Ramnit is designed to steal files from infected computers and targets Microsoft Windows software, according to the security firm Symantec. First discovered in 2010, it is distributed through data sticks, among other methods, and is intended to give an attacker remote control over a system when it is connected to the Internet.

Conficker has infected millions of Windows computers worldwide since it first came to light in 2008. It is able to spread through networks and by copying itself onto removable data drives, Symantec said.

RWE has informed Germany's Federal Office for Information Security (BSI), which is working with IT specialists at the group to look into the incident.

The BSI was not immediately available for comment.

Mikko Hypponen, chief research officer for Finland-based F-Secure, said that infections of critical infrastructure were surprisingly common, but that they were generally not dangerous unless the plant had been targeted specifically.

The most common viruses spread without much awareness of where they are, he said.

As an example, Hypponen said he had recently spoken to a European aircraft maker that said it cleans the cockpits of its planes every week of malware designed for Android phones. The malware spread to the planes only because factory employees were charging their phones with the USB port in the cockpit.

Because the plane runs a different operating system, nothing would befall it. But it would pass the virus on to other devices that plugged into the charger.

In 2013, a computer virus attacked a turbine control system at a U.S. power company after a technician inserted an infected USB computer drive into the network, keeping a plant off line for three weeks.

After Japan's Fukushima nuclear disaster five years ago, concern in Germany over the safety of nuclear power triggered a decision by the government to speed up the shutdown of nuclear plants. Tuesday was the 30th anniversary of the Chernobyl nuclear disaster.

Financial Times
Germany replaces head of external intelligence agency
Thursday, 28 April 2016
Byline: : Stefan Wagstyl

Berlin - The German government replaced the head of the country's external intelligence service on Wednesday after a barrage of criticism over the part it played in helping the US spy on European targets.

The Bundesnachrichtendienst (BND) has been in the public spotlight since 2013 leaks by Edward Snowden, a former US government contractor, that alleged that the US had tapped.the telephone of Angela Merkel, Germany's chancellor, for more than a decade.

Last year, German media reported that the BND had assisted the US National Security Agency to spy on European targets such as the French presidency, the European Commission and Airbus, the aerospace group.

The government's decision to replace 63-year-old Gerhard Schindler, who is retiring early as head of the BND on July 1, is an apparent attempt to draw a line under the affair.

But Ms Merkel's critics warned that the BND's conservative new chief -- Bruno Kahl, a 53-year-old official with close ties to Wolfgang Schäuble, Germany's finance minister -- might be more inclined to protect the service from outside scrutiny than to improve external political oversight.

Hans-Christian Ströbele, security spokesman for the opposition Green party, said that the nomination of a Schäuble confidant meant that "the hardliners" had won and opponents of intelligence service reform could succeed in blocking real change.

But Patrick Sensburg, a spokesman for Ms Merkel's ruling CDU, said the BND needed "a new start", depicting Mr Kahl as somebody who could see the agency's looming "reform process ... through to the end".

Mr Schindler, BND boss since 2012, had taken office promising "more fun, more risk" -- meaning that the agency had to engage more in security hotspots such as the Middle East.

In the event, his time was dominated by the revelations of Mr Snowden who disclosed widespread global electronic surveillance by the NSA, sometimes with the co- operation of its allies, notably the UK and, at times, Germany.

Germany is particularly sensitive to state-sponsored spying, due to its Nazi and communist East German past.

According to Spiegel magazine, the NSA provided the BND with information -- such as email addresses -- for tracking. Spiegel said that in 2013 the BND deleted 12,000 such pieces of information -- including some email addresses with the domain suffix .de, suggesting they were German-based.

The issue is highly sensitive since the BND is banned from operating within Germany -- the job of the Bundesamt für Verfassungsschutz (BfV), the country's domestic intelligence agency, which works under tighter laws.

Intelligence co-operation between Germany and the US, including information exchange, was intensified under a 2002 pact, forged amid growing concerns over Islamist terrorism.

However, the suggestion that targets unconnected with suspected terrorism had been spied on prompted an outcry, with opposition Green politicians leading the charge.

Ms Merkel's chancellery responded by saying it had asked the BND for explanations and "identified technical and organisational deficiencies in the BND".

Ms Merkel resisted opposition pressure for detailed clarifications, for stronger parliamentary supervision of the service, and for resignations, including Mr Schindler's.

The government instead tightened the chancellery's control of the service, instituted reforms in the BND, and prepared a new law, due to be presented to the Bundestag later this year, on clarifying the BND's legal responsibilities.

Mr Kahl comes to the BND with long government and political experience, much of it gained with Mr Schäuble.

Mr Schäuble specialised in security issues before he was finance minister and served as interior minister in 2005-9, when he recruited Mr Kahl for a succession of senior posts, including running his office.

The Intercept
Snowden Debates CNN's Fareed Zakaria on Encryption
Tuesday, 26 April 2016
Byline: Jenna McLaughlin

Washington - NSA whistleblower and privacy advocate Edward Snowden took part in his first public debate on encryption on Tuesday night, facing off against CNN's Fareed Zakaria, a journalist and author known for his coverage of international affairs.
Zakaria, in New York, defended the government's right to access any and all encrypted messages and devices as long as there's court approval. Snowden, speaking over a live video-link from Moscow, argued the security of the Internet is more important than the convenience of law enforcement. The debate was organized by NYU's Wagner School of Public Service and the Century Foundation.

Though Zakaria started off firm in his conviction that law enforcement should be able to get hold of all digital messages with court approval, he gradually conceded that it may not be that simple. Zakaria said he himself doesn't actively encrypt any of his communications, assuming everything will be fine -- though Snowden pointed out that, since he has an iPhone, some of his data and communications are encrypted by default.

Zakaria opened the debate by posing a hypothetical: Bank of America creates an "iVault" allowing anyone to store all their financial data totally encrypted. An embezzler could take advantage of that service to hide the evidence of their misdeeds, foiling investigators. "I understand within a democracy, you have to sacrifice liberty for democracy at some point. You cannot have an absolute zone of privacy," he said.

Snowden agreed with Zakaria that absolute zones of privacy don't exist, and that encryption does pose real problems for law enforcement. But he disagreed that universal access is the best way to solve the problem. "For the government to unlock everything there has to be a key to everything. Every other person in the world can find that key and use it too," he said. "It's a fundamental problem of science."

Instead, he suggested, police should take advantage of the many other options available to them. He cited the investigation into the founder of Silk Road, an anonymous, encrypted platform for black market drug sales. In that case, a team of investigators caught the mastermind at the library after he typed in his password.

"Encryption is not an unbreakable wall," Snowden said. "Or if it is, it is one we can get around, if we are patient, if we are careful, if we think and plan how to go about our investigations."

By the end of the debate, Zakaria said he did not support the legislation proposed by Sens. Richard Burr, R-N.C., and Dianne Feinstein, D-Calif., which would mandate companies to immediately decrypt all communications when asked by a court. The bill has been heavily criticized by technologists.

And Zakaria acknowledged that if it was genuinely impossible for a company to decrypt communications, then the court should accept that -- though it would be a "hard case."

"If WhatsApp says we literally do not know how to write this code -- WhatsApp could demonstrate to a court that they don't have to do it," Zakaria said.

He concluded by encouraging greater clarity about what kind of communications the government can and cannot access -- before the next disastrous terrorist attack. "We do face real threats out there. There are people out there trying to do bad things. Once they happen, the government will be given carte blanche," he said.

Snowden noted that former security officials now proclaiming the value of unbreakable encryption -- including former NSA Director Michael Hayden -- had considered those questions carefully and had fallen on the side of computer security.

Jerusalem Post
Are US, Israel winning or losing newest cyber battles
Thursday, 28 April 2016

Byline: Yonah Jeremy Bob

Jerusalem - Keeping track of the cyber battles between the US and Israel and their cyber adversaries is dizzying and constantly changing.
The US is certainly upgrading its cyber capabilities to undermine groups such as ISIS. The New York Times reported on Sunday that the US Department of Defense's Cyber Command unit is mounting an offensive against ISIS to block it from spreading its message, recruiting members, paying fighters and from exercising command and control functions such as issuing instructions online.

As part of its "cyber bomb," the US has placed implants within ISIS's networks so it can mimic their behaviors and orders, and make slight changes to redirect ISIS fighters in a way that leaves them exposed to ground or drone assaults.

These are the practical measures the US has shied away from using until now because of legal issues and the possibility of a boomerang effect. For example, there are also reports that the US came close to paralyzing Syria's air force a few years ago to hamper its barrel bombing of civilian populations, but held off because it could cause diplomatic complications with third countries.

Yet ISIS is adversary unlike any seen before; its ruthlessness has invited innovative ideas about how it can be defeated. In mid-April, Pentagon officials told the US Congress that it is developing cyber and other electronic weapons to attack enemy missile systems prior to launch. Such weapons act as a counterpunch to adversaries trying to overwhelm US defense systems with a volley of missiles.

The potential of these cyber offensive actions is awesome in their breadth, but they are really part of a defensive strategy. They have evolved to counter the possibility of a missile defense system being overwhelmed by sheer volume. Attack rockets cost less than defensive missiles, but only if the US can produce them en masse to avoid a costly arms race.

But on the flip side, the US, after sufferings years of cyber attacks from Chinese hackers (despite a pledge by President Xi Jinping to stamp out such activity) has not found any solutions. US President Barack Obama appears willing to keep his head down on the issue as he nears the end of his term.

The bilateral pledge between the US and China, agreed to in September, calls for an end to cyber hacking, especially commercial hacking. Obama pushed for the initiative since 2013.

Despite the pledge, V.-Adm. James D. Syring, chief of the US Missile Defense Agency, last week reiterated that China is still trying to hack into US missile defenses, even after the US has flagged this and other violations of the deal. Besides negotiations, the US embarrassed Beijing by indicting five senior Chinese officials for cyber spying in the summer of 2014 and considered offensive cyber retaliation by counter-hacking and publicly revealing Chinese secrets. Hacking could go as far as breaking down China's great firewall for censorship, opening China's citizenry to unguarded and unmonitored Internet access, along with spilling Chinese state secrets.

But Obama's truce, despite past Chinese transgressions as well as US weakness in the face of current breaches, shows that the US president believes avoiding conflict is more important than the payoff of enforcing the pact. Like the US, Israel has some impressive offensive cyber weapons. The Jerusalem Post reported in June 2015 that IDF Brig.-Gen. (res.) Pinchas Barel Buchris, a former head of Unit 8200, said that it has the ability to hack into Hezbollah's highly advanced computerized rockets to prevent their launch. This capability could save Israel from an arms race involving iron dome missiles versus rockets from Hezbollah and Hamas, much like the case with the US.

On March 31 the Institute for National Security Studies published a 81-page report with recommendations for Israeli cyber policy. In terms of using cyber offensives, the report recommended a multi-pronged approach, including integrating them with attacks by conventional armed forces, disrupting the enemy's communications system, using private sector proxies (as Israeli adversaries do), and utilizing restrained attacks to send deterrent messages.

Last week, the Post's Yaakov Lappin reported that the IDF's unit for information technology security held its first-ever cyber war drill. The drill was based on accumulated experience about what to expect from recent cyber attacks on the IDF's systems. But with all of these offensive and defensive innovations, Israel has recently admitted that a number of cyber hacks have been embarrassingly successful in targeting the country's most sensitive systems.

The first hack carried less severe operational consequences. In January, The Intercept magazine revealed that between 2008 and 2012, the US and British intelligence services hacked into Israeli drones and aircraft such as the F-16 fighter, in order to monitor their activity under a classified program code-named "Anarchist."

It was revealed that the UK's intelligence services, known as the Governments Communication Headquarters, which works in conjunction with the US National Security Agency, systematically surveyed Israeli drones from Cyprus.

The purpose was to collect information on military operations in Gaza, especially during 2008-9's Operation Cast Lead, monitor the possibility of Israeli strikes on Iran and tap into drone technology the Jewish state was exporting globally.

The UK and US intelligence services collected snapshot images from the Israeli drones, as well as data that mapped the paths taken by the unmanned aircraft.

Israel's arch enemies carried out the second hack, making it far more serious. On March 23, Islamic Jihad master hacker Maagad Ben Juwad Oydeh was indicted in the Beersheba District Court for grave cyber hacking crimes against Israel from 2011 to 2014. The announcement shockingly revealed that the Palestinian had hacked repeatedly into the IDF's drones hovering over Gaza enabling him to view the drones' video feed.

An indictment filed by the Southern District Attorney's Office also charged Oydeh with hacking into the police, transportation authority and Ben-Gurion Airport's video cameras, enabling the terrorist group to study the location of civilians and IDF personnel in real-time as fired rockets during past conflicts.

Also, in mid-March, former New York mayor and current cyber security guru Rudolph Giuliani told the Post that there are many cutting-edge cyber defense technologies that governments are not using and he is not sure why - although he did not list them, for security reasons.

Public relations for Israel's cyber strength could stress that the breaches were from 2014 or earlier and that Giuliani's criticism was vague.

And none of the defensive vulnerabilities detract from the US and Israel's cyber offensive prowess.

If anything, the latest developments simply stress that whoever is on the cyber offensive almost always has a serious advantage and that all sides of a cyber conflict are unlikely to avoid getting cyber-bloodied.

Toronto Star
Canada's spies in spat over privacy breach reporting
Sunday, 01 May 2016
Byline: Alex Boutilier

Ottawa - Canada's electronic spies are concerned reporting too many details about serious privacy breaches could reveal too much about the agency's highly secretive surveillance and cyber-defence activities, the Star has learned.
The Communications Security Establishment has been in a yearlong spat with privacy commissioner Daniel Therrien's office over reporting "material" privacy breaches.

The spy agency's reluctance comes despite government-wide regulations requiring all serious privacy breaches - - those that potentially could cause serious harm to an individual, or involving a large number of Canadians -- to be disclosed to the independent watchdog.

"As with all (government) departments and agencies, CSE is required to report material privacy breaches to the Office of the Privacy Commissioner," CSE spokesman Ryan Foreman wrote in a statement.

"However, we do continue to discuss the most effective manner to report material privacy breaches when they occur in the operational space, in a matter that safeguards the sensitive nature of information related to CSE's mandated activities."

Documents obtained by the Star show that "discussion" has been going on since at least January of last year.

In a letter sent to a senior Treasury Board employee, released under access to information law, Therrien took aim at a proposal to provide only limited information to his office about privacy violations at CSE.

"A report that does not state the number of breaches does not give the Office of the Privacy Commissioner enough information to have a clear discussion with the institution in question," Therrien wrote. "The expertise of the Office of the Privacy Commissioner can not, therefore, be put to use."

A change in Treasury Board policy under the previous Conservative government requires all federal departments and agencies to report "material" privacy breaches to the commissioner and the Treasury Board.

As the single largest repository of Canada's top secret information, CSE certainly handles sensitive information. The agency is a member of the Five Eyes alliance, a group of closely aligned security and intelligence agencies in the U.K., U.S., Australia and New Zealand.

The alliance was shaken by revelations from whistleblower Edward Snowden in 2013, who pulled back the curtain on those countries' mass surveillance capabilities and tools. In the wake of those disclosures,

the normally press-adverse CSE has been more open about its mandate and the steps it takes to protect Canadians' privacy.

Since 2007, CSE has kept a single database for all privacy violations, from the mundane to the serious. Every year, a small team at the CSE commissioner's office, an arm's-length review body, reviews privacy violations self-reported by the agency.

William Galbraith, a spokesman for CSE commissioner Jean-Pierre Plouffe, said that his office has been in discussions with Treasury Board and Therrien about CSE's privacy breach reporting.

Galbraith said the 12-person office already examines privacy infractions, and it's important to avoid "duplication" in reviewing CSE's activities.

"The CSE commissioner has spoken with the privacy commissioner on this issue, recognizing that (Therrien's) mandate covers all government departments and receives reports for breaches, and also noting that (Plouffe's) mandate is specific to CSE and includes examination of compliance with the law including the Charter and the Privacy Act," Galbraith wrote in a statement.

But Therrien's letter noted that while the CSE commissioner reviews the legality of CSE's actions, the expertise to investigate privacy breaches is housed in the privacy commissioner's office. Therrien is not an outsider on these questions, having served as a senior Department of Justice lawyer responsible for intelligence and law enforcement agencies.

Plouffe reported earlier this year that CSE illegally, if inadvertently, transmitted Canadian metadata to a Five Eyes partner. The mistake, which CSE says did not identify any specific Canadians, was reported by the agency to the commissioner, not uncovered by Plouffe's team themselves.

Documents tabled in Parliament earlier this month show that reporting serious privacy breaches has varied widely between government departments.

Treasury Board President Scott Brison, who is responsible for enforcing the government-wide reporting, vowed in an interview with iPolitics that Ottawa will do better on reporting the infractions.

"It's an area that we will work with the (privacy commissioner's) office and with departments and agencies to understand fully what we can do to improve results and we're seized with (the issue)," Brison told the outlet.

The details about what each side is proposing in the debate between CSE and Therrien's office remain secret. Details only emerged through multiple documents, obtained by the Star over the course of several months, from Treasury Board, CSE and the privacy commissioner's office.

In statements to the Star, all three organizations said they continue to discuss the matter and hope for a resolution in the near future.

Dutch News
Secret service can hack innocent people to reach target: Volkskrant
Saturday, 30 April 2016

Amsterdam - The new law giving greater powers to the secret service to intercept internet traffic will allow officials to hack innocent people despite protests by privacy groups, the Volkskrant said on Friday. The paper bases its claim on the new draft legislation, which has not yet been officially published.

The new powers mean that people who share the same server as suspects could be hacked by the spy service to get access to their targets.

Ministers say this is crucial because suspects are often well protected against hacking. The new powers will apply only to the security service, not the police, the Volkskrant said. Privacy groups have already warned that this will create 'unacceptable risks to privacy'.

'Someone who is completely innocent can suddenly find the secret service accessing their data,' Ton Siedsma of Bits of Freedom told the Volkskrant. This could include their phones, tablets, smart watches, fridges and even cars, the paper said. Ministers say that the security services will have to have permission from a special commission before they can access non-suspects internet traffic.

New York Times
Hackers' $81 Million Sneak Attack on World Banking
Sunday, 01 May 2016
Byline: Michael Corkery

Washington - Tens of millions of dollars siphoned from the Federal Reserve Bank of New York. A shadowy set of casinos in the Philippines. A large bank in Bangladesh with creaky technology. An unknown -- and perhaps uncatchable -- group of anonymous thieves with sophisticated hacking skills. What unites this curious cast of characters and enabled one of the most brazen digital bank heists ever is a ubiquitous and highly trusted international bank messaging system called Swift.

Swift -- the Society for Worldwide Interbank Financial Telecommunication -- is billed as a supersecure system that banks use to authorize payments from one account to another. "The Rolls-Royce of payments networks," one financial analyst said.

But last week, for the first time since hackers captured $81 million from Bangladesh's central bank in February, Swift acknowledged that the thieves have tried to carry out similar heists at other banks on its network by sneaking into the beating heart of the global banking system.

"There are many banks out there right now saying, 'There but for the grace of God go us,'" said Gareth Lodge, a payments analyst at Celent, a financial consulting firm.

The admission that the attack was not a one-time event in a developing country but perhaps part of a broader threat has thrust Swift into a spotlight, raising questions about how securely money is being moved around the world. Some financial security experts point out the Swift system is only as safe as its weakest link.

The attack also reflects a growing sophistication among digital criminals, who for years have been breaching personal bank accounts and stealing credit card credentials. The thieves in Bangladesh may have spent months lurking inside the central bank's computers, studying how to steal the necessary credentials to gain access to Swift.

It is the digital version of the heist depicted in the movie "Ocean's Eleven," said Adrian Nish, head of the cyberthreat intelligence team at BAE Systems, a defense and security company.

"The trend is moving from opportunistic crime to Hollywood-scale attacks," said Mr. Nish, whose firm has analyzed the malware believed to have been used in the Bangladesh breach.

In the United States, most banks take special precautions with their Swift computers, building multiple firewalls to isolate the system from the bank's other networks and keeping the machines physically isolated in a separate locked room.

But elsewhere, some banks take far fewer precautions. And security experts who have analyzed the Swift breach said they had concluded that the Bangladesh bank may have been particularly vulnerable to an attack.

"Swift is a great organization," said Chris Larsen, the founder of Ripple, a financial technology company that aims to speed up global money transmissions. "But the system is fractured and antiquated. The way it is set up, you cannot totally isolate problems in a place like Bangladesh from the whole network."

In some ways, Swift is a testament to how technology has helped all countries -- including poorer ones -- gain access to the financial system. But that broader access has a downside.

The central bank in Bangladesh, by some accounts, employed fewer protections against cyberattacks than many other large banks. The bank, for example, used $10 routers and no firewalls, according to news reports.

The server software that the Bangladesh bank employed was a Swift product called Alliance Access, which connects banks to the central messaging system. In a sign of how seriously Swift regards the breach of Alliance Access, the group issued a "mandatory software update" last week to help its members identify possible irregularities.

"These hackers figured out this was a weak point on the periphery, and they went for it," said Jeffrey Kutler, editor in chief at the Global Association of Risk Professionals, a trade group. "But they were not able to compromise the core."

Swift's core is built on technology that has been evolving for decades. What began in 1973 as a relatively small network of 240 banks in Europe and North America is now a sprawling network of 11,000 users that includes both banks and large corporations. At first, Swift could be used to authorize payments across national borders. But it is now also used to transmit messages related to domestic payments, securities settlements and other transactions.

Swift's growth in recent years -- it set a record for messages in March -- reflects the increasingly global and interconnected nature of finance. But it also shows the risk of so many financial instructions running through a single system made up of a patchwork of banks and companies with varying levels of online protection.

Each bank on the Swift network is identified by a set of codes. And it was the codes assigned to the Bank of Bangladesh that were recognized -- correctly -- by the Federal Reserve Bank of New York when it transferred $81 million of the Bangladesh bank's money to the Philippines, not knowing that someone, somewhere, had stolen the credentials of the Bangladesh bank and installed malware to cover his or her tracks.

Initially, the thieves requested the transfer of $951 million into a handful of bank accounts in Sri Lanka and the Philippines -- a number that prompted the New York Fed to ask the Bangladesh bank to reconfirm that it indeed wanted to move the money.

In the end, the Fed processed only five of the 35 fraudulent payment requests, after it could not reconfirm with officials in Bangladesh.

The hackers seemed to time the attack perfectly: When officials from the Fed tried to reach out to Bangladesh, it was a weekend there and no one was working. By the time central bankers in Bangladesh discovered the fraud, it was the weekend in New York and the Fed offices were closed.

To conceal the crime, the malware disabled a printer in the Bangladesh bank to prevent officials from reviewing a log of the fraudulent transfers.

The money was transferred to accounts in the Philippines and then into the Philippine casino system, which is exempt from many of the country's anti-money-laundering requirements.

The New York Fed has been criticized for letting the $81 million slip out. Representative Carolyn B. Maloney, a New York Democrat and member of the Financial Services Committee, has called for an investigation, warning that the breach "threatens to undermine the confidence that foreign central banks have in the Federal Reserve, and in the safety and soundness of international monetary transactions."

The New York Fed said in a statement that "there is no evidence that any Fed systems were compromised" and that the transfer of the money had been "fully authenticated" by Swift.

Swift, which prides itself on its secrecy and low public profile, also put out a statement about the attacks. But its executives declined to speak on the record about the episodes, which are still under investigation. The group's chairman, Yawar Shah, who is a senior executive at Citigroup, also declined to comment.

In its statement, Swift emphasized that the hackers had been able to breach only some of the banks that communicate over Swift, not the network itself.

"The commonality in what we have seen is that (internal or external) attackers have successfully compromised banks' own environments," Swift said.

Even if officials at the Bangladesh bank had employed the highest of security measures, the thieves displayed a level of skill, cunning and determination that may have been able to penetrate a far more secure system.

"If you have an attacker who really wants to get in and knows there is a big prize," Mr. Nish said, "keeping them out over the long term is really difficult."

The Mirror UK
ISIS hackers threaten to leak 'British secret intelligence' obtained from Ministry of Defence
Sunday, 01 May 2016
Byline: Jonathan Sharman

London - The hacking group made the claim in a hit-list document listing the identities of US Predator and Reaper drone operators, sparking fears of a version featuring UK personnel.
Islamic State hackers have threatened to leak "secret intelligence" they claim to have obtained from a mole at the Ministry of Defence, and say they are slowly "infiltrating" the UK and America.

A group calling itself the Islamic State Hacking Division made the claim in an anti-drone warfare document that purported to make public the identities, addresses and other details of US Predator and Reaper drone operators.

The terrorists used the hit-list document to suborn the murder of drone teams it dubbed "cowards".

But the the details of US military personnel appeared to have been scraped from publicly-accessible sources like Facebook, rather than obtained through a hack or leak, the Sunday Times reported.

Several British ISIS terrorists, including the murderer Mohammed Emwazi, known as Jihadi John, have been killed in drone strikes.

The hacker group said in the hit-list it circulated on Twitter: "In our next leak we may even disclose secret intelligence the Islamic State has just received from a source the brothers in the UK have spent some time acquiring from the Ministry of Defence in London as we slowly and secretly infiltrate England and the USA online and off."

The Ministry of Defence said: "We do not comment on alleged leaked documents."

It comes just days after a splinter group of the ISHD, the Caliphate Cyber Army, published a hit list including the names and home addresses of 3,000 ordinary New Yorkers and encouraged others to target them.

RAF air strikes have killed nearly 1,000 ISIS terrorists in Iraq and Syria since September 2014, the MoD said this week.

The campaign has intensified in recent months, with Typhoon and Tornado fighter jets attacking infrastructure targets such as oilfields and bomb factories as well as mortar and sniper positions.

The Advertiser
Nuclear-powered subs a 'no-brainer'
Sunday, 01 May 2016
Byline: Daniel Wills

Canberra - Australia's future submarine fleet could be transitioned to include a potent mix of both intelligence gathering diesel boats and rapid, fast-moving nuclear-powered vessels once the state develops a sophisticated atomic industry based around storage, Business SA says.
The Federal Government is facing calls from across the strategic policy and business communities, as well as from an outspoken SA Senator, to strongly consider the nuclear option.

SA rejoiced this week in the expectation of thousands of new jobs as the Federal Government selected French naval giant DCNS to build 12 new conventional diesel-powered subs in Port Adelaide, which are charged with defending the nation's waters for a generation.

Premier Jay Weatherill visited DCNS's Cherbourg shipyard on Friday Adelaide time, just hours after SA was chosen as the likely site of a low-level nuclear waste dump, and as former governor Kevin Scare puts the finishing touches on a Royal Commission due for release within days.

Business SA chief executive Nigel McBride, who joined the Cherbourg tour to observe the construction of a nuclear Barracuda sub that will become the template for Australia's diesel fleet, said there was strong national defence reasons for having a mix of the two. Diesel subs are prized for their ability to become completely silent when powered down, while nuclear vessels are much faster and do not need to resurface for fuel and battery charging.

Australian Strategic Policy institute senior analyst Mark Thomson said it was a "no-brainer" to go with nuclear subs if politics allowed it, and Family First Senator Bob Day claimed national security will be put at risk if the state fails to go for a more potent and tested design.

Mr McBride said storage was a "starting point" in a discussion about other applications. The first future sub is set to hit the water in the early 2030s, about the time when the state could have a storage industry up and running if it moved to do so immediately.

"We walked around a facility today which had a significant nuclear threat," Mr McBride said.

"Nobody even blinked. We walked around and took it for granted that it would be professionally contained.

"A lot will change over the next decade or so. I think right now that is a conversation that is very difficult to have or even raise. But, yes, logically given that investment you would think it would be valuable to have half conventional submarines and then half nuclear submarines." Senator Day said there was "no escaping" the strategic need for nuclear subs. "Australia's defence needs are best served by six conventional diesel-powered subs and six nuclear-powered, but not nuclear armed, subs," he said.

"The winning DCNS bid links SA with a French nation with nuclear subs and nuclear power. This opens up great opportunities for SA to learn how to embrace all facets of the nuclear fuel cycle." Australian law currently bars the use of nuclear subs.

Speaking in Cherbourg, Mr Weatherill said defence use of nuclear technology was not under consideration by the Royal Commission and "not something we are contemplating at the moment".

"We have a Nuclear Fuel Cycle Royal Commission which is considering elements of the fuel cycle, but that doesn't extent into defence." He has previously said it would take about two decades to build up such a technical capacity, which would require community backing and significant technical investment.

New York Times
The House Votes Unanimously to Strengthen Email Privacy
Saturday, 30 April 2016

Editorial: In a rare and remarkable display of bipartisanship, the House voted unanimously this week to strengthen a 30-year-old privacy law that governs how and when law enforcement agencies can obtain access to emails, photographs and other documents that people store online. If enacted, the changes will ensure that the law protects digital information as well as it does physical documents.
The bill will require law enforcement agencies to obtain search warrants from judges to gain access to personal messages and files stored on the servers of companies like Google, Yahoo and Dropbox. The legislation would substantially revise a 1986 law, the Electronic Communications Privacy Act, that allows agencies to get emails older than 180 days and other digital files by issuing subpoenas to technology companies without going to a judge.

This sensible update reflects how people store information today. And some courts have already recognized the principle that emails and files kept in the cloud should receive the same protection under the law as documents left in filing cabinets and closets. In 2010, the United States Court of Appeals for the Sixth Circuit ruled that the government must obtain warrants before searching emails stored online. But that ruling was not appealed to the Supreme Court, so it did not establish national precedent.

The bill is not perfect. When it was introduced, it required law enforcement agencies to notify people that their digital data had been obtained through a warrant. That provision was removed before the House voted on the bill because of law enforcement opposition. Technology companies, however, will be allowed to notify their customers about warrants.

Law enforcement agencies will be able to ask judges to temporarily forbid such notification if it would hurt investigations or cause other problems, but they will not be able to prevent disclosure indefinitely, as under current law. Microsoft filed a lawsuit earlier this month against the Justice Department arguing that the existing nondisclosure provision violates the Constitution.

The Obama administration has not taken a position on the House bill but has previously said it supports updating the 1986 law. In the Senate, Mike Lee, Republican of Utah, and Patrick Leahy, Democrat of Vermont, have sponsored a similar bill and won bipartisan support from 24 other senators.

But the proposals for reform could face opposition from key senators. The chairman of the Judiciary Committee, Chuck Grassley, Republican of Iowa, has not said whether he will schedule a vote. He seems concerned that changing current law could hurt the government's ability to get data it needs for criminal and civil investigations.

His fears are misplaced. Judges rarely turn down governmental requests for warrants. And civil enforcement agencies that cannot seek warrants, like the Securities and Exchange Commission, can still issue subpoenas directly to the people and businesses they are investigating.

Senator Mitch McConnell, the majority leader, ought to heed the resounding vote in the House and bring the legislation up for a vote.

Motherboard Blog
GCHQ Has Disclosed Over 20 Vulnerabilities This Year, Including Ones in iOS
Saturday, 30 April 2016
Byline: Joseph Cox
Section: Analysis

Analysis: Earlier this week, it emerged that a section of Government Communications Headquarters (GCHQ), the UK's signal intelligence agency, had disclosed a serious vulnerability in Firefox to Mozilla. Now, GCHQ has said it helped fix nearly two dozen individual vulnerabilities in the past few months, including in highly popular pieces of software like iOS.
"So far in 2016 GCHQ/CESG has disclosed more than 20 vulnerabilities across a number of software products," a GCHQ spokesperson told Motherboard in an email. CESG, or the National Technical Authority for Information Assurance, is the information security wing of GCHQ.

Those issues include a kernel vulnerability in OS X El Captain v10.11.4, the latest version, that would allow arbitrary code execution, and two in iOS 9.3, one of which would have done largely the same thing, and the other could have let an application launch a denial of service attack.

The spokesperson also pointed to two vulnerabilities in Squid, a caching proxy which can improve web response times. Recently, GCHQ intervened in the rollout of smart gas and electricity metres, which were planned to use a signal encryption key.

"We are not always credited by vendors for bugs that we disclose. We ask companies for credit in bulletins that they may publish, but recognise that this is not always possible," a GCHQ spokesperson said.

In a speech last year, the Director of GCHQ Robert Hannigan said: "GCHQ has disclosed vulnerabilities in every major mobile and desktop platform, including the big names that underpin British business."

However, governments sometimes withhold details of vulnerabilities from affected companies because the security holes can be used for hacking operations instead. Motherboard's question of whether the recent selection of vulnerabilities were only disclosed after they had already been exploited by the offensive arm of GCHQ went unanswered.

Sunday Times (UK)
Isis hackers publish hitlist of drone pilots

Sunday, 01 May 2016
Byline: Dipesh Gadher

London - ISIS hackers with links to Britain have published a "hitlist" of dozens of American military personnel purportedly involved in drone strikes against terrorists in Syria and Iraq.
A group calling itself the "Islamic State Hacking Division" yesterday circulated online the names, home addresses and photographs of more than 70 US staff, including women. It urged supporters: "Kill them wherever they are, knock on their doors and behead them, stab them, shoot them in the face or bomb them."

The group also claimed that it might have a mole in Britain's Ministry of Defence and threatened to publish "secret intelligence" in the future that could identify RAF drone operators. The claim could not be verified.

The Isis hacking division was previously led by Junaid Hussain, a former computer hacker from Birmingham who was killed by a US drone strike in Syria last August after he was discovered to be orchestrating attacks against the West. His wife, Sally Jones, a Muslim convert from Kent, is still believed to be involved in the organisation, which in the past has urged "lone wolf" attacks against RAF bases in the UK.

Inquiries made by The Sunday Times yesterday suggested that the names on the American hitlist are genuine.

However, the information published by Isis does not appear to be the result of a leak or genuine hack. Instead, the group seems to have painstakingly gleaned the names of Reaper and Predator drone operators from news articles and military newsletters, before matching them to addresses, photos and other personal details from publicly available sources on the internet.

Some of the information appears to have been taken from social media sites, including Facebook and LinkedIn.

Among those named on the list are Lieutenant-General Sean MacFarland, the US commander leading the coalition against Isis in Syria and Iraq.

His identity and role are already in the public domain.

Coalition drone strikes have been highly effective in killing senior figures within Isis in recent months and putting the terrorist group on the back foot in its self-declared "caliphate" in the Middle East.

At least five British Isis fighters, including Hussain, 21, and Mohammed Emwazi, 27, the murderer from London known as Jihadi John, have been killed by such strikes.

The US drone programme is mainly run from bases in Nevada and New Mexico.

The new hitlist features the Isis flag above the heading: "Target -- United States Military". The document, circulated via Twitter and posted on the JustPaste website, states: "You crusaders that can only attack the soldiers of the Islamic State with joysticks and consoles, die in your rage!

"Your military has no courage, neither has your president as he still refuses to send troops. So instead you press buttons thousands of miles away in your feeble attempt to fight us. A nation of cowards that holds no bravery as you resort to sending your remotecontrolled unmanned Reaper and Predator drones to attack us from the skies. So this is for you, America."

The group claimed that it had "acquired" information "to expose the location of your drone personnel".

It continued: "These 75 crusaders are posted as targets for our brothers and sisters in America and worldwide to hunt down and kill."

The group also warned: "In our next leak we may even disclose secret intelligence the Islamic State has just received from a source the brothers in the UK have spent some time acquiring from the Ministry of Defence in London as we slowly and secretly infiltrate England and the USA online and off."

After mini-biographies of each of the targeted US personnel, an apparent disclaimer states: "A few of the addresses may not be current due to the databases being outdated."

At the bottom of the Isis document is an image of the Statue of Liberty with its head cut off.

Jones, 46, a former member of a female punk rock band who now calls herself Umm Hussain, has used the same image for her Twitter profile picture.

Jones followed Hussain to Syria in 2013 after meeting him online. She travelled with Jojo, her 10-year-old son from a previous relationship.

Last October the American government listed Jones as a "specially designated global terrorist" after she urged an undercover reporter to plot an attack on the Queen at VJ-Day commemorations in London.

Using an alternative name for Isis, Major Adrian Rankine- Galloway, a Pentagon spokesman, said: "We are aware that Isil and other terrorist organisations have periodically purported to release personal information on US service members and military members of our coalition partners involved in operations against Isil.

"We take proactive measures to protect our service members and their families and keep them apprised of changes to the security situation," he added. "We will not comment on the authenticity of the information in question, and this will have no effect on operations against Isil."

The MoD said: "We do not comment on alleged leaked documents."

Toronto Star
Public still in the dark after tax deadline error
Saturday, 30 April 2016
Byline: Vanessa Lu

Toronto - The Canada Revenue Agency (CRA) gave us an extra five days to file our returns last year, but it is keeping details about the reason under wraps. Last year, on April 24 the CRA told tax preparers the deadline was May 5. Then it told us to ignore the message, insisting the deadline would remain April 30, the usual filing date.
Then the CRA reversed course, giving Canadians until May 5, promising no extra interest or penalties.

It blamed the goof on "human error," without further explanation. "The CRA takes full responsibility for the error and our first priority is to ensure that no Canadian is negatively affected," the agency said at the time. Immediately after the deadline was extended, the Star filed two separate requests for information under the Access to Information Act.

One asked for details of the mistake, how it was made and discovered. The other asked for financial implications of lost revenue related to the extension.

Now nearly a year later, the information hasn't been released - even though the agency indicated it would need up to a 90-day extension beyond the 30-day statutory limit, back in June 2015.

When contacted about the delay last week, an official in the access to information division said the agency was close to completing the request on lost revenues, likely within two weeks, but that the other one would take longer.

When pushed to explain why almost a year has passed on this request, Dianne Piercey said: "It's not unusual for a file to be so late."

Sue Brennan, also of the access to information division, followed up with another phone call, apologizing for the delay. She said the Star's request is not unique. Other files that are even older are still waiting for response.

CRA spokeswoman Jelica Zdero said in an email that timely information disclosure is in the public interest and a priority for the CRA, but it also must protect privacy and confidential information of taxpayers.

"The CRA received over 6,000 access to information and privacy requests last year and processes approximately two million responsive pages annually, the second highest volume across the Government of Canada," she said.

"Many of these requests involve documents containing personal or third-party information," Zdero said.

"The people or organizations to whom this information pertains must be consulted on whether the information requires protection from disclosure according to the exemptions under the Access to Information Act. "

Last year's deadline extension was the second time in a row that taxpayers got five extra days to fill out their returns.

In 2014, the CRA had to shut down its website to all electronic filing for five days, after determining someone had hacked into the service and accessed social insurance numbers.

This was at the time news broke that the Heartbleed Bug, a flaw in widely used encryption software, could leave online password and sensitive personal information exposed.

Online giants such as Google, Facebook and Yahoo had to scramble to deal with the threat.

A London, Ont., man has been charged in the case. Stephen Arthuro Solis-Reyes, 21, faces numerous charges including unauthorized use of a computer and mischief in relation to data.

The RCMP later laid new charges against Solis-Reyes related to other hacking including computers at Western University, the London District Catholic School Board and an email service Jersey Mail.

A spokeswoman for the Ontario Superior Court in Ottawa said a pretrial hearing in the Solis-Reyes case was scheduled for Friday.

London Times
Queen bans drones over estate amid terror fears
Monday, 02 May 2016
Byline: Staff report

London - The Queen has banned drones from being flown without permission over her Sandringham estate in an apparent move to prevent terrorist attacks and protect the privacy of the royal family. The ban covers all 20,000 acres of the estate in north Norfolk, making it potentially the largest single area in the UK to ban unmanned aircraft.

It comes amid fears that remotecontrolled drones could carry a bomb or chemical weapon. The ban will also help to foil paparazzi using drones to take aerial photographs.

Last December the Department for Transport made it a criminal offence for low-flying aircraft, including drones, to be flown within 1.5 miles of the Duke and Duchess of Cambridge's home at Anmer Hall on the estate. A similar ban is in place within 1.5 miles of Sandringham House from every December to the end of February when the Queen and other members of the royal family are often in residence.

The restrictions are similar to the drone bans around military bases, nuclear power stations and airports. Anyone breaking the restrictions faces a fine of up to £5,000.

A spokesman for the Civil Aviation Authority said that it was unclear how the ban could be enforced over the entire estate, because landowners did not automatically control the airspace over their land.

The spokesman said: "Nobody owns the air under UK law."

A Buckingham Palace spokeswoman refused to comment.

Wall Street Journal
Social Sites Slow Terror Fight
Monday, 02 May 2016
Byline: Multiple reporters

Washington - European counterterrorism officials say American laws and corporate policies are hampering their efforts to prevent a next attack, because legal procedures for getting international evidence from U.S.-based social-media firms are dangerously outdated.
European police officials who face a lengthy process to get communications data from companies such as Facebook, Twitter, YouTube and WhatsApp want to make American technology firms more responsive to overseas requests.

Even emergency requests for basic customer data -- which often don't require a legal and diplomatic review -- can cause friction between social media firms and European investigators, officials on both sides of the Atlantic say.

An online posting days after the Paris attacks in November made clear how acute those tensions are. In it, a suspected Islamic State supporter boasted that a similar attack would occur the following Sunday in Brussels, people familiar with the incident said.

When Belgian police sought to find out who was behind the account, the unidentified U.S. company in question decided it would provide the subscriber data only if the company could notify the suspect of the search and give him the contact information of the police official involved.

Belgian officials resisted that demand, fearing it could compromise the investigation and potentially endanger the police official, according to officials familiar with the discussions. The fight became tense enough that the U.S. Justice Department had to weigh in. That led to what one official called "a long discussion" that ultimately persuaded the company to give the Belgians the information.

On Nov. 21, just over a week after the Paris killings, Belgium raised its security alert to the highest level and warned of an imminent threat, closing the subway system and schools and canceling events. Belgian officials wouldn't say whether the online posting influenced the four-day lockdown.

With domestic investigations, American companies are required to cooperate with U.S. court orders to comply with such requests. But in many cases, U.S. law forbids companies to provide intercepted communications to foreign officials, unless it is through a diplomatic review process. People on all sides agree any real change for European access would have to come by changing U.S. law.

In the wake of the Paris and Brussels attacks, "people are pretty quick to point to the intelligence failures between France and Belgium, but in fact there's a very good chance there was information they couldn't get," said Terry Cunningham, president of the International Association of Chiefs of Police, which has pressed Congress on the issue. Other officials say leads in European terror cases can languish for as much as a year.

Even when European police believe suspects are plotting an attack on European soil, they can't get access to the suspects' real-time Internet conversations on American-owned social-media sites. Under U.S. law, authorities can't conduct a legally valid intercept of communications if the suspected activity doesn't involve American interests.

In other words, if a terror plot doesn't potentially threaten Americans in some way, European officials can't get legal authority to monitor the suspects' communications on an American social-media site.

Some industry executives worry that privacy would be eroded if technology firms had to start recognizing the authority of foreign courts and judges making cross-border demands for data. Microsoft's top lawyer, Brad Smith, has long argued firms should follow the legal process of the country in which the data is stored -- in the case of many American social-media firms, the U. S. -- not the legal process of whatever country is demanding data.

Still, many U.S. Internet companies agree there is a problem. They say their options are limited under current law.

A spokeswoman for Facebook, which also owns WhatsApp, said the legal process for international evidence requests can be "slow and cumbersome," adding that the firm is "actively pushing the U.S. and other governments for reforms."

Meanwhile, she said Facebook has "well-developed processes" for responding to international law-enforcement requests, including those that don't require a monthslong diplomatic review process. Emergency requests get priority, she added, and the company is often able to respond within hours or, if necessary, even minutes.

"Our legal and safety teams worked around the clock to respond to law-enforcement requests following the recent terrorist attacks," she said.

A spokeswoman for Google, which owns YouTube, said it responds to valid legal requests for user data from abroad "when they are consistent with the laws of the requesting country and the U.S., our policies, and international norms," a position echoed by Twitter.

Beyond legal restrictions, officials at social-media companies say other factors can complicate such requests. Some foreign requests may fall short of generally accepted legal practices in the U.S., they say, and sometimes foreign investigators and the officials at the firms don't have much of an everyday working relationship to smooth the process. But European officials say American Internet companies could be doing more, such as providing basic customer details in emergency situations.

Koen Geens, Belgium's justice minister, said the problem needs to be urgently addressed. "The level of cooperation strongly differs from provider to provider, but generally it is largely unsatisfactory and it endangers investigations and, by consequence, people's security," he said.

Many complaints focus on a diplomatic tool called Mutual Legal Assistance Treaties, which guide the exchange of evidence in criminal matters between the U.S. and other countries. Because of legal and bureaucratic steps, it can take nearly a year to obtain evidence through the process. By the time the search is approved, officials said, the key data has often been deleted because many U.S. companies retain it for a limited period.

American police agencies are engaged in their own struggle with Silicon Valley over issues of privacy and security, but the hurdles are higher for Europeans, officials said. The use of encryption, for example, increasingly means that an in-country wiretap may be useless because the only unencrypted version of a conversation between European suspects may reside in a computer server on U.S. soil.

Even with a law change, though, agreements would likely have to be negotiated with numerous countries. The Justice Department recently struck a deal to speed up the process for the U.K., but that change still requires congressional approval.

BBC News
Craig Wright revealed as Bitcoin creator Satoshi Nakamoto
Monday, 02 May 2016
Byline: Staff report

London - Australian entrepreneur Craig Wright has publicly identified himself as Bitcoin creator Satoshi Nakamoto.
His admission ends years of speculation about who came up with the original ideas underlying the digital cash system.

Mr Wright has provided technical proof to back up his claim using coins known to be owned by Bitcoin's creator.

Prominent members of the Bitcoin community and its core development team have also confirmed Mr Wright's claim.

Mr Wright has revealed his identity to three media organisations - the BBC, the Economist and GQ.

At the meeting with the BBC, Mr Wright digitally signed messages using cryptographic keys created during the early days of Bitcoin's development. The keys are inextricably linked to blocks of bitcoins known to have been created or "mined" by Satoshi Nakamoto.

"These are the blocks used to send 10 bitcoins to Hal Finney in January [2009] as the first bitcoin transaction," said Mr Wright during his demonstration.

Renowned cryptographer Hal Finney was one of the engineers who helped turn Mr Wright's ideas into the Bitcoin protocol, he said.

"I was the main part of it, but other people helped me," he said.

Mr Wright said he planned to release information that would allow others to cryptographically verify that he is Satoshi Nakamoto.

Soon after Mr Wright went public, Gavin Andresen, chief scientist at the Bitcoin Foundation, published a blog backing his claim.

"I believe Craig Steven Wright is the person who invented Bitcoin," he wrote.

Jon Matonis, an economist and one of the founding directors of the Bitcoin Foundation, said he was convinced that Mr Wright was who he claimed to be.

"During the London proof sessions, I had the opportunity to review the relevant data along three distinct lines: cryptographic, social, and technical," he said.

"It is my firm belief that Craig Wright satisfies all three categories."

Not everyone has been convinced by Mr Wright's claims and technical proofs. In its article about Mr Wright, The Economist said "important questions remain" about whether he was Satoshi Nakamoto.

In addition, many people involved in bitcoin have taken to social media to express their doubts and have called for further proof.

How Bitcoin works

Bitcoin is often referred to as a new kind of currency.

But it may be best to think of its units being virtual tokens rather than physical coins or notes.

However, like all currencies its value is determined by how much people are willing to exchange it for.

To process Bitcoin transactions, a procedure called "mining" must take place, which involves a computer solving a difficult mathematical problem with a 64-digit solution.

For each problem solved, one block of Bitcoins is processed. In addition the miner is rewarded with new Bitcoins.

This provides an incentive for people to provide computer processing power to solve the problems.

To compensate for the growing power of computer chips, the difficulty of the puzzles is adjusted to ensure a steady stream of new Bitcoins are produced each day.

There are currently about 15 million Bitcoins in existence.

To receive a Bitcoin, a user must have a Bitcoin address - a string of 27-34 letters and numbers - which acts as a kind of virtual post-box to and from which the Bitcoins are sent.

Since there is no registry of these addresses, people can use them to protect their anonymity when making a transaction.

These addresses are in turn stored in Bitcoin wallets, which are used to manage savings.

They operate like privately run bank accounts - with the proviso that if the data is lost, so are the Bitcoins owned.

The Hill
Snowden: Without encryption, everything stops
Monday, 02 May 2016

Byline: Rebecca Savransky

Washington - Edward Snowden defended the importance of encryption, calling it the "backbone of computer security."
"Encryption saves lives. Encryption protects property," the former National Security Agency (NSA) contractor said during a debate with CNN's Fareed Zakaria that aired Sunday.

"Without it, our economy stops. Our government stops. Everything stops."

Snowden, who previously leaked documents revealing the extent of the NSA's surveillance program, said we are in the midst of the "greatest crisis in computer security in history."

He said computer security bumped terrorism out of the top spot on our list of national security threats.

"Our intelligence agencies say computer security is a bigger problem than terrorism, than crime, than anything else," he said.

He called encryption a "field of mathematics."

"No matter how much we might hope otherwise, math is math. It works the same for Mother Teresa as it does for Osama bin Laden," he said.

"Lawful access to any device or communication cannot be provided to anybody without fatally compromising the security of everybody."

He also added that for the government to unlock everything, there has to be a key to everything.

"We can pass a law to require a key under every doormat in order to make things easier for police, but the problem is that every other person in the world can find that key, too, and they can use it," he said.

Former NSA Director Michael Hayden said America is more secure and safer with "unbreakable end to end encryption," Snowden said.

I can promise you ... one thing: If I am standing shoulder to shoulder with the director of the National Security Agency on something," Snowden said, "there's a damn good reason for that."

Saudi Gazette
60 million cyber-attacks against Saudi public sector annually
Monday, 02 May 2016
Byline: Maryam Al-Sughayar

Riyadh - Security expert and information security researcher Muhammad Amin revealed the number of cyber-attacks targeting the Kingdom last year was 60 million, a figure that made Saudi Arabia the most attacked country in the Middle East.
He attributed the high number of cyber- attacks to the Kingdom's status and distinct role in the region in the political, financial and security arenas.

"It is a country that is rich in oil and gas and it has potentials that criminals and other countries seek to take advantage of. All these factors make the Kingdom a target of these attacks, which is deemed the most prominent contemporary security problem," he said.

Amin added that the government sectors recorded the most number of hacking attempts with oil, gas, financial and telecommunications sectors ranking among the most affected.

Among the most vulnerable industries, Amin said the Saline Water Conversion Corporation (SWCC) and oil and gas installations are most likely to be targeted by hackers as they use industrial equipment that is remotely managed by the Internet. Of the most prominent hacking attacks in the world were those against Saudi Aramco.

He further said with all equipment being connected to the Internet, especially smart cities, there is a dire need to focus on how to protect them from being hijacked by hackers.

As for the hacking of banks, he said most hackers target customers' bank accounts but some also target automated teller machines (ATMs) and point of sales machines. More serious attacks against financial institutions, like the hacking of over 100 banks worldwide, cause the greatest financial losses. Such attacks are complicated and are carried out by criminal groups that use sophisticated methods, like transferring money from banks and changing the names of account owners.

Amin stressed the importance of protecting the Kingdom's institutions from cyber attacks and said a clear strategy that utilizes the latest technology is needed.

"Awareness is necessary for the user so they can ensure the safety of devices connected to the Internet. One should be aware about such crimes especially since terrorists benefit from illicit money stolen in cyber attacks," he added.

Pakistan Dawn
Govt requests to Facebook for user data rise sharply
Monday, 02 May 2016
Byline: Tauseef Razi Mallick

Karachi - The government made 471 requests to Facebook for data related to 706 accounts/users in the latter half of last year, marking a two-fold increase in the number of requests made to the social networking site during the first six months of 2015.
The details were given in a bi- annual transparency report, "Global Government Requests Report", issued by Facebook recently.

Between January and June of 2015, 192 such requests were made for data related to 275 users/ accounts, meaning that there was a 145 per cent jump in the number of requests made by the government to the social media giant during the second half of the year.

The website said: "Based on legal requests from the Pakistan Telecom Authority, Facebook restricted access to six items that were alleged to violate local laws prohibiting blasphemy."

Of the 471 requests made between July and December 2015, Facebook cooperated and provided information in 66.45pc of the cases.

Speaking to Dawn, founder and director of Digital Rights Foundation Nighat Daad said: "Not only is there an alarming increase in the number of data requests made by the Pakistan government, but the instances when Facebook obliged the requests are also increasing."

Ms Daad, however, questioned the legal process adopted by both parties in the transfer of private data. "All this is happening without any judicial oversight," she said.

She went on to say that Facebook still held the right to accept or deny any request for data, but once the proposed Cyber Crime Bill was passed, the website would be bound by law to provide data on each request made to it.

"The rise in complaints also shows how rigorously the government wants to control the internet," she pointed out.

The sole responsibility of data privacy didn't lie with the government but also with the international companies which otherwise preached freedom of expression, she said.

According to Facebook, the recently released report provided information about the number of government requests it received for data, and the number of items restricted for violating local laws.

The Facebook administration mentioned an overall global increase in government requests for user data and content restrictions pursuant to local law.

"Government requests for account data rose by 13pc, from 41,214 requests to 46,763. The number of items restricted for violating local law increased over the first half of 2015, to 55,827 items, up from 20,568," said the report.

Facebook said it only "responds to valid requests relating to criminal cases".

The social network added that each request received from a government was checked for legal sufficiency and was rejected unless it required greater specificity on requests which were overly broad or vague.

Jakarta Post
15,000 radical sites created to recruit new followers: BNPT
Monday, 02 May 2016
Byline: Suherdjoko

Jakarta - The National Counterterrorism Agency (BNPT) has warned of the growing efforts by radical movements to spread their views through social media.
The agency's deputy director for terrorism prevention, protection and deradicalization Maj. Gen. Abdul Rahman Kadir said the number of radical sites amounted to around 15,000.

"One of the radical groups whose existence has become more alarming is the Islamic State [IS]. As a new global terrorist power, the IS is striving to recruit young people as its members," said Rahman.

Several recent terrorism cases showed that the terror perpetrators were aged between 20 and 30 years, he added.

Rahman said recent terrorist incidents included those in Paris, Brussels, Lahore and the bomb and gun attack on Jl.Thamrin, Central Jakarta, in January.

The Thamrin attack was perpetrated by young people and it was terrorist propaganda spread by radical groups via the cyber world that had influenced those young people to commit the crimes.

"Many radical sites have used Islam to mask their crimes as their content contradicts Islamic values. The radical movements now have a new pattern; they are getting smarter to benefit from information technology," said Rahman.

The counterterrorism official was speaking at the opening of a dialogue entitled "Preventing the spread of radical and terrorist views and IS influence" held at the Military Area Command (Kodam) IV/Diponegoro in Semarang, Central Java, recently.

The BNPT's terrorism prevention director Brig. Gen. Hamidin said the radical sites had created terrorists who were radicalized via the internet. "They can learn how to create a home-made bomb or other terrorist actions on the internet," he said.

Hamidin further explained that the internet had revealed new groups other than the 21 radical groups known to have affiliated with IS.

Ansor Youth Movement (GP Ansor), the youth wing of Indonesia's biggest Islamic organization Nahdlatul Ulama (NU), says it has built up the Ansor Cyber Army (ACA) to fight against radicalism and terrorism in the cyber world.

"We are preparing ACA to attack the campaigns of radical groups in social media," GP Ansor chairman Yaqut Cholil Qoumas said.

He said cyber technology allowed all issues to develop on social media. Unfortunately, radical groups such as IS often used this technology as a propaganda and campaign tool.

That was why GP Ansor had instructed all elements of Ansor and Barisan Ansor Serbaguna (Banser), the NU youth wing, to fight against the radical groups' propaganda, which threatened the unity of the Republic of Indonesia, via the cyber world, Qoumas said.

"We, the Ansor members, have always been willing to fight against radical groups both in the written and cyber world," he asserted.

Qoumas explained the radical groups had continued to boost their campaigns. Citing an example, the Ansor leader mentioned the installing of banners and other attributes emblazoned with messages that called for the establishment of the Khilafah Islamiyah (Islamic Empire), which occurred in areas of NU support. "They're conducting a huge campaign; thus, we have to fight it on an equally big scale," said Qoumas.

Gulf News
Qatar National Bank says client accounts safe despite breach
Monday, 02 May 2016
Byline: Staff Report

Doha - Qatar National Bank, the Middle East's largest lender by assets, said it had taken immediate steps to ensure customers would not suffer any financial loss after a security breach last week exposed personal data of thousands of clients.
"We are taking every measure to protect the privacy of our customers and have engaged an external third party expert to review all our systems to ensure no vulnerabilities exist," the bank said in a statement on Sunday.

"All our customers' accounts are secure," it added, although it was not clear how the bank planned to protect accounts whose details, including customer names and passwords, have already been published.

The 1.5GB trove of leaked documents posted online last week included the bank details, telephone numbers and dates of birth of several journalists for satellite broadcaster Al-Jazeera, supposed members of the ruling al-Thani family and government and defence officials.

Some files had pictures of account holders from Facebook and LinkedIn, a potentially sensitive issue in a conservative country where privacy is valued.

The bank said the breach was an attack on its reputation, rather than specifically targeted at the customers, and only involved a portion of Qatar based customers. The statement did not mention the identity of the hackers.

QNB said some of the data released may be accurate but much of it was constructed and "contains a mixture of information from the attack as well as other non-QNB sources, such as personal data from social media channels." A copy of the leaked content seen by Reuters contained transaction data of QNB customers that showed overseas remittance data from as recently as September 2015.

One file had information on what appeared to be 465,437 QNB accounts, although only a fraction of these accounts had anything resembling full account details.

Several known Qatari figures in the government and media whose names appeared on the list confirmed to Reuters that their account details were accurate.

Middle Eastern banks are attractive targets for cyber criminals because of the high levels of wealth in the oil-rich region. Qatar is the wealthiest country in the world on a per capita basis, according to the World Bank.

Gulf News
Cyber warriors needed to protect online security in UAE
Monday, 02 May 2016
Byline: Samihah Zaman

Abu Dhabi - Although the UAE's online security frameworks are very robust, the threat of hacking cannot be ignored as the country strives to become a leading knowledge economy, a top information technology official said in the capital on Sunday.
"The UAE is working to implement smart government portals for the benefit of its residents, and introduce more and more services online. But these portals and their connected networks must be kept safe and reliable from the attacks of ever smarter hackers and online thieves," said Abdul Aziz Al Madhloum, head of training at federal cyber security regulator, the National Electronic Security Authority (Nesa).

"We need a generation of cyber warriors who can stay a step ahead of online criminals, and this is why we need to interest and inform our youth of cybersecurity measures," he added.

To ensure this, the Nesa organised in the capital its annual three-day cybersecurity competition, Cyber Quest, which pits teams of ethical hackers against one another. Through this, participants are taught about the importance of ethical hacking, and how it can help reveal the vulnerabilities of online and computer systems so that they can be resolved.

A total of 60 schoolchildren from public and private institutions across the UAE participated in this third edition of Cyber Quest. The youngest of them was a Grade 7 student. The participants worked in teams of two to crack up to 40 challenges using their knowledge of forensics, programming and scripts in order to hack into networks and servers.

As reported by Gulf News last November (2015), more than two million residents were victims of cybercrime in 2014-2015, losing Dh4.9 billion between them.

"Despite the threats posed by online criminals, every passing year, we note that children are becoming even more knowledgeable about the security threats facing us online. And we want to hone that knowledge and help these cyber enthusiasts develop into savvy online security experts," Al Madhloum said.

"I believe people are still careless about their online security and don't take simple measures. For myself, I use a 25-character long password. And I hope to one day become a cyber security expert," said Yousuf Awad, a Canadian participant from Dubai's Greenwood International School. Awad won the first prize at Cyber Quest along with his Emirati classmate, Mohammad Hamad.

"The best thing is that we were taught how to think like online attackers. So we can use this knowledge to defend ourselves," Hamad, who also wants to pursue a career in cybersecurity, added.

Over the next two days, the Nesa will continue to organise trial competitions for interested pupils, and also offer training activities focussing on automobile cyber-attacks, counterfeit detection, forensics and cryptography.

Fars News Agency
Rouhani Lauds Iran's Development of Advanced Technologies
Monday, 02 May 2016

Tehran - Iranian President Hassan Rouhani thanked experts and scientists for developing hi-tech in the country, and urged that Iran should become a knowledge-based economy.

"Some time in the past, we received advanced technologies from other countries, but today we enjoy hi-tech and can interact with other countries to further enhance these technologies," Rouhani said, addressing a ceremony on the occasion of the International Labors Day in Tehran on Sunday.

Voicing pleasure that the Iranian economic enterprises are now competing with their rivals at the international level, he said, "If we want to increase our income and wealth and improve the workers' situations, we should move towards a knowledge- based economy."

Iran is among the few world countries such as the US, Japan and Germany that have access to a number of hi-tech, including in nuclear, stem cell and aerospace technologies.

The country has taken wide strides in science and technology, particularly in medical and medicinal fields, in recent years.

In relevant remarks last year, Iran's Vice- President for Science and Technology Sorena Sattari underscored the necessity for paying special attention to the development of knowledge-based economy in Iran.

"Today we should move toward changing the old approach towards research, a kind of approach which has been created based on reliance on oil revenues and has influenced research environment of the country," Sattari said.

Changing the old habits needs firm determination for moving toward innovation by Iranian enterprises because reliance on mere oil revenues in research and technology has led to creation of luxury but inefficient infrastructures in the country and that is why we should leave behind a kind of culture which is based on dependence on oil economy, the official added.

He said expertise and skilled human resources make up the back bone of knowledge-based economy, adding today the country faces a big and exceptional opportunity to move toward materialization of knowledge- based economy and distance itself from oil-dependent economy.

Globe and Mail
Brazilian judge orders WhatsApp shutdown
Tuesday, 03 May 2016
Byline: Stephanie Nolen

A Brazilian judge has once again ordered the shutdown of the mobile messaging service WhatsApp, which is wildly popular in the country and used by more than 100 million people.
The order to the country's five telecommunications companies to suspend WhatsApp for 72 hours was issued by a lower court judge in Sergipe state in the northeast. The judge wants the company to share messages related to a case against drug traffickers with the federal police, something the company says it cannot do.

The telecom operators took the service offline; they faced a fine equivalent to $180,000 a day if they failed to comply, according to the newspaper Folha de Sao Paulo.

The suspension is an inconvenience for Brazilians, who rely on the service to share information between families, from schools and with their doctors; WhatsApp is the most-used app in the country. The court order is also symbolic of the immense power of even lower court judges in Brazil, a feature of the legal system, which has had considerable political importance in recent months.

Judge Marcel Montalvao had Diego Dzodan, Facebook's vicepresident for Latin America, arrested in March over failure to comply with a subpoena apparently related to the same case. Mr. Dzodan was held in custody for 24 hours until the arrest order was overturned in an appeals court.

Last December, WhatsApp was ordered offline for 48 hours by a lower court judge in Sao Paulo state, who wanted to compel the company to share information relevant to an unrelated criminal case. The service was restored after 13 hours.

The Sergipe case appears to hinge on the issue of end-to- end encryption, which WhatsApp recently began to offer - a security feature that means, the company says, that only the person who sends and the person who receives have access to what is in the text, audio, picture or video images transmitted through the service. So, says Facebook, which owns WhatsApp, it can't give the court the information the police want - it doesn't have access to it.

In February, yet another judge tried to suspend the service to compel the company to co-operate in a separate case, but that decision was appealed and struck down before the suspension took effect.

Judges have immense power in Brazil. This has been brought into vivid relief in the political upheaval that has gripped the country in recent months. In March, Sergio Moro, a federal court judge, released audio recordings of the current and former presidents' phone calls as part of a corruption investigation.

That same week, President Dilma Rousseff appointed the former president, Luiz Inacio Lula da Silva, to her cabinet, but he hasn't been able to take up the job because a series of lower courts issued injunctions to stop him.

Many Brazilians disgusted by the corruption scandal engulfing the political class have celebrated the actions of the judiciary, but the WhatsApp shutdowns illustrate how the broad scope of legal purview means a single judge can dramatically influence the course of national events.

An estimated 91 per cent of Brazilian mobile users countrywide use WhatsApp, and the shutdown order presents a conundrum for the telecom companies, who have made clear they don't like the service. The company has headquarters in California and doesn't pay taxes here, but it's sucking away the data and calling traffic that generates revenue for the mobile operators.

Bare-bones WhatsApp consumes minimal data, which makes it extremely popular with Brazilians, who face some of the highest mobile package tariffs in the world. The main competitor messaging service, Telegram, reported that it signed up more than a million new users in the hours after the suspension was announced - but while 5.7 million signed up during the December shutdown, very few stuck with the service, migrating en masse back to the familiar interface of WhatsApp as soon as the ban was lifted.

Motherboard
What Happens When Canadian Cops Find a Software Security Flaw?
Tuesday, 03 May 2016
Byline: Matthew Braga

When law enforcement and intelligence agencies in Canada discover flaws in computer software--say, a bug that could help hackers steal messages from a smartphone, or spy on unsuspecting victims via internet- connected webcams--do they disclose those holes to the software's creator so they can be plugged?
Or do they keep such flaws secret for their own use in future investigations, with the hope that no one else will find and use them maliciously first?

These types of weak spots, if left unpatched, can pose a very real security risk to users. But unlike counterparts in the US, the Canadian government has never gone on the record about how it handles the disclosure of newly discovered software bugs.

Often referred to as zero day vulnerabilities, such flaws are valuable to spies and police because their existence is not widely known, not even to the companies themselves. Thus, they can be used to gain access to computer networks, smartphones, or other electronic devices again and again, until the vulnerability is discovered, or disclosed and patched.

By keeping knowledge of such bugs secret--not only to consumers, but to the software's creator--critics have argued that the government is compromising the privacy and security of users so that it can build an arsenal of secret bugs for use in future digital attacks. The longer zero-day bugs remain unpatched, the more likely it is that criminals or other governments can discover and exploit them. Some zero day exploits, such as the ones used in the Stuxnet attack on a uranium enrichment facility in Iran, can go undetected for years.

In the United States, there is a policy called the Vulnerabilities Equities Process, or VEP. First introduced in 2010, it determines how and when the US government discloses information about flaws it discovers--or purchases--to the industry at large.

The VEP is supposed to weigh this trade-off between national security and user security by evaluating the implications of whether a bug is disclosed. In Canada, however, there is no publicly available documentation that suggests whether or not a similar process exists.

"I'm not aware of one," said Imran Ahmad, a lawyer at Cassels Brock in Toronto who works with clients on issues related to cybersecurity, privacy and data breaches. "To my knowledge, there's no formal process by which law enforcement regularly communicates with software manufacturers to flag vulnerabilities that they've come across in their own testing, to the extent that there's testing going on."

In an email, the RCMP would not answer questions related to its policy for disclosing software vulnerabilities, nor whether police purchase, discover or use software exploits as part of its investigations. "We generally do not comment on specific investigative methods, tools and techniques outside of court," wrote Sgt. Julie Gagnon.

Ryan Foreman, spokesperson for the Canadian government's cyberspy agency Communications Security Establishment (CSE), wrote in an email that CSE shares "cyber threat information" with government stakeholders that "may originate from CSE's own analysis," but did not not specifically address software exploits, nor whether a policy comparable to the VEP exists.

The VEP isn't perfect. In 2014, The The New York Times reported that the NSA typically reports bugs to software companies--unless those bugs can be used for "a clear national security or law enforcement need." Then, last November, the NSA wrote on its website that it had released "more than 91 percent of vulnerabilities discovered in products" but did not specify when the disclosures were made, nor how long those vulnerabilities had been exploited before being disclosed, if they were exploited at all.

Recent court battles, such as the fight between Apple and the FBI for access to a locked iPhone, and the FBI's mass-hacking of a child predator ring operating on the dark web, demonstrate the extent to which US police have relied on such bugs in their investigations. But as Electronic Frontier Foundation staff attorney Andrew Crocker recently told Motherboard's Joseph Cox, because the VEP is a closely held secret, "no one really knows if it's followed in any cases."

Apple, for example, told Reuters earlier this week that the first time the FBI had ever disclosed flaws in Apple software was April 14. Though an annual report on the VEP's implementation is required, none of these reports have ever been made public.

Toronto Star
Spy agency cagey on privacy breaches
Tuesday, 03 May 2016
Byline: Alex Boutilier

OTTAWA -- The Communications Security Establishment is refusing to release the number of privacy breaches the agency has logged since 2007.
Documents obtained by the Star state the intelligence and cyber defence agency has maintained a central database for certain privacy violations since 2007. These breaches are categorized as minor "procedural errors" or more serious "privacy incidents," and reviewed by the CSE Commissioner's office every year.

"In these files, CSE records any incidents it identifies that put at risk the privacy of a Canadian in a manner that runs counter to (or is not provided in) its operational policies," says a September 2014 letter from former CSE chief John Forster to a senior Treasury Board official.

The Star requested just the number of breaches - no details about what actually transpired or the Canadian personal information involved - but was told the agency could not comply due to "operational security concerns."

"Releasing the number of (breaches) would provide insight into CSE's capacity to conduct operations, the extent of its capabilities, the degree to which partner organizations benefit from sharing and the reach of the programs," wrote spokesperson Ryan Foreman in an email last week.

CSE is one of Canada's most technologically sophisticated agencies, responsible for collecting foreign intelligence and protecting Canadian networks from cyber attacks. It is forbidden to use its surveillance tactics against Canadian citizens, except under specific circumstances.

But disclosures from U.S. whistleblower Edward Snowden have aroused suspicion about CSE's tools and tactics as part of the Five Eyes alliance that also includes the U.S., U.K., Australia and New Zealand.

Documents tabled in Parliament last month show CSE logged 13 privacy and information breaches in 2015, affecting at least 630 individuals. The agency did not report any of the privacy breaches to the federal privacy commissioner, as CSE determined that there was "no significant risk" to the individuals involved.

CSE further refused to report the activities that led to the breaches.

The Star reported Sunday that the agency has been in a year-long debate with the Privacy Commissioner Daniel Therrien's office over how much information CSE is required to report about privacy breaches. A government-wide regulation requires all serious breaches to be reported to the privacy watchdog, but a "discussion" about how best to do that has been dragging on since at least January 2015.

On Monday, NDP foreign affairs critic Hélène Laverdière asked Defence Minister Harjit Sajjan to explain why CSE is resisting turning information over to Therrien's office.

"CSE has proactively worked with the commissioner on all aspects, and they do have a good working relationship," said Sajjan, who is responsible for the intelligence agency. "CSE abides by Canadian law, including the Privacy Act."

Wesley Wark, a professor at the University of Ottawa specializing in security and intelligence matters, said reviewing CSE's privacy breaches has typically fallen to the CSE commissioner, rather than the privacy watchdog.

"Really, the protection of privacy role, in terms of external review, has de facto been given to the CSE commissioner," Wark said in an interview last week.

The 12-person team at CSE Commissioner Jean-Pierre Plouffe's office is mandated to ensure that CSE complies with Canadian law.

Globe and Mail
Canadian arrested in Nepal over tweets
Tuesday, 03 May 2016
Byline: Tu Thanh Ha

A Canadian expatriate working in Kathmandu has been arrested and threatened with expulsion from Nepal because of his socialmedia posts criticizing the country's human-rights situation.
Robert Penner, a software developer living in Lalitpur, a district south of Kathmandu, had been writing about issues such as the problems of the Madhesi minority, the arrest of prominent journalist Kanak Mani Dixit and the local reaction to a recent report by Human Rights Watch on Nepal.

Mr. Penner said the local police came to his office on Monday afternoon.

"I repeatedly asked Nepal Police to tell me under what charges they're taking me but they won't say," he tweeted just before his arrest.

Mr. Penner was being held overnight on immigration charges that his Twitter posts were harming "security and mutual harmony in Nepal," his lawyer, Dipendra Jha, told The Globe and Mail.

"They're saying they plan to deport him back because they can cancel his visa."

Rishi Ram Sharma, chief district officer of Lalitpur, confirmed to The Globe that local police took Mr. Penner into custody at the request of immigration officials.

"Immigration asked us to hand [him] over," he said when reached by phone.

Kedar Neupane, director-general of the Department of Immigration, declined to comment when contacted by The Globe, saying he was busy with a meeting.

Mr. Neupane, however, told the Nepalese newspaper Republica that his department wants to expel Mr. Penner back to Canada.

"He obtained a visa for working at an IT company but he was found engaged in making provocative statements that may jeopardize national integrity," Mr. Neupane was quoted as saying.

"Foreigners are not allowed to engage in such activities."

"We are investigating into the matter, and will deport him if charges against him are proven true," The New York Times reported Mr. Neupane as saying.

Madhesi activist Puru Shah said Mr. Penner had riled up many Nepalese nationalists by questioning how their country was handling human-rights concerns.

"He's a very logical guy. He sees something that is not logical, he will call it out," Mr. Shah said in an interview.

The arrest puts a spotlight on the country's controversial new constitution, which has upset minorities such as the Madhesi, who say they will be marginalized under its citizenship rules.

Under the new constitution, children of Nepali women who marry foreigners won't have fullfledged citizenship rights, an issue for the Madhesis, who live near India and have a tradition of cross-border marriages, Mr. Shah said.

He said Mr. Penner had written two articles for a pro-Madhesi website. "He made a lot of people upset."

According to his social-media posts, Mr. Penner is a former resident of Kelowna, B.C., who first visited Nepal a decade ago and has been living in the Kathmandu area for the past four years, working for a technology outsourcing company, CloudFactory.

"My Twitter timeline is a war zone these days," Mr. Penner told a friend on Facebook last December.

He shared screen captures of people on Twitter accusing him of having a hidden agenda and using human-rights discussions as a cover to promote "the secessionist movement."

Some made threats. Others called on the Nepalese government to expel Mr. Penner.

Mr. Shah said he saw a tweet written in Nepali earlier this month that alerted an official government account about Mr. Penner's writings. The government account then replied, asking for more details, Mr. Shah said.

Under the new constitution, the right to freedom of expression is only guaranteed to Nepalese citizens, not foreign residents, human-rights lawyer Santosh Sigdel told The Globe.

Mr. Sigdel also noted that another Nepalese law makes it illegal to publish material in the electronic media that "may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes and communities."

New Zealand Herald
Trust a vital asset as NZ faces future
Tuesday, 03 May 2016
Byline: Gehan Gunasekara
Section: oped

With the recent announcements of manufacturing closures in New Zealand, such as Fisher & Paykel's Auckland plant, it is important to develop new knowledge-based jobs here. Twenty-first century business is increasingly data-driven by analytics and Big Data. Personal information is becoming the new oil and companies here must be able to tap into it.
A good example of information-based business is cloud providers. Currently, the United States is the dominant player. New Zealand has never competed on scale; instead its strength has been the quality of its products and the reputation of its brands. With cloud services reputation and trust is everything.

Legal safeguards for personal information and restraining unimpeded surveillance are crucial to allow businesses to make the most of this trust.

The recent Independent Review of Intelligence and Security by the Hon Sir Michael Cullen and Dame Patsy Reddy has produced remarkably detailed recommendations for revamped laws surrounding the activities of our spy agencies. If they are implemented in their entirety we will have some of the toughest controls on such agencies in the western world.

If instead the Government cherry-picks aspects of the Cullen-Reddy report then the gaps would quickly be exploited by the agencies concerned and we may as well not have bothered with any reform.

To give just one example, one of the currently neglected areas is "incidentally gathered information". Electronic surveillance tends to "vacuum up" vast amounts of information. Most is undoubtedly discarded by the likes of the GCSB but currently it can be sent to its partners in the Five-Eyes network who can do what they want with it.

The report recommends plugging this gap by requiring the New Zealand agency to decide which part of the data it wants to keep or share and to go through procedures (such as an obtaining an interception warrant). This would mean all surveillance is targeted and mass surveillance such as that exposed by Edward Snowden could not occur.

Into this heady mix must be factored the restrictions imposed on New Zealand by the TPP. Although this free-trade agreement requires its parties to adopt or maintain a legal framework providing for the protection of personal information, the requirement is weakly defined. It can be satisfied by laws providing for enforcing voluntary undertakings by enterprises relating to privacy. This is essentially the American approach and has not prevented frequent privacy invasions by the likes of Facebook and Google, for instance.

The TPP's article 14.11.2 mandates that cross-border data flows of personal information not be restricted, and article 14.13 prohibits laws that require data to be held in New Zealand and not, for example, elsewhere such as Australia.

Exceptions are subject to a complex four-step test with the onus being on the country imposing restrictions to show why they are essential for its public policies, and that they are non-discriminatory and proportionate.

Finally, there are the investor-state dispute settlement provisions prohibiting direct or indirect expropriation of overseas investors targeting New Zealand.

Should the Government follow recommendations for strengthening the Privacy Act by imposing strict liability on local agencies that outsource information or use cloud providers, it is likely that the agencies would seek to obtain indemnities from the overseas providers involved. This may lead to the latter refusing to provide the services.

Where existing facilities (say data storage) have already been built with a view to serving customers here, this may amount to indirect expropriation and lead to our government being sued by investors under investor-state provisions in the TPP. This may not be far-fetched and illustrates why delaying much-overdue reform of the Privacy Act has weakened our ability to project a privacy-friendly image.

Note: Gehan Gunasekara is an associate professor in commercial law at the University of Auckland Business School and advised the Law Commission on reform of the Privacy Act 1993.

South China Morning Post
Government 'powerless' against deep web threat
Tuesday, 03 May 2016
Byline: Allen Au-yeung

Hong Kong authorities are powerless to police clandestine activities flourishing in the "deep web" - the unseen portion of the internet that makes up 96 per cent of online content - because there is no legal basis to do so, according to local cybersecurity experts.
Duncan Wong, director of security and data sciences at the Hong Kong Applied Science and Technology Research Institute, told the Post that only 4 per cent of the web can be accessed by conventional search engines.

The rest, called the deep web, is unsearchable and password-protected. Inside the deep web, there is also an area known as the "dark web", which can only be accessed using identity- hiding encryption technology.

"The dark web is a collection of websites. This collection can be accessed anonymously," said Wong, who frequently surfs it to gather intelligence on the latest hacking trends. "A part of the dark web is pretty dark. People use it to exchange malicious software, like recently popular ransomware.

"On the dark web, people are also selling drugs and some websites are related to pornography."

Ransomware is malware that encrypts files in victims' computers, rendering them unrecoverable. Victims are then told to pay a ransom in bitcoin to unlock them.

As of mid- March, the Hong Kong Computer Emergency Response Team Coordination Centre had received 18 reports about the use of ransomware. Victims included small businesses and non-governmental organisations, and the team believed there were many more unreported cases.

While the latest attacks' origin was unclear, Wong said the type of malware involved was known to not infect computer systems operating in Russian.

Information technology lawmaker Charles Mok said he believed it was impossible for law enforcers by themselves to regulate the dark web as the bulk of its activities took place abroad.

"It's something that exists, unless you completely cut yourself off from the internet. It's impossible to shut it down," said Mok.

He said the government had been passive in helping the public protect themselves.

"The government has always been late in understanding the problems," Mok said.

Wong said the best way for businesses to protect themselves was to regularly back up files on a computer not always hooked up to the internet.

But he said people should not fear the dark web, which also serves as a channel for whistle-blowers who want to share sensitive information anonymously.

"I don't think there is anything to worry about," Wong said. "There is no way to stop the dark web, and it has its value for different people. It will be there forever. You can shut down some of the drug dealing sites like Silk Road and then Silk Road 2.0 is out."

Reuters
Canadian held for second day after social media criticism of Nepal government
Tuesday, 03 May 2016

Kathmandu - A Canadian computer programmer who has been vocally critical of the government of Nepal on social media has been held for a second day of questioning, a Nepali official said on Tuesday. Robert Penner was taken to the Department of Immigration for questioning on Monday by police who arrested him at his office in southern Kathmandu, said Lalitpur Senior Superintendent of Police Pitambar Adhikari. Penner lives in Kathmandu and works for Sound Cloud, an outsourcing company.

He criticized the Nepal government on social media during unrest that followed the passing of Nepal's constitution last year and he denounced the recent arrest and detention of Kanak Mani Dixit, a prominent journalist and civil rights activist.

"Yesterday we requested the police to bring him to the Department of Immigration for questioning," Prakash Neupane, director of immigration told Reuters.

"Penner is still under the process of investigation. We are investigating whether he has contravened the terms of his working visa, which state he can be punished if he engages in activities outside the terms of his working visa."

Lawyer Dipendra Jha, who is representing Penner, said he had been informed that the Canadian would be released on Tuesday, and his visa revoked. Officials at the Department of Immigration declined to confirm this.

The Canadian consulate in Kathmandu could not be reached for comment. The Canadian High Commission in the Indian capital New Delhi declined to comment.

Press Trust of India
Canadian arrested in Nepal for posting provocative tweets
Tuesday, 03 May 2016

Kathmandu - A Canadian national, who backed the Madhes movement, was today arrested by Nepal Police for allegedly posting provocative and anti- national comments on social media and visa violations. Robert Penner was arrested from Lalitpur on a request from the Department of Immigration (DoI), Nepalease media reported.

DoI Director-General Kedar Neupane said Penner was arrested to probe his posts on social media which are "liable to incite" social disharmony in the nation.

Penner had obtained working visa for a sprout technology company, which was already dissolved in 2012, but worked for Cloud Factory, a foreign outsourcing company, according to the DoI.

Penner is also accused of holding multiple visas and overstaying. "He obtained visa for working at an IT company but he was found engaged in making provocative statements that may jeopardise national integrity," said Neupane, adding, "foreigners are not allowed to engage in such activities."

The report said immigration laws bar any foreign national from expressing public comments on internal politics of the host nation.

A source at the DoI told MyRepublica that they received complaints that Penner had been engaging in activities that could harm Nepal's national integrity. "We had to arrest him due to his suspicious activities and for misusing his visa," said the source.

Penner has previously tweeted in favour of the Madhes movement. He had also written controversial tweets about the arrest of journalist Kanak Mani Dixit, MyRepublica reported.

Madhesis, mostly of Indian origin, have been demanding that Nepal's Constitution be amended to include their concerns over inadequate political representation and redrawing of federal boundaries.

They had enforced months-long blockade of Nepal's all trading points with India, creating huge shortage of essential commodities in the country.

The Intercept
WhatsApp, Used by 100 Million Brazilians, Was Shut Down Nationwide Today by a Single Judge
Tuesday, 03 May 2016
Byline: Glenn Greenwald, Adam Fishman

Washington - A BRAZILIAN STATE JUDGE ordered mobile phone operators to block nationwide the extremely popular WhatsApp chat service for 72 hours, a move that will have widespread international reverberations for the increasingly contentious debate over encryption and online privacy. The ruling, issued on April 26, became public today when it was served on mobile service providers. It took effect at 2 p.m. local time (1 p.m. ET); as of that time, people in Brazil who tried to use the service could not connect, nor could they send or receive any messages. Failure to comply will subject the service providers to a fine of 500,000 reals per day ($142,000 per day).
WhatsApp is the most-used app in Brazil, a country of 200 million people (it is now owned by Facebook, the country's second-most used app). An estimated 91 percent of Brazilian mobile users nationwide -- more than 100 million individuals -- use WhatsApp to communicate with one another for free (it has 900 million active daily users around the world). Brazilians spent this morning, in the hours before the block took effect, frantically sending each other messages on WhatsApp warning that the service was going down for three days.

This ruling comes from the same judge, Marcel Maia Montalvão, of a small town in Sergipe state, who two months ago ordered Facebook's vice president for Latin America, Diego Dzodan, to be detained over WhatsApp's failure to cooperate with a subpoena issued as part of a criminal investigation. The judge said the arrest was justified by Facebook's "repeatedly failing to comply with judicial orders" in a drug-trafficking case. Pursuant to that order, Dzodan was arrested by federal police and held in custody for a full day, until an appellate court overturned the order.

Afterward, the Facebook executive insisted that "the way that information is encrypted from one cellphone to another, there is no information stored that could be handed over to authorities." WhatsApp similarly said: "WhatsApp cannot provide information we do not have." According to Folha de São Paulo, Brazil's largest newspaper, today's ruling ordering the shutdown of WhatsApp stems from the same case.

The extraordinary orders reflect what is becoming a global controversy over the fight of technology companies to offer their users "end-to-end" encryption. That service, which has become quite in demand in the wake of reporting from the archive provided by Edward Snowden, ensures that only the users -- but not the company itself -- can access the content they are sharing. The post- Snowden fixation of tech companies to demonstrate a genuine commitment to protect the privacy of their users (motivated by business self-interest) has driven a wedge between the once-fully collaborative Silicon Valley and U.S. government surveillance state partners, creating a protracted and bitter public PR war that culminated last month in the Apple/FBI fight over access to iPhones.

As a result of its encryption protections, the position of WhatsApp in response to subpoenas has been that it is incapable of turning over users' communications because the encryption not only keeps governments and non-state actors out but also the company itself. Over the past several years, numerous countries have begun enacting laws to bar companies from using any encryption that they cannot circumvent, and the Obama administration has been debating whether to support legislation that would allow only the use of encryption to which government agencies have backdoor access (in the

1990s, the Clinton administration used the Oklahoma City bombing to argue for a similar law, but it was blocked by a coalition of privacy advocates from both parties in Congress).

THIS IS NOT the first time WhatsApp service has been interrupted in Brazil. Last December, in a separate case, a lower court judge in São Paulo state ordered service providers to block the app for 48 hours as retribution for its failure to cooperate in a criminal investigation. An appeals court overturned the ruling but only after hours of service outage, invoking "constitutional principles" to say that "it does not seem reasonable that millions of users are affected because of the inertia of a company."

In many ways, Brazil -- with huge numbers of internet users and a growing online population of young people -- is a key battleground for the global struggle for internet freedom. The Wall Street Journal called Brazil "the social media capital of the universe." In January, after the last WhatsApp shutdown, two analysts from the Brazil-based Igarapé Institute, Robert Muggah and Nathan Thompson, wrote in the New York Times, "The country has one of the fastest growing populations of internet users in the world. Online tools like Facebook, Twitter and WhatsApp are used not only to express opinions; they are an affordable alternative to exorbitantly priced Brazilian telecom providers."

In a country with turbulent political conflicts and a highly engaged online population, the debate over internet freedom has become very prominent. Along with Germany, the Brazilian government, in the wake of the Snowden revelations, was the most vocal in denouncing the U.S. for excessive NSA surveillance (Brazil was a key target for such spying). In 2014, the government enacted what it claimed was a law to protect internet freedom, "Marco Civil da Internet," that did provide some privacy protections but also granted new surveillance powers to the government. Just last month, the government demanded, and received, a new draconian anti-terrorism law that provided it with extreme new law enforcement powers (causing ex-President Lula da Silva to break with his party, which controls the government, by telling The Intercept in an interview that he opposes the new law).

And now, as The Intercept reported last week, a new cybercrime bill on the verge of being enacted could codify internet-shutdown powers of the type the state judge today imposed. In a Facebook post, Ronaldo Lemos, founding director of the Institute of Technology and Society of Rio de Janeiro and an architect of Brazil's landmark 2014 Marco Civil internet legislation, wrote: "Tomorrow, the Cybercrime CPI will vote on a proposal to make this type of block lawful. If the CPI proposal goes forward, this will be the new normal in the country. Every week we would have news of sites and services that are blocked, as it is in Saudi Arabia and North Korea."

It is stunning to watch a single judge instantly shut down a primary means of online communication for the world's fifth-largest country. The two security experts in the NYT wrote of the first WhatsApp shutdown: "The judge's action was reckless and represents a potentially longer-term threat to the freedoms of Brazilians." But there is no question that is just a sign of what is to come for countries far from Brazil: There will undoubtedly be similar battles in numerous countries around the world over what rights companies have to offer privacy protections to their users.

The Intercept
Inside the Assassination Complex
Tuesday, 03 May 2016
Byline: Edward Snowden

Comment - "I've been waiting 40 years for someone like you." Those were the first words Daniel Ellsberg spoke to me when we met last year. Dan and I felt an immediate kinship; we both knew what it meant to risk so much -- and to be irrevocably changed -- by revealing secret truths.
One of the challenges of being a whistleblower is living with the knowledge that people continue to sit, just as you did, at those desks, in that unit, throughout the agency, who see what you saw and comply in silence, without resistance or complaint. They learn to live not just with untruths but with unnecessary untruths, dangerous untruths, corrosive untruths. It is a double tragedy: What begins as a survival strategy ends with the compromise of the human being it sought to preserve and the diminishing of the democracy meant to justify the sacrifice.

But unlike Dan Ellsberg, I didn't have to wait 40 years to witness other citizens breaking that silence with documents. Ellsberg gave the Pentagon Papers to the New York Times and other newspapers in 1971; Chelsea Manning provided the Iraq and Afghan War logs and the Cablegate materials to WikiLeaks in 2010. I came forward in 2013. Now here we are in 2016, and another person of courage and conscience has made available the set of extraordinary documents that are published in The Assassination Complex, the new book out today by Jeremy Scahill and the staff of The Intercept. (The documents were originally published last October 15 in The Drone Papers.)

We are witnessing a compression of the working period in which bad policy shelters in the shadows, the time frame in which unconstitutional activities can continue before they are exposed by acts of conscience. And this temporal compression has a significance beyond the immediate headlines; it permits the people of this country to learn about critical government actions, not as part of the historical record but in a way that allows direct action through voting -- in other words, in a way that empowers an informed citizenry to defend the democracy that "state secrets" are nominally intended to support. When I see individuals who are able to bring information forward, it gives me hope that we won't always be required to curtail the illegal activities of our government as if it were a constant task, to uproot official lawbreaking as routinely as we mow the grass. (Interestingly enough, that is how some have begun to describe remote killing operations, as "cutting the grass.")

A single act of whistleblowing doesn't change the reality that there are significant portions of the government that operate below the waterline, beneath the visibility of the public. Those secret activities will continue, despite reforms. But those who perform these actions now have to live with the fear that if they engage in activities contrary to the spirit of society -- if even a single citizen is catalyzed to halt the machinery of that injustice -- they might still be held to account. The thread by which good governance hangs is this equality before the law, for the only fear of the man who turns the gears is that he may find himself upon them.

Hope lies beyond, when we move from extraordinary acts of revelation to a collective culture of accountability within the intelligence community. Here we will have taken a meaningful step toward solving a problem that has existed for as long as our government.

Not all leaks are alike, nor are their makers. Gen. David Petraeus, for instance, provided his illicit lover and favorable biographer information so secret it defied classification, including the names of covert operatives and the president's private thoughts on matters of strategic concern. Petraeus was not charged with a felony, as the Justice Department had initially recommended, but was instead permitted to plead guilty to a misdemeanor. Had an enlisted soldier of modest rank pulled out a stack of highly classified notebooks and handed them to his girlfriend to secure so much as a smile, he'd be looking at many decades in prison, not a pile of character references from a Who's Who of the Deep State.

There are authorized leaks and also permitted disclosures. It is rare for senior administration officials to explicitly ask a subordinate to leak a CIA officer's name to retaliate against her husband, as appears to have been the case with Valerie Plame. It is equally rare for a month to go by in which some senior official does not disclose some protected information that is beneficial to the political efforts of the parties but clearly "damaging to national security" under the definitions of our law.

This dynamic can be seen quite clearly in the al Qaeda "conference call of doom" story, in which intelligence officials, likely seeking to inflate the threat of terrorism and deflect criticism of mass surveillance, revealed to a neoconservative website extraordinarily detailed accounts of specific communications they had intercepted, including locations of the participating parties and the precise contents of the discussions. If the officials' claims were to be believed, they irrevocably burned an extraordinary means of learning the precise plans and intentions of terrorist leadership for the sake of a short-lived political advantage in a news cycle. Not a single person seems to have been so much as disciplined as a result of the story that cost us the ability to listen to the alleged al Qaeda hotline.

If harmfulness and authorization make no difference, what explains the distinction between the permissible and the impermissible disclosure?

The answer is control. A leak is acceptable if it's not seen as a threat, as a challenge to the prerogatives of the institution. But if all of the disparate components of the institution -- not just its head but its hands and feet, every part of its body -- must be assumed to have the same power to discuss matters of concern, that is an existential threat to the modern political monopoly of information control, particularly if we're talking about disclosures of serious wrongdoing, fraudulent activity, unlawful activities. If you can't guarantee that you alone can exploit the flow of controlled information, then the aggregation of all the world's unmentionables -- including your own -- begins to look more like a liability than an asset.

Truly unauthorized disclosures are necessarily an act of resistance -- that is, if they're not done simply for press consumption, to fluff up the public appearance or reputation of an institution. However, that

doesn't mean they all come from the lowest working level. Sometimes the individuals who step forward happen to be near the pinnacle of power. Ellsberg was in the top tier; he was briefing the secretary of defense. You can't get much higher, unless you are the secretary of defense, and the incentives simply aren't there for such a high-ranking official to be involved in public interest disclosures because that person already wields the influence to change the policy directly.

At the other end of the spectrum is Manning, a junior enlisted soldier, who was much nearer to the bottom of the hierarchy. I was midway in the professional career path. I sat down at the table with the chief information officer of the CIA, and I was briefing him and his chief technology officer when they were publicly making statements like "We try to collect everything and hang on to it forever," and everybody still thought that was a cute business slogan. Meanwhile I was designing the systems they would use to do precisely that. I wasn't briefing the policy side, the secretary of defense, but I was briefing the operations side, the National Security Agency's director of technology. Official wrongdoing can catalyze all levels of insiders to reveal information, even at great risk to themselves, so long as they can be convinced that it is necessary to do so.

Reaching those individuals, helping them realize that their first allegiance as a public servant is to the public rather than to the government, is the challenge. That's a significant shift in cultural thinking for a government worker today.

I've argued that whistleblowers are elected by circumstance. It's not a virtue of who you are or your background. It's a question of what you are exposed to, what you witness. At that point the question becomes Do you honestly believe that you have the capability to remediate the problem, to influence policy? I would not encourage individuals to reveal information, even about wrongdoing, if they do not believe they can be effective in doing so, because the right moment can be as rare as the will to act.

This is simply a pragmatic, strategic consideration. Whistleblowers are outliers of probability, and if they are to be effective as a political force, it's critical that they maximize the amount of public good produced from scarce seed. When I was making my decision, I came to understand how one strategic consideration, such as waiting until the month before a domestic election, could become overwhelmed by another, such as the moral imperative to provide an opportunity to arrest a global trend that had already gone too far. I was focused on what I saw and on my sense of overwhelming disenfranchisement that the government, in which I had believed for my entire life, was engaged in such an extraordinary act of deception.

At the heart of this evolution is that whistleblowing is a radicalizing event -- and by "radical" I don't mean "extreme"; I mean it in the traditional sense of radix, the root of the issue. At some point you recognize that you can't just move a few letters around on a page and hope for the best. You can't simply report this problem to your supervisor, as I tried to do, because inevitably supervisors get nervous. They think about the structural risk to their career. They're concerned about rocking the boat and "getting a reputation." The incentives aren't there to produce meaningful reform. Fundamentally, in an open society, change has to flow from the bottom to the top.

As someone who works in the intelligence community, you've given up a lot to do this work. You've happily committed yourself to tyrannical restrictions. You voluntarily undergo polygraphs; you tell the government everything about your life. You waive a lot of rights because you believe the fundamental goodness of your mission justifies the sacrifice of even the sacred. It's a just cause.

And when you're confronted with evidence -- not in an edge case, not in a peculiarity, but as a core consequence of the program -- that the government is subverting the Constitution and violating the ideals you so fervently believe in, you have to make a decision. When you see that the program or policy is inconsistent with the oaths and obligations that you've sworn to your society and yourself, then that oath and that obligation cannot be reconciled with the program. To which do you owe a greater loyalty?

One of the extraordinary things about the revelations of the past several years, and their accelerating pace, is that they have occurred in the context of the United States as the "uncontested hyperpower." We now have the largest unchallenged military machine in the history of the world, and it's backed by a political system that is increasingly willing to authorize any use of force in response to practically any justification. In today's context that justification is terrorism, but not necessarily because our leaders are particularly concerned about terrorism in itself or because they think it's an existential threat to society. They recognize that even if we had a 9/11 attack every year, we would still be losing more people to car accidents and heart disease, and we don't see the same expenditure of resources to respond to those more significant threats.

What it really comes down to is the political reality that we have a political class that feels it must inoculate itself against allegations of weakness. Our politicians are more fearful of the politics of terrorism -- of the charge that they do not take terrorism seriously -- than they are of the crime itself.

As a result we have arrived at this unmatched capability, unrestrained by policy. We have become reliant upon what was intended to be the limitation of last resort: the courts. Judges, realizing that their decisions are suddenly charged with much greater political importance and impact than was originally intended, have gone to great lengths in the post- 9/11 period to avoid reviewing the laws or the operations of the executive in the national security context and setting restrictive precedents that, even if entirely proper, would impose limits on government for decades or more. That means the most powerful institution that humanity has ever witnessed has also become the least restrained. Yet that same institution was never designed to operate in such a manner, having instead been explicitly founded on the principle of checks and balances. Our founding impulse was to say, "Though we are mighty, we are voluntarily restrained."

When you first go on duty at CIA headquarters, you raise your hand and swear an oath -- not to government, not to the agency, not to secrecy. You swear an oath to the Constitution. So there's this friction, this emerging contest between the obligations and values that the government asks you to uphold, and the actual activities that you're asked to participate in.

These disclosures about the Obama administration's killing program reveal that there's a part of the American character that is deeply concerned with the unrestrained, unchecked exercise of power. And there is no greater or clearer manifestation of unchecked power than assuming for oneself the authority to execute an individual outside of a battlefield context and without the involvement of any sort of judicial process.

Traditionally, in the context of military affairs, we've always understood that lethal force in battle could not be subjected to ex ante judicial constraints. When armies are shooting at each other, there's no room for a judge on that battlefield. But now the government has decided -- without the public's participation, without our knowledge and consent -- that the battlefield is everywhere. Individuals who don't represent an imminent threat in any meaningful sense of those words are redefined, through the subversion of language, to meet that definition.

Inevitably that conceptual subversion finds its way home, along with the technology that enables officials to promote comfortable illusions about surgical killing and nonintrusive surveillance. Take, for instance, the Holy Grail of drone persistence, a capability that the United States has been pursuing forever. The goal is to deploy solar-powered drones that can loiter in the air for weeks without coming down. Once you can do that, and you put any typical signals collection device on the bottom of it to monitor, unblinkingly, the emanations of, for example, the different network addresses of every laptop, smartphone, and iPod, you know not just where a particular device is in what city, but you know what apartment each device lives in, where it goes at any particular time, and by what route. Once you know the devices, you know their owners. When you start doing this over several cities, you're tracking the movements not just of individuals but of whole populations.

By preying on the modern necessity to stay connected, governments can reduce our dignity to something like that of tagged animals, the primary difference being that we paid for the tags and they're in our pockets. It sounds like fantasist paranoia, but on the technical level it's so trivial to implement that I cannot imagine a future in which it won't be attempted. It will be limited to the war zones at first, in accordance with our customs, but surveillance technology has a tendency to follow us home.

Here we see the double edge of our uniquely American brand of nationalism. We are raised to be exceptionalists, to think we are the better nation with the manifest destiny to rule. The danger is that some people will actually believe this claim, and some of those will expect the manifestation of our national identity, that is, our government, to comport itself accordingly.

Unrestrained power may be many things, but it's not American. It is in this sense that the act of whistleblowing increasingly has become an act of political resistance. The whistleblower raises the alarm and lifts the lamp, inheriting the legacy of a line of Americans that begins with Paul Revere.

The individuals who make these disclosures feel so strongly about what they have seen that they're willing to risk their lives and their freedom. They know that we, the people, are ultimately the strongest and most reliable check on the power of government. The insiders at the highest levels of government

have extraordinary capability, extraordinary resources, tremendous access to influence, and a monopoly on violence, but in the final calculus there is but one figure that matters: the individual citizen.

And there are more of us than there are of them.

Note: From The Assassination Complex: Inside the Government's Secret Drone Warfare Program by Jeremy Scahill and the staff of The Intercept, with a foreword by Edward Snowden and afterword by Glenn Greenwald, published by Simon & Schuster.

New York Times
Canadian Held Over Twitter Post
Tuesday, 03 May 2016
Byline: Bhadra Sharma

Kathmandu - A Canadian man in Nepal who writes frequently about political issues on social media was arrested on Monday afternoon after "posting a provocative message on Twitter aimed at spreading social discord," according a Nepalese immigration official.
The man, Robert Penner, has been living in Nepal for at least two years. He was arrested at his office in the Lalitpur district by a team of police officers on the instructions of the Department of Immigration, according to Pitambar Adhikari, the district police chief. Mr. Penner was turned over to the immigration authorities, who have held him since then.

Mr. Penner has been prolific online, often weighing in on political controversies. After Nepal passed a new Constitution last year, he questioned a citizenship provision that was seen as discriminatory against women. In November, he responded to critics of a Human Rights Watch report about violations in southern Nepal.

More recently, he criticized the detention of Kanak Mani Dixit, a journalist who was arrested last month on suspicion of abusing his position as the chairman of a transportation cooperative.

According to his Twitter profile, Mr. Penner works as a scientist at Cloud Factory, a technology company with an office in Lalitpur. An official at the Department of Immigration said Mr. Penner had a valid work visa.

The immigration official, Kedar Neupane, said Mr. Penner had been arrested because he had was "spreading unnecessary messages about Nepal" on social media, but did not say who had made the complaint.

Manila Bulletin
Anonymous PH declares ceasefire from hacking gov't sites

Tuesday, 03 May 2016
Byline: Argyll Cyrus B. Geducos

Manila - A ceasefire from hacking government websites until a new president is elected was declared yesterday by members of Anonymous Philippines, a group of hackers who had claimed responsibility for defacing the website of the Commission on Elections (Comelec).
Around 30 members of the group trooped to the Department of Justice (DOJ) on Padre Faura Street in Manila yesterday and demanded that the government hire the arrested hackers instead. The group also called for the release of two arrested hackers.

The National Privacy Commission (NPC) had explained that it is difficult to hire the arrested hackers - Paul Biteng and Joenel de Asis - as this may imply to the jobless technology experts that there are jobs waiting for them.

Wearing their signature masks similar to the mask in the movie "V for Vendetta," the members endured the morning heat to insist that defacing the poll body's website only showed that their system was indeed weak.

"Ito po ay pagpapatibay lamang din na ang gobyerno ay naging pabaya sa seguridad ng data ng bawat Pilipino (This is just proof that the government has been careless in securing the data of everybody)," they said.

They also reiterated that Biteng only defaced the Comelec website and was not responsible of leaking the data, a statement already confirmed by De Asis, the hacker arrested by the National Bureau of Investigation (NBI) last Thursday.

De Asis earlier said that their group, LulzSec Philippines, had leaked the 340-gigabyte data online through a fake Facebook account. However, they claimed that the hacker website "WeHaveYourData.com" which contained the sensitive data was put up by somebody else.

Anonymous Philippines also revealed that they have forewarned Comelec officials back in 2013 about the many vulnerabilities in their website. "Ibinunyag na namin noong 2013 na mahina ang inyong sistema ngunit ano ang nangyari? Hindi ba't kapabayaan ito? (We have already revealed in 2013 that their system is weak but this still happened. Isn't this negligence on their part?)" The group also said that they had been watching the Comelec's system since 2010.

Meanwhile, the National Bureau of Investigation (NBI) warned those who have downloaded and seeded the leaked data from the Comelec website that the Bureau will soon be hunting them down.

This came after the arrest of De Asis, the second hacker, on Thursday afternoon for reportedly leaking the 340-gigabyte data after it was hacked by Biteng on March 22.

NBI-Cybercrime Division (CCD) Chief Ronald Aguto Jr. said that the next step is to hunt down and file cases against individuals who downloaded and used the said data.

Bangkok Post
Regime goes after ringleaders
Tuesday, 03 May 2016
Byline: Wassana Nanuam

Bangkok - Tougher steps are likely to deal with anti-coup elements, the army chief says, as the regime looks for evidence to pursue ringleaders including red-shirt leader Jatuporn Prompan and persistent critic Sombat Boon-ngamanong.
The coup critics are bent on causing public unrest, he added. Teerachai Nakwanich's comment followed the arrests last week of eight Facebook users for online messages allegedly criticising the prime minister and the regime.

The suspects have been charged with inciting public unrest under the Criminal Code's Section 116 and breaching the Computer Crime Act for Facebook posts that can be used to instigate chaos.

As police held a press briefing last Thursday, they revealed an "anti-coup" chart showing the connections between the suspects and their alleged links to Mr Jatuporn and Sombat. Police are also gathering evidence to seek warrants for the arrest of the pair.

Gen Teerachai said the anti-coup chart was based on the suspects' statements given to police. He also warned various protest groups opposing the draft constitution, saying these groups are made up of "the same old faces".

The army chief said he will not let them do anything to stir up trouble. Asked if he will adopt harsh measures to deal with protesters, Gen Teerachai said: "Wait and see. But we will no longer use 'attitude adjustment' because it's hard to talk to them now."

Based on the investigation findings, one of the eight suspects, Natthika Worathaiyawich, was hired to operate websites for Mr Jatuporn and Mr Sombat, police said.

According to police, Ms Natthika was the administrator of several sites that were highly critical of the government and military regime, including "We Love Prayuth", "UDD Thailand" and "Red Intelligence". She had received 110,000 baht monthly from another suspect, Harit Mahaton, since March 2014 and split the money with five other suspects, who are team members, police said.

Police said Ms Natthika also worked for the "Jatuporn Prompan" and "Peace TV" sites and was paid 20,000 baht per month. She was also allegedly paid 992,500 baht by Mr Sombat to operate sites criticising the People's Democratic Reform Committee from December 2013 to March 2014, police said.

Mr Harit was identified as a content adviser for "We Love Prayuth" and "UDD Thailand" and paid 28,000 baht for his services. His contact was allegedly Chaitat Rattanajan, a ninth suspect who is currently overseas and is believed to have received instructions from another unidentified person.

The rest of the eight suspects in custody are Noppakao Kongsuwan, Worawit Saksamutnan, Yothin Mangkhangsanga, Thanawat Buranasiri, Supachai Saibut, and Kannasit Tangboonthina.

Gen Teerachai says attempts to incite unrest are the jobs of the 'Facebook 8' arrested last week, red-shirt icon Jatuporn Prompan and regime critic Sombat Boon- ngamanong (insets).

Ten people were rounded up by the military last Wednesday, but two were released shortly after being cleared of any involvement. Deputy police spokesman Krissana Pattanacharoen talked Monday about a report that Panthongtae Shinawatra, the son of former prime minister Thaksin Shinawatra, was linked to the eight suspects.

A police source said when the police investigator submitted a request seeking the Military Court's permission to detain eight suspects, they also named Mr Panthongtae as a supporter of the suspects in the detention request.

Pol Col Krissana said investigators needed to gather clear evidence before issuing warrants for anyone. If evidence points to Mr Panthongtae, he will be summoned for questioning, Pol Col Krissana said.

Mr Jatuporn on Monday led a group of United Front for Democracy against Dictatorship members including Nattawut Saikuar, Weng Tojirakarn and Tida Tawornseth to the Bangkok Remand Prison to visit the eight detainees. The Military Court has denied the detainees bail as their charges carry a heavy penalty.

Speaking after the meeting, Mr Jatuporn said the charges levelled against the suspects for inciting unrest under Section 116 were unwarranted. The eight were only involved in making web pages with "political mockery" content, he said.

Mr Jatuporn also called on Prime Minister Prayut Chan-o-cha to be open to criticism as suggested by ex-premier Yingluck Shinawatra.

The prime minister is a public figure and should not be easily offended by criticism or mockery, Mr Jatuporn said. He also dismissed claims of Mr Panthongtae's links to the eight suspects as groundless.

Coup critic Mr Sombat said Monday he did not think pages mocking the prime minister would have an impact on national security. He denied any links to the so-called anti-coup chart.

Also on Monday, the Military Court approved a request from the Crime Suppression Division to further detain Pheu Thai Party key member Watana Muangsook.

Gulf News
QNB hackers to leak more data of another big bank soon
Tuesday, 03 May 2016
Byline: Naushad K. Cherrayil

Dubai - The hackers who attacked Qatar National Bank last week have attacked a second bank and are set to leak more data, a security expert told Gulf News on Monday.
"They have announced that they are going to release data from another big bank dating back to 2001. This data could be used for ransomware. They have said they are going to make it public, either today or tomorrow. We are monitoring it," said Mohammad Amin Hasbini, senior security researcher, global research and analysis team at Kaspersky Lab Middle East, Turkey and Africa. He said that the hackers have Turkish roots and are known as Bozkurtlar.

The hackers, which has uploaded a video online, have claimed responsibility for the bank breach. Al Habsini said could be linked to Syrian conflict.

Hasbini said that the hackers have not asked for any money yet, but have only leaked the data online. It [QNB breach] could be a political motive but "we are not sure yet. It is strange, normally hackers do hack for a goal."

Global losses from hacking and undesired spamming exceed $100 billion a year, according to Kaspersky Lab. Hackers stole $101 million from Bangladesh's central bank in February, and at least 40 million credit cards were compromised in a data breach at Target Corp in 2013.

News of the breach comes just weeks after Bangladesh's central bank announced that cybercriminals managed to steal over $100 million from one of its accounts at the Federal Reserve Bank of New York. The bank managed to recover some of the money, but $81 million that were transferred to the Philippines are still missing.

"Going by the motivation of financial gains, GCC region and the regional financial institutions could be more vulnerable because of the high concentration of wealthy individuals in the region. In the light of the increasing attacks it is important for regional institutions to take additional steps to protect their key data," said Stephen Bailey, who leads the cyber security team in PA Consulting's technical security practice in the Middle East and North Africa region.

"The motive of the QNB hacking can't be pinpointed at this stage. Although the bank has claimed it is an attack on its reputation, there could be a "financial angle" as these professional hackers are hired by someone with a motive, which could be from tarnishing someone's reputation to making financial gains

from personal data of customers. But at this stage, it is difficult to believe anyone hacking into a bank's data system just for defaming the institution.

"The strangest part of the QNB incident is that the hackers reportedly had access to the bank's data systems for a fairly long period -- by some accounts about 200 days -- and the bank's security system could not detect it until they made off with 1.4GB of data, and worse, the bank came to know of it when some of the data was published," he said.

Hasbini said the hackers have used an 'SQL injection" method to bypass the security of the bank and leak the data.

SQL injection is an open source tool that is used to attack data-driven programs. It must exploit security vulnerability in software, and is the most common method for attacking websites. It allows the hackers to complete disclosure of all data on the system, spoof identity (gaining an illegitimate advantage into the network by falsifying data), destroy the data or tamper with the existing data.

Most of the time vulnerabilities in security systems occur when modifications are done to existing websites and applications. Institutions must get their basics right in securing their critical data, Bailey said.

"There needs to be more care taken when modifications or new modules to the existing data system is introduced. There needs to be classification of data at various levels, the storing and securing should be done according to the importance of these data," he said.

Symantec figures show the total number of breaches has risen slightly by two per cent in 2015. The year also saw nine mega-breaches, surpassing 2013's record of eight breaches containing more than 10 million identities each.

Hassam Sidani, regional manager for Symantec Gulf, said over half a billion personal records were stolen or lost in 2015 globally. Data breaches continue to impact the enterprise.

In fact, he said that large businesses that are targeted for attack will on average be targeted three more times within the year. Additionally, the largest data breach ever publicly reported occurred last year with 191 million registered US voters' records compromised in a single incident. There were also a record-setting total of nine reported mega-breaches. While 429 million identities were exposed, the number of companies that chose not to report the number of records lost jumped by 85 per cent.

He said that businesses in the UAE were a victim of 2.7 per cent of global targeted attacks, with an organisation facing an average of 2.2 attacks through the year.

"Organisations in the finance, insurance and real estate sectors were the most affected by targeted attacks in the UAE in 2015, with 31.5 per cent of overall attacks being directed towards them. Small

organisations (1-250 employees), were the target of the most number of (64.2 per cent) spear-phishing attacks in the country," he said.

These organisations may be targeted as they have "less robust security" parameters, and can be used to gain access to its partner ecosystem, which may comprise larger and more lucrative companies.

Hasbini said banks will need to protect them from SQL injection attacks and they need to fine-tune and well protect its products and customers.

Nextgov.com (US)
Feds have found 'unbelievable' amounts of child porn on National Security computers. Is this the answer?
Tuesday, 03 May 2016
Byline: Staff report

Washington - A top National Security Agency official wants to keep tabs on national security personnel off-the-clock, in part by tracking their online habits at home. The aim is to spot behavior that might not be in America's best interests.
Historically, some illicit activity, like downloading child pornography, has occurred on government computers and been prosecuted.

But today, the digital lives of employees cleared to access classified information extend beyond the office.

About 80 percent of the National Security Agency workforce has retired since Sept. 11, 2001, says Kemp Ensor, NSA director of security. When the millennial and Gen Y staff that now populate the spy agency get home, they go online.

"That is where were we need to be, that's where we need to mine," Ensor said.

Currently, managers only look for aberrant computer behavior on internal, agency-owned IT systems - it's a practice known as "continuous monitoring."

But the military and intelligence communities are beginning to broaden checks on cleared personnel in the physical and digital worlds. It used to be that national security workers were re-investigated only every five or 10 years.

Under the evolving "continuous evaluation" model, the government will periodically search for signs of problems through, for example, court records, financial transactions, and -- if authorized -- social media posts.

Ensor and other federal officials spoke April 28 about new trends in personnel security at an Intelligence and National Security Alliance symposium in Chantilly, Virginia.

On government devices, "the amount of child porn I see is just unbelievable," said Daniel Payne, director of the Pentagon's Defense Security Service. The point being, there's a need to routinely scan agency network activity and criminal records to gauge an individual's suitability to handle classified information.

Payne, whose 34 years of counterintelligence experience have spanned the military, CIA and National Counterintelligence and Security Center, was not referring to any specific agency or any specific timeframe, his current employer told Nextgov.

Payne just returned to the Defense Security Service in February, after starting his career there.

"Director Payne provided this example to demonstrate the range of issues identified during the personnel security process, and the range and value of different data sources that have a bearing on an individual's ability to access sensitive information," the Defense Security Service said in an emailed statement.

Ensor echoed his colleague's concerns, noting he sees child pornography on NSA IT systems. In the national security space, "what people do is amazing," he said. Ensor's guess about the presence of explicit material is that there are many "introverts staring at computer screens" day in and day out. This is why it is so important to look at individuals holistically when determining who might be a so-called insider threat, Ensor said.

In the past, military and intelligence personnel have exploited minors online, without notice, for years or even an entire career.

The Boston Globe broke a story in 2010 that a significant number of federal employees and contractors with high- level security clearances downloaded child pornography -- sometimes on government computers -- at NSA and the National Reconnaissance Office, among other defense agencies.

At least one NSA contractor holding a top secret clearance told investigators in 2007 he had been spending $50 to $60 monthly fees on various sexually explicit websites for the past three years, according to a Defense inspector general report on the matter. After each session on the porn sites, he would wipe the browsing history of that system. The Pentagon investigation did not state who owned the computer.

More recently, a military official pleaded guilty to pedophile crimes and accessing child pornography through the Internet -- but at home.

On April 15, a U.S. district judge sentenced former Army Corps of Engineers official Michael Beeman, of Virginia, to 30 years in prison for molesting minors, beginning in the 1980s while working in public affairs

at Patrick Air Force Base. He later downloaded child pornography to personal devices, court records show.

Case files state the illegal online activity occurred between 2010 and 2014, which according to LinkedIn, was when Beeman served as an Army Corps of Engineers public affairs regional chief.

New York Times
Judge Shuts Down WhatsApp in Brazil
Tuesday, 03 May 2016
Byline: Vinod Sreeharsha

Rio de Janeiro - WhatsApp, a messaging service owned by Facebook, was shut down in Brazil on Monday after a court order from a judge who is seeking user data from the service for a criminal investigation. Judge Marcel Maia Montalvão ordered telecom companies operating in Brazil to suspend WhatsApp nationwide for 72 hours. As of just after midday Monday, Brazilians said they could not use the popular messaging service.

The shutdown is the latest twist in a case that has embroiled WhatsApp in legal trouble. The case, which is under seal, involves an organized crime and drug trafficking investigation in the court in Lagarto, in the northeastern state of Sergipe. The court has been seeking data from WhatsApp to aid in the investigation. Diego Dzodan, a Facebook executive, was briefly taken into custody in March for refusing to comply with orders to turn over WhatsApp information in the case.

The judge who ordered WhatsApp's shutdown on Monday is the same one who ordered Mr. Dzodan's arrest. Mr. Dzodan was released after one night when a higher court judge said the arrest was "an extreme measure."

"This decision punishes more than 100 million Brazilians who rely on our services," a WhatsApp spokesman said of the shutdown, adding that the company had cooperated to the "full extent of our ability with local courts."

The shutdown is the second time a Brazilian judge has ordered a nationwide ban of WhatsApp in the last few months. In December, a judge in São Paulo ordered telecommunications carriers to block WhatsApp for 48 hours because it had not complied with police eavesdropping requests in a separate criminal drug case.

An appeals court overturned the ban the same day it took effect, saying that "it was not reasonable" to suspend a service used by so many people simply because the company had not provided information sought by the courts.

A debate over law enforcement access to tech companies' data has been raging. In the United States, Apple recently grappled with a court order asking it to help unlock an iPhone used by a terrorist. Apple refused, leading to a standoff with the United States government that was tabled when the F.B.I. found an alternate way into the device.

American tech companies and law enforcement are now sparring over access to digital data in other venues, including Washington, where many are lobbying over a new draft encryption bill released last month by Senator Richard Burr, a North Carolina Republican and chairman of the Senate Intelligence Committee, and Senator Dianne Feinstein of California, the ranking Democrat on the committee.

Concern is growing in Brazil that its Congress may pass laws that would weaken digital privacy. One measure calls for Internet companies to remove content deemed critical of politicians within 48 hours, while another calls for imprisonment for violating an Internet's site's terms of use. The proposals worry many Internet privacy advocates, including the authors of Brazil's widely respected Internet bill of rights or Marco Civil.

The full Congress is considering several of these proposals and could vote on them this week.

On Monday, Brazilians took to Twitter to lament the loss of WhatsApp, which is used there as much by professionals as by students. But some appreciated the respite. @IZATLEITE, a Twitter user, wrote, "now without WhatsApp, I'll finally be able to read without being disturbed or interrupted."

Toronto Star
To Serve, Protect, Watch and Predict
Saturday, 07 May 2016
Byline: Alex Ballingall

Analysis: Try to imagine what policing will look like in the future. Microwave heat cannons and sound bazookas dispersing rowdy crowds? Robocops patrolling the streets while whirring drones keep watch from the sky?
Or maybe we'll arrive at a world where all crime is wiped away, where people peacefully coexist in sleeper pods while life is played out through virtual reality helmets.

Maybe.

The more realistic picture, according to police technology experts, is that surveillance and the collection and analysis of information will play a central role in solving and preventing crime.

The public safety regime of tomorrow, in other words, is all about data. "This is the future of policing," says Christopher Schneider, an associate professor of sociology at Brandon University in Manitoba.

Cops in the coming decades will gather information online, interact with the public through social media and even use data gleaned from the Internet and past crimes to predict and prevent future law-breaking, Schneider says. This is already happening, to varying degrees, in American cities and places such as Vancouver and Toronto, where police used a program to comb through Twitter to gather evidence for a recent online harassment trial.

"Policing as an apparatus is going to be much more mediated, and it's going to be much more community-oriented than it currently is, through the Internet, through social media," Schneider says.

"This is going to expand the gaze, as it were, toward crime and deviance."

The nexus between police and the public they serve has already expanded beyond the traditional 911 call (if you're even more of a troglodyte, just yell: "Help! Police!"). Ritesh Kotak, a police consultant for agencies in Canada and overseas, said tools like social media have created space for the "co-creating of public safety," with new and convenient avenues to report crimes and follow police data shared over the Internet.

"That's where it's headed with 'next generation 911.' That's where it's headed with the ability to see something and communicate right through our smartphones with police," Kotak said. "Data is the currency of the future."

With an open data mentality and deeper engagement through social media, Kotak added, police forces can repair and engender trust with the citizenry. "People feel like they're part of something," he said.

But data collection can also be used for more futuristic means. Ryan Prox, a special constable with the Vancouver Police Department, is one of the pre-eminent experts in the emerging field of "predictive policing." Prox prefers to call it crime "forecasting," in which police forces use complex computer programs that churn through mountains of data to try and predict when and where future crimes will occur.

This has yet to catch on in full force in Canada, but police in cities such as Los Angeles and Miami have signed on to "predictive" programs designed by companies such as PredPol, Prox explains. PredPol uses three data points -- time, place and type of crime -- to draw up boundaries in which crimes are most likely to occur, then local police patrol these areas in the hopes of catching the bad guys.

Prox cautions, however, that little independent scientific research has been done on these programs in the U.S. and suggests they may not be as accurate as their makers claim.

That's why he's spearheading a six-month predictive-policing pilot project in Vancouver, which began Feb. 1, that uses an intricate software program that has been designed by a team of mathematicians and geospatial engineers. The program sifts through crime data as far back as March 2001, including the time, place and nature of an offence, Prox says. But it also considers 60 "non-crime" factors, such as neighbourhood income, area traffic density, locations of illicit graffiti and even wind speed, to forecast the probability of a future crime being committed in the coming hours within a 100-metre radius of a given location.

Plainclothes cops will be dispatched to monitor these areas, with uniformed officers on standby to make an arrest in the event that a crime is witnessed, Prox says.

Tests have already shown a 60 to 70 per cent accuracy rate for some property crimes such as break and enters, which are easiest to predict because they're high frequency and often involve repeat offenders, Prox says. The more police use the program, the more data they have and the more accurate officials hope it can become.

"It sounds really sci-fi goofy," he laughs, "but they basically call it an 'artificial learning neural network.' That's the mathematical model."

The endgame of such programs, Prox says, is maximum police efficiency. In an era of ballooning police budgets -- now more than $1 billion a year in Toronto, for example -- that could be a welcome prospect.

But critics point to controversial information-gathering programs such as "carding" in Toronto, which many argue disproportionately target visible minorities.

To rely on such practices to fuel computer software programs that dictate how cops are deployed, could entrench existing police biases, Schneider says.

"Are we going to then be criminalizing certain people, certain segments of the population? Who are the police going to be looking at?" he asks.

Prox acknowledges this is a legitimate concern, but says the Vancouver police program only considers data from crime reports and other objective factors. It's generated by the public rather than fuelled by the cops themselves.

Others have brought forward concerns about how predictive policing will affect individual rights. Brenda McPhail, director of the Canadian Civil Liberties Association's Privacy, Technology and Surveillance Project, says the main worry is that the types of data currently used to forecast crime will expand to include more personal information -- social media posts, online purchase histories, travel bookings or location data from public Wi-Fi use.

This could not only invade individual privacy, it could erode the presumption of innocence, McPhail adds, citing court decisions in Canada and the U.S. that have suggested it is disproportionate to comb through data of many individuals to find a single criminal.

"The concern is that it is the thin edge of a wedge," she says. "Before any such programs are implemented, we as a society need to compare the benefits with the costs, particularly the costs to our rights and civil liberties. We need to consider the risks."

Such worries go beyond crime-forecasting programs.

Some point to privacy issues in the face of intensifying means of surveillance, such as the extensive camera networks that are used by police in Fresno, Calif., where police can monitor live feeds throughout the community through their Real Time Crime Center.

David Lyon, a Queen's University sociologist and head of the school's Surveillance Studies Centre, has argued that people's lives are being watched to the point that it already makes sense to label many western countries "surveillance societies." Lyon is co-author of a 2014 book on the subject, in which he and his colleagues argue we're at a "historic turning point" for the expansion of surveillance measures, developments with obvious consequences for privacy and state power.

Much of this can be viewed as part of a social shift toward a so-called "safety state," where more and more government policies - - and police actions -- are justified through fear of danger, says Charles Raab, a political science professor at the University of Edinburgh.

"As long as there are some plausible reasons to think we live in exceptionally dangerous times" -- such as terrorist attacks in big cities -- "there will be public fears and demands for more security and safety," says Raab. "Other values, such as equality, fairness and the exercise of rights and liberties, are constrained by the imperative to make everything safe and secure."

This isn't inevitable, Raab says. But with terrorism and climate change dominating the media and politicians routinely emphasizing this danger in their quests for votes, safety will continue to be a top social priority.

And that probably means the police of tomorrow will find ways to use our data and train cameras on us in an effort to keep us safe.

Mail on Sunday
Now Experts Say Don't Change Your Password
Sunday, 08 May 2016
Byline: Martin Beckford

London - It is one of the banes of modern life - you finally come up with a memorable yet secure password for your office computer, only to be told just a few months later that it has expired and you have to find a new one.
But now Britain's security services themselves have decreed that workers may be safer from hackers if they do not have to keep changing passwords. In a new briefing to Whitehall, power stations, banks and the public sector, cyber experts at CESG - the information security arm of intelligence agency GCHQ - concluded: 'It's one of those counter-intuitive security scenarios; the more often users are forced to change passwords, the greater the overall vulnerability to attack.'

The advice continues: 'Most password policies insist that we have to keep changing them. And when forced to change one, the chances are that the new password will be similar to the old one. Attackers can exploit this... New passwords are also more likely to be forgotten, and this carries the productivity costs of users being locked out... CESG now recommends organisations do not force regular password expiry.'

The advice comes as Ministers urge greater protection against cyber crime, after a survey found two-thirds of large businesses suffered an attack or security breach in the past year.

Fox News
Romanian hacker who claims he breached Clinton server says he spoke with FBI at length
Saturday, 07 May 2016
Byline: Catherine Herridge

Washington - The Romanian hacker who says he easily breached Hillary Clinton's personal email server also claimed, in a series of interviews with Fox News, that he spoke with the FBI at length on the plane when extradited from Romania to Virginia last month.

"They came after me, a guy from the FBI, from the State Department," 44-year-old Marcel Lehel Lazar, who goes by the moniker "Guccifer," told Fox News during a jailhouse phone interview. He said the conversation was "80 minutes ... recorded," and he took his own notes.

A government source confirmed that the hacker had a lot to say on the plane but provided no other details. Lazar was flown to the U.S. to face separate cyber-crime charges.

In addition to the apparent conversation with the FBI on the plane, Fox News has learned a meeting was expected as early as this week at the Alexandria, Va., detention center where he's being held involving Guccifer, the FBI, the U.S. attorney and the defendant's court- appointed lawyer.

These officials have not commented on his clams or detention.

An intelligence source close to the investigation, speaking with Fox News last month, questioned the timing of Lazar's extradition to the U.S., coming amid the Clinton email probe. As for what was discussed on that plane, Lazar said he told a State Department representative on the plane about "hot" data, some of which was hidden in Google drives, and other data that was too sensitive and deleted. The hacker, who offered no proof for his claims, said cryptically that he could not say more.

"I can't tell [you] now. I can't tell because I want to talk to the FBI. It is a matter of national security. Yeah," he said. Pressed by Fox News, Lazar seemed to indicate the data was not connected to the ongoing FBI criminal probe of Clinton's server.

Fox News recently met with Lazar in the secure visitor center in Alexandria, then followed up with a series of phone calls which he gave permission to be recorded. Separated by reinforced glass, Lazar was polite and methodical as he explained how he allegedly accessed the Clinton server in early 2013, by using her longtime confidant Sidney Blumenthal's AOL account as a stepping stone.

Fox News was first to report the hacker's claims of accessing the Clinton server, which he said "was easy."

Lazar said he got into the Blumenthal account by correctly guessing his security question, after doing extensive research on the web. He said his hacking always followed a "four step process": identify the target, do extensive web research on the target, access the target's account to harvest data, and send it out to the media.

Lazar said he was puzzled by the American media. He said he sent the Blumenthal emails, which is how the Clintonemail.com account first came to light, to many large news organizations in 2013, and it was The Smoking Gun that picked it up. Lazar said he started his "Guccifer archive," releasing materials in October and November 2012, and it ended "like August 2013."

Three cybersecurity experts said they found Lazar's explanation for accessing the Clinton server plausible but had questions.

Cybersecurity expert Morgan Wright explained how the FBI could marry up available evidence, including forensics or the configuration of the server and its folders, to assess his claims. "So we're going to map these things together, and if those things match up together, they're going to say 'yes, this was compromised,' then it means it was open to other people to compromise as well," he said.

Since Fox News reported on Guccifer's claims Wednesday, anonymous sources have reported that a review of the Clinton hard drives does not appear to indicate a breach. However, Wright and other experts warned that Clinton IT specialist Bryan Pagliano was the server's administrator and not principally a cybersecurity specialist - and may not have installed an adequate detection system for a Cabinet secretary's email.

"If you have a bank and you have one video camera when you need 20, then you missed it," Wright said. "If they weren't capturing all the activity, their security logs may say they didn't see anything."

Asked about Lazar's claims at Thursday's press briefing, State Department spokesman Mark Toner also said he's not aware of such an incident.

"We don't have any reason to believe that it might be true," he said.

At the same time, Toner repeatedly stressed he did not want to comment on the security of the server, citing ongoing investigations. Asked if he's in a position to even know whether Lazar's claims are true, Toner again said he did not want to comment. The Clinton campaign has rejected Lazar's claims, calling them "baseless" and emphasizing he is a convicted hacker.

Other cyber specialists like Bob Gourley with Cognitio warned there will "always be uncertainty and ambiguity" with hackers like Guccifer. But he said: "One thing I would say with certainty however -- if this computer were in a well- managed facility, where everything was being monitored and watched, we would have more information and ground truth."

Catherine Herridge is an award- winning Chief Intelligence correspondent for FOX News Channel (FNC) based in Washington, D.C. She covers intelligence, the Justice Department and the Department of Homeland Security. Herridge joined FNC in 1996 as a London- based correspondent.

Pamela K. Browne is Senior Executive Producer at the FOX News Channel (FNC) and is Director of Long-Form Series and Specials. Her journalism has been recognized with several awards. Browne first joined FOX in 1997 to launch the news magazine "Fox Files" and later, "War Stories."

London Free Press

Canada Revenue Agency hacker pleads guilty, says he's sorry
Saturday, 07 May 2016
Byline: Jane Sims

London - Stephen Solis-Reyes is one of those brainiac computer whiz kids who, it seems, was a little too smart for his own good.
Two years ago, when the London, Ont. man was just 19, and with what he maintains were the best of intentions, he was able to steal 900 social insurance numbers from the files of the Canada Revenue Agency. He says he wanted to demonstrate its online vulnerability to the Heartbleed computer bug.

The result was a sudden, panicked shutdown of the agency's website for four days that sent techno-fear shivers about online security across Canada and prompted the CRA to extend Canadians' tax-filing deadline by a week.

On Friday, now a top- notch computer science student at Western University, the 21-year-old pleaded guilty in an Ottawa courtroom to four charges.

Two were for mischief -- one for the Canada Revenue breach, another for exposing security breaches in JerseyMail, the now-defunct online arm of the postal service in Jersey, one of the Channel Islands off the coast of Great Britain.

The two other guilty pleas were to one count each of unauthorized use of a computer and obstructing a police officer by swiping information off a computer at his arrest.

"I want to express to Your Honour my most sincere regret and remorse for the wide-reaching effects of damage and harm my actions have caused to many different people and organizations," he wrote in a letter to the court.

"I truly understand the severity and gravity of the situation. I want to say that I never had any malicious intent and I never intended to cause harm or damage to anyone in any way."

The Crown dropped 13 other charges that, had be been convicted, could have sent him to prison for as long as 10 years.

For all of the national hubbub surrounding his activities in April 2014, Solis-Reyes was sentenced to an 18-month conditional sentence -- the first four months under house arrest, the rest under supervision.

The defence gave the judge more than 20 reference letters from professors, teachers, friends and family who spoke of Solis-Reyes' intellect and quiet, sensitive and respectful nature.

He's carrying a 98.6 per cent grade average in his fourth year and has already been named to the dean's honour list three times.

Assistant Crown attorney James Cavanaugh read an agreed statement that outlined how Solis-Reyes was able to breach the computer systems from his laptop computer.

Defence lawyer Faisal Joseph told the judge Solis-Reyes was able to get into the CRA system in "six seconds."

Central to the case, was Solis-Reyes' intentions. Joseph told the judge it would have been easy for Solis-Reyes to sell the information or make money off it. None of that happened.

"He did it because he could, because he was capable of breaking into these national security places," Joseph said, and that Solis-Reyes "has done the country a service" by exposing the flaws in the system.

One professor referred to him as "not only one of the smartest students around, but he is also one of the nicest, friendliest and most honest."

"His code is a thing of beauty," another wrote.

His father, Roberto Solis-Oba, the graduate chairman of Western's computer science department, wrote it was his son's "insatiable curiosity that led him to perform the actions that got him in trouble with the law.

The defence was harshly critical of what he alleges were the interrogation methods the RCMP put Solis-Reyes through after his arrest at his London home.

He said his client was questioned for six hours without a lawyer present. He was accused of being a terrorist and was asked "what would Jesus think" about his activities, Joseph said.

Joseph pointed out an RCMP corporal suggested Solis-Reyes's father's job could be in jeopardy and how, in France, it's not illegal to tie somebody up in a hot water tank until he speaks.

"In over 30 years of practising law as a prosecutor and a defence lawyer I have never met a better family or a more respectful, loving, intelligent boy as my client," Joseph said. "Murderers and rapists haven't expereince what my 19-year old client received at the hands of the RCMP's investigating officer for hours on end."

Reached for comment late Friday, the RCMP had not yet responded to the lawyer's characterization.

Solis-Reyes must serve two years of probation, with 200 hours of community service ordered.

He said in his letter he "will never again be in trouble with the law."

"This situation has taught me the importance of thinking before acting and I know every action I take has consequences."

Calgary Herald
Police trying to stay ahead of technology
Saturday, 07 May 2016
Byline: Kim Bolan

Calgary - Mounties were trying to investigate a threat to national security. But because they couldn't get critical information from a telecommunications company, they hit a roadblock.
Despite pursuing other investigative avenues, the case went nowhere, Chief Supt. Jeff Adam, director-general of the RCMP's technical investigation services, said in an interview.

"We spent roughly six months trying to design and implement a partial solution in order to get some of that data. But the gaps remained. And despite the judicial authorization, we've been unable to collect the evidence." The national security case is just one example of the obstacles police face as criminals and terrorists use cutting-edge technology to cover their tracks, Adam said. In another case, the RCMP got a court order "to intercept email messages between suspected criminals - high-level drug traffickers in Canada - and we could intercept, but we could not read the email traffic that they were sending," Adam said. "It was encrypted and this particular investigation involved some of our international law enforcement partners and we were unable to assist ourselves or them in getting the evidence."

Adam said the inability to decipher encrypted messages even when police get warrants is a challenge in many investigations - particularly those involving national security, organized crime and child exploitation.

Another issue, he said, is "lack of requirements for data retention by our telecommunications service providers."

Say police get a court order to obtain the text messages of a suspect in a case of threatening. But the company then tells investigators that it "doesn't keep anything more than 24 hours, so that evidence is therefore expunged from the system," Adam said.

On a recent trip to B.C., RCMP Commissioner Bob Paulson warned that while emerging technology has many benefits, "it's also changing criminality and it is putting us at risk and maybe you have to think that through more."

He cited the recent U.S. case where the FBI took Apple to court to get the iPhone of one of the San Bernardino terrorists unlocked. Apple refused. The FBI finally found a third party who could crack the password.

"It's just a taste of what's before us in terms of how we are going to go down this road," Paulson said. "It shouldn't be up to the police to say how we are going to roll. I think the community needs to engage because the threat is manifest."

Ann Cavoukian, executive director of Ryerson's Privacy and Big Data Institute, thinks police exaggerate the technological obstacles they face. And she said they rarely "point out the advantages they have from technology."

"It is deceptive because while it's true that occasionally they won't have access to one or two communications that have been encrypted, largely speaking they have more access now to a wide variety, a wide swath of information that they never had access to before," said Cavoukian, Ontario's former privacy commissioner.

"They're only pointing you to the small tiny percentage of cases where they might not be able to decrypt a phone because it has got end-to-end encryption. But that happens rarely."

The law-abiding public relies on encryption to protect sensitive personal information - often including health and banking records - that they now store on their phones.

"All of this information is accessed through your iPhone and you want people to be able to encrypt that safely to protect it from all the cyber attacks that are taking place," she said.

Cavoukian said there are huge privacy concerns with some of the technology police use in their investigations.

Media reports from a Montreal Mafia trial recently revealed that the RCMP had used a device known as a Stingray to intercept suspects' calls.

The device is controversial because it mimics a cellphone tower, allowing police to collect information from their targets' phones, but also from anyone else in the vicinity.

Last month, the office of the federal privacy commission confirmed it was investigating complaints about the RCMP's refusal to discuss its use of the Stingray device.

Cavoukian said the lack of transparency by police just increases the public's skepticism and distrust.

She said she has no problem with police getting proper warrants and getting the specific information they need for criminal investigations. But the fear is that law enforcement agencies have the ability to cast a wider net that unfairly ensnares lawabiding citizens, she said. She also acknowledged that the public puts its own privacy at risk with by using wireless devices and fitness trackers that can send personal information to "dozens of parties unbeknownst to the individual and the information can be used against them."

In a recent Pennsylvania case, a woman's claim to police that she'd been raped was disproven by her Fitbit data.

Le Journal De Montreal
Recrutés sur Instagram
Saturday, 07 May 2016
Byline: Hugo Jocas

Montréal - «Quelqu'un» a utilisé le réseau social Instagram pour tenter de recruter les jeunes arrêtés en mai 2015, selon la déclaration de la GRC à la Cour du Québec.
Un adolescent de Saint-Léonard «se sentait comme hypnotisé par le discours du suspect», selon son père, qui a appelé la police fédérale pour le dénoncer.

Son fils utilisait son téléphone iPhone pour naviguer sur Instagram et échanger avec le recruteur.

«L'homme lui a dit que vivre au Canada était péché, car ce n'est pas un pays musulman», mentionne la dénonciation de la police fédérale.

Le recruteur allégué utilisait toujours un profil différent sur Instagram pour communiquer, mais il commençait toujours par le même nom, caviardé dans le document de l'Équipe intégrée de sécurité nationale.

FAUX VOYAGE

L'adolescent avait fait croire à sa famille qu'il partait pour un voyage en Grèce avec son école.

Son père a interrogé la direction: aucun voyage n'était organisé. Il a alors confronté son fils, qui a éclaté en sanglots.

Contrairement aux autres, le jeune a été arrêté chez lui et non à l'aéroport.

Un autre des 10jeunes s'était rendu avec lui dans une agence de voyages pour s'informer sur le prix de billets pour Rome, avec escale à Istanbul, selon nos informations. Il avait acheté un billet, mais lui aussi a abandonné le projet.

Toronto Star
Reveal high-tech privacy violations: Editorial
Sunday, 08 May 2016

Editorial: We know Ottawa's electronic spy agency has violated the privacy of Canadians on multiple occasions. Indeed, the highly secretive Communications Security Establishment maintains a central database of such transgressions dating back to 2007.
What we don't know is how many such breaches have occurred. As reported by the Star's Alex Boutilier, the organization refuses to reveal this number, citing "operational security concerns." The CSE is evidently worried that disclosing the total might give Canada's enemies insight into its "capacity to conduct operations" and "the extent of its capabilities."

It's far more likely that what actually troubles this agency is having Canadians see its capacity for misconduct and the extent of its abuses.

To assure people that the principle of public accountability is being respected it's important for the CSE to level with Canadians and reveal how often it has violated their privacy.

There's no doubt wrongdoing has taken place. That was revealed earlier this year when Parliament was told the electronic eavesdropping agency had inadvertently shared Canadians' "metadata" with foreign allies.

This class of information can include the destination and duration of phone calls, emails, and text messages. To protect privacy, such material was supposed to be scrubbed of key details before being passed along to other members of the "Five Eyes" alliance -- the United States, United Kingdom, Australia and New Zealand. But the CSE learned, in 2013, that a technical glitch had resulted in a leak of confidential data.

It informed government officials but kept the mistake hidden from the Canadian public for two years. This gives rise to an obvious question: how many other privacy violations might this agency be keeping secret?

As reported by Boutilier, documents tabled in Parliament last month show the CSE admitting to 13 privacy and information breaches in 2015, affecting at least 630 people. None of these cases were reported to Canada's privacy commissioner on grounds that they posed "no significant risk" to anyone.

It's hard to see how presenting a similar tally, dating back to 2007, would pose a serious security threat. It would, however, give Canadians some insight into how well their rights are being protected.

The Liberal government came to office promising a new level of openness and accountability. Responsibility for fulfilling that pledge now rests with Treasury Board President Scott Brison. And a good place for him to start would be to let Canadians know how often their privacy has been violated by a shadowy agency that refuses to fully answer even to this country's information and privacy commissioner.

BDNews24
Technicians from SWIFT left Bangladesh Bank exposed to hackers
Monday, 09 May 2016

Dhaka - The technicians introduced the vulnerabilities when they connected SWIFT to Bangladesh's first real-time gross settlement (RTGS) system, said Mohammad Shah Alam, the head of the criminal investigation department of the Bangladesh police who is leading the probe into one of the biggest cyber-heists in the world.
"We found a lot of loopholes," Alam said in an interview in Dhaka. "The changes caused much more risk for Bangladesh Bank."

He and a senior central bank official said the SWIFT employees made missteps in connecting the RTGS to the central bank's messaging platform.

The technicians did not appear to have followed their own procedures to ensure the system was secure, according to the Bangladesh Bank official, who said he was not authorised to publicly comment because of the ongoing investigation.

Because of this, SWIFT messaging at the central bank was widely accessible, including remote access with only a simple password, police said. It had no firewalls and only a rudimentary switch. "It was the responsibility of SWIFT to check for weaknesses once they had set up the system. But it does not appear to have been done," said the bank official.

SWIFT's chief spokeswoman Natasha de Teran said she had no comment on the allegations by authorities in Bangladesh. She also declined comment on any aspect of the Bangladesh project, including whether the firm had deployed any employees or outside contractors to Bangladesh Bank.

Reuters was not able to independently verify the allegations by Bangladeshi officials about the SWIFT technicians. If they are validated, however, that could undermine confidence in the cooperative that is the backbone of global financial transactions.

The officials in Dhaka discussed their findings with Reuters ahead of a meeting this week in Basel, Switzerland where Bangladesh Bank officials have said their governor and a lawyer appointed by the bank will discuss recovery of about $81 million stolen by the hackers with the head of the Federal Reserve Bank of New York and a senior executive from SWIFT.

Bangladesh Bank officials have said they believed SWIFT, and the New York Fed, bear some responsibility for the February cyber heist. SWIFT has declined comment on that claim.

The RTGS, which enables domestic banks and the central bank to settle large transfers between themselves, was installed at Bangladesh Bank in October last year and then connected to SWIFT. In

February, hackers sent fraudulent messages, ostensibly from the central bank in Dhaka, on the SWIFT system to the New York Fed seeking to transfer nearly $1 billion from Bangladesh Bank's account there.

Most of the transfers were blocked but about $81 million was sent to a bank in the Philippines and much of that money remains missing.

A spokesman for Bangladesh Bank declined comment on the investigation into the heist. He said, however, that RTGS continued to work well, noting that a large number of countries use SWIFT messaging for similar systems. "There is no inherent risk in this," he said.

According to the Bangladeshi police, the technicians linked the RTGS to SWIFT computers on the same network as about 5,000 central bank computers that are accessible from the open Internet.

Instead, they should have set up a separate local area network, or LAN, that could not connect to the rest of the bank or the Internet, police said.

The technicians also failed to install a firewall between the RTGS and the SWIFT room so that the bank could block malicious traffic from coming into the facility.

When they installed a networking switch to control access to SWIFT, they chose to use a rudimentary old one they had found unused in the bank, rather than a more sophisticated, managed switch that gave the bank the ability to control access to the network, police said.

During the job, the technicians set up a wireless connection so they could access computers in the locked SWIFT room from other offices inside the bank. When they finished, they failed to disconnect the remote access, which was only secured with a simple password, police and the bank official said.

They also failed to disable a USB port on the computer attached to the SWIFT system, as is usual for critical networks to prevent malicious software from being installed through a tainted thumb drive, police said. Police did not provide any evidence for any of the assertions.

But another central bank official familiar with the SWIFT room operations confirmed that the port was "active" until the heist came to light. He had no explanation. The hackers used malicious software to modify the SWIFT messaging software to help hide their tracks.

Bangladeshi police said they have asked SWIFT to facilitate interviews with the SWIFT technicians. "Whether it is intentional or negligence, we are trying to find out," said Alam.

SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, is used by about 8,000 banks around the world to order funds transfers and other communications. It is connected to RTGS systems installed at scores of banks worldwide, and there have been no reports of problems elsewhere

with connections between those two systems. The US FBI, which is leading investigations into the case, has made no comment so far.

New York Fed executive Richard Dzina said at a conference last week that bank workers "acted properly" in releasing the funds. The system was penetrated, he said, because the hackers had acquired valid credentials to order the transfers

Former central bank governor Mohammed Farashuddin, who is heading an internal probe by Bangladesh Bank into the heist, said SWIFT needed to review its technology in the wake of the heist.

"It seems to be a case of extreme carelessness," he told Reuters. He declined to provide more details saying a final report was due in the next few weeks.

Agence France-Presse
Indonesia's Muslim cyber warriors take on IS
Monday, 09 May 2016

Jakarta - A group of Indonesian "cyber warriors" sit glued to screens, as they send out messages promoting a moderate form of Islam in the world's most populous Muslim-majority country.
Armed with laptops and smartphones, some 500 members of the Nahdlatul Ulama (NU) -- one of the world's biggest Muslim organizations -- are seeking to counter the Islamic State group's extremist messages.

"We'll never let Islam be hijacked by fools who embrace hate in their heart," tweeted Syafi' Ali, a prominent member of the NU's online army, a typical message to his tens of thousands of followers.

They are trying to hit back at IS's sophisticated Internet operations, which have been credited with attracting huge numbers from around the world to their cause.

Internet propaganda is believed to have played a key role in drawing some 500 Indonesians to the Middle East to join IS, particularly among those living in cities where it is easier to get online.

The dangers of the growing IS influence in Indonesia were starkly illustrated in January when militants linked to the jihadists launched a gun and suicide bombing attack in Jakarta, leaving four assailants and four civilians dead.

It was the first major attack in Indonesia for seven years, following a string of Islamic militant bombings in the early 2000s that killed hundreds.

As well as firing off tweets, the NU members have sought to dominate cyberspace by establishing websites promoting the group's moderate views, an Android app and web-based TV channels, whose broadcasts include sermons by moderate preachers.

The initiative has been building momentum for a while but started to pick up pace a few months ago. A handful of cyber warriors operate from a small office in Jakarta, while the rest work remotely, and the group mostly communicate with one another over the web.

But it will be an uphill battle and the NU, which has been promoting moderate Islam for decades, conceded they have previously struggled to take on IS's hate-filled messages.

"NU has for a while wrestled with this radical propaganda," said Yahya Cholil Staquf, secretary general of the NU, which claims at least 40 million followers. "Every time we defeated them, it didn't take long for them to regain their strength."

The online drive comes as the NU is set to take its campaign to promote their tolerant form of Islam onto the international stage this week, with a two-day meeting from Monday of moderate religious leaders from around the world.

They aim to showcase their particular brand of the Muslim faith, known as "Islam Nusantara", to counter the IS jihadists' radical interpretation of Islam.

Meaning "Islam of the Archipelago" -- Indonesia is the world's biggest archipelago, comprising over 17,000 islands -- it is accepting of diversity and stresses non-violence.

It grew up organically in Indonesia, as the religion entered the country gradually and had to mix with existing traditional beliefs such as praying at tombs, making it a naturally tolerant form of Islam.

Nowadays, most of the approximately 225 million Muslims in Indonesia practice a moderate form of Islam.

The NU wants to persuade Muslims from around the world to look for inspiration to Indonesia, where religious minorities and a multitude of ethnic groups mostly coexist harmoniously, rather than to harsher forms of Islam from the Middle East.

The group nevertheless has a long way to go to fight the rising tide of IS propaganda. Despite their good intentions, the NU cyber warriors appear amateur next to IS's well-funded set-up.

The jihadists, who control huge swathes of territory in Iraq and Syria, have a sophisticated online operation, using social media, apps and slickly produced videos.

They send about 200,000 tweets a day into the United States alone, according to US officials. It even has its own news agency, Amaq, which is often the first to report that IS is claiming responsibility for attacks.

In Indonesia, there are two main ways that IS propaganda spreads -- by supporters posting on websites and apps such as Whatsapp, Facebook, Twitter and Line, and through returnees from the Middle East preaching the group's radical ideology.

Most of the NU's online army are volunteers, often reaching into their own pockets to cover costs.

"ISIS has oil, while the only oil we have is for hair," Ali said, explaining the project's start was delayed for more than a year due to funding problems. Oil smuggling has been a key revenue source for IS.

Robi Sugara, a terrorism expert from NGO the Indonesian Muslim Crisis Center, welcomed the NU's online approach. "It's a good strategy to make Google searches fill up with moderate Islamic content," he told AFP.

"The battleground for Islamic ideology has moved to the Internet, and by producing as many moderate websites as they can, they can keep more minds healthy."

Haaretz
Classified Documents Stolen From Israel Police Cybersecurity Expert
Monday, 09 May 2016
Byline: Yaniv Kubovich

Jerusalem - Thief presumably used a grabber tool to filch the folder from a table through an open window, together with the officer's house and car keys. A file folder containing classified documents was stolen on Thursday from the central-Israel home of a police expert in computer security.
The Walla Hebrew-language news site reported that the deputy head of the cyber security division of the Israel Police left the folder on a table after returning home. The assumption is that the unknown thief used a long-handled rake or other instrument to grab the folder, as well as the officer's key ring, through a window. The thief then apparently entered the house using the keys and stole a wallet before fleeing.

The police are investigating and have notified security agencies that could potentially be affected by the theft of critical information. The fact that neither valuables nor the officer's unmarked car were stolen suggest that the motive may have gone behind simple financial gain.

The official was not identified -- the Israel Police said this was in order to protect the official's privacy, but it is known that he was recruited into the police from the army's signal intelligence unit 8200.

All possible motives for the theft are being explored, however, including simple theft.

Haaretz recently reported on the disappearance of 27 files from the police station in the Tel Aviv suburb of Givatayim under unclear circumstances.

About a month ago, police officers from the station went on vacation to Eilat. On their return, one investigator noted the disappearance of the files, which had been either awaiting investigation or were to be transferred to other offices. This case too involved sensitive files that appeared to be left unprotected.

Khaleej Times
The future of media? It's digitization
Monday, 09 May 2016
Byline: Bernd Debusmann Jr.

Dubai - Digitisation is setting the future of the media industry in the Middle East and North Africa as increased broadband usage leads to soaring use of portable devices, according to the newly-released fifth edition of the Arab Media Outlook.
The report, which was released on Sunday, highlights the current media landscape of 14 Arab countries, and identifies future trends that will shape the industry between 2016 and 2018.

In 2015, according to the report, the digital sector accounted for 15 per cent of the Mena's media industry, which was valued at over $11.36 billion. In 2020, that number is expected to rise to 27 per cent. In that same time, the total size of the Mena media industry is expected to rise by 3.7 per cent to over $13.63 billion.

Mona Ghanim Al Marri, president of the Dubai Press Club, said that the findings brought into stark focus the need to find solutions that allow for "effective competition" between media outlets, and ways in which to couple digital media platforms and traditional media outlets, as well as using these platforms to maintain the position of media and develop content.

Print media - which in 2015 represented 45 per cent of the region's media industry - is expected to decline to 31 per cent. In the Mena region, a total of 41 per cent of the average time spent on media in 2015 - 11 hours - is done online, compared to 49 per cent in the UK and 47 per cent in Australia.

Al Marri also noted the noticeable growth of the paid media sector compared to advertising sector, where spending on advertising is set to increase by 2.5 per cent annually between 2016-18, while spending on paid media is set to grow by 3.7 per cent.

Paid media, the report notes, will largely by backed by the growth of video games, which will account for over $1.14 billion in revenue in 2018, 62 per cent of which will be driven by social gaming, compared to

52 per cent in 2015. Paid TV revenue, for its part, is expected to grow 10 per cent in the same timeframe, to over $1.53 billion.

"While paid media is a synonym of 'excellent content', we should stop at this noticeable progress and think about what our local and Arab media should do in terms of development steps, to keep pace with the rapid changes," Al Marri said.

Notably, digital video is expected to form 30 per cent of the media industry by 2018. Already in 2015, video accounted for an average of 71 minutes of daily time spent by 15-to-24-year-olds, compared to 51 minutes on social networks, 29 minutes on search engines and business sites, and only 14 minutes on news websites.

Dr Amina Al Rustamani, group chief executive officer of Tecom Group - of which Dubai Media City is part - noted that a careful study of the findings will be crucial in forming future media and communications strategies.

"The dynamics and trends of the media industry have always provided valuable insight into consumer behaviour and have helped shape the thinking of government and business as to what are the most effective means of communication with their citizens and customers," she said. "Launching the Arab Media Outlook Report 2016-2018 is especially timely and relevant, against a backdrop of a paradigm shift in the media industry, and unprecedented change and innovation. This report enables us to guide our partners in forming their own strategies for growth."

A print version of the executive summary of the report will be available during the 15th edition of the Arab Media Forum, to be held on Tuesday and Wednesday at the Dubai World Trade Centre.

Albert Oil
How To Do Business in Brazil
Monday, 09 May 2016
Byline: Staff reporter

After raising the hopes of foreign investors in Brazil and opening up its vast reserves to overseas drillers, the country's political system has lurched into instability recently with millions of people taking to the streets demanding the president's head over a vast corruption scandal at state-owned Petrobras, which operates globally.
Niko Resources of Alberta has offshore exploration assets in Brazil, as does Brasoil.

Opportunities

In 2014, Brazil produced 2.95 million b/d of oil-- up 9.5 percent from 2013--making it the world's ninth-largest producer. The U.S. Energy Information Administration (EIA) estimates that in 2015, Brazil had 15

billion barrels of proved oil reserves, second only on the continent to Venezuela. More than 94 percent of Brazil's reserves are located offshore. About a quarter of its output comes from the deep water presalt layer, where production hit a record 865,000 b/d in 2015 as new wells came on stream in the Santos basin.

Brazil opened up to private and foreign investment in 1997. Canadian companies brought their offshore Atlantic experience to the table. Some service firms went inland. Weatherhaven, on the heels of the visit of former prime minister Stephen Harper to Brazil, closed a deal to build exploration camps for production in the Amazon. Gran Tierra Energy entered onshore Brazil in 2009, following Encana, and later entered the offshore in 2011 with Statoil and Petrobras in the Camamu-Almada basin. Canadian firms operate some of those blocks, including Brasoil, and Calgary's Tuscany International Drilling. Tuscany went there looking for year-round work, instead of the seasonal cash flows of Alberta, although the company has since gone bankrupt.

Risks

In 2013, Brazilian President Dilma Rousseff accused the Communications Security Establishment Canada (CSEC) of spying on Brazil's Ministry of Mines and Energy. She based her intelligence on documents leaked to Brazilian media by Edward Snowden. Snowden worked for the U.S. National Security Agency--the counterpart of Canada's CSEC. It's alleged that the Harper government spied to provide Canadian energy firms with intelligence to give them the edge over rivals when bidding for concessions. Today, Rousseff is fighting for her political survival as she faces impeachment for allegedly cooking the books to hide a budget deficit, and millions of people have taken to the streets as a massive corruption scandal at state-owned oil giant Petrobras threatens to bring down the government.

Police picked up former president Luiz Inacio Lula da Silva, Rousseff's mentor, for questioning in a federal investigation, dubbed "Operation Carwash," into a corruption scheme that apparently turned Petrobras into a giant slush fund for the ruling Workers' Party. The former president was questioned about allegedly receiving illicit kickbacks from Petrobras in the form of cash payments and luxury real estate. Rousseff quickly made da Silva a member of her cabinet to protect him from prosecution. Many of Brazil's top figures in business and politics have been implicated in deepening the worst recession in decades in South America's biggest economy.

As well as navigating Brazil's muddy political torrents, Canadian firms have to deal with blowback from neighboring nations. Amazon tribespeople from Peru and Brazil have joined forces to stop Toronto's Pacific Rubiales from allegedly destroying land and putting at risk the lives of uncontacted tribes. Pacific Rubiales is exploring in Block 135 in Peru, which is an area proposed as a reserve for uncontacted tribes

Gulf Daily News
Security technologies 'crucial for aviation industry'

Monday, 09 May 2016

Manama - Security technologies like encryption, intrusion protection, firewalls and right technical design and architecture are critical to ensure sustainable growth of the aviation industry, a leading expert has said.
According to Gulf Air's director of information technology (IT) Dr Jassim Haji, the incidence of cyber attacks against airlines around the world has been rising as has the damage and loss they have caused.

Addressing leading IT industry experts at global market intelligence and advisory provider International Data Corporation's Security Roadshow in Bahrain, Dr Haji said a diverse digital ecosystem had brought security to the forefront as it underpinned every operation, process and service within the industry.

Explaining how latest technologies and phenomena like mobile, social, cloud and Big Data had brought benefits to the industry, he said there had also been an increase in risks as well as actual and potential threats. "Airlines hold private and confidential information about their passengers and it is critical that this information was protected and kept safe from unauthorised access or manipulation," he said.

This, he added, assumes greater significance in the case of governments and border controls which are custodians of sensitive information about passengers with possible national security implications.

Talking about new generation of aircraft, Dr Haji said every equipment and part has become a piece of electronics thus becoming susceptible to external manipulation and control. He said all airlines needed to have a cutting-edge risk management framework that would be used to efficiently identify potential risks, their impact, likelihood of occurring, mitigation plans and regular assessments of such risks.

Referring to drones as one of the new and obvious risks, Dr Haji said they were increasingly becoming uncontrolled and unmanaged, citing a recent incident at an airport in London where an aircraft was hit by a drone as an example of the damage that can occur from this unmanaged state.

He also emphasised that initiatives based around becoming "smart," were bringing about a need for secure, open platforms. "The culture of security has to be instilled in every single employee so they protect their own company and act vigilantly." Dr Haji also serves on the SITA Council and sits on the board of directors of a leading hospitality and tourism technology provider in the Middle East.

Through his myriad initiatives, he has managed to achieve 26 top Middle-Eastern technology awards for Gulf Air, including best project implementations for cloud computing, virtualisation, Big Data, mobility applications and IT security. Held at the Diplomat Radisson Blu Hotel, Residence and Spa, the event saw participation from more than 100 professionals and executives.

Sky News (UK)
Small Firms 'Underinvesting' In Cyber Security

Monday, 09 May 2016

London - Half of small manufacturers in the UK have failed to increase cyber security investment in the past two years, according to a survey.
Research by manufacturers' organisation EEF found that 56% of businesses have not increased their spending.

A fifth fail to make employees aware of cyber risks, while only 56% say cyber security is given serious attention by their board.

Just over a third, or 36% of manufacturers, have an incident response plan in place, and only 24% monitor cyber threats.

EEF Chief Economist Lee Hopley, is urging manufacturers to step up their planning to counter the increasing number of cyber threats.

"As technology and data start to play increasingly critical roles in manufacturing, companies will inevitably find themselves more vulnerable to cyber breaches," said Mr Hopley.

"Our survey highlights that investment in new technology isn't being matched by investment in managing risks, especially among smaller firms.

"It is important that manufacturers are able to identify, understand and put the correct strategies in place to keep their businesses safe and cyber secure."

The Government has also called for industries to act to protect themselves while announcing it will launch a National Cyber Security Centre this autumn and spend £1.9m over the next five years.

Its research revealed that 90% of large businesses and 74% of small businesses reported cyber security breaches last year. Average breaches cost up to to £3.14m for large firms and up to £311,000 for small businesses.

A quarter of large firms come under attack at least once a month, according to the Department for Culture, Media and Sport.

The research shows the most common attacks detected involved viruses, spyware or malware and could have been prevented using the Government's Cyber Essentials scheme.

A TalkTalk cyber attack last year cost the telecoms group up to £45m and triggered a sharp drop in customers.

Washington Free Beacon
Obama Policies Toward Hackers From China, Iran, Syria Produce Few Results
Monday, 09 May 2016
Byline: Bill Gertz

Column - Recent federal indictments of Iranians and Syrians for cyber attacks on U.S. networks further highlight the failure of President Obama and his administration to counter the growing threat of foreign hacker strikes on American networks.
In March, the Justice Department indicted two groups of hackers, one from Iran linked to cyber intrusions of an industrial control system operating a New York dam, and a second from Syria engaged in illegal activities that included causing damage to computers and extortion.

The indictments are largely symbolic, since none of the Iranians or Syrians are within reach of U.S. law enforcement and the chances the hackers will ever face justice in a courtroom are slim.

Like many of President Obama's foreign policies, the indictments appear designed to provide the president and his administration with political cover by adopting seemingly proactive measures, but without having much impact.

The approach to cyber threats coincides with the president's generally pacifistic approach to foreign affairs, which he is reported to have summed up as "don't do stupid shit." In practice, this approach often amounts to doing as little as possible, and doing nothing that might require the use of military force.

The policy was captured in a New York Times profile last week of Ben Rhodes, the White House deputy national security adviser for communications who was described as "The Boy Wonder" of the White House.

Leon Panetta, who served as CIA director and defense secretary under Obama, explained that the president's approach to foreign affairs has been dominated by the desire to avoid possible conflicts.

"I think the whole legacy that he was working on was, 'I'm the guy who's going to bring these wars to an end, and the last goddamn thing I need is to start another war,'" Panetta said of Obama's approach to Iran and the nuclear deal. The former defense secretary said the president believes that "if you ratchet up sanctions, it could cause a war. If you start opposing their interests in Syria, well, that could start a war, too."

On cyber security, the president and his advisers have rejected policy options from military and civilian national security experts since at least 2011 for a show of force in cyberspace against China or other states and groups engaged in widespread cyber attacks, according to officials familiar with internal discussions.

Private industry, which is barred by federal statute from conducting its own cyber counterattacks, has pressed the White House and the U.S. intelligence community to do more against the onslaught of hacks. So far the response has been a firm "no" from the president.

Symbolic indictments or other diplomatic measures have not worked to deter cyber attacks. The FBI announced in July it was revamping its cyber counter- espionage unit after logging a 53 percent increase in its caseload.

A State Department security report published on March 30 noted that in the indictments of the Iranian Syrian hackers, U.S. private sector institutions were the main victims.

"These cyber attacks resulted in disrupted customer communications, data infringement, and significant financial losses," the report said, adding, "the hackers will likely not face prosecution in the U.S. for their actions ... [h]owever, some analysts believe the U.S. government will continue publicly blaming foreign hackers in an effort to deter future attacks."

The indictments followed a similar May 2014 action by the Justice Department against five Chinese military hackers who also remain out of reach of law enforcement and who likely will never be brought to trial.

The indictment was a response to Chinese government denials to the Justice Department about its cyber activities and a demand to produce legal evidence implicating China's cyber warfare troops in what the United States has charged is widespread theft of corporate and government secrets.

John Carlin, the Justice Department's national security chief, explained that the indictment was simply following through on Beijing's dare.

"We heard directly from the Chinese who said, 'If you have evidence, hard evidence, that we're committing this type of activity that you can prove in court, show us.' So we did," Carlin told a security conference months after the indictment.

A short time after the indictment, the Chinese military was linked to the theft of 80 million records from Anthem, the American health care provider. Then came the pillaging, also by Chinese military hackers, of Office of Personnel Management networks. The hack resulted in the loss of another 22 million records, including sensitive data from background investigations for security clearances.

Obama came close to imposing sanctions on the Chinese for the large-scale data hacking but backed off in September during the visit to Washington by Chinese President Xi Jinping, who promised to halt Chinese economic espionage in cyberspace. U.S. intelligence officials recently told Congress they were unable to verify that the Chinese ended the cyber attacks, a clear indication they have continued.

The State Department report, produced for a public-private partnership called the Overseas Security Advisory Council, or OSAC, said the indictment of Chinese military hackers was an "an unprecedented announcement, publicly blaming the Chinese government for espionage against the U.S. private sector."

"The five indicted Chinese military officers have also not yet been brought to court in the U.S.," the report said. "However, this case was among the first to highlight the threat of intellectual property theft from a nation-state, which remains a concern among many OSAC constituent organizations operating overseas."

The report said the indictments of the Iranians and Syrians highlighted the "blended threat" posed by foreign government and non-government hackers. It also showed that cyber attacks were behind the economic espionage confirmed in the PLA case, including cyber denial-of-service, intimidation, and extortion activities.

"The threat to the private sector is heightened as hackers look to carry out these various operations for both professional and personal gain," the report said.

"The traditional categories of threat actors-- nation-state, criminal, politically-motivated--no longer define all of the malicious network activity affecting U.S. private sector organizations," it added. "The 'blended threat' of hackers who are willing to work as proxies for governments or other organizations can hinder detection and prosecution in multiple ways."

The use of non-state hackers for foreign government cyber attacks makes it more difficult for authorities to identify the attackers, and allows nation-states or terrorist groups to benefit from the technical expertise of private sector hackers.

Additionally, proxies give foreign governments what spy agencies call plausible deniability--a key information warfare tactic allowing governments to avoid being linked to cyber attacks, the report said.

The report concluded that the recent indictments of Chinese, Iranian, and Syrian hackers "are unlikely to deter malicious cyber actors from exploiting this blended threat to target the U.S. private sector."

As Obama winds down his final term as president, it appears one of his legacies will be an unwillingness to take effective steps to counter cyber attacks against the United States that have caused serious damage to U.S. security.

As former NSA Director Keith Alexander has said, China is stealing everything it can to boost its economy. "It's intellectual property, it's our future. I think it's the greatest transfer of wealth in history," Alexander said.

New Zealand Herald

IRD team to sift through papers on foreign-owned trusts
Sunday, 08 May 2016
Byline: Nicholas Jones

Canberra - The IRD has set up a team to sift through documents about foreign-owned trusts from the Panama Papers.
A cache of material from the leak of documents from the Panamanian law firm Mossack Fonseca is due to be released today. Prime Minister John Key said the information could lead to law changes.

"It is quite useful that the Panama Papers get released," Mr Key said, "if that helps assist the New Zealand Government in making improvements to any of the laws that we have, or the partners that we work with like the OECD."

He said he did not condone the hacking of private information, but now that information would be released "there might be some benefits to gain from that".

Any New Zealanders found to be avoiding tax could expect a "knock at the door", he said, and if there was evidence of trusts being used improperly by foreigners the rules could be tightened.

Labour leader Andrew Little said the Prime Minister's tone had changed.

"There may well be now a rapidly changing position, which is because they discovered that, actually, most New Zealanders don't like this, and don't like us to be party to this."

Talk of the IRD investigating Kiwis was something of a distraction, he said, when the real issue was the use of the trusts by foreigners to avoid tax.

Labour wants the foreign trust industry shut down, but Mr Key called that a "knee-jerk" reaction.

Following the first release of details from the papers last month, the Government began a review of the disclosure rules for NZ's foreign trusts. Opposition parties have criticised the review's narrow focus.

An article in the Australian Financial Review on Friday shed new light on the number of foreign investors who had moved their cash and assets into tax-free New Zealand-based trusts, and the way these investors were able to minimise their tax.

It also said Auckland-based lawyer Ken Whitney, whose clients include Mr Key, had written a reference for Auckland law firm Cone Marshall to get accreditation with Mossack Fonseca in 2009.

After the release of the papers, Mr Key said Mr Whitney had assured him he had not had any dealings with Mossack Fonseca.

Yesterday the Prime Minister said the reference did not contradict that: "People give references all of the time."

Wall Street Journal
Twitter Bars Intelligence Agencies From Using Analytics Service
Monday, 09 May 2016
Byline: Christopher S. Stewart, Mark Maremont

New York - Twitter Inc. cut off U.S. intelligence agencies from access to a service that sifts through the entire output of its social-media postings, the latest example of tension between Silicon Valley and the federal government over terrorism and privacy.
The move, which hasn't been publicly announced, was confirmed by a senior U.S. intelligence official and other people familiar with the matter. The service--which sends out alerts of unfolding terror attacks, political unrest and other potentially important events--isn't directly provided by Twitter, but instead by Dataminr Inc., a private company that mines public Twitter feeds for clients.

Twitter owns about a 5% stake in Dataminr, the only company it authorizes both to access its entire real-time stream of public tweets and sell it to clients.

Dataminr executives recently told intelligence agencies that Twitter didn't want the company to continue providing the service to them, according to a person familiar with the matter. The senior intelligence official said Twitter appeared to be worried about the "optics" of seeming too close to American intelligence services.

Twitter said it has a long-standing policy barring third parties, including Dataminr, from selling its data to a government agency for surveillance purposes. The company wouldn't comment on how Dataminr--a close business partner--was able to provide its service to the government for two years, or why that arrangement came to an end.

In a statement, Twitter said its "data is largely public and the U.S. government may review public accounts on its own, like any user could."

The move doesn't affect Dataminr's service to financial industry, news media or other clients outside the intelligence community. The Wall Street Journal is involved in a trial of Dataminr's news product.

Dataminr's software detects patterns in hundreds of millions of daily tweets, traffic data, news wires and other sources. It matches the data with market information and geographic data, among other things, to determine what information is credible or potentially actionable.

For instance, Dataminr gave the U.S. intelligence community an alert about the Paris terror attacks shortly after they began to unfold last November. That type of information makes it "an extremely valuable tool" to detect events in real time, the intelligence official said.

In March, the company says it first notified clients about the Brussels attacks 10 minutes ahead of news media, and has provided alerts on ISIS attacks on the Libya oil sector, the Brazilian political crisis, and other sudden upheaval in the world.

U.S. government agencies that used the Dataminr service are unhappy about the decision and are hoping the companies will reconsider, according to the intelligence official.

"If Twitter continues to sell this [data] to the private sector, but denies the government, that's hypocritical," said John C. Inglis, a former deputy director of the National Security Agency who left in 2014. "I think it's a bad sign of a lack of appropriate cooperation between a private-sector organization and the government."

Analysis of Twitter and other social-media services has become increasingly important to intelligence and law-enforcement agencies tracking terror groups. Islamic State posts everything from battlefield positions to propaganda and threats over Twitter. San Francisco-based Twitter deletes thousands of accounts a month for violating its antiterror policies, but Islamic State supporters create new accounts almost as quickly.

"The volume of the group's activity on Twitter yields a vast amount of data that is a crucial tool for counterterrorism practitioners working to manage threats," said Michael S. Smith II, chief operating officer of the security consulting firm Kronos Advisory. "Twitter's decision could have grave consequences."

In a speech last September, David S. Cohen, a deputy director of the Central Intelligence Agency, discussed the importance of "open source" social-media data gathered by the CIA, saying Islamic State's "tweets and other social- media messages publicizing their activities often produce information that, especially in the aggregate, provides real intelligence value."

Silicon Valley and the U.S. government have been locked in intensifying conflicts over cooperation since the revelations by former National Security contractor Edward Snowden about government surveillance of electronic communication.

Most recently, Apple Inc. and the Justice Department were embroiled in a legal showdown over demands by the Federal Bureau of Investigation to unlock an iPhone used by one of the killers in the San Bernardino, Calif., attack in December. That fight--which unlike the Dataminr product involved the release of private data--ended in March when the FBI found another way to access the phone.

In-Q-Tel, a venture-capital arm of the U.S. intelligence community, has been investing in data-mining companies to beef up the government's ability to sort through massive amounts of information. In-Q-Tel, for example, has invested in data-mining firms Palantir Technologies Inc. and Recorded Future Inc.

U.S. intelligence agencies gained access to Dataminr's service after an In-Q-Tel investment in the firm, according to a person familiar with the matter.

When a pilot program arranged by In-Q-Tel ended recently, Twitter told Dataminr it didn't want to continue the relationship with intelligence agencies, this person said.

"Post-Snowden, American-based information technology companies don't want to be seen as an arm of the U.S. intelligence community," said Peter Swire, a Georgia Institute of Technology law professor and expert on data privacy.

Dataminr, based in New York, was launched seven years ago by three former Yale University roommates. A financing round early last year valued it at $700 million, according to Dow Jones VentureSource.

Its product goes beyond what a typical Twitter user could find in the jumble of daily tweets, employing sophisticated algorithms and geolocation tools to unearth relevant patterns.

Dataminr has a separate, $255,000 contract to provide its breaking news-alert service to the Department of Homeland Security, which is still in force.

Associated Press
Lawmakers, advocates push to reveal extent of surveillance
Monday, 09 May 2016

Washington - Even though the bulk collection of Americans' telephone records has ended, calls and emails are still being swept up by U.S. surveillance work targeting foreigners. Congress is making a renewed push to find out how many.
Six Republicans and eight Democrats on the House Judiciary Committee have asked the nation's top intelligence official for the number of Americans' emails and phone calls collected under programs authorized by Section 702 of the Foreign Intelligence Surveillance Act.

The programs target foreigners, but domestic communications sometimes are vacuumed up as well. They were first revealed to the public by Edward Snowden, who leaked files from the National Security Agency.

"Surely the American public is entitled to some idea of how many of our communications are swept up by these programs," the committee members wrote in their April 22 letter to Director of National Intelligence James Clapper.

They weren't the first to request the information.

In the past five years, Democratic Sens. Ron Wyden of Oregon and Tom Udall of New Mexico have asked repeatedly. Last October, a coalition of more than 30 civil liberties groups wrote Clapper seeking the information. Unsatisfied with the answer they received, they wrote him again in January.

Intelligence officials have tried to assuage concerns of Congress and others by saying that any domestic communications collected are "incidental" to the targeting of foreigners. They say Section 702 allows the government to target only non-U.S. persons reasonably believed to be located outside the United States. They say the law explicitly bars the government from targeting a foreigner to acquire the communications of an American or someone in the U.S. But they say intelligence agencies are authorized under Section 702 to query communications made with U.S. persons under certain cases with certain approvals.

Late last month, Clapper said intelligence agencies are looking into several options for providing an estimate and will do their best to come up with a number.

"This tool is a terrific producer of critical intelligence for this country and our allies," Clapper said recently about continued need for Section 702 programs.

He did not say how soon an estimate could be released and cautioned that "any methodology we come up with will not be completely satisfactory to all parties."

Even Congress acknowledges that producing an estimate could require reviewing actual emails, for instance, those acquired under Section 702, which itself could raise privacy concerns. But lawmakers say they are only advocating a "one- time, limited sampling" of communications.

Intelligence officials held briefings last week for congressional aides to explain ways an estimate could be provided. That is something Congress wants to get before it starts debating whether to reauthorize Section 702, which is set to expire at the end of next year. The Senate Judiciary Committee plans a hearing Tuesday on the issue.

Intelligence officials also briefed privacy advocates in March and are expected to hold another this month on the best way to estimate the extent to which domestic communications are ensnared in the quest for foreign intelligence. Among the problems is determining the citizenship of a caller or emailer, or whether the person is inside or outside the United States.

"We can't go into what I hope will be an extensive public debate without this basic information," said Elizabeth Goitein, co-director of the Brennan Center for Justice's program on liberty and national security.

In a recent article, Goitein wrote: "The National Security Agency acquires more than 250 million Internet communications each year under this program. Given the ubiquity of international communication, this number is virtually certain to include tens of millions of exchanges that involve Americans, but there is no official public data on how many Americans' communications are swept up."

Congress and privacy advocates got a glimpse into Section 702 surveillance from a congressionally mandated report that Clapper's office released this past week. The report said Section 702 surveillance targeted 94,368 foreign persons, groups or entities outside the U.S. last year, up slightly from 92,707 in 2014.

While the year-to-year increase is small, Jameel Jaffer, deputy legal director at the American Civil Liberties Union, notes that the number of targets has risen to more than 94,000 since the surveillance became legal in 2008.

The report also said that 23,800 queries concerning U.S. persons were conducted on the database, although the report notes that one of the intelligence agencies involved in the queries, which was not identified, did not provide this information.

The report also said 4,672 search terms concerning U.S. persons were used to retrieve information from Section 702 data, but privacy experts point out that the number excludes queries conducted by the FBI.

"It's true that the targets are foreigners, but in the course of targeting those 94,000 people, the government collects the communications of many, many - we don't know the number - Americans," Jaffer said. "That number is missing."

New York Times
Police and Tech Giants Wrangle Over Encryption on Capitol Hill
Monday, 09 May 2016
Byline: Cecilia Kang

Washington - Cyrus R. Vance Jr., the district attorney of Manhattan, visited Washington late last month to argue his case on a pressing issue: encryption.
In a string of meetings with members of Congress, Mr. Vance told central lawmakers that encryption needed to be diminished during criminal investigations. During a 45-minute session with Senator Angus King, an independent from Maine who is on the Senate Intelligence Committee, Mr. Vance said his office had 230 iPhones that might contain crucial information for cases but were useless because Apple refused to help the police break the encryption on the devices.

"I wanted to express a sense of urgency around resolution of this issue," Mr. Vance said in an interview about his Washington visit.

A day after Mr. Vance was on Capitol Hill, tech executives including Kent Walker, the general counsel of Google, and Brad Smith, president of Microsoft, also met with lawmakers -- but with a very different message on encryption. Tech executives at the meetings said they were concerned about any laws that would force companies to weaken the security of their technology, according to news officials representing these companies.

This kind of behind-the-scenes lobbying has become de rigueur in Washington as the battle over encryption shifts to Capitol Hill. It is the next phase of a bitter divide that spilled into public view this year when Apple refused to comply with a court order to help bypass security functions on an encrypted iPhone used by an attacker in the San Bernardino, Calif., mass shooting last year. Doing so would have let the F.B.I. gain access to the phone. That case ended after the F.B.I. found an alternative way into the device.

Yet the standoff between the United States government and Silicon Valley tech companies continues -- and the flurry of activity around the issue is broadening. Last month, a Senate draft encryption bill, written by Richard M. Burr, Republican of North Carolina, and Dianne Feinstein, Democrat of California, rallied the attention of both sides. The bill would require tech companies to give access to encrypted data with court orders.

Law enforcement officials immediately announced their support of the bill and began to push lawmakers to back it. Trade groups representing tech companies like Apple and Facebook have flooded into congressional offices, sent letters expressing concerns that the bill weakens consumer privacy and security, and delivered scorching speeches about the proposals.

"This is an escalating fight," said Robert D. Atkinson, president of the Information Technology and Innovation Foundation, a research firm based in Washington that is funded by tech companies including Google and Microsoft. "It's become the focus now in Washington, with hearings and legislative activity."

Law enforcement officials blame tech companies for creating the impasse.

"There's no question our relationship with the tech industry has gotten worse, and now it seems like the tech industry is taking every opportunity they have to put up obstacles in our way, including trying to derail legislative efforts that would give law enforcement what they need to keep people safe," said Terrence Cunningham, president of the International Association of Chiefs of Police.

Facebook, Google and Microsoft declined to comment on their lobbying activity. An Apple spokesman said the company has met regularly with members of Congress on encryption and other issues.

The amount of lobbying on the encryption bill is unusual at this early stage of a bill's life, showing the stakes involved. Tech companies are reluctant to give access to encrypted information from their users, for privacy reasons and because it may affect their businesses. Law enforcement officials say their efforts to prevent and solve crime are hampered if they cannot see digital data on phones, messaging services and other technology services.

"Today, terrorists and criminals are increasingly using encryption to foil law enforcement efforts, even in the face of a court order," Senator Feinstein said in a statement about the draft bill. "We need strong encryption to protect personal data, but we also need to know when terrorists are plotting to kill Americans."

The rhetoric in Washington around encryption has grown increasingly sharp. Last month, when the contents of the draft encryption bill were leaked, the president of the Consumer Technology Association, a trade group that counts Apple, Google, Facebook and Amazon among its 4,000 members, spoke to an audience filled with government officials at a lunch hosted by the Media Institute.

The bill is "dangerously overreaching and technically unsophisticated," said Gary Shapiro, president of the association. "This bill would essentially make effective cybersecurity illegal in the United States, pushing companies that take cybersecurity seriously offshore."

Other tech trade groups, including Reform Government Surveillance and the Business Software Alliance, have also waded into the fray, sending critical letters and meeting with senators to warn of the dangers of the bill. And Silicon Valley executives have, in increasing numbers, made the trek to Washington to make their cases directly.

Bob Lord, chief information security officer at Yahoo, visited several members of Congress in late April to talk about the technology behind encryption and to warn of the "unintended consequences" of legislation that could weaken security. While he did not specifically mention the Burr-Feinstein bill, he emphasized how consumers and human rights activists worldwide depend on encrypted technology for their safety and privacy.

"The notion that we would weaken encryption or provide back doors, those suggestions will have unintended consequences," Mr. Lord said.

Law enforcement officials, in turn, have frequently met with the same lawmakers in the Senate and House intelligence, judiciary and commerce committees who are being targeted by the tech companies, according to congressional staff members. Chief Cunningham and other members of the police chiefs' group have talked with Mr. Burr and Ms. Feinstein, given opinions during the drafting of the legislation and hosted panels on encryption for House and Senate lawmakers.

Tech companies have turned to certain politicians to champion their cause, such as Senator Ron Wyden, a Democrat from Oregon. On the day the draft encryption bill was introduced, Mr. Wyden, who voted

against the 2012 copyright bills known as the Stop Online Piracy Act and the Protect Intellectual Property Act, which were also opposed by the tech industry, said he had been flooded with calls from tech companies wanting to know what he would do.

Mr. Wyden said he intended to filibuster the proposal. He has since met with Intelligence Committee members to persuade them to kill the bill.

"I have not filibustered many issues, but I think the stakes are enormous," Mr. Wyden said in an interview. "The bill as written is a lose- lose, because it will create less security, American families will be less safe, and your liberty and privacy will be damaged."

For all the lobbying, few lawmakers have expressed their views on the encryption bill.

"I'm reserving judgment," said Senator King, who met with Mr. Vance last month. "The issues are so complex, it's like trying to nail Jell-O to the wall."

Toronto Star
To Serve, Protect, Watch and Predict
Saturday, 07 May 2016
Byline: Alex Ballingall

Analysis: Try to imagine what policing will look like in the future. Microwave heat cannons and sound bazookas dispersing rowdy crowds? Robocops patrolling the streets while whirring drones keep watch from the sky?
Or maybe we'll arrive at a world where all crime is wiped away, where people peacefully coexist in sleeper pods while life is played out through virtual reality helmets.

Maybe.

The more realistic picture, according to police technology experts, is that surveillance and the collection and analysis of information will play a central role in solving and preventing crime.

The public safety regime of tomorrow, in other words, is all about data. "This is the future of policing," says Christopher Schneider, an associate professor of sociology at Brandon University in Manitoba.

Cops in the coming decades will gather information online, interact with the public through social media and even use data gleaned from the Internet and past crimes to predict and prevent future law-breaking, Schneider says. This is already happening, to varying degrees, in American cities and places such as Vancouver and Toronto, where police used a program to comb through Twitter to gather evidence for a recent online harassment trial.

"Policing as an apparatus is going to be much more mediated, and it's going to be much more community-oriented than it currently is, through the Internet, through social media," Schneider says.

"This is going to expand the gaze, as it were, toward crime and deviance."

The nexus between police and the public they serve has already expanded beyond the traditional 911 call (if you're even more of a troglodyte, just yell: "Help! Police!"). Ritesh Kotak, a police consultant for agencies in Canada and overseas, said tools like social media have created space for the "co-creating of public safety," with new and convenient avenues to report crimes and follow police data shared over the Internet.

"That's where it's headed with 'next generation 911.' That's where it's headed with the ability to see something and communicate right through our smartphones with police," Kotak said. "Data is the currency of the future."

With an open data mentality and deeper engagement through social media, Kotak added, police forces can repair and engender trust with the citizenry. "People feel like they're part of something," he said.

But data collection can also be used for more futuristic means. Ryan Prox, a special constable with the Vancouver Police Department, is one of the pre-eminent experts in the emerging field of "predictive policing." Prox prefers to call it crime "forecasting," in which police forces use complex computer programs that churn through mountains of data to try and predict when and where future crimes will occur.

This has yet to catch on in full force in Canada, but police in cities such as Los Angeles and Miami have signed on to "predictive" programs designed by companies such as PredPol, Prox explains. PredPol uses three data points -- time, place and type of crime -- to draw up boundaries in which crimes are most likely to occur, then local police patrol these areas in the hopes of catching the bad guys.

Prox cautions, however, that little independent scientific research has been done on these programs in the U.S. and suggests they may not be as accurate as their makers claim.

That's why he's spearheading a six-month predictive-policing pilot project in Vancouver, which began Feb. 1, that uses an intricate software program that has been designed by a team of mathematicians and geospatial engineers. The program sifts through crime data as far back as March 2001, including the time, place and nature of an offence, Prox says. But it also considers 60 "non-crime" factors, such as neighbourhood income, area traffic density, locations of illicit graffiti and even wind speed, to forecast the probability of a future crime being committed in the coming hours within a 100-metre radius of a given location.

Plainclothes cops will be dispatched to monitor these areas, with uniformed officers on standby to make an arrest in the event that a crime is witnessed, Prox says.

Tests have already shown a 60 to 70 per cent accuracy rate for some property crimes such as break and enters, which are easiest to predict because they're high frequency and often involve repeat offenders, Prox says. The more police use the program, the more data they have and the more accurate officials hope it can become.

"It sounds really sci-fi goofy," he laughs, "but they basically call it an 'artificial learning neural network.' That's the mathematical model."

The endgame of such programs, Prox says, is maximum police efficiency. In an era of ballooning police budgets -- now more than $1 billion a year in Toronto, for example -- that could be a welcome prospect.

But critics point to controversial information-gathering programs such as "carding" in Toronto, which many argue disproportionately target visible minorities.

To rely on such practices to fuel computer software programs that dictate how cops are deployed, could entrench existing police biases, Schneider says.

"Are we going to then be criminalizing certain people, certain segments of the population? Who are the police going to be looking at?" he asks.

Prox acknowledges this is a legitimate concern, but says the Vancouver police program only considers data from crime reports and other objective factors. It's generated by the public rather than fuelled by the cops themselves.

Others have brought forward concerns about how predictive policing will affect individual rights. Brenda McPhail, director of the Canadian Civil Liberties Association's Privacy, Technology and Surveillance Project, says the main worry is that the types of data currently used to forecast crime will expand to include more personal information -- social media posts, online purchase histories, travel bookings or location data from public Wi-Fi use.

This could not only invade individual privacy, it could erode the presumption of innocence, McPhail adds, citing court decisions in Canada and the U.S. that have suggested it is disproportionate to comb through data of many individuals to find a single criminal.

"The concern is that it is the thin edge of a wedge," she says. "Before any such programs are implemented, we as a society need to compare the benefits with the costs, particularly the costs to our rights and civil liberties. We need to consider the risks."

Such worries go beyond crime-forecasting programs.

Some point to privacy issues in the face of intensifying means of surveillance, such as the extensive camera networks that are used by police in Fresno, Calif., where police can monitor live feeds throughout the community through their Real Time Crime Center.

David Lyon, a Queen's University sociologist and head of the school's Surveillance Studies Centre, has argued that people's lives are being watched to the point that it already makes sense to label many western countries "surveillance societies." Lyon is co-author of a 2014 book on the subject, in which he and his colleagues argue we're at a "historic turning point" for the expansion of surveillance measures, developments with obvious consequences for privacy and state power.

Much of this can be viewed as part of a social shift toward a so-called "safety state," where more and more government policies - - and police actions -- are justified through fear of danger, says Charles Raab, a political science professor at the University of Edinburgh.

"As long as there are some plausible reasons to think we live in exceptionally dangerous times" -- such as terrorist attacks in big cities -- "there will be public fears and demands for more security and safety," says Raab. "Other values, such as equality, fairness and the exercise of rights and liberties, are constrained by the imperative to make everything safe and secure."

This isn't inevitable, Raab says. But with terrorism and climate change dominating the media and politicians routinely emphasizing this danger in their quests for votes, safety will continue to be a top social priority.

And that probably means the police of tomorrow will find ways to use our data and train cameras on us in an effort to keep us safe.

Mail on Sunday
Now Experts Say Don't Change Your Password
Sunday, 08 May 2016
Byline: Martin Beckford

London - It is one of the banes of modern life - you finally come up with a memorable yet secure password for your office computer, only to be told just a few months later that it has expired and you have to find a new one.
But now Britain's security services themselves have decreed that workers may be safer from hackers if they do not have to keep changing passwords. In a new briefing to Whitehall, power stations, banks and the public sector, cyber experts at CESG - the information security arm of intelligence agency GCHQ - concluded: 'It's one of those counter-intuitive security scenarios; the more often users are forced to change passwords, the greater the overall vulnerability to attack.'

The advice continues: 'Most password policies insist that we have to keep changing them. And when forced to change one, the chances are that the new password will be similar to the old one. Attackers can exploit this... New passwords are also more likely to be forgotten, and this carries the productivity costs of users being locked out... CESG now recommends organisations do not force regular password expiry.'

The advice comes as Ministers urge greater protection against cyber crime, after a survey found two-thirds of large businesses suffered an attack or security breach in the past year.

Fox News
Romanian hacker who claims he breached Clinton server says he spoke with FBI at length
Saturday, 07 May 2016
Byline: Catherine Herridge

Washington - The Romanian hacker who says he easily breached Hillary Clinton's personal email server also claimed, in a series of interviews with Fox News, that he spoke with the FBI at length on the plane when extradited from Romania to Virginia last month.

"They came after me, a guy from the FBI, from the State Department," 44-year-old Marcel Lehel Lazar, who goes by the moniker "Guccifer," told Fox News during a jailhouse phone interview. He said the conversation was "80 minutes ... recorded," and he took his own notes.

A government source confirmed that the hacker had a lot to say on the plane but provided no other details. Lazar was flown to the U.S. to face separate cyber-crime charges.

In addition to the apparent conversation with the FBI on the plane, Fox News has learned a meeting was expected as early as this week at the Alexandria, Va., detention center where he's being held involving Guccifer, the FBI, the U.S. attorney and the defendant's court- appointed lawyer.

These officials have not commented on his clams or detention.

An intelligence source close to the investigation, speaking with Fox News last month, questioned the timing of Lazar's extradition to the U.S., coming amid the Clinton email probe. As for what was discussed on that plane, Lazar said he told a State Department representative on the plane about "hot" data, some of which was hidden in Google drives, and other data that was too sensitive and deleted. The hacker, who offered no proof for his claims, said cryptically that he could not say more.

"I can't tell [you] now. I can't tell because I want to talk to the FBI. It is a matter of national security. Yeah," he said. Pressed by Fox News, Lazar seemed to indicate the data was not connected to the ongoing FBI criminal probe of Clinton's server.

Fox News recently met with Lazar in the secure visitor center in Alexandria, then followed up with a series of phone calls which he gave permission to be recorded. Separated by reinforced glass, Lazar was polite and methodical as he explained how he allegedly accessed the Clinton server in early 2013, by using her longtime confidant Sidney Blumenthal's AOL account as a stepping stone.

Fox News was first to report the hacker's claims of accessing the Clinton server, which he said "was easy."

Lazar said he got into the Blumenthal account by correctly guessing his security question, after doing extensive research on the web. He said his hacking always followed a "four step process": identify the target, do extensive web research on the target, access the target's account to harvest data, and send it out to the media.

Lazar said he was puzzled by the American media. He said he sent the Blumenthal emails, which is how the Clintonemail.com account first came to light, to many large news organizations in 2013, and it was The Smoking Gun that picked it up. Lazar said he started his "Guccifer archive," releasing materials in October and November 2012, and it ended "like August 2013."

Three cybersecurity experts said they found Lazar's explanation for accessing the Clinton server plausible but had questions.

Cybersecurity expert Morgan Wright explained how the FBI could marry up available evidence, including forensics or the configuration of the server and its folders, to assess his claims. "So we're going to map these things together, and if those things match up together, they're going to say 'yes, this was compromised,' then it means it was open to other people to compromise as well," he said.

Since Fox News reported on Guccifer's claims Wednesday, anonymous sources have reported that a review of the Clinton hard drives does not appear to indicate a breach. However, Wright and other experts warned that Clinton IT specialist Bryan Pagliano was the server's administrator and not principally a cybersecurity specialist - and may not have installed an adequate detection system for a Cabinet secretary's email.

"If you have a bank and you have one video camera when you need 20, then you missed it," Wright said. "If they weren't capturing all the activity, their security logs may say they didn't see anything."

Asked about Lazar's claims at Thursday's press briefing, State Department spokesman Mark Toner also said he's not aware of such an incident.

"We don't have any reason to believe that it might be true," he said.

At the same time, Toner repeatedly stressed he did not want to comment on the security of the server, citing ongoing investigations. Asked if he's in a position to even know whether Lazar's claims are true, Toner again said he did not want to comment. The Clinton campaign has rejected Lazar's claims, calling them "baseless" and emphasizing he is a convicted hacker.

Other cyber specialists like Bob Gourley with Cognitio warned there will "always be uncertainty and ambiguity" with hackers like Guccifer. But he said: "One thing I would say with certainty however -- if this computer were in a well- managed facility, where everything was being monitored and watched, we would have more information and ground truth."

Catherine Herridge is an award- winning Chief Intelligence correspondent for FOX News Channel (FNC) based in Washington, D.C. She covers intelligence, the Justice Department and the Department of Homeland Security. Herridge joined FNC in 1996 as a London- based correspondent.

Pamela K. Browne is Senior Executive Producer at the FOX News Channel (FNC) and is Director of Long-Form Series and Specials. Her journalism has been recognized with several awards. Browne first joined FOX in 1997 to launch the news magazine "Fox Files" and later, "War Stories."

London Free Press

Canada Revenue Agency hacker pleads guilty, says he's sorry
Saturday, 07 May 2016
Byline: Jane Sims

London - Stephen Solis-Reyes is one of those brainiac computer whiz kids who, it seems, was a little too smart for his own good.
Two years ago, when the London, Ont. man was just 19, and with what he maintains were the best of intentions, he was able to steal 900 social insurance numbers from the files of the Canada Revenue Agency. He says he wanted to demonstrate its online vulnerability to the Heartbleed computer bug.

The result was a sudden, panicked shutdown of the agency's website for four days that sent techno-fear shivers about online security across Canada and prompted the CRA to extend Canadians' tax-filing deadline by a week.

On Friday, now a top- notch computer science student at Western University, the 21-year-old pleaded guilty in an Ottawa courtroom to four charges.

Two were for mischief -- one for the Canada Revenue breach, another for exposing security breaches in JerseyMail, the now-defunct online arm of the postal service in Jersey, one of the Channel Islands off the coast of Great Britain.

The two other guilty pleas were to one count each of unauthorized use of a computer and obstructing a police officer by swiping information off a computer at his arrest.

"I want to express to Your Honour my most sincere regret and remorse for the wide-reaching effects of damage and harm my actions have caused to many different people and organizations," he wrote in a letter to the court.

"I truly understand the severity and gravity of the situation. I want to say that I never had any malicious intent and I never intended to cause harm or damage to anyone in any way."

The Crown dropped 13 other charges that, had be been convicted, could have sent him to prison for as long as 10 years.

For all of the national hubbub surrounding his activities in April 2014, Solis-Reyes was sentenced to an 18-month conditional sentence -- the first four months under house arrest, the rest under supervision.

The defence gave the judge more than 20 reference letters from professors, teachers, friends and family who spoke of Solis-Reyes' intellect and quiet, sensitive and respectful nature.

He's carrying a 98.6 per cent grade average in his fourth year and has already been named to the dean's honour list three times.

Assistant Crown attorney James Cavanaugh read an agreed statement that outlined how Solis-Reyes was able to breach the computer systems from his laptop computer.

Defence lawyer Faisal Joseph told the judge Solis-Reyes was able to get into the CRA system in "six seconds."

Central to the case, was Solis-Reyes' intentions. Joseph told the judge it would have been easy for Solis-Reyes to sell the information or make money off it. None of that happened.

"He did it because he could, because he was capable of breaking into these national security places," Joseph said, and that Solis-Reyes "has done the country a service" by exposing the flaws in the system.

One professor referred to him as "not only one of the smartest students around, but he is also one of the nicest, friendliest and most honest."

"His code is a thing of beauty," another wrote.

His father, Roberto Solis-Oba, the graduate chairman of Western's computer science department, wrote it was his son's "insatiable curiosity that led him to perform the actions that got him in trouble with the law.

The defence was harshly critical of what he alleges were the interrogation methods the RCMP put Solis-Reyes through after his arrest at his London home.

He said his client was questioned for six hours without a lawyer present. He was accused of being a terrorist and was asked "what would Jesus think" about his activities, Joseph said.

Joseph pointed out an RCMP corporal suggested Solis-Reyes's father's job could be in jeopardy and how, in France, it's not illegal to tie somebody up in a hot water tank until he speaks.

"In over 30 years of practising law as a prosecutor and a defence lawyer I have never met a better family or a more respectful, loving, intelligent boy as my client," Joseph said. "Murderers and rapists haven't expereince what my 19-year old client received at the hands of the RCMP's investigating officer for hours on end."

Reached for comment late Friday, the RCMP had not yet responded to the lawyer's characterization.

Solis-Reyes must serve two years of probation, with 200 hours of community service ordered.

He said in his letter he "will never again be in trouble with the law."

"This situation has taught me the importance of thinking before acting and I know every action I take has consequences."

Calgary Herald
Police trying to stay ahead of technology
Saturday, 07 May 2016
Byline: Kim Bolan

Calgary - Mounties were trying to investigate a threat to national security. But because they couldn't get critical information from a telecommunications company, they hit a roadblock.
Despite pursuing other investigative avenues, the case went nowhere, Chief Supt. Jeff Adam, director-general of the RCMP's technical investigation services, said in an interview.

"We spent roughly six months trying to design and implement a partial solution in order to get some of that data. But the gaps remained. And despite the judicial authorization, we've been unable to collect the evidence." The national security case is just one example of the obstacles police face as criminals and terrorists use cutting-edge technology to cover their tracks, Adam said. In another case, the RCMP got a court order "to intercept email messages between suspected criminals - high-level drug traffickers in Canada - and we could intercept, but we could not read the email traffic that they were sending," Adam said. "It was encrypted and this particular investigation involved some of our international law enforcement partners and we were unable to assist ourselves or them in getting the evidence."

Adam said the inability to decipher encrypted messages even when police get warrants is a challenge in many investigations - particularly those involving national security, organized crime and child exploitation.

Another issue, he said, is "lack of requirements for data retention by our telecommunications service providers."

Say police get a court order to obtain the text messages of a suspect in a case of threatening. But the company then tells investigators that it "doesn't keep anything more than 24 hours, so that evidence is therefore expunged from the system," Adam said.

On a recent trip to B.C., RCMP Commissioner Bob Paulson warned that while emerging technology has many benefits, "it's also changing criminality and it is putting us at risk and maybe you have to think that through more."

He cited the recent U.S. case where the FBI took Apple to court to get the iPhone of one of the San Bernardino terrorists unlocked. Apple refused. The FBI finally found a third party who could crack the password.

"It's just a taste of what's before us in terms of how we are going to go down this road," Paulson said. "It shouldn't be up to the police to say how we are going to roll. I think the community needs to engage because the threat is manifest."

Ann Cavoukian, executive director of Ryerson's Privacy and Big Data Institute, thinks police exaggerate the technological obstacles they face. And she said they rarely "point out the advantages they have from technology."

"It is deceptive because while it's true that occasionally they won't have access to one or two communications that have been encrypted, largely speaking they have more access now to a wide variety, a wide swath of information that they never had access to before," said Cavoukian, Ontario's former privacy commissioner.

"They're only pointing you to the small tiny percentage of cases where they might not be able to decrypt a phone because it has got end-to-end encryption. But that happens rarely."

The law-abiding public relies on encryption to protect sensitive personal information - often including health and banking records - that they now store on their phones.

"All of this information is accessed through your iPhone and you want people to be able to encrypt that safely to protect it from all the cyber attacks that are taking place," she said.

Cavoukian said there are huge privacy concerns with some of the technology police use in their investigations.

Media reports from a Montreal Mafia trial recently revealed that the RCMP had used a device known as a Stingray to intercept suspects' calls.

The device is controversial because it mimics a cellphone tower, allowing police to collect information from their targets' phones, but also from anyone else in the vicinity.

Last month, the office of the federal privacy commission confirmed it was investigating complaints about the RCMP's refusal to discuss its use of the Stingray device.

Cavoukian said the lack of transparency by police just increases the public's skepticism and distrust.

She said she has no problem with police getting proper warrants and getting the specific information they need for criminal investigations. But the fear is that law enforcement agencies have the ability to cast a wider net that unfairly ensnares lawabiding citizens, she said. She also acknowledged that the public puts its own privacy at risk with by using wireless devices and fitness trackers that can send personal information to "dozens of parties unbeknownst to the individual and the information can be used against them."

In a recent Pennsylvania case, a woman's claim to police that she'd been raped was disproven by her Fitbit data.

Le Journal De Montreal
Recrutés sur Instagram
Saturday, 07 May 2016
Byline: Hugo Jocas

Montréal - «Quelqu'un» a utilisé le réseau social Instagram pour tenter de recruter les jeunes arrêtés en mai 2015, selon la déclaration de la GRC à la Cour du Québec.
Un adolescent de Saint-Léonard «se sentait comme hypnotisé par le discours du suspect», selon son père, qui a appelé la police fédérale pour le dénoncer.

Son fils utilisait son téléphone iPhone pour naviguer sur Instagram et échanger avec le recruteur.

«L'homme lui a dit que vivre au Canada était péché, car ce n'est pas un pays musulman», mentionne la dénonciation de la police fédérale.

Le recruteur allégué utilisait toujours un profil différent sur Instagram pour communiquer, mais il commençait toujours par le même nom, caviardé dans le document de l'Équipe intégrée de sécurité nationale.

FAUX VOYAGE

L'adolescent avait fait croire à sa famille qu'il partait pour un voyage en Grèce avec son école.

Son père a interrogé la direction: aucun voyage n'était organisé. Il a alors confronté son fils, qui a éclaté en sanglots.

Contrairement aux autres, le jeune a été arrêté chez lui et non à l'aéroport.

Un autre des 10jeunes s'était rendu avec lui dans une agence de voyages pour s'informer sur le prix de billets pour Rome, avec escale à Istanbul, selon nos informations. Il avait acheté un billet, mais lui aussi a abandonné le projet.

Toronto Star
Reveal high-tech privacy violations: Editorial
Sunday, 08 May 2016

Editorial: We know Ottawa's electronic spy agency has violated the privacy of Canadians on multiple occasions. Indeed, the highly secretive Communications Security Establishment maintains a central database of such transgressions dating back to 2007.
What we don't know is how many such breaches have occurred. As reported by the Star's Alex Boutilier, the organization refuses to reveal this number, citing "operational security concerns." The CSE is evidently worried that disclosing the total might give Canada's enemies insight into its "capacity to conduct operations" and "the extent of its capabilities."

It's far more likely that what actually troubles this agency is having Canadians see its capacity for misconduct and the extent of its abuses.

To assure people that the principle of public accountability is being respected it's important for the CSE to level with Canadians and reveal how often it has violated their privacy.

There's no doubt wrongdoing has taken place. That was revealed earlier this year when Parliament was told the electronic eavesdropping agency had inadvertently shared Canadians' "metadata" with foreign allies.

This class of information can include the destination and duration of phone calls, emails, and text messages. To protect privacy, such material was supposed to be scrubbed of key details before being passed along to other members of the "Five Eyes" alliance -- the United States, United Kingdom, Australia and New Zealand. But the CSE learned, in 2013, that a technical glitch had resulted in a leak of confidential data.

It informed government officials but kept the mistake hidden from the Canadian public for two years. This gives rise to an obvious question: how many other privacy violations might this agency be keeping secret?

As reported by Boutilier, documents tabled in Parliament last month show the CSE admitting to 13 privacy and information breaches in 2015, affecting at least 630 people. None of these cases were reported to Canada's privacy commissioner on grounds that they posed "no significant risk" to anyone.

It's hard to see how presenting a similar tally, dating back to 2007, would pose a serious security threat. It would, however, give Canadians some insight into how well their rights are being protected.

The Liberal government came to office promising a new level of openness and accountability. Responsibility for fulfilling that pledge now rests with Treasury Board President Scott Brison. And a good place for him to start would be to let Canadians know how often their privacy has been violated by a shadowy agency that refuses to fully answer even to this country's information and privacy commissioner.

BDNews24
Technicians from SWIFT left Bangladesh Bank exposed to hackers
Monday, 09 May 2016

Dhaka - The technicians introduced the vulnerabilities when they connected SWIFT to Bangladesh's first real-time gross settlement (RTGS) system, said Mohammad Shah Alam, the head of the criminal investigation department of the Bangladesh police who is leading the probe into one of the biggest cyber-heists in the world.
"We found a lot of loopholes," Alam said in an interview in Dhaka. "The changes caused much more risk for Bangladesh Bank."

He and a senior central bank official said the SWIFT employees made missteps in connecting the RTGS to the central bank's messaging platform.

The technicians did not appear to have followed their own procedures to ensure the system was secure, according to the Bangladesh Bank official, who said he was not authorised to publicly comment because of the ongoing investigation.

Because of this, SWIFT messaging at the central bank was widely accessible, including remote access with only a simple password, police said. It had no firewalls and only a rudimentary switch. "It was the responsibility of SWIFT to check for weaknesses once they had set up the system. But it does not appear to have been done," said the bank official.

SWIFT's chief spokeswoman Natasha de Teran said she had no comment on the allegations by authorities in Bangladesh. She also declined comment on any aspect of the Bangladesh project, including whether the firm had deployed any employees or outside contractors to Bangladesh Bank.

Reuters was not able to independently verify the allegations by Bangladeshi officials about the SWIFT technicians. If they are validated, however, that could undermine confidence in the cooperative that is the backbone of global financial transactions.

The officials in Dhaka discussed their findings with Reuters ahead of a meeting this week in Basel, Switzerland where Bangladesh Bank officials have said their governor and a lawyer appointed by the bank will discuss recovery of about $81 million stolen by the hackers with the head of the Federal Reserve Bank of New York and a senior executive from SWIFT.

Bangladesh Bank officials have said they believed SWIFT, and the New York Fed, bear some responsibility for the February cyber heist. SWIFT has declined comment on that claim.

The RTGS, which enables domestic banks and the central bank to settle large transfers between themselves, was installed at Bangladesh Bank in October last year and then connected to SWIFT. In

February, hackers sent fraudulent messages, ostensibly from the central bank in Dhaka, on the SWIFT system to the New York Fed seeking to transfer nearly $1 billion from Bangladesh Bank's account there.

Most of the transfers were blocked but about $81 million was sent to a bank in the Philippines and much of that money remains missing.

A spokesman for Bangladesh Bank declined comment on the investigation into the heist. He said, however, that RTGS continued to work well, noting that a large number of countries use SWIFT messaging for similar systems. "There is no inherent risk in this," he said.

According to the Bangladeshi police, the technicians linked the RTGS to SWIFT computers on the same network as about 5,000 central bank computers that are accessible from the open Internet.

Instead, they should have set up a separate local area network, or LAN, that could not connect to the rest of the bank or the Internet, police said.

The technicians also failed to install a firewall between the RTGS and the SWIFT room so that the bank could block malicious traffic from coming into the facility.

When they installed a networking switch to control access to SWIFT, they chose to use a rudimentary old one they had found unused in the bank, rather than a more sophisticated, managed switch that gave the bank the ability to control access to the network, police said.

During the job, the technicians set up a wireless connection so they could access computers in the locked SWIFT room from other offices inside the bank. When they finished, they failed to disconnect the remote access, which was only secured with a simple password, police and the bank official said.

They also failed to disable a USB port on the computer attached to the SWIFT system, as is usual for critical networks to prevent malicious software from being installed through a tainted thumb drive, police said. Police did not provide any evidence for any of the assertions.

But another central bank official familiar with the SWIFT room operations confirmed that the port was "active" until the heist came to light. He had no explanation. The hackers used malicious software to modify the SWIFT messaging software to help hide their tracks.

Bangladeshi police said they have asked SWIFT to facilitate interviews with the SWIFT technicians. "Whether it is intentional or negligence, we are trying to find out," said Alam.

SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, is used by about 8,000 banks around the world to order funds transfers and other communications. It is connected to RTGS systems installed at scores of banks worldwide, and there have been no reports of problems elsewhere

with connections between those two systems. The US FBI, which is leading investigations into the case, has made no comment so far.

New York Fed executive Richard Dzina said at a conference last week that bank workers "acted properly" in releasing the funds. The system was penetrated, he said, because the hackers had acquired valid credentials to order the transfers

Former central bank governor Mohammed Farashuddin, who is heading an internal probe by Bangladesh Bank into the heist, said SWIFT needed to review its technology in the wake of the heist.

"It seems to be a case of extreme carelessness," he told Reuters. He declined to provide more details saying a final report was due in the next few weeks.

Agence France-Presse
Indonesia's Muslim cyber warriors take on IS
Monday, 09 May 2016

Jakarta - A group of Indonesian "cyber warriors" sit glued to screens, as they send out messages promoting a moderate form of Islam in the world's most populous Muslim-majority country.
Armed with laptops and smartphones, some 500 members of the Nahdlatul Ulama (NU) -- one of the world's biggest Muslim organizations -- are seeking to counter the Islamic State group's extremist messages.

"We'll never let Islam be hijacked by fools who embrace hate in their heart," tweeted Syafi' Ali, a prominent member of the NU's online army, a typical message to his tens of thousands of followers.

They are trying to hit back at IS's sophisticated Internet operations, which have been credited with attracting huge numbers from around the world to their cause.

Internet propaganda is believed to have played a key role in drawing some 500 Indonesians to the Middle East to join IS, particularly among those living in cities where it is easier to get online.

The dangers of the growing IS influence in Indonesia were starkly illustrated in January when militants linked to the jihadists launched a gun and suicide bombing attack in Jakarta, leaving four assailants and four civilians dead.

It was the first major attack in Indonesia for seven years, following a string of Islamic militant bombings in the early 2000s that killed hundreds.

As well as firing off tweets, the NU members have sought to dominate cyberspace by establishing websites promoting the group's moderate views, an Android app and web-based TV channels, whose broadcasts include sermons by moderate preachers.

The initiative has been building momentum for a while but started to pick up pace a few months ago. A handful of cyber warriors operate from a small office in Jakarta, while the rest work remotely, and the group mostly communicate with one another over the web.

But it will be an uphill battle and the NU, which has been promoting moderate Islam for decades, conceded they have previously struggled to take on IS's hate-filled messages.

"NU has for a while wrestled with this radical propaganda," said Yahya Cholil Staquf, secretary general of the NU, which claims at least 40 million followers. "Every time we defeated them, it didn't take long for them to regain their strength."

The online drive comes as the NU is set to take its campaign to promote their tolerant form of Islam onto the international stage this week, with a two-day meeting from Monday of moderate religious leaders from around the world.

They aim to showcase their particular brand of the Muslim faith, known as "Islam Nusantara", to counter the IS jihadists' radical interpretation of Islam.

Meaning "Islam of the Archipelago" -- Indonesia is the world's biggest archipelago, comprising over 17,000 islands -- it is accepting of diversity and stresses non-violence.

It grew up organically in Indonesia, as the religion entered the country gradually and had to mix with existing traditional beliefs such as praying at tombs, making it a naturally tolerant form of Islam.

Nowadays, most of the approximately 225 million Muslims in Indonesia practice a moderate form of Islam.

The NU wants to persuade Muslims from around the world to look for inspiration to Indonesia, where religious minorities and a multitude of ethnic groups mostly coexist harmoniously, rather than to harsher forms of Islam from the Middle East.

The group nevertheless has a long way to go to fight the rising tide of IS propaganda. Despite their good intentions, the NU cyber warriors appear amateur next to IS's well-funded set-up.

The jihadists, who control huge swathes of territory in Iraq and Syria, have a sophisticated online operation, using social media, apps and slickly produced videos.

They send about 200,000 tweets a day into the United States alone, according to US officials. It even has its own news agency, Amaq, which is often the first to report that IS is claiming responsibility for attacks.

In Indonesia, there are two main ways that IS propaganda spreads -- by supporters posting on websites and apps such as Whatsapp, Facebook, Twitter and Line, and through returnees from the Middle East preaching the group's radical ideology.

Most of the NU's online army are volunteers, often reaching into their own pockets to cover costs.

"ISIS has oil, while the only oil we have is for hair," Ali said, explaining the project's start was delayed for more than a year due to funding problems. Oil smuggling has been a key revenue source for IS.

Robi Sugara, a terrorism expert from NGO the Indonesian Muslim Crisis Center, welcomed the NU's online approach. "It's a good strategy to make Google searches fill up with moderate Islamic content," he told AFP.

"The battleground for Islamic ideology has moved to the Internet, and by producing as many moderate websites as they can, they can keep more minds healthy."

Haaretz
Classified Documents Stolen From Israel Police Cybersecurity Expert
Monday, 09 May 2016
Byline: Yaniv Kubovich

Jerusalem - Thief presumably used a grabber tool to filch the folder from a table through an open window, together with the officer's house and car keys. A file folder containing classified documents was stolen on Thursday from the central-Israel home of a police expert in computer security.
The Walla Hebrew-language news site reported that the deputy head of the cyber security division of the Israel Police left the folder on a table after returning home. The assumption is that the unknown thief used a long-handled rake or other instrument to grab the folder, as well as the officer's key ring, through a window. The thief then apparently entered the house using the keys and stole a wallet before fleeing.

The police are investigating and have notified security agencies that could potentially be affected by the theft of critical information. The fact that neither valuables nor the officer's unmarked car were stolen suggest that the motive may have gone behind simple financial gain.

The official was not identified -- the Israel Police said this was in order to protect the official's privacy, but it is known that he was recruited into the police from the army's signal intelligence unit 8200.

All possible motives for the theft are being explored, however, including simple theft.

Haaretz recently reported on the disappearance of 27 files from the police station in the Tel Aviv suburb of Givatayim under unclear circumstances.

About a month ago, police officers from the station went on vacation to Eilat. On their return, one investigator noted the disappearance of the files, which had been either awaiting investigation or were to be transferred to other offices. This case too involved sensitive files that appeared to be left unprotected.

Khaleej Times
The future of media? It's digitization
Monday, 09 May 2016
Byline: Bernd Debusmann Jr.

Dubai - Digitisation is setting the future of the media industry in the Middle East and North Africa as increased broadband usage leads to soaring use of portable devices, according to the newly-released fifth edition of the Arab Media Outlook.
The report, which was released on Sunday, highlights the current media landscape of 14 Arab countries, and identifies future trends that will shape the industry between 2016 and 2018.

In 2015, according to the report, the digital sector accounted for 15 per cent of the Mena's media industry, which was valued at over $11.36 billion. In 2020, that number is expected to rise to 27 per cent. In that same time, the total size of the Mena media industry is expected to rise by 3.7 per cent to over $13.63 billion.

Mona Ghanim Al Marri, president of the Dubai Press Club, said that the findings brought into stark focus the need to find solutions that allow for "effective competition" between media outlets, and ways in which to couple digital media platforms and traditional media outlets, as well as using these platforms to maintain the position of media and develop content.

Print media - which in 2015 represented 45 per cent of the region's media industry - is expected to decline to 31 per cent. In the Mena region, a total of 41 per cent of the average time spent on media in 2015 - 11 hours - is done online, compared to 49 per cent in the UK and 47 per cent in Australia.

Al Marri also noted the noticeable growth of the paid media sector compared to advertising sector, where spending on advertising is set to increase by 2.5 per cent annually between 2016-18, while spending on paid media is set to grow by 3.7 per cent.

Paid media, the report notes, will largely by backed by the growth of video games, which will account for over $1.14 billion in revenue in 2018, 62 per cent of which will be driven by social gaming, compared to

52 per cent in 2015. Paid TV revenue, for its part, is expected to grow 10 per cent in the same timeframe, to over $1.53 billion.

"While paid media is a synonym of 'excellent content', we should stop at this noticeable progress and think about what our local and Arab media should do in terms of development steps, to keep pace with the rapid changes," Al Marri said.

Notably, digital video is expected to form 30 per cent of the media industry by 2018. Already in 2015, video accounted for an average of 71 minutes of daily time spent by 15-to-24-year-olds, compared to 51 minutes on social networks, 29 minutes on search engines and business sites, and only 14 minutes on news websites.

Dr Amina Al Rustamani, group chief executive officer of Tecom Group - of which Dubai Media City is part - noted that a careful study of the findings will be crucial in forming future media and communications strategies.

"The dynamics and trends of the media industry have always provided valuable insight into consumer behaviour and have helped shape the thinking of government and business as to what are the most effective means of communication with their citizens and customers," she said. "Launching the Arab Media Outlook Report 2016-2018 is especially timely and relevant, against a backdrop of a paradigm shift in the media industry, and unprecedented change and innovation. This report enables us to guide our partners in forming their own strategies for growth."

A print version of the executive summary of the report will be available during the 15th edition of the Arab Media Forum, to be held on Tuesday and Wednesday at the Dubai World Trade Centre.

Albert Oil
How To Do Business in Brazil
Monday, 09 May 2016
Byline: Staff reporter

After raising the hopes of foreign investors in Brazil and opening up its vast reserves to overseas drillers, the country's political system has lurched into instability recently with millions of people taking to the streets demanding the president's head over a vast corruption scandal at state-owned Petrobras, which operates globally.
Niko Resources of Alberta has offshore exploration assets in Brazil, as does Brasoil.

Opportunities

In 2014, Brazil produced 2.95 million b/d of oil-- up 9.5 percent from 2013--making it the world's ninth-largest producer. The U.S. Energy Information Administration (EIA) estimates that in 2015, Brazil had 15

billion barrels of proved oil reserves, second only on the continent to Venezuela. More than 94 percent of Brazil's reserves are located offshore. About a quarter of its output comes from the deep water presalt layer, where production hit a record 865,000 b/d in 2015 as new wells came on stream in the Santos basin.

Brazil opened up to private and foreign investment in 1997. Canadian companies brought their offshore Atlantic experience to the table. Some service firms went inland. Weatherhaven, on the heels of the visit of former prime minister Stephen Harper to Brazil, closed a deal to build exploration camps for production in the Amazon. Gran Tierra Energy entered onshore Brazil in 2009, following Encana, and later entered the offshore in 2011 with Statoil and Petrobras in the Camamu-Almada basin. Canadian firms operate some of those blocks, including Brasoil, and Calgary's Tuscany International Drilling. Tuscany went there looking for year-round work, instead of the seasonal cash flows of Alberta, although the company has since gone bankrupt.

Risks

In 2013, Brazilian President Dilma Rousseff accused the Communications Security Establishment Canada (CSEC) of spying on Brazil's Ministry of Mines and Energy. She based her intelligence on documents leaked to Brazilian media by Edward Snowden. Snowden worked for the U.S. National Security Agency--the counterpart of Canada's CSEC. It's alleged that the Harper government spied to provide Canadian energy firms with intelligence to give them the edge over rivals when bidding for concessions. Today, Rousseff is fighting for her political survival as she faces impeachment for allegedly cooking the books to hide a budget deficit, and millions of people have taken to the streets as a massive corruption scandal at state-owned oil giant Petrobras threatens to bring down the government.

Police picked up former president Luiz Inacio Lula da Silva, Rousseff's mentor, for questioning in a federal investigation, dubbed "Operation Carwash," into a corruption scheme that apparently turned Petrobras into a giant slush fund for the ruling Workers' Party. The former president was questioned about allegedly receiving illicit kickbacks from Petrobras in the form of cash payments and luxury real estate. Rousseff quickly made da Silva a member of her cabinet to protect him from prosecution. Many of Brazil's top figures in business and politics have been implicated in deepening the worst recession in decades in South America's biggest economy.

As well as navigating Brazil's muddy political torrents, Canadian firms have to deal with blowback from neighboring nations. Amazon tribespeople from Peru and Brazil have joined forces to stop Toronto's Pacific Rubiales from allegedly destroying land and putting at risk the lives of uncontacted tribes. Pacific Rubiales is exploring in Block 135 in Peru, which is an area proposed as a reserve for uncontacted tribes

Gulf Daily News
Security technologies 'crucial for aviation industry'

Monday, 09 May 2016

Manama - Security technologies like encryption, intrusion protection, firewalls and right technical design and architecture are critical to ensure sustainable growth of the aviation industry, a leading expert has said.
According to Gulf Air's director of information technology (IT) Dr Jassim Haji, the incidence of cyber attacks against airlines around the world has been rising as has the damage and loss they have caused.

Addressing leading IT industry experts at global market intelligence and advisory provider International Data Corporation's Security Roadshow in Bahrain, Dr Haji said a diverse digital ecosystem had brought security to the forefront as it underpinned every operation, process and service within the industry.

Explaining how latest technologies and phenomena like mobile, social, cloud and Big Data had brought benefits to the industry, he said there had also been an increase in risks as well as actual and potential threats. "Airlines hold private and confidential information about their passengers and it is critical that this information was protected and kept safe from unauthorised access or manipulation," he said.

This, he added, assumes greater significance in the case of governments and border controls which are custodians of sensitive information about passengers with possible national security implications.

Talking about new generation of aircraft, Dr Haji said every equipment and part has become a piece of electronics thus becoming susceptible to external manipulation and control. He said all airlines needed to have a cutting-edge risk management framework that would be used to efficiently identify potential risks, their impact, likelihood of occurring, mitigation plans and regular assessments of such risks.

Referring to drones as one of the new and obvious risks, Dr Haji said they were increasingly becoming uncontrolled and unmanaged, citing a recent incident at an airport in London where an aircraft was hit by a drone as an example of the damage that can occur from this unmanaged state.

He also emphasised that initiatives based around becoming "smart," were bringing about a need for secure, open platforms. "The culture of security has to be instilled in every single employee so they protect their own company and act vigilantly." Dr Haji also serves on the SITA Council and sits on the board of directors of a leading hospitality and tourism technology provider in the Middle East.

Through his myriad initiatives, he has managed to achieve 26 top Middle-Eastern technology awards for Gulf Air, including best project implementations for cloud computing, virtualisation, Big Data, mobility applications and IT security. Held at the Diplomat Radisson Blu Hotel, Residence and Spa, the event saw participation from more than 100 professionals and executives.

Sky News (UK)
Small Firms 'Underinvesting' In Cyber Security

Monday, 09 May 2016

London - Half of small manufacturers in the UK have failed to increase cyber security investment in the past two years, according to a survey.
Research by manufacturers' organisation EEF found that 56% of businesses have not increased their spending.

A fifth fail to make employees aware of cyber risks, while only 56% say cyber security is given serious attention by their board.

Just over a third, or 36% of manufacturers, have an incident response plan in place, and only 24% monitor cyber threats.

EEF Chief Economist Lee Hopley, is urging manufacturers to step up their planning to counter the increasing number of cyber threats.

"As technology and data start to play increasingly critical roles in manufacturing, companies will inevitably find themselves more vulnerable to cyber breaches," said Mr Hopley.

"Our survey highlights that investment in new technology isn't being matched by investment in managing risks, especially among smaller firms.

"It is important that manufacturers are able to identify, understand and put the correct strategies in place to keep their businesses safe and cyber secure."

The Government has also called for industries to act to protect themselves while announcing it will launch a National Cyber Security Centre this autumn and spend £1.9m over the next five years.

Its research revealed that 90% of large businesses and 74% of small businesses reported cyber security breaches last year. Average breaches cost up to to £3.14m for large firms and up to £311,000 for small businesses.

A quarter of large firms come under attack at least once a month, according to the Department for Culture, Media and Sport.

The research shows the most common attacks detected involved viruses, spyware or malware and could have been prevented using the Government's Cyber Essentials scheme.

A TalkTalk cyber attack last year cost the telecoms group up to £45m and triggered a sharp drop in customers.

Washington Free Beacon
Obama Policies Toward Hackers From China, Iran, Syria Produce Few Results
Monday, 09 May 2016
Byline: Bill Gertz

Column - Recent federal indictments of Iranians and Syrians for cyber attacks on U.S. networks further highlight the failure of President Obama and his administration to counter the growing threat of foreign hacker strikes on American networks.
In March, the Justice Department indicted two groups of hackers, one from Iran linked to cyber intrusions of an industrial control system operating a New York dam, and a second from Syria engaged in illegal activities that included causing damage to computers and extortion.

The indictments are largely symbolic, since none of the Iranians or Syrians are within reach of U.S. law enforcement and the chances the hackers will ever face justice in a courtroom are slim.

Like many of President Obama's foreign policies, the indictments appear designed to provide the president and his administration with political cover by adopting seemingly proactive measures, but without having much impact.

The approach to cyber threats coincides with the president's generally pacifistic approach to foreign affairs, which he is reported to have summed up as "don't do stupid shit." In practice, this approach often amounts to doing as little as possible, and doing nothing that might require the use of military force.

The policy was captured in a New York Times profile last week of Ben Rhodes, the White House deputy national security adviser for communications who was described as "The Boy Wonder" of the White House.

Leon Panetta, who served as CIA director and defense secretary under Obama, explained that the president's approach to foreign affairs has been dominated by the desire to avoid possible conflicts.

"I think the whole legacy that he was working on was, 'I'm the guy who's going to bring these wars to an end, and the last goddamn thing I need is to start another war,'" Panetta said of Obama's approach to Iran and the nuclear deal. The former defense secretary said the president believes that "if you ratchet up sanctions, it could cause a war. If you start opposing their interests in Syria, well, that could start a war, too."

On cyber security, the president and his advisers have rejected policy options from military and civilian national security experts since at least 2011 for a show of force in cyberspace against China or other states and groups engaged in widespread cyber attacks, according to officials familiar with internal discussions.

Private industry, which is barred by federal statute from conducting its own cyber counterattacks, has pressed the White House and the U.S. intelligence community to do more against the onslaught of hacks. So far the response has been a firm "no" from the president.

Symbolic indictments or other diplomatic measures have not worked to deter cyber attacks. The FBI announced in July it was revamping its cyber counter- espionage unit after logging a 53 percent increase in its caseload.

A State Department security report published on March 30 noted that in the indictments of the Iranian Syrian hackers, U.S. private sector institutions were the main victims.

"These cyber attacks resulted in disrupted customer communications, data infringement, and significant financial losses," the report said, adding, "the hackers will likely not face prosecution in the U.S. for their actions ... [h]owever, some analysts believe the U.S. government will continue publicly blaming foreign hackers in an effort to deter future attacks."

The indictments followed a similar May 2014 action by the Justice Department against five Chinese military hackers who also remain out of reach of law enforcement and who likely will never be brought to trial.

The indictment was a response to Chinese government denials to the Justice Department about its cyber activities and a demand to produce legal evidence implicating China's cyber warfare troops in what the United States has charged is widespread theft of corporate and government secrets.

John Carlin, the Justice Department's national security chief, explained that the indictment was simply following through on Beijing's dare.

"We heard directly from the Chinese who said, 'If you have evidence, hard evidence, that we're committing this type of activity that you can prove in court, show us.' So we did," Carlin told a security conference months after the indictment.

A short time after the indictment, the Chinese military was linked to the theft of 80 million records from Anthem, the American health care provider. Then came the pillaging, also by Chinese military hackers, of Office of Personnel Management networks. The hack resulted in the loss of another 22 million records, including sensitive data from background investigations for security clearances.

Obama came close to imposing sanctions on the Chinese for the large-scale data hacking but backed off in September during the visit to Washington by Chinese President Xi Jinping, who promised to halt Chinese economic espionage in cyberspace. U.S. intelligence officials recently told Congress they were unable to verify that the Chinese ended the cyber attacks, a clear indication they have continued.

The State Department report, produced for a public-private partnership called the Overseas Security Advisory Council, or OSAC, said the indictment of Chinese military hackers was an "an unprecedented announcement, publicly blaming the Chinese government for espionage against the U.S. private sector."

"The five indicted Chinese military officers have also not yet been brought to court in the U.S.," the report said. "However, this case was among the first to highlight the threat of intellectual property theft from a nation-state, which remains a concern among many OSAC constituent organizations operating overseas."

The report said the indictments of the Iranians and Syrians highlighted the "blended threat" posed by foreign government and non-government hackers. It also showed that cyber attacks were behind the economic espionage confirmed in the PLA case, including cyber denial-of-service, intimidation, and extortion activities.

"The threat to the private sector is heightened as hackers look to carry out these various operations for both professional and personal gain," the report said.

"The traditional categories of threat actors-- nation-state, criminal, politically-motivated--no longer define all of the malicious network activity affecting U.S. private sector organizations," it added. "The 'blended threat' of hackers who are willing to work as proxies for governments or other organizations can hinder detection and prosecution in multiple ways."

The use of non-state hackers for foreign government cyber attacks makes it more difficult for authorities to identify the attackers, and allows nation-states or terrorist groups to benefit from the technical expertise of private sector hackers.

Additionally, proxies give foreign governments what spy agencies call plausible deniability--a key information warfare tactic allowing governments to avoid being linked to cyber attacks, the report said.

The report concluded that the recent indictments of Chinese, Iranian, and Syrian hackers "are unlikely to deter malicious cyber actors from exploiting this blended threat to target the U.S. private sector."

As Obama winds down his final term as president, it appears one of his legacies will be an unwillingness to take effective steps to counter cyber attacks against the United States that have caused serious damage to U.S. security.

As former NSA Director Keith Alexander has said, China is stealing everything it can to boost its economy. "It's intellectual property, it's our future. I think it's the greatest transfer of wealth in history," Alexander said.

New Zealand Herald

IRD team to sift through papers on foreign-owned trusts
Sunday, 08 May 2016
Byline: Nicholas Jones

Canberra - The IRD has set up a team to sift through documents about foreign-owned trusts from the Panama Papers.
A cache of material from the leak of documents from the Panamanian law firm Mossack Fonseca is due to be released today. Prime Minister John Key said the information could lead to law changes.

"It is quite useful that the Panama Papers get released," Mr Key said, "if that helps assist the New Zealand Government in making improvements to any of the laws that we have, or the partners that we work with like the OECD."

He said he did not condone the hacking of private information, but now that information would be released "there might be some benefits to gain from that".

Any New Zealanders found to be avoiding tax could expect a "knock at the door", he said, and if there was evidence of trusts being used improperly by foreigners the rules could be tightened.

Labour leader Andrew Little said the Prime Minister's tone had changed.

"There may well be now a rapidly changing position, which is because they discovered that, actually, most New Zealanders don't like this, and don't like us to be party to this."

Talk of the IRD investigating Kiwis was something of a distraction, he said, when the real issue was the use of the trusts by foreigners to avoid tax.

Labour wants the foreign trust industry shut down, but Mr Key called that a "knee-jerk" reaction.

Following the first release of details from the papers last month, the Government began a review of the disclosure rules for NZ's foreign trusts. Opposition parties have criticised the review's narrow focus.

An article in the Australian Financial Review on Friday shed new light on the number of foreign investors who had moved their cash and assets into tax-free New Zealand-based trusts, and the way these investors were able to minimise their tax.

It also said Auckland-based lawyer Ken Whitney, whose clients include Mr Key, had written a reference for Auckland law firm Cone Marshall to get accreditation with Mossack Fonseca in 2009.

After the release of the papers, Mr Key said Mr Whitney had assured him he had not had any dealings with Mossack Fonseca.

Yesterday the Prime Minister said the reference did not contradict that: "People give references all of the time."

Wall Street Journal
Twitter Bars Intelligence Agencies From Using Analytics Service
Monday, 09 May 2016
Byline: Christopher S. Stewart, Mark Maremont

New York - Twitter Inc. cut off U.S. intelligence agencies from access to a service that sifts through the entire output of its social-media postings, the latest example of tension between Silicon Valley and the federal government over terrorism and privacy.
The move, which hasn't been publicly announced, was confirmed by a senior U.S. intelligence official and other people familiar with the matter. The service--which sends out alerts of unfolding terror attacks, political unrest and other potentially important events--isn't directly provided by Twitter, but instead by Dataminr Inc., a private company that mines public Twitter feeds for clients.

Twitter owns about a 5% stake in Dataminr, the only company it authorizes both to access its entire real-time stream of public tweets and sell it to clients.

Dataminr executives recently told intelligence agencies that Twitter didn't want the company to continue providing the service to them, according to a person familiar with the matter. The senior intelligence official said Twitter appeared to be worried about the "optics" of seeming too close to American intelligence services.

Twitter said it has a long-standing policy barring third parties, including Dataminr, from selling its data to a government agency for surveillance purposes. The company wouldn't comment on how Dataminr--a close business partner--was able to provide its service to the government for two years, or why that arrangement came to an end.

In a statement, Twitter said its "data is largely public and the U.S. government may review public accounts on its own, like any user could."

The move doesn't affect Dataminr's service to financial industry, news media or other clients outside the intelligence community. The Wall Street Journal is involved in a trial of Dataminr's news product.

Dataminr's software detects patterns in hundreds of millions of daily tweets, traffic data, news wires and other sources. It matches the data with market information and geographic data, among other things, to determine what information is credible or potentially actionable.

For instance, Dataminr gave the U.S. intelligence community an alert about the Paris terror attacks shortly after they began to unfold last November. That type of information makes it "an extremely valuable tool" to detect events in real time, the intelligence official said.

In March, the company says it first notified clients about the Brussels attacks 10 minutes ahead of news media, and has provided alerts on ISIS attacks on the Libya oil sector, the Brazilian political crisis, and other sudden upheaval in the world.

U.S. government agencies that used the Dataminr service are unhappy about the decision and are hoping the companies will reconsider, according to the intelligence official.

"If Twitter continues to sell this [data] to the private sector, but denies the government, that's hypocritical," said John C. Inglis, a former deputy director of the National Security Agency who left in 2014. "I think it's a bad sign of a lack of appropriate cooperation between a private-sector organization and the government."

Analysis of Twitter and other social-media services has become increasingly important to intelligence and law-enforcement agencies tracking terror groups. Islamic State posts everything from battlefield positions to propaganda and threats over Twitter. San Francisco-based Twitter deletes thousands of accounts a month for violating its antiterror policies, but Islamic State supporters create new accounts almost as quickly.

"The volume of the group's activity on Twitter yields a vast amount of data that is a crucial tool for counterterrorism practitioners working to manage threats," said Michael S. Smith II, chief operating officer of the security consulting firm Kronos Advisory. "Twitter's decision could have grave consequences."

In a speech last September, David S. Cohen, a deputy director of the Central Intelligence Agency, discussed the importance of "open source" social-media data gathered by the CIA, saying Islamic State's "tweets and other social- media messages publicizing their activities often produce information that, especially in the aggregate, provides real intelligence value."

Silicon Valley and the U.S. government have been locked in intensifying conflicts over cooperation since the revelations by former National Security contractor Edward Snowden about government surveillance of electronic communication.

Most recently, Apple Inc. and the Justice Department were embroiled in a legal showdown over demands by the Federal Bureau of Investigation to unlock an iPhone used by one of the killers in the San Bernardino, Calif., attack in December. That fight--which unlike the Dataminr product involved the release of private data--ended in March when the FBI found another way to access the phone.

In-Q-Tel, a venture-capital arm of the U.S. intelligence community, has been investing in data-mining companies to beef up the government's ability to sort through massive amounts of information. In-Q-Tel, for example, has invested in data-mining firms Palantir Technologies Inc. and Recorded Future Inc.

U.S. intelligence agencies gained access to Dataminr's service after an In-Q-Tel investment in the firm, according to a person familiar with the matter.

When a pilot program arranged by In-Q-Tel ended recently, Twitter told Dataminr it didn't want to continue the relationship with intelligence agencies, this person said.

"Post-Snowden, American-based information technology companies don't want to be seen as an arm of the U.S. intelligence community," said Peter Swire, a Georgia Institute of Technology law professor and expert on data privacy.

Dataminr, based in New York, was launched seven years ago by three former Yale University roommates. A financing round early last year valued it at $700 million, according to Dow Jones VentureSource.

Its product goes beyond what a typical Twitter user could find in the jumble of daily tweets, employing sophisticated algorithms and geolocation tools to unearth relevant patterns.

Dataminr has a separate, $255,000 contract to provide its breaking news-alert service to the Department of Homeland Security, which is still in force.

Associated Press
Lawmakers, advocates push to reveal extent of surveillance
Monday, 09 May 2016

Washington - Even though the bulk collection of Americans' telephone records has ended, calls and emails are still being swept up by U.S. surveillance work targeting foreigners. Congress is making a renewed push to find out how many.
Six Republicans and eight Democrats on the House Judiciary Committee have asked the nation's top intelligence official for the number of Americans' emails and phone calls collected under programs authorized by Section 702 of the Foreign Intelligence Surveillance Act.

The programs target foreigners, but domestic communications sometimes are vacuumed up as well. They were first revealed to the public by Edward Snowden, who leaked files from the National Security Agency.

"Surely the American public is entitled to some idea of how many of our communications are swept up by these programs," the committee members wrote in their April 22 letter to Director of National Intelligence James Clapper.

They weren't the first to request the information.

In the past five years, Democratic Sens. Ron Wyden of Oregon and Tom Udall of New Mexico have asked repeatedly. Last October, a coalition of more than 30 civil liberties groups wrote Clapper seeking the information. Unsatisfied with the answer they received, they wrote him again in January.

Intelligence officials have tried to assuage concerns of Congress and others by saying that any domestic communications collected are "incidental" to the targeting of foreigners. They say Section 702 allows the government to target only non-U.S. persons reasonably believed to be located outside the United States. They say the law explicitly bars the government from targeting a foreigner to acquire the communications of an American or someone in the U.S. But they say intelligence agencies are authorized under Section 702 to query communications made with U.S. persons under certain cases with certain approvals.

Late last month, Clapper said intelligence agencies are looking into several options for providing an estimate and will do their best to come up with a number.

"This tool is a terrific producer of critical intelligence for this country and our allies," Clapper said recently about continued need for Section 702 programs.

He did not say how soon an estimate could be released and cautioned that "any methodology we come up with will not be completely satisfactory to all parties."

Even Congress acknowledges that producing an estimate could require reviewing actual emails, for instance, those acquired under Section 702, which itself could raise privacy concerns. But lawmakers say they are only advocating a "one- time, limited sampling" of communications.

Intelligence officials held briefings last week for congressional aides to explain ways an estimate could be provided. That is something Congress wants to get before it starts debating whether to reauthorize Section 702, which is set to expire at the end of next year. The Senate Judiciary Committee plans a hearing Tuesday on the issue.

Intelligence officials also briefed privacy advocates in March and are expected to hold another this month on the best way to estimate the extent to which domestic communications are ensnared in the quest for foreign intelligence. Among the problems is determining the citizenship of a caller or emailer, or whether the person is inside or outside the United States.

"We can't go into what I hope will be an extensive public debate without this basic information," said Elizabeth Goitein, co-director of the Brennan Center for Justice's program on liberty and national security.

In a recent article, Goitein wrote: "The National Security Agency acquires more than 250 million Internet communications each year under this program. Given the ubiquity of international communication, this number is virtually certain to include tens of millions of exchanges that involve Americans, but there is no official public data on how many Americans' communications are swept up."

Congress and privacy advocates got a glimpse into Section 702 surveillance from a congressionally mandated report that Clapper's office released this past week. The report said Section 702 surveillance targeted 94,368 foreign persons, groups or entities outside the U.S. last year, up slightly from 92,707 in 2014.

While the year-to-year increase is small, Jameel Jaffer, deputy legal director at the American Civil Liberties Union, notes that the number of targets has risen to more than 94,000 since the surveillance became legal in 2008.

The report also said that 23,800 queries concerning U.S. persons were conducted on the database, although the report notes that one of the intelligence agencies involved in the queries, which was not identified, did not provide this information.

The report also said 4,672 search terms concerning U.S. persons were used to retrieve information from Section 702 data, but privacy experts point out that the number excludes queries conducted by the FBI.

"It's true that the targets are foreigners, but in the course of targeting those 94,000 people, the government collects the communications of many, many - we don't know the number - Americans," Jaffer said. "That number is missing."

New York Times
Police and Tech Giants Wrangle Over Encryption on Capitol Hill
Monday, 09 May 2016
Byline: Cecilia Kang

Washington - Cyrus R. Vance Jr., the district attorney of Manhattan, visited Washington late last month to argue his case on a pressing issue: encryption.
In a string of meetings with members of Congress, Mr. Vance told central lawmakers that encryption needed to be diminished during criminal investigations. During a 45-minute session with Senator Angus King, an independent from Maine who is on the Senate Intelligence Committee, Mr. Vance said his office had 230 iPhones that might contain crucial information for cases but were useless because Apple refused to help the police break the encryption on the devices.

"I wanted to express a sense of urgency around resolution of this issue," Mr. Vance said in an interview about his Washington visit.

A day after Mr. Vance was on Capitol Hill, tech executives including Kent Walker, the general counsel of Google, and Brad Smith, president of Microsoft, also met with lawmakers -- but with a very different message on encryption. Tech executives at the meetings said they were concerned about any laws that would force companies to weaken the security of their technology, according to news officials representing these companies.

This kind of behind-the-scenes lobbying has become de rigueur in Washington as the battle over encryption shifts to Capitol Hill. It is the next phase of a bitter divide that spilled into public view this year when Apple refused to comply with a court order to help bypass security functions on an encrypted iPhone used by an attacker in the San Bernardino, Calif., mass shooting last year. Doing so would have let the F.B.I. gain access to the phone. That case ended after the F.B.I. found an alternative way into the device.

Yet the standoff between the United States government and Silicon Valley tech companies continues -- and the flurry of activity around the issue is broadening. Last month, a Senate draft encryption bill, written by Richard M. Burr, Republican of North Carolina, and Dianne Feinstein, Democrat of California, rallied the attention of both sides. The bill would require tech companies to give access to encrypted data with court orders.

Law enforcement officials immediately announced their support of the bill and began to push lawmakers to back it. Trade groups representing tech companies like Apple and Facebook have flooded into congressional offices, sent letters expressing concerns that the bill weakens consumer privacy and security, and delivered scorching speeches about the proposals.

"This is an escalating fight," said Robert D. Atkinson, president of the Information Technology and Innovation Foundation, a research firm based in Washington that is funded by tech companies including Google and Microsoft. "It's become the focus now in Washington, with hearings and legislative activity."

Law enforcement officials blame tech companies for creating the impasse.

"There's no question our relationship with the tech industry has gotten worse, and now it seems like the tech industry is taking every opportunity they have to put up obstacles in our way, including trying to derail legislative efforts that would give law enforcement what they need to keep people safe," said Terrence Cunningham, president of the International Association of Chiefs of Police.

Facebook, Google and Microsoft declined to comment on their lobbying activity. An Apple spokesman said the company has met regularly with members of Congress on encryption and other issues.

The amount of lobbying on the encryption bill is unusual at this early stage of a bill's life, showing the stakes involved. Tech companies are reluctant to give access to encrypted information from their users, for privacy reasons and because it may affect their businesses. Law enforcement officials say their efforts to prevent and solve crime are hampered if they cannot see digital data on phones, messaging services and other technology services.

"Today, terrorists and criminals are increasingly using encryption to foil law enforcement efforts, even in the face of a court order," Senator Feinstein said in a statement about the draft bill. "We need strong encryption to protect personal data, but we also need to know when terrorists are plotting to kill Americans."

The rhetoric in Washington around encryption has grown increasingly sharp. Last month, when the contents of the draft encryption bill were leaked, the president of the Consumer Technology Association, a trade group that counts Apple, Google, Facebook and Amazon among its 4,000 members, spoke to an audience filled with government officials at a lunch hosted by the Media Institute.

The bill is "dangerously overreaching and technically unsophisticated," said Gary Shapiro, president of the association. "This bill would essentially make effective cybersecurity illegal in the United States, pushing companies that take cybersecurity seriously offshore."

Other tech trade groups, including Reform Government Surveillance and the Business Software Alliance, have also waded into the fray, sending critical letters and meeting with senators to warn of the dangers of the bill. And Silicon Valley executives have, in increasing numbers, made the trek to Washington to make their cases directly.

Bob Lord, chief information security officer at Yahoo, visited several members of Congress in late April to talk about the technology behind encryption and to warn of the "unintended consequences" of legislation that could weaken security. While he did not specifically mention the Burr-Feinstein bill, he emphasized how consumers and human rights activists worldwide depend on encrypted technology for their safety and privacy.

"The notion that we would weaken encryption or provide back doors, those suggestions will have unintended consequences," Mr. Lord said.

Law enforcement officials, in turn, have frequently met with the same lawmakers in the Senate and House intelligence, judiciary and commerce committees who are being targeted by the tech companies, according to congressional staff members. Chief Cunningham and other members of the police chiefs' group have talked with Mr. Burr and Ms. Feinstein, given opinions during the drafting of the legislation and hosted panels on encryption for House and Senate lawmakers.

Tech companies have turned to certain politicians to champion their cause, such as Senator Ron Wyden, a Democrat from Oregon. On the day the draft encryption bill was introduced, Mr. Wyden, who voted

against the 2012 copyright bills known as the Stop Online Piracy Act and the Protect Intellectual Property Act, which were also opposed by the tech industry, said he had been flooded with calls from tech companies wanting to know what he would do.

Mr. Wyden said he intended to filibuster the proposal. He has since met with Intelligence Committee members to persuade them to kill the bill.

"I have not filibustered many issues, but I think the stakes are enormous," Mr. Wyden said in an interview. "The bill as written is a lose- lose, because it will create less security, American families will be less safe, and your liberty and privacy will be damaged."

For all the lobbying, few lawmakers have expressed their views on the encryption bill.

"I'm reserving judgment," said Senator King, who met with Mr. Vance last month. "The issues are so complex, it's like trying to nail Jell-O to the wall."

Canadian Press
IBM and universities join forces in battle against cybercrime
Wednesday, 11 May 2016

Ottawa - IBM wants its Watson computer system to learn how to fight cybercrime and it's asking eight leading universities, including three in Canada, for help. Watson - IBM's question answering computer system - was originally designed to compete (and win) on the television quiz show Jeopardy, but the technology has since been used on other problem-solving projects.
Now IBM is launching Watson for Cyber-security - a cloud-based version of their cognitive technology - that will be trained over the next year to examine threats of cybercrime.

Caleb Barlow, vice-president of IBM Security, said it is becoming increasingly difficult for security staffto deal with the growing number of cyber threats.

"Your average enterprise is dealing with 200,000 incidents a day that they've got to dig through. Human beings simply cannot look at all of that data," he said.

"Combine that with the fact we have a major skill shortage in the security industry - around 1.5 million jobs by 2020 - and even if we could fill all those jobs we still can't get through the data as it continues to grow."

Barlow said experts are doing a good job to examine cyber threats, but their work often ends up in various forms such as reports, blogs and presentations and in numbers too large for others to read and remember.

That's where Watson comes in.

Students at the eight universities, including the University of New Brunswick, University of Ottawa and the University of Waterloo, will put the information in a form the computer can understand and help train the system to use that information to examine cyber threats.

"The more information that Watson has, the better reasoning it can provide and therefore in some cases the better prediction it can provide," said Ali Ghorbani, dean of the faculty of computer science at the University of New Brunswick in Fredericton.

The students will input about 15,000 security documents per month during the year-long project, starting this fall.

"Our students are getting involved in a real-world cyber-security project with a global company. Not only will they increase their knowledge, but also create a relationship with IBM for future collaborations - either jobs for our students or more research and development projects with IBM," Ghorbani said.

He said IBM is hoping that not only will Watson be able to provide early warnings of potential attacks, it will also do it fast.

Barlow said IBM opened its entire threat intelligence database to the world a year ago, and invited people to develop applications to work with their QRadar software.

That software was developed by Q1 Labs, developed in turn at the University of New Brunswick, and purchased more than four years ago by IBM.

He said by getting information out to security staffaround the world, cybercrime may become less lucrative for organized crime.

"We start changing the dynamic for the bad guys because it's not worth investing $100,000 or more in that new attack you've got if it's only going to be viable for a few minutes before we find it and tell the rest of the world," Barlow said.

CBC.CA
Air Canada employees told to seek extra ID from kids even after feds' screening directive
Wednesday, 11 May 2016
Byline: Shanifa Nasser

Ottawa - A passport, a school ID card or even an Aeroplan number are among the pieces of identification Air Canada employees were instructed to obtain from children, even as the federal public safety minister said additional security screening was not required for people under 18.
Screenshots of documents taken by an Air Canada employee in January, sent to CBC News show the airline carrier issued a directive to employees stating children are not subject to extra screening measures, but goes on to list numerous such steps to clear what is known as the "deemed high profile" or DHP list. CBC News agreed to protect the employee's identity because of concerns of job termination.

"Children are not subject to extra screening under the Transport Canada Secure Air Travel Act (SATA) and Passenger Protect Program; however, until a passenger has been seen by an Airport agent, we cannot confirm their identity and date of birth," the screenshot says.

The revelations come just after the Minister Goodale announced that Canada and the U.S. set up a working group to help prevent false-positives for children matching names on no-fly lists.

The no-fly list is generated by the government, but "piggybacked onto the computer systems of the airlines. It's not an interactive system," he said Tuesday, admitting changes to the problem of false security-list matches won't be quick or easy.

By contrast, the American system is entirely government run and is entirely interactive, Goodale said.

"You've got to change the entire database."

In a statement, Air Canada representative Peter Fitzpatrick told CBC News it is a legal requirement that all passengers be vetted against watch lists, adding that children whose names are similar to a flagged name are "uniquely identified and cleared."

Employees are "instructed to use an Aeroplan number because it is a unique identifier (unlike a birthday because people share birth dates and the information can sometimes be entered incorrectly,)" Fitzpatrick said.

But to Toronto-area Khadija Cajee, whose six-year-old son, Adam Ahmed, nearly missed an Air Canada flight to Boston last year because his name showed up on the DHP list, an Aeroplan number makes little sense.

"I can log on as Bugs Bunny and get an Aeroplan number. It's not a foolproof government identification. It's a loyalty program," Cajee said.

Since Ahmed's case made headlines, more than 40 other parents have come forward through social media and other means, with the same complaint.

Cajee, meanwhile, has found herself the unwitting liaison for the group #NoFlyListKids and the government.

One of those mothers, based in Kamloops, said on Tuesday that Air Canada employees have recommended she change her baby's name to bypass the delays.

"I wasn't happy with that," Faaria Siddiqui told CBC News. "How do we know if we change his name it won't be on the list or the name we choose won't be on list?"

Reuters
SWIFT rejects Bangladeshi claims over $81 million cyber heist
Wednesday, 11 May 2016

Dhaka - SWIFT has rejected allegations by officials in Bangladesh that technicians with the global messaging system made the nation's central bank more vulnerable to hacking before an $81 million cyber heist in February.
The comments were in response to a Reuters story that cited Bangladeshi police and a central bank official as saying that SWIFT technicians introduced security holes into the bank's network while connecting SWIFT to Bangladesh's first real-time gross settlement (RTGS) system.

"SWIFT was not responsible for any of the issues cited by the officials, or party to the related decisions," the Brussels-based bank-owned cooperative said in a statement posted on its website on Monday.

"As a SWIFT user like any other, Bangladesh Bank is responsible for the security of its own systems interfacing with the SWIFT network and their related environment - starting with basic password protection practices - in much the same way as they are responsible for their other internal security considerations," the statement said.

But Bangladesh's main police investigator maintained there were loopholes in the way SWIFT carried out the integration of its network with the RTGS platform that left the central bank's computer systems vulnerable to hackers.

Mohammad Shah Alam, the head of the Criminal Investigation Department of the Bangladesh Police, said the probe had identified specific deviations from set procedures that compromised Bangladesh Bank's security. "We stand by our investigation," he said in response to the comments by SWIFT.

But he added he did not want to engage in a debate and urged greater international cooperation to identify the culprits behind one of the world's biggest cyber thefts.

Reuters has not been able to independently verify the allegations by Bangladeshi officials about the SWIFT technicians.

US investigators suspect the involvement of employees of the Bangladesh Bank in helping the hackers breach the systems, the Wall Street Journal said, quoting people familiar with the matter.

It said the Federal Bureau of Investigation had found evidence that at least one bank employee acted as an accomplice but there could be more who assisted the hackers in navigating around Bangladesh Bank's computer systems.

Bangladesh Police said they have been looking for inside involvement in the heist from the beginning of the probe, but no evidence has turned up against anyone.

Investigators say they think there was some level of local facilitation in the attack on the central bank's computers but haven't identified it as yet. "If the FBI has uncovered evidence, they should share with us," a police officer said.

The revelations came ahead of a meeting on Tuesday in Basel, Switzerland, where Bangladesh Bank officials have said their governor and a lawyer appointed by the bank would discuss recovery of about $81 million stolen by hackers with the head of the Federal Reserve Bank of New York and a senior executive from SWIFT.

The money was stolen from Bangladesh Bank's account at the New York Fed through fraudulent transfer orders sent on the SWIFT system.

SWIFT's statement said it "looks forward to the meeting with Bangladesh Bank and New York Federal Reserve Bank officials in Basel on 10th May, when the bank's security issues and these baseless allegations will be discussed."

Bangladesh Bank officials have said they believed SWIFT, and the New York Fed, bear some responsibility for the February cyber heist.

Gulf News
Banks to face growing challenge on data security
Wednesday, 11 May 2016
Byline: Babu Das Augustine

Dubai - In the context of rising cases of data breaches across regional financial institutions, KPMG expects the UAE based banks to face growing challenges from hackers and other malicious actors. "In November 2015, we surveyed a broad range of KPMG clients in the UAE to better understand their cyber security arrangements and their level of preparedness to respond to a cyber-attack. What we learned clearly showed that many organizations in the UAE -- including financial institutions -- continue to struggle in a number of different areas," said Cristian Carstoiu, Director, Management Consulting.

The survey showed that many UAE organisations find it difficult to develop an adequate investment case to recruit the right level of expertise and to implement appropriate security technologies, even against a backdrop of increasing concern over cyber security attacks in the region.

"We believe many organisations in the UAE need to improve their emergency response and contingency plans in order to appropriately respond to, and recover from, a cyber breach. Organisations in the UAE also need to better understand their threat profile: who, when and why they are likely to be targeted," said Carstoiu.

The study also said that many boards in the UAE -- where the ultimate responsibility for cyber security lies -- do not have a comprehensive or accurate view of their cyber risks, often because threat intelligence and cyber monitoring have been inconsistently implemented.

Global Times
Activist's cyber hunt violates moral codes
Wednesday, 11 May 2016
Section: editorial

Internet activist Wen Yunchao on Sunday launched a cyber manhunt on Twitter aimed at five experts and technical personnel who helped improve China's Great Firewall. Wen encouraged Net users to find out whether the five, four of whom are professors and postgraduate students from a university in Nanjing, have any personal issues or are engaged in academic corruption.
Wen is a radical political dissident, who was disciplined many times at his Chinese university for various reasons. After he began his studies in the US in 2009, he gradually became a democracy activist against the Chinese political system.

Wen often voices aggressive opinions over freedom of speech and judicial justice. But the manhunt he initiated is a far cry from his philosophy.

These cyber manhunts go severely against cyber ethics, and for a number of reasons are violations of the law. However, it is unfortunate that Twitter has done nothing about it after the case was reported by some Western media. Imagine if Edward Snowden called for a cyber manhunt against all the designers of the US surveillance program PRISM on social networks, would Twitter still be so indifferent?

Certain dissidents have totally lost their moral bottom line nowadays. They flatter themselves that they stand on the moral high ground. Assuming that they did everything for a just cause, they think they can thus trample on ordinary people's codes of conduct.

Every country is responsible for its own cyber management. Technical inventions by a few researchers do not have any political nature.

Yet Wen attacked those technical workers online because of objections to the Chinese firewall. Such paranoia is familiar to us.

No matter how many grudges one has over social governance, he cannot publicly infringe on the rights of others like Wen has done. Otherwise, the entire society will fall into chaos.

After some dissidents fled to the US and other Western countries, they have not only had "more freedom" to express their political views, but also showed the dark side in their humanity. They seem to be so anxious to witness great disorder in China in no time. There is no telling whether their behavior stems from their own issues or the influence of the anti-China forces in the US.

That these malcontented dissidents living abroad, who are losers in life, are washed out by China's reform and opening-up is amusing and thought-provoking.

Khaleej Times
Smart tech set to revolutionize airports
Wednesday, 11 May 2016
Byline: Staff Report

Dubai - The 16th edition of the Airport Show, currently under way at the Dubai International Convention and Exhibition Centre with over 300 exhibitors from 55 countries, has been utilised as a platform to showcase technologies and innovative solutions by multi-national and regional companies.
Some of the prominent technology devices that are being showcased include the Intelligent Trolley and Trolley Security Scanner by Denmark-based Exruptive, an associate company of Dubai-based emaratech, airport runway cleaning systems by US-based Cyclone Technology, Smart Tray cargo and baggage handling systems by Siemens, driverless shuttle by Navya ARMA and the latest face recognition technology by Rockwell Collins.

The Intelligent Trolley will act as a passenger's personal guide through the airport. It can be used to power personal devices, act as a real-time way finding device in the airport via an interactive 3D-map. For flight and gate information, the device updates information on a real-time basis and keeps the passenger updated.

"We are extremely pleased with the response from trade visitors. There have been invitations to visit many airports," said Morten Pankoke, chief operating officer of Exruptive.

Rockwell Collins'face recognition technology captures a traveller's identity using biometrics and matches it with the passenger's passport and boarding pass information.

Dr Ian Bache PMP, technical pre-sales director, Arinc Airports Information Management Services, Rockwell Collins, said: "Airports are always looking to automate passenger processing while maintaining the highest security levels. We offer tailor-made solutions which can be configured with airport identity management solutions. Many airports in this region are showing interest in these technologies." US-based Cyclone Technology has displayed an ultra high water pressure system, The Cyclone 4006, which cleans airport runways and apron surfaces more effectively and in less time than other methods. The patented cleaning and recovery head cleans and removes rubber and paint build-up without damage to the surface.

Siemens is showcasing its latest baggage handling systems, prominent among them is 'smart tray' or SmartTilter, Siemens' solution for the dynamic tilting of tray conveyors, which help get baggage to its destination as quickly as possible.

Navya ARMA introduced a 100 per cent electric and intelligent driverless shuttle which can transport up to 15 passengers and safely drive up to 45 km/h. Navya, the French company which has conceptualised and manufactured the vehicle, is keen on introducing the shuttle at airports across the Middle East region.

The National (UAE)
Beijing postpones implementing new e-commerce regulations

Wednesday, 11 May 2016
Byline: Saibal Dasgupta

Beijing - In a rare move, China today held back implementation of new regulations that were passed last month on goods imported from overseas markets using e-commerce platforms. The government said it will now make adjustments to the rules before they are brought in.
The decision indicated that Beijing is going through a process of rethinking over the use of the internet for a variety of business and security-related functions.

On Monday, the government ordered Beijing's Baidu, one of the world's largest search engines, to revamp its vast business spanning several countries. The cyber administration of China asked the Nasdaq-listed Baidu to formulate a new and more credible algorithm and restrict the amount of promotional content by May 31.

These developments have taken place against the backdrop of the government drafting and finalising three different laws on cybersecurity and new counter terrorism laws. Foreign companies and industry lobby groups are worried that the proposed regulations may impinge on their privacy and force them to share "sensitive intellectual property" with the government in the name of "national security".

"Foreign companies feel they are vulnerable towards potential scrutiny and even attacks by Chinese authorities," Yun Sun, a senior associate with the East Asia programme at the Washington think tank Stimson Center, told The National today.

She said the new laws make foreign companies vulnerable towards potential scrutiny or even potential investigation by Chinese authorities. "This reduces the security level for these companies and their products, and also threatens the credibility for their operations in the global market," she said.

Beijing says the new laws have mainly been brought to deal with the threat of terrorism from militants involved in the East Turkmenistan movement in western China's Xinjiang province, and the enhanced global fears after the recent terrorist attacks in parts of Europe and Egypt. The Xinjiang-based militants have attacked targets in Beijing and Kunming cities besides carrying out bomb attacks in the western province in recent years.

"The government's main objective is to fight terrorist using the cyber space to further their activities. But it also wants to control data flow. It is this aspect that would hurt businesses," Ada Wang, a legal counsel and compliance officer with TUVRheinland, said yesterday.

"The new laws will not just affect foreign companies. It would also hamper Chinese companies operating overseas because the government does not want sensitive date to leave the country," she said. Indeed, the rules make it obligatory for companies to use specified infrastructure, and ensure that their websites are hosted in satellites hovering over China, and not in foreign locations.

Other Chinese experts and businessmen see it differently. "There will be a new phase for internet development in China," said Xiong Huang, a researcher at Communication University of China, said listening to the Chinese president Xi Jinping talk about the importance of internet security at a conference in Beijing last month.

Following the event, Jack Ma, the founder and chairman of China's giant e-commerce company Alibaba Group, said: "This is the first high-profile meeting in the internet field for our country. Not only does the meeting show how much China values the internet as a national strategy, but the country has a quite high level in both practice and theory on the development of the internet. I'm firm about the internet development in China after the speech."

What the regulations might do is force more foreign companies to enter into joint ventures with local enterprises to make sure they do not cross the line and attract the wrath of the authorities empowered with the new legislation.

The laws cover all businesses engaged in transmission of data via cyber space. The regulations state that companies are expected to: assist authorities in unravelling complicated data whenever required; use data infrastructure that is based in China; use encryption technology before transmitting data outside China; never generate or use data in any manner that would affect the country's national security; disallow any person, groups or organisation to use their internet platforms to disseminate propaganda against Chinese political systems, or instigate the local population against government authorities.

One of the implications of the new law is that it will involve additional costs to build secure internet infrastructure and hire legal services to deal with compliance issue. This is partly because the new law is vague about compliance requirements, and not specifically pinpointed, an analysts said.

Companies based in Hong Kong will now be treated as offshore enterprises, and treated as foreign firms under these laws. This can be a bothersome to foreign companies because many of them are registered in Hong Kong, and not in mainland China.

One analyst, who declined to be named, said that the rules are not meant to target foreign companies. "They have merely come in the way of these laws because they impose a wide range of restrictions on the use of internet, and flow of data," he said.

New York Times
Sensitive Email Routinely Sent as Unclassified
Wednesday, 11 May 2016
Byline: Steven Lee Myers

Washington - On the morning of March 13, 2011, the assistant secretary of state for Near Eastern affairs, Jeffrey D. Feltman, wrote an urgent email to more than two dozen colleagues informing them

that Saudi Arabia and the United Arab Emirates were sending troops into Bahrain to put down antigovernment protests there.
Mr. Feltman's email prompted a string of 10 replies and forwards over the next 24 hours, including to Secretary of State Hillary Clinton, as the Obama administration debated what was happening and how to respond.

The chain contained information now declared classified, including portions of messages written by Mr. Feltman; the former ambassador in Kuwait, Deborah K. Jones; and the current director of the Central Intelligence Agency, John O. Brennan.

The top administration officials discussed the Bahrain situation on unclassified government computer networks, except for Mrs. Clinton, who used a private email server while serving as secretary of state.

Her server is now the subject of an F.B.I. investigation, which is likely to conclude in the next month, about whether classified information was mishandled.

Whatever the disposition of the investigation, the discussion of troops to Bahrain reveals how routinely sensitive information is emailed on unclassified government servers, reflecting what many officials describe as diplomacy in the age of the Internet, especially in urgent, fast-developing situations.

A review of the 30,322 emails from Mrs. Clinton's private server that the State Department has made public under the Freedom of Information Act provide an extensive record of how such sensitive information often looped throughout President Obama's foreign policy apparatus on unclassified systems, from embassies to the United Nations to the White House.

The senders included Denis R. McDonough, currently the White House chief of staff and previously the deputy national security adviser, and Susan E. Rice, the former American representative at the United Nations who is now Mr. Obama's national security adviser.

Many of the emails were sent over the State Department's unclassified system, state.gov, which is considered secure but not at the level of the State Department's system for emailing classified information.

At the State Department, the Pentagon and the White House, among other agencies, officials have two systems for email, one for classified messages and one for more routine business. They are nicknamed the "high side" and the "low side."

Mrs. Clinton's private server -- set up in her home in Westchester County, N.Y. -- was assumed to be even less secure than the State Department's "low side," although the unclassified servers at some government agencies have been hacked in recent years.

One result of Mrs. Clinton's decision to maintain a private server is that it has put State Department officials on the defensive about their use of state.gov for some business that might be considered classified.

Of the 30,322 emails made public, 2,028 have had portions redacted and are now classified at the lowest level of classification, "confidential."

Nearly three-quarters of those emails were classified because they contained what is called "foreign government information" -- a vast category of information, gathered through conversations and meetings with foreign counterparts that are the fundamentals of diplomacy, but which had to be protected when the emails were released.

Last week, in an apparent attempt to dispel criticism that many of the emails were improperly sent, a top State Department official argued in a letter to three Senate Democrats that the nation's diplomats and officials were in fact allowed to send "foreign government information" through the government's unclassified computer systems.

"Department officials of necessity routinely receive such information through unclassified channels," said the letter, dated May 2 and written by the assistant secretary of state for legislative affairs, Julia Frifield.

"For example, diplomats engage in meetings with counterparts in open settings, have phone calls with foreign contacts over unsecure lines, and email with and about foreign counterparts via unclassified systems."

The letter went on to say that using "foreign government information" in unclassified emails "does not amount to mishandling the information."

The State Department, unlike some other federal agencies, does not have the authority to redact that category of information even if it is required to release documents under the Freedom of Information Act.

Thus, the only way the State Department could withhold "foreign government information" in the emails being released under court order was to classify it, according to the letter.

The letter was a reply to one sent in March to Senators Patrick J. Leahy of Vermont, Thomas R. Carper of Delaware and Dianne Feinstein of California. A copy was given to The New York Times by a government official who believed the classification of the emails was unfairly implicating diplomats and other officials conducting diplomacy in the modern era.

Of the 30,322 emails, the F.B.I.'s investigation has focused on a smaller number, including 22 that the C.I.A. insisted contained information classified "top secret."

Those emails have not been released, even with redactions, because they include material classified at the highest levels, known as "top secret/SAP," according to a letter from the inspector general of the nation's intelligence agencies, I. Charles McCullough III.

That designation refers to "special access programs," which are among the nation's most guarded secrets. The emails are said to include references to, among other things, the C.I.A.'s program to hunt and kill suspected terrorists with armed drones in Pakistan.

An additional 65 emails, which have been released, have had portions redacted because they included information classified at the level of "secret."

One exchange of emails typical of those now classified because they contain "foreign government information" involved Mr. McDonough, Ms. Rice and her deputy at the time, Rosemary A. DiCarlo, and the Palestinian effort in September 2011 to be recognized as a state by the United Nations.

The exchange included eight separate emails, all sent on unclassified networks. Of those, six were redacted almost completely when the State Department released them in January.

According to the subject line and what information does appear, the three discussed deliberations between the United Nations secretary general, Ban Ki-moon, and the Palestinian president, Mahmoud Abbas, as well as Ms. Rice's discussion with the Palestinian representative at the United Nations, Riyad H. Mansour, on the bid for statehood -- all instances of "foreign government information."

The chain of emails eventually encompassed 16 officials, including political appointees and career diplomats, and was ultimately forwarded to Mrs. Clinton's inbox by Jake Sullivan, her deputy then and now the senior policy adviser for her election campaign.

Philip H. Gordon, an assistant secretary of state under Mrs. Clinton, said, "If all these respected, senior foreign service officers and experienced ambassadors are sending these emails, then this issue is not about how Hillary Clinton managed her email, but how the State Department communicates in the 21st century."

Mr. Gordon, later a special assistant to the president for the Middle East, wrote more than 40 emails that were redacted on the grounds that they contained classified information.

Mrs. Clinton herself wrote, responded to or forwarded 96 emails that have been classified in part, including one that is classified secret; 46 of those contained the "foreign government information" that the department's letter addressed.

There are, to be sure, other emails that do not fall into the category of "foreign government information," and some raise questions about the sort of information senior officials sent in unclassified emails.

In 18 emails, for example, information has been classified on the grounds that it identifies C.I.A. officials, including two instances that are now considered "secret."

One of those was a seemingly benign photo opportunity listed on Mrs. Clinton's daily schedule, with the person who gave her a daily intelligence briefing, making it obvious that the person was an agency employee.

That email was originally released as "confidential" but upgraded to "secret," probably reflecting that the person holds an undercover position now.

Another exchange involving the C.I.A. came the day after David H. Petraeus resigned as the agency's director in November 2012. Mr. Brennan, then still at the White House, sent an email -- detailing the provisions for Mr. Petraeus's personal security following his surprise resignation -- to Thomas E. Donilon, Mr. Obama's national security adviser. Mr. Donilon then forwarded it to Mrs. Clinton.

"Madam Secretary -- Attached is an update on the security for Dave P.," he wrote. The entirety of Mr. Brennan's note has now been redacted and classified as "confidential" on the grounds that it involves "vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security."

Mr. Petraeus ultimately pleaded guilty to a misdemeanor for keeping highly classified information in eight black notebooks he kept in his home, including such details as the names of covert officers and programs, and sharing them with his biographer and lover.

A spokesman at the C.I.A., Ryan Trapani, said in a statement that Mr. Brennan had believed that the information he sent in the email was unclassified.

"When operating in a position like he was at the White House, officials often have to make spot judgments about whether information is classified or not," he wrote.

"In most cases, the determinations are correct, but in some situations, another agency may consider certain information classified that the author does not."

The Hill
19 months before deadline, lawmakers draw battle lines on spying powers
Tuesday, 10 May 2016
Byline: Julian Hattem

Washington - Members of Congress are starting to put down markers in a major battle over U.S. spying powers that it expected to drag on for more than a year.
The early action appears to reflect an effort by leading Republicans and national security hawks to get out in front of privacy advocates who want to restrict the National Security Agency's power to collect reams of data about foreigners suspected of being spies, terrorists or other targets.

Information about an unknown number of U.S. residents is also included in sweeps authorized by Section 702 of the Foreign Intelligence Surveillance Act.

The law must be renewed by December 2017, but the Senate Judiciary Committee on Tuesday held a hearing on the issue 19 months before that deadline.

"I'd like to begin a conversation about it well in advance of that reauthorization," Chairman Chuck Grassley (R-Iowa) said at the start of Tuesday's hearing.

Recent terror attacks in Paris, Brussels and San Bernardino, Calif., he said, "underscore that one of the responsibilities of our government is to ensure that those who protect us every day, including the intelligence community, have the tools to keep us safe."

The law undergirds high-profile spying activities such as the PRISM and Upstream programs, but many of the details about its use remain in the shadows.

"We're still missing a lot of facts about Section 702 implementation," Sen. Patrick Leahy (D-Vt.), the committee's ranking member, said on Tuesday.

"It sweeps up a sizable amount of information about Americans who are communicating with foreigners," he added. "Despite these concerns about Americans' communications being swept up, we still do not know how much of our data is collected under this authority."

Despite repeated requests from Capitol Hill, intelligence officials have given no estimates of the number of Americans whose communications are caught up in warrantless government searches targeting foreigners. Because of the global nature of the internet, privacy advocates have warned that the number could be high.

Director of National Intelligence James Clapper has bristled at calls to estimate how many U.S. residents have their data swept up by the program, saying it would be difficult to calculate.

Leahy and a small handful of Democrats appeared open to modifications requiring officials to obtain a warrant before searching for data on citizens.

But any effort at reform appears primed to run into stiff opposition from lawmakers in both parties, given the broad consensus about the importance of the data gathering for combating terrorism.

"The question to me is do we want to somehow limit ourselves in terms of access to foreign intelligence in a way that could make us less safe?" asked John Cornyn (Texas), the No. 2 Senate Republican, rhetorically. "That's an important conversation to have, but I'm pretty clear on where I come down."

Lawmakers wondered on Tuesday whether implementing new warrant requirements could rebuild "walls" between U.S. surveillance agencies similar to those blamed, in part, for failing to prevent the 9/11 attacks.

And erring too far on the side of individual privacy might keep intelligence officials from finding important information, Cornyn warned. He pointed to examples in which al Qaeda operatives have used words like "wedding" and "marriage" as code words during a terror plots.

"In our zeal to protect love letters, we don't want to protect terrorists who might use code words to escape scrutiny by the intelligence community," he warned.

Sen. Dianne Feinstein (D-Calif.), the vice chairwoman of the Intelligence Committee, said that if anything, the government should be more forthcoming about the ways in which Section 702 is used.

"Those of us who meet two afternoons a week and go over intelligence ... see the value of this program," said Feinstein, referring to the Intelligence Committee's biweekly meetings. "But I think the general public does not."

"I really think it is lawful and well-balanced," she said.

"In my view, it's only intelligence, lawfully collected, that's able to prevent another attack in this country."

The Intercept
Hackers Attempt to Hold Capitol Hill Data for Ransom
Wednesday, 11 May 2016
Byline: Jenna McLaughlin

Washington - The House is under attack by hackers hoping to infiltrate congressional computers, encrypt their contents, and then force users to pay a ransom to get their access back.
"In the past 48 hours, the House Information Security Office has seen an increase of attacks on the House Network using third party, web-based mail applications such as YahooMail, Gmail," the House's Technology Service Desk wrote in an email to House staffers on April 30.

According to the email obtained by The Intercept, the hacked emails impersonate familiar people and invite staffers to download an attachment laced with malware--what's known as a "phishing" attack.

"When a user clicks on the link in the attack e-mail, the malware encrypts all files on that computer, including shared files, making them unusable until a 'ransom' is paid," the email said.

But House administrative offices refused to say how many if any attacks have been successful, what sort of data may have been affected, or how much has been paid in ransom, if anything.

"The potential for ransomware attacks the House faces is similar to any large organization," a spokesman for the Chief Administrative Officer of the House wrote in a statement to The Intercept. "The House recognizes the importance of taking steps to employ a cyber security plan to protect our infrastructure, and we constantly work to improve training and education for all House users."

A lockdown on parts of the House internet network--from WiFi to Ethernet--remains ongoing.

Access to both YahooMail and Google Cloud services hosted by Google's appspot.com appear to be completely blocked on the House's network, according to Ted Henderson, a former Hill staffer and founder of two social-network applications designed for Capitol Hill communication: Cloakroom and Capitol Bells. It's unclear if both blockages, not just Yahoo's, are related to the ransomware attacks.

Henderson says his several thousand users cannot post to the social networks inside the House office buildings. The way Cloakroom works, you're normally able to log-in either anonymously simply by using Capitol Hill Wi-Fi or with your staff email address. The Senate office buildings don't appear to be affected.

"This is the first time I've seen this happen at a scale like this in five years," Henderson wrote The Intercept in an email.

In recent months, several lawmakers have penned letters asking the Obama administration how it's dealing with the problem of ransomware--a type of attack more than two dozen government agencies have admitted to confronting in the past as well.

Now that Congress itself is the target, security researchers are hopeful the issue will draw more national attention. "What you're seeing in Congress is just part of what's happening," Markus Jakobsson, founder of "Zapfraud", a scam email detection service, and an expert on phishing attacks told The Intercept. "This will hopefully bring some awareness to decision makers...once they start [going after Congress], there will be changes."

Ransomware attacks take many forms. Some hackers have managed to infect entire websites with malware.

It's not clear whether the current spate of attacks on the House network were targeted, or whether House users just happened to find themselves among the ever-growing number of victims.

Ransomware is a major and growing threat to security. Just the day before the House emailed its staff about the attacks, the FBI published a press release titled "Incidents of Ransomware on the Rise," warning that "hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses" are all under increasing threat of being hacked and ransomed.

Nonprofit healthcare organization Health Information Trust Alliance warned in April that more than half of 30 hospitals it surveyed were infected with malware--most of it ransomware. Los Angeles hospital Hollywood Presbyterian paid $17,000 to recover its data in March.

Police departments have also been victims of ransomware attacks, sometimes forced to pay up to recover everything. One police chief compared the extortion to "what felt like terrorist threats."

It's not at all clear how to solve the problem, though researchers have come up with some solutions and recommendations. "This is something that the technical community is still struggling with getting a firm grip on," Jakobsson said.

He suggests Congress install several levels of filters to detect possible spam and scams, backup their data, and launch awareness campaigns to alert people to the reality of the problem. "The problem of social engineering is so vast that you can't just do one and hope that's enough," he said.

Motherboard (Vice)
Encryption Gets in The Way of 75% of Cases, Europol Chief Says
Tuesday, 10 May 2016
Byline: Joseph Cox

New York - In the US, police and prosecutors continue to say encryption--the use of math to protect data from outside eyes, including those of the government--presents a significant barrier to solving crimes or following leads.
Now, on the other side of the Atlantic, the head of Europe's law enforcement body is saying that encryption is an issue in the vast majority of cases the agency sees.

"Encryption dilemma must be solved soon. Real problem in 75% of all Europol cases," Rob Wainwright, director of Europol, tweeted on Sunday.

The tweet came in response to an op-ed written by John Naughton, a professor from the Open University, and published by the Guardian, that said an opportunity for more permanently addressing law enforcement's concerns around encryption had been lost during the FBI and Apple legal fight in San Bernardino.

It is not clear what sort of encryption Wainwright was referring to; be that message encryption to secure communications, or hard-drive encryption that protects data stored on devices, which was the issue at hand in the recent Apple case.

When asked about it, Claire Georges from Europol's corporate communications answered broadly about technologies used by criminals, citing encryption, anonymisation tools such as Tor, and even implied that virtual currencies such as bitcoin are part of the problem.

"The use of anonymisation and encryption technologies is widening and is key issue for law enforcement in all criminal areas," she told Motherboard in an email.

"Technology in general is used not only by cybercriminals, but also by drug dealers, child sexual offenders and other criminals involved in different illegal activities. Encryption is commonly used in secure communications and is becoming a standard protection feature in many products, such as e-wallets for virtual currencies."

Georges also pointed to Europol's Internet Organised Crime Threat Assessment (iOCTA) from 2014, which reads "The use of anonymisation tools is ubiquitous amongst the cyber underground."

Responding to a question of whether backdoors are an avenue for law enforcement, Wainwright wrote in another tweet that "back doors not the solution but regulated front door access. Finding how is key question."

Security experts say any sort of "front door," even if designed only for law enforcement, would be vulnerable to exploitation from hackers and malicious actors, undermining the security of all devices that used it.

Encryption, in some cases, may present an issue for law enforcement. But lumping message and hard-drive encryption, along with technologies such as Tor, all into the same basket is not helpful for anyone; as each requires a unique response, all balancing privacy, security, and access for police.

The Guardian (London)
Court refuses request to force alleged hacker to divulge passwords
Tuesday, 10 May 2016
Byline: Jamie Grierson, Diane Taylor

London - An alleged hacker fighting extradition to the US will not have to give the passwords for his encrypted computers to British law enforcement officers, following a landmark legal ruling.

Lauri Love, a 31- year-old computer scientist, has been accused of stealing "massive quantities" of sensitive data from US Federal Reserve and Nasa computers. His lawyers say he faces up to 99 years in prison if found guilty in the US.

The National Crime Agency (NCA) raided Love's family home in Stradishall, Suffolk, in October 2013, seizing encrypted computers and hard drives. No charges were brought against him in Britain and Love is suing the NCA for the return of six items of encrypted hardware, which he says contain his entire digital life.

The NCA applied to the courts to force Love to hand over his passwords before it returns the computers but this was rejected by a judge on Tuesday.

Speaking to the Guardian, Love called on governments around the world to set aside differences with activists and hackers and to work together to improve global computer security.

"The US government is conducting a war against information activists like me," he said. "This kind of thing is a distraction from what is really important - keeping the world secure. I am offering a 'third way' where governments and hackers work together and bridge the divide. Governments should be making the most of the talent that computer hackers have to try to work together to solve the problems of computer lack of security.

"If someone hacks into your computer they can take over your life and your identity. We are more and more reliant on computer security for security for ourselves."

Love said there was a lot of distrust of governments from activists as a result of scandals involving surveillance and undercover policing. "We have to put our differences aside," he urged. "What we really need to do is sit round the table together and start to have a conversation."

Love said the past few years of interactions with the police and US authorities had taken an enormous personal toll on both him and his family. "I spent two years in an acute and crippling state of mental distress," he said. "I developed eczema and had a lot of difficulty sleeping. Now I am feeling recovered enough to continue studying for my electrical engineering degree and have my finals coming up."

District judge Nina Tempia refused the NCA's application at Westminster magistrates court on Tuesday, saying that to do so would "circumvent specific legislation that has been passed in order to deal with the disclosure sought".

Speaking outside court after the ruling, Love said he was happy with the result and accused the NCA of trying to undermine protections safeguarding individuals' property.

"It is a victory, although it is a more an avoidance of disaster," he said. "It retains the status quo, which means there has to be safeguards before you force people to undermine their security."

His lawyer, Karen Todner, of Kaim Todner, said the ruling was right. "The case raised important issues of principle in relation to the right to respect for private life and right to enjoyment of property and the use of the court's case management powers.

"A decision in the NCA's favour would have set a worrying precedent for future investigations of this nature and the protection of these important human rights."

Love was arrested on 15 July 2015 on behalf of the US government, which had issued several indictments and corresponding extradition warrants.

The FBI and US Department of Justice allege that Love was involved in hacking into various government agencies, including the US army, Nasa, the Federal Reserve and the Environmental Protection Agency. His extradition hearing will be held on 28 and 29 June.

Outside court, Love said he was scared at the prospect of being sent to the US for criminal prosecution. "It is the worst thing I could imagine happening to me. I have to get on with my work and my studies, I can't afford to be stressed or depressed or anxious about it."

Love's case has echoes of the FBI and Apple dispute in the US. In 2015 and 2016, Apple received, and objected to or challenged, at least 11 orders issued by US district courts which sought to compel the firm to extract data, such as contacts, photos and calls from locked iPhones.

The most well-known instance was in February 2016, when the FBI wanted Apple to create and electronically sign new software that would enable the FBI to unlock an iPhone recovered from one of the shooters in the December 2015 terrorist attack in San Bernardino, California.

The government ultimately said it had found a third party able to assist in unlocking the iPhone and withdrew its request.

Columbia Journalism Review
Snowden interview: Why the media isn't doing its job
Wednesday, 11 May 2016
Byline: Emily Bell
Section: Interview

Interview - The Tow Center for Digital Journalism's Emily Bell spoke to Edward Snowden over a secure channel about his experiences working with journalists and his perspective on the shifting media world. This is an excerpt of that conversation, conducted in December 2015.
Emily Bell: Can you tell us about your interactions with journalists and the press?

Edward Snowden: One of the most challenging things about the changing nature of the public's relationship to media and the government's relationship to media is that media has never been stronger than it is now. At the same time, the press is less willing to use that sort of power and influence because of its increasing commercialization. There was this tradition that the media culture we had inherited from early broadcasts was intended to be a public service. Increasingly we've lost that, not simply in fact, but in ideal, particularly due to the 24-hour news cycle.

We see this routinely even at organizations like The New York Times. The Intercept recently published The Drone Papers, which was an extraordinary act of public service on the part of a whistleblower within the government to get the public information that's absolutely vital about things that we should have known more than a decade ago. These are things that we really need to know to be able to analyze and assess policies. But this was denied to us, so we get one journalistic institution that breaks the story, they manage to get the information out there. But the majors--specifically The New York Times-- don't actually run the story, they ignore it completely. This was so extraordinary that the public editor, Margaret Sullivan, had to get involved to investigate why they suppressed such a newsworthy story. It's a credit to the Times that they have a public editor, but it's frightening that there's such a clear need for one.

In the UK, when The Guardian was breaking the NSA story, we saw that if there is a competitive role in the media environment, if there's money on the line, reputation, potential awards, anything that has material value that would benefit the competition, even if it would simultaneously benefit the public, the institutions are becoming less willing to serve the public to the detriment of themselves. This is typically exercised through the editors. This is something that maybe always existed, but we don't remember it as always existing. Culturally, we don't like to think of it as having always existed. There are things that we need to know, things that are valuable for us, but we are not allowed to know, because The Telegraph or the Times or any other paper in London decides that because this is somebody else's exclusive, we're not going to report it. Instead, we'll try to "counter-narrative" it. We'll simply go to the government and ask them to make any statement at all, and we will unquestioningly write it down and publish it, because that's content that's exclusive to us. Regardless of the fact that it's much less valuable, much less substantial than actual documented facts that we can base policy discussions on. We've seemingly entered a world where editors are making decisions about what stories to run based on if it'll give oxygen to a competitor, rather than if it's news.

I would love to hear your thoughts on this, because while I do interact with media, I'm an outsider. You know media. As somebody who has worked in these cultures, do you see the same thing? Sort of the Fox News effect, where facts matter less?

Bell: It's a fascinating question. When you look at Donald Trump, there's a problem when you have a press which finds it important to report what has happened, without a prism of some sort of evaluation on it. That's the Trump problem, right? He says thousands of Muslims were celebrating in the streets of New Jersey after 9/11 and it's demonstrably not true. It's not even a quantification issue, it's just not

true. Yet, it dominates the news cycle, and he dominates the TV, and you see nothing changing in the polls--or, rather, him becoming more popular.

There are two things I think here, one of which is not new. I completely agree with you about how the economic dynamics have actually produced, bad journalism. One of the interesting things which I think is hopeful about American journalism is that within the last 10 years there's been a break between this relationship, which is the free market, which says you can't do good journalism unless you make a profit, into intellectually understanding that really good journalism not only sometimes won't make a profit, but is almost never going to be anything other than unprofitable.

I think your acts and disclosures are really interesting in that it's a really expensive story to do, and it is not the kind of story that advertisers want to stand next to. Actually people didn't want to pay to read them. Post hoc they'll say, we like The Guardian; we're going to support their work. So I agree with you that there's been a disjuncture between facts and how they are projected. I would like to think it's going to get better.

You're on Twitter now. You're becoming a much more rounded out public persona, and lots of people have seen Citizenfour. You've gone from being this source persona, to being more actively engaged with Freedom of the Press Foundation, and also having your own publishing stream through a social media company. The press no longer has to be the aperture for you. How do you see that?

Snowden: Today, you have people directly reaching an audience through tools like Twitter, and I have about 1.7 million followers right now (this number reflects the number of Twitter followers Snowden had in December 2015). These are people, theoretically, that you can reach, that you can send a message to. Whether it's a hundred people or a million people, individuals can build audiences to speak with directly. This is actually one of the ways that you've seen new media actors, and actually malicious actors, exploit what are perceived as new vulnerabilities in media control of the narrative, for example Donald Trump.

At the same time these strategies still don't work [...] for changing views and persuading people on a larger scope. Now this same thing applies to me. The director of the FBI can make a false statement, or some kind of misleading claim in congressional testimony. I can fact-check and I can say this is inaccurate. Unless some entity with a larger audience, for example, an established institution of journalism, sees that themselves, the value of these sorts of statements is still fairly minimal. They are following these new streams of information, then reporting out on those streams. This is why I think we see such a large interplay and valuable interactions that are emerging from these new media self-publication Twitter-type services and the generation of stories and the journalist user base of Twitter.

If you look at the membership of Twitter in terms of the influence and impact that people have, there are a lot of celebrities out there on Twitter, but really they're just trying to maintain an image, promote a band, be topical, remind people that they exist. They're not typically effecting any change, or having any kind of influence, other than the directly commercial one.

Bell: Let's think about it in terms of your role in changing the world, which is presenting these new facts. There was a section of the technology press and the intelligence press who, at the time of the leaks, said we already know this, except it's hidden in plain sight. Yet, a year after you made the disclosures, there was a broad shift of public perception about surveillance technologies. That may recede, and probably post-Paris, it is receding a little bit. Are you frustrated that there isn't more long-term impact? Do you feel the world has not changed quickly enough?

Snowden: I actually don't feel that. I'm really optimistic about how things have gone, and I'm staggered by how much more impact there's been as a result of these revelations than I initially presumed. I'm famous for telling Alan Rusbridger that it would be a three-day story. You're sort of alluding to this idea that people don't really care, or that nothing has really changed. We've heard this in a number of different ways, but I think it actually has changed in a substantial way.

Now when we talk about the technical press, or the national security press, and you say, this is nothing new, we knew about this, a lot of this comes down to prestige, to the same kind of signaling where they have to indicate we have expertise, we knew this was going on. In many cases they actually did not. The difference is, they knew the capabilities existed.

This is, I think, what underlies why the leaks had such an impact. Some people say stories about the mass collection of internet records and metadata were published in 2006. There was a warrantless wiretapping story in The New York Times as well. Why didn't they have the same sort of transformative impact? This is because there's a fundamental difference when it comes down to the actionability of information between knowledge of capability, the allegation that the capability could be used, and the fact that it is being used. Now what happened in 2013 is we transformed the public debate from allegation to fact. The distance between allegation and fact, at times, makes all the difference in the world.

That, for me, is what defines the best kind of journalism. This is one of the things that is really underappreciated about what happened in 2013. A lot of people laud me as the sole actor, like I'm this amazing figure who did this. I personally see myself as having a quite minor role. I was the mechanism of revelation for a very narrow topic of governments. It's not really about surveillance, it's about what the public understands--how much control the public has over the programs and policies of its governments. If we don't know what our government really does, if we don't know the powers that authorities are claiming for themselves, or arrogating to themselves, in secret, we can't really be said to be holding the leash of government at all.

One of the things that's really missed is the fact that as valuable and important as the reporting that came out of the primary archive of material has been, there's an extraordinarily large, and also very valuable amount of disclosure that was actually forced from the government, because they were so back-footed by the aggressive nature of the reporting. There were stories being reported that showed

how they had abused these capabilities, how intrusive they were, the fact that they had broken the law in many cases, or had violated the Constitution.

When the government is shown in a most public way, particularly for a president who campaigned on the idea of curtailing this sort of activity, to have continued those policies, in many cases expanded them in ways contrary to what the public would expect, they have to come up with some defense. So in the first weeks, we got rhetorical defenses where they went, nobody's listening to your phone calls. That wasn't really compelling. Then they went, "It's just metadata." Actually that worked for quite some time, even though it's not true. By adding complexity, they reduced participation. It is still difficult for the average person in the street to understand that metadata, in many cases, is actually more revealing and more dangerous than the content of your phone calls. But stories kept coming. Then they went, well alright, even if it is "just metadata," it's still unconstitutional activity, so how do we justify it? Then they go--well they are lawful in this context, or that context.

They suddenly needed to make a case for lawfulness, and that meant the government had to disclose court orders that the journalists themselves did not have access to, that I did not have access to, that no one in the NSA at all had access to, because they were bounded in a completely different agency, in the Department of Justice.

This, again, is where you're moving from suspicion, from allegation, to factualizing things. Now of course, because these are political responses, each of them was intentionally misleading. The government wants to show itself in the best possible light. But even self- interested disclosures can still be valuable, so long as they're based on facts. They're filling in a piece of the puzzle, which may provide the final string that another journalist, working independently somewhere else, may need. It unlocks that page of the book, fills in the page they didn't have, and that completes the story. I think that is something that has not been appreciated, and it was driven entirely by journalists doing follow- up.

There's another idea that you mentioned: that I'm more engaged with the press than I was previously. This is very true. I quite openly in 2013 took the position that this is not about me, I don't want to be the face of the argument. I said that I don't want to correct the record of government officials, even though I could, even though I knew they were making misleading statements. We're seeing in the current electoral circus that whatever someone says becomes the story, becomes the claim, becomes the allegation. It gets into credibility politics where they're going, oh, you know, well, Donald Trump said it, it can't be true. All of the terrible things he says put aside, there's always the possibility that he does say something that is true. But, because it's coming from him, it will be analyzed and assessed in a different light. Now that's not to say that it shouldn't be, but it was my opinion that there was no question that I was going to be subject to a demonization campaign. They actually recorded me on camera saying this before I revealed my identity. I predicted they were going to charge me under the Espionage Act, I predicted they were going to say I helped terrorists, blood on my hands, all of that stuff. It did come to pass. This was not a staggering work of genius on my part, it's just common sense, this is how it always works in the case of prominent whistleblowers. It was because of this that we needed other voices, we needed the media to make the argument.

Because of the nature of the abuse of classification authorities in the United States, there is no one that's ever held a security clearance who's actually able to make these arguments. Modern media institutions prefer never to use their institutional voice to factualize a claim in a reported story, they want to point to somebody else. They want to say this expert said, or this official said, and keep themselves out of it. But in my mind, journalism must recognize that sometimes it takes the institutional weight to assess the claims that are publicly available, and to make a determination on that basis, then put the argument forth to whoever the person under suspicion is at the time, for example, the government in this case, and go--look, all of the evidence says you were doing this. You say that's not the case, but why should we believe you? Is there any reason that we should not say this?

This is something that institutions today are loath to do because it's regarded as advocacy. They don't want to be in the position of having to referee what is and is not fact. Instead they want to play these "both sides games" where they say, instead we'll just print allegations, we'll print claims from both sides, we'll print their demonstrations of evidence, but we won't actually involve ourselves in it.

Because of this, I went the first six months without giving an interview. It wasn't until December 2013 that I gave my first interview to Barton Gellman of The Washington Post. In this intervening period my hope was that some other individual would come forth on the political side, and would become the face of this movement. But more directly I thought it would inspire some reflection in the media institutions to think about what their role was. I think they did a fairly good job, particularly for it being unprecedented, particularly for it being a segment in which the press has been, at least in the last 15 years, extremely reluctant to express any kind of skepticism regarding government claims at all. If it involved the word "terrorism," these were facts that wouldn't be challenged. If the government said, look, this is secret for a reason, this is classified for a reason, journalists would leave it at that. Again, this isn't to beat up on The New York Times, but when we look at the warrantless wiretapping story that was ready to be published in October of an election year, that [election] was decided by the smallest margin in a presidential election, at least in modern history. It's hard to believe that had that story been published, it would not have changed the course of that election.

Bell: Former Times Executive Editor Jill Abramson has said her paper definitely made mistakes, "I wish we had not withheld stories." What you're saying certainly resonates with what I know and understand of the recent history of the US press, which is that national security concerns post-9/11 really did alter the relationship of reporting, particularly with administration and authority in this country. What we know about drone programs comes from reporting, some of it comes from the story which The Intercept got hold of, and Jeremy Scahill's reporting on it, which has been incredibly important. But a great deal of it has also come from the ground level. The fact that we were aware at all that drones were blowing up villages, killing civilians, crossing borders where they were not supposed to be really comes from people who would report from the ground.

Something interesting has definitely happened in the last three years, which makes me think about what you are telling us about how the NSA operates. We're seeing a much closer relationship now between

journalism and technology and mass communication technology than we've ever seen before. People are now completely reliant on Facebook. Some of that is a commercial movement in the US, but you also have activists and journalists being regularly tortured or killed in, say, Bangladesh, where it's really impossible to operate a free press, but they are using these tools. It is almost like the American public media now is Facebook. I wonder how you think about this? It's such a recent development.

Snowden: One of the biggest issues is that we have many more publishers competing for a finite, shrinking amount of attention span that's available. This is why we have the rise of these sort of hybrid publications, like a BuzzFeed, that create just an enormous amount of trash and cruft. They're doing AB testing and using scientific principles. Their content is specifically engineered to be more attention getting, even though they have no public value at all. They have no news value at all. Like here's 10 pictures of kittens that are so adorable. But then they develop a news line within the institution, and the idea is that they can drive traffic with this one line of stories, theoretically, and then get people to go over onto the other side.

Someone's going to exploit this; if it's not going to be BuzzFeed, it's going to be somebody else. This isn't a criticism of any particular model, but the idea here is that the first click, that first link is actually consuming attention. The more we read about a certain thing, that's actually reshaping our brains. Everything that we interact with, it has an impact on us, it has an influence, it leaves memories, ideas, sort of memetic expressions that we then carry around with us that shape what we look for in the future, and that are directing our development.

Bell: Yes, well that's the coming singularity between the creation of journalism and large-scale technology platforms, which are not intrinsically journalistic. In other words, they don't have a primary purpose.

Snowden: They don't have a journalistic role, it's a reportorial role.

Bell: Well, it's a commercial role, right? So when you came to Glenn and The Guardian, there wasn't a hesitation in knowing the primary role of the organization is to get that story to the outside world as securely and quickly as possible, avoiding prior restraint, protecting a source.

Is source protection even possible now? You were extremely prescient in thinking there's no point in protecting yourself.

Snowden: I have an unfair advantage.

Bell: You do, but still, that's a big change from 20 years ago.

Snowden: This is something that we saw contemporary examples of in the public record in 2013. It was the James Rosen case where we saw the Department of Justice, and government more broadly, was

abusing its powers to demand blanket records of email and call data, and the AP case where phone records for calls that were made from the bureaus of journalism were seized.

That by itself is suddenly chilling, because the traditional work of journalism, the traditional culture, where the journalist would just call their contact and say, hey, let's talk, suddenly becomes incriminating. But more seriously, if the individual in question, the government employee who is working with a journalist to report some issue of public interest, if this individual has gone so far to commit an act of journalism, suddenly they can be discovered trivially if they're not aware of this.

I didn't have that insight at the time I was trying to come forward because I had no relationship with journalists. I had never talked to a journalist in any substantive capacity. So, instead I simply thought about the adversarial relationship that I had inherited from my work as an intelligence officer, working for the CIA and the NSA. Everything is a secret and you've got two different kinds of cover. You've got cover for status, which is: You're overseas, you're living as a diplomat because you have to explain why you're there. You can't just say, oh, yeah, I work for the CIA. But you also have a different kind of cover which is what's called cover for action. Where you're not going to live in the region for a long time, you may just be in a building and you have to explain why you're walking through there, you need some kind of pretext. This kind of trade-craft unfortunately is becoming more necessary in the reportorial process. Journalists need to know this, sources need to know this. At any given time, if you were pulled over by a police officer and they want to search your phone or something like that, you might need to explain the presence of an application. This is particularly true if you're in a country like Bangladesh. I have heard that they're now looking for the presence of VPN [virtual private network software] for avoiding censorship locks and being able to access uncontrolled news networks as evidence of opposition, allegiance, that could get you in real trouble in these areas of the world.

At the time of the leaks I was simply thinking, alright the government--and this isn't a single government now--we're actually talking about the Five Eyes intelligence alliance [the United States, the United Kingdom, New Zealand, Australia, Canada] forming a pan-continental super-state in this context of sharing, they're going to lose their minds over this. Some institutions in, for example, the UK, can levy D notices, they can say, look, you can't publish that, or you should not publish that. In the United States it's not actually certain that the government would not try to exercise prior restraint in slightly different ways, or that they wouldn't charge journalists as accomplices in some kind of criminality to interfere with the reporting without actually going after the institutions themselves, single out individuals. We have seen this in court documents before. This was the James Rosen case, where the DOJ had named him as sort of an accessory--they said he was a co-conspirator. So the idea I thought about here was that we need institutions working beyond borders in multiple jurisdictions simply to complicate it legally to the point that the journalists could play games, legally and journalistically more effectively and more quickly than the government could play legalistic games to interfere with them.

Bell: Right, but that's kind of what happened with the reporting of the story.

Snowden: And in ways that I didn't even predict, because who could imagine the way a story like that would actually get out of hand and go even further: Glenn Greenwald living in Brazil, writing for a US institution for that branch, but headquartered in the UK, The Washington Post providing the institutional clout and saying, look, this is a real story, these aren't just crazy leftists arguing about this, and Der Spiegel in Germany with Laura [Poitras]. It simply represented a system that I did not believe could be overcome before the story could be put out. By the time the government could get their ducks in a row and try to interfere with it, that would itself become the story.

Bell: You're actually giving a sophisticated analysis of much of what's happened to both reporting practice and media structures. As you say, you had no prior interactions with journalists. I think one of the reasons the press warmed to you was because you put faith in journalists, weirdly. You went in thinking I think I can trust these people, not just with your life, but with a huge responsibility. Then you spent an enormous amount of time, particularly with Glenn, Laura, and Ewen [MacAskill] in those hotel rooms. What was that reverse frisking process like as you were getting to know them? My experience is as people get closer to the press, they often like it less. Why would you trust journalists?

Snowden: This gets into the larger question--how did you feel about journalists, what was the process of becoming acquainted with them? There's both a political response and a practical response. Specifically about Glenn, I believe very strongly that there's no more important quality for a journalist than independence. That's independence of perspective, and particularly skepticism of claims. The more powerful the institution, the more skeptical one should be. There's an argument that was put forth by an earlier journalist, I.F. Stone: "All governments are run by liars and nothing they say should be believed." In my experience, this is absolutely a fact. I've met with Daniel Ellsberg and spoken about this, and it comports with his experience as well. He would be briefing the Secretary of Defense on the airplane, and then when the Secretary of Defense would disembark right down the eight steps of the plane and shake hands with the press, he would say something that he knew was absolutely false and was completely contrary to what they had just said in the meeting [inside the place] because that was his role. That was his job, his duty, his responsibility as a member of that institution.

Now Glenn Greenwald, if we think about him as an archetype, really represents the purest form of that. I would argue that despite the failings of any journalist in one way or another, if they have that independence of perspective, they have the greatest capacity for reporting that a journalist can attain. Ultimately, no matter how brilliant you are, no matter how charismatic you are, no matter how perfect or absolute your sourcing is, or your access, if you simply take the claims of institutions that have the most privilege that they must protect, at face value, and you're willing to sort of repeat them, all of those other things that are working in your favor in the final calculus amount to nothing because you're missing the fundamentals.

There was the broader question of what it's like working with these journalists and going through that process. There is the argument that I was naïve. In fact, that's one of the most common criticisms about me today--that I am too naïve, that I have too much faith in the government, that I have too much faith in the press. I don't see that as a weakness. I am naïve, but I think that idealism is critical to achieving

change, ultimately not of policy, but of culture, right? Because we can change this or that law, we can change this or that policy or program, but at the end of the day, it's the values of the people in these institutions that are producing these policies or programs. It's the values of the people who are sitting at the desk with the blank page in Microsoft Office, or whatever journalists are using now.

Bell: I hope they're not using Microsoft Office, but you never know.

Snowden: They have the blank page ...

Bell: They have the blank page, exactly.

Snowden: In their content management system, or whatever. How is that individual going to approach this collection of facts in the next week, in the next month, in the next year, in the next decade? What will the professor in the journalism school say in their lecture that will impart these values, again, sort of memetically into the next cohort of reporters? If we do not win on that, we have lost comprehensively. More fundamentally, people say, why did you trust the press, given their failures? Given the fact that I was, in fact, quite famous for criticizing the press.

Bell: If they had done their job, you would be at home now.

Snowden: Yeah, I would still be living quite comfortably in Hawaii.

Bell: Which is not so bad, when you put it that way.

Snowden: People ask how could you do this, why would you do this? How could you trust a journalist that you knew had no training at all in operational security to keep your identity safe because if they screw up, you're going to jail. The answer was that that was actually what I was expecting. I never expected to make it out of Hawaii. I was going to try my best, but my ultimate goal was simply to get this information back in the hands of the public. I felt that the only way that could be done meaningfully was through the press. If we can't have faith in the press, if we can't sort of take that leap of faith and either be served well by them, or underserved and have the press fail, we've already lost. You cannot have an open society without open communication. Ultimately, the test of open communication is a free press. If they can't look for information, if they can't contest the government's control of information, and ultimately print information--not just about government, but also about corporate interests, that has a deleterious impact on the preferences of power, on the prerogatives of power. You may have something, but I would argue it's not the traditional American democracy that I believed in.

So the idea here was that I could take these risks because I already expected to bear the costs. I expected the end of the road was a cliff. This is actually illustrated quite well in Citizenfour because it shows that there was absolutely no plan at all for the day after.

The planning to get to the point of working with the journalists, of transmitting this information, of explaining, contextualizing--it was obsessively detailed, because it had to be. Beyond that, the risks were my own. They weren't for the journalists. They could do everything else. That was by design as well, because if the journalists had done anything shady--for example, if I had stayed in place at the NSA as a source and they had asked me for this document, and that document, it could have undermined the independence, the credibility of the process, and actually brought risks upon them that could have led to new constraints upon journalism.

Bell: So nothing you experienced in the room with the team, or what happened after, made you question or reevaluate journalism?

Snowden: I didn't say that. Actually working more closely with the journalists has radically reshaped my understanding of journalism, and that continues through to today. I think you would agree that anybody who's worked in the news industry, either directly or even peripherally, has seen journalists-- or, more directly, editors--who are terrified, who hold back a story, who don't want to publish a detail, who want to wait for the lawyers, who are concerned with liability.

You also have journalists who go out on their own and they publish details which actually are damaging, directly to personal safety. There were details published by at least one of the journalists that were discussing communication methods that I was still actively using, that previously had been secret. But the journalists didn't even forewarn me, so suddenly I had to change all of my methods on the fly. Which worked out OK because I had the capabilities to do that, but dangerous.

Bell: When did that happen?

Snowden: This was at the height of public interest, basically. The idea here is that a journalist ultimately, and particularly a certain class of journalist, they don't owe any allegiance to their source, right? They don't write the story in line with what the sources desires, they don't go about their publication schedule to benefit, or to detriment, in theory, the source at all. There are strong arguments that that's the way it should be: public knowledge of the truth is more important than the risks that knowledge creates for a few. But at the same time, when a journalist is reporting on something like a classified program implicating one of the government's sources, you see an incredibly high standard of care applied to make sure they can't be blamed if something goes wrong down the road after publication. The journalists will go, well we'll hold back this detail from that story reporting on classified documents, because if we name this government official it might expose them to some harm, or it might get this program shut down, or even if it might cause them to have to rearrange the deck chairs in the operations in some far away country.

That's just being careful, right? But ask yourself--should journalists be just as careful when the one facing the blowback of a particular detail is their own source? In my experience, the answer does not seem to be as obvious as you might expect.

Bell: Do you foresee a world where someone won't have to be a whistleblower in order to reveal the kinds of documents that you revealed? What kinds of internal mechanisms would that require on behalf of the government? What would that look like in the future?

Snowden: That's a really interesting philosophical question. It doesn't come down to technical mechanisms, that comes down to culture. We've seen in the EU a number of reports from parliamentary bodies, from the Council of Europe, that said we need to protect whistleblowers, in particular national security whistleblowers. In the national context no country really wants to pass a law that allows individuals rightly, or wrongly, to embarrass the government. But can we provide an international framework for this? One would argue, particularly when espionage laws are being used to prosecute people, they already exist. That's why espionage, for example, is considered a political offense, because it's just a political crime, as they say. That's a fairly weak defense, or fairly weak justification, for not reforming whistleblower laws. Particularly when, throughout Western Europe they're going, yeah, we like this guy, he did a good thing. But if he shows up on the doorstep we're going to ship him back immediately, regardless of whether it's unlawful, just because the US is going to retaliate against us. It's extraordinary that the top members of German government have said this on the record--that it's realpolitik; it's about power, rather than principle.

Now how we can fix this? I think a lot of it comes down to culture, and we need a press that's more willing and actually eager to criticize government than they are today. Even though we've got a number of good institutions that do that, or that want to do that, it needs a uniform culture. The only counterargument the government has made against national security whistleblowing, and many other things that embarrassed them in the past, is that well, it could cause some risk, we could go dark, they could have blood on their hands.

Why do they have different ground rules in the context of national security journalism?

We see that not just in the United States, but in France, Germany, the UK, in every Western country, and of course, in every more authoritarian country by comparison they are embracing the idea of state secrets, of classifications, or saying, you can't know this, you can't know that.

We call ourselves private citizens, and we refer to elected representatives as public officials, because we're supposed to know everything about them and their activities. At the same time, they're supposed to know nothing about us, because they wield all the power, and we hold all of the vulnerability. Yet increasingly, that's becoming inverted, where they are the private officials, and we are the public citizens. We're increasingly monitored and tracked and reported, quantified and known and influenced, at the same time that they're getting themselves off and becoming less reachable and also less accountable.

Bell: But Ed, when you talk about this in those terms, you make it sound as though you see this as a progression. Certainly there was a sharp increase, as you demonstrated, in overreach of oversight post-9/11. Is it a continuum?

It felt from the outside as though America, post-9/11, for understandable reasons, it was almost like a sort of national psychosis. If you grew up in Europe, there were regular terrorist acts in almost every country after the Second World War, though not on the same scale, until there was a brief, five-year period of respite, weirdly running up to about 2001. Then the nature of the terrorism changed. To some extent, that narrative is predictable. You talk about it as an ever increasing problem. With the Freedom Act in 2015, the press identified this as a significant moment where the temperature had changed. You don't sound like you really think that. You sound as though you think that this public/private secrecy, spying, is an increasing continuum. So how does that change? Particularly in the current political climate where post-Paris and other terrorist attacks we've already seen arguments for breaking encryption.

Snowden: I don't think they are actually contradictory views to hold. I think what we're talking about are the natural inclinations of power and vice, what we can do to restrain it, to maintain a free society. So when we think about where things have gone in the USA Freedom Act, and when we look back at the 1970s, it was even worse in terms of the level of comfort that the government had that it could engage in abuses and get away with them. One of the most important legacies of 2013 is not anything that was necessarily published, but it was the impact of the publication on the culture of government. It was a confirmation coming quite quickly in the wake of the WikiLeaks stories, which were equally important in this regard. That said, secrecy will not hold forever. If you authorize a policy that is clearly contrary to law, you will eventually have to explain that.

The question is, can you keep it under wraps long enough to get out of the administration, and hopefully for it to be out of the egregious sort of thing where you'll lose an election as a result. We see the delta between the periods of time that successive administrations can keep a secret is actually diminishing--the secrets are becoming public at an accelerated pace. This is a beneficial thing. This is the same in the context of terrorism.

There is an interesting idea--when you were saying it's sort of weird that the US has what you described as a collective psychosis in the wake of 9/11 given that European countries have been facing terrorist attacks routinely. The US had actually been facing the same thing, and actually one would argue, experienced similarly high-impact attacks, for example, the Oklahoma City bombing, where a Federal building was destroyed by a single individual or one actor.

Bell: What do you think about the relationship between governments asking Facebook and other communications platforms to help fight ISIS?

Snowden: Should we basically deputize companies to become the policy enforcers of the world? When you put it in that context suddenly it becomes clear that this is not really a good idea, particularly because terrorism does not have a strong definition that's internationally recognized. If Facebook says, we will take down any post from anybody who the government says is a terrorist, as long as it comes from this government, suddenly they have to do that for the other government. The Chinese allegations of who is and who is not a terrorist are going to look radically different than what the FBI's are going to

be. But if the companies try to be selective about them, say, well, we're only going to do this for one government, they immediately lose access to the markets of the other ones. So that doesn't work, and that's not a position companies want to be in.

However, even if they could do this, there are already policies in place for them to do that. If Facebook gets a notification that says this is a terrorist thing, they take it down. It's not like this is a particularly difficult or burdensome review when it comes to violence.

The distinction is the government is trying to say, now we want them to start cracking down on radical speech. Should private companies be who we as society are reliant upon to bound the limits of public conversations? And this goes beyond borders now. I think that's an extraordinarily dangerous precedent to be embracing, and, in turn, irresponsible for American leaders to be championing.

The real solutions here are much more likely to be in terms of entirely new institutions that bound the way law enforcement works, moving us away from the point of military conflict, secret conflict, and into simply public policing.

There's no reason why we could not have an international counter-terrorism force that actually has universal jurisdiction. I mean universal in terms of fact, as opposed to actual law.

Canadian Press
IBM and universities join forces in battle against cybercrime
Wednesday, 11 May 2016

Ottawa - IBM wants its Watson computer system to learn how to fight cybercrime and it's asking eight leading universities, including three in Canada, for help. Watson - IBM's question answering computer system - was originally designed to compete (and win) on the television quiz show Jeopardy, but the technology has since been used on other problem-solving projects.
Now IBM is launching Watson for Cyber-security - a cloud-based version of their cognitive technology - that will be trained over the next year to examine threats of cybercrime.

Caleb Barlow, vice-president of IBM Security, said it is becoming increasingly difficult for security staffto deal with the growing number of cyber threats.

"Your average enterprise is dealing with 200,000 incidents a day that they've got to dig through. Human beings simply cannot look at all of that data," he said.

"Combine that with the fact we have a major skill shortage in the security industry - around 1.5 million jobs by 2020 - and even if we could fill all those jobs we still can't get through the data as it continues to grow."

Barlow said experts are doing a good job to examine cyber threats, but their work often ends up in various forms such as reports, blogs and presentations and in numbers too large for others to read and remember.

That's where Watson comes in.

Students at the eight universities, including the University of New Brunswick, University of Ottawa and the University of Waterloo, will put the information in a form the computer can understand and help train the system to use that information to examine cyber threats.

"The more information that Watson has, the better reasoning it can provide and therefore in some cases the better prediction it can provide," said Ali Ghorbani, dean of the faculty of computer science at the University of New Brunswick in Fredericton.

The students will input about 15,000 security documents per month during the year-long project, starting this fall.

"Our students are getting involved in a real-world cyber-security project with a global company. Not only will they increase their knowledge, but also create a relationship with IBM for future collaborations - either jobs for our students or more research and development projects with IBM," Ghorbani said.

He said IBM is hoping that not only will Watson be able to provide early warnings of potential attacks, it will also do it fast.

Barlow said IBM opened its entire threat intelligence database to the world a year ago, and invited people to develop applications to work with their QRadar software.

That software was developed by Q1 Labs, developed in turn at the University of New Brunswick, and purchased more than four years ago by IBM.

He said by getting information out to security staffaround the world, cybercrime may become less lucrative for organized crime.

"We start changing the dynamic for the bad guys because it's not worth investing $100,000 or more in that new attack you've got if it's only going to be viable for a few minutes before we find it and tell the rest of the world," Barlow said.

CBC.CA
Air Canada employees told to seek extra ID from kids even after feds' screening directive
Wednesday, 11 May 2016
Byline: Shanifa Nasser

Ottawa - A passport, a school ID card or even an Aeroplan number are among the pieces of identification Air Canada employees were instructed to obtain from children, even as the federal public safety minister said additional security screening was not required for people under 18.
Screenshots of documents taken by an Air Canada employee in January, sent to CBC News show the airline carrier issued a directive to employees stating children are not subject to extra screening measures, but goes on to list numerous such steps to clear what is known as the "deemed high profile" or DHP list. CBC News agreed to protect the employee's identity because of concerns of job termination.

"Children are not subject to extra screening under the Transport Canada Secure Air Travel Act (SATA) and Passenger Protect Program; however, until a passenger has been seen by an Airport agent, we cannot confirm their identity and date of birth," the screenshot says.

The revelations come just after the Minister Goodale announced that Canada and the U.S. set up a working group to help prevent false-positives for children matching names on no-fly lists.

The no-fly list is generated by the government, but "piggybacked onto the computer systems of the airlines. It's not an interactive system," he said Tuesday, admitting changes to the problem of false security-list matches won't be quick or easy.

By contrast, the American system is entirely government run and is entirely interactive, Goodale said.

"You've got to change the entire database."

In a statement, Air Canada representative Peter Fitzpatrick told CBC News it is a legal requirement that all passengers be vetted against watch lists, adding that children whose names are similar to a flagged name are "uniquely identified and cleared."

Employees are "instructed to use an Aeroplan number because it is a unique identifier (unlike a birthday because people share birth dates and the information can sometimes be entered incorrectly,)" Fitzpatrick said.

But to Toronto-area Khadija Cajee, whose six-year-old son, Adam Ahmed, nearly missed an Air Canada flight to Boston last year because his name showed up on the DHP list, an Aeroplan number makes little sense.

"I can log on as Bugs Bunny and get an Aeroplan number. It's not a foolproof government identification. It's a loyalty program," Cajee said.

Since Ahmed's case made headlines, more than 40 other parents have come forward through social media and other means, with the same complaint.

Cajee, meanwhile, has found herself the unwitting liaison for the group #NoFlyListKids and the government.

One of those mothers, based in Kamloops, said on Tuesday that Air Canada employees have recommended she change her baby's name to bypass the delays.

"I wasn't happy with that," Faaria Siddiqui told CBC News. "How do we know if we change his name it won't be on the list or the name we choose won't be on list?"

Reuters
SWIFT rejects Bangladeshi claims over $81 million cyber heist
Wednesday, 11 May 2016

Dhaka - SWIFT has rejected allegations by officials in Bangladesh that technicians with the global messaging system made the nation's central bank more vulnerable to hacking before an $81 million cyber heist in February.
The comments were in response to a Reuters story that cited Bangladeshi police and a central bank official as saying that SWIFT technicians introduced security holes into the bank's network while connecting SWIFT to Bangladesh's first real-time gross settlement (RTGS) system.

"SWIFT was not responsible for any of the issues cited by the officials, or party to the related decisions," the Brussels-based bank-owned cooperative said in a statement posted on its website on Monday.

"As a SWIFT user like any other, Bangladesh Bank is responsible for the security of its own systems interfacing with the SWIFT network and their related environment - starting with basic password protection practices - in much the same way as they are responsible for their other internal security considerations," the statement said.

But Bangladesh's main police investigator maintained there were loopholes in the way SWIFT carried out the integration of its network with the RTGS platform that left the central bank's computer systems vulnerable to hackers.

Mohammad Shah Alam, the head of the Criminal Investigation Department of the Bangladesh Police, said the probe had identified specific deviations from set procedures that compromised Bangladesh Bank's security. "We stand by our investigation," he said in response to the comments by SWIFT.

But he added he did not want to engage in a debate and urged greater international cooperation to identify the culprits behind one of the world's biggest cyber thefts.

Reuters has not been able to independently verify the allegations by Bangladeshi officials about the SWIFT technicians.

US investigators suspect the involvement of employees of the Bangladesh Bank in helping the hackers breach the systems, the Wall Street Journal said, quoting people familiar with the matter.

It said the Federal Bureau of Investigation had found evidence that at least one bank employee acted as an accomplice but there could be more who assisted the hackers in navigating around Bangladesh Bank's computer systems.

Bangladesh Police said they have been looking for inside involvement in the heist from the beginning of the probe, but no evidence has turned up against anyone.

Investigators say they think there was some level of local facilitation in the attack on the central bank's computers but haven't identified it as yet. "If the FBI has uncovered evidence, they should share with us," a police officer said.

The revelations came ahead of a meeting on Tuesday in Basel, Switzerland, where Bangladesh Bank officials have said their governor and a lawyer appointed by the bank would discuss recovery of about $81 million stolen by hackers with the head of the Federal Reserve Bank of New York and a senior executive from SWIFT.

The money was stolen from Bangladesh Bank's account at the New York Fed through fraudulent transfer orders sent on the SWIFT system.

SWIFT's statement said it "looks forward to the meeting with Bangladesh Bank and New York Federal Reserve Bank officials in Basel on 10th May, when the bank's security issues and these baseless allegations will be discussed."

Bangladesh Bank officials have said they believed SWIFT, and the New York Fed, bear some responsibility for the February cyber heist.

Gulf News
Banks to face growing challenge on data security
Wednesday, 11 May 2016
Byline: Babu Das Augustine

Dubai - In the context of rising cases of data breaches across regional financial institutions, KPMG expects the UAE based banks to face growing challenges from hackers and other malicious actors. "In November 2015, we surveyed a broad range of KPMG clients in the UAE to better understand their cyber security arrangements and their level of preparedness to respond to a cyber-attack. What we learned clearly showed that many organizations in the UAE -- including financial institutions -- continue to struggle in a number of different areas," said Cristian Carstoiu, Director, Management Consulting.

The survey showed that many UAE organisations find it difficult to develop an adequate investment case to recruit the right level of expertise and to implement appropriate security technologies, even against a backdrop of increasing concern over cyber security attacks in the region.

"We believe many organisations in the UAE need to improve their emergency response and contingency plans in order to appropriately respond to, and recover from, a cyber breach. Organisations in the UAE also need to better understand their threat profile: who, when and why they are likely to be targeted," said Carstoiu.

The study also said that many boards in the UAE -- where the ultimate responsibility for cyber security lies -- do not have a comprehensive or accurate view of their cyber risks, often because threat intelligence and cyber monitoring have been inconsistently implemented.

Global Times
Activist's cyber hunt violates moral codes
Wednesday, 11 May 2016
Section: editorial

Internet activist Wen Yunchao on Sunday launched a cyber manhunt on Twitter aimed at five experts and technical personnel who helped improve China's Great Firewall. Wen encouraged Net users to find out whether the five, four of whom are professors and postgraduate students from a university in Nanjing, have any personal issues or are engaged in academic corruption.
Wen is a radical political dissident, who was disciplined many times at his Chinese university for various reasons. After he began his studies in the US in 2009, he gradually became a democracy activist against the Chinese political system.

Wen often voices aggressive opinions over freedom of speech and judicial justice. But the manhunt he initiated is a far cry from his philosophy.

These cyber manhunts go severely against cyber ethics, and for a number of reasons are violations of the law. However, it is unfortunate that Twitter has done nothing about it after the case was reported by some Western media. Imagine if Edward Snowden called for a cyber manhunt against all the designers of the US surveillance program PRISM on social networks, would Twitter still be so indifferent?

Certain dissidents have totally lost their moral bottom line nowadays. They flatter themselves that they stand on the moral high ground. Assuming that they did everything for a just cause, they think they can thus trample on ordinary people's codes of conduct.

Every country is responsible for its own cyber management. Technical inventions by a few researchers do not have any political nature.

Yet Wen attacked those technical workers online because of objections to the Chinese firewall. Such paranoia is familiar to us.

No matter how many grudges one has over social governance, he cannot publicly infringe on the rights of others like Wen has done. Otherwise, the entire society will fall into chaos.

After some dissidents fled to the US and other Western countries, they have not only had "more freedom" to express their political views, but also showed the dark side in their humanity. They seem to be so anxious to witness great disorder in China in no time. There is no telling whether their behavior stems from their own issues or the influence of the anti-China forces in the US.

That these malcontented dissidents living abroad, who are losers in life, are washed out by China's reform and opening-up is amusing and thought-provoking.

Khaleej Times
Smart tech set to revolutionize airports
Wednesday, 11 May 2016
Byline: Staff Report

Dubai - The 16th edition of the Airport Show, currently under way at the Dubai International Convention and Exhibition Centre with over 300 exhibitors from 55 countries, has been utilised as a platform to showcase technologies and innovative solutions by multi-national and regional companies.
Some of the prominent technology devices that are being showcased include the Intelligent Trolley and Trolley Security Scanner by Denmark-based Exruptive, an associate company of Dubai-based emaratech, airport runway cleaning systems by US-based Cyclone Technology, Smart Tray cargo and baggage handling systems by Siemens, driverless shuttle by Navya ARMA and the latest face recognition technology by Rockwell Collins.

The Intelligent Trolley will act as a passenger's personal guide through the airport. It can be used to power personal devices, act as a real-time way finding device in the airport via an interactive 3D-map. For flight and gate information, the device updates information on a real-time basis and keeps the passenger updated.

"We are extremely pleased with the response from trade visitors. There have been invitations to visit many airports," said Morten Pankoke, chief operating officer of Exruptive.

Rockwell Collins'face recognition technology captures a traveller's identity using biometrics and matches it with the passenger's passport and boarding pass information.

Dr Ian Bache PMP, technical pre-sales director, Arinc Airports Information Management Services, Rockwell Collins, said: "Airports are always looking to automate passenger processing while maintaining the highest security levels. We offer tailor-made solutions which can be configured with airport identity management solutions. Many airports in this region are showing interest in these technologies." US-based Cyclone Technology has displayed an ultra high water pressure system, The Cyclone 4006, which cleans airport runways and apron surfaces more effectively and in less time than other methods. The patented cleaning and recovery head cleans and removes rubber and paint build-up without damage to the surface.

Siemens is showcasing its latest baggage handling systems, prominent among them is 'smart tray' or SmartTilter, Siemens' solution for the dynamic tilting of tray conveyors, which help get baggage to its destination as quickly as possible.

Navya ARMA introduced a 100 per cent electric and intelligent driverless shuttle which can transport up to 15 passengers and safely drive up to 45 km/h. Navya, the French company which has conceptualised and manufactured the vehicle, is keen on introducing the shuttle at airports across the Middle East region.

The National (UAE)
Beijing postpones implementing new e-commerce regulations

Wednesday, 11 May 2016
Byline: Saibal Dasgupta

Beijing - In a rare move, China today held back implementation of new regulations that were passed last month on goods imported from overseas markets using e-commerce platforms. The government said it will now make adjustments to the rules before they are brought in.
The decision indicated that Beijing is going through a process of rethinking over the use of the internet for a variety of business and security-related functions.

On Monday, the government ordered Beijing's Baidu, one of the world's largest search engines, to revamp its vast business spanning several countries. The cyber administration of China asked the Nasdaq-listed Baidu to formulate a new and more credible algorithm and restrict the amount of promotional content by May 31.

These developments have taken place against the backdrop of the government drafting and finalising three different laws on cybersecurity and new counter terrorism laws. Foreign companies and industry lobby groups are worried that the proposed regulations may impinge on their privacy and force them to share "sensitive intellectual property" with the government in the name of "national security".

"Foreign companies feel they are vulnerable towards potential scrutiny and even attacks by Chinese authorities," Yun Sun, a senior associate with the East Asia programme at the Washington think tank Stimson Center, told The National today.

She said the new laws make foreign companies vulnerable towards potential scrutiny or even potential investigation by Chinese authorities. "This reduces the security level for these companies and their products, and also threatens the credibility for their operations in the global market," she said.

Beijing says the new laws have mainly been brought to deal with the threat of terrorism from militants involved in the East Turkmenistan movement in western China's Xinjiang province, and the enhanced global fears after the recent terrorist attacks in parts of Europe and Egypt. The Xinjiang-based militants have attacked targets in Beijing and Kunming cities besides carrying out bomb attacks in the western province in recent years.

"The government's main objective is to fight terrorist using the cyber space to further their activities. But it also wants to control data flow. It is this aspect that would hurt businesses," Ada Wang, a legal counsel and compliance officer with TUVRheinland, said yesterday.

"The new laws will not just affect foreign companies. It would also hamper Chinese companies operating overseas because the government does not want sensitive date to leave the country," she said. Indeed, the rules make it obligatory for companies to use specified infrastructure, and ensure that their websites are hosted in satellites hovering over China, and not in foreign locations.

Other Chinese experts and businessmen see it differently. "There will be a new phase for internet development in China," said Xiong Huang, a researcher at Communication University of China, said listening to the Chinese president Xi Jinping talk about the importance of internet security at a conference in Beijing last month.

Following the event, Jack Ma, the founder and chairman of China's giant e-commerce company Alibaba Group, said: "This is the first high-profile meeting in the internet field for our country. Not only does the meeting show how much China values the internet as a national strategy, but the country has a quite high level in both practice and theory on the development of the internet. I'm firm about the internet development in China after the speech."

What the regulations might do is force more foreign companies to enter into joint ventures with local enterprises to make sure they do not cross the line and attract the wrath of the authorities empowered with the new legislation.

The laws cover all businesses engaged in transmission of data via cyber space. The regulations state that companies are expected to: assist authorities in unravelling complicated data whenever required; use data infrastructure that is based in China; use encryption technology before transmitting data outside China; never generate or use data in any manner that would affect the country's national security; disallow any person, groups or organisation to use their internet platforms to disseminate propaganda against Chinese political systems, or instigate the local population against government authorities.

One of the implications of the new law is that it will involve additional costs to build secure internet infrastructure and hire legal services to deal with compliance issue. This is partly because the new law is vague about compliance requirements, and not specifically pinpointed, an analysts said.

Companies based in Hong Kong will now be treated as offshore enterprises, and treated as foreign firms under these laws. This can be a bothersome to foreign companies because many of them are registered in Hong Kong, and not in mainland China.

One analyst, who declined to be named, said that the rules are not meant to target foreign companies. "They have merely come in the way of these laws because they impose a wide range of restrictions on the use of internet, and flow of data," he said.

New York Times
Sensitive Email Routinely Sent as Unclassified
Wednesday, 11 May 2016
Byline: Steven Lee Myers

Washington - On the morning of March 13, 2011, the assistant secretary of state for Near Eastern affairs, Jeffrey D. Feltman, wrote an urgent email to more than two dozen colleagues informing them

that Saudi Arabia and the United Arab Emirates were sending troops into Bahrain to put down antigovernment protests there.
Mr. Feltman's email prompted a string of 10 replies and forwards over the next 24 hours, including to Secretary of State Hillary Clinton, as the Obama administration debated what was happening and how to respond.

The chain contained information now declared classified, including portions of messages written by Mr. Feltman; the former ambassador in Kuwait, Deborah K. Jones; and the current director of the Central Intelligence Agency, John O. Brennan.

The top administration officials discussed the Bahrain situation on unclassified government computer networks, except for Mrs. Clinton, who used a private email server while serving as secretary of state.

Her server is now the subject of an F.B.I. investigation, which is likely to conclude in the next month, about whether classified information was mishandled.

Whatever the disposition of the investigation, the discussion of troops to Bahrain reveals how routinely sensitive information is emailed on unclassified government servers, reflecting what many officials describe as diplomacy in the age of the Internet, especially in urgent, fast-developing situations.

A review of the 30,322 emails from Mrs. Clinton's private server that the State Department has made public under the Freedom of Information Act provide an extensive record of how such sensitive information often looped throughout President Obama's foreign policy apparatus on unclassified systems, from embassies to the United Nations to the White House.

The senders included Denis R. McDonough, currently the White House chief of staff and previously the deputy national security adviser, and Susan E. Rice, the former American representative at the United Nations who is now Mr. Obama's national security adviser.

Many of the emails were sent over the State Department's unclassified system, state.gov, which is considered secure but not at the level of the State Department's system for emailing classified information.

At the State Department, the Pentagon and the White House, among other agencies, officials have two systems for email, one for classified messages and one for more routine business. They are nicknamed the "high side" and the "low side."

Mrs. Clinton's private server -- set up in her home in Westchester County, N.Y. -- was assumed to be even less secure than the State Department's "low side," although the unclassified servers at some government agencies have been hacked in recent years.

One result of Mrs. Clinton's decision to maintain a private server is that it has put State Department officials on the defensive about their use of state.gov for some business that might be considered classified.

Of the 30,322 emails made public, 2,028 have had portions redacted and are now classified at the lowest level of classification, "confidential."

Nearly three-quarters of those emails were classified because they contained what is called "foreign government information" -- a vast category of information, gathered through conversations and meetings with foreign counterparts that are the fundamentals of diplomacy, but which had to be protected when the emails were released.

Last week, in an apparent attempt to dispel criticism that many of the emails were improperly sent, a top State Department official argued in a letter to three Senate Democrats that the nation's diplomats and officials were in fact allowed to send "foreign government information" through the government's unclassified computer systems.

"Department officials of necessity routinely receive such information through unclassified channels," said the letter, dated May 2 and written by the assistant secretary of state for legislative affairs, Julia Frifield.

"For example, diplomats engage in meetings with counterparts in open settings, have phone calls with foreign contacts over unsecure lines, and email with and about foreign counterparts via unclassified systems."

The letter went on to say that using "foreign government information" in unclassified emails "does not amount to mishandling the information."

The State Department, unlike some other federal agencies, does not have the authority to redact that category of information even if it is required to release documents under the Freedom of Information Act.

Thus, the only way the State Department could withhold "foreign government information" in the emails being released under court order was to classify it, according to the letter.

The letter was a reply to one sent in March to Senators Patrick J. Leahy of Vermont, Thomas R. Carper of Delaware and Dianne Feinstein of California. A copy was given to The New York Times by a government official who believed the classification of the emails was unfairly implicating diplomats and other officials conducting diplomacy in the modern era.

Of the 30,322 emails, the F.B.I.'s investigation has focused on a smaller number, including 22 that the C.I.A. insisted contained information classified "top secret."

Those emails have not been released, even with redactions, because they include material classified at the highest levels, known as "top secret/SAP," according to a letter from the inspector general of the nation's intelligence agencies, I. Charles McCullough III.

That designation refers to "special access programs," which are among the nation's most guarded secrets. The emails are said to include references to, among other things, the C.I.A.'s program to hunt and kill suspected terrorists with armed drones in Pakistan.

An additional 65 emails, which have been released, have had portions redacted because they included information classified at the level of "secret."

One exchange of emails typical of those now classified because they contain "foreign government information" involved Mr. McDonough, Ms. Rice and her deputy at the time, Rosemary A. DiCarlo, and the Palestinian effort in September 2011 to be recognized as a state by the United Nations.

The exchange included eight separate emails, all sent on unclassified networks. Of those, six were redacted almost completely when the State Department released them in January.

According to the subject line and what information does appear, the three discussed deliberations between the United Nations secretary general, Ban Ki-moon, and the Palestinian president, Mahmoud Abbas, as well as Ms. Rice's discussion with the Palestinian representative at the United Nations, Riyad H. Mansour, on the bid for statehood -- all instances of "foreign government information."

The chain of emails eventually encompassed 16 officials, including political appointees and career diplomats, and was ultimately forwarded to Mrs. Clinton's inbox by Jake Sullivan, her deputy then and now the senior policy adviser for her election campaign.

Philip H. Gordon, an assistant secretary of state under Mrs. Clinton, said, "If all these respected, senior foreign service officers and experienced ambassadors are sending these emails, then this issue is not about how Hillary Clinton managed her email, but how the State Department communicates in the 21st century."

Mr. Gordon, later a special assistant to the president for the Middle East, wrote more than 40 emails that were redacted on the grounds that they contained classified information.

Mrs. Clinton herself wrote, responded to or forwarded 96 emails that have been classified in part, including one that is classified secret; 46 of those contained the "foreign government information" that the department's letter addressed.

There are, to be sure, other emails that do not fall into the category of "foreign government information," and some raise questions about the sort of information senior officials sent in unclassified emails.

In 18 emails, for example, information has been classified on the grounds that it identifies C.I.A. officials, including two instances that are now considered "secret."

One of those was a seemingly benign photo opportunity listed on Mrs. Clinton's daily schedule, with the person who gave her a daily intelligence briefing, making it obvious that the person was an agency employee.

That email was originally released as "confidential" but upgraded to "secret," probably reflecting that the person holds an undercover position now.

Another exchange involving the C.I.A. came the day after David H. Petraeus resigned as the agency's director in November 2012. Mr. Brennan, then still at the White House, sent an email -- detailing the provisions for Mr. Petraeus's personal security following his surprise resignation -- to Thomas E. Donilon, Mr. Obama's national security adviser. Mr. Donilon then forwarded it to Mrs. Clinton.

"Madam Secretary -- Attached is an update on the security for Dave P.," he wrote. The entirety of Mr. Brennan's note has now been redacted and classified as "confidential" on the grounds that it involves "vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security."

Mr. Petraeus ultimately pleaded guilty to a misdemeanor for keeping highly classified information in eight black notebooks he kept in his home, including such details as the names of covert officers and programs, and sharing them with his biographer and lover.

A spokesman at the C.I.A., Ryan Trapani, said in a statement that Mr. Brennan had believed that the information he sent in the email was unclassified.

"When operating in a position like he was at the White House, officials often have to make spot judgments about whether information is classified or not," he wrote.

"In most cases, the determinations are correct, but in some situations, another agency may consider certain information classified that the author does not."

The Hill
19 months before deadline, lawmakers draw battle lines on spying powers
Tuesday, 10 May 2016
Byline: Julian Hattem

Washington - Members of Congress are starting to put down markers in a major battle over U.S. spying powers that it expected to drag on for more than a year.
The early action appears to reflect an effort by leading Republicans and national security hawks to get out in front of privacy advocates who want to restrict the National Security Agency's power to collect reams of data about foreigners suspected of being spies, terrorists or other targets.

Information about an unknown number of U.S. residents is also included in sweeps authorized by Section 702 of the Foreign Intelligence Surveillance Act.

The law must be renewed by December 2017, but the Senate Judiciary Committee on Tuesday held a hearing on the issue 19 months before that deadline.

"I'd like to begin a conversation about it well in advance of that reauthorization," Chairman Chuck Grassley (R-Iowa) said at the start of Tuesday's hearing.

Recent terror attacks in Paris, Brussels and San Bernardino, Calif., he said, "underscore that one of the responsibilities of our government is to ensure that those who protect us every day, including the intelligence community, have the tools to keep us safe."

The law undergirds high-profile spying activities such as the PRISM and Upstream programs, but many of the details about its use remain in the shadows.

"We're still missing a lot of facts about Section 702 implementation," Sen. Patrick Leahy (D-Vt.), the committee's ranking member, said on Tuesday.

"It sweeps up a sizable amount of information about Americans who are communicating with foreigners," he added. "Despite these concerns about Americans' communications being swept up, we still do not know how much of our data is collected under this authority."

Despite repeated requests from Capitol Hill, intelligence officials have given no estimates of the number of Americans whose communications are caught up in warrantless government searches targeting foreigners. Because of the global nature of the internet, privacy advocates have warned that the number could be high.

Director of National Intelligence James Clapper has bristled at calls to estimate how many U.S. residents have their data swept up by the program, saying it would be difficult to calculate.

Leahy and a small handful of Democrats appeared open to modifications requiring officials to obtain a warrant before searching for data on citizens.

But any effort at reform appears primed to run into stiff opposition from lawmakers in both parties, given the broad consensus about the importance of the data gathering for combating terrorism.

"The question to me is do we want to somehow limit ourselves in terms of access to foreign intelligence in a way that could make us less safe?" asked John Cornyn (Texas), the No. 2 Senate Republican, rhetorically. "That's an important conversation to have, but I'm pretty clear on where I come down."

Lawmakers wondered on Tuesday whether implementing new warrant requirements could rebuild "walls" between U.S. surveillance agencies similar to those blamed, in part, for failing to prevent the 9/11 attacks.

And erring too far on the side of individual privacy might keep intelligence officials from finding important information, Cornyn warned. He pointed to examples in which al Qaeda operatives have used words like "wedding" and "marriage" as code words during a terror plots.

"In our zeal to protect love letters, we don't want to protect terrorists who might use code words to escape scrutiny by the intelligence community," he warned.

Sen. Dianne Feinstein (D-Calif.), the vice chairwoman of the Intelligence Committee, said that if anything, the government should be more forthcoming about the ways in which Section 702 is used.

"Those of us who meet two afternoons a week and go over intelligence ... see the value of this program," said Feinstein, referring to the Intelligence Committee's biweekly meetings. "But I think the general public does not."

"I really think it is lawful and well-balanced," she said.

"In my view, it's only intelligence, lawfully collected, that's able to prevent another attack in this country."

The Intercept
Hackers Attempt to Hold Capitol Hill Data for Ransom
Wednesday, 11 May 2016
Byline: Jenna McLaughlin

Washington - The House is under attack by hackers hoping to infiltrate congressional computers, encrypt their contents, and then force users to pay a ransom to get their access back.
"In the past 48 hours, the House Information Security Office has seen an increase of attacks on the House Network using third party, web-based mail applications such as YahooMail, Gmail," the House's Technology Service Desk wrote in an email to House staffers on April 30.

According to the email obtained by The Intercept, the hacked emails impersonate familiar people and invite staffers to download an attachment laced with malware--what's known as a "phishing" attack.

"When a user clicks on the link in the attack e-mail, the malware encrypts all files on that computer, including shared files, making them unusable until a 'ransom' is paid," the email said.

But House administrative offices refused to say how many if any attacks have been successful, what sort of data may have been affected, or how much has been paid in ransom, if anything.

"The potential for ransomware attacks the House faces is similar to any large organization," a spokesman for the Chief Administrative Officer of the House wrote in a statement to The Intercept. "The House recognizes the importance of taking steps to employ a cyber security plan to protect our infrastructure, and we constantly work to improve training and education for all House users."

A lockdown on parts of the House internet network--from WiFi to Ethernet--remains ongoing.

Access to both YahooMail and Google Cloud services hosted by Google's appspot.com appear to be completely blocked on the House's network, according to Ted Henderson, a former Hill staffer and founder of two social-network applications designed for Capitol Hill communication: Cloakroom and Capitol Bells. It's unclear if both blockages, not just Yahoo's, are related to the ransomware attacks.

Henderson says his several thousand users cannot post to the social networks inside the House office buildings. The way Cloakroom works, you're normally able to log-in either anonymously simply by using Capitol Hill Wi-Fi or with your staff email address. The Senate office buildings don't appear to be affected.

"This is the first time I've seen this happen at a scale like this in five years," Henderson wrote The Intercept in an email.

In recent months, several lawmakers have penned letters asking the Obama administration how it's dealing with the problem of ransomware--a type of attack more than two dozen government agencies have admitted to confronting in the past as well.

Now that Congress itself is the target, security researchers are hopeful the issue will draw more national attention. "What you're seeing in Congress is just part of what's happening," Markus Jakobsson, founder of "Zapfraud", a scam email detection service, and an expert on phishing attacks told The Intercept. "This will hopefully bring some awareness to decision makers...once they start [going after Congress], there will be changes."

Ransomware attacks take many forms. Some hackers have managed to infect entire websites with malware.

It's not clear whether the current spate of attacks on the House network were targeted, or whether House users just happened to find themselves among the ever-growing number of victims.

Ransomware is a major and growing threat to security. Just the day before the House emailed its staff about the attacks, the FBI published a press release titled "Incidents of Ransomware on the Rise," warning that "hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses" are all under increasing threat of being hacked and ransomed.

Nonprofit healthcare organization Health Information Trust Alliance warned in April that more than half of 30 hospitals it surveyed were infected with malware--most of it ransomware. Los Angeles hospital Hollywood Presbyterian paid $17,000 to recover its data in March.

Police departments have also been victims of ransomware attacks, sometimes forced to pay up to recover everything. One police chief compared the extortion to "what felt like terrorist threats."

It's not at all clear how to solve the problem, though researchers have come up with some solutions and recommendations. "This is something that the technical community is still struggling with getting a firm grip on," Jakobsson said.

He suggests Congress install several levels of filters to detect possible spam and scams, backup their data, and launch awareness campaigns to alert people to the reality of the problem. "The problem of social engineering is so vast that you can't just do one and hope that's enough," he said.

Motherboard (Vice)
Encryption Gets in The Way of 75% of Cases, Europol Chief Says
Tuesday, 10 May 2016
Byline: Joseph Cox

New York - In the US, police and prosecutors continue to say encryption--the use of math to protect data from outside eyes, including those of the government--presents a significant barrier to solving crimes or following leads.
Now, on the other side of the Atlantic, the head of Europe's law enforcement body is saying that encryption is an issue in the vast majority of cases the agency sees.

"Encryption dilemma must be solved soon. Real problem in 75% of all Europol cases," Rob Wainwright, director of Europol, tweeted on Sunday.

The tweet came in response to an op-ed written by John Naughton, a professor from the Open University, and published by the Guardian, that said an opportunity for more permanently addressing law enforcement's concerns around encryption had been lost during the FBI and Apple legal fight in San Bernardino.

It is not clear what sort of encryption Wainwright was referring to; be that message encryption to secure communications, or hard-drive encryption that protects data stored on devices, which was the issue at hand in the recent Apple case.

When asked about it, Claire Georges from Europol's corporate communications answered broadly about technologies used by criminals, citing encryption, anonymisation tools such as Tor, and even implied that virtual currencies such as bitcoin are part of the problem.

"The use of anonymisation and encryption technologies is widening and is key issue for law enforcement in all criminal areas," she told Motherboard in an email.

"Technology in general is used not only by cybercriminals, but also by drug dealers, child sexual offenders and other criminals involved in different illegal activities. Encryption is commonly used in secure communications and is becoming a standard protection feature in many products, such as e-wallets for virtual currencies."

Georges also pointed to Europol's Internet Organised Crime Threat Assessment (iOCTA) from 2014, which reads "The use of anonymisation tools is ubiquitous amongst the cyber underground."

Responding to a question of whether backdoors are an avenue for law enforcement, Wainwright wrote in another tweet that "back doors not the solution but regulated front door access. Finding how is key question."

Security experts say any sort of "front door," even if designed only for law enforcement, would be vulnerable to exploitation from hackers and malicious actors, undermining the security of all devices that used it.

Encryption, in some cases, may present an issue for law enforcement. But lumping message and hard-drive encryption, along with technologies such as Tor, all into the same basket is not helpful for anyone; as each requires a unique response, all balancing privacy, security, and access for police.

The Guardian (London)
Court refuses request to force alleged hacker to divulge passwords
Tuesday, 10 May 2016
Byline: Jamie Grierson, Diane Taylor

London - An alleged hacker fighting extradition to the US will not have to give the passwords for his encrypted computers to British law enforcement officers, following a landmark legal ruling.

Lauri Love, a 31- year-old computer scientist, has been accused of stealing "massive quantities" of sensitive data from US Federal Reserve and Nasa computers. His lawyers say he faces up to 99 years in prison if found guilty in the US.

The National Crime Agency (NCA) raided Love's family home in Stradishall, Suffolk, in October 2013, seizing encrypted computers and hard drives. No charges were brought against him in Britain and Love is suing the NCA for the return of six items of encrypted hardware, which he says contain his entire digital life.

The NCA applied to the courts to force Love to hand over his passwords before it returns the computers but this was rejected by a judge on Tuesday.

Speaking to the Guardian, Love called on governments around the world to set aside differences with activists and hackers and to work together to improve global computer security.

"The US government is conducting a war against information activists like me," he said. "This kind of thing is a distraction from what is really important - keeping the world secure. I am offering a 'third way' where governments and hackers work together and bridge the divide. Governments should be making the most of the talent that computer hackers have to try to work together to solve the problems of computer lack of security.

"If someone hacks into your computer they can take over your life and your identity. We are more and more reliant on computer security for security for ourselves."

Love said there was a lot of distrust of governments from activists as a result of scandals involving surveillance and undercover policing. "We have to put our differences aside," he urged. "What we really need to do is sit round the table together and start to have a conversation."

Love said the past few years of interactions with the police and US authorities had taken an enormous personal toll on both him and his family. "I spent two years in an acute and crippling state of mental distress," he said. "I developed eczema and had a lot of difficulty sleeping. Now I am feeling recovered enough to continue studying for my electrical engineering degree and have my finals coming up."

District judge Nina Tempia refused the NCA's application at Westminster magistrates court on Tuesday, saying that to do so would "circumvent specific legislation that has been passed in order to deal with the disclosure sought".

Speaking outside court after the ruling, Love said he was happy with the result and accused the NCA of trying to undermine protections safeguarding individuals' property.

"It is a victory, although it is a more an avoidance of disaster," he said. "It retains the status quo, which means there has to be safeguards before you force people to undermine their security."

His lawyer, Karen Todner, of Kaim Todner, said the ruling was right. "The case raised important issues of principle in relation to the right to respect for private life and right to enjoyment of property and the use of the court's case management powers.

"A decision in the NCA's favour would have set a worrying precedent for future investigations of this nature and the protection of these important human rights."

Love was arrested on 15 July 2015 on behalf of the US government, which had issued several indictments and corresponding extradition warrants.

The FBI and US Department of Justice allege that Love was involved in hacking into various government agencies, including the US army, Nasa, the Federal Reserve and the Environmental Protection Agency. His extradition hearing will be held on 28 and 29 June.

Outside court, Love said he was scared at the prospect of being sent to the US for criminal prosecution. "It is the worst thing I could imagine happening to me. I have to get on with my work and my studies, I can't afford to be stressed or depressed or anxious about it."

Love's case has echoes of the FBI and Apple dispute in the US. In 2015 and 2016, Apple received, and objected to or challenged, at least 11 orders issued by US district courts which sought to compel the firm to extract data, such as contacts, photos and calls from locked iPhones.

The most well-known instance was in February 2016, when the FBI wanted Apple to create and electronically sign new software that would enable the FBI to unlock an iPhone recovered from one of the shooters in the December 2015 terrorist attack in San Bernardino, California.

The government ultimately said it had found a third party able to assist in unlocking the iPhone and withdrew its request.

Columbia Journalism Review
Snowden interview: Why the media isn't doing its job
Wednesday, 11 May 2016
Byline: Emily Bell
Section: Interview

Interview - The Tow Center for Digital Journalism's Emily Bell spoke to Edward Snowden over a secure channel about his experiences working with journalists and his perspective on the shifting media world. This is an excerpt of that conversation, conducted in December 2015.
Emily Bell: Can you tell us about your interactions with journalists and the press?

Edward Snowden: One of the most challenging things about the changing nature of the public's relationship to media and the government's relationship to media is that media has never been stronger than it is now. At the same time, the press is less willing to use that sort of power and influence because of its increasing commercialization. There was this tradition that the media culture we had inherited from early broadcasts was intended to be a public service. Increasingly we've lost that, not simply in fact, but in ideal, particularly due to the 24-hour news cycle.

We see this routinely even at organizations like The New York Times. The Intercept recently published The Drone Papers, which was an extraordinary act of public service on the part of a whistleblower within the government to get the public information that's absolutely vital about things that we should have known more than a decade ago. These are things that we really need to know to be able to analyze and assess policies. But this was denied to us, so we get one journalistic institution that breaks the story, they manage to get the information out there. But the majors--specifically The New York Times-- don't actually run the story, they ignore it completely. This was so extraordinary that the public editor, Margaret Sullivan, had to get involved to investigate why they suppressed such a newsworthy story. It's a credit to the Times that they have a public editor, but it's frightening that there's such a clear need for one.

In the UK, when The Guardian was breaking the NSA story, we saw that if there is a competitive role in the media environment, if there's money on the line, reputation, potential awards, anything that has material value that would benefit the competition, even if it would simultaneously benefit the public, the institutions are becoming less willing to serve the public to the detriment of themselves. This is typically exercised through the editors. This is something that maybe always existed, but we don't remember it as always existing. Culturally, we don't like to think of it as having always existed. There are things that we need to know, things that are valuable for us, but we are not allowed to know, because The Telegraph or the Times or any other paper in London decides that because this is somebody else's exclusive, we're not going to report it. Instead, we'll try to "counter-narrative" it. We'll simply go to the government and ask them to make any statement at all, and we will unquestioningly write it down and publish it, because that's content that's exclusive to us. Regardless of the fact that it's much less valuable, much less substantial than actual documented facts that we can base policy discussions on. We've seemingly entered a world where editors are making decisions about what stories to run based on if it'll give oxygen to a competitor, rather than if it's news.

I would love to hear your thoughts on this, because while I do interact with media, I'm an outsider. You know media. As somebody who has worked in these cultures, do you see the same thing? Sort of the Fox News effect, where facts matter less?

Bell: It's a fascinating question. When you look at Donald Trump, there's a problem when you have a press which finds it important to report what has happened, without a prism of some sort of evaluation on it. That's the Trump problem, right? He says thousands of Muslims were celebrating in the streets of New Jersey after 9/11 and it's demonstrably not true. It's not even a quantification issue, it's just not

true. Yet, it dominates the news cycle, and he dominates the TV, and you see nothing changing in the polls--or, rather, him becoming more popular.

There are two things I think here, one of which is not new. I completely agree with you about how the economic dynamics have actually produced, bad journalism. One of the interesting things which I think is hopeful about American journalism is that within the last 10 years there's been a break between this relationship, which is the free market, which says you can't do good journalism unless you make a profit, into intellectually understanding that really good journalism not only sometimes won't make a profit, but is almost never going to be anything other than unprofitable.

I think your acts and disclosures are really interesting in that it's a really expensive story to do, and it is not the kind of story that advertisers want to stand next to. Actually people didn't want to pay to read them. Post hoc they'll say, we like The Guardian; we're going to support their work. So I agree with you that there's been a disjuncture between facts and how they are projected. I would like to think it's going to get better.

You're on Twitter now. You're becoming a much more rounded out public persona, and lots of people have seen Citizenfour. You've gone from being this source persona, to being more actively engaged with Freedom of the Press Foundation, and also having your own publishing stream through a social media company. The press no longer has to be the aperture for you. How do you see that?

Snowden: Today, you have people directly reaching an audience through tools like Twitter, and I have about 1.7 million followers right now (this number reflects the number of Twitter followers Snowden had in December 2015). These are people, theoretically, that you can reach, that you can send a message to. Whether it's a hundred people or a million people, individuals can build audiences to speak with directly. This is actually one of the ways that you've seen new media actors, and actually malicious actors, exploit what are perceived as new vulnerabilities in media control of the narrative, for example Donald Trump.

At the same time these strategies still don't work [...] for changing views and persuading people on a larger scope. Now this same thing applies to me. The director of the FBI can make a false statement, or some kind of misleading claim in congressional testimony. I can fact-check and I can say this is inaccurate. Unless some entity with a larger audience, for example, an established institution of journalism, sees that themselves, the value of these sorts of statements is still fairly minimal. They are following these new streams of information, then reporting out on those streams. This is why I think we see such a large interplay and valuable interactions that are emerging from these new media self-publication Twitter-type services and the generation of stories and the journalist user base of Twitter.

If you look at the membership of Twitter in terms of the influence and impact that people have, there are a lot of celebrities out there on Twitter, but really they're just trying to maintain an image, promote a band, be topical, remind people that they exist. They're not typically effecting any change, or having any kind of influence, other than the directly commercial one.

Bell: Let's think about it in terms of your role in changing the world, which is presenting these new facts. There was a section of the technology press and the intelligence press who, at the time of the leaks, said we already know this, except it's hidden in plain sight. Yet, a year after you made the disclosures, there was a broad shift of public perception about surveillance technologies. That may recede, and probably post-Paris, it is receding a little bit. Are you frustrated that there isn't more long-term impact? Do you feel the world has not changed quickly enough?

Snowden: I actually don't feel that. I'm really optimistic about how things have gone, and I'm staggered by how much more impact there's been as a result of these revelations than I initially presumed. I'm famous for telling Alan Rusbridger that it would be a three-day story. You're sort of alluding to this idea that people don't really care, or that nothing has really changed. We've heard this in a number of different ways, but I think it actually has changed in a substantial way.

Now when we talk about the technical press, or the national security press, and you say, this is nothing new, we knew about this, a lot of this comes down to prestige, to the same kind of signaling where they have to indicate we have expertise, we knew this was going on. In many cases they actually did not. The difference is, they knew the capabilities existed.

This is, I think, what underlies why the leaks had such an impact. Some people say stories about the mass collection of internet records and metadata were published in 2006. There was a warrantless wiretapping story in The New York Times as well. Why didn't they have the same sort of transformative impact? This is because there's a fundamental difference when it comes down to the actionability of information between knowledge of capability, the allegation that the capability could be used, and the fact that it is being used. Now what happened in 2013 is we transformed the public debate from allegation to fact. The distance between allegation and fact, at times, makes all the difference in the world.

That, for me, is what defines the best kind of journalism. This is one of the things that is really underappreciated about what happened in 2013. A lot of people laud me as the sole actor, like I'm this amazing figure who did this. I personally see myself as having a quite minor role. I was the mechanism of revelation for a very narrow topic of governments. It's not really about surveillance, it's about what the public understands--how much control the public has over the programs and policies of its governments. If we don't know what our government really does, if we don't know the powers that authorities are claiming for themselves, or arrogating to themselves, in secret, we can't really be said to be holding the leash of government at all.

One of the things that's really missed is the fact that as valuable and important as the reporting that came out of the primary archive of material has been, there's an extraordinarily large, and also very valuable amount of disclosure that was actually forced from the government, because they were so back-footed by the aggressive nature of the reporting. There were stories being reported that showed

how they had abused these capabilities, how intrusive they were, the fact that they had broken the law in many cases, or had violated the Constitution.

When the government is shown in a most public way, particularly for a president who campaigned on the idea of curtailing this sort of activity, to have continued those policies, in many cases expanded them in ways contrary to what the public would expect, they have to come up with some defense. So in the first weeks, we got rhetorical defenses where they went, nobody's listening to your phone calls. That wasn't really compelling. Then they went, "It's just metadata." Actually that worked for quite some time, even though it's not true. By adding complexity, they reduced participation. It is still difficult for the average person in the street to understand that metadata, in many cases, is actually more revealing and more dangerous than the content of your phone calls. But stories kept coming. Then they went, well alright, even if it is "just metadata," it's still unconstitutional activity, so how do we justify it? Then they go--well they are lawful in this context, or that context.

They suddenly needed to make a case for lawfulness, and that meant the government had to disclose court orders that the journalists themselves did not have access to, that I did not have access to, that no one in the NSA at all had access to, because they were bounded in a completely different agency, in the Department of Justice.

This, again, is where you're moving from suspicion, from allegation, to factualizing things. Now of course, because these are political responses, each of them was intentionally misleading. The government wants to show itself in the best possible light. But even self- interested disclosures can still be valuable, so long as they're based on facts. They're filling in a piece of the puzzle, which may provide the final string that another journalist, working independently somewhere else, may need. It unlocks that page of the book, fills in the page they didn't have, and that completes the story. I think that is something that has not been appreciated, and it was driven entirely by journalists doing follow- up.

There's another idea that you mentioned: that I'm more engaged with the press than I was previously. This is very true. I quite openly in 2013 took the position that this is not about me, I don't want to be the face of the argument. I said that I don't want to correct the record of government officials, even though I could, even though I knew they were making misleading statements. We're seeing in the current electoral circus that whatever someone says becomes the story, becomes the claim, becomes the allegation. It gets into credibility politics where they're going, oh, you know, well, Donald Trump said it, it can't be true. All of the terrible things he says put aside, there's always the possibility that he does say something that is true. But, because it's coming from him, it will be analyzed and assessed in a different light. Now that's not to say that it shouldn't be, but it was my opinion that there was no question that I was going to be subject to a demonization campaign. They actually recorded me on camera saying this before I revealed my identity. I predicted they were going to charge me under the Espionage Act, I predicted they were going to say I helped terrorists, blood on my hands, all of that stuff. It did come to pass. This was not a staggering work of genius on my part, it's just common sense, this is how it always works in the case of prominent whistleblowers. It was because of this that we needed other voices, we needed the media to make the argument.

Because of the nature of the abuse of classification authorities in the United States, there is no one that's ever held a security clearance who's actually able to make these arguments. Modern media institutions prefer never to use their institutional voice to factualize a claim in a reported story, they want to point to somebody else. They want to say this expert said, or this official said, and keep themselves out of it. But in my mind, journalism must recognize that sometimes it takes the institutional weight to assess the claims that are publicly available, and to make a determination on that basis, then put the argument forth to whoever the person under suspicion is at the time, for example, the government in this case, and go--look, all of the evidence says you were doing this. You say that's not the case, but why should we believe you? Is there any reason that we should not say this?

This is something that institutions today are loath to do because it's regarded as advocacy. They don't want to be in the position of having to referee what is and is not fact. Instead they want to play these "both sides games" where they say, instead we'll just print allegations, we'll print claims from both sides, we'll print their demonstrations of evidence, but we won't actually involve ourselves in it.

Because of this, I went the first six months without giving an interview. It wasn't until December 2013 that I gave my first interview to Barton Gellman of The Washington Post. In this intervening period my hope was that some other individual would come forth on the political side, and would become the face of this movement. But more directly I thought it would inspire some reflection in the media institutions to think about what their role was. I think they did a fairly good job, particularly for it being unprecedented, particularly for it being a segment in which the press has been, at least in the last 15 years, extremely reluctant to express any kind of skepticism regarding government claims at all. If it involved the word "terrorism," these were facts that wouldn't be challenged. If the government said, look, this is secret for a reason, this is classified for a reason, journalists would leave it at that. Again, this isn't to beat up on The New York Times, but when we look at the warrantless wiretapping story that was ready to be published in October of an election year, that [election] was decided by the smallest margin in a presidential election, at least in modern history. It's hard to believe that had that story been published, it would not have changed the course of that election.

Bell: Former Times Executive Editor Jill Abramson has said her paper definitely made mistakes, "I wish we had not withheld stories." What you're saying certainly resonates with what I know and understand of the recent history of the US press, which is that national security concerns post-9/11 really did alter the relationship of reporting, particularly with administration and authority in this country. What we know about drone programs comes from reporting, some of it comes from the story which The Intercept got hold of, and Jeremy Scahill's reporting on it, which has been incredibly important. But a great deal of it has also come from the ground level. The fact that we were aware at all that drones were blowing up villages, killing civilians, crossing borders where they were not supposed to be really comes from people who would report from the ground.

Something interesting has definitely happened in the last three years, which makes me think about what you are telling us about how the NSA operates. We're seeing a much closer relationship now between

journalism and technology and mass communication technology than we've ever seen before. People are now completely reliant on Facebook. Some of that is a commercial movement in the US, but you also have activists and journalists being regularly tortured or killed in, say, Bangladesh, where it's really impossible to operate a free press, but they are using these tools. It is almost like the American public media now is Facebook. I wonder how you think about this? It's such a recent development.

Snowden: One of the biggest issues is that we have many more publishers competing for a finite, shrinking amount of attention span that's available. This is why we have the rise of these sort of hybrid publications, like a BuzzFeed, that create just an enormous amount of trash and cruft. They're doing AB testing and using scientific principles. Their content is specifically engineered to be more attention getting, even though they have no public value at all. They have no news value at all. Like here's 10 pictures of kittens that are so adorable. But then they develop a news line within the institution, and the idea is that they can drive traffic with this one line of stories, theoretically, and then get people to go over onto the other side.

Someone's going to exploit this; if it's not going to be BuzzFeed, it's going to be somebody else. This isn't a criticism of any particular model, but the idea here is that the first click, that first link is actually consuming attention. The more we read about a certain thing, that's actually reshaping our brains. Everything that we interact with, it has an impact on us, it has an influence, it leaves memories, ideas, sort of memetic expressions that we then carry around with us that shape what we look for in the future, and that are directing our development.

Bell: Yes, well that's the coming singularity between the creation of journalism and large-scale technology platforms, which are not intrinsically journalistic. In other words, they don't have a primary purpose.

Snowden: They don't have a journalistic role, it's a reportorial role.

Bell: Well, it's a commercial role, right? So when you came to Glenn and The Guardian, there wasn't a hesitation in knowing the primary role of the organization is to get that story to the outside world as securely and quickly as possible, avoiding prior restraint, protecting a source.

Is source protection even possible now? You were extremely prescient in thinking there's no point in protecting yourself.

Snowden: I have an unfair advantage.

Bell: You do, but still, that's a big change from 20 years ago.

Snowden: This is something that we saw contemporary examples of in the public record in 2013. It was the James Rosen case where we saw the Department of Justice, and government more broadly, was

abusing its powers to demand blanket records of email and call data, and the AP case where phone records for calls that were made from the bureaus of journalism were seized.

That by itself is suddenly chilling, because the traditional work of journalism, the traditional culture, where the journalist would just call their contact and say, hey, let's talk, suddenly becomes incriminating. But more seriously, if the individual in question, the government employee who is working with a journalist to report some issue of public interest, if this individual has gone so far to commit an act of journalism, suddenly they can be discovered trivially if they're not aware of this.

I didn't have that insight at the time I was trying to come forward because I had no relationship with journalists. I had never talked to a journalist in any substantive capacity. So, instead I simply thought about the adversarial relationship that I had inherited from my work as an intelligence officer, working for the CIA and the NSA. Everything is a secret and you've got two different kinds of cover. You've got cover for status, which is: You're overseas, you're living as a diplomat because you have to explain why you're there. You can't just say, oh, yeah, I work for the CIA. But you also have a different kind of cover which is what's called cover for action. Where you're not going to live in the region for a long time, you may just be in a building and you have to explain why you're walking through there, you need some kind of pretext. This kind of trade-craft unfortunately is becoming more necessary in the reportorial process. Journalists need to know this, sources need to know this. At any given time, if you were pulled over by a police officer and they want to search your phone or something like that, you might need to explain the presence of an application. This is particularly true if you're in a country like Bangladesh. I have heard that they're now looking for the presence of VPN [virtual private network software] for avoiding censorship locks and being able to access uncontrolled news networks as evidence of opposition, allegiance, that could get you in real trouble in these areas of the world.

At the time of the leaks I was simply thinking, alright the government--and this isn't a single government now--we're actually talking about the Five Eyes intelligence alliance [the United States, the United Kingdom, New Zealand, Australia, Canada] forming a pan-continental super-state in this context of sharing, they're going to lose their minds over this. Some institutions in, for example, the UK, can levy D notices, they can say, look, you can't publish that, or you should not publish that. In the United States it's not actually certain that the government would not try to exercise prior restraint in slightly different ways, or that they wouldn't charge journalists as accomplices in some kind of criminality to interfere with the reporting without actually going after the institutions themselves, single out individuals. We have seen this in court documents before. This was the James Rosen case, where the DOJ had named him as sort of an accessory--they said he was a co-conspirator. So the idea I thought about here was that we need institutions working beyond borders in multiple jurisdictions simply to complicate it legally to the point that the journalists could play games, legally and journalistically more effectively and more quickly than the government could play legalistic games to interfere with them.

Bell: Right, but that's kind of what happened with the reporting of the story.

Snowden: And in ways that I didn't even predict, because who could imagine the way a story like that would actually get out of hand and go even further: Glenn Greenwald living in Brazil, writing for a US institution for that branch, but headquartered in the UK, The Washington Post providing the institutional clout and saying, look, this is a real story, these aren't just crazy leftists arguing about this, and Der Spiegel in Germany with Laura [Poitras]. It simply represented a system that I did not believe could be overcome before the story could be put out. By the time the government could get their ducks in a row and try to interfere with it, that would itself become the story.

Bell: You're actually giving a sophisticated analysis of much of what's happened to both reporting practice and media structures. As you say, you had no prior interactions with journalists. I think one of the reasons the press warmed to you was because you put faith in journalists, weirdly. You went in thinking I think I can trust these people, not just with your life, but with a huge responsibility. Then you spent an enormous amount of time, particularly with Glenn, Laura, and Ewen [MacAskill] in those hotel rooms. What was that reverse frisking process like as you were getting to know them? My experience is as people get closer to the press, they often like it less. Why would you trust journalists?

Snowden: This gets into the larger question--how did you feel about journalists, what was the process of becoming acquainted with them? There's both a political response and a practical response. Specifically about Glenn, I believe very strongly that there's no more important quality for a journalist than independence. That's independence of perspective, and particularly skepticism of claims. The more powerful the institution, the more skeptical one should be. There's an argument that was put forth by an earlier journalist, I.F. Stone: "All governments are run by liars and nothing they say should be believed." In my experience, this is absolutely a fact. I've met with Daniel Ellsberg and spoken about this, and it comports with his experience as well. He would be briefing the Secretary of Defense on the airplane, and then when the Secretary of Defense would disembark right down the eight steps of the plane and shake hands with the press, he would say something that he knew was absolutely false and was completely contrary to what they had just said in the meeting [inside the place] because that was his role. That was his job, his duty, his responsibility as a member of that institution.

Now Glenn Greenwald, if we think about him as an archetype, really represents the purest form of that. I would argue that despite the failings of any journalist in one way or another, if they have that independence of perspective, they have the greatest capacity for reporting that a journalist can attain. Ultimately, no matter how brilliant you are, no matter how charismatic you are, no matter how perfect or absolute your sourcing is, or your access, if you simply take the claims of institutions that have the most privilege that they must protect, at face value, and you're willing to sort of repeat them, all of those other things that are working in your favor in the final calculus amount to nothing because you're missing the fundamentals.

There was the broader question of what it's like working with these journalists and going through that process. There is the argument that I was naïve. In fact, that's one of the most common criticisms about me today--that I am too naïve, that I have too much faith in the government, that I have too much faith in the press. I don't see that as a weakness. I am naïve, but I think that idealism is critical to achieving

change, ultimately not of policy, but of culture, right? Because we can change this or that law, we can change this or that policy or program, but at the end of the day, it's the values of the people in these institutions that are producing these policies or programs. It's the values of the people who are sitting at the desk with the blank page in Microsoft Office, or whatever journalists are using now.

Bell: I hope they're not using Microsoft Office, but you never know.

Snowden: They have the blank page ...

Bell: They have the blank page, exactly.

Snowden: In their content management system, or whatever. How is that individual going to approach this collection of facts in the next week, in the next month, in the next year, in the next decade? What will the professor in the journalism school say in their lecture that will impart these values, again, sort of memetically into the next cohort of reporters? If we do not win on that, we have lost comprehensively. More fundamentally, people say, why did you trust the press, given their failures? Given the fact that I was, in fact, quite famous for criticizing the press.

Bell: If they had done their job, you would be at home now.

Snowden: Yeah, I would still be living quite comfortably in Hawaii.

Bell: Which is not so bad, when you put it that way.

Snowden: People ask how could you do this, why would you do this? How could you trust a journalist that you knew had no training at all in operational security to keep your identity safe because if they screw up, you're going to jail. The answer was that that was actually what I was expecting. I never expected to make it out of Hawaii. I was going to try my best, but my ultimate goal was simply to get this information back in the hands of the public. I felt that the only way that could be done meaningfully was through the press. If we can't have faith in the press, if we can't sort of take that leap of faith and either be served well by them, or underserved and have the press fail, we've already lost. You cannot have an open society without open communication. Ultimately, the test of open communication is a free press. If they can't look for information, if they can't contest the government's control of information, and ultimately print information--not just about government, but also about corporate interests, that has a deleterious impact on the preferences of power, on the prerogatives of power. You may have something, but I would argue it's not the traditional American democracy that I believed in.

So the idea here was that I could take these risks because I already expected to bear the costs. I expected the end of the road was a cliff. This is actually illustrated quite well in Citizenfour because it shows that there was absolutely no plan at all for the day after.

The planning to get to the point of working with the journalists, of transmitting this information, of explaining, contextualizing--it was obsessively detailed, because it had to be. Beyond that, the risks were my own. They weren't for the journalists. They could do everything else. That was by design as well, because if the journalists had done anything shady--for example, if I had stayed in place at the NSA as a source and they had asked me for this document, and that document, it could have undermined the independence, the credibility of the process, and actually brought risks upon them that could have led to new constraints upon journalism.

Bell: So nothing you experienced in the room with the team, or what happened after, made you question or reevaluate journalism?

Snowden: I didn't say that. Actually working more closely with the journalists has radically reshaped my understanding of journalism, and that continues through to today. I think you would agree that anybody who's worked in the news industry, either directly or even peripherally, has seen journalists-- or, more directly, editors--who are terrified, who hold back a story, who don't want to publish a detail, who want to wait for the lawyers, who are concerned with liability.

You also have journalists who go out on their own and they publish details which actually are damaging, directly to personal safety. There were details published by at least one of the journalists that were discussing communication methods that I was still actively using, that previously had been secret. But the journalists didn't even forewarn me, so suddenly I had to change all of my methods on the fly. Which worked out OK because I had the capabilities to do that, but dangerous.

Bell: When did that happen?

Snowden: This was at the height of public interest, basically. The idea here is that a journalist ultimately, and particularly a certain class of journalist, they don't owe any allegiance to their source, right? They don't write the story in line with what the sources desires, they don't go about their publication schedule to benefit, or to detriment, in theory, the source at all. There are strong arguments that that's the way it should be: public knowledge of the truth is more important than the risks that knowledge creates for a few. But at the same time, when a journalist is reporting on something like a classified program implicating one of the government's sources, you see an incredibly high standard of care applied to make sure they can't be blamed if something goes wrong down the road after publication. The journalists will go, well we'll hold back this detail from that story reporting on classified documents, because if we name this government official it might expose them to some harm, or it might get this program shut down, or even if it might cause them to have to rearrange the deck chairs in the operations in some far away country.

That's just being careful, right? But ask yourself--should journalists be just as careful when the one facing the blowback of a particular detail is their own source? In my experience, the answer does not seem to be as obvious as you might expect.

Bell: Do you foresee a world where someone won't have to be a whistleblower in order to reveal the kinds of documents that you revealed? What kinds of internal mechanisms would that require on behalf of the government? What would that look like in the future?

Snowden: That's a really interesting philosophical question. It doesn't come down to technical mechanisms, that comes down to culture. We've seen in the EU a number of reports from parliamentary bodies, from the Council of Europe, that said we need to protect whistleblowers, in particular national security whistleblowers. In the national context no country really wants to pass a law that allows individuals rightly, or wrongly, to embarrass the government. But can we provide an international framework for this? One would argue, particularly when espionage laws are being used to prosecute people, they already exist. That's why espionage, for example, is considered a political offense, because it's just a political crime, as they say. That's a fairly weak defense, or fairly weak justification, for not reforming whistleblower laws. Particularly when, throughout Western Europe they're going, yeah, we like this guy, he did a good thing. But if he shows up on the doorstep we're going to ship him back immediately, regardless of whether it's unlawful, just because the US is going to retaliate against us. It's extraordinary that the top members of German government have said this on the record--that it's realpolitik; it's about power, rather than principle.

Now how we can fix this? I think a lot of it comes down to culture, and we need a press that's more willing and actually eager to criticize government than they are today. Even though we've got a number of good institutions that do that, or that want to do that, it needs a uniform culture. The only counterargument the government has made against national security whistleblowing, and many other things that embarrassed them in the past, is that well, it could cause some risk, we could go dark, they could have blood on their hands.

Why do they have different ground rules in the context of national security journalism?

We see that not just in the United States, but in France, Germany, the UK, in every Western country, and of course, in every more authoritarian country by comparison they are embracing the idea of state secrets, of classifications, or saying, you can't know this, you can't know that.

We call ourselves private citizens, and we refer to elected representatives as public officials, because we're supposed to know everything about them and their activities. At the same time, they're supposed to know nothing about us, because they wield all the power, and we hold all of the vulnerability. Yet increasingly, that's becoming inverted, where they are the private officials, and we are the public citizens. We're increasingly monitored and tracked and reported, quantified and known and influenced, at the same time that they're getting themselves off and becoming less reachable and also less accountable.

Bell: But Ed, when you talk about this in those terms, you make it sound as though you see this as a progression. Certainly there was a sharp increase, as you demonstrated, in overreach of oversight post-9/11. Is it a continuum?

It felt from the outside as though America, post-9/11, for understandable reasons, it was almost like a sort of national psychosis. If you grew up in Europe, there were regular terrorist acts in almost every country after the Second World War, though not on the same scale, until there was a brief, five-year period of respite, weirdly running up to about 2001. Then the nature of the terrorism changed. To some extent, that narrative is predictable. You talk about it as an ever increasing problem. With the Freedom Act in 2015, the press identified this as a significant moment where the temperature had changed. You don't sound like you really think that. You sound as though you think that this public/private secrecy, spying, is an increasing continuum. So how does that change? Particularly in the current political climate where post-Paris and other terrorist attacks we've already seen arguments for breaking encryption.

Snowden: I don't think they are actually contradictory views to hold. I think what we're talking about are the natural inclinations of power and vice, what we can do to restrain it, to maintain a free society. So when we think about where things have gone in the USA Freedom Act, and when we look back at the 1970s, it was even worse in terms of the level of comfort that the government had that it could engage in abuses and get away with them. One of the most important legacies of 2013 is not anything that was necessarily published, but it was the impact of the publication on the culture of government. It was a confirmation coming quite quickly in the wake of the WikiLeaks stories, which were equally important in this regard. That said, secrecy will not hold forever. If you authorize a policy that is clearly contrary to law, you will eventually have to explain that.

The question is, can you keep it under wraps long enough to get out of the administration, and hopefully for it to be out of the egregious sort of thing where you'll lose an election as a result. We see the delta between the periods of time that successive administrations can keep a secret is actually diminishing--the secrets are becoming public at an accelerated pace. This is a beneficial thing. This is the same in the context of terrorism.

There is an interesting idea--when you were saying it's sort of weird that the US has what you described as a collective psychosis in the wake of 9/11 given that European countries have been facing terrorist attacks routinely. The US had actually been facing the same thing, and actually one would argue, experienced similarly high-impact attacks, for example, the Oklahoma City bombing, where a Federal building was destroyed by a single individual or one actor.

Bell: What do you think about the relationship between governments asking Facebook and other communications platforms to help fight ISIS?

Snowden: Should we basically deputize companies to become the policy enforcers of the world? When you put it in that context suddenly it becomes clear that this is not really a good idea, particularly because terrorism does not have a strong definition that's internationally recognized. If Facebook says, we will take down any post from anybody who the government says is a terrorist, as long as it comes from this government, suddenly they have to do that for the other government. The Chinese allegations of who is and who is not a terrorist are going to look radically different than what the FBI's are going to

be. But if the companies try to be selective about them, say, well, we're only going to do this for one government, they immediately lose access to the markets of the other ones. So that doesn't work, and that's not a position companies want to be in.

However, even if they could do this, there are already policies in place for them to do that. If Facebook gets a notification that says this is a terrorist thing, they take it down. It's not like this is a particularly difficult or burdensome review when it comes to violence.

The distinction is the government is trying to say, now we want them to start cracking down on radical speech. Should private companies be who we as society are reliant upon to bound the limits of public conversations? And this goes beyond borders now. I think that's an extraordinarily dangerous precedent to be embracing, and, in turn, irresponsible for American leaders to be championing.

The real solutions here are much more likely to be in terms of entirely new institutions that bound the way law enforcement works, moving us away from the point of military conflict, secret conflict, and into simply public policing.

There's no reason why we could not have an international counter-terrorism force that actually has universal jurisdiction. I mean universal in terms of fact, as opposed to actual law.

1. Yonhap News Agency

Samsung likely to countersue Huawei in U.S. in July: watchers

Friday, 27 May 2016

Byline: Staff reporter

Seoul - South Korean top tech giant Samsung Electronics Co. is likely to file a countersuit against Huawei Technologies Co. with a U.S. court in July, industry watchers here said Friday, after the Chinese company launched lawsuits claiming Samsung's infringement of its patents.

Earlier this week, Huawei brought two suits against the world's top smartphone maker with a U.S. federal court in California and the Chinese city of Shenzhen, seeking financial compensation for the alleged unlicensed use of 4G technology.

Industry watchers forecast that Samsung will take the counteraction sometime as early as July, since it usually takes at least two months to review a complaint in patent infringement battles.

"A Samsung- Huawei suit is likely to proceed slowly as the two sides are likely to pursue negotiations outside of the court after judging several circumstances," an industry watcher said.

Huawei, the world's third-largest smartphone maker, claimed Samsung and its affiliates gained huge profits by using the firm's technology without its permission.

Industry watchers further forecast that this will take a different course than an earlier patent battle between Samsung and its U.S. rival Apple Inc.

Samsung filed a countersuit against Apple in April 21, 2011, just four days after Apple first launched a patent infringement suit with the U.S. federal court of the Northern District of California. Soon, Samsung filed multiple suits in different countries, including South Korea, Japan and Germany.

"It will be very different from a Samsung-Apple suit, which was very spectacle," the watcher said.

Experts further forecast that there is very slim chance that Samsung may take legal action here or in other countries since more than half of Huawei phones are sold in the Chinese market.

The latest lawsuit highlights the rise of Asian competitors as technology creators and possible patent wars between tech firms.

Samsung sold 81.18 million smartphone units around the globe in the first quarter of this year, taking up 23.2 percent of the total, followed by Apple with 14.8 percent and Huawei with 8.3 percent.

2. Yonhap News Agency

Kim Jong-un orders users of Chinese cell phones to be punished: source

Friday, 27 May 2016

Byline: Staff reporter

Seoul - North Korean leader Kim Jong-un has instructed North Koreans using Chinese mobile phones to be punished for treason in order to fend off defections and internal information leaks to the outside world, a Seoul- based news outlet specializing in North Korea reported Friday.

"Kim Jong-un recently issued an order to treat people using Chinese cell phones like betrayers who conspire with South Koreans," the Daily NK quoted its source in the communist country's North Hamkyong Province as saying.

Agents from the North's state security ministry are eavesdropping on mobile phone communications made in areas bordering China 24 hours a day by mobilizing wiretapping equipment, military trucks and motor bikes, the source said.

The atmosphere in the border area is very tense as the security authorities continuously threaten to execute those who communicate with South Korea via mobile phones, according to the source.

The North issued a similar order to thoroughly crack down on the use of Chinese cell phones in January 2014.

3. China Daily

'More cybersecurity awareness needed' as challenges grow

Friday, 27 May 2016

Byline: Li Yang

Chengdu - China must raise people's overall awareness of cybersecurity and strengthen research and development of core technology in the sector to better address mounting challenges, top Chinese network security experts said at a conference in Chengdu, Sichuan province, on Thursday.

The 13th China Cyberspace Security Annual Conference, hosted by the National Computer Network Emergency Response Technical Coordination Center of China, covered a range of cyberspace topics, including security threat intelligence, cybersecurity talent development, security vulnerabilities and mobile internet and data security.

About 900 people from institutes, the government and domestic and foreign enterprises attended the three-day event, which started on Tuesday.

According to the 2015 China Internet Network Security Report, which the center issued during the conference, the center received 126,916 reports on network security incidents from home and abroad last year, an increase of 126 percent from 2014.

The three main targets of cyberattacks in China are government departments, financial agencies and basic telecommunication enterprises, the report said. The most common network security concerns are webpage counterfeiting and security vulnerabilities, it added.

Huang Chengqing, director of the center, said that the security capabilities of the cloud platform and big data in China will face big challenges this year. Equipment involved in the Internet of Thing swill face more security threats, and network fraud and racketeering in China will become more rampant this year, Huang predicted.

In the past year, the security protection level of China's basic telecommunication network improved, and so did its domain name system's ability to resist server attacks, the report said.

"But China's industrial internet faces harsher security challenges, and the advanced persistent threat to China's important information system became more severe last year," said Wu Jianping, an academician in computer science at the Chinese Academy of Engineering.

According to the report, the security condition of China's public internet is generally stable, and the security of the main telecommunication operators has improved. But the number of personal information leaks rose, it said.

4. Edmonton Journal

'Digital swatting' may be behind worldwide school bomb threats, including one in Edmonton

Friday, 27 May 2016

Byline: Paige Parsons

Edmonton - A bomb threat called into an Edmonton high school Wednesday was one of many that triggered emergencies at schools across the world this week.

Two schools in Alberta and two in Saskatchewan were among those that received phone threats of explosives being present in school buildings, and police forces in Alberta are exploring the possibility of a link between the threats.

The Edmonton Police Service (EPS) and Red Deer RCMP are working together to investigate whether the threat originated from the same individual or group, EPS spokesman Scott Pattison said Thursday.

"The investigation is ongoing, though the practice of digital swatting, which is what is alleged to have happened (Wednesday), takes time and is sometimes difficult to source," Pattison said.

Swatting is the practice of falsely reporting a serious incident or crime, in hopes of triggering an emergency response, possibly by a heavily armed SWAT team, as they are called in the United States.

Students and staff at Edmonton's Jasper Place High School, 8950 163 St., were evacuated Wednesday morning, following a phone message around 9:55 a.m. An investigation by city police determined the school was safe and classes resumed around 12:30 p.m.

Hunting Hills High School in Red Deer was also evacuated following a phoned-in bomb threat Wednesday about 9:45 a.m., 10 minutes earlier than the call to Jasper Place High School.

A release from Red Deer Public Schools identified the call as a pre-recording similar to those made to other schools internationally, but Red Deer RCMP Cpl. Karyn Kay said the school staff member who took the call couldn't confirm the threat was indeed a recording. Kay said RCMP have not confirmed a link between the call to Hunting Hills and threats to other schools.

"The RCMP can't speculate or link these files without a level of proof, and at this time we don't have that proof," Kay said.

Two schools in Saskatchewan also received pre- recorded bomb threats Wednesday morning. Jack MacKenzie Elementary in Regina and Silverspring School in Saskatoon were both searched, but nothing unusual was found.

The Canadian Security Intelligence Service said Thursday it does not comment on specific investigations, but said it works with law enforcement across Canada on public safety matters when it is required.

The threats to Canadian schools are similar to dozens of recent threats made via robocalls to schools in the United States and the United Kingdom.

Asked about a connection between calls made to Canadian and American schools, the U.S. Federal Bureau of Investigation would only address incidents in the United States.

"We are aware of recent bomb threats at various schools in different states, and we remain in touch with our law enforcement partners to provide assistance if needed. As always, we encourage the public to remain vigilant and to promptly report suspicious activities which could represent a threat to public safety," FBI spokeswoman Carol Cratty said.

Since Monday, it's estimated that about 85 schools in the United States and the United Kingdom have taken precautionary measures as a result of receiving recorded threats. The majority of the evacuations took place in the United States, with schools being evacuated in Colorado, Utah, Delaware, Minnesota, New Hampshire and Wisconsin. British media outlets also reported evacuations across the United Kingdom early this week.

Threats were made against American elementary, middle and high schools, with some schools choosing to continue classes and others to put buildings on lockdown rather than evacuate. Some schools resumed classes after sweeps by authorities failed to turn up explosives or other threats.

Some American officials described the threats as automated or robotic and at least two -- at Lakewood High School outside Denver and at Ben Franklin Elementary School in Rochester, Minn. -- came in just

before noon local time. Also in Minnesota, Forest Lake Elementary in the city of Forest Lake was evacuated after getting a bomb-threat call around 12:15 p.m.

With files from the Associated Press and Regina Leader-Post

5. Timaru Herald

GCSB to lose $6M

Friday, 27 May 2016

Wellington - The Government Communications Security Bureau's budget has been cut by $6.3m, down from $143.5m in 2015/16 to $137.2m in 2016/17. However, the spy agency is in line for a significant boost the following year, to $152.9m - though how the money will be spent remains a mystery. Budget papers setting out the estimates for Vote Communications Security and Intelligence do not provide any details of the GCSB's spending plans. (Full Report)

6. The Intercept

Secret Text in Senate Bill Would Give FBI Warrantless Access to Email Records

Friday, 27 May 2016

Byline: Jenna McLaughlin

Washington - A provision snuck into the still-secret text of the Senate's annual intelligence authorization would give the FBI the ability to demand individuals' email data and possibly web-surfing history from their service providers without a warrant and in complete secrecy.

If passed, the change would expand the reach of the FBI's already highly controversial national security letters. The FBI is currently allowed to get certain types of information with NSLs -- most commonly, information about the name, address, and call data associated with a phone number or details about a bank account.

Since a 2008 Justice Department legal opinion, the FBI has not been allowed to use NSLs to demand "electronic communication transactional records," such as email subject lines and other metadata, or URLs visited.

The spy bill passed the Senate Intelligence Committee on Tuesday, with the provision in it. The lone no vote came from Sen. Ron Wyden, D-Ore., who wrote in a statement that one of the bill's provisions "would allow any FBI field office to demand email records without a court order, a major expansion of federal surveillance powers."

Wyden did not disclose exactly what the provision would allow, but his spokesperson suggested it might go beyond email records to things like web-surfing histories and other information about online behavior. "Senator Wyden is concerned it could be read that way," Keith Chu said.

It's unclear how or when the provision was added, although Sens. Richard Burr, R-N.C., -- the committee's chairman -- and Tom Cotton, R-Ark., have both offered bills in the past that would address what the FBI calls a gap and privacy advocates consider a serious threat to civil liberties.

"At this point, it should go without saying that the information the FBI wants to include in the statue is extremely revealing -- URLs, for example, may reveal the content of a website that users have visited, their location, and so on," Andrew Crocker, staff attorney for the Electronic Frontier Foundation, wrote in an email to The Intercept.

"And it's particularly sneaky because this bill is debated behind closed doors," Robyn Greene, policy counsel at the Open Technology Institute, said in an interview.

In February, FBI Director James Comey testified during a Senate Intelligence Committee hearing on worldwide threats that the FBI's inability to get email records with NSLs was a "typo" -- and that fixing it was one of the FBI's top legislative priorities.

Greene warned at the time: "Unless we push back against Comey now, before you know it, the long slow push for an [electronic communication transactional records] fix may just be unstoppable."

The FBI used to think that it was, in fact, allowed to get email records with NSLs, and did so routinely until the Justice Department under George W. Bush told the bureau that it had interpreted its powers overly broadly.

Ever since, the FBI has tried to get that power and has been rejected, including during negotiations over the USA Freedom Act.

The FBI's power to issue NSLs is actually derived from the Electronic Communications Privacy Act -- a 1986 law that Congress is currently working to update to incorporate more protections for electronic communications -- not fewer. The House unanimously passed the Email Privacy Act in late April, while the Senate is due to vote on its version this week.

Sen. John Cornyn, R-Texas, is expected to offer an amendment that would mirror the provision in the intelligence bill.

Privacy advocates warn that adding it to the broadly supported reform effort would backfire.

"If [the provision] is added to ECPA, it'll kill the bill," Gabe Rottman, deputy director of the Center for Democracy and Technology's freedom, security, and technology project, wrote in an email to The Intercept. "If it passes independently, it'll create a gaping loophole. Either way, it's a big problem and a massive expansion of government surveillance authority."

NSLs have a particularly controversial history. In 2008, Justice Department Inspector General Glenn Fine blasted the FBI for using NSLs supported by weak evidence and documentation to collect information on Americans, some of which "implicated the target's First Amendment rights."

"NSLs have a sordid history. They've been abused in a number of ways, including ... targeting of journalists and ... use to collect an essentially unbounded amount of information," Crocker wrote.

One thing that makes them particularly easy to abuse is that recipients of NSLs are subject to a gag order that forbids them from revealing the letters' existence to anyone, much less the public.

7. USA Today

ACLU joins privacy fight against feds

Friday, 27 May 2016

Byline: Marco della Cava

Washington - Microsoft got an ally in its lawsuit against the Justice Department on Thursday.

The American Civil Liberties Union has filed a motion to join Microsoft's effort to challenge Justice Department gag orders that prevent the tech company from telling customers when the government has ordered it to turn over data.

The ACLU is a Microsoft customer. Microsoft filed its lawsuit in April, one of a number of legal challenges the Redmond, Wash., company has mounted against growing law enforcement requests for its cloud-based consumer data.

"A basic promise of our Constitution is that the government must notify you at some point when it searches or seizes your private information," said Alex Abdo, a senior staff attorney with the ACLU Speech, Privacy and Technology Project. "Notice serves as a crucial check on executive power, and it has been a regular and constitutionally required feature of searches and seizures since the nation's founding."

Microsoft spokesman David Cuddy said the company "appreciates the support from the ACLU and many others in the business, legal and policy communities who are concerned about secrecy becoming the norm rather than the exception."

Requests from law enforcement agencies for access to users' personal information routinely flood tech companies that store vast amounts of data in the cloud. Massive data centers run by Microsoft, Amazon and other big tech companies allow businesses and individuals to access email, photos and other content from multiple devices, wherever they are.

Law enforcement officials say that access to such data is critical to fighting crime and terrorism.

Using the Electronic Communications Privacy Act, the U.S. government is increasingly targeting such data, according to Microsoft, which says the government has mandated secrecy in 2,576 instances over the past 18 months. People would know if the government went through their filing cabinet or their hard drive but are unaware when their privacy in the cloud is intruded upon, they argue.

The 1986 law was written before the Web was born and long before Americans started storing so much of their personal communications on the Internet.

Microsoft alleges the Electronic Communications Privacy Act violates users' Fourth Amendment right that a search be reasonable and Microsoft's First Amendment right to talk to its users.

"Notably and even surprisingly, 1,752 of these secrecy orders, or 68% of the total, contained no fixed end date at all. This means that we effectively are prohibited forever from telling our customers that the government has obtained their data," Microsoft chief legal officer Brad Smith wrote in an April blog post when the suit was announced.

8. Pajhwok Afghan News

Pentagon does not rule out hitting new Taliban leader

Friday, 27 May 2016

Byline: Lalit K Jha

Washington - Not ruling out the possibility of targeting the new Taliban leader if needed, the Pentagon Thursday hoped that the new leadership would pursue a path of peaceful resolution with the Afghan Government.

"Right now, as you know, we carried out a strike against a Taliban leader who had plotted against the United States forces and had led a group that carried out attacks against U.S. forces. And we will continue to do whatever we need to do to protect our forces," the Pentagon Press Secretary, Peter Cook, told reporters at a news conference.

He was being asked of the Pentagon trying to kill the new Taliban leader, who was appointed this week after its last leader Mullah Mansour was killed in an US air strike on Saturday.

The responsible thing for the Taliban leadership to do at this point would be to pursue a pathway to a peaceful resolution with the unity government in Afghanistan, Cook said in response to a question.

"That would be the responsible thing to do, because the Afghan forces with the support of the United States, our partners there, are going to continue to improve and show more skills and capabilities," he said.

"And they're going to continue to be able to work towards ultimately securing the country on their own. That's the ultimate goal here. They're going to have our support in the process. So the wise thing for the

Taliban leadership to do would be to factor that into their decision-making and choose a different path. We will wait to see what they do," Cook said.

In the meantime, the United States is going to do everything we can to support the Afghan forces, to continue to bolster those forces, to make them more capable, more able to defend themselves, to defend the country.

"We've talked about the aviation assets that are now coming online; the training that continues for Afghan forces. This is a difficult situation and this does present an opportunity for the Taliban to chart a new path should they choose to do so. Well wait to see if they do the responsible thing," Cook said.

9. New York Times

Hillary Clinton Addresses Email Questions Again

Friday, 27 May 2016

Byline: Thomas Kaplan, Amy Chozick

Las Vegas - Unable to shake what has become a lingering distraction for her campaign, Hillary Clinton on Thursday played down a report from the State Department's inspector general that criticized her use of a private email server while she was secretary of state.

In an interview with ABC News, Mrs. Clinton repeated her concession that using the private email server was a mistake. But she suggested that voters had more important issues to consider when making up their minds between her and the presumptive Republican presidential nominee, Donald J. Trump.

"As I've said many times, if I could go back, I would do it differently," Mrs. Clinton said. "I know people have concerns about this. I understand that. But I think voters are going to be looking at the full picture of what I have to offer, my life and my service, and the full threat that Donald Trump offers our country."

The inspector general's report presented to Congress on Wednesday said that Mrs. Clinton had not sought or received permission to use the private email server. The report also said that, through her lawyers, Mrs. Clinton declined to be interviewed by the inspector general.

The report gave new ammunition to Mr. Trump and threatened to bolster the perception already held by a majority of voters, according to polling, that Mrs. Clinton is not trustworthy.

In the interview, Mrs. Clinton gave little ground over the email issue, asserting that the report "makes clear that personal email use was the practice for other secretaries of state."

Asked if using private email was an error of judgment, she responded: "Well, it was allowed. And the rules have been clarified since I left about the practice."

She added, "Having said that, I have said many times, it was a mistake."

Mrs. Clinton reiterated that argument in a phone interview with CNN on Thursday afternoon. "I thought it was allowed," she told Wolf Blitzer. Asked why she declined to be interviewed for the review, Mrs. Clinton said, "I'd already said everything I could on this matter."

In both interviews, she cited her 11-hour testimony to a House committee investigating the Sept. 11, 2012, attack on the United States mission in Benghazi, Libya, when extensive questions about her private email use came up. But unlike the Benghazi committee, an effort led by congressional Republicans, the State Department report was not partisan, a detail not lost on Mr. Trump.

"This is not a Republican group or a conservative group," he said in an interview on Wednesday. "This is a group that is much more to her liking."

Mr. Trump repeated his criticism of Mrs. Clinton at a news conference on Thursday, while Mrs. Clinton used her interviews to call her likely Republican rival "an unqualified loose cannon."

"President Obama came out of meetings with our closest allies in the world and reported that they are quote 'rattled' by the threat Donald Trump represents," Mrs. Clinton said on CNN.

The interviews came as Mrs. Clinton spoke here on Thursday at a conference for the United Food and Commercial Workers International Union, which endorsed her in January. Later in the afternoon, she returned to California to hold a pair of rallies ahead of the California primary on June 7. After Mrs. Clinton previously led by double digits, a poll released Wednesday night showed her in a tight race with Senator Bernie Sanders.

"I really don't pay a lot of attention to polls because they are usually, and increasingly, all over the place," Mrs. Clinton said on CNN when asked about the tightening race in California. "We are already insurmountably ahead" in the race for the 2,383 delegates needed to clinch the nomination, she added.

10. Washington Times

Government still holding on to 5 years of NSA phone-snooping metadata

Friday, 27 May 2016

Byline: Stephen Dinan

Washington - The National Security Agency's phone-snooping program ended six months ago this Saturday, but the government is still holding on to the mountain of data it piled up over the previous five years, worrying civil liberties advocates who say it's time to start expunging the legally questionable information.

Government officials say they no longer access the information, but the intelligence community's past behavior has some civil libertarians skeptical of those assurances. And the mere existence of the data,

which includes the time, duration and numbers involved in phone calls, worries critics who say there's no reason for it to be sitting under government control.

The intelligence community, though, says its hands are tied -- chiefly by the very same advocates who are demanding that most of the data be expunged.

Some of those groups are helping pursue lawsuits seeking damages from the government's snooping program, and courts have ordered all of the data to be preserved. That means the NSA can't purge the information, even though it says it wants to.

"We take seriously the public's concerns about the government's retention of bulk telephony metadata collected under the now-terminated bulk metadata program," said Timothy Barrett, spokesman for the Office of the Director of National Intelligence. "Retention of this data is necessary to comply with preservation obligations in civil litigation challenging that program, including court orders entered in two of those cases."

The phone records program began under President George W. Bush and was kept in place by President Obama, based on powers claimed under the Patriot Act's "business records" provision. The NSA demanded that phone companies turn over their records of calls, which were then stored in government databanks for five years.

Analysts queried the data when they had a number they believed associated with terrorism, and could pursue up to three "hops," meaning they could see check numbers associated with the initial lead, all the numbers associated with that set and then all the numbers associated with the second set.

Former government contractor Edward Snowden revealed the program's existence in 2013, spawning a massive public backlash that forced Congress to curtail the program. Lawmakers passed the USA Freedom Act last year, giving the NSA 180 days to shut down its own database and instead rely on private companies to keep the data, which the government could query under more strict circumstances.

The program expired on Nov. 28, and the government was to dispose of its data.

But the administration got an order from the Foreign Intelligence Surveillance Court allowing it to preserve all of the data, arguing that the government needs it to fight the 10 court cases challenging the defunct program.

The Electronic Frontier Foundation, which is assisting the plaintiffs in several of the key cases, said the government should find a way to get rid of most of the data.

"Talks are continuing about a plan under which the government would destroy the phone records -- including those still lingering in its various databases -- while ensuring that the courts can still consider our challenge to 14 years of NSA telephone records collection from millions of innocent Americans," said EFF Civil Liberties Director David Greene.

But government attorneys say it's impossible to cull the data to just the 10 ongoing cases. Indeed, the attorneys won't even acknowledge what records they have or which phone carriers they have targeted -- creating a legal morass.

The government is not holding on to only the metadata, but it also still has everything it derived from the data -- the information it turned up in the "hops" when it investigated suspects' phone numbers.

Mr. Barrett, the intelligence office spokesman, said they plan to expunge the query data once they are free to get rid of the metadata itself, with "narrow exceptions" laid out in a November order from the secret court.

The court order suggests those exceptions could be broad. The court said the government can retain "information derived from the metadata that has been previously disseminated," as well as "select query results generated that formed the basis of such disseminations."

Patrick C. Toomey, a staff attorney at the American Civil Liberties Union, said limits must be imposed.

"The government should purge the call records it collected illegally, including the results of its queries, and should retain only the data necessary to comply with its legal obligations," he said.

But he said that's not enough. "The NSA continues to search and store Americans' private information in vast quantities under other spying programs, all without ever obtaining a warrant," he said.

Not all of those challenging the NSA want the data expunged.

Larry Klayman, a conservative lawyer who won his case against the NSA in federal district court in Washington, says the data are needed so he can win a massive settlement from the administration.

"We basically want to show what it is that they have control over, and have had access to, to make our claim to damages," he said.

Mr. Klayman also doesn't trust the NSA to expunge the data even if it's ordered to.

"To me it's irrelevant, any kind of agreement you reach with them," he said. "I want them to preserve all of it because I know even if they say they're purging it, they're not going to."

He said the only acceptable solution is to have the federal judge in his case, Judge Richard J. Leon, oversee the NSA's activities going forward.

11. New York Times

Clinton Wasn't Adept at Using a Computer for Email, an Inquiry Is Told

Friday, 27 May 2016

Byline: Eric Lichtblau, Steven Lee Myers

Washington - Hillary Clinton and her advisers have offered a series of explanations over the last year for her decision to use a private email server as secretary of state, a decision that she said again on Thursday had been "a mistake."

She did not want the inconvenience of carrying two phones, Mrs. Clinton said initially. She did not want a government account that might pull in nonwork matters, she said later. Or perhaps, an adviser has said, she simply did not want Republican lawmakers rifling through her personal emails.

Yet another explanation emerged Thursday: She was not comfortable with using a computer to read email.

Lewis A. Lukens, a former State Department administrative official, said in a sworn deposition last week that after Mrs. Clinton became secretary of state in 2009, he had proposed accommodating her by setting up a desktop computer in her office that would not be connected to the department's system. That would have allowed her to send and receive email on a personal account, Mr. Lukens said in the deposition, which he gave as part of a lawsuit brought by Judicial Watch, a conservative legal advocacy group. The group released a transcript of the deposition on Thursday.

But that idea was abandoned, Mr. Lukens testified, after an aide to the secretary told him that Mrs. Clinton was "very comfortable checking her emails on a BlackBerry, but she's not adept or not used to checking her emails on a desktop."

His explanation will not be the last word. Nor will a highly critical report that came out Wednesday from the State Department's inspector general, which challenged many of the explanations Mrs. Clinton and her supporters have offered over the past year.

While the report said that Mrs. Clinton had never been authorized to set up a private email server and that her decision to use one had compromised security at the department she ran, it left a number of questions unanswered. One was why she had decided to use her own server, and ultimately risk damage to her political career, in the first place.

And it raised new questions, including why Mrs. Clinton had declined to speak with the investigators who prepared the report.

Asked about that decision in an interview with ABC News on Thursday, Mrs. Clinton said only that she had already testified for 11 hours before the select House committee investigating the attacks in Benghazi, Libya, in 2012, and that she had offered repeatedly to speak with the F.B.I.

"I have talked about this for many, many months," she said.

She sounded exasperated by her inability to move past the controversy and defended her actions as common practice at the State Department, even as she again acknowledged that the private server had been a mistake.

"As I've said many times, if I could go back, I would do it differently," she said. "I know people have concerns about this. I understand that, but I think voters are going to be looking at the full picture of what I have to offer, my life and my service."

Mrs. Clinton said once again that the arrangement had been "allowed" at the time, though the inspector general's report said that she had not sought permission and that it would not have been granted because of security concerns.

She also said that her use of a nonofficial email address had been "widely known," though the report said the extent of her use had not been known beyond a small number of officials who were privy to her private accounts.

At the State Department on Thursday, a spokesman, Mark C. Toner, faced repeated questions about why the department had not done more to ensure that Mrs. Clinton's email arrangement complied with department rules and federal laws. "There was only a partial understanding of how much Secretary Clinton relied on personal email, and we just did not have a complete picture," he said.

According to the inspector general's report, two records information officials in the department raised concerns as early as 2010 that emails sent and received on Mrs. Clinton's server might contain information that should be preserved under federal law.

Their superior told them that the arrangement had been reviewed and approved, though the inspector general found "no evidence" that this had happened. The supervisor told them their job was to support the secretary and "instructed the staff never to speak of the secretary's personal email system again."

The report did not name the supervisor, but several people with knowledge of the episode identified him as John Bentel, the former director of information resource management in the State Department's Executive Secretariat office. Randall J. Turk, a lawyer for Mr. Bentel, declined to comment Thursday.

Senator Charles E. Grassley, the Iowa Republican who is chairman of the Senate Judiciary Committee, mentioned Mr. Bentel's role in remarks Thursday on the Senate floor, and complained that Mr. Bentel had refused a request to speak with the committee.

"Good and honest employees just trying to do their job were told to shut up and sit down," Mr. Grassley said. "Concerns about the secretary's email system being out of compliance with federal record-keeping laws were swept under the rug."

He also said Mr. Bentel had warned Mrs. Clinton that any emails that passed through the State Department's systems would be subject to disclosure under the Freedom of Information Act.

For Mrs. Clinton, the biggest obstacle to getting past the email controversy is the F.B.I., which has not yet completed its criminal investigation to determine whether any laws were broken in the handling of classified material or other matters relating to the emails. Mrs. Clinton is expected to be interviewed as part of the investigation, but it is not clear when that will happen.

The investigation could drag past the Democratic National Convention this summer and what is expected to be the kickoff to Mrs. Clinton's general-election campaign against Donald J. Trump. In the meantime, depositions will continue in the Judicial Watch suit. Cheryl D. Mills, a longtime confidante of Mrs. Clinton who was her counselor at the State Department, is scheduled to testify on Friday, and at least a half-dozen other former officials are scheduled to follow.

12. Tech Insider

America shut down the original NSA because 'gentlemen do not read each other's mail'

Friday, 27 May 2016

Byline: Paul Szoldra

Baltimore - The precursor to the National Security Agency was shut down because the Secretary of State at the time believed that "gentlemen do not read each other's mail."

It's an interesting anecdote we were reminded of during a visit to the NSA's public museum in Maryland, where it has an exhibit on the so-called "Black Chamber" founded in 1919 by Herbert O. Yardley.

Officially known as The Cipher Bureau, it was America's first peacetime organization dedicated to code breaking. Located in New York City and disguised behind a public-facing commercial code company, its existence was a highly-secret affair that was jointly funded by the State Department and the US Army.

Throughout the 1920's, the bureau cracked thousands of diplomatic messages. Most notably, it intercepted and deciphered the communications of Great Britain and Japan during the Washington Naval Conference in 1921.

"Yardley's team had a major success when it broke the Japanese diplomatic code and learned of the Japanese government's instructions to its ambassadors," an Army historical feature notes. "Naturally, knowing the lowest naval ratio the Japanese were willing to accept put the US in a powerful negotiating position."

But the peace throughout the 1920's meant there was less to intercept, and its budget was continually reduced. Then its time came to a close soon after President Herbert Hoover came into office. Initially, Yardley didn't let new Secretary of State Henry Stimson know about his code-making chamber for a few months.

As James Bamford wrote in "The Puzzle Palace":

Then in May, after Yardley had deciphered a new group of Japanese messages, he decided the time had come to share the dark secret with the man who was paying the bills, and a few selected translations were laid on the Secretary's desk.

Stimson's reaction was immediate and violent. Branding the Black Chamber highly illegal, he at once directed that all its State Department funds be cut off. Since the Chamber was now getting almost its entire support from the State Department, that mean instant doom.

Dealing with ambassadors from friendly nations, Stimson saw interception of those communications as quite disrespectful. "Gentlemen do not read each other's mail," he wrote in his memoirs.

That attitude didn't hold for long, of course. The codebreaking was back in full swing during World War II and beyond, and even at present, the NSA targets friendly and foe embassies alike. The confirmation of that fact set off a firestorm of criticism from allies after it was revealed by ex-NSA contractor Edward Snowden.

Still, it was Yardley who had the last laugh.

Out of a job in the midst of the Great Depression, Yardley wrote a tell-all memoir of his time secretly breaking codes, called "The American Black Chamber." The NSA's museum described its being published because of a "loophole" in the law, but in reality, there was absolutely no legal precedent to stop the book from coming out.

Though the US government certainly tried. As Bamford notes, it considered prosecution or outright suppression of the book, but ultimately these avenues were rejected since there was no legal standing to go on.

It was published in 1931. A law that closed the "loophole" and prevented any further secrets from being revealed was passed two years later.

13. The Guardian (London)

Bill would expand FBI's warrantless access to online records, senators warn

Friday, 27 May 2016

Byline: Spencer Ackerman

New York - Two US senators have warned that a new bill would vastly expand the FBI's warrantless access to Americans' online records.

Although the text of the 2017 intelligence authorization bill is not yet available to the public, two members of the Senate intelligence committee have said the bill could expand the remit of a nonjudicial subpoena called a National Security Letter (NSLs) to acquire Americans' email records, chat or messaging accounts, account login records, browser histories and social- media service usage.

While NSLs typically apply to phone or banking records and email addresses, the bill, which cleared the Senate intelligence panel on Tuesday by a 14-1 vote, appears to change the scope of the longstanding term "electronic communications transaction records".

Senator Ron Wyden criticized the change as a sweeping expansion of warrantless surveillance.

"While this bill does not clearly define 'electronic communication transaction records', this term could easily be read to encompass records of whom individuals exchange emails with and when, as well as their login history, IP addresses, and internet browsing history," Wyden, a Democrat from Oregon who voted against the bill, told the Guardian.

Wyden's colleague on the panel, Democrat Martin Heinrich of New Mexico, said in a Thursday statement that the measure represents "a massive expansion of government surveillance that lacks independent oversight and potentially gives the FBI access to Americans' email and browser histories with little more than the approval of a manager in the field".

Heinrich voted for the bill because of its other provisions. His office said he would seek to remove the NSL expansion when it comes to the Senate floor.

"The FBI has not made a convincing case that it needs any process other than the one that already exists, especially one that freely allows the FBI access to law-abiding Americans' emails and web activity," Henrich said.

Obscure before the 9/11 attacks, the FBI has come to rely significantly on NSLs, which come exclusively from the executive branch, and not with a judge's approval. They are served not to the targets of investigation but to communications providers or banks, and come with gag orders preventing the recipient from disclosing anything about them.

A 2014 panel advising Barack Obama on surveillance found the FBI typically issues an average of 60 NSLs each day, or 21,900 annually, up from 8,500 in 2000. The office of the director of national intelligence and the justice department recently reported that the FBI issued 12,870 NSLs in 2015, representing 48,642 warrantless requests for information.

Last year, a recipient of an NSL won a decade-long fight to disclose aspects of the subpoena his web-hosting company received. The NSL served to Nicholas Merrill in 2004 included demands for cellular location information and "any other information which you consider to be an electronic communication transactional record" - an indication that the phraseology in the fiscal 2017 intelligence bill has direct NSL precedent.

In Senate testimony earlier this year, FBI Director James Comey said that a "typo" in a 1993 statute concerning electronic communications transaction records was leading "some companies" to resist providing the FBI with "ordinary transaction records that we can get in most contexts with a non-court order". He called a legislative fix a high legislative priority for the bureau.

A statement released by the Senate panel's leadership, Republican Richard Burr of North Carolina and Democrat Dianne Feinstein of California, after the bill passed the committee on Tuesday did not include information on the bill's changes to the NSL scope.

Burr spokeswoman Rebecca Watkins indicated a public version bill would be released as early as next week.

"Committee members have three working days to submit supplemental, minority, or additional views to the committee. The resulting report will be made public after member comments are compiled, as has been consistently the process for the Senate intelligence committee," Watkins told the Guardian.

14. New York Times

North Korea Linked to Digital Attacks on Global Banks

Friday, 27 May 2016

Byline: Nicole Perlroth, Michael Corkery

San Francisco - Security researchers have tied the recent spate of digital breaches on Asian banks to North Korea, in what they say appears to be the first known case of a nation using digital attacks for financial gain.

In three recent attacks on banks, researchers working for the digital security firm Symantec said, the thieves deployed a rare piece of code that had been seen in only two previous cases: the hacking attack at Sony Pictures in December 2014 and attacks on banks and media companies in South Korea in 2013. Government officials in the United States and South Korea have blamed those attacks on North Korea, though they have not provided independent verification.

On Thursday, the Symantec researchers said they had uncovered evidence linking an attack at a bank in the Philippines last October with attacks on Tien Phong Bank in Vietnam in December and one in February on the central bank of Bangladesh that resulted in the theft of more than $81 million.

"If you believe North Korea was behind those attacks, then the bank attacks were also the work of North Korea," said Eric Chien, a security researcher at Symantec, who found that identical code was used across all three attacks.

"We've never seen an attack where a nation- state has gone in and stolen money," Mr. Chien added. "This is a first."

The attacks have raised alarms in the global banking industry because the thieves gained access to Swift, a Brussels-based banking consortium that runs what is considered the world's most secure payment messaging system. Swift's system is used by 11,000 banks and companies to move money from one country to another -- one reason that it is a tempting target for criminals.

Swift has warned publicly that the attacks are part of a broad coordinated assault on banks, though it has not assigned blame. It has also emphasized that it was the banks' connection points to its network -- and not the core Swift messaging network itself -- that the attackers were able to breach. Also,

American bankers have noted that the security lapses all occurred at banks in third-world countries, which may give some comfort to banking customers in the United States.

Security researchers and American government officials have tied thousands of attacks to nations in the past. They have linked the United States and Israel to an attack that destroyed Iranian centrifuges, and the Chinese military and contractors to attacks that stole military and trade secrets from thousands of foreign entities.

But the latest spate of attacks on banks in Bangladesh and Southeast Asia would be the first time, security researchers say, that a nation has used malicious code to steal purely for financial profit.

The idea that Pyongyang had turned to digital theft would not be surprising. North Korea's economy has been ravaged by sanctions, food shortages and other deprivations. Pyongyang does not publish economic data, but estimates have put North Korea's gross domestic product between $12 billion and $40 billion, tiny when compared with South Korea's economic output of more than $1.4 trillion.

In the attack at Bangladesh's central bank in February, the thieves tried to transfer $1 billion in funds from an account at the Federal Reserve Bank of New York. Fed officials became suspicious of the some of requested transfers and released only $81 million to accounts in the Philippines.

"If you presume it's North Korea, $1 billion is almost 10 percent of their G.D.P.," Mr. Chien said. "This is not small change for them."

Symantec researchers said it was possible that the bank in the Philippines containing the North Korean code was also involved in the Bangladesh bank scheme and the attempted breach on the Vietnamese bank. The researchers would not identify the Philippines bank and did not say whether the thieves had been successful in transferring funds. Researchers were able to confirm only that the attackers had managed to breach the bank and install identical code strings on the bank's computer systems -- the same code that they discovered in Bangladesh, Vietnam and the two previous attacks at Sony in 2014 and South Korea in 2013.

Mr. Chien noted that the attackers not only used identical numbers but wrote the code in the same, unusual sequence across all three attacks.

Mr. Chien said the evidence pointed to all three attacks being the work of the "Lazarus Group," a name his team gave to the attackers behind the Sony and South Korean attacks.

Officials have pointed to North Korea's threat of "merciless countermeasures" against Sony if the studio released "The Interview," a movie by Seth Rogen and Evan Goldberg that made fun of North Korea and includes a fictional assassination of its leader. F.B.I. analysts also note critical mistakes North Korean hackers made, such as logging into their attack servers from known North Korean Internet addresses and even logging into both their Facebook account and Sony's servers from the same computers.

In the months since evidence of the attacks involving the Swift network started to emerge, investigators have been looking for commonalities at numerous other potential breaches. It remains unclear whether

these breaches are connected to the ones in Bangladesh and Vietnam, but they too have occurred in or around Southeast Asia.

There is no evidence to date that the thieves have gone after large American or European banks, though new possible attacks are being reported weekly. Last week, evidence emerged that Banco del Austro, an Ecuadorean bank, was infiltrated by hackers who were also able to sneak onto the Swift network. The thieves transferred several million dollars to accounts around the world, according to a lawsuit the bank filed in federal court in the United States against Wells Fargo, which facilitated one of the transfers.

Researchers have yet to unearth any of the code used in the Ecuador attack, but banking analysts say it is probably no coincidence that these attacks are happening in the developing world, where security measures tend not to be as tight as they are in financial hubs like New York and London.

Swift has issued numerous warnings in recent weeks urging banks to step up their security protocols. Analysts worry that the breaches could have a chilling effect on global finance; larger banks may become reluctant or even refuse to transact with smaller banks in the developing world unless they can have assurances that their networks have not been compromised by thieves and malware.

At a conference on Tuesday in Brussels, Swift's chief executive, Gottfried Leibbrandt, said the recent attacks could do far more damage than breaches on retailers and telephone companies, which he said suffer largely reputational and legal hits.

"Banks that are compromised like this can be put out of business," Mr. Leibbrandt said.

North Korea has long been known for creative attempts to generate badly needed hard currency. In the last decade, United States government officials accused North Korea of counterfeiting $100 bills, which were known as "superdollars" or "supernotes" because the fakes were nearly flawless. The Federal Reserve began thwarting that effort by circulating a new $100 bill over the last three years that makes counterfeiting nearly impossible: The redesigned $100 is easier to authenticate and harder to replicate.

"North Korea is hurting for money," said Herb Lin, the senior research scholar for cyberpolicy and security at Stanford University's Center for International Security and Cooperation and a fellow at Stanford's Hoover Institution. "They've been cut out of the financial system because of sanctions. They had been among the best counterfeiters in the world, and only recently have they been stymied in the counterfeiting of superdollars. If it's true that we've cut them off from that, then it's not at all surprising that they would turn to something else."

15. Reuters

Push for encryption law falters despite Apple case spotlight

Friday, 27 May 2016

Byline: Multiple reporters

Washington - After a rampage that left 14 people dead in San Bernardino, key U.S. lawmakers pledged to seek a law requiring technology companies to give law enforcement agencies a "back door" to encrypted communications and electronic devices, such as the iPhone used by one of the shooters.

Now, only months later, much of the support is gone, and the push for legislation dead, according to sources in congressional offices, the administration and the tech sector.

Draft legislation that Senators Richard Burr and Dianne Feinstein, the Republican and Democratic leaders of the Intelligence Committee, had circulated weeks ago likely will not be introduced this year and, even if it were, would stand no chance of advancing, the sources said.

Key among the problems was the lack of White House support for legislation in spite of a high-profile court showdown between the Justice Department and Apple Inc over the suspect iPhone, according to Congressional and Obama Administration officials and outside observers.

"They've dropped anchor and taken down the sail," former NSA and CIA director Michael Hayden said.

For years, the Justice Department lobbied unsuccessfully for a way to unmask suspects who "go dark," or evade detection through coded communications in locked devices.

When the Federal Bureau of Investigation took Apple to court in February to try to open the iPhone in its investigation of the San Bernardino slayings, the cause gained traction in Washington. The political landscape had shifted - or so it seemed.

The short life of the push for legislation illustrates the intractable nature of the debate over digital surveillance and encryption, which has been raging in one form or another since the 1990s.

Tech companies, backed by civil liberties groups, insist that building law enforcement access into phones and other devices would undermine security for everyone-including the U.S. government itself.

Law enforcement agencies maintain they need a way to monitor phone calls, emails and text messages, along with access to encrypted data. Polls show the public is split on whether the government should have access to all digital data.

The legal battle between the FBI and Apple briefly united many around the idea that Congress - not the courts - should decide the issue. But the consensus was fleeting.

Feinstein's Democratic colleagues on the Intelligence Committee - along with some key Republicans - backed away. The House never got on board.

The CIA and NSA were ambivalent, according to several current and former intelligence officials, in part because officials in the agencies feared any new law would interfere with their own encryption efforts.

Even supporters worried that if a bill were introduced but failed, it would give Apple and other tech companies another weapon to use in future court battles.

Burr had said repeatedly that legislation was imminent.

But last week, he and Feinstein told Reuters there was no timeline for the bill. Feinstein said she planned to talk to more tech stakeholders, and Burr said, "be patient."

In the meantime, tech companies have accelerated encryption efforts in the wake of the Apple case. The court showdown ended with a whimper when the FBI said it had found a way to get into the phone, and subsequently conceded privately it had found nothing of value.

THE FBI GOES TO BATTLE

A week after the San Bernardino attack, Burr told Reuters passing encryption legislation was urgent because "if we don't, we will be reading about terrorist attacks on a more frequent basis."

FBI Director James Comey told the Senate Intelligence Committee soon after that encryption was "overwhelmingly affecting" the investigation of murders, drug trafficking and child pornography.

A week later, the Justice Department persuaded a judge to issue a sweeping order demanding Apple write software to open an iPhone used by San Bernardino suspect Sayeed Farook, who died in a shootout with law enforcement.

Apple fought back, arguing, among other things, that only Congressional legislation could authorize what the court was demanding. Many saw the Justice Department's move as a way to bring pressure on Congress to act.

President Obama appeared to tacitly support Comey's court fight and the idea that there should be limits on criminal suspects' ability to hide behind encryption. But even as the drive for legislation seemed to be gaining momentum, consensus was dissipating.

Senator Lindsey Graham, an influential Republican, withdrew support in a sudden about-face.

"I was all with you until I actually started getting briefed by the people in the intel community," Graham told Attorney General Loretta Lynch during a hearing in March. "I'm a person that's been moved by the arguments of the precedent we set and the damage we may be doing to our own national security."

On the Democratic side, Senator Ron Wyden vowed to filibuster what he called a "dangerous proposal," that "would leave Americans more vulnerable to stalkers, identity thieves, foreign hackers and criminals."

Senator Mark Warner advanced a competing bill to form a commission to study the issue.

A half dozen people familiar with the White House deliberations said they were hamstrung by a long-standing split within the Obama Administration, pitting Comey and the DOJ against technology advisors and other agencies including the Commerce and State Departments.

They also said there was reluctance to take on the tech industry in an election year.

16. The Register (UK)

More than half of people on UK counter-terror biometrics databases are innocent

Thursday, 26 May 2016

Byline: Alexander J. Martin

London - A new report from the UK's independent biometrics commissioner has revealed that more than half of people on British counter- terrorism databases are innocent, more than a thousand more than previously thought.

The commissioner has revised upwards his figures on fingerprint and DNA profile retention, stating that 53 per cent of the 9,600 individuals on counter-terrorism databases have never been convicted of a crime, and not just 7,800 people as was previously thought.

The extent to which police in the UK have been exploiting counter-terrorism laws to keep innocent suspects' biometric details on file is now understood to be much greater, following the new report's publication at the Home Secretary's request.

Biometrics commissioner Alastair MacGregor QC's 20-page report, published today, provides an update to his annual report from 2015, revising some of the key figures. It reveals even more police misuse of National Security Determinations (NSDs) than previously raised in his 119-page report for 2015.

Today's report was rushed out (alongside many others) ahead of purdah* for the EU referendum.

Last year MacGregor reported that the police were holding onto the biometric data of 6,500 and 7,800 subjects of counter- terrorism investigations in 2013 and 2015 respectively, many of whom have never been charged with an offence. Those numbers, along with previous figures, have now been increased.

He wrote: "It now appears that those figures were incorrect and that the true figures as at 31 October 2013 and 31 October 2015 were 8,300 and 9,600 respectively."

4,500 - 53 per cent - of these records, which were being held on counter-terror databases, related to individuals who "had never been convicted of a recordable offence".

Despite the time limits on the retention of fingerprints and DNA profiles in the cases of uncharged suspects, as established by the Protection of Freedoms Act 2012, which also established the biometrics commissioner's role, chief police officers are, in exceptional circumstances, allowed to make a NSD to retain this material for longer. These decisions must be examined by the commissioner, however.

MacGregor reported that 217 applications for NSDs had been made by 31 October 2015, with 117 being approved internally by police and forwarded to him as biometrics commissioner. In turn, he approved just 73 of these requests because several were made outside the permitted time limits, while others had been approved by police officers too junior to legally do so.

He added: "At the date of my 2015 Report it was my understanding that it was possible that NSDs would have been applied for in about 45 of the cases that were at that time thought to have expired by 31 October 2015, it is now my understanding that applications for NSDs would undoubtedly have been made in at least 108 of the cases that had in fact expired by 31 March 2016 and that the actual figure might well have been appreciably larger."

This is the last report that MacGregor, the first person appointed to the role, will write as biometrics commissioner because his two-year term, which was extended until 31 May so he could complete his additional report, is all but over. No decision has yet been made on his replacement.

17. Pajhwok Afghan News

Afghan war may not escalate with Hibatullah succession: NATO

Friday, 27 May 2016

Byline: Navid Ahmad Barekzai

Kabul - NATO's Resolute Support Mission (RS) in Afghanistan on Thursday said it did not expect the war in Afghanistan would escalate with the election of Taliban's new leadership.

Brig. Gen. Charles Cleveland, RS spokesman, told a press conference here that Mullah Akhtar Mohammad Mansour was targeted because he was a direct threat to Afghan and coalition forces and he was against peace in the country.

Five days ago, Mansour was targeted by US drones while returning from Iran in the Balochistan province of Pakistan.

On the appointment of Mullah Hibatullah Akhunzada as Taliban's new supreme commander, Cleveland said "the Taliban leadership has two options which are to continue killing innocent people or to join the peace process."

However, he was optimistic about future, saying "it is expected that Mullah Hibat would choose the peace option."

Choosing peace could introduce the Taliban leader as a personality of peace and could also prevent his supporters from dying, he said.

Taliban should realize that they could not win the war and would face defeat, he declared.

The NATO official said the Afghan ground and air forces had improved during the past year and had many achievements.

By choosing offensive state, the Afghan forces could dismantle the plans of terrorists, he said, adding terrorists have been defeated once again in northern Afghanistan and now attention was being paid to southern provinces.

The Taliban have also no courage to fight face to face against Afghan security forces, he concluded.

18. Gulf News

Region lacks resources to fight hackers

Friday, 27 May 2016

Byline: Scott Shuey

Dubai - There may be a silver lining to the recent increase in cyber attacks in the Middle East, according to Wael Mohammad, the president and COO of digital security firm TrendMicro.

The obvious, although also worrisome, way to look at the recent attacks, such as the recent release of customers information following the hacking of Qatar National Bank, is that regional financial institutions are now viewed as both worth the effort and attention of potential hackers.

"I honest believe it's good news, because 10 years ago ... they used to use Middle Eastern sites as an examples of how they could penetrate and nobody was home. There was nothing to actually get," he said.

The fact that attacks are now taking place indicates a number of things for the Middle East, says Mohamed, who is based in Texas but was in Dubai on Wednesday.

"Number one is that there is something valuable to actually be taken, which means that digitalisation and online dependence is higher than it once was. That's important," he said.

However, the attacks also mean that there is now a substantial amount of computer talent in the Middle East, though most of it does not come with the practical experience or pedigree that most people in the computer industry would include on a CV. That's an issue not just in the Middle East but across emerging markets.

"This is the challenge and opportunity in this region. The skill and knowledge that exist that is not fully utilised is an opportunity," he said.

This opportunity exists across emerging markets, he said, but for it to be fully utilised, "institutions and mindsets need to change."

However, the growing rise in technology fluency is also being coupled with another kind of fluency -- fluency in Arabic. And while that too might sound like a good thing for the Arab world, it is instead translating into an increase in Arabic-language specific attacks.

Cyber attackers have used English, French or Russian as their primary language of attack. These attacks were not technical attacks, but email-based attacks (called phishing attacks) meant to trick a users into revealing their password or other information, which a hacker could use to access a system. Early attacks in Arabic were often so bad -- in terms of the language -- that they failed. Fluency in Arabic has now improved to the point that recipients are falling victim at a higher rate than before.

"Now there are bots that speak Arabic," Mohammad says. "[We are seeing] email that is designed in an Arabic context and all of sudden is fair more damaging that it ever was." Bots are third-party internet applications that can be used for a number of tasks, including simulating conversations.

This means that security company can no longer simply be software vendors in the Middle East, he says. Mohamed says sales of software in the Middle East have doubled over the past two years and will likely double again. Attacks in the Middle East have been growing, but despite the amount of raw talent available, there are a lack of resources, both for TrendMicro and customers in the region, to implement the security.

"I have a lot of customers who are saying 'give me the resources to do the work.' That's not scalable. I'm not in the business of providing professional services," he says.

This has created a vacuum of security resources that "is massive and needs to be filled eventually."

It World Canada
Canada should be prepared for "unprecedented" levels of cyber risk, warns ex-CSIS official
Thursday, 02 June 2016
Byline: Cindy Baker

If you think that $500 billion in worldwide cyber crime is a problem now, brace yourself. It's about to get even more intense, said speakers Tuesday at a panel discussion at the Tech Day on Parliament Hill, organized by TechConnex and Northof41.
"I've never seen it at this velocity and level of complexity in my 30 years in security," said Ray Boisvert, the president and CEO of I-Sec Integrated Strategies and a senior associate at communications firm Hill & Knowlton Strategies.

Boisvert should know. He's also the former assistant director for intelligence at the Canadian Security Intelligence Service (CSIS). He noted that technology trends are a contributing factor in the escalating level of cyber threats. The proliferation of devices, the Internet of Things (IoT), virtualization and the growth in data are overwhelming our defences, he said. As well, there are increasing opportunities for email cyber fraud based on information collected from social media.

Cyber Crime -- By the Numbers

Boisvert presented a current snapshot of the impact of cyber crime. He said that 600 million people have been affected, often through the theft of personal identity or a blackmail computer lockdown scheme. "It's a traumatic event that you never want to go through," he said.

For businesses, 74 per cent have been compromised by cyber events. The health care sector is heavily targeted, Boisvert said, with 81 cent of its executives admitting to a network breach.

The tech industry should pay attention to the fact that 90 per cent of executives say they can't read a cyber security report, he added. This needs to be addressed given that it can take an average of $1 million and five days to recover from a cyber event.

At its root, Boisvert said, "the advantage is in the hands of the attacker." Insider facilitation is a big problem, sometimes deliberate, but also by the unwitting employee who clicks on a suspicious link. However, the most significant threats are by organized crime groups. "It's a low-risk, high-yield approach. The Internet has been bountiful for them," he said.

Playbook Priorities

Prevention is the first priority to combat cyber threats, said Boisvert, given that about 80% of malware is low level and can be prevented from entering your network. It's also important to focus on early detection because the average dwell time is over 200 days, a long time for someone to be sitting on your network, he warned.

Panel members outlined three priority areas.

The skills shortage is an important issue, said Tyson Macaulay, chief security strategist and vice president of security Services at Fortinet. He pointed to the recent attacks reported by the global bank transfer co-operative, SWIFT, where hackers targeted banks in countries with acute skills shortages. Automated solutions could help fill that void, he noted.

We need to use data analytics to identify serious threats inside a network, said Patrick Patterson, President and CEO of Carillon Information Security. "If you look back at well known hacks," he said, "People were drowning in alerts. The question is to determine what's important." Analytics can be used, in real time, to sort through massive amounts of data to identify abnormal behaviour in the network.

Raising the bar in the use of credentials has to be a priority, said Grant Woodward, Public Safety and Defence Specialist at SAS. "We can make social engineering harder by eliminating the use of usernames and passwords in Canada," he said. Woodward suggested other approaches should be adopted, such as two-factor authentication, the U.S. standard (FIPS 201), and attribute-based access controls.

The Role of Government

The Government has been responding in a coordinated way, according to Erin O'Toole, the Conservative Member of Parliament for Durham. But, he stressed that "vital partnerships" will be a critical area for the new Government. "For Canadians, there is more impact on our lives if there are disruptions in our financial services or critical infrastructure," O'Toole said.

The Government also needs to examine recent regulatory changes in Europe and the U.S., said Patterson. Canada needs to ensure that it is keeping pace so that businesses are not put in a disadvantaged position.

While the rapid growth in cyber attacks is a serious threat, the panelists also noted that there are significant business opportunities for innovative approaches to deal with the problem. "All of us would agree that it will affect our future prosperity as a nation," said Boisvert.

Globe and Mail
Spy agency shared Canadians' data for years with allies
Thursday, 02 June 2016
Byline: Colin Freeze

A federal spy agency inadvertently shared logs of Canadians' phone calls and Internet exchanges with intelligence allies such as the United States for years, a newly disclosed report says.

The revelation that the Communications Security Establishment compromised Canadians' privacy while sharing clandestinely captured data appears in a confidential watchdog's report obtained by The Globe and Mail from court filings related to a lawsuit against the Canadian government.

The report said software that was supposed to remove identifying information on Canadians from material CSE captured during international surveillance operations had failed. This meant that Canada's intelligence allies received data that Canadian laws say they should not see.

The 2015 report puts in sharper focus the spy agency's struggles to protect Canadians from foreign threats while also safeguarding individual citizens' privacy. The problem was first revealed publicly in January by Defence Minister Harjit Sajjan and CSE officials.

The confidential report was written by Jean-Pierre Plouffe, a retired Quebec judge who heads the Office of the CSE Commissioner, the spy agency's watchdog agency.

In it, he suggests the unlawful seepage of Canadians' phone and Internet records to foreign intelligence agencies could date back to the mid-2000s, and that the overall amount of compromised material is unclear.

Given this, Mr. Plouffe is urging Parliament to pass laws spelling out how it wants the spy agency to function. "As CSE's collection posture has strengthened ... the volume of metadata collected has increased considerably," Mr. Plouffe writes in his 2015 report.

He urged federal politicians to give clearer direction on surveillance.

"Metadata" are logs of communications without the content of the conversation. The watchdog's report reveals that, during its international spying, CSE has been capturing phone logs and sharing them with allies since 2005. Internet logs have been shared since 2009.

In 2014, CSE suspended sharing both sorts of records when it realized its automated systems had failed to scrub out what it calls the "Canadian identifying information" that turned up in the wider mix. Mr. Plouffe, who has the last word on such matters, eventually ruled that although CSE's system failures were inadvertent, they violated the Privacy Act and National Defence Act.

CSE is part of the world's most powerful spying alliance. Since the 1940s, the "Five Eyes" - electronic-espionage agencies in the United States, the United Kingdom, Canada, Australia and New Zealand - have been working closely together. The collective's members cannot eavesdrop on their own citizens, but their governments have relaxed their rules covering telecommunications trails - metadata - in the hopes it could help the Five Eyes track al-Qaeda terrorists.

Metadata collected and shared on a massive, global scale can show intelligence analysts who is talking to who, even when the contents of the underlying conversations are unknown.

Parliament passed a law in 2001 giving CSE increased latitude to collect data, subject to orders from defence ministers that spell out what it can and cannot do. The Globe reported in 2013 that both Liberal and Conservative governments have since signed such metadata ministerial directives.

The 2015 watchdog's report reproduces one of these directives. "CSE may search any metadata acquired" to help track "a foreign individual, state organization, terrorist group, or other such entities," the directive says. It adds: "CSE will share metadata ... with international allies to maximize" surveillance capabilities, but "Canada's allies shall not be granted access to metadata known to be associated with Canadians located anywhere."

But CSE cannot guarantee it can avoid capturing Canadian telecommunications trails. On Wednesday, a director-general with the agency, Scott Millar, attested to this fact in a Federal Court proceeding related to the lawsuit. He said that while CSE does sometimes collect metadata on Canadians, this is a "very rare occurrence."

Just how CSE collects metadata is a state secret, but it is known that it is gathered in huge volumes indiscriminately.

In his 2015 report, Mr. Plouffe says CSE "metadata is acquired without having gone through a targeting selection process."

Only after the initial collection do CSE analysts seek to "minimize" privacy violations by scrubbing out Canadian identifying information, the report says.

The agency refers to this as "minimization."

The report reveals that CSE refers to the phone logs it collects as "Dialled Number Recognition" (DNR) metadata. The agency started sharing such material with Five Eyes allies in 2005, thinking it had devised ways to automatically strike out telling portions of any Canadian phone numbers that turned up.

Then, starting two years ago, CSE discovered that "DNR metadata was not being minimized properly," according to the watchdog report. Mr. Plouffe added: "CSE is unable to determine how many systems were impacted and for how long."

CSE calls the Internet logs it collects "Digital Network Intelligence" (DNI) metadata, and this material can consist of e-mail addresses and Internet protocol addresses that indicate who is communicating to who.

A scrubbing system was developed for that material as well - but this, too, failed. "DNI metadata was being shared with [Five Eyes] Second Parties ... with minimization applied to Canadian e-mail address fields, but no minimization applied to Canadian IP address fields," Mr. Plouffe writes.

He adds that "CSE was under the impression that minimization was taking place, when in fact it was not."

The spy agency suspended sharing when the problems were discovered in 2014, and apparently have not resumed it.

If CSE is to return to exchanging such information, the report said, the Liberal government will likely have to enshrine in law how it wants CSE to reconcile individual privacy and security imperatives.

"I am recommending to the Minister of National Defence that the National Defence Act be amended in order to clarify CSE's authority to collect, use, retain, share and disclose metadata," Mr. Plouffe wrote in a letter to the Minister of National Defence last fall.

Records show Mr. Sajjan has since replied to say he accepted recommendations - but he did not commit to introduce new laws or directives.

Agence France-Presse
Chinese cyber spies hack Taiwan ruling party: security firm
Thursday, 02 June 2016

Beijing - Mainland hackers were likely to be behind an attack on the website of Taiwan's ruling party, a US-based security firm said Thursday, as the island warns of growing cyber threats.
Cross-strait relations have turned increasingly frosty since Taiwan's new president Tsai Ing-wen of the China-sceptic Democratic Progressive Party (DPP) won elections in January and took office last month, with Beijing wary the new government may seek independence.

Taiwan has been self-ruling since the two sides split in 1949 after a civil war -- but China still sees it as part of its territory.

The party's website came under attack in early April, redirecting visitors to a fake website, California-based FireEye said in a statement Thursday.

The tactic is one often used by Chinese hackers, it said.

Administrators fixed the problem the next day but the website was compromised again a few days later, suggesting the site is being monitored, according to the statement.

"FireEye believes this operation likely reflects continued efforts by China-based cyber espionage operators to collect intelligence related to the DPP as it moves Taiwan away from pro-mainland China policies," it said.

The government has raised concerns that its websites frequently fall prey to Chinese hackers.

Taiwan's Ministry of Transportation and Communication said in a report to a legislative committee last month that the scale of cyber attacks on Taiwan is "near warfare."

It added the most active hackers are from the mainland and had infiltrated the island's systems including defence, air traffic, and communication.

The defence ministry says it will establish a "cyber army", one of the policies put forward by Tsai during her presidential campaign.

A "Fourth Service" should be formed along with army, navy, and air force to protect "national digital territory," according to the DPP's proposal.

However, the DPP played down the findings of the new FireEye report and said it was not currently seeing "unusual hacking activities".

"The DPP has always put great importance on cyber safety," spokesman Wang Min-sheng told AFP.

Wang added that the party is not in contact with FireEye and that the security firm had been monitoring its website independently.

Wall Street Journal
Congress Opens Inquiry Into Cyberheist
Thursday, 02 June 2016
Byline: Kate Davidson

Washington - A congressional panel is seeking more details related to the $101 million cyberheist from the Bangladeshi central bank's account at the Federal Reserve Bank of New York earlier this year. The chairman of the House Committee on Science, Space and Technology has asked New York Fed officials to brief the committee on its handling of the security breach. It also requested documents related to the New York Fed's oversight of the secure interbank messaging system known as Swift, which the hackers used to submit fraudulent payment orders of nearly $1 billion.

The thieves spirited $101 million out of Bangladesh Bank's account in February before the requests raised red flags at the New York Fed.

Officials were able to stop payment on one of the fraudulent orders, but the bulk of the remaining $81 million ultimately ended up with at least one casino and two gambling-junket operators in the Philippines, according to the Philippines's Anti-Money Laundering Council.

"In light of the recent cyberattacks on our global financial systems, the committee believes it is imperative to receive information from the NY Fed about its response, its oversight of SWIFT, the status of the investigation and any remedial steps taken to address vulnerabilities," Chairman Lamar Smith (R., Texas) said in a May 31 letter to New York Fed President William Dudley. The committee is requesting the documents be turned over by June 14.

Mr. Smith isn't the first lawmaker to raise concerns about the breach.

Rep. Carolyn Maloney, a New York Democrat and member of the House Financial Services Committee, sent a letter in March asking for more information.

"What is especially thought-provoking here is that stops and recalls on these transfers weren't issued for days after initial doubts were raised," Ms. Maloney said in April.

The New York Fed has defended its procedures for fund transfers, which are intended to prevent dollars from being transferred to individuals or firms that have been placed under sanctions and "are not designed to protect our customers from an unauthorized transfer," Thomas Baxter, the bank's head lawyer, said in a letter to Ms. Maloney.

News of Mr. Smith's letter followed a Reuters report Wednesday on cybersecurity threats at the Federal Reserve in Washington.

Computers used by the central bank were breached more than 50 times from 2011 to 2015, according to cybersecurity reports issued by the Fed.

The security reports, obtained by Reuters through a Freedom of Information Act request and provided to The Wall Street Journal, didn't show who was behind the attacks, if funds were stolen or whether sensitive information was accessed.

The disclosures cover only those security breaches affecting the Fed's Board of Governors, as the Fed's regional reserve banks aren't subject to FOIA. Of the 310 security reports issued by the Fed, 140 disclosed hacking attempts, Reuters reported.

"As with other government agencies, the Federal Reserve is a target for cyberattacks," a Fed spokesman said in a statement on the Reuters report. "However, our security program and processes for detecting and countering attacks are robust and our critical operations have never been affected."

Wall Street Journal
China's Huawei Is Coy On Ties to Israeli Firm
Thursday, 02 June 2016
Byline: Orr Hirschauge

Tel Aviv - Huawei Technologies Co., the Chinese telecommunications firm that has barreled into emerging markets around the world, has been cautious about its footprint here.
For the past seven years, Huawei has been developing technologies, some potentially sensitive, through a locally registered company called Toga Networks Ltd., according to former and current employees of both companies.

At Toga, Israeli engineers are developing a range of software and equipment related to networking, storage and information security, including encryption, said former and current employees of the company. Toga is also developing tools that can help telecommunication providers examine data moving through their routers. This so-called deep-packet inspection technology is typically used to prioritize traffic, such as phone calls over emails, but it can also identify individuals who surf specific websites or use certain keywords in emails.

The work here comes against a backdrop of intense U.S. scrutiny over Israeli technology transfers to China, and concern that some products developed here could be used to eavesdrop on global internet and telecom users.

While Toga hasn't advertised its links to Huawei, it doesn't exactly hide the relationship. Several patents submitted by Huawei since 2013, some relating to the deep-packet inspection algorithms, have Toga employees listed as inventors, according to a former Toga employee and public patent records.

Also, Toga is identified as a unit of Huawei by Israeli government documents, Israeli officials, and current and former Toga employees.

"Toga Networks is a private company. It doesn't provide to the public any information concerning either its business activities or its connections with clients," Toga said in an emailed response.

Huawei said Toga Networks isn't a subsidiary of the company, but that it collaborates with research partners. "Huawei believes open innovation is the key to the development of the industry, so we cooperate with local partners to better leverage local talents and offer the most innovative and leading solutions to customers all over the world," a company spokesman said in an email.

The tech company rejected the idea of opening an official research center here because an Israeli arm was seen as limiting the company's business outreach to Arab countries, according to current and former employees.

Huawei's networking equipment has been effectively shut out of the U.S. market following a 2012 congressional report which cited concerns that it could be used for Chinese espionage. The company has disputed such claims.

Further, the increasing involvement of Chinese companies in the development of sensitive technology inside Israel has raised some concerns in U.S. security circles, according to a former Israeli official familiar with the matter. The U.S. Department of Defense declined to comment.

Several high-profile Chinese companies such as Alibaba Group Holding Ltd, Baidu Inc. and Xiaomi Corp. have built links with Israel's technology sector in recent years. The firms, over the years, have invested in Israel-based venture funds and startups.

Avi Hasson, the chief scientist at the Israeli Ministry of Economy, said that the ministry wants to encourage further involvement of Chinese entities in the local industry.

"We view favorably the influx of Chinese investments in the Israeli technology industry. Asian markets are part of the future of this industry, and it is almost impossible to sell in these markets without a local partner," Mr. Hasson said in an email.

The worries around the influx of "nontraditional investors" like the Chinese in Israel center on access to technologies that can be applied for military uses, says Oded Eran, a senior researcher fellow at Israel's Institute for National Security Studies and a former deputy director general of the Israeli Ministry of Foreign Affairs. Companies that employ veterans of technological units in the Israeli army, such as unit 8200 -- the country's equivalent of the National Security Agency -- are one point of access to such technologies, Mr. Oded said.

"These veterans go and work for commercial companies but there are no walls in their mind separating what they did in military service from what they do in civilian life," he added.

The U.S. and Israel have clashed over technology transfers to China before. In 2000, the U.S. stopped Israel from selling China an advanced airborne warning system called Phalcon, leading to a diplomatic rift between Israel and China. In 2004, the Pentagon stepped in again, attempting to block the return of several Israeli-made unmanned combat aerial vehicles China had sent to Israel for maintenance and possible upgrades.

Reuters
Fed records show dozens of cybersecurity breaches
Wednesday, 01 June 2016

Washington - The U.S. Federal Reserve detected more than 50 cyber breaches between 2011 and 2015, with several incidents described internally as "espionage," according to Fed records.
The central bank's staff suspected hackers or spies in many of the incidents, the records show. The Fed's computer systems play a critical role in global banking and hold confidential information on discussions about monetary policy that drives financial markets.

The cybersecurity reports, obtained by Reuters through a Freedom of Information Act request, were heavily redacted by Fed officials to keep secret the central bank's security procedures.

The Fed declined to comment, and the redacted records do not say who hacked the bank's systems or whether they accessed sensitive information or stole money.

"Hacking is a major threat to the stability of the financial system. This data shows why," said James Lewis, a cybersecurity expert at the Center for Strategic and International Studies, a Washington think tank. Lewis reviewed the files at the request of Reuters.

The records represent only a slice of all cyber attacks on the Fed because they include only cases involving the Washington- based Board of Governors, a federal agency that is subject to public records laws. Reuters did not have access to reports by local cybersecurity teams at the central bank's 12 privately owned regional branches.

The disclosure of breaches at the Fed comes at a time when cybersecurity at central banks worldwide is under scrutiny after hackers stole $81 million from a Bank Bangladesh account at the New York Fed.

Cyber thieves have targeted large financial institutions around the world, including America's largest bank JPMorgan, as well as smaller players like Ecuador's Banco del Austro and Vietnam's Tien Phong Bank.

Hacking attempts were cited in 140 of the 310 reports provided by the Fed's board. In some reports, the incidents were not classified in any way.

In eight information breaches between 2011 and 2013 - a time when the Fed's trading desk was buying massive amounts of bonds - Fed staff wrote that the cases involved "malicious code," referring to software used by hackers.

Four hacking incidents in 2012 were considered acts of "espionage," according to the records. Information was disclosed in at least two of those incidents, according to the records. In the other two incidents, the records did not indicate whether there was a breach.

In all, the Fed's national team of cybersecurity experts, which operates mostly out of New Jersey, identified 51 cases of "information disclosure" involving the Fed's board. Separate reports showed a local team at the board registered four such incidents.

The cases of information disclosure can refer to a range of ways unauthorized people see Fed information, from hacking attacks to Fed emails sent to the wrong recipients, according to two former Fed cybersecurity staffers who spoke on condition of anonymity.

The former employees said that cyber attacks on the Fed are about as common as at other large financial institutions.

It was unclear if the espionage incidents involved foreign governments, as has been suspected in some hacks of federal agencies. Beginning in 2014, for instance, hackers stole more than 21 million background check records from the federal Office of Personnel Management, and U.S. officials attributed the breach to the Chinese government, an accusation denied by Beijing.

TARGET FOR SPYING

Security analysts said foreign governments could stand to gain from inside Fed information. China and Russia, for instance, are major players in the $13.8 trillion federal debt market where Fed policy plays a big role in setting interest rates.

"Obviously that makes it a very clear (hacking) target for other nation states," said Ari Schwartz, a former top cybersecurity adviser at the White House who is now with the law firm Venable.

U.S. prosecutors in March accused hackers associated with Iran's government of attacking dozens of U.S. banks.

In the records obtained by Reuters, espionage might also refer to spying by private companies, or even individuals such British activist Lauri Love, who is accused of infiltrating a server at a regional Fed branch in October 2012. Love stole names, e-mail addresses, and phone numbers of Fed computer system users, according to a federal indictment.

The redacted reports obtained by Reuters do not mention Love or any other hacker by name.

The records point to breaches during a sensitive period for the Fed, which was ramping up aid for the struggling U.S. economy by buying massive quantities of U.S. government debt and mortgage-backed securities.

In 2010 and 2011, the Fed went on a $600 billion bond-buying spree that lowered interest rates and made bonds more expensive. It restarted purchases in September 2012 and expanded them up in December of that year.

The Fed cybersecurity records did not indicate whether hackers accessed sensitive information on the timing or amounts of bond purchases or used it for financial gain.

UP ALL NIGHT

The Fed's national cybersecurity team - the National Incident Response Team, or NIRT - created 263 of the incident reports obtained by Reuters.

NIRT operates in a fortress-like building in East Rutherford, New Jersey that also processes millions of dollars in cash everyday as part of the central bank's duty to keep the financial system running, according to the New York Fed's website. The unit provides support to the local cybersecurity teams at the Fed's Board and regional banks, which process more than $3 trillion in payments every day.

The NIRT handles "higher impact" cases, according to a 2013 report by the Board of Governor's Office of Inspector General.

One of the two former NIRT employees interviewed by Reuters described being on a team that once worked around the clock for five-straight days to patch software hackers had used to gain access to Fed systems in an attempt to obtain passwords. The former employee worked through several of those nights, taking naps at a desk in the office.

In that case, Fed security staff found no signs that sensitive information had been disclosed, the former employee said. Information about future interest rate policy discussions is isolated from other Fed networks and is more difficult for hackers to access, the former NIRT worker said.

But the Fed was under constant assault, much like any large company, the former employee said, and was "compromised frequently."

An internal watchdog has criticized the central bank for cybersecurity shortcomings. A 2015 audit by the Fed board's Office of Inspector General found the board was not adequately scanning databases for vulnerabilities or putting enough restrictions on system access.

"There is heightened risk of unauthorized disclosure and inappropriate use of sensitive board information," according to the audit released in November.

The Guardian (London)
Snooper's charter: Teresa May makes concessions
Wednesday, 01 June 2016
Byline: Alan Travis

London - The home secretary, Theresa May, has made further concessions on the snooper's charter, including on the key issue of privacy, before a Commons battle over the bill next week.
The concessions, intended to meet concerns raised by the parliamentary intelligence and security committee (ISC) as well as by Labour, Liberal Democrat and backbench Tory critics, include the introduction of a privacy clause designed to ensure that the new mass surveillance powers are not authorised in situations where less intrusive means could be used.

The two-day Commons report stage of the investigatory powers bill, which will extend the powers of the security services, is scheduled for Monday and Tuesday next week. It will be the last substantive piece of parliamentary business before the EU referendum in three weeks' time.

The home secretary's concessions also cover protection for journalists, the Wilson doctrine on shielding MPs from snooping, and the retention and use of "bulk personal datasets" such as medical records.

The ISC, chaired by the former Conservative attorney general Dominic Grieve, and parliament's joint human rights committee, chaired by the former Labour cabinet minister Harriet Harman, have also tabled amendments to the bill demanding much tougher safeguards preventing the powers from being abused.

The ISC in particular demanded that privacy protections should be made an overarching part of the bill.

The bill not only enshrines in law the bulk data collection and mass computer and phone-hacking operations carried out by GCHQ, which were revealed by the whistleblower Edward Snowden in 2013, but also extends the security services' powers to track everyone's web history by introducing internet connection records that can be stored for 12 months and that can be accessed by the police and security services.

The new Home Office concessions include:

. Privacy: a new clause that makes clear that warrants and other authorisations should not be granted where the information could reasonably be obtained by less intrusive means. The clause makes explicit the implicit privacy safeguards in the bill and puts "beyond doubt" that there will be severe penalties for those who deliberately misuse the powers.

. Protection for journalists: clarification that the judicial commissioner will be required to consider 'the overriding public interest' when authorising the use of communications data to identify a journalist's sources.

. Wilson doctrine: prime minister must give explicit approval for law enforcement agencies to hack into MPs' phones and computer as well as to access their communications data.

. Bulk personal datasets and medical records: the legal test needed to retain and examine these highly personal records is to be raised to "exceptional and compelling" cases only.

A Home Office spokesperson said: "We have always been clear that we will listen to the constructive views of politicians from all sides of the House to ensure the passage of this important bill. We have said the government will be bringing forward amendments at report stage and are willing to consider amendments that are in the interest of both improving the bill and of demonstrating the necessity of the powers it contains."

Labour has already secured from May a commitment to an independent review of the operational case for bulk personal data collection and hacking powers by Britain's watchdog on terrorism laws, David Anderson, and protection from surveillance for legitimate trade union activities.

However, Labour intends to press for further changes, including stronger safeguards in five areas: privacy, using internet connection records only in serious crime cases, toughening rules on the judicial authorisation of intercept warrants, stronger safeguards on the use of medical records and other bulk datasets, and protections for legal and journalistic confidentiality.

The Liberal Democrats, who could prove influential when the bill reaches the Lords, have tabled amendments that would remove "internet connection records" - tracking everyone's web use - from the bill and that would ensure that people who are the targets of unlawful surveillance are told what data of theirs has been accessed so they can seek redress.

The Liberal Democrats' home affairs spokesman, Alistair Carmichael, said the ISC told May to go away and rewrite the bill to include a dedicated section on privacy: "Instead she re-labelled the title 'General Protections' to 'General Privacy Protections', a one-word aesthetic addition that fools no one. That is why the Liberal Democrats will continue to fight, both in the Commons and Lords, for privacy to form the backbone of this legislation.

"Theresa May's concession allowing for an independent review into bulk powers is welcome but this goes nowhere near far enough. Too many of the proposals in the bill are vaguely drafted and disproportionate; for example, we are clear that proposals to collect and store everyone's web histories for 12 months has to go. We should be equipping our police and security services with the resources they need, not drowning them in data," he said.

Haaretz
Sirin Labs Unveils Smartphone With $14,000 Price Tag
Thursday, 02 June 2016
Byline: Eliran Rubin

Jerusalem - How much is your mobile privacy worth to you? If it's at least $14,000, Sirin Labs, the Switzerland-based startup backed by Israeli technology entrepreneur Moshe Hogeg, has the phone for you.
The company's Solarin smartphone, unveiled on Tuesday in London, comes in four models with a starting price of 9,500 pounds ($13,766) not including value-added tax. For now, it is available only at the company's store in London's Mayfair and at Harrods.

Inside a case made of "Black Carbon Leather with Titanium," the phone sports 2,500 components, including anti-cyberattack software supplied by the company Zimperium; encryption technology from KoolSpan, speeds of 450 megabits per second of downlink and up to 150 uplink speeds and a 23.8-megapixel camera.

Two years in the making at research and development offices in Lund, Sweden, and Tel Aviv, the phone is "aimed at the international business person who carries a lot of sensitive information but doesn't want to compromise on usability, quality or design," Sirin said.

Sirin Labs had been operating in stealth mode until a month ago, when Hogeg revealed that he and other investors, who include Kazakh businessman Kenges Rakishev and Chinese internet company Renren, had put $72 million into the company, which was formed three years ago.

"Cyber attacks are endemic across the globe. This trend is on the increase. Just one attack can severely harm reputations and finances. Solarin is pioneering new, uncompromising privacy measures to provide customers with greater confidence and the reassurance necessary to handle business-critical information," Tal Cohen, Sirin's CEO and cofounder, said in a statement.

Hogeg told the technology website TechCrunch that the phone's security features were so powerful that to prevent abuse by criminals and terrorists, it would only be sold to people who are identified with their passports. He said the company was preparing a list of countries that the phone won't be sold to.

The Solarin phone is being offered as an alternative to mass-market smartphones like the iPhone for business people who want to protect confidential information. After Apple's high-profile standoff with the U.S. government over encryption, Sirin Labs' timing for a highly secure alternative is good. In addition, the secure phone market has had no dominant player since Blackberry left in 2013.

Pajhwok Afghan News
MoI rejects Taliban's access to biometric system
Thursday, 02 June 2016
Byline: Ajmal Kakar

Kabul - The Ministry of Interior on Wednesday rejected as baseless claims that the Taliban had gained access to 'biometric' system to identify their opponents.
After recent kidnapping of passengers in northern Kunduz province, some reports emerged that the Taliban had gained access to the biometric system in the province and it was rumored the insurgents could identify security personnel travelling on highways especially on the Northern Highway.

A statement from the Ministry of Interior said after investigation into the reports, the MoI could satisfy people that there were no such things happening and all such claims were untrue.

The ministry said the rumours were just part of the enemy's propaganda and was a psychological war against the Afghan security forces.

It said the biometric system, the ministry is using to register identities of police members and access criminal records, was completely secure and under control.

The insurgents in no way could gain access to the system to identify police officials and no insurgent group was able to do so, the statement added.

However, Lt. Gen Shir Aziz Kamawal, the 808th Spinghar Zone commander in the northeast, told Pajhwok Afghan News that according to passengers freed from the Taliban, the group had gained access to the system and identified passengers using it.

The MoI in its statement said the biometric system has two parts --- central and local. The central part is located in Kabul, which can be only accessed by some specific officials and the other in provinces does not have any possible way to identify registered identities through it, the statement said.

"If the system in an emergency situation faces any kind of problem, the central biometric system deactivates all local systems in provinces after which it cannot be used or accessed," it added.

Fars News Agency
Iranian Defense Minister Unveils 3 New Technological Achievements
Thursday, 02 June 2016

Tehran - Iranian Defense Minister Brigadier General Hossein Dehqan unveiled three new home-made technological achievements in Tehran on Wednesday.
The achievements include 1-MW national GPS system, robotic vacuum plasma coating and vacuum arc remelting furnace which have all been designed and built by Iranian researchers at Malek-e Ashtar University.

Elaborating on the new achievements, General Dehqan said that the 1-MW national GPS system is a reliable substitute for the GPS which can be used in critical conditions.

Also, the robotic vacuum plasma coating is one of the laboratorial equipment used in different research processes, turbines and jet engines that has the capability to resist high temperatures, he added.

General Dehqan also said that the vacuum arc remelting furnace can be used for melting and purification of titanium, remelting the super alloys and special steels and can be operated both manually and automatically.

In a relevant development in February, General Dehqan unveiled 4 products of the defense industry and inaugurated the production line of a key medicine that fights the effects of chemical elements.

The new achievements included 'Pars Kam' detector system that tracks chemical substances dangerous to health, a new system that can detect explosives and drugs, anti-strike and explosion-proof polymer coatings, a new generation of NBC protective clothes based on Travagzin membranes, as well as the production line of Obidoxime chloride medicine that fixes the effects of chemical substances on the body.

Speaking to reporters, Dehqan said the defense ministry will continue to design, invent and produce modern equipment and products for protection of its armed forces.

Also in February, the defense ministry had also unveiled 7 national geographic projects.

The projects included a remote defense lab - national spectral sensing, first unmanned smart hydrography Fajr 1 (Dawn 1), coastal development of Makran, production line of digital marine maps, digital geomorphology maps, magnetic marine measuring systems, climate database, and geographic data production line using drone images.

Minister Dehqan said, "The Fajr 1 hydrography is a remote control system, able to transmit data and image, GPS, measure depths, advance multibeam systems, and side scan sonar and radar data."

On the applications of digital maps of geomorphology system, he said they can be used in scientific and research projects, as well as in geography, environment, construction, development, agriculture, defense logistics, civil defense, and military affairs.

According to Dehqan, the database on climate will be used for military and defense purposes, including in tarmacs, military drills, and troop deployments.

Yonhap News Agency
China takes note of media reports that Huawei faces U.S. probe on N. Korea exports
Friday, 03 June 2016

Beijing - China's foreign ministry said Friday that it took note of U.S. media reports that Huawei Technologies Co., a Chinese telecom equipment maker, is facing a U.S. probe over its exports to North Korea, Cuba, Iran and Syria.
The U.S. Department of Commerce has ordered Huawei's U.S. units to clarify whether the Chinese company exported goods containing American technology to the rogue nations, The New York Times reported.

"I have noted relevant reports," China's foreign ministry spokeswoman Hua Chunying told reporters.

Hua did not elaborate further, citing Huawei's statement, which was reported by U.S. media, that the Chinese company has "abided by local laws and regulations."

The U.S. media reports came days before U.S. Secretary of State John Kerry and Treasury Secretary Jacob Lew arrive in Beijing for annual meetings on strategic and economic issues with senior Chinese officials.

Sputnik
Le Canada a partagé des données sur ses citoyens avec ses alliés
Thursday, 02 June 2016
Byline: Journaliste maison

Ottawa - Selon un rapport de 2015 sur la protection des données personnelles au Canada, les services secrets canadiens ont créé un risque de divulgation de données personnelles des citoyens canadiens dans le cadre de leur coopération avec les services secrets américains, britanniques, australiens et néo-zélandais.
Le Centre de la sécurité des télécommunications (CST), un service de renseignement canadien, a fourni des métadonnées sur les entretiens téléphoniques et les messages en ligne des Canadiens à des services de renseignement étrangers depuis le début des années 2000, a annoncé le journal canadien The Globe and Mail.

Les logiciels du CST, chargés de supprimer automatiquement les informations d'identification obtenues dans le cadre d'opérations de renseignement internationales, n'arrivaient pas à accomplir leur mission, ressort-il d'un rapport de Jean-Pierre Plouffe, commissaire du CST cité par le journal.

Cela signifie que des services secrets étrangers ont reçu ces informations en violation des lois canadiennes sur la défense nationale et sur la protection de la vie privée. Le nombre précis des métadonnées ainsi transférées reste inconnu, selon M.Plouffe.

Le commissaire a appelé le parlement canadien à adopter des lois réglementant les devoirs des services secrets dans ce domaine et à mieux définir les mesures de contrôle puisque les services de renseignement avaient récemment intensifié la collecte d'informations sensibles.

Les métadonnées servent à décrire d'autres données sans préciser leur contenu.

Selon le rapport, le CST partage des métadonnées sur les entretiens téléphoniques avec ses alliés étrangers depuis 2005 et sur les adresses électroniques et adresses IP depuis 2009. Le transfert des métadonnées a été suspendu en 2014, après que le CST a appris que les systèmes automatiques ne supprimaient pas toutes "les informations d'identification canadiennes".

Le CSE, qui fait partie d'une grande alliance de renseignement surnommée "Five eyes" ("les cinq yeux"), collabore avec la NSA américaine, le GCHQ britannique, l'ASD australien et le GCSB néo-zélandais depuis les années 1940.

Il a décidé d'espionner les citoyens canadiens dans l'espoir de traquer les terroristes d'Al-Qaïda en 2011. Dans cette optique, le parlement canadien a adopté en 2011 une loi modifiant les normes de collecte des métadonnées et le gouvernement a adopté un règlement permettant au CST de collecter des métadonnées pour surveiller des ressortissants étrangers, des organisations publiques, des groupes terroristes et d'autres structures.

Un responsable du CSE, Scott Millar, a reconnu mercredi que le CST ne pouvait pas éviter la collecte de données d'identification canadiennes, mais qu'il ne le faisait pas souvent.

Selon la loi, le CST partage ses métadonnées avec ses alliés internationaux pour élargir le potentiel des services secrets, mais les alliés du Canada ne peuvent pas obtenir les informations concernant les Canadiens où qu'ils se trouvent.

Palestinian Sentenced to Year in Prison for 'Facebook Incitement'
Friday, 03 June 2016
Byline: Jack Khoury

Jerusalem - A Bethlehem resident was sentenced Thursday to one year in prison after he was convicted of incitement in his Facebook posts.
Kusai Issa, 22, posted messages encouraging and supporting terror activities, according to the charge sheet presented against him at the Ofer military court.

The posts were made on October 4-8, at the beginning of the violence wave, under the name "Shahid [martyr] in waiting," according to the charges.

In one case Issa was charged for posting a photo of one of the assailants, which garnered praise from his Facebook friends. The next day he put up a clip captioned: "The clip is more than amazing and shows how a freedom fighter kills four Zionist soldiers with a knife," according to the indictment.

On October 7 Issa is charged with posting: "The youngsters confronting the occupation, put your shirts under your trousers because the mista'arvim [members of IDF counterterrorism units dressed as Palestinians] put it outside their trousers to hide the gun - post this and defend our nation's youngsters."

Issa was arrested last October and has been in custody since. His verdict was handed down as part of a plea bargain, under which he is also required to pay a 2,000-shekel fine.

Issa's attorney, Mohammed Shahin of the Palestinian Prisoners Club, said the military prosecution presented his various posts and said they won much support and were shared by many.

Shahin said the prosecution first demanded a 15-month prison term, among other things because Issa's posts had 18,000 followers and therefore, according to the prosecution, his influence was great.

Shahin said these offenses carry a sentence of eight months to two years, according to the posts' circulation.

On Thursday morning police arrested Bassam Safadi, an Arab journalist from the north of the country and an Iranian television reporter, on suspicion of publishing "support for a terrorist organization and incitement to violence or terror." The Nazareth Magistrate's Court extended his custody to Sunday.

The Iranian Al-Alam channel that Safadi, 43, works for reported his arrest and claimed he had broadcast numerous reports about Israel's conduct in the Golan Heights, including what he called "gas stealing from the Syrian Golan."

Safadi's wife said police and troops came to their home late at night and arrested her husband, confiscating a large amount of equipment, including telephones.

Times of Israel
After slew of cyber-strikes, BDS movement points finger at Israel
Friday, 03 June 2016

Jerusalem - The international movement calling for a boycott against Israel said Thursday its website was repeatedly attacked earlier this year, and raised suspicions that Israel was behind the attacks.

The BDS (boycott, divestment and sanctions) movement released a report Thursday showing that its main website suffered six attacks in February and March. The denial of service attacks, which work by flooding a target website with bogus traffic, knocked out the BDS website for several hours at a time.

The report, compiled by nonprofit online security service eQualit.ie, said the attacks had a level of "sophistication and commitment" it normally does not see. It also noted that an unidentified Israeli human rights group had been attacked at the same time, indicating there was a "common adversary."

Assigning responsibility for cyber-attacks is notoriously difficult and the report didn't speculate on who might be behind the rogue traffic.

In a statement, the BDS movement said the "advanced technology used in the attacks and the size of the botnets involved may show that Israel was directly involved" but it offered no hard evidence.

Israeli cyber- security expert Gilad Yoshi said such attacks do not cause serious damage, adding it was unlikely a government was behind them. "These are not high- level attacks," said Yoshi, an expert at the electronic defense training company CyberGym.

BDS calls for boycotts, sanctions and divestment from Israel in what it calls a nonviolent struggle against occupation. Israel says BDS's goal is to destroy the country, and it has identified the movement as a serious threat.

Jerusalem has earmarked funds for Israeli tech companies for digital initiatives aimed at gathering intelligence on activist groups and countering their efforts.

Initiatives are largely being kept covert. Participants at one recent invite-only forum, held on the sidelines of a cyber technology conference, repeatedly stood up to remind people that journalists were in the room.

Israel's Ministry of Strategic Affairs, which is spearheading the government's battle against BDS, was reviewing Thursday's report and had no immediate comment.

Khaleej Times
Cybersecurity top priority of UAE government
Friday, 03 June 2016
Byline: Sandhya D'Mello

Dubai - What is the point in feeling safe when your house is locked but your window is open? Or is it safe when you locked the house and slipped the key under the doormat? Or can you outsmart hackers by simply having a very predictable password - 123456 - to your device controlled security?

These anecdotes will make one ponder that nowadays when we are constantly hooked in cyberworld, security not only becomes prime concern but inevitable to track best solutions to live safe and that is exactly the top priority of the UAE government towards its residents.

"The UAE is extremely conscious about the cybersecurity being offered to its residents as it globally evolves to be among the top smart cities in the world," Faisal Al Bannai, chief executive officer of DarkMatter told Khaleej Times in an exclusive interview.

DarkMatter is a UAE headquartered company that is transforming the cybersecurity landscape by providing a complete range of state-of-the- art services and solutions to government and commercial clients. Its end-to- end expertise extends to: governance, risk and compliance; cyber network defence; managed security services; secure communications; infrastructure and system integration; smart solutions; agile and innovative.

"Cybersecurity needs to be viewed as collective measure at corporate levels as companies not only need to invest more but invest in a smart way so as to get maximum benefit to ensure they stay protected. Higher connectivity only means higher vulnerability and hence companies need to be extra prudent as to where they are investing in terms of boosting their safety."

Most employees use their devices for their personal use and the same is used for their corporate needs giving rise to massive vulnerability issues.

"Cybersecurity now stands at the centre of further progress of the modern, electronic-based global economy. Pro-activity and a holistic approach to cybersecurity has never been more important as it is critical now," added Al Bannai. "Buying few pieces of hardware and firewalls means nothing, its like staying in home safely with doors open."

Cybersecurity is not only a local but a global concern and in a day where we all need to stay connected it makes the world shrink. The security needs in US may not differ much from any other developed or developing country the issues remain more or less same.

The company's CEO strongly recommends that security needs to cover end to end points covering policies, hardware to monitoring and implementation of the solutions and many entities are yet on learning curve.

The cybersecurity is dominated by large entities either US or Europe headquartered and this made it inevitable for DarkMatter to not only set up its operations here but bring global pool of talent to UAE headquarters and position itself as global player.

"We are currently developing our own IP, product development and research and development centres that are already developing products for next generation which will be out by 2017. The aim is to support the vision of His Highness Shaikh Mohammed bin Rashid Al Maktoum, Vice-President and Prime

Minister of the UAE and Ruler of Dubai, to build the nation which is known for innovation and the one which can develop its own IP - Internet Protocol.

Currently with 150 extremely talented and specialised staff serve the company and by the end of the year this number can be seen reaching 600. The company will launch products in first-half of 2017, which will see technologies, patents, IP developed from the UAE and competing in global markets. The company is all set to announce series of peer-to-peer partnerships in current and next year targeting over 300 per cent growth in 2016," said Al Bannai.

The regional network security spend in a GCC-wide sector set to grow from $340 million to $1 billion by 2018, according to a Frost & Sullivan.

The international cybersecurity firm headquartered in the UAE, has found that 48 per cent of respondents to its DarkMatter Cyber Security Poll said their organisations do not have a senior management executive assigned to oversee cybersecurity, while 46 per cent of respondents said their organisations did not have a board-level representative responsible for cybersecurity.

The statistics are extracted from a poll conducted by DarkMatter during the Gulf Information Security Expo & Conference 2016 held in Dubai, at which the company was the Cyber Security Innovation Partner. DarkMatter was able to poll the answers of over 200 information and communication technology visitors present at the event, with the aim of the exercise being to identify attitudes held by enlightened ICT professionals towards the role of cybersecurity in modern, highly digitised economies, and the state of their organisations' cyber threat resilience.

The poll identified that 23 per cent of respondents believe that their organisations have been victim to an internal cybersecurity breach, while 32 per cent believe their organisations have fallen victim to an external attack.

This suggests external threats pose a greater threat to organisations' digital assets than internal ones, with a further poll result indicating 46 per cent of respondents believe cybersecurity breaches are most often the result of human factors.

Saudi Gazette
Al-Watan newspaper confirms website hacked
Friday, 03 June 2016
Byline: Staff Report

Abha - Al-Watan newspaper confirmed that its website had been hacked and false statements attributed to Crown Prince Muhammad Bin Naif, deputy premier and minister of interior, were posted on the website, Saudi Press Agency said.

In a statement, the newspaper said the hacker posted false statements, which he attributed to the Crown Prince. These statements are baseless and untrue. The daily stressed that the reader would not be deceived by such lies and fabricated statements, as the daily relies for its official news on what is transmitted by the official Saudi Press Agency (SPA).

The website was hacked on Thursday (June 2) at 9.20 a.m. by a hostile group from outside the Kingdom. They were able to control the website for some time. During this period, they were able to publish fabricated stories including statements attributed to Crown Prince Muhammad Bin Naif on Decisive Storm. Thanks to Allah, specialists in the newspaper were able to restore the website and begin investigations in coordination with the authorities concerned.

Al-Watan said it will publish full details of this crime, aside from what it mentioned on the social media about the hacking, when it occurred and on the false stories posted on the website.

Al-Watan newspaper said its constant stand towards the issues of the region, its full support for the state's policy and exposing those who are lying in wait to undermine the Kingdom's security have aroused the anger of those who harbor hatred against the Kingdom and are the enemies of the nation.

Therefore, they tried to hack the newspaper's website. This will only increase the determination of the daily to defend the security of the nation and citizen and expose the external conspiracies aimed at shaking the security of the Kingdom and the whole region.

Canadian Press
'Loss of faith' from spy allies possible if Canada proceeds with court disclosure: CSE official
Friday, 03 June 2016
Byline: Jim Bronskill

Ottawa - Close allies will curb or even halt the flow of intelligence to the Communications Security Establishment if the electronic spy agency is forced to spill its closely guarded secrets in open court, argues a senior CSE official.
In turn, that could dry up the flow of "quality information necessary to ensure the safety and protection of Canadians and Canadian interests," says Scott Millar, director general of strategic policy and planning at CSE.

Millar's warning comes in an affidavit filed in a legal tug-of-war between the federal government and a civil liberties watchdog over what CSE must disclose in court.

The British Columbia Civil Liberties Association is suing the national surveillance agency, claiming it breaches the constitutional rights of Canadians by intercepting their private communications.

The organization filed the lawsuit almost three years ago in the Supreme Court of British Columbia. But an initial phase of the legal saga played out this week in Federal Court in Ottawa with cross-examination of witnesses over disclosure of federal records in the broader case.

The Ottawa-based CSE uses highly advanced technology to intercept, sort and analyze foreign communications for morsels of intelligence interest to the federal government. It is a member of the Five Eyes intelligence alliance that also includes the United States, Britain, Australia and New Zealand.

A federal watchdog declared earlier this year that the spy agency broke privacy laws by sharing information about Canadians with foreign partners.

Certain types of metadata containing Canadian identity information were not being properly "minimized" - stripped of potentially revealing details - before being shared with the CSE's four key foreign partners.

Metadata is information associated with a communication - such as a telephone number or email address - but not the message itself. Still, privacy advocates argue it can be highly revealing.

CSE's activities are shrouded in secrecy, says Grace Pastine, the civil liberties association's litigation director.

"CSE is required to have policies in place to protect the privacy of Canadians, but it has not provided the details of those policies to Canadians," she said in a statement. "We're calling on the federal government to state clearly who it is watching, what is being collected, what is being shared with foreign governments and how it is handling Canadians' private communications and information."

In his affidavit, Millar says if CSE is forced to reveal sensitive material provided to it by a Five Eyes agency, or related to the alliance's processes, it is very likely to be damaging.

"Damaging trust and respect through disclosure of information against the expressed wishes of one or more of our Five Eyes partners would have a detrimental effect on future collaborative efforts, consequently harming not only the interests of Canada, but also those of our closest partners."

The federal Liberals have expressed concerns about CSE, committing during the election campaign to limit the agency's power by requiring a warrant to engage in the surveillance of Canadians, the civil liberties association noted.

However, to date, the government continues to oppose the lawsuit.

Globe and Mail Online
The 'top secret' surveillance directives

Friday, 03 June 2016

Ottawa - In 2013, the British Columbia Civil Liberties Association sued the federal government, alleging that a Canadian spy agency's indiscriminate surveillance violated citizens' constitutional rights against illegal search and seizure.
While that allegation is unproven, the BCCLA has been forcing into the public domain disclosures from Communications Security Establishment, the highly secretive "signals intelligence" agency conducting such surveillance. But now, the federal government is fighting to move the case behind closed doors.

To get a sense of what's at stake, swipe back and forth on the following document, known as the CSE "metadata ministerial directive." This 2011 executive order effectively gave a legal green light to CSE surveillance.

The version on the left is what was released to The Globe following an Access to Information request. The version on right is a much more illuminating document, disclosed in court filings as part of the BCCLA lawsuit.

Jakarta Post
Cyberattacks in Indonesia rising at alarming rate
Friday, 03 June 2016
Byline: News Desk

Jakarta - Indonesia is in a cyberattack emergency amid a growing number of attacks over the past few years on account of a lack of cybersecurity, officials said on Friday.
Cyberattacks in Indonesia rose 33 per cent in 2015 from the previous year, Coordinating Political, Legal and Security Affairs Minister Luhut B. Pandjaitan said. From the figure, 54.5 per cent of the attacks were aimed at e-commerce-related websites, he said, adding that most of the attacks caused the systems to stop working.

"Indonesia experiences many cyberattacks every day and we don't have coordinated cyberdefence yet," he said in his office as reported by Antara news agency.

The government is setting up a National Cyber Agency to tackle cyber-related issues and also as part of its national policy on information technology defence.

National cyberspace desk head at the Office of the Coordinating Political, Legal and Security Affairs Minister, Agus Barnas, said the plan for the agency establishment had been initiated in January last year during the tenure of former coordinating minister Tedjo Edhy Wibowo.

However, there is detailed plan in place yet on when the National Cyber Agency will be officiated, Agus said.

"Various issues have been raised related to whether we need the new agency," he said without giving further details.

Indonesia is ranked second among countries where cyberattacks are launched and is the most prone to cyberattacks, according to data from the office of the coordinating minister.

"The most alarming fact is that in 2015 there was a fourfold increase in cybercrimes from 2014. The cybercrimes did not come from overseas, [the attacks] came from Indonesia with also domestic targets," Agus said as quoted by Antara.

Furthermore, Bank Indonesia also recorded an increase in cybercrimes, in the form of network misuse, with a rise of 66.7 per cent in 2015. The network misuse in financial transaction crimes were aimed at stealing financial data as well as passwords for logins, Agus said.

There were also cases of financial data manipulation, especially related to electronic transactions and the use of electronic payment systems, he added.

The office of the coordinating minister's cyberspace desk has conducted a thorough study from 2013 to assess the technical, legal and institutional sectors of cybercrimes.

The desk has also mapped the sectors and the authorities of government offices in managing cyber-related issues, which include cyberdefence, cybercrime, cyberinteligence, cybersecurity, cyberresilience and cyberdiplomacy.

New York Times
U.S. Subpoenas Huawei Over Its Dealings in Iran and North Korea
Friday, 03 June 2016
Byline: Paul Mozur

Hong Kong - Huawei Technologies has become China's most successful international technology company, in part by tapping markets as varied as Britain, India and Kenya.
But it also moved into markets like Syria, where American officials have imposed limits on sales of technology that could be used to commit human rights abuses, and into Iran, where sanctions have only recently been eased. And its presence in such countries is now coming under greater scrutiny.

The United States Commerce Department is demanding that the company, based in the south China city of Shenzhen, turn over all information regarding the export or re-export of American technology to Cuba, Iran, North Korea, Sudan and Syria, according to a subpoena sent to Huawei and viewed by The New York Times. The subpoena is part of an investigation into whether Huawei broke United States export controls.

Sent to Huawei's American headquarters in the Dallas suburb of Plano, the subpoena called for Huawei to turn over information related to shipments to those countries over the past five years. It also sought evidence of shipments to the countries indirectly through front or shell companies. The subpoena directed company officials to testify last month in Irving, Tex., or to provide information before then; it was not clear whether the meeting took place.

Huawei has not been accused of wrongdoing. In a statement, the company said it was committed to complying with laws and regulations where it operated. The document, which was issued by the Commerce Department office that investigates export violations, is an administrative subpoena, meaning it does not indicate a criminal investigation.

Still, the scrutiny over Huawei's dealings with those countries is emblematic of growing discord between the United States and China over control of global communications technology. It also illustrates how technology companies from both countries have been pulled into the high-stakes geopolitical contest over cybersecurity and the global management of the internet.

If the investigation finds that Huawei was acting counter to United States national security or foreign policy interests, it could limit the company's access to crucial American-made components and other tech products. Given Huawei's size and reach, that could affect the development of cellular networks and other large-scale technology infrastructure projects across the world.

"We do not comment with regard to ongoing investigations," a Commerce Department spokesman said.

The subpoena was issued after the United States briefly blocked in March sales of American technology to Huawei's smaller Chinese rival, ZTE, over similar concerns. As part of their move against ZTE, American officials released internal ZTE documents that showed the Chinese company used a rival's business efforts in those countries as a model. While the rival was not named in the documents, its description matched Huawei.

With the new investigation into Huawei, the United States is going after a much larger target. In 2014, Huawei reported revenue of about $60 billion, about four times that of ZTE. Depending on the measure, it ranks with Ericsson of Sweden as the world's largest supplier of the base stations and other equipment that make mobile telecommunications systems run.

Though the subpoena did not indicate whether any actions would be taken against Huawei, any major United States step to block the sales of American tech equipment to Huawei would have major implications for telecom networks across the world. Many of Huawei's products use American components or work with American technology.

Huawei has long benefited from access to easy credit from China's state-run lenders as it has expanded into areas where China seeks influence. But the company has drawn skepticism in the United States,

where officials have put an effective block on selling its telecom infrastructure equipment. China has used the move as a justification to push back against the market dominance of American companies like Cisco, IBM and Qualcomm in China.

Disclosures by the former American intelligence contractor Edward J. Snowden revealed that as the United States publicly raised concerns about the security of Huawei products, the United States National Security Agency was busy working to tunnel its own backdoor access into Huawei equipment and to snoop on Huawei's communications to look for links to the Chinese military.

Huawei has not shied from agreements that could draw criticism. In September, it signed a deal with Syria's Communications and Technology Ministry to help the country develop its communications networks.

Huawei's business in Iran has fallen under American criticism in the past. In 2011, Huawei said in a statement that it would voluntarily restrict the growth of its business in Iran. A year later, six American lawmakers wrote a letter to the State Department, calling for an investigation into whether Huawei was violating sanctions on Iran. Recently, the Congressional Research Service released a report that said that companies like Huawei appeared to have fulfilled pledges not to sell technology for blocking telecommunications in 2014.

Computer Weekly
MPs' private emails are routinely accessed by GCHQ
Thursday, 02 June 2016
Byline: Duncan Campbell, Bill Goodwin

London - GCHQ and the US National Security Agency (NSA) have access to intercepted emails sent and received by all members of the UK Parliament and peers, including with their constituents, a Computer Weekly investigation has established.
The intelligence agency in Cheltenham has been able to harvest traffic details of all parliamentary emails, including details of the sender, recipient and subject matter, for at least three years. As a result, details of private email correspondence between MPs and constituents are being collected by GCHQ as a matter of routine.

GCHQ documents classified above top secret, released by NSA whistleblower Edward Snowden, also reveal that the spy agency has the capability to scan the content of parliamentary emails for "keywords" through an established cyber defence network that is connected to commercial software used to filter spam emails from MPs' inboxes.

The disclosures, which come as the House of Commons prepares for the Third Reading of the government's controversial Investigatory Powers Bill on Monday 6 June, raise new questions over the sweeping powers to be granted in the bill to police and the security services.

The controversial decision by Parliament to replace its internal email and desktop office software with Microsoft's Office 365 service in 2014, means that parliamentary data and documents constantly pass in and out of the UK to Microsoft's datacentres in Dublin and the Netherlands, across the backbone of the internet.

Because files and emails leave the UK's borders in this way, they are automatically accessible to GCHQ's bulk interception system, Tempora. According to previously published Snowden documents, Tempora uses "probes" on commercial optical fibre cables crossing the Irish Sea and English Channel to harvest data.

Under existing law, GCHQ is permitted automatically to store datasets containing details of the senders, recipients and headings of all emails in and out of the UK, including internal UK-to-UK messages.

Computer Weekly has carried out a forensic analysis of hundreds of emails sent to the magazine or the writers from parliamentary email addresses, using "header" information within the emails to trace the route of the emails.

The study showed that most of the mail messages (65%) were routed internationally, through Dublin and the Netherlands. About one-third were relayed by Microsoft's new London datacentre. Cloud providers, such as Microsoft, use load-sharing procedures to distribute emails and data to more than one datacentre.

Every message also contained references to having been passed through clusters of scanning computers connected to GCHQ and located in the UK, France and Germany.

The NSA's Prism system offers access to all parliamentary documents and email through Microsoft Office 365 software, as a result of secret directives given to Microsoft under controversial US 2008 surveillance laws. The directives were implemented at the same time as Microsoft was selling its cloud system, Office 365, to the Houses of Parliament.

Since concerns were raised about the NSA's ability to access data stored by US technology companies, Microsoft has been rushing to build two new UK datacentres.

MPs' communications have been partially protected from interception for over 40 years under the "Wilson Doctrine", introduced by the former prime minister Harold Wilson in 1968. But this offered no protection to communications that leave the UK's borders, which are subject to automatic bulk collection by GCHQ.

"The House of Commons administration has serious questions to answer," according to former Home Office minister and Conservative MP David Davis. "On whose authority was 'consent' granted to view

members' emails? How did they manage to obtain that consent from every one of the 650 members whose constituents' confidentiality is affected?

"The government too has questions to answer as to why it did not explain this when asked on many occasions about the effect of the Wilson Doctrine," he added.

"The government should also make it clear to parliament the extent to which scanning of all mail by a US-controlled company has made Parliamentary communications vulnerable to agencies of a foreign power, namely the American NSA."

Labour deputy leader Tom Watson MP told Computer Weekly: "This will shock many of my parliamentary colleagues and provides a further illustration of why it is right for the government to give additional protections in law to MPs, lawyers and journalists. Theresa May has the opportunity to do this during the passage of the IP Bill in Parliament."

"There is no doubt that MPs, by virtue of their work, are more likely to be targeted by the UK's enemies. It is understandable that our security services want to takes steps to protect them, but any and all measures they introduce must be based on consent," he added.

SNP spokesperson Gavin Newlands MP said: "The SNP share the concerns that have been expressed over the partial removal of protection offered to privileged correspondence. It is of the upmost importance to any modern democracy that parliamentarians are able to communicate with constituents and advisers in complete confidence."

The MP's comments came as the home secretary, Theresa May, made last-minute concessions on the Investigatory Powers Bill to strengthen the Wilson Doctrine.

Under revisions announced on 1 June, the prime minister must in future give explicit approval for law enforcement agencies to hack into MP's computers and phones or to access their communications data.

Computer Weekly's investigation also confirmed that MPs' incoming and outgoing emails are automatically scanned through a network run by MessageLabs, a subsidiary of another US corporation, Symantec, which has been contracted by Parliament to provide services including spam filtering and malware detection.

MessageLabs provides GCHQ with direct access to parliamentary emails, through a secret cyber security network called Haruspex, according to GCHQ's "Cyber Defence Operations" legal policy instructions disclosed by Edward Snowden. The scanning system has been in operation for at least a decade. The documents reveal that Haruspex has been extended beyond "the detection, analysis and prevention of network-based attacks" against government computer systems, to allow it to be used to report other activities, provided they are in the interests of "national security" - a concept the government has refused to define.

Members of the Scottish National Party and Labour Party, who have scrutinised the Investigatory Powers Bill, have criticised the government for misusing "national security" to justify surveillance operations against trade unionists and critics of the police.

The MessageLabs scanning system, used on all emails to and from Parliament, can be programmed to detect keywords as well as to look for malicious attachments or spam. MPs and peers have not been told about the MessageLabs system, nor specifically asked for permission for their emails to be scanned in this way.

Computer Weekly put a series of questions to Symantec, the US corporation that supplies the MessageLabs service, about the role of MessageLabs in Parliament and its links to Haruspex. A spokesperson said: "Symantec has legal non-disclosure agreements with all of our customers and, as a result, cannot discuss specific cases."

Parliament began the path to an updated IT system that ultimately left MPs' emails and documents exposed to greater risks of surveillance from the UK and US intelligence services in May 2013.

Joan Miller, then the director of Parliamentary ICT (PICT), told the House of Lords management board: "Office 365 had a slightly higher risk relating to data sovereignty, but Microsoft's and the House's lawyers...felt that the chance of the risk materialising was low."

Less than a month later the Guardian revealed the Snowden document leak and the existence of the NSA's Prism programme, which requires US companies, including Microsoft, to build systems to allow the NSA and the FBI to access, on-demand, their customers' messages and files, including documents held in cloud datacentres.

Within a week, Miller told Parliament's management board that "PICT had reviewed its advice on data sovereignty and cloud computing following news stories about PRISM and was content that the risk was unchanged."

"We didn't think there was no risk, we thought it was a low risk [in 2013]," she told Computer Weekly. Asked if "UK parliamentary data may end up being requisitioned by the NSA", she said: "We did consider that, yes."

Miller, who retired as director of parliamentary IT in 2014, told Computer Weekly that Microsoft claimed to have doubts over the legality of the secret orders issued by the US government to obtain data under Prism and would be prepared to challenge it in court.

Microsoft is currently fighting a US federal court order to hand over customer email data stored in its Dublin datacentre in connection with an investigation into drugs trafficking. "It is taking legal action

against the US government, after being served 2,576 secret legal demands in a year, effectively silencing Microsoft from speaking to customers about warrants or other legal processes affecting their data."

Microsoft's president and chief legal officer, Brad Smith, visited Parliament in person to offer reassurances over the sovereignty of parliamentary data, as negotiations over Office 365 were underway, Miller revealed.

In 2014, then leader of the House of Commons William Hague was forced to reassure MPs about the security of their emails after an MP raised concerns that US authorities could gain access to Microsoft's European datacentres.

Miller said she also received reassurances that GCHQ would not abuse its access to monitor MPs' communications, which might include emails to MPs from constituents passing on sensitive information or blowing the whistle on wrong-doing or corruption.

"GCHQ is quite clear, every time I have spoken to them, that they follow the law. It would not be lawful for them to look at those emails. That sounds a bit naive, I don't think it is," she said. MPs are concerned that current laws place no restriction on the use of interception, when this is allegedly carried out with "consent".

At the same time as Microsoft was negotiating the sale of Office 365 to Parliament, the supplier was arranging for its cloud storage system, then called SkyDrive, to be connected to Prism, to allow the US to obtain foreign intelligence, documents from Edward Snowden revealed.

An NSA information bulletin, dated 7 March 2013 and marked "Top Secret - No Foreign Dissemination", boasted that Microsoft's SkyDrive system had been open to full NSA inspection, including Word, PowerPoint and Excel files.

"Fundamentally, the decision to move to [Office] 365 sits on the sensitivity of the data that we were looking at and the risk that we felt, and combining those together, but the business decision was that it was an acceptable risk," said Miller.

Miller told Computer Weekly that she believed MPs would have been made aware of security risks, and asked to agree to the interception. She said, having retired, she could not refer to any current documents.

Computer Weekly has obtained copied of the 2015 "acceptable use" agreement for parliamentary digital services and signed by MPs and peers, and also the 2015 Members' Handbook. Neither document warns MPs that their incoming and outgoing mails are scanned for keywords by the US-owned MessageLabs network that has links to the intelligence services.

All MPs are given a "parliament.uk" email address, although many also use private email addresses for non-parliamentary work. MPs and peers contacted by Computer Weekly said they had not been told about the potential security risks of using parliamentary email and the Office 365 system.

A Microsoft spokesperson declined to comment to Computer Weekly, saying only: "Due to client confidentiality, Microsoft does not disclose the terms of any of our customer agreements."

Global Times
Illegal mapping 'serious' in western China
Friday, 03 June 2016
Byline: Li Ruohan

Beijing - Illegal mapping is a "serious" problem in remote areas of western China, according to five annual announcements on typical illegal mapping practices released by the National Administration of Surveying, Mapping and Geoinformation (NASG).
Most of those areas are underprivileged and lack sufficient mapping information, and they are often targeted by espionage because many key national defense and military facilities are stationed there, Zhao Kangning, former deputy director of China's National Administration of Global Navigation Satellite Systems and Applications, told the Global Times.

The disclosure of detailed geographic information related to defense or military facilities leaves them open to threats of attack, as many modern military devices are capable of conducting long-range precise attacks, military experts previously told the Global Times.

According to NASG, the most frequent unlawful actions are unauthorized mapping and the processing or printing of "problematic maps," which contain information that is wrong or that is classified to protect national security, China's National Defense News reported Wednesday.

Of the seven examples of illegal mapping cases revealed by the NASG in April, three involved unauthorized mapping, including an April 2015 case in which six Taiwanese illegally entered a closed military area in Hami, Northwest China's Xinjiang Uyghur Autonomous Region to collect geographic information.

One of the Taiwanese was fined 30,000 yuan ($4,560) after he was found to have used GPS receivers in the mainland to collect 35,207 sets of geographic coordinates from seven provinces and cities since 2009, according to the NASG's announcement.

China's National Defense News reported that the illegal obtainment of geographic information by overseas organizations and individuals is common, particularly in Xinjiang, Northwest China's Shaanxi Province, Northeast China's Liaoning Province and Northeast China's Jilin province.

"Shaanxi has captured many overseas individuals that conducted illegal mapping in recent years, and illegal mapping is on the rise," a Shaanxi Administration of Surveying, Mapping and Geoinformation official told the newspaper.

The official claimed that many foreigners and associates of foreign organizations pretend to travel, investigate water resources, hike or conduct archaeological studies in order to target national defense projects and military facilities.

A Japanese national was deported in 2011 after being caught illegally surveying and mapping in Shaanxi Province. The government of Yunnan Province also investigated Coca- Cola for illegally mapping part of the province using electronic devices in 2013, according to previous reports.

Xu Yitian, an expert at the National University of Defense Technology, was quoted by the newspaper as saying that the leaks of geographic information and cases of illegal mapping that have occurred in recent years were mainly due to a lack of national autonomy over the collection, supervision and application of data needed for mapping.

According to the NASG report, domestically produced geographic information technologies and equipment account for over 50 percent of those available in China, but the long way to go to realize autonomous control presents a potential danger that cannot be overlooked.

Reuters
Bangladesh Bank heist perpetrators may never be identified
Tuesday, 07 June 2016

Dhaka - A former top US intelligence official on cyber security has warned that government investigators may never be able to ascertain who carried out a cyber heist that led to the theft of $81 million from Bangladesh's central bank in February.
Sean Kanuck, who was the most senior official in charge of cyber security at the Office of the Director of National Intelligence for five years until mid-May, told Reuters that there had been no official determination on who committed the cyber heist, one of the biggest ever.

"They may never be able to make one," Kanuck said on the sidelines of the annual Shangri-La Dialogue, Asia's premier security forum, held at the weekend in Singapore. He said he had some knowledge of the case but was not directly involved in the probe.

Investigations into the heist are being coordinated by the US Federal Bureau of Investigation. The authorities in Bangladesh, the Philippines and some other countries are also carrying out inquiries.

The hackers stole money from Bangladesh Bank's account at the New York Federal Reserve. One fraudulent transfer to a Sri Lankan entity was reversed, but four transfers for a combined $81 million went to the Philippines and wound up being laundered through casinos and casino agents there.

Most of the money remains missing. Kanuck said that he believed either an extremely sophisticated criminal group or a rogue nation carried out the theft.

BAE Systems has said malware used to erase the tracks of hackers in the Bangladesh Bank heist was similar to code used to attack Sony Corp in 2014, a strike blamed by the FBI on North Korea.

"We have actually seen criminal enterprises that were able to bring together a range of capabilities, ranging from insider access to credentials, going through to people who were willing to go physically remove money from ATMs," said Kanuck.

"There is a black market for different capabilities and you can actually assemble a team like in Ocean's 11," he said, referring to the Hollywood movie about a crime syndicate robbing Las Vegas casinos.

"On the other side of the table, you have a growing number of nation-states developing very broad capabilities to do different kinds of operations," Kanuck said. "The water is very muddy, it's very complex."

Such states could be seeking to undermine the credibility of a central bank, or looking for hard currency funds, Kanuck added.

But Kanuck warned of deceptive signals from those involved in such a heist. "An analyst or an investigator would need to consider that nation states may try to make their activity look like it's the work of criminals," he said.

"And criminals might also try to make their activity look like it's the work of nation-states or even ideologically motivated cyber actors."

Gulf News
UAE face growing cyber security risk
Tuesday, 07 June 2016
Byline: Cleofe Maceda

Dubai - Given the vast number of virtual payment and banking options, UAE consumers are increasingly going online to shop and transact with their bank. Recent data show that more than half of residents in the country access the internet to make purchases alone.
But while you might think that buying clothes on the internet or swiping your credit card at a coffee shop is now more secure than ever, think again. According to security experts, cyber criminals are becoming aggressive in finding ways to access your personal data in order to steal your money.

Mohammed Abukhater, regional director for Middle East and Africa at FireEye, a payment and cyber security intelligence company, cautioned that with the proliferation of mobile devices and expansion of banking services, banks and other financial organisations in the GCC are facing the biggest threat these days.

"Online banking services and online shopping portals, as well as credit cards and debit cards, are potentially at risk," Abukhater told Gulf News. "Organisations would be well-advised to think ahead and have a strong cyber defence infrastructure in place to combat a new wave of threats by a new generation of savvy attackers."

There haven't been any major security breaches reported publicly by financial institutions in the UAE, but this doesn't mean consumers have not lost any money to cyber criminals. "This doesn't mean that there haven't been financially damaging attacks in the GCC," said Abukhater.

"Around the world, bank breaches often go unreported to regulators and the wider public because the losses are not deemed material. That doesn't mean they're not a significant problem."

According to Norton by Symantec, at least 2 million residents in the country reported having experienced cybercrime in one year and lost Dh4.9 billion in the process.

The Gulf Cooperation Council region is considered an energy powerhouse and it has established itself as a hub for finance, aviation, retail, tourism and real estate. This makes the region attractive to cyber criminals.

"This has made entities and governments in the region an enticing target for myriad cyberattackers and threat groups, who often go after financial resources, intellectual property and crippling critical infrastructure, " said Abukhater. "Geopolitics are also another factor behind the region drawing the attention of cyber attackers."

The Online Shopping Behaviour study released by MasterCard in 2015 showed that a growing number of consumers is relying on the internet for their shopping needs. Most people go online to buy air tickets, book hotels and get the latest gadgets and clothes.

"Online is quickly becoming the norm for more shoppers in the UAE due to the high level of awareness amongst consumers about the convenience, speed and safety of their transactions," said Aaron Oliver, head of emerging payments for Middle East and Africa at MasterCard.

The Hindustan Times
Now, mobile apps come under Cyberdome scanner to check malware threats
Tuesday, 07 June 2016

Kozhikode - Beware of mobile apps. Kerala Police's Cyberdome has launched a thorough screening of the apps after it was found that Pakistan's ISI has been uploading malwares in apps to steal vital information from the smartphones which are downloading it.
Generally an alert has been issued among the senior officers in the police, defence and other security agencies to be wary of such apps as downloading of such apps will compromise the data and information stored in phone, emails and other folders. "We are aware of the development and Cyberdome is scanning such apps hosted by ISI to spy on security agencies," said Thiruvananthapuram Range Inspector General Manoj Abraham, who is the nodal officer of the Cyderdome.

As per a Ministry of Home Affairs (MHA) report, Pakistan intelligence agencies are spying on Indian security forces by sending malwares in gaming, music, video and entertainment apps. The apps so far detected include game app-Top Gun, music app-mpjunkie, video app-vdjunky and entertainment app-talking frog.

According to cyber wing officers, though Google has been taking action to remove such apps from the store, a few malwares continue to evade surveillance and infect the apps. Recently, Google removed 13 apps from Play Store following alerts from cyber security agencies.

Officers warn that the users should download apps only from trusted sources as the malwares in the apps would automatically download programmes in the phone which will get all the data stored in the

phone mainly targetting emails, phone banking apps and contacts. Installing anti-virus and scanning the phones is the only way to ensure security of the data.

What to do if your device gets infected with malware? Put the device in safe mode, remove its administrator status and then uninstall the app. Also go for factory reset to clear the infection.

The Register (UK)
The Fog of Cyberwar: Now theft and sabotage instead of just spying
Tuesday, 07 June 2016
Byline: John Leyden

London - Cyber-conflict between nations has entered a new phase with a switch from espionage to sabotage and theft, according to infosec guru Mikko Hyppönen.
The BlackEnergy-related attacks on the electricity grid last December and the more recent attack on at least four international banks have upped the ante in the sphere of cyber-conflict, according to F?Secure's chief research officer.

Russia and North Korea, respectively, are the chief suspects in the two campaigns. Hyppönen said the attacks mark an escalation in a "cyber arms race" which he compares to the Cold War nuclear arms race.

"We've switched from cyber-espionage to offensive cyber action," Hyppönen told El Reg. "The cyber arms race is just beginning and it's going to get much worse."

"Ukraine was a game changer: the first offensive cyber action. The SWIFT attacks were about stealing money rather than secrets," he added.

Hackers tried to steal $1bn through the SWIFT attacks and successfully robbed $81m from funds held by the biggest victim, the central bank of Bangladesh.

"This tells us how desperate North Korea is," according to Hyppönen.

Hyppönen said that in some way, the cyber arms race might be more dangerous than previous arms races. We knew who had nuclear warheads and how many, but we don't know who has the biggest cyber capability.

US, Israel, Russia in that order probably have the greatest offensive capability in cyberspace, but we don't know the abilities of other nations, according to Hyppönen. Worse yet there's no deterrence, and hacking or planting malware on enemy systems can be both effective and cheap.

"When someone used a B-52 to drop bombs, the victim knew pretty well where it came from, but cyber attacks give an adversary deniability," according to Hyppönen.

International law experts have worked hard to put together a Geneva convention for cyberconflict, in the shape of the Tallinn Manual. Hyppönen praised these efforts as "ground-breaking," while cautioning that they've yet to be tested practically.

Many experts describe the infamous Student worm of 2010 as the first cyber weapon and the attacks on Estonia in 2007 as the first conflict. For Hyppönen, however, we ain't seen nothing yet.

The Intercept
Facing Data Deluge, Secret U.K. Spying Report Warned of Intelligence Failure
Tuesday, 07 June 2016
Byline: Ryan Gallagher

Washington - A secret report warned that British spies may have put lives at risk because their surveillance systems were sweeping up more data than could be analyzed, leading them to miss clues to possible security threats.
The concern was sent to top British government officials in an explosive classified document, which outlined methods being developed by the United Kingdom's domestic intelligence agency to covertly monitor internet communications.

The Security Service, also known as MI5, had become the "principal collector and exploiter" of digital communications within the U.K., the eight-page report noted, but the agency's surveillance capabilities had "grown significantly over the last few years."

MI5 "can currently collect (whether itself or through partners ...) significantly more than it is able to exploit fully," the report warned. "This creates a real risk of 'intelligence failure' i.e. from the Service being unable to access potentially life-saving intelligence from data that it has already collected."

A draft copy of the report, obtained by The Intercept from National Security Agency whistleblower Edward Snowden, is marked with the classification "U.K. Secret" and dated February 12, 2010. It was prepared by British spy agency officials to brief the government's Cabinet Office and Treasury Department about the U.K.'s surveillance capabilities.

Notably, three years after the report was authored, two Islamic extremists killed and attempted to decapitate a British soldier, Lee Rigby, on a London street. An investigation into the incident found that the two perpetrators were well- known to MI5, but the agency had missed significant warning signs about the men, including records of phone calls one of them had made to an al Qaeda- affiliated radical in Yemen, and an online message in which the same individual had discussed in graphic detail his intention to murder a soldier.

The new revelations raise questions about whether problems sifting through the troves of data collected by British spies may have been a factor in the failure to prevent the Rigby killing. But they are also of broader relevance to an ongoing debate in the U.K. about surveillance. In recent months, the British government has been trying to pass a new law, the Investigatory Powers Bill, which would grant MI5 and other agencies access to more data.

Silkie Carlo, a policy officer at the London-based human rights group Liberty, told The Intercept that the details contained in the secret report highlighted the need for a comprehensive independent review of the proposed new surveillance powers.

"Intelligence whistleblowers have warned that the agencies are drowning in data -- and now we have it confirmed from the heart of the U.K. government," Carlo said. "If our agencies have risked missing 'life-saving intelligence' by collecting 'significantly' more data than they can analyze, how can they justify casting the net yet wider in the toxic Investigatory Powers Bill?"

The British government's Home Office, which handles media requests related to MI5, declined to comment for this story.

"Lack of staff and tools"

The leaked report outlines efforts by British agencies to conduct both "large- scale" and "small-scale" eavesdropping of domestic communications within the U.K. It focuses primarily on an MI5 program called DIGINT, or digital intelligence, which was aimed at transforming the agency's ability to covertly monitor internet communications.

DIGINT was established for counterterrorism purposes, and "more generally for wider national security purposes," the report said. The program was described as being focused on "the activities of key investigative targets, and on those exploitation activities that will drive greatest investigative benefits with respect to U.K. domestic threats."

The amount of data being collected, however, proved difficult for MI5 to handle. In March 2010, in another secret report, concerns were reiterated about the agency's difficulties processing the material it was harvesting. "There is an imbalance between collection and exploitation capabilities, resulting in a failure to make effective use of some of the intelligence collected today," the report noted. "With the exception of the highest priority investigations, a lack of staff and tools means that investigators are presented with raw and unfiltered DIGINT data. Frequently, this material is not fully assessed because of the significant time required to review it."

The problem was not unique to MI5.

Many of the agency's larger-scale surveillance operations were being conducted in coordination with the National Technical Assistance Centre, a unit of the electronic eavesdropping agency Government Communications Headquarters, better known as GCHQ.

The Centre plays a vital but little-known role. One of its main functions is to act as a kind of intermediary, managing the highly sensitive data-sharing relationships that exist among British telecommunications companies and law enforcement and spy agencies.

Perhaps the most important program the Centre helps deliver is code-named PRESTON, which covertly intercepts phone calls, text messages, and internet data sent or received by people or organizations in the U.K. who have been named as surveillance targets on warrants signed off by a government minister.

A top-secret 2009 study found that, in one six-month period, the PRESTON program had intercepted more than 5 million communications. Remarkably, 97 percent of the calls, messages, and data it had collected were found to have been "not viewed" by the authorities.

The authors of the study were alarmed because PRESTON was supposedly focused on known suspects, and yet most of the communications it was monitoring appeared to be getting ignored -- meaning crucial intelligence could have been missed.

"Only a small proportion of the Preston Traffic is viewed," they noted. "This is of concern as the collection is all warranted."

"Politically contentious"

For most of the last decade, successive British governments have attempted to obtain more surveillance powers, but their efforts have met with public opposition and ultimately failed. The present government's effort to push through a sweeping surveillance law -- the Investigatory Powers Bill -- is currently being considered by the Parliament.

Documents provided by Snowden show that the U.K.'s intelligence and security agencies have wanted to obtain new powers to store domestic data about internet communications to address the "growing range of services available to internet users." This reflects the position that has been adopted publicly in recent years by the government, which has argued that expanded internet surveillance is necessary to keep up with changes in technology.

However, the Snowden documents also reveal a more candid internal assessment of the need for bolstered spy laws and shine light on major aspects of the U.K.'s existing surveillance apparatus that government and security officials have not publicly acknowledged in their pursuit of the new powers.

In one document dated from 2012, GCHQ stated that it was "not dependent" on a new surveillance law coming into force, presumably due to the extensive capabilities already at its disposal. GCHQ added that

new powers were of greater importance to the U.K.'s law enforcement agencies, which were facing "a significant decline" in ability to intercept communications due to people increasingly using internet services -- as opposed to conventional landlines and cellphones -- to talk or exchange messages.

But passing a new surveillance law would be a "politically contentious [and] technically complex" process, GCHQ said in the document. In the meantime, therefore, it devised something of a workaround by creating a secret stop-gap surveillance solution for law enforcement officials.

As part of a program named MILKWHITE, GCHQ made some of its huge troves of metadata about people's online activities accessible to MI5, London's Metropolitan Police, the tax agency Her Majesty's Revenue and Customs, the Serious Organized Crime Agency (now merged into the National Crime Agency), the Police Service of Northern Ireland, and an obscure Scotland-based surveillance unit called the Scottish Recording Centre.

Metadata reveals information about communications -- such as the sender and recipient of an email, or the phone numbers someone called and at what time -- but not the written content of the message or the audio of the call. GCHQ's definition of metadata is broad and also encompasses location data that can be used to track people's movements, login passwords, and website browsing histories, as The Intercept has previously revealed.

The MILKWHITE program was developed as early as September 2009, and it seems to have been operational under both the Labour and the Conservative-Liberal Democrat governments of that period. One of its purposes was to allow law enforcement agencies and MI5 to sift through the troves of metadata to discover internet "selectors" for their surveillance targets -- meaning unique identifiers, such as a username or IP address, that can be used to home in on and monitor a person's online activities.

GCHQ focuses primarily on intercepting foreign communications that are "external" to the U.K. But in the process of doing so -- by tapping into international cables that carry phone calls and internet traffic between countries -- the agency vacuums up large quantities of data on British calls, emails, and web browsing habits, too. It is this British data -- some of which appears to have been made accessible through MILKWHITE -- that would be of most interest to MI5, police, and tax officers, as it is their role to conduct "internal" investigations within the U.K.

A GCHQ document dated from late 2010 indicated that MILKWHITE was storing data about people's usage of smartphone chat apps like WhatsApp and Viber, instant messenger services such as Jabber, and social networking websites, including Facebook, MySpace, and LinkedIn. Access to the data was provided to law enforcement through an "internet data unit" hosted by the Serious Organized Crime Agency and it was accessible to tax investigators through what one GCHQ document described as established "business as usual" channels.

By March 2011, GCHQ noted that there was "increasing customer demand" for the service offered by MILKWHITE and the agency planned to grow its capacity, seeking £20.8 million ($30.6 million) to update the program's "advanced analytics" capabilities and to maintain its "bulk" storage of metadata records. "Bulk" is a term GCHQ uses to refer to large troves of data that are not focused on individual targets; rather, they include millions and in some cases billions of records about ordinary people's communications and internet activity.

Carlo, the policy analyst with Liberty, said the revelations about MILKWHITE suggested members of Parliament had been misled about how so-called bulk data is handled. "While MPs have been told that bulk powers have been used only by the intelligence community, it now appears it has been 'business as usual' for the tax man to access mass internet data for years," she said. "This vindicates the warnings of security experts and the call by opposition parties for an urgent, independent review of bulk powers. The compromise review recently announced is a poor substitute and without the time and technical expertise, will struggle to address this issue of national importance."

GCHQ declined to answer questions for this story. A spokesperson for the agency said in a statement: "It is long-standing policy that we do not comment on intelligence matters. Furthermore, all of GCHQ's work is carried out in accordance with a strict legal and policy framework, which ensures that our activities are authorized, necessary and proportionate, and that there is rigorous oversight, including from the Secretary of State, the Interception and Intelligence Services Commissioners and the Parliamentary Intelligence and Security Committee. All our operational processes rigorously support this position. In addition, the U.K.'s interception regime is entirely compatible with the European Convention on Human Rights."

USA Today
Power execs rebuff Koppel claims of eventual attack on U.S. grid
Tuesday, 07 June 2016
Byline: Bill Loveless

Washington - Eight months after veteran broadcast journalist Ted Koppel published a book predicting a devastating cyberattack on the U.S. power grid, leaders of the utility industry are sounding off over what they say is an exaggerated claim.
"We're speaking out on it now because we think there is an important story to tell," Scott Aaronson, the managing director for cyber and infrastructure security at the Edison Electric Institute, said last week at a briefing for reporters. "If it's only going to be the movie- script scenarios, then I can understand why customers might lose confidence."

What Aaronson and others in the utility industry are taking issue with is a warning by Koppel in his bestselling book, Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath.

According to Koppel, who anchored the ABC news program Nightline from 1980 to 2005, the U.S. is likely to eventually suffer a cyberattack on its grid that could leave millions of Americans in the dark, short of water and food, and generally desperate for months.

The risk is considerable, Koppel claims, because the U.S. government and the utility industry are ill prepared to fend off such an assault by foreign adversaries and to help the nation recover from it.

Not so, Aaronson told reporters.

"Part of what we want to do is interject a little bit of sanity and engineering and thoughtfulness into what can quickly devolve into a bit of a hysterical discussion," he said at the Washington headquarters of EEI, the trade association for investor-owned electric utilities.

As he did at recent House and Senate hearings on cybersecurity, Aaronson ticked off a number of steps taken by utilities and the government to address the threat, including standards requiring stepped-up protective measures and carrying penalties of up to $1 million per violation per day.

Moreover, utilities are increasingly coordinating to share information and expertise and to test their preparedness, including a drill conducted last fall by the industry's North American Electric Reliability Corporation, in which 4,400 participants from the industry and governments in the U.S., Canada and Mexico simulated coordinated cyber and physical attacks on the grid.

In the event of an incursion that disables electric infrastructure, power providers are expanding programs to share transformers and other equipment and replace damaged equipment relatively quickly, Aaronson said.

"I disagree with the premise that we would be in a situation where we would have to deal with a months-long outage that would require people to shelter in place," he said.

As a sign of that resiliency, Aaronson recalled an attack on Pacific Gas & Electric's Metcalf substation south of San Jose in 2013 by unidentified snipers. The attack left 17 of the facility's 21 transformers destroyed and caused $15 million in damage.

"The lights didn't even blink in San Francisco and Silicon Valley," he said, adding that the substation was back in service in just over a month. Nevertheless, Koppel remains unpersuaded by the industry's criticism of his book.

"It is surely only a matter of time before a terrorist group, unrestrained by any geopolitical interests, acquires the capability to attack one of our power grids," he testified at a Senate hearing in May where Aaronson also appeared.

There's no dispute in the industry or the government that hackers want to disrupt power supplies and cause havoc in the U.S. In fact, the National Security Agency has acknowledged that "cyber intrusions" on control systems for the grid have increased, though none has caused a blackout.

But what Aaronson and his colleagues in the utility sector are trying to convey more now than before is that while there will always be room for improvement in addressing the risk, it isn't going unattended.

"You've got to be a little sensitive about how much you talk about it publicly," said Philip Moeller, EEI's senior vice president of energy delivery and a former member of the Federal Energy Regulatory Commission, who joined Aaronson at the press briefing.

"Particularly in the aftermath of Metcalf, we didn't want copycat attacks, which are much more likely to happen once it's in the headlines. But just because we don't talk about it doesn't mean a lot isn't being done."

Washington Free Beacon
Cybercom Trains for Infrastructure Attack as Power Companies Play Down Threat to Grid
Monday, 06 June 2016
Byline: Bill Gertz

Column - The U.S. Cyber Command will conduct large-scale military exercises this week simulating cyber attacks against critical U.S. infrastructure, and the war games will highlight the growing threat posed by foreign states capable of crippling the electrical grid and financial networks through digital attacks.
The exercise, known as Cyber Guard 16, is the latest annual war game involving scores of military personnel and civilians at the Fort Meade-based command. Other players will include officials from the Pentagon, FBI, Homeland Security Department, and private industry.

"Cyber Guard offers a fascinating, realistic (but not predictive) scenario of a cyber attack of significant consequence on U.S. critical infrastructure," Maj. Gen. Paul Nakasone, head of the command's National Mission Force, said last week.

Nakasone, whose mission team is tasked with defending military networks, also is in charge of the military unit that would be called in to counter and respond to a cyber attack on elements of critical infrastructure.

The month-long exercise is an example of both interagency security cooperation as well as working with private sector stakeholders in dealing with cyber threats, he told Federal News Radio in an online chat.

A command spokesman declined to provide details on the Cyber Guard exercise and referred questions to a fact sheet produce for last year's version. The exercise ends June 29. Last year, 100 organizations

from government, academia, industry, and allied nations took part at the Joint Staff Suffolk Complex, a high-security war-gaming facility in Suffolk, Va.

The command's cyber warfare game comes amid concerns that the federal government is not doing enough to protect the electrical grid, arguably the most critical of the 16 different elements of critical infrastructure, as most other elements require electricity to operate.

Currently, the federal government is relying on a private consortium of companies that appears to be playing down threats to the power grid from cyber and other attacks.

The non-profit North American Electric Reliability Corporation is the official organization designated by the federal government to be in charge of setting security standards for electrical networks. It is responsible for making sure electrical owners and operators of the bulk power system are taking the steps needed to protect the lattice of power companies stretching throughout the United States, Canada, and Baja California, Mexico.

The private regulatory authority was given the task of setting grid security standards by the Federal Energy Regulatory Commission, or FERC. Testimony before the commission last week reveals that current industry standards for reporting cyber security incidents are allowing power companies to game the system to underreport potential attacks.

In 2014, for example, the non-profit corporation reported only three cyber security incidents, and a draft of the forthcoming annual reliability report is said to report zero incidents.

The consortium's low numbers conflict sharply with those of the Department of Homeland Security's Industrial Control Systems Cyber Emergency Readiness Team that monitors infrastructure cyber incidents.

According to the DHS group, 46 cyber security incidents were reported in 2015, and 79 were reported the year before that. The department did not differentiate which energy sectors were involved in the cyber incidents but it is likely electric companies were among the targets in the numerous incidents.

Incidents involving electricity companies have included hacks into smart meters to steal power, failure in control systems that forced power plants to shut down, and malicious software that disabled safety monitoring systems.

"Clearly there is a gap in [North American Electric Reliability Corporation] cyber security incident reporting; this gap should be addressed by more stringent FERC-mandated reporting standards," said Tom Popik with the Foundation for Resilient Society, a group that advocates for better grid security.

In April, Cybercom commander Adm. Mike Rogers voiced doubts about whether the command could help the country from multiple cyber attacks against the electrical power grid.

The danger was highlighted by the first known successful cyber attack against a nation's power grid in December. Following the attack, which targeted Ukraine, the FBI in March began briefing American electric power companies on the threat to the U.S. power grid.

"We have the skills. The challenge for us at the moment is one of capacity," Rogers said, noting a current shortage of skilled people could hamper efforts "if we had multiple events simultaneously."

Rogers noted that the electrical power industry and a couple of others in charge of critical infrastructure are resisting efforts to bolster cyber defenses since doing so would require rate increases.

That seems to be one factor motivating the North American Electric Reliability Corporation to undercount in its reporting of cyber incidents.

A congressional General Accountability Office report states that since 2011 the Federal Energy Regulatory Commission has not been checking private electric companies to ensure they are complying with voluntary cyber security standards. The report recommended that the commission begin conducting periodic evaluations of security compliance. "However, FERC has not implemented this recommendation," the GAO said in November.

"As they become increasingly reliant on computerized technologies, the electricity industry's systems and networks are susceptible to an evolving array of cyber-based threats," the report said.

The problem is not simply potential increased costs for cyber security by electric companies. Opposition within private industry to tightening cyber security of electric grid control networks also is the result of concerns over the large operational costs involved in shutting down power systems to hunt for and remove malicious software.

The dangers to the nation's electric security are too great and protecting the most critical of infrastructures is too important. The Federal Energy Regulatory Commission should require power companies to invest in better cyber security--before a major cyber attack turns out the lights.

Washington Post
FBI wants access to Internet browser history without a warrant in terrorism and spy cases
Tuesday, 07 June 2016
Byline: Ellen Nakashima

Washington - The Obama administration is seeking to amend surveillance law to give the FBI explicit authority to access a person's Internet browser history and other electronic data without a warrant in terrorism and spy cases.

The administration made a similar effort six years ago but dropped it after concerns were raised by privacy advocates and the tech industry.

FBI Director James B. Comey has characterized the legislation as a fix to "a typo" in the Electronic Communications Privacy Act, which he says has led some tech firms to refuse to provide data that Congress intended them to provide.

But tech firms and privacy advocates say the bureau is seeking an expansion of surveillance powers that infringes on Americans' privacy.

Now, at the FBI's request, some lawmakers are advancing legislation that would allow the bureau to obtain "electronic communication transactional records" using an administrative subpoena known as a national security letter. An NSL can be issued by the special agent in charge of a bureau field office without a judge's approval.

Such records may include a person's Internet protocol address and how much time a person spends on a given site. But they don't include content, such as the text of an e-mail or Google search queries. There's also a limit to how much visibility the bureau would have into which part of a website a person had visited. For instance, according to the bureau, if the person went to any part of The Washington Post's website, law enforcement would see only washingtonpost.com -- nothing more specific.

Comey said that making this change to the law is the bureau's top legislative priority this year.

The inability to obtain the data with an NSL "affects our work in a very, very big and practical way," he told the Senate Intelligence Committee in February.

The Senate panel recently voted out an authorization bill with the NSL amendment. The Senate Judiciary Committee this week is considering a similar provision introduced by Sen. John Cornyn (R-Texas) as an amendment to ECPA, a law governing domestic surveillance.

Cornyn said that what he characterized as a "scrivener's error" in the law is "needlessly hamstringing our counterintelligence and counterterrorism efforts."

But privacy groups and tech firms are again warning that the expansion of power would erode civil-liberties protections.

The fix the FBI seeks would "dramatically expand the ability of the FBI to get sensitive information about users' online activities without oversight," said a coalition of privacy and civil society groups and industry organizations in a letter sent to the Hill Monday.

The new categories of information that could be collected using an NSL "would paint an incredibly intimate picture" of a person's life, said the letter, signed by the American Civil Liberties Union, Amnesty

International USA, the Computer & Communications Industry Association, Google, Facebook and Yahoo, among others. For example, a person's browsing history, location information and certain email data could reveal details about a person's political affiliation, medical conditions, religion and movements throughout the day, they said.

In addition, the NSL would come with a gag order preventing the company from disclosing it had a received a government request, said Neema Singh Guliani, ACLU legislative counsel. The letter noted that over the past 10 years, the FBI has issued more than 300,000 NSLs, most of which had gag orders. "That's the perfect storm of more information gathered, less transparency and no accountability," Gulani said.

But a law passed last year, the USA Freedom Act, requires the Justice Department to review gag orders periodically to assess whether they are still justified.

The amendment being considered Thursday by the Judiciary Committee is part of a broader effort by lawmakers to update ECPA to require law enforcement to get a warrant for all email content, regardless of whether it is one day or one year old.

Privacy groups and tech companies support the broader ECPA update, versions of which some lawmakers have sought for years.

But the groups and tech organizations in their letter said that if the ECPA bill includes the NSL provision, they will pull their support.

A November 2008 opinion from the Justice Department's Office of Legal Counsel made clear that ECPA allows the FBI to obtain with an NSL only four types of basic subscriber information from Internet companies: name, address, length of service and telephone bill records. There is no reference in the law to browser history, for instance. The opinion said the four existing categories were "exhaustive."

The FBI's Office of General Counsel, however, has argued that electronic communication transactional records are the functional equivalent of telephone billing records. To eliminate any uncertainty, the FBI wants the law to explicitly cover such data.

Sens. Patrick J. Leahy (D- Vt.), the ranking minority-party member on the Judiciary Committee, and Mike Lee (R-Utah), a committee member, oppose the Cornyn amendment. They say they will push for a clean version of the ECPA update similar to a bill passed by the House earlier this year.

Globe and Mail
Digital Hostage
Thursday, 09 June 2016
Byline: Bertrand Marotte

What is ransomware?
Ransomware is a type of hostile computer program known as malware that blocks users from some or all of the data in their computer systems. The more advanced form of ransomware is known as crypto-ransomware, which encrypts computer files such as documents, pictures and music, allowing the attacker to demand a ransom in exchange for the necessary decrypt key to unlock the data.

How does ransomware get in?

There are a variety of ways in which ransomware can break into an individual's personal computer or mobile phone, or into a company or organization's computer system. Ransomware can infiltrate with the simple click on a link contained in a mass e-mail to employees of a company. In one documented incident, employees received fake invoices from a well-known ride-sharing service suggesting that huge fees were owed. All it took was one click from a panicky staffer to infect the whole system.

If proper security precautions are not in place or the ransomware is not detected in time, it installs itself and begins encrypting data.

Three years ago, ransomware infected Android mobile devices by posing as an anti-virus program that had discovered "critical threats," according to a report by U.S. cybersecurity think tank Institute for Critical Infrastructure Technology. Victims were coerced into paying for a fake software licence. Another method involved the mimicking of an adult website application; once installed, the app flashed a law-enforcement warning and demanded a $500 (U.S.) fine to unlock the device.

How prevalent is it?

Individuals, companies, public institutions - including hospitals, schools, churches and law-enforcement agencies - law firms and financial institutions are increasingly being targeted. Critical services such as fire, police and hospitals make easy targets.

The Institute for Critical Infrastructure Technology report says 2016 is shaping up to be "the year ransomware will wreak havoc on America's critical infrastructure community."

Ransomware is increasingly popular among cyberattackers because it is a "volume business." It's simple, relatively anonymous and fast. Some people will pay, some will not pay, so what. With a wide enough set of targets, there is enough upside for these types of attacks to generate a steady revenue stream," said Brian Contos, vicepresident and chief security strategist at Securonix, a security analytics firm.

Recent victims include the University of Calgary, Kansas Heart Hospital in Wichita, Hollywood Presbyterian Medical Center in Los Angeles and MedStar Health in Washington.

Network service provider Infoblox says there was a 35-fold increase in observations of ransomware-related websites in the first quarter of 2016. The FBI recently disclosed that ransomware victims in the United States reported costs of $209-million in the first quarter of 2016, up dramatically from $24-million for all of 2015, according to Infoblox.

And that doesn't include all the unreported cases.

Canada last month announced a major co-operative effort with the United States, Britain, Australia and New Zealand to use their secretive electronic-intelligence-gathering assets to go after cybercriminals. The Canadian Cyber Incident Response Centre (CCIRC) is aware of 1,762 cybersecurity-related incidents last year, including thefts of intellectual property from foreign governments and a significant rise in the use of ransomware.

What can be done to guard against attack?

There is no foolproof way to prevent attack, but measures to minimize the risk include regularly updating anti-virus software and computer firewalls; backing up files based on the 3-2-1 rule (three backup copies located on two different computer platforms with one backup located on a separate and isolated disc drive); and ensuring employees know the dangers of potentially disruptive e- mails and hyperlinks.

"Tight security measures, upto-date software, user best practices and clean, protected backup data" are fundamental, Infoblox says.

What action can be taken in the event of an attack?

Institutions often find they have no choice but to pay the ransom to get their data back. Some companies and organizations have even been stocking up on bitcoins, an anonymous and untraceable digital currency, in the event they are targeted and need to pay up.

But some cybersecurity experts and law-enforcement officials say paying the ransom only encourages and emboldens cybercriminals.

Hollywood Presbyterian reportedly tried to thwart its attackers by switching to paper medical records and forms, but ended up paying the equivalent of about $17,000 in bitcoins to get its locked systems back up.

In some cases, a one-time payment isn't enough. "Unfortunately, even when organizations have paid up, attackers have been known to ask for more money, said Chris Mayers, chief security architect at Citrix Systems Inc. in London.

It World Canada
Some Canadian firms still think they won't be targets of cyber attacks, conference told
Thursday, 09 June 2016
Byline: Howard Solomon

Many Canadian organizations - particularly small ones - still wrongly think they aren't in the sights of cyber attackers, says a major provider of business connectivity to small and medium businesses. "There's a sense of safety" that isn't justified, Stewart Cawthray, general manager of network security for Rogers Communications' enterprise business unit, told the annual Canadian Telecom Summit in Toronto on Tuesday.

Speaking on a panel on cyber security, Cawthray said corporate awareness of the threat is good among large organizations. Medium sized firms are where large ones were five years ago, he added in terms of investing in security technology.

Still, he noted that some customers still say 'We're not the target,' Yet studies suggest 54 per cent of Canadian organizations have suffered a breach.

Perhaps he suggested, it's because there are few reported breaches here. That will change, he predicted, when the mandatory data breach reporting law comes into effect for firms covered under the federal Personal Information Protection and Electronic Documents Act (PIPEDA).

Ottawa is now consulting with the private sector on disclosure regulations, but they aren't expected to come into law until next year.

But several panellists also spoke of the importance of organizations getting over the shame of admitting they've been breached. Cawthray argued that organizations can be respected by the public if they face up to a problem and explain what is being done to reduce the risk of another breach. Om the other hand trying to hide a breach ends up losing customer trust.

(By coincidence the University of Calgary acknowledged this week it had to pay $20,000 after being struck last month by ransomware.)

And while some noted that large organizations such as Home Depot and Target have survived huge data breaches, panel moderator Scott Jones, assistant deputy minister for IT security at the Communications Security Establishment, charged with protecting sensitive federal data as well as being the country's electronic spy agency, cited research that half of small companies suffering a breach don't survive.

The session also got a small peek into the operations of the Communications Security Establishment (CSE) when Jones said his department blocks 100 million malicious acts a day.

On the other hand, Jones said "at the end of the day you'll never win because the actors are very diverse," ranging from nation states to script kiddies who have access to a wide range of tools that can hide their behaviour. At the moment , he conceded, all of the advantage is with attackers.

There was no shortage of advice on what has to be done. Kellman Meghu, Toronto-based head of data centre virtualization at Check Point Software, warned that "we're not solving a technology problem. We're solving a people problem. There's no accounting for what people will do when attacking. So the appraoch (by enterprises) that ' We're secure because we're protected.'.makes for great marketing but they still have to manage their risks

"One thing I fear from a marketing perspective is is we (vendors) try to sell it off as easier than it is, and I think we need to be honest with customers: This is not easy, it's hard. It's not going to get easier but it's not something we can ignore. We need to step up and do the work and use the tools for what they really are, not try to market them as a magic box. This is an ongoing thing has to be part of the infrastructure."

Unfortunately, according to Darren Anstee, chief security technologist at Arbor Networks, many organizations are still talking about reducing the cost of security. "I very much wish it was about the value of security to the business, how it can differentiate the business, how it applies to various frameworks."

The conversation has to change from a technology discussion to one of business outcomes, said Cawthray. Security has to be something organizations just do as part of normal operations, that it's a risk management problem. Then technology decisions are more business-oriented.

The culture of organizations has to change, agreed Jennifer Blatnick, vice-president of cloud and enterprise product marketing at Juniper Networks. But, she added, when her firm surveys customers it finds security is still an afterthought. -- and the proof is security is only 10 per cent of IT budgets. "Why wouldn't you spend 100 per cent of your budget to protect 100 per cent of your budget?"

Meghu also suggested that user awareness training is a waste. "Trying to teach someone what a bad Web site is, forget it." More important, he said, is teaching developers to write secure code.

There was also discussion on security in an era when organizations are increasingly moving to cloud computing. That means securing data -- whether through encryption or tokenization or other techniques is vital, Cawthray said. Regardless of whether it's in the cloud or on-premise, he added "if we have well-protected data it can live on insecure infrastructure and still operate."

Gulf News
Millions of dirhams lost to IT security breaches in Middle East
Thursday, 09 June 2016
Byline: Cleofe Maceda

Dubai - Companies in the Middle East are incurring millions of dirhams in financial losses due to cyber security breaches.
Over the last five years, organisations in the region incurred a total financial loss of approximately $1,493,590 (Dh5.4 million) after hackers broke into "system perimeters" in an attempt to steal passwords, customer data and other sensitive information from corporate databases.

The annual Data Security Confidence Index, released by Gemalto on Wednesday, showed that companies spent about $35,232,000 to fix the intrusion.

"Data breaches include loss of passwords and personal data," Sebastien Pavie, regional director for Middle East and North Africa, identity and data protection, at Gemalto, told Gulf News.

Businesses, as a result, suffered from delays in getting products and services to the market (56 per cent; decreased customer confidence (38 per cent) and the loss of a new or incremental business opportunity (32 per cent). Companies affected are based in the UAE, Saudi Arabia and other parts of the Middle East.

Those targeted by hackers and lost more than $1 million in the process include companies operating in the financial sector (8 per cent), manufacturing (8 per cent), private health (8 per cent), public (8 per cent) and utilities (8 per cent) industries, among others.

The biggest proportion of affected organisations (25 per cent) are in the telecommunications sector, while 16 per cent are in retail and 16 per cent in business and professional services. "This research shows that there is indeed a big divide between perception and reality when it comes to the effectiveness of perimeter security," said Pavie.

"The days of breach prevention are over, yet many IT organizations continue to rely on perimeter security as the foundation of their security strategies. The new reality is that IT professionals need to shift their mindset from breach prevention to breach acceptance and focus more on securing the breach by protecting the data itself and the users accessing the data."

According to the research findings, 58 per cent of IT decision makers said they would adjust their strategies as a result of high-profile data breaches and allocate more spending to data security (encryption, fraud detection and/or key management).

More than half (52 per cent) said they had increased spending on perimeter security and believe that their current investments are going to the right security technologies.

Despite the increased focus on perimeter security, the findings show the reality many organisations face when it comes to preventing data breaches.

All organizations surveyed in the Middle East (100 per cent of them) said their companies experienced a breach at some time over the past five years. This suggests that organisations have not made significant improvements in reducing the number of data breaches despite increased investments in perimeter security.

"While companies are confident in the amount of spending and where they are spending it, it's clear the security protocols they are employing are not living up to expectations," said Privie.

"While protecting the perimeter is important, organisations need to come to the realisation that they need a layered approach to security in the event the perimeter is breached. By employing tools such as end-to-end encryption and two-factor authentication across the network and the cloud, they can protect the whole organisation and, most importantly, the data," concluded Pavie.

Agence France Presse
Singapore to block Internet access for government workstations within a year
Thursday, 09 June 2016

Singapore - Singapore confirmed Wednesday it would cut off internet access for government work stations within a year for security reasons, a surprise move in one of the world's most wired countries. The decision will not disrupt government operations, the Infocomm Development Authority (IDA) said after local daily The Straits Times reported that some 100,000 computers would be affected.

"We have started to separate Internet access from the work stations of a selected group of public service officers, and will do so for the rest of the public service officers progressively over a one-year period," the IDA said in a written reply to AFP queries.

Industry sources said the measure was aimed at preventing cyber attacks as well as the spread of malware that might enter the government email network thought Internet-enabled work stations.

Singapore is one of the world's most Internet-savvy societies, offering broadband speeds envied by many.

A wide range of government services are available online, including registering for marriage, filing complaints to the police and video consultations with doctors.

Government services will not be disrupted by the security measures, sources familiar with the plan said.

The Straits Times said public servants would still have access to the internet on their personal devices such as tablets and smartphones.

Dedicated Internet- linked terminals will be issued to civil servants who need them for work, the newspaper added.

The IDA said the government regularly reviews measures to make its network more secure. "There are alternatives for Internet access and the work that officers need to do, does not change."

Singapore announced in 2014 it was stepping up IT security measures following attacks on a section of the prime minister's website, as well the website of the presidential residence.

Times of India
Chinese hackers may have stolen government info: Experts
Thursday, 09 June 2016
Byline: Siddharth Tadepalli

Hyderabad - Chinese cyber espionage group Danti may have breached computers of top-ranking bureaucrats in Delhi and elsewhere, according to cyber security company Kaspersky Labs.
While department of electronics and information technology (DeitY) officials admitted a "big" cyber-attack, they refused to divulge details, saying the probe was sensitive. But, an official source, reacting to the report, said there was indeed a breach in a few computers in the Union Cabinet secretariat, but it has been plugged now.

"It was identified during an investigation and requisite steps were taken immediately," the source said, adding "opportunities for misuse" exist in such attacks. "However, this did not seem to be a serious threat," the official said.

According to Kaspersky Labs, one of the world's top cyber- security companies, Danti possibly breached dozens of computers that are used by Cabinet-rank officials in the national capital. Speaking to TOI over the phone from Mumbai, Kaspersky LabsSoutheast Asia managing director Altaf Halde said, "We've been following a trail of malware that was used to siphon away sensitive information from government computers.

"Our team tracked the malware strain to computers used by Cabinet secretariat of the Indian central government. These hackers have a special focus on diplomatic entities. We presume they may already have full access to internal networks in the Indian government," Halde said. He said it delivers the malware through spear-phishing emails and comments written in Mandarin, but in order to attract the attention of potential victims, the email addresses are in the names of several high-ranking government officials.

Once a victim, in this case a bureaucrat, opens the mail, the Danti backdoor is installed and sensitive data is siphoned off from the infected computer. Kaspersky said they tracked several such malicious emails to Indian embassies in Hungary, Denmark and Colombia, which were targeted by Danti. "In the case of the Indian embassy in Hungary, it looks like the original message was forwarded from the embassy to the Indian IT security team in the MEA," Halde added. Experts said they've come across similar complaints and will probe whether it is the handiwork of Danti group.

Khaleej Times
Middle East firms lost $1 million in data breaches in last five years
Thursday, 09 June 2016
Byline: Staff Report

Dubai - Middle Eastern organisations have incurred a total financial loss of approximately $1,493,590 over the last five years due to system perimeter breaches, findings of the third annual Data Security Confidence Index released by Gemalto have found.
The average cost of detecting and fixing these breaches was $35,232,000. Despite the increasing number of data breaches and more than 3.9 billion data records worldwide being lost or stolen since 2013, organisations continue to believe that basic perimeter security technologies are effective.

"This research shows that there is a big divide between perception and reality when it comes to the effectiveness of perimeter security," said Sebastien Pavie, regional director for the Mena region, identity and data protection at Gemalto.

"Many IT organisations continue to rely on perimeter security as the foundation of their security strategies. The new reality is that IT professionals need to shift their mindset from breach prevention to breach acceptance and focus more on securing the breach by protecting the data itself and the users accessing the data."

Of the 1,100 IT decision makers surveyed worldwide, 50 were based in the Middle East. Of these respondents, 94 per cent said their perimeter security systems such as firewall, IDPS, AV, content filtering and anomaly detection were effective at keeping unauthorised users out of their network.

Despite this, 54 per cent said they have suffered from a perimeter security system breach in the past 12 months. Furthermore, 60 per cent believe unauthorised users can access their network, and 36 per cent said unauthorised users could access their entire network in the event of a data breach.

Despite the increased focus on perimeter security, the findings show the reality many organisations face when it comes to preventing data breaches.

All organisations surveyed in the Middle East - 100 per cent of them - said they experienced a breach at some time over the past five years. This suggests that organisations have not made significant

improvements in reducing the number of data breaches despite increased investments in perimeter security.

London Times
Computers will crack our toughest codes, spies admit
Thursday, 09 June 2016
Byline: Tom Whipple

London - Britain's top code breaker is preparing for the day when almost all internet encryption will be rendered useless thanks to a computing advance that may also lead to a mass release of secret correspondence across the globe.
Robert Hannigan, the head of GCHQ, said that the arrival of powerful quantum computers, which some believe could be viable in a decade, will undermine encryption, the "foundation of internet security".

Senior scientists have also warned that the advance will not only mean that the way we encode data will have to change but that vast caches of western encrypted data from past decades will suddenly be accessible by Russia and China -- and vice versa.

While messages between embassies and the Foreign Office often use different proprietary systems, a significant proportion of previously encrypted commercial secrets, private correspondence and government data may become readable.

"The whole of the cryptographic world has been worrying about this and how to make things safe," he said.

Mr Hannigan, the first serving head of GCHQ to answer questions at The Times Cheltenham Science Festival, added: "It's our job to make sure we are starting to plan to protect government secrets, machines and power grids now against the arrival of serious quantum computing. That could be ten to twenty years off. We just don't know."

Most internet security works on the basis of "public key cryptography", which involves encrypting data using a large number that is itself the multiple of two very large prime numbers. The method was invented at GCHQ.

Anyone trying to decrypt a message must be able to find out what those prime numbers are from their multiple. To do so is not possible using a conven-tional computer. Quantum computers will change that. Rather than using a binary system, quantum computers harness the behaviour of subatomic particles, which can exist in many different states at the same time, vastly multiplying the computing power available. Governments and universities are rushing to develop quantum computers. One of the biggest British collaborations is at Oxford but there are also teams at Bristol and Cambridge. Whoever succeeds first will be able to read uncracked messages from friends and foes alike.

Since he took over as head of GCHQ Mr Hannigan has worked to open it up, including recently giving The Times access to the organisation's Cheltenham headquarters. Appearing at a public event to answer audience questions is part of that process.

Mr Hannigan also talked about the fallout from one of the most serious breaches of recent years, the intelligence leaks by Edward Snowden. The files may have resulted in deaths. He said terrorists who were being tracked before the disclosures suddenly vanished. "Who knows what they went on to do?" Mr Hannigan said that GCHQ was working on techniques to hit hackers over the internet. These powers would be important as the spread of internetenabled devices meant that more of our society was becoming exposed.

Motherboard (Vice)
One of the World's Largest Botnets Has Vanished
Wednesday, 08 June 2016
Byline: Jospeh Cox

New York - With no warning, one of the world's largest criminal botnets--a massive collection of computers used to launch attacks--has disappeared. Researchers have reported huge drops in traffic for two of the most popular pieces of malware which rely on it.
"We can only tell that the Dridex and Locky spam campaigns stopped since June 1 in our observation. We cannot confirm how the botnet was brought down yet," Sarah Coutermarsh, a spokesperson for cybersecurity company FireEye, told Motherboard in an email.

Dridex is a piece of malware typically used to empty bank accounts, while Locky is a particularly widespread form of ransomware, which encrypts a victim's files until they pay a hefty bounty in bitcoin. The two campaigns have been linked in the past.

It's not clear what exactly will happen to Locky victims now that its infrastructure has seemingly gone offline. There's a chance that those infected with the ransomware may be unable to successfully pay the criminals and have their files unlocked.

Back when Locky was launched in February of this year, security researcher Kevin Beaumont wrote, "The deployment of Locky was a masterpiece of criminality-- the infrastructure is highly developed, it was tested in the wild on a small scale on Monday (ransomware beta testing, basically), and the ransomware is translated into many languages. In short, this was well planned."

In October 2015, the FBI, UK's National Crime Agency and other law enforcement agencies disrupted the Dridex malware, but that didn't stop it.

After the botnet, called Necurs, vanished, Beaumont told Motherboard in a Twitter message, "We've seen a huge decrease in malicious traffic since. Locky has completely disappeared," and added that no new command and control servers-- which hackers use to keep tabs on and direct their botnet--have popped up since. Beaumont claimed Necurs was the world's largest botnet.

There is only circumstantial evidence that may point to why the botnet has vanished. On June 1, the same day FireEye and Beaumont reported a large dip in malicious traffic, Russia's FSB security service said it had arrested a gang of around 50 hackers, Reuters reported. Those hackers had stolen over 1.7 billion roubles ($25.33 million) from Russian institutions and banks, and used a trojan called Lurk.

Group-IB, a Russian cybersecurity firm that works with law enforcement, doesn't think there's a link with the arrests though.

"We don't see any connection between Necurs Botnet going down and recent arrests in Russia. The arrests of 50 hackers were made in connection to the Lurk group, and that particular group only targeted Russian and Ukrainian banks in their fraudulent activity," Nikolay Grunin, PR manager for Group-IB told Motherboard in an email.

For the time being, why exactly Necurs disappeared remains a mystery.

Fars News Agency
Drones to Play More Active Role in IRGC Navy Operations
Thursday, 09 June 2016

Tehran - Commander of the Islamic Revolution Guards Corps Navy Rear Admiral Ali Fadavi announced IRGC's plans to increase drone missions in its naval operations.
"Drones comprise the fifth pillar of the IRGC Navy considering their combat and operational power," Fadavi said after visiting the IRGC Navy's Drone Command Center on Wednesday.

"Drones can find their place within the framework of the IRGC Navy's definitions of naval power which are different from the normal definitions in the world," he added.

Elsewhere, Fadavi underlined that Iran's power and capabilities are deterring the enemies from attacking Iran, and said, "Our main enemy is the Americans and not certain weak and little countries."

The IRGC Aerospace force enjoys high capabilities and has taken wide strides in building different home-made aircraft, including drones.

The Islamic Republic has so far unveiled various domestically produced drones, including Ababil, Fotros, Hazem, Karrar (long range attack drone), Mohajer, Sarir, Shahed 129, Yasir and Zohal.

IRGC Lieutenant Commander Brigadier General Hossein Salami said last year that the IRGC has developed a drone technology which has empowered its radar-evading pilotless aircraft to fly 3,000km nonstop for reconnaissance and combat missions.

"Our defensive achievements and tests have grown so much that we avoid releasing reports about them in order not to prevail a security atmosphere in the society," Salami said in Tehran.

Noting that Iran which one day merely test-fired short-range missiles is now in possession of high-precision long-range missiles, he said, "Today, our drones' 3,000-km operational range and their ability to carry out offensive operations is no more surprising to us."

Salami also said Iran rejects many arms sales proposals from foreign manufacturers as it can build more advanced weapons and equipment.

Associated Press
Experts: Clinton emails could have compromised CIA names
Wednesday, 08 June 2016
Byline: Staff report

Washington - The names of CIA personnel could have been compromised not only by hackers who may have penetrated Hillary Clinton's private computer server or the State Department system, but also by the release itself of tens of thousands of her emails, security experts say.
Clinton, the presumptive Democratic presidential nominee, turned over to the State Department 55,000 emails from her private server that were sent or received when she was secretary of state. Some contained information that has since been deemed classified, and those were redacted for public release with notations for the reason of the censorship.

At least 47 of the emails contain the notation "B3 CIA PERS/ORG," which indicates the material referred to CIA personnel or matters related to the agency. And because both Clinton's server and the State Department systems were vulnerable to hacking, the perpetrators could have those original emails, and now the publicly released, redacted versions showing exactly which sections refer to CIA personnel.

"Start with the entirely plausible view that foreign intelligence services discovered and rifled Hillary Clinton's server," said Stewart Baker, a Washington lawyer who spent more than three years as an assistant secretary of the Homeland Security Department and is former legal counsel for the National Security Agency.

If so, those infiltrators would have copies of all her emails with the names not flagged as being linked to the agency.

In the process of publicly releasing the emails, however, classification experts seem to have inadvertently provided a key to anyone who has the originals. By redacting names associated with the CIA and using the "B3 CIA PERS/ORG" exemption as the reason, "Presto -- the CIA names just fall off the page," Baker said.

The CIA declined to comment.

A U.S. official said the risk of the names of CIA personnel being revealed in this way is "theoretical and probably remains so at this time." The official, who did not have the authority to publicly address the matter, spoke on condition of anonymity and would not elaborate.

Steven Aftergood, who directs the Federation of American Scientists' Project on Government Secrecy, said even if any identities were revealed, they might be the names of analysts or midlevel administrators, not undercover operatives.

"I don't think there's any particular vulnerability here," Aftergood said.

Clinton has acknowledged that the email server, set up in the basement of her New York home, was a mistake. But she says she never sent or received anything that was marked classified at the time of transmission. Clinton, who was secretary of state from 2009 to 2013, insists the personal server she used was never actually breached.

The AP discovered last year that Clinton's private server was directly connected to the internet in ways that made it more vulnerable to hackers. A recent State Department inspector general's report indicated the server was temporarily unplugged by a Clinton aide at one point during attacks by hackers, but her campaign has said there's no evidence the server was hacked.

In each year from 2011 to 2014, the State Department's poor cybersecurity was identified by its inspector general as a "significant deficiency" that put the department's information at risk. Another State Department inspector general report revealed that hacking attempts forced Clinton off her private email at one point in 2011.

Then in 2014, the State Department's unclassified email system was breached by hackers with links to Russia. They stole an unspecified number of emails. The hack was so deep that State's email system had to be cut off from the internet while experts worked to eliminate the infestation.

Baker points out another instance where Clinton's server might have been hacked.

A March 2, 2009, email warned against State Department officials using Blackberries. Eric Boswell, assistant secretary of state, says the "vulnerabilities and risks associated with the use of Blackberries ... considerably outweigh their convenience."

Nine days later, another email states that Clinton approached Boswell and says she "gets" the risk. The email also said: "Her attention was drawn to the sentence that indicates we (the diplomatic security office officials) have intelligence concerning this vulnerability during her recent trip to Asia."

Clinton traveled to China, Indonesia, Japan and South Korea in February 2009.

Times of India
Doors open for India to military logistics, cutting-edge weaponry
Thursday, 09 June 2016
Byline: Rajat Pandit

New Delhi - Doors are now being yanked open for Indian armed forces to extend their operational reach in the critical Asia Pacific region and beyond with logistical help from the US, as also acquire some cutting-edge military products like the Predator surveillance and armed drones after joining the Missile Technology Control Regime (MTCR).
These, in effect, were the key takeaways in the defence sector from the flurry of announcements made after the Modi-Obama meet in Washington on Tuesday. The bilateral Logistics Exchange Memorandum of Agreement (LEMOA), which will now be inked after finalisation of its text, envisages Indian and American militaries providing logistics support, refuelling and berthing facilities to each other's warships and aircraft on an equal-value exchange basis seamlessly.

The LEMOA will give the US forces regular access to Indian military bases, which has led to some criticism about India surrendering its traditional strategic autonomy. But, as reported by TOI earlier, the pact will also allow Indian forces access to US bases ranging from Djibouti (Horn of Africa) and Diego Garcia (central Indian Ocean) to Guam (western Pacific) and Subic Bay (the Philippines).

The LEMOA basically revolves around "functional arr- angements" for exercises, joint trainings, port calls and HADR (humanitarian assist- ance and disaster relief) operations. Defence minister Manohar Parrikar and top officials have stressed the pact will not lead to any permanent stationing of US troops on Indian soil. India will also have the right to refuse logistical support for any US military action.

India's quest to acquire armed HALE (high-altitude, long endurance) drones or UAVs (unmanned aerial vehicles) as well as some key space technologies, in turn, will now become easier after joining the 34-member MTCR, which prevents proliferation of missiles and UAVs over the range of 300-km. India has been in talks with the US for acquiring Predator/Avenger drones, which have been used extensively in the Af-Pak region to take out terrorists with their deadly Hellfire missiles, for quite some time but not being an MTCR member was a major hurdle in the way till now.

Apart from the launch of the bilateral maritime security dialogue, the conclusion of a technical arrangement for sharing of commercial 'White Shipping' information between India and the US is another step towards promoting overall maritime domain awareness. India, incidentally, is trying to

finalise such pacts with over 25 countries from the African east coast to the western Pacific to strengthen maritime security from conventional as well as unconventional threats.

Categorisation of India as a 'Major Defence Partner' by the US on Tuesday is also a step forward, which will help process Indian applications faster through the American bureaucracy and control regulations. But it's still not enough to meet the aspirations of India, which has given arms co- ntracts worth over $13 billion to the US over the last decade.

The Mirror (UK)
ISIS kill list names '39 Brits' as terror targets its supporters should 'follow' and 'avenge for Muslims' (Canada)
Thursday, 09 June 2016
Byline: Stephen Jones

London - A pro-terrorist hacking group published and shared their addresses and email contact details on a secretive messaging app service - and urged to 'kill them strongly'
A pro- ISIS hacking group have published a list of names - including 39 Brits - as fresh terror targets on a chilling 'kill list'.

The United Cyber Caliphate (UCC) shared the full list of 8,318 people including their addresses and email contact details on a secretive messaging app service.

It urged its supporters to "follow" those listed - and "kill them strongly to take revenge for Muslims".

An image it attached to the posts declared: "All world can't stop Islamic State" - and talked of 'Ghosts' and a 'Caliphate Cyber Army' - together with a picture of a lone, masked and armed soldier wandering a battlefield.

It is one of the longest kill lists any ISIS-affiliated group has distributed to date - but the believed to be the first the group has issued to contain details of non-US citizens.

It is not known if the 39 Brits named are military or government workers - or people in the public eye like royalty or celebrities.

The list - written in both English and Arabic - was uncovered by the media group Vocativ which specialises in investigating the hidden side of the web. It discovered it on a messaging app service called Telegram on Monday night.

It said most of the names and the accompanying addresses listed "appear to belong to people in the United States, Australia, and Canada".

The numbers of people listed in each country were:

USA - 7,848

Canada - 312

Australia - 69

UK - 39

The rest of the people listed are reported to be from a variety of nations including: Belgium, Brazil, China, Estonia, France, Germany, Greece, Guatemala, Indonesia, Ireland, Israel, Italy, Jamaica, New Zealand, Trinidad and Tobago, South Korea and Sweden.

Read more: 'ISIS terrorists kidnap' terrified actress in sick TV prank that leaves her in tears

Vocativ last night refused to share further details of those named on the list.

Searches on the Telegram service on Wednesday failed to uncover any list - suggesting it had since been removed.

It is not clear if any of the information published was already available in the public domain or if it had been passed on to relevant authorities.

UCC has previously been criticised for 'taking credit for others' work' in a recent study by data and intelligence specialists Flashpoint.

An article in The Wall Street Journal last month claimed authorities were at odds over whether the lists pose an actual threat or are merely scare tactics.

Mirror Online has contacted the Home Office for comment.

Vocativ.com (US)
New ISIS 'Kill' List Claims To Target Thousands Of Americans (Canada)
Thursday, 09 June 2016
Byline: Gilad Shiloach

New York - A pro-ISIS "hacking" group calling itself the United Cyber Caliphate distributed its latest "kill" list this week. The group claims the list includes names, addresses, and email addresses belonging to 8,318 people, making it one of the longest target lists ISIS-affiliated groups have distributed.

In a post Vocativ uncovered on the messaging app Telegram that was written in both English and Arabic, the United Cyber Caliphate called on its supporters to "follow" those listed and "kill them strongly to take revenge for Muslims."

Most of the names and the accompanying addresses listed appear to belong to people in the United States, Australia, and Canada. Out of 7,848 people identified as being in the U.S. alone, 1,445 were listed as having addresses in California, 643 in Florida, 341 in Washington, 333 in Texas, 331 in Illinois, and 290 in New York. Another 312 names and addresses allegedly belong to people in Canada, while 69 allegedly belong to people in Australia. Another 39 are affiliated with the U.K. and the rest are listed with addresses in Belgium, Brazil, China, Estonia, France, Germany, Greece, Guatemala, Indonesia, Ireland, Israel, Italy, Jamaica, New Zealand, South Korea, Sweden and Trinidad and Tobago.

It is unclear, however, if the list, posted on Telegram on Monday, includes any new information or details that weren't already accessible online. It's also unclear why the specific names and addresses outlined were selected, and whether or not they're in some way related. The group that posted the directory is also dubious. A recent study by Flashpoint, an intelligence firm, showed that the United Cyber Caliphate--a merger of pro- ISIS groups--is incompetent when it comes to hacking. Their highest-profile "hack" involved taking credit for others' work, according to the study.

But the latest list shows how ISIS-linked groups claiming to be hackers persist with what has become a well-known--even if potentially superficial--tactic: posting "kill" lists calling on ISIS loyalists to attack everyone from Minnesota cops to State Department employees and ordinary Americans. Counterterrorism officials have been at odds over whether such lists are simply efforts to instill fear or instead truly threaten those listed, The Wall Street Journal reported.

The United Cyber Caliphate also published satellite images on its Telegram channel showing U.S air bases around the world on Monday. The same images can be found on Google Earth.

London Daily Telegraph
Terrorist groups acquiring the cyber capability to bring major cities to a standstill, warns GCHQ chief
Wednesday, 08 June 2016
Byline: Henry Bodkin

London - Terrorists and rogue states are gaining the capability to bring a major city to a standstill with the click of a button, the Director of GCHQ has warned.
In a rare public appearance, Robert Hannigan said the risk to cities like London would increase as more physical objects, such as cars and household appliances, are connected online - the so-called "internet of things".

Speaking at the Cheltenham Science festival, the intelligence chief warned that nation states were currently developing the kind of cyber programmes that could attack the UK, but that terrorist groups were also looking to take advantage of the technology.

"At some stage they will get the capability," he said.

"There are certainly states and groups with the intent to do it, terrorist groups, for example, who have no threshold when it comes to the loss of life.

"We're not quite there yet, but as the world becomes ever more connected that will become a greater risk."

Speaking as the controversial Investigatory Powers Bill passed its third reading in the House of Commons, Mr Hannigan also defended the surveillance of internet activity by the intelligence services, saying seven attacks against the UK had been foiled in the last 18 months due to bulk data analysis.

Pakistan Dawn
Seven Indian embassy websites hacked by group claiming Pakistan 'support'
Friday, 10 June 2016

Islamabad - Hackers claiming to be from Pakistan defaced websites of seven Indian embassies, high commissions, and consulates in various countries with pro-Pakistan Army slogans on Wednesday.
In an email sent to journalists, the hackers claimed to target Indian missions in Ankara, Athens, and Mexico City.

Missions in Sao Paulo, Brazil and Bucharest, Romania as well as Dushanbe, Tajikistan and South Africa's Pretoria were also defaced by the hackers referring to themselves as "Romantic" and "Intruder".

A screenshot of the Embassy of India in Athens' hacked website. The text defacing the sites of Dushanbe, Ankara and Athens read brief, jarring phrases such as "Don't Be Panic", "We Rock and U Shock", "Pakistan Zindabad", and "Feel the Power of Pakistan".

When Dawn.com attempted to access the seven sites, only Athens, Dushanbe, and Ankara seemed to be defaced, while the others appeared to be restored. A representative from the Indian High Commission in Islamabad declined to comment on the issue.

Cross-border hacking attacks have been sporadic yet common since at least 1998. The Lahore High Court's website has been hacked twice by Indian hackers recently, while Pakistani hackers have attacked National Institute of Technology (NIT) Raipur's website.

Jakarta Post
Indonesian Cyber Agency to Curb Rampant Cyber Attacks
Friday, 10 June 2016
Byline: News Desk

Jakarta - Lacking adequate cyber security, Indonesia is in a state of emergency following increasing incidents of cyber attacks mostly from within the country.
Indonesia is ranked second among countries where cyber attacks are launched and is the most prone to them, according to the office of the coordinating minister for political, legal and security affairs. Last year, the country had witnessed a fourfold increase in cybercrimes from 2014.

Cyber attacks in Indonesia rose 33 percent in 2015 compared to the previous year, Coordinating Political, Legal and Security Affairs Minister Luhut B. Pandjaitan stated recently.

In 2013, the quarterly State of the Internet Report by Akamai Technologies revealed that Indonesia had seen a massive increase in the number of cybercrimes and hacking attacks, so much so that Indonesia had pushed China out of the top spot for the Q2 2013 period.

Prevalence of cybercrimes and hacking in Indonesia was partially attributed to its lack of laws governing such crimes, the report said.

Meanwhile, Minister Pandjaitan believes that the country is in dire need of an agency that can coordinate on matters related to cyber defense.

Therefore, the government plans to set up a national cyber agency that will soon function as a coordinator for the country's cyber security. One of the agency's tasks would be to prepare a Bill on cyber security.

The agency would be formed based on a presidential decree and have a coordinating function, Air Vice Marshal Agus Ruchyan Barnas, chairman of the National Cyber Information Security and Resilience Desk of the Coordinating Ministry of Political, Legal and Security Affairs, said recently.

The agency would act as a coordinator for synergy, execution, and synchronization on everything related to cyber issues, without overstepping on the authority of other relevant institutions, he said. The desk has identified six cyber security categories.

The first category is Cyber Defense under the authority of the defense ministry and the defense forces based on the law on defense and the government regulation on State Territorial Spatial in their role as state defense.

The second category is Cyber Crime under the authority of the National Police and the Attorney Generals Office in their role in maintaining community and public orders.

The third category is Cyber Intelligence under the authority of the National Intelligence Agency (BIN) and the State Encryption Institution (Lemsaneg) in the roles such as early detection, early warning, and information security.

The fourth category is Cyber Security, which is under the authority of the communication and informatics ministry and the home affairs ministry in their roles and public service and demographic administration providers.

The fifth category is Cyber Resilience, which is under the authority of the political, legal and security affairs and the National Resilience Council (Wantanas) in coordination, synchronization, control, and defense roles.

The sixth category is Cyber Diplomacy, which is under the foreign ministry in its diplomatic role function.

Discussions on the plan to form the agency was held on January 6, 2015, by President Joko Widodo (Jokowi) and the cabinet secretary, the then Coordinating Minister for Political, Legal and Security

Affairs, Tedjo Edhy Purdijatno, Defense Minister Ryamizard Ryacudu, and Communication and Informatics Minister Rudiantara.

Cyber is a new space so it is normal if many institutions feel that they have the authority over the space and want to be a leading sector, according to him.

The BCN will not overlap with the authorities of other existing institutions, as it will have authorities not granted to any other institution.

"In line with a recommendation of the National Resilience Institute (Lemhannas), the BCN should become a regulator in managing, controlling, and coordinating cyber activities in Indonesia," he affirmed.

The Lemhannas had suggested the formation of BCN to the president through its study titled "Anticipation of Cyber Crime To Strengthen Security and Public Order for National Resilience," on August 19, 2014.

While conducting its coordinating tasks, the agency will not require a huge presence of personnel, he revealed. Relevant institutions will be accountable for the technical operations and implementation, he noted.

Indonesia is now in a state of cyber attack emergency due to the absence of a reliable instrument to offer protection against cyber attacks, he remarked.

Barnas expressed optimism that BCN would become a body that will boost cyber alertness and resilience in the country.

The vice marshal also believes that public awareness could minimize cyber threats and attacks, strengthen information resilience, and encourage information and knowledge sharing by establishing collaboration among various elements of the cyber sector, including academicians, and experts, as well as gray and white hackers.

Last year, the Jakarta Metropolitan police revealed that more and more international crime syndicates are using Indonesia as one of their bases for carrying out cybercrimes.

"Indonesia is no longer a destination for transnational crimes, but has slowly transformed into a hub for the operations of international crime syndicates," the Director of General Crime Investigation for the Jakarta Metropolitan Police Command, Senior Commissioner Krishna Murti, stated on Aug. 20, 2015.

He said several crime syndicates had entered Indonesia, organized their activities, rented places, and carried out criminal acts. "The criminals are recruited from China, and the main players are members of Yakuza, Japan," he revealed.

Murti drew this conclusion following a number of raids conducted on mostly young Chinese nationals, who were illegally residing in luxurious houses in Jakarta and were found to be equipped with various Internet-based and phone equipment.

On Aug. 20, 2015, for example, the Jakarta Metro Jaya Police detained 91 Chinese and Taiwanese nationals for allegedly committing transnational cybercrimes from Jakarta.

The Straits Times
Government e-services will not be affected by move to delink Internet access: Cyber Security Agency chief
Friday, 10 June 2016

Singapore - Government e-services will not be affected and public servants will still be able to respond to queries from citizens, said David Koh, chief executive of Singapore's Cyber Security Agency.
He was speaking to the media late Thursday (June 9) to address concerns from the public that government services would be affected following a decision to disallow Web surfing on the work computers of public servants from next May.

An online frenzy ensued after new broke on Wednesday that the 100,000 computers used by the public service would not have direct Internet access to keep work e-mail and shared documents safe.

Web surfing will still be allowed but only on employees' personal mobile devices. Non-sensitive e-mail can also be forwarded to personal accounts. Dedicated Internet terminals will be issued to those who need them for work..

Some criticised the Government for being backward while others made fun of the move memes such as a picture of a lady searching paper file cabinets as the way civil servants would work in the future.

Mr Koh spoke at length about why the Internet lockdown is necessary to keep citizen data safe. "Cyber security is key enabler for smart nation. We can't be a smart nation that is trusted and resilient if our systems are open and vulnerable," he said.

However, he said that Singapore is under constant attack by cyber criminals, gangs, hacktivists and even state actors.

So it is crucial to hive off Internet surfing to other machines that do not have access to the Government's internal networks and systems.

"This move of Internet surfing separation will significantly reduce the attack surface and make it harder for attackers to exploit our systems," he said. "As public servants, we have a duty and responsibility to protect the government and the citizens' information and data," he added.

The Straits Times
Government segregating secure systems, not cutting off Internet access for civil servants
Friday, 10 June 2016
Byline: Jeremy Au Yong

Washington - The move to stop web access on computers used by public servants is not an attempt to cut off the government from the Internet, but rather to segregate secure systems from activities like browsing, said Foreign Affairs Minister and Minister-In-Charge of the Smart Nation Initiative Vivian Balakrishnan in Washington on Thursday (June 9).
Responding to a question from The Straits Times about how to reconcile the recent move with the push to be a smart nation, Dr Balakrishnan said that the plan has occasionally been misconstrued as an attempt to shut off the government from the Internet. He stressed that the civil servants do need Internet access and will continue to have it.

"What we are really doing is not cutting off Internet access because, in fact, we all need Internet access on a daily basis in order to access information, in order to transact and in order to deliver information to our citizens," he said.

"So there is no possibility of cutting off ourselves from the Internet. What we are actually doing is segregating secure e-mail systems from other activities which you conduct on the Internet like browsing and transacting... Segregation is not the same as cutting off access."

The move is aimed at plugging potential leaks from work e-mail and shared documents amid heightened security threats.

The head of Singapore's Cyber Security Agency said that government e-services would not be affected and that public servants will still be able to respond to queries from citizens. He was speaking to reporters during a three-day working visit to the US capital.

The Straits Times reported on Wednesday that 100,000 public service computers will not have Internet access from next May. Web surfing can be done on employee's personal devices and dedicated Internet terminals will be issues to those who need them for work.

Dr Balakrishnan said the step was necessary in the name of cybersecurity and not incompatible with the idea of smart nation. "Cybersecurity is absolutely essential if we are to become a smart nation. You can't have electronic medical records, you can't have financial technology, you can't have large databases

with information that could be abused or misused, you can't afford a breach of privacy. So the way I look at it, cybersecurity is the flip side of the coin of being a smart nation," he said.

The foreign minister warned that the threat of cyber crime needed to be heeded. "Most people underestimate the dangers of breaches of our systems and the fact that there is a clear and present threat from espionage and criminal activity on the Internet. And the sooner people realise this and take steps, not just on the civil service but even individually to protect themselves, the better."

Prime Minister Lee Hsien Loong said on Thursday that the move was "absolutely necessary" to keep Government data secure. He added that he "locked down" from the Internet on his work computer at the beginning of the year. "It's a nuisance, it takes some getting used to, but you can do it."

Press Trust of India
With China on its mind, India set to export BrahMos cruise missile to Vietnam
Friday, 10 June 2016

New Delhi - India has stepped up efforts to sell an advanced cruise missile system to Vietnam and has at least 15 more markets in its sights, a push experts say reflects concerns in New Delhi about China's growing military assertiveness.
Selling the supersonic BrahMos missile , made by an Indo-Russian joint venture, would mark a shift for the world's biggest arms importer, as India seeks to send weapons the other way in order to shore up partners' defences and boost revenues.

The Narendra Modi government has ordered BrahMos Aerospace, which produces the missiles, to accelerate sales to a list of five countries topped by Vietnam, according to a government note viewed by Reuters and previously unreported. The others are Indonesia, South Africa, Chile and Brazil.

The Philippines is at the top of a second list of 11 nations including Malaysia, Thailand and United Arab Emirates, countries which had "expressed interest but need further discussions and analysis", the undated note added. A source familiar with the matter would only say the note was issued earlier this year.

New Delhi had been sitting on a 2011 request from Hanoi for the BrahMos for fear of angering China, which sees the weapon, reputed to be the world's fastest cruise missile with a top speed of up to three times the speed of sound, as destabilising.

Indonesia and the Philippines had also asked for the BrahMos, which has a range of 290km and can be fired from land, sea and submarine. An air-launched version is under testing.

Unlike Vietnam, the Philippines and Malaysia, India is not a party to territorial disputes in the South China Sea, a vital global trade route which China claims most of.

But India has an unsettled land border with China and in recent years has grown concerned over its powerful neighbour's expanding maritime presence in the Indian Ocean.

It has railed against China's military assistance to arch-rival Pakistan and privately fumed over Chinese submarines docking in Sri Lanka, just off the toe of India.

"Policymakers in Delhi were long constrained by the belief that advanced defence cooperation with Washington or Hanoi could provoke aggressive and undesirable responses from Beijing," said Jeff M Smith, director of Asian Security Programs at the American Foreign Policy Council in Washington.

"Prime Minister Modi and his team of advisers have essentially turned that thinking on its head, concluding that stronger defence relationships with the US, Japan, and Vietnam actually put India on stronger footing in its dealings with China."

India's export push comes as it emerges from decades of isolation over its nuclear arms programme. On June 7, India cleared all hurdles to become a member of the 34-member Missile Technology Control Regime (MTCR), a non-proliferation regime of which China is not a member. June 6 was the deadline for any member to object to a new entrant, and none had.

BrahMos's range means it falls short of the 300km limit set by the MTCR . India's accession to the MTCR may also strengthen its case for joining another non-proliferation body, the Nuclear Suppliers Group , a move China has effectively blocked. Both groups would give India greater access to research and technology.

BrahMos Aerospace, co-owned by the Indian and Russian governments, said discussions were underway with several countries on missile exports, but it was too early to be more specific. "Talks are going on, there will be a deal," said spokesman Praveen Pathak.

India is still a marginal player in global arms exports. The unit cost of the missile, fitted on Indian naval ships, is estimated at around $3 million.

India has been steadily building military ties with Vietnam and is supplying offshore patrol boats under a $100 million credit line, its biggest overseas military aid.

This week defence minister Manohar Parrikar held talks with his Vietnamese counterpart General Ngo Xuan Lich in Hanoi and both sides agreed to exchange information on commercial shipping as well as expand hydrographic cooperation, the Indian defence ministry said in a statement on Monday.

A source at the defence ministry said India was hoping to conclude negotiations on the supply of BrahMos to Vietnam by the end of the year.

The Indian government is also considering a proposal to offer Vietnam a battleship armed with the BrahMos missiles instead of just the missile battery, the source said.

"A frigate integrated with the BrahMos can play a decisive role, it can be a real deterrent in the South China Sea," the source said, adding New Delhi would have to expand the line of credit to cover the cost of the ship.

Indian warships are armed with configurations of eight or 16 BrahMos missiles each, while sets of two or four would go on smaller vessels.

A Russian official said exports of BrahMos to third countries was part of the founding agreement of the India-Russia joint venture. Only now India had armed its own military with the BrahMos was there capacity to consider exporting, he added.

Jerusalem Post
Why are terrorist groups allowed on Twitter?
Friday, 10 June 2016
Byline: Niv Elis

Jerusalem - News of the terrorist attack in Tel Aviv's Sarona Market had barely broken Wednesday night when Hamas leader Ismail Haniyeh took to Twitter to praise the slaughter.
"One of the #TelAviv bomber heroes. Mercy and light on the kindness of your soul," the former Hamas prime minister tweeted in Arabic at 10:45 p.m., alongside a picture of one of the attackers, shot in the street.

Haniyeh's Twitter account has been active since March 2012, and has 314,000 followers.

Khaled Mashaal, the group's leader, has had an account active since last May, now with 45,800 followers. The main Hamas Twitter page, active since October 2010, has 239,000 followers. It even has an English-language account to helpfully convey the organization's support of shooting innocents at a shopping center, dubbing it "a natural response to Israeli crimes."

What some Israeli counter- terrorism experts want to know is why Twitter, a US-based company, is not shutting down accounts belonging to organizations that the United States designates as terrorist groups.

"Essentially, the war against radical Islamic terror is occurring over social media," said Uzi Shaya, a former senior intelligence official. "So Twitter is facilitating terror, with full knowledge," he added.

Shaya admitted that the US government may lack legal support for shutting down social media pages for groups designated as terrorists, and says that legislation should be taken up to further the cause.

But Twitter, he noted, can act on its own. "Twitter is protected by a law of freedom of expression in the United States, but this is an absurd argument," he said.

Entities that are barred from opening a US bank account, he argues, should not be given a platform to spread their ideas through American companies. Beyond legal action, Twitter's own terms of service explicitly ban support for terrorism.

Accounts that "make threats of violence or promote violence, including threatening or promoting terrorism," may be suspended temporarily or permanently, the terms say. Further, they ban "hateful conduct," which includes promoting violence, attacking or threatening others on the basis of, among other thing, national origin or religious affiliation.

Twitter has acted on these problems in the past. In February, the company said that it had suspended 125,000 ISIS- linked accounts over the course of six months, that it was "horrified by the atrocities perpetrated by extremist groups," and that it condemned such behavior.

Indeed, it has also taken action against Hamas in the past, but unevenly. "There is not always a rhyme or reason," said Steve Stalinsky, the executive director of MEMRI, a group that monitors and translates extremist content from the Middle East with the aim of influencing US policy.

MEMRI, he said, has been monitoring jihadist and terrorist groups on Twitter for about 5 years, "and there's always been ebbs and flows on removing content.

"When we issued a report on the Kassam Brigades [the armed wing of Hamas], it was taken down right away. But then it came back," he said.

Twitter, which did not return requests for comment, said in its February blog post that it is working hard to identify and remove terrorist accounts, working with law enforcement, international bodies, foreign governments and NGOs to remove such pages.

"As many experts and other companies have noted, there is no 'magic algorithm' for identifying terrorist content on the Internet, so global online platforms are forced to make challenging judgment calls based on very limited information and guidance," the post said, alongside a vow to "aggressively enforce" the rules in the area.

But with the exception of the Izzadin Kassam Brigades, whose current account dates back 13 months, many of the current official Hamas pages have been around for years without interruption.

Shaya believes the company is still holding back on acting against Hamas pages. "It's not that they're hiding their identity. They're not. Terrorist organizations that are defined as terrorist organizations all over the world have pages on Twitter," he said.

When lawsuits linking terrorist social media accounts to specific attacks start rolling in, he suggested, the behavior might change, though legal experts believe such suits would face difficulties.

Still, Twitter's announcement on the ISIS account purge came just a month after Tamara Fields, an American woman who lost her husband to an ISIS attack, filed a lawsuit against the social media company.

Saudi Gazette
Accessing your internet browsing history is FBI's top legislative priority
Friday, 10 June 2016
Byline: Justin Yu

Undisclosed placeline - Tech firms and privacy groups are fighting back against an amendment that would give the FBI a top-level view of "electronic communication transactional records" (ECTRs) without the need for a warrant in terrorism and spy cases.
ECTRs include everything from the websites you've visited to how long you browsed a particular page. It's all up for grabs as part of an amendment to the Electronic Communications Privacy Act being considered this week by the Senate Judiciary Committee. The legislation would expand the government's ability to collect data using a National Security Letter, or NSL, which doesn't require a court order and typically includes a gag order saying the recipient cannot publicly acknowledge the letter.

FBI Director James Comey has said the amendment is needed to fix a typo in the ECPA that has hindered the bureau's ability to work in "a very, very big and practical way." As such, amending the existing surveillance laws has become a top priority for the FBI, Comey told a Senate Intelligence Committee in February

An FBI agent backed by an NSL could potentially "paint an incredibly intimate picture" of a person's life on the internet, said the American Civil Liberties Union in a letter sent Monday to lawmakers. Several privacy advocates and tech companies, including Facebook and Google, also signed the letter against the amendment.

Fars News Agency
Russian Fighter Jets Cut Off Terrorists' Communition Lines with Turkish Intelligence Agency
Friday, 10 June 2016

Tehran - The Russian air force targeted and destroyed the telecommunication towers in Northern Syria near the borders with Turkey and cut off the terrorists' internet and lines of communication with Turkey's MIT intelligence agency.

According to a report by al-Mayadeen news channel, the Russian warplanes smashed two telecommunication towers at the Syrian-Turkish borders, disconnecting the terrorists' contacts with the Turkish intelligence agency.

Other sources said the terrorists who have be caught off hand are now thinking of ways to reestablish their contacts with Turkey.

Earlier reports said that the European satellite operators give terrorists, specially the ISIL members, an opportunity to upload propaganda, exchange information and possibly even prepare terrorist attacks.

The ISIL members located in Syria and Iraq are gaining access to the Internet using opportunities offered by European satellite operators, Spiegel online wrote last year.

The communication is reported to be carried out via satellites of European companies Avanti Communications headquartered in the UK and Eutelsat in France.

According to the magazine, there are thousands of devices in Syria and Iraq, which enable terrorists to use the satellite Internet. Theoretically, everyone who wants to get online can do so only by using the satellite technology, as the telecommunications infrastructure in the country is destroyed.

However, for ordinary people living in the cities captured by the ISIL militants it is almost impossible. ISIL is controlling Internet access and prohibits private individuals from buying the required devices. Only members of the terrorist group have the right to use the Internet, others are being threatened with severe punishment. As reported by the magazine, the devices are being exported to Syria through Turkey.

Wall Street Journal
Not-Guilty Pleas in Hacking Case
Friday, 10 June 2016
Byline: Nicole Hong

New York - In their first U.S. court appearances, two Israeli men pleaded not guilty on Thursday to charges that they broke into computer networks of a dozen companies, including J.P. Morgan Chase & Co., to facilitate a global network of criminal activity.
Gery Shalon and Ziv Orenstein recently were extradited to the U.S. from Israel, where they had been in custody since their arrest last summer. At the time, a third defendant, Josh Aaron, had been at large. Mr. Aaron, a U.S. citizen, has since been arrested in Russia and is expected to be brought to the U.S., people familiar with the matter said.

Federal prosecutors accused the three men and their accomplices of carrying out data breaches at a dozen companies and turning the stolen information, including customers' email addresses and phone

numbers, into hundreds of millions of dollars. The hacking allegedly facilitated other crimes, including illegal internet casinos, pump-and-dump schemes, a payment-processing service for other criminals and an unlicensed bitcoin exchange.

Mr. Shalon's lawyer, Paul Shechtman, and Mr. Orenstein's lawyer, Alan Futerfas, didn't arranged for bail at Thursday's hearing in Manhattan federal court, so the two men will stay in federal custody.

Mr. Shechtman and Mr. Futerfas declined to comment. A lawyer for Mr. Aaron couldn't be identified.

In the alleged scheme, one of the biggest cyberattacks was against J.P. Morgan, the largest U.S. bank by assets, where the men stole the contact information of more than 83 million customers, according to officials.

Prosecutors also say the men orchestrated hacks into E*Trade Financial Corp., Scottrade Inc. and Dow Jones & Co., the parent of The Wall Street Journal.

Toronto Star
Why the meaningless hack attacks?
Friday, 10 June 2016
Byline: Vinay Menon

Analysis: Motivation guides all human behaviour.
For example, my wife often starts conversations with, "Can I ask you something?" Her true motivation is to tell me something. When she does, I listen and follow instructions because my motivation is to avoid sleeping in the shed.

We can extend the principle of core motivation to explain why members of groups often behave in similar ways: Politicians lie to snag votes. Marathoners run for the endorphin high. Firefighters risk their lives to rescue others. Birthday clowns are driven by a sadistic impulse to forever haunt our dreams.

As a species, I believe we are hard-wired to feel confused when not grasping where someone is coming from. It's a survival instinct. It's why we cross the street when a ruffian approaches or would freeze with disbelief if a car salesperson said, "Why don't we go to my office now so I can screw around with numbers and rip you off."

Donald Trump is a polarizing figure because his motivations are not clear.

Which brings us to the most baffling people in the universe right now: the rascals hacking into celebrity Twitter accounts for no apparent reason.

On Monday, Drake was hacked. On Tuesday, Lana Del Rey was hacked. This followed a spate of social media hijackings, including virtual violations of Katy Perry, Kylie Jenner, the NFL and Chelsea Handler.

As the Huffington Post noted: "It Appears Every Celebrity Twitter Account Is Being Hacked Right Now."

It does. But to what end?

Before we go any further, let me be clear: Hackers, I am not making fun of you. I'm not. Since I can barely recall my passwords - remind me to change my Star email to xd7wg43sasd+jgs68#?s after this column - I respect your ability to unearth ones you never created. So please do not steal my identity or pilfer my meagre RRSP or commandeer my texts unless you have time to send long overdue replies to distant relatives, in which case I'll give you the damn password.

I'm just trying to understand your motivation.

Consider what happened over the weekend, when multiple celebrity accounts were hacked. Someone gained access to Tame Impala's feed and sent out a fake bomb threat. Someone subverted Bon Iver and changed the handle to @ihavelegcancer. Someone assumed control of Keith Richards' account and used the opportunity to write: "i love killing people and blowing s--t up lmaooooo ima bomb..."

The person who slipped into Lana Del Rey's account fooled nobody with eyeball emoji, racist messages ("all muslims are terrorists"), dated conspiracies ("bush did 911") and sophomoric word play ("lana del GAY").

You have an audience of six million and this is your command performance?

Why not just cut-and-paste a knock-knock joke or dirty limerick?

This is hackneyed hacking and it's a hack at the heart of anyone who believes hacking should at least be a creative dark art. Come on, hackers. Use your new-found power to negotiate a ransom. Land a record deal. Set up a date with another celebrity. Say something so profound, it earns you a hefty book advance. Encourage your new followers to send over a pizza.

Do something.

The person who hacked Jenner's account was so tediously predictable with the impersonation - "I love being so famous with no talent" - Jenner barely yawned. She instead posted a clip on Snapchat and said, "So my Twitter was hacked and I don't really care. I'm just letting him have fun."

Now that is a slap in the face. It's like a carjacking that ends with the owner giving the pistol-pointing thief gas money and directions for the best possible getaway. And where is the fun in posting

scatological juvenilia or toothless barbs or death hoaxes for Jack Black or NFL commissioner Roger Goodell? What is the motivation? What is the higher purpose? What is the point?

Lately, it's like the hackers don't even know who they are pretending to be. The person who took over George Harrison's account this week encouraged the ex-Beatle to message him to regain access, unaware such an exchange would need to be routed through the Pearly Gates since Harrison died 15 years ago.

So what does the hacker do next? He apologizes.

They should all be sorry for wasting our time. We are exposed to enough dreck from real celebrities. The fake stuff should at least be enlightening.

Campus Safely Blog
Univ. of Calgary Pays Hacker After Ransomware Attack
Friday, 10 June 2016
Byline: Staff Writer

Calgary - The University of Calgary paid $20,000 Canadian dollars to restore access to its computer network after a ransomware attack paralyzed the campus May 28.
University officials paid the hacker June 7 and received a decryption key that is being used to restore faculty access to previously blocked online databases, including email servers.

Vice President of Finances and Services Linda Dalgetty says the university paid the hacker "because we do world-class research here and we did not want to be in a position that we had exhausted the option to get people's potential life work back in the future if they came today and said 'I'm encrypted, I can't get my files.' We did that solely so we could protect the quality and the nature of the information we generate at the university."

When university officials realized some network access was restricted, the IT department attempted to isolate the effects of the attack. CBC.ca reports that the decryption included a note confirming it was a ransomware attack.

The university also worked with Calgary Police Services, which continues investigating the attack, and consulted with various cybersecurity experts.

Although the full extent of the cyberattack has not been revealed, the university confirmed that email servers were affected. The attack made faculty and staff emails inaccessible, although university officials do not believe student emails were ever compromised.

Still, administrators initially advised students not to connect their computers to the school network.

After paying the hackers in bitcoin, administrators received a decryption key. The university confirmed that the decryption key works, but it has taken several days to decrypt all of their files.

Ransomware decryption keys can differ depending on what the hacker's intentions are and the type of malware used in the attack. Some decryption keys will fully restore access to a computer network automatically, but that doesn't appear to be the case at the University of Calgary.

Campus Safety magazine has reported on institutions paying a ransom only for the hackers to demand a second ransom. Other institutions have effectively responded to ransomware attacks and regained access to their network without paying a fee. Campus Safety has also looked at how seven different institutions handled ransomware attacks with varying levels of success.

Although there's significant uncertainty about the best way to respond to a ransomware attack (paying ransoms should be considered a last resort), cybersecurity experts seem to be in agreement that it's a growing threat that institutions need to prepare themselves for.

Ottawa Citizen
Local tech firm gets U.S. intelligence funds
Friday, 10 June 2016
Byline: Vito Pilieci

Ottawa - Computer security company Interset has attracted an undisclosed amount of investment from American venture capital firm In-Q- Tel, the organization that invests in firms and technology on behalf of the Central Intelligence Agency and the Federal Bureau of Investigation in the United States The major news comes a little over a year after the small, 60- employee company announced a $10-million round of financing, which it planned to use to improve its computer-security technologies and expand its operations.
The investment from In-Q-Tel is a major shot in the arm for the Ottawa firm, which can now say that it has received something akin to a seal of approval from some of the world's leading intelligence and security organizations.

"After a rigorous evaluation and due diligence process, Interset demonstrated how anomalous behaviours can be accurately surfaced and conveyed with actionable information, allowing government security experts to focus on mitigating risks and stopping attacks that may threaten our safety," said Dale Quayle, chief executive officer at Interset in a statement released Thursday. "U.S. intelligence and law-enforcement communities have long sought to protect critical data with an approach that surfaces attacks faster and more accurately, in a highly contextual, proactive way."

Originally incorporated in 2001 as GridIron Software, Interset has been bumping along various paths to the business it is today. The Ottawa company began life with a product that helped businesses use

networked computing and eventually evolved into FileTrek Software to help manage multiple computers across a network while tracking data that might be sent to cloud-computing servers.

Those earlier versions collected more than $16 million over the years, but Quayle realized that if he stripped away the noise, the company actually had a novel security product with little competition.

The company's expertise in tracking and monitoring large amounts of complex data led to a suite of security tools, which were eventually called the Interset Advanced Threat Detection Platform. The tools can be used to track an employee's data use across large corporate networks and set offalarm bells if someone tries to tamper with sensitive files without authorization. For example, an employee who regularly accesses a certain set of files every day would be flagged if they suddenly reached out for sensitive information on the network. The alarm could signal that the employee is stealing information or that their computer has been compromised. In the case that the employee was actually authorized to access the sensitive files, an investigation by corporate IT workers could be quickly dismissed. According to documents that were leaked online, Interset was invited to attend an In-Q-Telhosted "CEO Summit" in February. The annual event invites computer and network security firms to showcase their products in a bid to get noticed by the U.S. government. The event was attended by James Comey, director of the FBI, and Robert Work, U.S. deputy secretary of defence, among other prominent U.S. government officials.

Canberra Times
Students to form cyber militia and study hacks
Friday, 10 June 2016
Byline: Henry Belot

Canberra - Students at a Canberra university will form the future of a cyber security militia capable of defending national infrastructure and studying tactics of hacker armies in North Korea and Iran. UNSW Canberra professor Greg Austin, who has previously warned of glaring holes in Australia's cyber security policy, said many of his students were Australian Defence Force personnel and extremely capable.
"Australia is at a historic choice point when it comes to cyber defence," he said.
"We will have to build a cyber militia soon, and we need research and debate now on what that looks like. "We have found the students have a high level of capability and can work together to develop advanced policy ideas and we want to put them to the test." He said students would study "the hacker armies of Iran and North Korea, the tactics of Anonymous and WikiLeaks, and the development of cyber reserve forces in the UK, USA, Israel and Estonia".

Professor Austin, an executive with the Australian Centre for Cyber Security, said the coursework would produce graduates capable of working with the government of defence to protect infrastructure. "We need to think about a new form of organisation that is not a traditional part of the defence force,

but a halfway point between civilian life and the army reserve." Prime Minister Malcolm Turnbull launched a new $230 million strategy to bolster cyber security in April with an acknowledgement Australia was prepared to take offensive action to protect the national interest. The funding boost came after $400 million was allocated for staff with hacking experience at the Australian Signals Directorate and the announcement of 800 new intelligence and cyber roles within the Department of Defence.

"The Defence White Paper and the national cyber security strategy foreshadowed great leaps in technological advancement, but we are not quite hitting the mark when it comes to protecting our critical infrastructure or fighting cybercrime."

In the past six months, the computer system at the Bureau of Meteorology experienced a "massive breach", believed to have originated in China, and it was reported that 97 federal agencies were told to encrypt more data amid "hundreds" of attempted intrusions a month. Professor Austin said a national cyber security college was "urgently needed" and hoped his coursework would stimulate a conversation about a national curriculum.

But he has warned many Australians do not understand the risks cybercrime posed and, as a result, are unlikely to support large-scale investments by the government.

The Advertiser
Police widen boy hacker case
Friday, 10 June 2016
Byline: Sean Fewster

Canberra - An Adelaide teenager already facing a maximum 10-year jail term for hacking three secure websites is now a suspect in other acts of cyber crime, a court has heard.
The case against the boy, 15, of Woodcroft, was expected to be resolved by way of a plea bargain in the Christies Beach Youth Court yesterday.

Instead, Brevet Sergeant Kimberly White, for SA Police, asked it be adjourned while detectives ran a further investigation into the boy's alleged online activities. "There are some other matters that detectives are investigating at the moment, and they may potentially lead to further charges being filed," she said.

"The defendant is not here ... his counsel assures me he is willing to attend court.

"But I ask the court to issue an arrest warrant to activate (if he does not attend) on the next occasion."
The boy, who cannot be identified under SA law, has yet to plead to three counts of unauthorised impairment of computer systems.

Under the terms of his bail, he is banned from using the internet for any reason. If convicted, he faces a maximum 10-year jail term.

Police have alleged the offences occurred at Reynella on March 10, and at Woodcroft on April 4 and 6 this year.

Court documents allege he "directly caused an unauthorised impairment of electronic communications, knowing the impairment was unauthorised, and caused inconvenience".

The boy's arrest followed a two-week battle by Adelaide-based internet service provider NuSkope to defend itself, Reynella East College and a government agency from cyber attack. The agency has not been named in court.

It is alleged the incident was one of Australia's largest-ever denial-of-service attacks - a hack in which a targeted website is flooded with data requests, causing it to crash.

It is alleged about 10,000 NuSkope customers were affected by the incident. The boy has insisted he meant no harm and staged the attack "simply to see if he could".

Yesterday, Sgt White said she had spoken to the boy's lawyer, James Caldicott, about the change in circumstances.

"There is a need for the prosecution to have time to investigate these further matters," she said. "He asked that he and his client's attendance be excused ... I don't oppose that, but I ask for the warrant." Magistrate Kym Boxall declined, saying the boy's bail conditions were sufficient, and adjourned the case until August.An SA Police spokeswoman told The Advertiser: "As a matter of normal policy, SA Police don't provide details about active investigations and nor do we comment about matters before the courts."

Gloucestershire Echo
Bill on GCHQ's intercept powers passes Commons vote with huge majority
Friday, 10 June 2016
Byline: Aled Thomas

Cheltenham - The Investigatory Powers Bill, which updates the regulation surrounding GCHQ's work come a step closer to becoming law this week.
MPS voted by an overwhelming majority to pass the bill on its third reading in the House of Commons, with labour MPs joining Conservatives to see the Bill pass the vote by 444 votes to 69

The proposals will now go to the House of Lords before returning to the Commons for the final vote and then Royal Assent.

But the government has promised a review by an David Anderson QC into how powers of 'bulk access' to internet data should be used, in a concession to Labour MPs to allow the bill to pass.

The bill seeks to update and formalise the powers of data access used by law enforcement and security and intelligence services including Cheltenham's GCHQ, the UK's signals intelligence (Sigint) authority.

It replaces the communications data Bill which was introduced by the Coalition government, but ditched when the Liberal Democrats refused to support what was criticised as a snooper's charter.

Security Minister at the Home Office, John Hays said: "We have always been clear that we will listen and respond to the constructive views of politicians from all sides of the House to ensure passage of this important bill. We have encouraged rigorous scrutiny and are willing to act in the interest of both improving the bill and demonstrating the necessity of the powers it contains."

Cheltenham MP Alex Chalk, who voted for the Bill at its third reading this week, had said in March after its second reading that it wasn't 'the finished article.'

But he said changes made to the Bill after the committee and report stage had improved it: "The Investigatory Powers Bill is arguably the most important piece of legislation for a decade. It is fundamentally about giving our intelligence agencies the tools they need to get on even terms with terrorists and serious criminals, enabling the authorities to foil plots before they cause carnage. It's vital because the current measures available to our agencies are confusing and out of date. They are analogue provisions in a digital age. This Bill is about restoring capabilities that have been lost, partly as a result of the Snowden leaks, and partly as a result of changes in the way people communicate.

"I was one of the critics of the Bill in its early stages. The early draft put too much power in the hands of one person, the Home Secretary, to decide on whether to authorise intrusive measures like equipment interference warrants. I wanted to see independent judges involved in the process. The Government listened. Now there is a vital 'double-lock' mechanism, which means that warrants issued by Theresa May will have to be reviewed by independent judicial commissioners, who can assess if they are fair. If not, they will be struck down. It's a vital safeguard for our liberty.

"I also said openly at the Second Reading stage (before the Bill goes into committee for line by line scrutiny) that the Bill needed further work in several areas. What has taken place in committee has been hugely impressive. Hundreds of amendments have been suggested and debated. Different parties have come together to work hard in the national interest to improve the legislation.

Mr Chalk added: "The key remaining issue is over whether the agencies should have powers to collect bulk data. They already have them of course. Now the Government has published a strong operational case for bulk powers alongside the Bill, giving unprecedented detail on why the agencies need their existing powers, and how they are used. The core argument in favour is that you can't sensibly find the

needle in the haystack (where the 'needle' might be the vital information you need to thwart an atrocity) unless you've got access to the haystack in the first place. But to address any last lingering vestige of concern, Theresa May (wisely in my view) agreed to establish an independent review to examine the operational case for these powers. It will be led by David Anderson QC, and it will report back on whether these powers really are necessary before the Bill reaches its final stages. All the parties have confidence in David Anderson, and so this step should provide real comfort to those who want to see the strongest possible case made.

"What it comes to is this: in light of the enormous progress that has been made, this Bill has been moulded into a world-leading code that will help keep our country safe, whilst protecting our essential liberties. That conclusion is widely held across the political spectrum, and is reflected in the fact that Conservatives, Labour, DUP, UUP and Independents all came together to vote for the IP Bill at Third Reading.

"It is perplexing and disappointing that the Lib Dems voted against this Bill. I'm afraid I think that was a profound misjudgement. The threat to our country is real and we need this legislation urgently. Obstructing it is a mistake."

Harmit Kambo, campaign manager for Privacy International, who has criticised the bill and the powers it gives to security agencies said the review by Mr Anderson was "long overdue" after "the government had repeatedly failed to justify to the public collecting and retaining data keeps us safe."

Wall Street Journal
Emails in Clinton Probe Dealt With Planned Drone Strikes
Friday, 10 June 2016
Byline: Adam Entous, Devlin Barrett

Washington - At the center of a criminal probe involving Hillary Clinton's handling of classified information is a series of emails between American diplomats in Islamabad and their superiors in Washington about whether to oppose specific drone strikes in Pakistan.
The 2011 and 2012 emails were sent via the "low side"--government slang for a computer system for unclassified matters--as part of a secret arrangement that gave the State Department more of a voice in whether a Central Intelligence Agency drone strike went ahead, according to congressional and law-enforcement officials briefed on the Federal Bureau of Investigation probe.

Some of the emails were then forwarded by Mrs. Clinton's aides to her personal email account, which routed them to a server she kept at her home in suburban New York when she was secretary of state, the officials said. Investigators have raised concerns that Mrs. Clinton's personal server was less secure than State Department systems.

The vaguely worded messages didn't mention the "CIA," "drones" or details about the militant targets, officials said.

The still-secret emails are a key part of the FBI investigation that has long dogged Mrs. Clinton's campaign, these officials said.

They were written within the often-narrow time frame in which State Department officials had to decide whether or not to object to drone strikes before the CIA pulled the trigger, the officials said.

Law-enforcement and intelligence officials said State Department deliberations about the covert CIA drone program should have been conducted over a more secure government computer system designed to handle classified information.

State Department officials told FBI investigators they communicated via the less-secure system on a few instances, according to congressional and law-enforcement officials. It happened when decisions about imminent strikes had to be relayed fast and the U.S. diplomats in Pakistan or Washington didn't have ready access to a more-secure system, either because it was night or they were traveling.

Emails sent over the low side sometimes were informal discussions that occurred in addition to more-formal notifications through secure communications, the officials said.

One such exchange came just before Christmas in 2011, when the U.S. ambassador sent a short, cryptic note to his boss indicating a drone strike was planned. That sparked a back- and-forth among Mrs. Clinton's senior advisers over the next few days, in which it was clear they were having the discussions in part because people were away from their offices for the holiday and didn't have access to a classified computer, officials said.

The CIA drone campaign, though widely reported in Pakistan, is treated as secret by the U.S. government. Under strict U.S. classification rules, U.S. officials have been barred from discussing strikes publicly and even privately outside of secure communications systems.

The State Department said in January that 22 emails on Mrs. Clinton's personal server at her home have been judged to contain top-secret information and aren't being publicly released. Many of them dealt with whether diplomats concurred or not with the CIA drone strikes, congressional and law-enforcement officials said.

Several law-enforcement officials said they don't expect any criminal charges to be filed as a result of the investigation, although a final review of the evidence will be made only after an expected FBI interview with Mrs. Clinton this summer.

One reason is that government workers at several agencies, including the departments of Defense, Justice and State, have occasionally resorted to the low-side system to give each other notice about sensitive but fast-moving events, according to one law-enforcement official.

When Mrs. Clinton has been asked about the possibility of being criminally charged over the email issue, she has repeatedly said "that is not going to happen." She has said it was a mistake to use a personal server for email but it was a decision she made as a matter of convenience.

Clinton campaign spokesman Brian Fallon said: "If these officials' descriptions are true, these emails were originated by career diplomats, and the sending of these types of emails was widespread within the government."

U.S. officials said there is no evidence Pakistani intelligence officials intercepted any of the low-side State Department emails or used them to protect militants.

State Department spokesman Mark Toner said the agency "is not going to speak to the content of documents, nor would we speak to any ongoing review."

The email issue has dogged Mrs. Clinton for more than a year. Despite her success in nailing down the Democratic presidential nomination, polls show many voters continue to doubt her truthfulness and integrity. Her campaign manager has acknowledged the email matter has hurt her.

Republican rival Donald Trump has attacked Mrs. Clinton repeatedly on the issue, calling her "Crooked Hillary," saying what she did was a crime and suggesting the Justice Department would let her off because it is run by Democrats.

Beyond the campaign implications, the investigation exposes the latest chapter in a power struggle that pits the enforcers of strict secrecy, including the FBI and CIA, against some officials at the State Department and other agencies who want a greater voice in the use of covert lethal force around the globe, because of the impact it has on broader U.S. policy goals.

In the case of Pakistan, U.S. diplomats found themselves in a difficult position.

Despite being treated as top secret by the CIA, the drone program has long been in the public domain in Pakistan. Television stations there go live with reports of each strike, undermining U.S. efforts to foster goodwill and cooperation against militants through billions of dollars in American aid.

Pakistani officials, while publicly opposing the drone program, secretly consented to the CIA campaign by clearing airspace in the militant- dense tribal areas along the Afghan border, according to former U.S. and Pakistani officials.

CIA and White House officials credit a sharp ramp-up in drone strikes early in Mr. Obama's presidency with battering al Qaeda's leadership in the Pakistani tribal areas and helping protect U.S. forces next door in Afghanistan. Targets have also included some of the Pakistan government's militant enemies.

In 2011, Pakistani officials began to push back in private against the drone program, raising questions for the U.S. over the extent to which the program still had their consent.

U.S. diplomats warned the CIA and White House they risked losing access to Pakistan's airspace unless more discretion was shown, said current and former officials. Within the administration, State Department and military officials argued that the CIA needed to be more "judicious" about when strikes were launched. They weren't challenging the spy agency's specific choice of targets, but mainly the timing of strikes.

The CIA initially chafed at the idea of giving the State Department more of a voice in the process. Under a compromise reached around the year 2011, CIA officers would notify their embassy counterparts in Islamabad when a strike in Pakistan was planned, so then-U.S. ambassador Cameron Munter or another senior diplomat could decide whether to "concur" or "non-concur." Mr. Munter declined to comment.

Diplomats in Islamabad would communicate the decision to their superiors in Washington. A main purpose was to give then-Secretary of State Clinton and her top aides a chance to consider whether she wanted to weigh in with the CIA director about a planned strike.

With the compromise, State Department-CIA tensions began to subside. Only once or twice during Mrs. Clinton's tenure at State did U.S. diplomats object to a planned CIA strike, according to congressional and law-enforcement officials familiar with the emails.

U.S. diplomats in Pakistan and Washington usually relayed and discussed their concur or non-concur decisions via the State Department's more-secure messaging system. But about a half-dozen times, when they were away from more-secure equipment, they improvised by sending emails on their smartphones about whether they backed an impending strike or not, the officials said.

The time available to the State Department to weigh in on a planned strike varied widely, from several days to as little as 20 or 30 minutes. "If a strike was imminent, it was futile to use the high side, which no one would see for seven hours," said one official.

Adding to those communications hurdles, U.S. intelligence officials privately objected to the State Department even using its high-side system. They wanted diplomats to use a still-more-secure system called the Joint Worldwide Intelligence Community Systems, or JWICs. State Department officials don't have ready access to that system, even in Washington. If drone-strike decisions were needed quickly, it wouldn't be an option, officials said.

Some officials chafed at pressure to send internal deliberations through intelligence channels, since they were discussing whether to push back against the CIA, congressional officials said.

The Wall Street Journal first reported on the State Department-CIA tug-of-war over the drone program in 2011.

Under pressure to address critics abroad, Mr. Obama pledged to increase the transparency of drone operations by shifting, as much as possible, control of drone programs around the world to the U.S. military instead of the CIA. An exception was made for Pakistan.

But even in Pakistan, Mr. Obama recently signaled a shift. The drone strike that killed Taliban leader Mullah Akhtar Mansour last month was conducted by the military, not the CIA, and the outcome was disclosed.

While the CIA still controls drones over the tribal areas of Pakistan near Afghanistan, the pace of strikes has declined dramatically in recent years. U.S. officials say there are fewer al Qaeda targets there now that the CIA can find.

Fars News Agency
ISIL Posts Online Target List Including British, American, Canadian, Australian Residents
Friday, 10 June 2016

Tehran - The ISIL hackers posted the full names and home addresses of around 8,000 "targets" and urged extremist sympathizers to "kill them strongly" in a chilling new online threat.
The list includes 39 British residents as well as 7,848 Americans, 312 Canadians and 69 Australians which it wants murdered "as revenge", Daily Express reported.

It is not known if the list, which was published in English and Arabic, consisted of new names or those featured in earlier kill lists posted by the warped online ISIL activists.

Hackers claiming to be from the 'Cyber Caliphate' also posted satellite images of US air bases on its Telegram account, but the same images could be found on Google Earth.

The United Cyber Caliphate has previously published similar lists, such as one in 2015 revealing the full names of 3,600 New York residents as well as their addresses underneath the headline: "We Want Them #Dead."

The twisted online fanatics also reportedly hacked into US State Department records last year and released private information about 43 employees it wanted executed.

In November 2015, the cyber terrorists leaked details of 54,000 Twitter accounts, including passwords, in a show of online power that sent shockwaves through social media.

According to a report by American intelligence firm Flashpoint, the United Cyber Caliphate was formed in April 2015 after a merger of several radical hacking groups.

But the report also revealed that the collective is "poorly organized". It is not known if there have already been any attacks on the individuals named on any of the terrorists' lists.

Canberra Times

Dotcom, Assange warn of hacking

Sunday, 26 June 2016

Byline: Chris Zappone

Section: general

Canberra - Did Kim Dotcom warn the world the Democratic Party hacking was coming? Megaupload founder Kim Dotcom said last year he knew of information that would create an obstacle for Hillary Clinton's 2016 presidential election bid, explaining WikiLeaks' Julian Assange would prove a thorn in the side of the presumptive presidential candidate.
Last week a hacker going by the name Guccifer 2.0 released what appeared to be the Democratic Party's research on presumptive Republican nominee Donald Trump.

The hacker has since produced more reports with alleged information about Mrs Clinton's donors. Mr Assange, who reportedly holds the rest of the Democratic Party hack information, says more will soon be released.

When contacted about future data releases, WikiLeaks replied only: "We have a very big publishing year ahead." While hacks of US presidential campaigns have happened before, the prospect of hackers - especially ones backed by a foreign nation - dumping US election- related data during the campaign and for the global public's consumption is new.

It's significant that the Russian actions against US political targets were potentially tipped months earlier. In the shadowy world of the cyber competition, attributions of hacking is often as slow as seven months after they are discovered.Mr Dotcom's warning suggested evidence of such an attack was available months before the event was revealed. Guccifer 2.0 said his hacking effort had been under way for almost a year. Based on the nature and details of the attack, independent researchers in the US concluded the hack was conducted by a group linked to the Russian government.

Asked this week if the information Mr Assange claimed to have on Mrs Clinton's campaign came from Russian hacks, Mr Dotcom replied: "No comment." Earlier this month, Mr Assange said his site would provide enough evidence to indict Mrs Clinton. Although Mrs Clinton is the subject of investigations over her handling of emails, Mr Assange admitted it was unlikely the US Justice Department would indict her based on whatever information he had.

Mr Assange, who has lived at the Ecuadorian embassy in London since 2012 to avoid a series of extraditions that could have him tried in the US for his role in the Cablegate leak, is considered friendly to Russian interests. Mr Assange claims to have helped former NSA contractor Edward Snowden travel to Russia.

Reuters

Google, Facebook quietly move toward automatic blocking of extremist videos

Saturday, 25 June 2016

Section: general

San Francisco and Washington-- Some of the web's biggest destinations for watching videos have quietly started using automation to remove extremist content from their sites, according to two people familiar with the process.
The move is a major step forward for internet companies that are eager to eradicate violent propaganda from their sites and are under pressure to do so from governments around the world as attacks by extremists proliferate, from Syria to Belgium and the United States.

YouTube and Facebook are among the sites deploying systems to block or rapidly take down Islamic State videos and other similar material, the sources said.

The technology was originally developed to identify and remove copyright-protected content on video sites. It looks for hashes," a type of unique digital fingerprint that internet companies automatically assign to specific videos, allowing all content with matching fingerprints to be removed rapidly.

Such a system would catch attempts to repost content already identified as unacceptable, but would not automatically block videos that have not been seen before.

The companies would not confirm that they are using the method or talk about how it might be employed, but numerous people familiar with the technology said that posted videos could be checked against a database of banned content to identify new postings of, say, a beheading or a lecture inciting violence.

The two sources would not discuss how much human work goes into reviewing videos identified as matches or near-matches by the technology. They also would not say how videos in the databases were initially identified as extremist.

Use of the new technology is likely to be refined over time as internet companies continue to discuss the issue internally and with competitors and other interested parties.

In late April, amid pressure from U.S. President Barack Obama and other U.S. and European leaders concerned about online radicalization, internet companies including Alphabet Inc's YouTube, Twitter Inc, Facebook Inc and CloudFlare held a call to discuss options, including a content-blocking system put forward by the private Counter Extremism Project, according to one person on the call and three who were briefed on what was discussed.

The discussions underscored the central but difficult role some of the world's most influential companies now play in addressing issues such as terrorism, free speech and the lines between government and corporate authority.

None of the companies at this point has embraced the anti- extremist group's system, and they have typically been wary of outside intervention in how their sites should be policed.

It's a little bit different than copyright or child pornography, where things are very clearly illegal," said Seamus Hughes, deputy director of George Washington University's Program on Extremism.

Extremist content exists on a spectrum, Hughes said, and different web companies draw the line in different places.

Most have relied until now mainly on users to flag content that violates their terms of service, and many still do. Flagged material is then individually reviewed by human editors who delete postings found to be in violation.

The companies now using automation are not publicly discussing it, two sources said, in part out of concern that terrorists might learn how to manipulate their systems or that repressive regimes might insist the technology be used to censor opponents.

There's no upside in these companies talking about it," said Matthew Prince, chief executive of content distribution company CloudFlare. Why would they brag about censorship?"

The two people familiar with the still-evolving industry practice confirmed it to Reuters after the Counter Extremism Project publicly described its content-blocking system for the first time last week and urged the big internet companies to adopt it.

WARY OF OUTSIDE SOLUTION

The April call was led by Facebook's head of global policy management, Monika Bickert, sources with knowledge of the call said. On it, Facebook presented options for discussion, according to one participant, including the one proposed by the non-profit Counter Extremism Project.

The anti-extremism group was founded by, among others, Frances Townsend, who advised former president George W. Bush on homeland security, and Mark Wallace, who was deputy campaign manager for the Bush 2004 re-election campaign.

Three sources with knowledge of the April call said that companies expressed wariness of letting an outside group decide what defined unacceptable content.

Other alternatives raised on the call included establishing a new industry- controlled nonprofit or expanding an existing industry-controlled nonprofit. All the options discussed involved hashing technology.

The model for an industry-funded organization might be the nonprofit National Center for Missing and Exploited Children, which identifies known child pornography images using a system known as PhotoDNA. The system is licensed for free by Microsoft Corp.

Microsoft announced in May it was providing funding and technical support to Dartmouth College computer scientist Hany Farid, who works with the Counter Extremism Project and helped develop PhotoDNA, to develop a technology to help stakeholders identify copies of patently terrorist content."

Facebook's Bickert agreed with some of the concerns voiced during the call about the Counter Extremism Project's proposal, two people familiar with the events said. She declined to comment publicly on the call or on Facebook's efforts, except to note in a statement that Facebook is exploring with others in industry ways we can collaboratively work to remove content that violates our policies against terrorism."

In recent weeks, one source said, Facebook has sent out a survey to other companies soliciting their opinions on different options for industry collaboration on the issue.

William Fitzgerald, a spokesman for Alphabet's Google unit, which owns YouTube, also declined to comment on the call or about the company's automated efforts to police content.

A Twitter spokesman said the company was still evaluating the Counter Extremism Project's proposal and had not yet taken a position."

A former Google employee said people there had long debated what else besides thwarting copyright violations or sharing revenue with creators the company should do with its Content ID system. Google's system for content-matching is older and far more sophisticated than Facebook's, according to people familiar with both.

Lisa Monaco, senior adviser to the U.S. president on counterterrorism, said in a statement that the White House welcomed initiatives that seek to help companies better respond to the threat posed by terrorists' activities online.

The post Google, Facebook quietly move toward automatic blocking of extremist videos appeared first on Cyprus Mail.

CBC.CA

Cybersecurity threat 'keeps us up at night,' says Hydro Ottawa CEO

Saturday, 25 June 2016

Byline: Staff Writer

Section: general

Ottawa- As the electricity grid becomes more and more connected to the internet, Hydro Ottawa says it's investing heavily to protect the system from cyber attacks.
"It's huge," said Hydro Ottawa CEO Bryce Conrad of cybersecurity. "It keeps us up at night."

Conrad described how someone sitting in a bedroom at a computer on the other side of the world can try to hack into a utility's information systems and do damaging things ? like take down a grid.

"There are lots of examples out there where this has come true."

And Conrad says he doesn't pretend it can't happen in Ottawa.

"We're a G7 capital, so we're not just Hydro Ottawa, we're the provider of electricity to a G7 capital. If you don't have electricity in the morning, you're not doing a whole lot," he added.

Connecting customers while preventing attacks

Cybersecurity is detailed as a risk facing the utility in the five-year strategy document that Hydro Ottawa tabled earlier this week at an Ottawa city council meeting.

The strategy describes an industry in the midst of transformation in which electricity systems are converging with, and are increasingly dependent on, information technology.

Hydro Ottawa anticipates big changes in the coming years ? from increased sales of electric cars to innovations that come from more customers being digitally connected to a smart grid, a system of resources to better manage consumption.

But having people, their homes, their appliances, and their vehicles connected to the internet all the time poses a security challenge for an electric utility like Hydro Ottawa.

"As we become more customer-centric, and give customers more tools to sort of manage these things, you're effectively opening up your system for your customers," said Conrad.

"What you're trying to do is open it up for them and keep the back door closed to someone who wants to do something nefarious."

Heavy investment in command and control centre

That's why Hydro Ottawa considers cybersecurity every time it buys a piece of software or technology, according to Conrad.

"We have to invest heavily in cybersecurity and making sure our systems, particularly our command and control systems, are as robust and protected as they possibly can be," he said.

The electricity industry gets together regularly to discuss best practices for protecting utilities from the threat of hacks emanating from terrorists, organized crime groups, or other foreign entities.

"I'll never say we're 100 per cent protected, but we're in pretty good shape."

ITAR-TASS World Service

State Duma adopts package of anti-terrorist bills

Saturday, 25 June 2016

Byline: Staff Writer

Section: general

Russia's State Duma on Friday adopted in the second and third, final reading a package of anti-terrorist bills proposed by lower house member Irina Yarovaya and upper house member Viktor Ozerov.

The initiatives sparked great public controversy and continued to be edited up to the last moment. Eventually the idea of terminating the Russian citizenship of those dual or multiple citizens who have committed terrorist crimes or proved to have been employed by foreign special services was dropped. Under the just- adopted version communication operators will be obliged to keep information about their subscribers' connections for a period of three years, and of the content transmitted, including videos, for six months. For the owners of messenger services and social networks these rules have been eased somewhat: they will be not allowed to delete information about the content transmitted and their users for twelve months, and not three years, contrary to the original version of the bill.

Messenger services, such as WhatsApp and Telegram will be fined up to one million rubles, should they refuse to disclose content at the request of the federal security service FSB.

Anti- sect amendments

A special group of amendments defines what "missionary activity" is and prohibits attempts to conduct it on behalf of religious associations whose aims contradict the law. The legislators banned missionary activities that violate public security and order, extremist actions, coercion into ruining families, and encroachments on the freedom of the person and rights and freedoms of citizens. A ban is imposed on missionary activities aimed at inducing suicide, at creating obstructions to getting mandatory education and at persuasion of individuals to refuse to perform their legally mandatory civic duties.

Missionary and preaching activities that breech legislation on the freedom of conscience and faith and on religious associations will be punishable with a fine of 5,000 rubles to 50,000 rubles ($77 to $7700) for individuals, and 100,000 rubles to 1,000,000 ($1,500 to $15,000). Foreign citizens will face expulsion from Russia. Under the new rules, all printed, audio and video content being distributed by a religious organization must have proper markings and bear the organization's full name.

Life sentence for international terrorism

The Criminal Code's list of crimes against peace and security of humanity was expanded to incorporate "international terrorism" and life imprisonment established as the maximum punishment. The minimum prison term for a terrorist attack will be increased from eight years to ten and from ten years to twelve (if the crime was committed by a group of persons or resulted in loss of human life).

The newly-adopted law contains a new, fuller definition of the financing of terrorism. It will be understood as "provision or raising of funds or provision of financial services with the awareness that they are meant for financing a terrorist organization, or plotting or committing terrorist crimes."

Public calls for terrorism or statements made in public in the Internet with the aim of excusing it will be punishable with a fine of up to 1,000,000 rubles ($15,000) or a prison term of five to seven years. Publicly expressed excuses are defined as "public statements to the effect the ideology and practices of terrorism are correct and worth supporting and following." Participation in a terrorist organization will

be punishable with prison terms of ten to twenty years (in contrast to the currently established ones of five to ten years).

Failure to report a terrorist attack

Failure to report preparations for terrorist crimes or committed terrorist crimes will entail a fine of up to 100,000 rubles ($15,000) or forced labor of up to twelve months or a twelve-month prison term. Failure to report preparations for a terrorist attack or a committed terrorist attack by one's spouse or close relative will not be punishable.

Minimum punishments

Punishments for organizing or participating in armed groups, including those abroad will be tightened. The maximum prison term for this offence is raised to five years. The Criminal Code is complemented with a new article establishing punishment for suborning into or recruitment for mass unrest. Such wrongdoing will be fined with 300,000 rubles to 700,000 rubles ($4,600 to $10,800) or a prison term of five to ten years.

Minimum punishments have been introduced under Article 282 of the Criminal Code (Incitement of Hatred or Humiliation of Human Dignity). The mildest punishment is set at three years and the maximum one, at six. Punishment for organizing an extremist organization or extremist community or financing extremist activities was tightened accordingly.

The age of accountability for terrorism is lowered to 14 years. The list of aggravating circumstances has been expanded to incorporate crimes committed in the context of an armed conflict or combat operations.

The amendments will take effect on July 20, 2016.

The Nation Multi

Military chiefs call for more robots for national security

Monday, 27 June 2016

Byline: Juthathip Lucksanawong

Section: general

Bangkok - The 26-kilogram, rectangular Portable Rescue Robot (PRR) stretched its manipulator arm, complete with a night vision camera, to surveil the area. With a wireless control system and two additional blades in front, the PRR showed off its ability to move freely in hostile terrain.
The display was performed in front of veteran military officers and weapons experts who met at a recent seminar on the development of military technology.

Mahanakorn University of Technology developed the robot, one of several robot prototypes that experts are collaboratively trying to develop to support national security missions. Using robots, especially for bomb retrieval missions, has long been considered by the Thai military.

Over the recent decade, Thailand has seen both the Southern insurgency and terrorism plaguing national security, said Sqn Leader Jiradett Kerdsri, director of data and communication division of the Defence Technology Institute (DTI).

"While insurgency and explosions are ongoing in the South, the dreadful bombing in August last year at Ratchaprasong intersection, the heart of Bangkok city, also irked state security," he said.

Such troubles affect the country's tourism, economy and trustworthiness, Jiradett said. "Foreign investors and tourists won't risk coming to a hazardous territory," he said.

It is essential, he added, for the DTI to select much-needed defence technology to be developed to serve the country's security goals.

Inventing bomb retrieval robots is part of the DTI's research plan initiated in 2009 to promote self-reliance in terms of national security and reduce the need to procure defence systems and equipment from other countries, said General Sompong Mukdaskul, DTI director-general.

Since its official establishment seven years ago, the DTI, under Ministry of Defence (MoD) oversight, has carried out five defence technology research plans focusing on rockets, unmanned aerial vehicles (UAVs), simulation technology, infantry fighting vehicles (IFVs), and military information and communication technology.

The DTI's prototypes in each category have been distributed to the three branches of the Armed Forces - Army, Navy and Air Force - and the police.

When the DTI began supplying defence forces with equipment and systems, Sompong found that each user had different technology requirements. To meet those requirements, the DTI needed to listen to what users required before research began, he added.

"Collecting feedback and comments from military and police authorities is the DTI's normal practice before and after each piece of defence equipment is unveiled," the director-general said.

The PRR's recent demonstration, and that of its robotic colleagues, in front of veteran officers and experts was part of that feedback process to fulfil the ambition to build sophisticated robots that can help to keep people safe in the field.

Air Force representatives told the seminar that the force needs robots that support remote operations with wireless and fibre optic control systems. The force has to patrol remote, inaccessible areas where land mines are a danger that could be mitigated by capable remote control robots, said Wing Commander Navin Vudhironnarith, deputy chief of the Air Force's Explosive Ordnance Disposal (EOD) force.

The robots also need to be lightweight with fire-suppression systems, including recoilless water jets, for safety, he added.

The Army, on the other hand, needs user-friendly robots with very high capabilities, said Colonel Krittipas Cruanate, chief of the Army's EOD.

"A single robot should not have all the functions. Some tasks do not need a full, heavy scanning system. Only reliable and enduring sensors and portable X-rays are necessary," he said

The colonel, who has seen numerous officers and ordinary people killed in bombings in the Southern violence, said robots are necessary because they could help to reduce fatalities explosive disposal missions. "If we'd had high-tech robotics to carry out deadly missions, people and authorities would not have died," he said.

To accomplish this new technological mission, participants agreed that academic institutions play a crucial role in developing new innovations because they act as centres of "know how" bringing together scholars and experts, Sompong said.

"Education institutions have performed tonnes of research but have no chance to apply their studies [in real situations]," he said.

The DTI director-general said he sees potential for knowledge transfers between these institutions and his agency.

"Their knowledge needs to be transferred and applied to the DTI's work. By doing this, they have an opportunity to further develop their technology and it saves time for us to conduct research on the robots," he said.

In addition to educational institutions, the industrial sector also has the potential to contribute to robotics projects.

To pioneer useful robots, industrial stakeholders need to get involved in terms of manufacturing, said Djitt Laowattana, lecturer at King Mongkut's University of Technology Thon Buri and founder and director of the Institute of Field Robotics (FIBO).

Djitt said industry is important because of its expertise in effectively managing resources in manufacturing and, especially, marketing and distribution.

The DTI knows how to invent technology but does not specialise in managing resources and budgets, he said. The government's support is required to entice the public sector to become more involved in robotics development, he added.

The government should catalyse the industry by introducing a "local materials" requirement to promote companies to use components available in the country, rather than imported ones, Djitt said, adding companies that utilise local materials should get government incentives. That would encourage others to adopt more technology and robotic components made in Thailand, he said.

When robots are produced and sold on a large scale, the lecturer said, the robotics industry would increasingly grow, leading innovators and manufacturers to become eager to help to produce defence systems contributing to national security.

"I just hope that future robots answer the needs of defence suppliers. [We should] not just launch [the idea] and then put it on a shelf after our lengthy discussion today," Sompong said. "And I just hope that the bomb retrieval robots will eventually be practical and meet international standards."

Press Trust of India

India to become full member of Missile Technology Control Regime

Monday, 27 June 2016

Section: general

New Delhi - In its first entry into any multilateral export control regime, India will today join the Missile Technology Control Regime (MTCR) as a full member, three days after it failed to get NSG membership due to stiff opposition from China and a few other countries.
"We applied for the membership of MTCR last year and all the procedural formalities have been completed. Tomorrow, Foreign Secretary S Jaishankar will sign the document of accession into MTCR in the presence of Ambassadors of France, Netherlands and Luxembourg," External Affairs Ministry spokesperson Vikas Swarup said.

Significantly, China, which stonewalled India's entry into the 48-nation Nuclear Suppliers Group (NSG) at the just- concluded Seoul plenary, is not a member of 34-nation MTCR.

Since its civil nuclear deal with the US, India has been trying to get into export control regimes like NSG, MTCR, the Australia Group and the Wassenaar Arrangement that regulate the conventional, nuclear, biological and chemicals weapons and technologies.

India's case in MTCR was opposed last year by Italy which is not happy with New Delhi over the marines dispute. However, after both marines, accused of murdering two fishermen off the Kerala coast in 2012, were allowed to return, the Italians have softened their opposition.

India's efforts to get into the MTCR also got a boost after it agreed to join the Hague Code of Conduct, dealing with the ballistic missile non- proliferation arrangement, earlier this month.

MTCR membership will enable India to buy high-end missile technology and also enhance its joint ventures with Russia.

The aim of the MTCR is to restrict the proliferation of missiles, complete rocket systems, unmanned air vehicles and related technology for those systems capable of carrying a 500 kilogramme payload for at least 300 kilometres, as well as systems intended for the delivery of weapons of mass destruction (WMD).

India to get access to almost 99% of U.S. defence technologies

Monday, 27 June 2016

Section: general

Washington - India will be the only country outside Washington's formal treaty allies that will gain access to almost 99 per cent of latest U.S.'s defence technologies after being recognised as a 'Major Defence Partner', a senior Obama administration official has said.
"India [now] enjoys access to [defence] technologies that is on a par with our treaty allies. That is a very unique status. India is the only other country that enjoys that status outside our formal treaty allies," the official told PTI explaining what 'Major Defence Partner' status means for India.

Early this month, after a meeting between U.S. President Barack Obama and Prime Minister Narendra Modi at the White House, the U.S., in a joint statement, recognised India as a 'Major Defence Partner'

"We were looking for something unique. This language you would not find in any arms transfer legislation or any of our existing policies. This is new guidance and new language that is intended to reflect the unique things that we have done with India under our defence partnership," the senior administration official said.

"This is intended to solidify the India-specific forward leaning policies for approval that the [U.S.] President and [Defence] Secretary [Ashton] Carter...and our export control system have implemented in the last eight years," the official said.

Under this recognition India would receive licence-free access to a wide range of dual-use technologies in conjunction with steps that New Delhi has committed to taking to advance its export control objectives.

Acknowledging that the impression in New Delhi was that India was not getting access to the kind of technology it needed from the U.S., the official said it was a constant source of discussion.

"[In reality], less than one per cent of all exports [requests] are denied [to India]. They are not denied because of India. They are denied because of global U.S. licencing policies. We do not share certain technologies with anybody in the world," the official asserted.

The perception in India that the denial of such technologies is reflective of India-U.S. relationship is far from the truth, the official has said.

According to the official, India being recognised as a "major defence partner puts it on par with our treaty allies." Inside the American bureaucratic system, such a recognition removes a number of major export control hurdles for India.

The category of 'Major Defence Partner' was created specifically for India, observed Ashley Tellis, of Carnegie Endowment for International Peace, a top American think-tank.

"It was meant to recognise that although India will not be an alliance partner of the United States, the administration seeks to treat it as such for purposes of giving it access to advanced technologies of the kind that are reserved for close US allies," Mr. Tellis told PTI.

"The U.S. expects that bilateral defence ties will only grow in the years ahead, that India and the United States will continue to work together especially regarding maritime security, that India will eventually be admitted to global non-proliferation regimes, and that it will sign the foundational agreements," he said in response to a question.

"As these developments materialise, India's access to U.S. technology will also increase, and the "major defence partner" moniker is intended to signal to both the outside world and to the U.S. bureaucracy

that oversees licensing that India is viewed as a unique collaborator and will be treated as such where access to advanced technologies are concerned," Mr. Tellis said.

Calling India a "Major Defence Partner" is "more a term of art than a technical designation", noted Richard M. Rossow, Wadhwani Chair in U.S. India Policy Studies at the Centre for Strategic and International Studies, another top American think-tank.

"It certainly captures what is emerging as a unique relationship, exhibited by programs such as the Defence Technology and Trade Initiative [DTTI] and the establishment of a dedicated 'India Rapid Reaction Cell' inside the Pentagon. Neither exists for a country other than India," he said.

"But the term 'Major Defence Partner' does not automatically trigger a specific process or program in the U.S. system. Our two countries are feeling their way around the contours of our defence relationship," Mr. Rossow told PTI.

"India desires advanced U.S. technology today, while the U.S. would like more clarity on the specific operations India may be willing to undertake in the future to contribute to regional security. It is a process that has seen great progress, which we hope will carry over into the next U.S. administration," Mr. Rossow said in response to a question.

Over the last one decade the defence trade between India and the U.S. has increased from being almost non-existent to more than $14 billion. This is expected to increase manifold as India embarks on a major defence modernisation drive.

Times of Israel

CyberArk eyes expansion in Asia

Monday, 27 June 2016

Byline: Shoshanna Solomon

Section: general

Jerusalem - Petah Tikva-based CyberArk, Israel's second-largest public cybersecurity company, plans to target the Asian and Latin American markets and mid-sized customers in the longer term to boost growth, Udi Mokady, president and chief executive officer of CyberArk, said in an interview.
Speaking with reporters last week at the sidelines of a cybersecurity conference in Tel Aviv, Mokady said enterprise customers are still the main focus of the company and CyberArk is still just "scratching the

surface" of the potential of these companies.But in the longer term the firm is also "looking at ways to address also the mid-market as part of our strategy."

CyberArk is a cybersecurity company that specializes in protecting "privileged accounts" on corporate servers. Privileged accounts are computer system user accounts that have extra privileges so that owners of those accounts can control important aspects of a server or network. Large computer systems, especially those that have been around for years, usually contain many such accounts that are no longer in use - either because they were set up specifically for certain no-longer relevant missions or because they belonged to former employees. These accounts are especially vulnerable to hacker accounts, as they aren't watched too closely.

CyberArk chokes off the possibility that privileged accounts will be abused by identifying and cutting off access to the accounts. The system sets up a policy on user accounts that forces users to change passwords on a regular basis, including dormant privileged accounts. In addition, the system sets up a "safe zone" for data to be managed when accessed from an account.

"We found that even though we were targeting enterprise, we got pull from mid-market -- universities, credit unions, law firms, things we weren't necessarily targeting, and so it shows us there is an opportunity and we are looking for ways to address that in 2017 and beyond," Mokady said in the interview. "Right now it is very much enterprise-focused."

The company, which held an initial public offering of shares on the Nasdaq in 2014, saw its shares surge as corporations flocked to buy security software amid higher levels of data breaches worldwide.

Today CyberArk, the largest Israeli public information security company in both revenue and in market capitalization, has more than 2,600 customers globally, of which more than 40% are Fortune 100 customers, according to data from a May 2016 presentation.

Revenues grew over 50 percent in 2014 and 2015, and in the first quarter of the year revenue jumped 43% to around $47 million compared to the same quarter a year earlier. Net income for the first quarter of 2016 rose to $4.3 million from $4.2 million in the same quarter in 2015. CyberArk in May forecast total revenue to rise by around 30% in 2016 to a range of $209 million to $211 million.

The company is also looking to increase its presence in the Asia Pacific, Mokady said. Last year the Americas accounted for 61% of its revenues while Europe, Middle East and Africa accounted for 31 percent. Just around 8% of sales were in Asia Pacific and Japan, according to the presentation. "We want to bring it much higher," Mokady said. "We want it to be toward the teens in the long term. The opportunity is tremendous." Latin America is also an opportunity for growth, he said. "They have the same problems, the same IT infrastructure, the same weaknesses."

Even as the company has posted strong results, its share price has has declined about 26% in the past year amid concerns that enterprise spending in cybersecurity software has started to slow, lackluster

results from peers and on worries about too-high valuations in the sector. The company has a market capitalization of about $1.61 billion, according to data compiled by Bloomberg.

CyberArk's share decline spurred speculation in January that the company would become an acquisition target for Israel's Check Point Software Technologies Ltd.

Mokady shrugged off the possibility of a company sale even as he sees the possibility of some consolidation in the industry among the smaller companies. "CyberArk is a buyer," he said. "We are going for it and being acquisitive. Naturally in any step of the way we will do what is right for the shareholders. But left alone, we are building it big. "

The company has made two acquisitions, Viewfinity, Inc., a Waltham, Massachusetts-based provider of Windows privilege management and application control software, for $30.5 million in cash, and Israeli firm CyberIntel.

Acquisitions "is part of our growth strategy and we are very pleased with the first two," Mokady said. "There is appetite and willingness to do more but there is no pressure because we have such a huge organic opportunity."

Wall Street Journal

Russian Hack Said To Reach Beyond Democrats

Monday, 27 June 2016

Byline: Nicole Hong

Section: general

New York - The attack on the Democratic National Committee's computer network this past spring was part of a broader monthslong campaign by Russian hackers against groups with ties to U.S. politics, according to a new report.
Party officials and security researchers disclosed about two weeks ago that the DNC's system was compromised in April by two hacking groups with links to Russian intelligence services, one of the largest known breaches of a U.S. political organization.

On Sunday, cybersecurity firm SecureWorks Corp. concluded that one of the hacking groups, dubbed "Fancy Bear" in security circles, also targeted the emails of presumptive Democratic nominee Hillary

Clinton's campaign, as well as email accounts belonging to U.S.-based military spouses, political activists and journalists who wrote critically about Russia and others.

Over the past year or so, the hackers tried to penetrate nearly 4,000 individual email accounts, researchers said.

Researchers believe the hackers wanted access to email accounts as part of an intelligence-gathering operation, as opposed to stealing information for financial gain. In one tactic, the hackers sent out mass emails containing links that asked victims to reset their passwords.

Users at two dozen email addresses associated with the DNC and Mrs. Clinton's campaign clicked on the links, but SecureWorks says it is unclear whether information was accessed. Researchers previously said the hackers gained access to the DNC's chat systems and research files, including the party's opposition research on presumptive Republican nominee Donald Trump.

The DNC is "confident" that Russian government hackers were responsible for the breach and has "deployed the recommended technology" to secure their systems, said a senior DNC official.

A representative of the Russian government couldn't be reached for comment. In a previous statement, a Kremlin spokesman said: "I completely rule out the possibility of the government or government structures being involved in this."

A spokesman for the Clinton campaign didn't respond to a request for comment.

New York Magazine

I, Snowbot

Monday, 27 June 2016

Byline: Andrew Rice

Section: general

New York - Edward Snowden lay on his back in the rear of a Ford Escape, hidden from view and momentarily unconscious, as I drove him to the Whitney museum one recent morning to meet some friends from the art world. Along West Street, clotted with traffic near the memorial pools of the World Trade Center, a computerized voice from my iPhone issued directions via the GPS satellites above. Snowden's lawyer, Ben Wizner of the American Civil Liberties Union, was sitting shotgun, chattily

recapping his client's recent activities. For a fugitive wanted by the FBI for revealing classified spying programs who lives in an undisclosed location in Russia, Snowden was managing to maintain a rather busy schedule around Manhattan.
A couple nights earlier, at the New York Times building, Wizner had watched Snowden trounce Fareed Zakaria in a public debate over computer encryption. "He did Tribeca," the lawyer added, referring to a surprise appearance at the film festival, where Snowden had drawn gasps as he crossed the stage at an event called the Disruptive Innovation Awards. Wizner stopped himself mid- sentence, laughing at the absurdity of his pronoun choice: "He!" Behind us, Snowden stared blankly upward, his face bouncing beneath a sheet of Bubble Wrap as the car rattled over the cobblestones of the Meatpacking District.

Snowden's body might be confined to Moscow, but the former NSA computer specialist has hacked a work-around: a robot. If he wants to make his physical presence felt in the United States, he can connect to a wheeled contraption called a BeamPro, a flat-screen monitor that stands atop a pair of legs, five-foot-two in all, with a camera that acts as a swiveling Cyclops eye. Inevitably, people call it the "Snowbot." The avatar resides at the Manhattan offices of the ACLU, where it takes meetings and occasionally travels to speaking engagements. (You can Google pictures of the Snowbot posing with Sergey Brin at TED.) Undeniably, it's a gimmick: a tool in the campaign to advance Snowden's cause -- and his case for clemency -- by building his cultural and intellectual celebrity. But the technology is of real symbolic and practical use to Snowden, who hopes to prove that the internet can overcome the power of governments, the strictures of exile, and isolation. It all amounts to an unprecedented act of defiance, a genuine enemy of the state carousing in plain view.

We unloaded the Snowbot in front of the Whitney, where a small group had gathered to meet us for a private viewing of a multimedia exhibition by the filmmaker Laura Poitras. It was Poitras whom Snowden first contacted, anonymously, in 2013, referring to the existence of a surveillance system "whose reach is unlimited but whose safeguards are not." Their relationship resulted in explosive news articles and a documentary, Citizenfour -- work that won a Pulitzer and an Oscar and incited global outrage. But the disclosures came at a high price for their source. If Snowden couldn't come home, Poitras at least wanted him to share vicariously in the experience of her Whitney show, "Astro Noise," which took its name from an encrypted file of documents he had spirited out of the secret NSA site where he worked in Hawaii. So she had arranged a personal tour.

Outside an eighth-floor gallery, a crowd of Poitras's collaborators and Whitney curators clustered around the Snowbot as a white circle twirled on its monitor. Then, suddenly, the screen awoke and Snowden was there.

"Hey!" Wizner said, and the group erupted in awkward laughter. The famous fugitive was wearing a gray T-shirt, his face pallid and unshaven. (He calls himself "an indoor cat.") His voice sounded choppy, but some fiddling resolved the problem, and Poitras, soft-spoken and clad in black, made introductions. Snowden's preternaturally eloquent Hong Kong hotel-room encounter with Poitras and the Guardian journalists investigating his leaks formed the core of Citizenfour, but even some of those who worked on

the documentary had never met its protagonist. One of the cinematographers came forward and wrapped him in a hug.

"I don't have hands," Snowden apologized. "The most I can do is maybe ..."

He scooted forward.

Sitting in the same homemade studio he uses for his frequent speaking engagements, Snowden could control the robot's movements with his computer, maneuvering with uncanny agility, swiveling to make eye contact with people as they spoke to him.

Poitras began with the show's opening piece, a colorful array of prints that resembled modern abstracts but were actually found objects: visualizations of intercepted satellite signals that turned up in the vast trove of NSA documents. "The whole show, there's a lot of deep research that's going on behind it," she said. She led Snowden into a darkened gallery, where a spooky ambient soundscape was playing over video footage of a U.S. military interrogation. Momentarily disoriented, he careened into a bench. But Snowden quickly figured out how to navigate in the dark. When he came to parts of the exhibit that required complicated movements -- lying on a platform to take in the watchful night sky over Yemen, or craning to look at an NSA document through a slit in the wall -- the humans hoisted him into position.

"Wow, okay, I see it," Snowden said as one of Poitras's researchers held him up to view footage of a drone strike's aftermath. "This is a surreal experience for a number of reasons."

When the tour was over, Snowden held an impromptu discussion, likening his decision to become a dissident to a risky artistic choice. "There's always that moment where you step out and there's nothing underneath you," he said. "You hope that you can build that airplane on the way down, or if you don't, that the world will catch you. In my case, I've been falling ever since." Still, Snowden said he had no regrets. "I do have to say," he told Poitras, "that I will be forever grateful that you took me seriously."

As usual, though, when the questions turned to the details of his non-robotic existence, Snowden remained courteously evasive. "What's a day in the life now?" asked Nicholas Holmes, the Whitney's general counsel. "Do you go for walks in the park?"

"Well," the Snowbot replied, "I go for walks in the Whitney, apparently."

The idea that Snowden is still walking the American streets, virtually or otherwise, is infuriating to his former employers in the U.S.-intelligence community. Its leaders no longer make ominous jokes about wanting to put him on a drone kill list -- as former NSA and CIA director Michael Hayden did in 2013 -- but they still vilify him and maintain that he did real harm to America's safety and international standing. While Snowden's leaks revealed the NSA's controversial and possibly unconstitutional bulk collection of domestic internet traffic and telephone metadata, they also exposed technical details about many other classified activities, including overseas surveillance programs, secret diplomatic arrangements, and

operations targeting legitimate adversaries. The spy agencies warn that the public doesn't comprehend the degree of damage done to their protective capabilities, even as events like the Orlando nightclub massacre demonstrate the destructive reach of terrorist ideology. The fallout from Snowden's actions may have prompted a debate about security and privacy that even President Obama acknowledges "will make us stronger," but there has been no such reassessment, at least officially, of Snowden himself. He still faces charges of violating the federal Espionage Act, crimes that could carry a decades-long prison sentence.

When Snowden first revealed the NSA's surveillance -- and his own identity -- to the world three years ago this month, there was little reason to believe that he would be in a position to communicate much of anything in the future. The last person to leak classified information of such magnitude, Chelsea Manning, was sentenced to 35 years in prison. (Manning, who was held in solitary confinement while awaiting trial, has largely communicated to the public through letters.) Yet so far, to his own surprise, Snowden has managed to avoid the long arm of U.S. law enforcement by finding asylum in Russia. Leaving aside, at least for the moment, the ethics of his actions (and the internal contradictions of his residence in an authoritarian state ruled by a former KGB operative), Snowden's case is, in fact, a study in the boundless freedoms the internet enables. It has allowed him to become a champion of civil liberties and an adviser to the tech community -- which has lately become radicalized against surveillance -- and, in the process, the world's most famous privacy advocate. After he appeared on Twitter last September -- his first message was "Can you hear me now?" -- he quickly amassed some two million followers.

"I feel like we're sort of dancing around the leadership conversation," Snowden said to me recently as I sat with him at the ACLU offices. Over the past few months, we have encountered one another with some regularity, and while I can't claim to know him as a flesh-and-blood person, I've seen his intellect in its native habitat. He is at once exhaustively loquacious and reflexively self-protective, prone to hide behind smooth oratory. But occasionally, he has let down his guard and talked like a human being. "I'm able to actually have influence on the issues that I care about, the same influence I didn't have when I was sitting at the NSA," Snowden told me. He claims that many of his former colleagues would agree that the programs he exposed were wrongfully intrusive. "But they have no voice, they have no clout," he said. "One of the weirder things that's come out of this is the fact that I can actually occupy that role." Even as the White House and the intelligence chiefs brand him a criminal, he says, they are constantly forced to contend with his opinions. "They're saying they still don't like me -- tut-tut, very bad -- but they recognize that it was the right decision, that the public should have known about this."

Needless to say, it is initially disorienting to hear messages of usurpation emitted, with a touch of Daft Punk-ish reverb, from a $14,000 piece of electronic equipment. Upon meeting the Snowbot, people tend to become flustered -- there he is, that face you know, looking at you. That feeling, familiar to anyone who's spotted a celebrity in a coffee shop, is all the more strange when the celebrity is supposed to be banished to the other end of the Earth. And yet he is here, occupying the same physical space. The technology of "telepresence" feels different from talking to a computer screen; somehow, the fact that Snowden is standing in front of you, looking straight into your eyes, renders the experience less like

enhanced telephoning and more like primitive teleporting. Snowden sometimes tries to put people at ease by joking about his limitations, saying humans have nothing to fear from robots so long as we have stairs and Wi-Fi dead zones in elevators. Still, he is quite good at maneuvering on level ground, controlling the robot's movements with his keyboard like a gamer playing Minecraft. The eye contact, however, is an illusion--Snowden has learned to look straight into his computer's camera instead of focusing on the faces on his screen.

Here's the really odd thing, though: After a while, you stop noticing that he is a robot, just as you have learned to forget that the disembodied voice at your ear is a phone. Snowden sees this all the time, whether he is talking to audiences in auditoriums or holding meetings via videoconference. "There's always that initial friction, that moment where everybody's like, 'Wow, this is crazy,' but then it melts away," Snowden told me, and after that, "regardless of the fact that the FBI has a field office in New York, I can be hanging out in New York museums." The technology feels irresistible, inevitable. He's the first robot I ever met; I doubt he'll be the last.

Wizner, the head of the ACLU's Speech, Privacy, and Technology Project, says that Snowden asked him to do some research on telepresence in their first conversation, back when he was still very much on the lam. Now that his situation has stabilized -- at least for the time being -- he and Snowden's small coterie of advisers are discussing ways they might use it for a widening range of purposes. Glenn Greenwald, one of Snowden's original journalistic collaborators, jokingly talks about taking the Snowbot on the road. "I would love to let it loose in the parking lot of Fort Meade," where the NSA is headquartered, he said. "Or to randomly go into grocery stores." More seriously, Snowden's advisers are in discussions about a research fellowship at a major American university. Already, the Snowbot has twice taken road trips to Princeton University, where he has participated in wide-ranging discussions about the NSA's capabilities with a group of renowned academic computer-security experts, rolling up to cryptographers during coffee breaks and dutifully posing for selfies.

For larger gatherings, Snowden usually dispenses with the robot, addressing audiences from giant screens. (He often opens with an ironic reference to Big Brother.) He is scheduled to make more than 50 such appearances around the world this year, earning speaking fees that can reach more than $25,000 per appearance, though many speeches are pro bono. Besides allowing Snowden to make a good living, his virtual travels on the public- lecture circuit are part of a concerted campaign to situate him within a widening zone of political acceptability. "One of the things we were trying to do is to normalize him," says Greenwald. "Normalize his life, normalize his presence." In 2014, Snowden joined Poitras and Greenwald on the board of the Freedom of the Press Foundation, a San Francisco nonprofit, and last year he was elected chairman. It serves as a base for his advocacy and gives him access to a staff of technologists with whom he has been working on encryption projects, tools intended to allow journalists to communicate with "people that live in situations of threat" -- in other words, people like Snowden himself.

Through a network of intermediaries -- chief among them Wizner, who acts as his advocate, gatekeeper, and talent agent in the United States -- Snowden is able to establish contact with almost anyone he

desires to meet. "Ed's now getting a lot of people on the phone, and it's broadening his horizons," says the author Ron Suskind, who has spoken with him on several occasions and recently had him lecture to a class he and Lawrence Lessig were teaching at Harvard Law School. Snowden also recently spoke to Amal Clooney's law class at Columbia, starred in an episode of the Vice show on HBO, and published a manifesto on whistle-blowing on the Intercept, the website Poitras and Greenwald started with the billionaire Pierre Omidyar. And he has been maintaining his presence on Twitter, where he has been playfully talking up Oliver Stone's forthcoming film, Snowden, which will star Joseph Gordon-Levitt.

The biopic's September release date matches up with Wizner's timetable for mobilizing a clemency appeal to Obama. "We're going to make a very strong case between now and the end of this administration that this is one of those rare cases for which the pardon power exists," Wizner said. "It's not for when somebody didn't break the law. It's for when they did and there are extraordinary reasons for not enforcing the law against the person." He says that while no single event is likely to shift opinion in Washington, Snowden's activities work "in the aggregate" to further his cause.

One thing Snowden refuses to do, however, is apologize. If anything, the last three years have turned him more strident. Whereas he once espoused a fuzzy dorm-room libertarianism -- "some of it was kind of rudimentary," Greenwald recalls -- today he offers a more traditional leftist critique of the "deep state." On Twitter, he has been admiring of Bernie Sanders, acerbic about Hillary Clinton's foreign policy, and bitingly sarcastic about her handling of classified emails. In February, he tweeted: "2016: a choice between Donald Trump and Goldman Sachs." He sees himself as part of a hacktivist movement, and he took pride when the anonymous source behind the massive cache of offshore banking data known as the Panama Papers cited Snowden's example. In his Intercept essay, he called such leaking "an act of resistance."

WNYC recently staged a sold-out Friday-night event at the Brooklyn Academy of Music, not far from Fort Greene Park, where some artists surreptitiously erected a Snowden bust last year. At the appointed time, the fugitive appeared on a screen at the front of an ornate opera hall. It was around 2:30 a.m. in Moscow, but Snowden looked wide-awake, wearing an open-collared shirt and blazer and his customary stubble. "In an extraordinary and unpredictable way," he told the audience, "my own circumstances show there is a model that ensures that even if we're left without a state, we aren't left without a voice."

When Snowden went public, one of the first people he sought out was a historical antecedent: Daniel Ellsberg, the military analyst who leaked the Pentagon Papers. He, too, was briefly a fugitive and faced Espionage Act charges, until they were dropped because of the illegal retaliatory actions of President Nixon. Now 85, Ellsberg was eager to talk to Snowden and they connected over an encrypted chat program.

"I had the feeling that, as I suspected from the beginning, we really were kindred souls," Ellsberg told me.

Ellsberg, mindful of Manning's experience, advised Snowden to give up any thought of returning home. Snowden was inclined to agree. From the beginning, he had spoken fatalistically about the consequences of his actions. "All my options are bad," Snowden acknowledged in his first interview in Hong Kong, which was published in the Guardian. If the American government didn't grab him, the Chinese might, just to find out what he knew. He hinted that the CIA might even try to kill him, either directly or through an intermediary like a triad gang. "And that's a fear I'll live under for the rest of my life, however long that happens to be," Snowden said at the time.

"He didn't have a plan," says Wizner. Snowden assumed that he would probably be silenced in one way or another, so he worked with a sympathetic programmer in the United States to design a website, supportonlinerights.com, which was to contain a letter addressed to the public. But instead, he more or less got away with it. After a nervy flight and an agonizing five-week wait in limbo at the Moscow airport, he was granted temporary asylum in Russia by President Vladimir Putin. Photos soon appeared in the Russian media showing Snowden pushing a grocery cart and looking slyly over his shoulder on a riverboat ride. It was an uneasy deliverance, though, one seemingly subject to Putin's unpredictable geopolitical power considerations.

Snowden argues that he was put in Russia by the U.S. government, which canceled his passport while he was en route to Ecuador, trapping him in Moscow during a layover. But to critics, his dependence on Putin is discrediting. "I am not saying that he is a Russian spy, but he is in a tough spot," says journalist Fred Kaplan, author of the recent book Dark Territory: The Secret History of Cyber War. "He is in a position where, because of his captive status, he can't really say anything that terribly critical about his hosts, who happen to be some of the most sophisticated and intrusive cyberespionage hackers in the world." Many in the intelligence community darkly speculate about the nature of Snowden's accommodation with the FSB, the Russian security service, which is not renowned for its hospitality or respect for civil liberties.

Although Snowden acknowledges that he was approached by the FSB, he claims he has given them no information or assistance, and he vehemently denies he is anyone's puppet. He cheered the release of the Panama Papers, which contained voluminous evidence of corruption in Putin's inner circle. "I have called the Russian president a liar based on his statements on surveillance, in print, in the Guardian," he said with an uncharacteristic flash of annoyance, when I asked whether he felt any constraints in discussing Russia. "I have criticized Russia's laws on this, that, and the other. It's just frustrating to get the question because it's like, look, what do I have to do?"

Snowden seems determined to refute predictions that he would end up broken, like so many whistle-blowers before him, or drunk and disillusioned, like a stereotypical Cold War defector. (He has claimed that he drinks nothing but water.) "People think of Moscow as being hell on earth," he said during his Whitney visit. "But when you're actually there, you realize it's not that much different than other European cities. Their politics are wildly different, and of course really they're problematic in so many ways, but the normal people, they want the same things." He says he does his own shopping and takes

the metro. Family members come to visit. His longtime girlfriend, Lindsay Mills, reunited with him in Moscow and has posted Instagram snapshots of her life there.

Last year, before Halloween, Mills posted a Photoshopped picture that posed the couple in front of FBI headquarters, with Snowden costumed as the capped protagonist of Where's Waldo? As improbable as it may sound, he has told confidants that he doesn't think the U.S. government has managed to pin down his exact whereabouts. He says he has designed his new life around his unique "threat model," minimizing his vulnerability to tracking by giving up modern conveniences like carrying a phone. "He does not believe that he's shadowed all the time by the CIA," says Ellsberg, who has been in regular contact. "But he does believe that he is in the sights of the FSB all the time, partly to keep him safe." Snowden is most at ease when he's on the internet, an environment he feels he can control. As a former systems engineer, he has been able to construct back-end protections that allow him to feel confident that he can evade locational detection, even when he is using the internet like a civilian. He has sometimes chatted via video on Google Hangouts.

Snowden is more wary about in-person meetings, typically conducting them in hotels like the Metropol near Red Square. More than a year after they began speaking, Ellsberg finally had the opportunity to meet Snowden in person, when he visited Moscow with an informal goodwill delegation that also included the actor John Cusack and the leftist Indian author Arundhati Roy. At the appointed time, Snowden called and said to meet him in the lobby of their hotel. Cusack took the elevator downstairs, and Snowden surprised him by getting on at the fourth floor. When they returned to the room, Ellsberg greeted Snowden by saying, "I've been waiting 40 years for someone like you."

Two days of marathon bull sessions and room-service dining ensued. Ellsberg tried -- unsuccessfully -- to get confirmation of some long-held suspicions about the extent of the NSA's spying on Americans. Periodically, Snowden would point to the ceiling, to remind the room that others were probably listening. Cusack and Roy later recounted the conversation in a 13,000-word essay, writing that when the meeting was over, Ellsberg lay down "on John's bed, Christ-like, with his arms flung open, weeping for what the United States has turned into -- a country whose 'best people' must either go to prison or into exile."

The notion that Snowden has become, to some, a sort of mythic figure -- the Oracle of the Metropol -- is profoundly annoying to the people who actually hold the nation's intelligence secrets. "I'd love to see him come back to the U.S. and take his medicine," says Robert Litt, general counsel for the Office of the Director of National Intelligence, who has been deeply involved in both the legislative fallout from the NSA revelations and internal government discussions over the potential prosecution of Snowden. Litt says he sees the consequences of Snowden's actions on extremist message boards, which now exhort jihadis to use encryption. "It cannot be disputed," he told me, "that this has had immeasurable impact."

Snowden believes that officials like Litt are merely trying to scare the public into acquiescence. Last October, the two had a showdown of sorts when they spoke back-to-back at a conference at Bard College. "Each time we have an election, it's like another round of a game," Snowden told the students.

Using a livecasting program designed for gamers that allows him to project illustrations, he filled the auditorium screen with an image of George W. Bush shaking hands with Obama. "The policies of one president become the policies of another." Then he played a video clip of the cleric Anwar al-Awlaki's son, a 16-year-old American citizen killed by a drone strike in Yemen. He cited a leaked 2015 email in which Litt addressed the hostile legislative climate, recommending "keeping our options open" for a change "in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."

"Surveillance is ultimately not about safety," Snowden said. "Surveillance is about power. Surveillance is about control."

Litt opened his remarks by joking that he could sympathize with the act that went on Ed Sullivan after the Beatles. "I can hear the NSA's opinion any day," one student stage-whispered, as he and many others got up to head for the exits. Litt called after them, saying he was "disappointed" with the disdain "given that this is an academic environment." He then elaborated on the ominous sentiment expressed in his email.

"Every time something bad happens, the finger gets pointed at the intelligence community," Litt said. "There is a pendulum that swings back and forth, in terms of the public view of the intelligence community, between, 'You mean you're doing what?' and 'Why didn't you protect us?' And that's a pendulum that's going to swing again."

While much of Washington remains hostile to him, Snowden is far more hopeful about Silicon Valley and is increasingly focusing his efforts on influencing technology and the people who make it. "Like me, they grew up with this stuff," he told me. "They remember what the internet was like before everybody felt it was being watched."

The Snowden leak "was like a gut punch for people across Silicon Valley," says Chris Sacca, a venture capitalist who invested early in Twitter and Uber and who now appears on the television show Shark Tank. Sacca was personally friendly with Obama, raising large sums for his 2012 campaign, but was shocked when he discovered the extent of the NSA's spying and has since become a vocal Snowden supporter. Last November, Sacca did an admiring interview with Snowden at the Summit at Sea, an invite-only weekend of seminar talks and techno dancing aboard a cruise ship, which was attended by the likes of Eric Schmidt, chairman of Alphabet, and Travis Kalanick, CEO of Uber. "After fielding over an hour of tough questions," Sacca says, "he got a resounding standing ovation from the room."

Even as Snowden captivated the audience on the boat, though, terrorists were mounting a bloody coordinated attack in Paris. The pendulum was swinging back. At first, Wizner says, Snowden was shaken -- he worried that the attacks had wiped out all of his progress. Almost immediately, anonymous security sources blamed encryption for giving cover to the attackers. (Subsequent reports suggest they may have been more reliant on primitive tactics, like using burner phones.) "They dragged out all the old CIA directors, the line of disgrace, to suddenly try to reclaim a halo," Snowden told me. "It did look really

exploitative." For three weeks, he went quiet, posting just once to Twitter, quoting Nelson Mandela about triumphing over fear. Meanwhile, Syed Farook and Tashfeen Malik attacked in San Bernardino, and Trump called for a ban on Muslim immigration.

Wizner advised his client to be patient. Snowden sometimes says he thinks of his existence like a video game: a series of challenges that culminate in a final screen, where you either win or it's game over. But political outcomes are never so final -- it's an iterative process. In February, when Apple announced it was refusing to break into Farook's iPhone for the FBI, Snowden was suddenly scoring points again. ("The @FBI is creating a world where citizens rely on #Apple to defend their rights," he tweeted, "rather than the other way around.") In an open letter, Tim Cook, Apple's chief executive, talked the way Snowden does about privacy, encryption, and government "overreach." The next day, Snowden spoke at Johns Hopkins University, where hundreds of shivering students lined up to get into a packed auditorium. "This is a case that's not about San Bernardino at all; it's not a case that's about terrorism at all," Snowden warned. "It's about the precedent."

Litt believes that, besides giving information to enemies, Snowden's disclosures have also had a radicalizing effect in the private sector. "The technology and communications community has moved from a position of willingness to cooperate," he told me, "to an attitude that ranges from neutrality to outright hostility, which is an extremely bad thing." Recently, Snowden has been working with technical experts who are mobilizing to fortify the internet's weak spots, both through collaborations with academic researchers and back-channel conversations with employees at major tech companies.

In all of these conversations, Snowden is operating on the assumption that a truly private space on the internet could be easier to create than to legislate -- that it may be more fruitful to coax programmers to invent something that is difficult to hack than it would be to try to reshape the entire national-security bureaucracy so it stops trying. "I'm regularly interacting with some of the most respected technologists and cryptographers in the world," Snowden said. "I believe that there's actually a lot more influence that results from those sorts of conversations, because so much of technology is an expert game."

The aspect of the Snowden leaks that most outraged technology experts was not the NSA's communications surveillance but its efforts to undermine encryption, which had broad impacts on computer security. That news has "created a period of innovation" in encryption, says Moxie Marlinspike, the San Francisco-based security specialist who developed Signal, the messaging program that Snowden likes to use to communicate. Marlinspike has become friendly with Snowden, whom he met in Moscow, where they had a lengthy discussion about the trade- offs between security and usability. (Snowden is always seeing holes hackers can poke through; Marlinspike wants to make encryption accessible to laypeople.) In April, WhatsApp, which is owned by Facebook, announced that it had integrated the Signal protocol Marlinspike developed, allowing it to offer end-to-end encryption. Those sorts of technical decisions, like Apple's strengthened encryption standards, affect the privacy of millions of customers.

But Snowden is skeptical of the motives of tech companies. "Corporations aren't friends of the people, corporations are friends of money," he said. He prefers to collaborate with academics and hacktivists, some of whom are helping him with projects he is developing for the Freedom of the Press Foundation. It already manages SecureDrop, a system for anonymously leaking documents, and the nonprofit's technical staff is working with Snowden to develop other programs tailored to protect journalists and whistle-blowers. "His goal with us is to start designing and prototyping what the tools of the future will look like," says Trevor Timm, the foundation's executive director. One of Snowden's priorities, unsurprisingly, is improving the security of videoconferencing.

About once a week, the team meets on a beta-stage video platform, where they discuss the painstaking work of testing their technology, a probing process called "dogfooding." As a prime target for hacking attacks, Snowden is in a unique position to appreciate extreme-threat models. He often comes up with exotic problems to solve and is able to bring in outside minds for confidential consultations. "We're building small projects," Snowden says, but he can't help but see larger applications. He talks enthusiastically about virtual reality, which could soon supplant videoconferencing. "In five years this shit's going to blow your mind," Snowden told me. But he also sees potential dangers. "Suddenly, you've got every government in the world sitting in every meeting with you."

Snowden is especially concerned about the monitoring power of Facebook, which acquired Oculus VR, the virtual-reality headset maker, for $2 billion. "What if Facebook has a copy of every memory that you ever made with someone else in these closed spaces?" he asked rhetorically. "We need to have space to ourselves, where nobody's watching, nobody's recording what we're doing, nobody's analyzing, nobody's selling our experiences."

It is clear that in virtual reality, Snowden sees more than just a work tool. "Right now, the technology is not quite there, but this is the first step," the Snowbot told Peter Diamandis, the space entrepreneur and Singularity University co-founder, in an interview at this year's Consumer Electronics Show. "I have someone who is very close to me," Snowden explained, "who was the victim of a serious car accident, and because of that they can't travel." Virtual reality could bring them together. Or it could allow him to visit home for Thanksgiving, overcoming what he calls "the tyranny of distance."

More than one person told me that, after talking to Snowden for hours on end, they got the sense that he is lonely. His conversation is preoccupied with the theme of escape. He recently collaborated on a track with a French musician, delivering a spoken-word monologue on surveillance over an electronic beat, and recommended the title: "Exit."

Snowden sometimes says that although he lives in Russia, he does not expect to die there, and he told me he is optimistic that he will find a way out, somehow. Maybe some Scandinavian country will offer him asylum. Maybe he can work out some kind of deal -- whether outright clemency or a plea bargain -- with the Justice Department. Wizner has been working with Plato Cacheris, a well-connected Washington defense attorney, but so far, there have been no official signals that the Justice Department would be willing to offer the kind of lenient terms Snowden would accept. And a window may be

closing. He is unlikely to receive a more receptive hearing from Hillary Clinton, who has said he shouldn't be allowed to return without "facing the music." As for Donald Trump: He has called Snowden a "total traitor" and suggested he should be executed. "If I'm president," he predicted last year, "Putin says, 'Hey, boom -- you're gone.'?"

So the comparatively thoughtful Obama may be Snowden's best hope, but even Snowden's allies concede that they doubt the outgoing president has the inclination to offer a pardon. "There is an element of absurdity to it," Snowden told me. "More and more, we see the criticisms leveled toward this effort are really more about indignation than they are about concern for real harm." He says he would return and face the Espionage Act charges if he could argue to a jury that he acted in the public interest, but the law does not currently allow such a defense. "These people have been thinking about the law for so long that they have forgotten that the system is actually about justice," Snowden said. "They want to throw somebody in prison for the rest of his life for what even people around the White House now are recognizing our country needed to talk about."

Earlier this year, Snowden was buoyed by an invitation from an unexpected source. David Axelrod, the president's former top political strategist, asked him to appear at the institute he now runs at the University of Chicago. Beforehand, they had a video chat. "The president of the United States' closest advisers," Snowden told me later, "are now introducing me and sharing the stage with me in ways that aren't actually critical. I'm not saying this to build myself up. I'm talking about the recognition by even the people who have the largest incentives to delegitimize me as a person, that maybe we overreacted, maybe this is a legitimate conversation that we need to have."

Axelrod asked Geoffrey Stone, a liberal law professor who is friendly with Obama, to moderate the public talk. Stone is a member of the ACLU's National Advisory Council and the author of a book titled Top Secret: When Our Government Keeps Us in the Dark, but he also served on Obama's commission to review the NSA's surveillance programs, an experience that gave him access to classified information and a dim view of Snowden. "My view is that he cannot be granted clemency, because he did commit a criminal offense and it did considerable harm," Stone told me. "The people who are celebrating Snowden have no understanding of the harm, for the reason that the people in the intelligence world can't really explain the harm to them." Snowden considered Stone's position to be "an example of regulatory capture," proof of the seductive power of security clearances. Secret knowledge, Snowden says, "is a very intoxicating thing."

Still, Snowden was looking forward to the debate, if only because it illustrates his progress. Wizner, who considered the Axelrod relationship important to his future clemency push, attended the May event in person. "We've gone from the president saying 'We're not going to scramble jets for a 29-year-old hacker' to talking with the president's rabbi,'?" Wizner said backstage as event staff set up computers and projection equipment. "That's a good journey for us."

Axelrod shambled in, looking sleepy-eyed as always, as students filled the auditorium and Wizner texted last-minute instructions to his client over Signal. "Whatever you think about Edward Snowden and his

actions, and the adjectives range from traitor to hero," Axelrod said by way of introduction, "he has indisputably triggered a really vital public debate about how we strike a balance between civil liberties and security." He sat down in the front row as Snowden's bashful grin filled a large screen.

Snowden had already done one event that day, a cybersecurity conference in Zurich, and he seemed weary as Stone probed for logical weaknesses. The law professor asked when it was appropriate for "a relatively low-level official in the national-security realm to take it upon himself to decide that it is in the national interest to disclose the existence of programs that have been approved ... To decide for himself that 'I think they're wrong.'?" Snowden gave his usual homilies about the Constitution, whistle-blowing, and civil disobedience. "Do we want to create a precedent that dissidents should be volunteering themselves not for the 11 days in jail of Martin Luther King or the single night of Thoreau," he asked, "but 30 years or more in prison, for what is an act of public service?"

Stone pointed out that Congress could pass a law allowing defendants to make a whistle-blowing defense in Espionage Act cases but shows no signs of doing it. "You believe in democracy," Stone said. "But democracy doesn't agree with you." The professor jabbed and Snowden weaved, setting his jaw and taking swigs from a big plastic water bottle. But when the floor opened for questions, it was clear who had won the audience. One student after another got up to offer Snowden praise.

"Did you expect to become a celebrity in this way?" one asked.

"If you go back to June 2013," Snowden said, "I said, 'Look, guys, stop talking about me, talk about the NSA.'?" But he added, "Our biology, our brains, the way we relate to things, is about character stories. So they simply would not let me go."

Axelrod watched impassively, his fingers tented under his nose. The full effect of Snowden's performance did not become clear until a few weeks later, when Axelrod had Eric Holder -- the former attorney general, once Snowden's chief pursuer -- on his podcast, The Axe Files. Holder allowed that Snowden "actually performed a public service," while Axelrod calmly presented Snowden's arguments.

"I think there has to be a consequence for what he has done," Holder replied. "But I think, you know, in deciding what an appropriate sentence should be, I think a judge could take into account the usefulness of having had that national debate."

Holder's concession made international headlines. It didn't mean anything legally, but symbolically it spoke volumes. Political realities were starting to come into alignment with Snowden's virtual ones. From his computer in Moscow, Snowden tweeted:

2013: It's treason!

2014: Maybe not, but it was reckless

2015: Still, technically it was unlawful

2016: It was a public service but

2017:

Canberra Times

Dotcom, Assange warn of hacking

Sunday, 26 June 2016

Byline: Chris Zappone

Section: general

Canberra - Did Kim Dotcom warn the world the Democratic Party hacking was coming? Megaupload founder Kim Dotcom said last year he knew of information that would create an obstacle for Hillary Clinton's 2016 presidential election bid, explaining WikiLeaks' Julian Assange would prove a thorn in the side of the presumptive presidential candidate.
Last week a hacker going by the name Guccifer 2.0 released what appeared to be the Democratic Party's research on presumptive Republican nominee Donald Trump.

The hacker has since produced more reports with alleged information about Mrs Clinton's donors. Mr Assange, who reportedly holds the rest of the Democratic Party hack information, says more will soon be released.

When contacted about future data releases, WikiLeaks replied only: "We have a very big publishing year ahead." While hacks of US presidential campaigns have happened before, the prospect of hackers - especially ones backed by a foreign nation - dumping US election- related data during the campaign and for the global public's consumption is new.

It's significant that the Russian actions against US political targets were potentially tipped months earlier. In the shadowy world of the cyber competition, attributions of hacking is often as slow as seven months after they are discovered.Mr Dotcom's warning suggested evidence of such an attack was available months before the event was revealed. Guccifer 2.0 said his hacking effort had been under way for almost a year. Based on the nature and details of the attack, independent researchers in the US concluded the hack was conducted by a group linked to the Russian government.

Asked this week if the information Mr Assange claimed to have on Mrs Clinton's campaign came from Russian hacks, Mr Dotcom replied: "No comment." Earlier this month, Mr Assange said his site would provide enough evidence to indict Mrs Clinton. Although Mrs Clinton is the subject of investigations over her handling of emails, Mr Assange admitted it was unlikely the US Justice Department would indict her based on whatever information he had.

Mr Assange, who has lived at the Ecuadorian embassy in London since 2012 to avoid a series of extraditions that could have him tried in the US for his role in the Cablegate leak, is considered friendly to Russian interests. Mr Assange claims to have helped former NSA contractor Edward Snowden travel to Russia.

Reuters

Google, Facebook quietly move toward automatic blocking of extremist videos

Saturday, 25 June 2016

Section: general

San Francisco and Washington-- Some of the web's biggest destinations for watching videos have quietly started using automation to remove extremist content from their sites, according to two people familiar with the process.
The move is a major step forward for internet companies that are eager to eradicate violent propaganda from their sites and are under pressure to do so from governments around the world as attacks by extremists proliferate, from Syria to Belgium and the United States.

YouTube and Facebook are among the sites deploying systems to block or rapidly take down Islamic State videos and other similar material, the sources said.

The technology was originally developed to identify and remove copyright-protected content on video sites. It looks for hashes," a type of unique digital fingerprint that internet companies automatically assign to specific videos, allowing all content with matching fingerprints to be removed rapidly.

Such a system would catch attempts to repost content already identified as unacceptable, but would not automatically block videos that have not been seen before.

The companies would not confirm that they are using the method or talk about how it might be employed, but numerous people familiar with the technology said that posted videos could be checked against a database of banned content to identify new postings of, say, a beheading or a lecture inciting violence.

The two sources would not discuss how much human work goes into reviewing videos identified as matches or near-matches by the technology. They also would not say how videos in the databases were initially identified as extremist.

Use of the new technology is likely to be refined over time as internet companies continue to discuss the issue internally and with competitors and other interested parties.

In late April, amid pressure from U.S. President Barack Obama and other U.S. and European leaders concerned about online radicalization, internet companies including Alphabet Inc's YouTube, Twitter Inc, Facebook Inc and CloudFlare held a call to discuss options, including a content-blocking system put forward by the private Counter Extremism Project, according to one person on the call and three who were briefed on what was discussed.

The discussions underscored the central but difficult role some of the world's most influential companies now play in addressing issues such as terrorism, free speech and the lines between government and corporate authority.

None of the companies at this point has embraced the anti- extremist group's system, and they have typically been wary of outside intervention in how their sites should be policed.

It's a little bit different than copyright or child pornography, where things are very clearly illegal," said Seamus Hughes, deputy director of George Washington University's Program on Extremism.

Extremist content exists on a spectrum, Hughes said, and different web companies draw the line in different places.

Most have relied until now mainly on users to flag content that violates their terms of service, and many still do. Flagged material is then individually reviewed by human editors who delete postings found to be in violation.

The companies now using automation are not publicly discussing it, two sources said, in part out of concern that terrorists might learn how to manipulate their systems or that repressive regimes might insist the technology be used to censor opponents.

There's no upside in these companies talking about it," said Matthew Prince, chief executive of content distribution company CloudFlare. Why would they brag about censorship?"

The two people familiar with the still-evolving industry practice confirmed it to Reuters after the Counter Extremism Project publicly described its content-blocking system for the first time last week and urged the big internet companies to adopt it.

WARY OF OUTSIDE SOLUTION

The April call was led by Facebook's head of global policy management, Monika Bickert, sources with knowledge of the call said. On it, Facebook presented options for discussion, according to one participant, including the one proposed by the non-profit Counter Extremism Project.

The anti-extremism group was founded by, among others, Frances Townsend, who advised former president George W. Bush on homeland security, and Mark Wallace, who was deputy campaign manager for the Bush 2004 re-election campaign.

Three sources with knowledge of the April call said that companies expressed wariness of letting an outside group decide what defined unacceptable content.

Other alternatives raised on the call included establishing a new industry- controlled nonprofit or expanding an existing industry-controlled nonprofit. All the options discussed involved hashing technology.

The model for an industry-funded organization might be the nonprofit National Center for Missing and Exploited Children, which identifies known child pornography images using a system known as PhotoDNA. The system is licensed for free by Microsoft Corp.

Microsoft announced in May it was providing funding and technical support to Dartmouth College computer scientist Hany Farid, who works with the Counter Extremism Project and helped develop PhotoDNA, to develop a technology to help stakeholders identify copies of patently terrorist content."

Facebook's Bickert agreed with some of the concerns voiced during the call about the Counter Extremism Project's proposal, two people familiar with the events said. She declined to comment publicly on the call or on Facebook's efforts, except to note in a statement that Facebook is exploring with others in industry ways we can collaboratively work to remove content that violates our policies against terrorism."

In recent weeks, one source said, Facebook has sent out a survey to other companies soliciting their opinions on different options for industry collaboration on the issue.

William Fitzgerald, a spokesman for Alphabet's Google unit, which owns YouTube, also declined to comment on the call or about the company's automated efforts to police content.

A Twitter spokesman said the company was still evaluating the Counter Extremism Project's proposal and had not yet taken a position."

A former Google employee said people there had long debated what else besides thwarting copyright violations or sharing revenue with creators the company should do with its Content ID system. Google's system for content-matching is older and far more sophisticated than Facebook's, according to people familiar with both.

Lisa Monaco, senior adviser to the U.S. president on counterterrorism, said in a statement that the White House welcomed initiatives that seek to help companies better respond to the threat posed by terrorists' activities online.

The post Google, Facebook quietly move toward automatic blocking of extremist videos appeared first on Cyprus Mail.

CBC.CA

Cybersecurity threat 'keeps us up at night,' says Hydro Ottawa CEO

Saturday, 25 June 2016

Byline: Staff Writer

Section: general

Ottawa- As the electricity grid becomes more and more connected to the internet, Hydro Ottawa says it's investing heavily to protect the system from cyber attacks.
"It's huge," said Hydro Ottawa CEO Bryce Conrad of cybersecurity. "It keeps us up at night."

Conrad described how someone sitting in a bedroom at a computer on the other side of the world can try to hack into a utility's information systems and do damaging things ? like take down a grid.

"There are lots of examples out there where this has come true."

And Conrad says he doesn't pretend it can't happen in Ottawa.

"We're a G7 capital, so we're not just Hydro Ottawa, we're the provider of electricity to a G7 capital. If you don't have electricity in the morning, you're not doing a whole lot," he added.

Connecting customers while preventing attacks

Cybersecurity is detailed as a risk facing the utility in the five-year strategy document that Hydro Ottawa tabled earlier this week at an Ottawa city council meeting.

The strategy describes an industry in the midst of transformation in which electricity systems are converging with, and are increasingly dependent on, information technology.

Hydro Ottawa anticipates big changes in the coming years ? from increased sales of electric cars to innovations that come from more customers being digitally connected to a smart grid, a system of resources to better manage consumption.

But having people, their homes, their appliances, and their vehicles connected to the internet all the time poses a security challenge for an electric utility like Hydro Ottawa.

"As we become more customer-centric, and give customers more tools to sort of manage these things, you're effectively opening up your system for your customers," said Conrad.

"What you're trying to do is open it up for them and keep the back door closed to someone who wants to do something nefarious."

Heavy investment in command and control centre

That's why Hydro Ottawa considers cybersecurity every time it buys a piece of software or technology, according to Conrad.

"We have to invest heavily in cybersecurity and making sure our systems, particularly our command and control systems, are as robust and protected as they possibly can be," he said.

The electricity industry gets together regularly to discuss best practices for protecting utilities from the threat of hacks emanating from terrorists, organized crime groups, or other foreign entities.

"I'll never say we're 100 per cent protected, but we're in pretty good shape."

ITAR-TASS World Service

State Duma adopts package of anti-terrorist bills

Saturday, 25 June 2016

Byline: Staff Writer

Section: general

Russia's State Duma on Friday adopted in the second and third, final reading a package of anti-terrorist bills proposed by lower house member Irina Yarovaya and upper house member Viktor Ozerov.

The initiatives sparked great public controversy and continued to be edited up to the last moment. Eventually the idea of terminating the Russian citizenship of those dual or multiple citizens who have committed terrorist crimes or proved to have been employed by foreign special services was dropped. Under the just- adopted version communication operators will be obliged to keep information about their subscribers' connections for a period of three years, and of the content transmitted, including videos, for six months. For the owners of messenger services and social networks these rules have been eased somewhat: they will be not allowed to delete information about the content transmitted and their users for twelve months, and not three years, contrary to the original version of the bill.

Messenger services, such as WhatsApp and Telegram will be fined up to one million rubles, should they refuse to disclose content at the request of the federal security service FSB.

Anti- sect amendments

A special group of amendments defines what "missionary activity" is and prohibits attempts to conduct it on behalf of religious associations whose aims contradict the law. The legislators banned missionary activities that violate public security and order, extremist actions, coercion into ruining families, and encroachments on the freedom of the person and rights and freedoms of citizens. A ban is imposed on missionary activities aimed at inducing suicide, at creating obstructions to getting mandatory education and at persuasion of individuals to refuse to perform their legally mandatory civic duties.

Missionary and preaching activities that breech legislation on the freedom of conscience and faith and on religious associations will be punishable with a fine of 5,000 rubles to 50,000 rubles ($77 to $7700) for individuals, and 100,000 rubles to 1,000,000 ($1,500 to $15,000). Foreign citizens will face expulsion from Russia. Under the new rules, all printed, audio and video content being distributed by a religious organization must have proper markings and bear the organization's full name.

Life sentence for international terrorism

The Criminal Code's list of crimes against peace and security of humanity was expanded to incorporate "international terrorism" and life imprisonment established as the maximum punishment. The minimum prison term for a terrorist attack will be increased from eight years to ten and from ten years to twelve (if the crime was committed by a group of persons or resulted in loss of human life).

The newly-adopted law contains a new, fuller definition of the financing of terrorism. It will be understood as "provision or raising of funds or provision of financial services with the awareness that they are meant for financing a terrorist organization, or plotting or committing terrorist crimes."

Public calls for terrorism or statements made in public in the Internet with the aim of excusing it will be punishable with a fine of up to 1,000,000 rubles ($15,000) or a prison term of five to seven years. Publicly expressed excuses are defined as "public statements to the effect the ideology and practices of terrorism are correct and worth supporting and following." Participation in a terrorist organization will

be punishable with prison terms of ten to twenty years (in contrast to the currently established ones of five to ten years).

Failure to report a terrorist attack

Failure to report preparations for terrorist crimes or committed terrorist crimes will entail a fine of up to 100,000 rubles ($15,000) or forced labor of up to twelve months or a twelve-month prison term. Failure to report preparations for a terrorist attack or a committed terrorist attack by one's spouse or close relative will not be punishable.

Minimum punishments

Punishments for organizing or participating in armed groups, including those abroad will be tightened. The maximum prison term for this offence is raised to five years. The Criminal Code is complemented with a new article establishing punishment for suborning into or recruitment for mass unrest. Such wrongdoing will be fined with 300,000 rubles to 700,000 rubles ($4,600 to $10,800) or a prison term of five to ten years.

Minimum punishments have been introduced under Article 282 of the Criminal Code (Incitement of Hatred or Humiliation of Human Dignity). The mildest punishment is set at three years and the maximum one, at six. Punishment for organizing an extremist organization or extremist community or financing extremist activities was tightened accordingly.

The age of accountability for terrorism is lowered to 14 years. The list of aggravating circumstances has been expanded to incorporate crimes committed in the context of an armed conflict or combat operations.

The amendments will take effect on July 20, 2016.

The Nation Multi

Military chiefs call for more robots for national security

Monday, 27 June 2016

Byline: Juthathip Lucksanawong

Section: general

Bangkok - The 26-kilogram, rectangular Portable Rescue Robot (PRR) stretched its manipulator arm, complete with a night vision camera, to surveil the area. With a wireless control system and two additional blades in front, the PRR showed off its ability to move freely in hostile terrain.
The display was performed in front of veteran military officers and weapons experts who met at a recent seminar on the development of military technology.

Mahanakorn University of Technology developed the robot, one of several robot prototypes that experts are collaboratively trying to develop to support national security missions. Using robots, especially for bomb retrieval missions, has long been considered by the Thai military.

Over the recent decade, Thailand has seen both the Southern insurgency and terrorism plaguing national security, said Sqn Leader Jiradett Kerdsri, director of data and communication division of the Defence Technology Institute (DTI).

"While insurgency and explosions are ongoing in the South, the dreadful bombing in August last year at Ratchaprasong intersection, the heart of Bangkok city, also irked state security," he said.

Such troubles affect the country's tourism, economy and trustworthiness, Jiradett said. "Foreign investors and tourists won't risk coming to a hazardous territory," he said.

It is essential, he added, for the DTI to select much-needed defence technology to be developed to serve the country's security goals.

Inventing bomb retrieval robots is part of the DTI's research plan initiated in 2009 to promote self-reliance in terms of national security and reduce the need to procure defence systems and equipment from other countries, said General Sompong Mukdaskul, DTI director-general.

Since its official establishment seven years ago, the DTI, under Ministry of Defence (MoD) oversight, has carried out five defence technology research plans focusing on rockets, unmanned aerial vehicles (UAVs), simulation technology, infantry fighting vehicles (IFVs), and military information and communication technology.

The DTI's prototypes in each category have been distributed to the three branches of the Armed Forces - Army, Navy and Air Force - and the police.

When the DTI began supplying defence forces with equipment and systems, Sompong found that each user had different technology requirements. To meet those requirements, the DTI needed to listen to what users required before research began, he added.

"Collecting feedback and comments from military and police authorities is the DTI's normal practice before and after each piece of defence equipment is unveiled," the director-general said.

The PRR's recent demonstration, and that of its robotic colleagues, in front of veteran officers and experts was part of that feedback process to fulfil the ambition to build sophisticated robots that can help to keep people safe in the field.

Air Force representatives told the seminar that the force needs robots that support remote operations with wireless and fibre optic control systems. The force has to patrol remote, inaccessible areas where land mines are a danger that could be mitigated by capable remote control robots, said Wing Commander Navin Vudhironnarith, deputy chief of the Air Force's Explosive Ordnance Disposal (EOD) force.

The robots also need to be lightweight with fire-suppression systems, including recoilless water jets, for safety, he added.

The Army, on the other hand, needs user-friendly robots with very high capabilities, said Colonel Krittipas Cruanate, chief of the Army's EOD.

"A single robot should not have all the functions. Some tasks do not need a full, heavy scanning system. Only reliable and enduring sensors and portable X-rays are necessary," he said

The colonel, who has seen numerous officers and ordinary people killed in bombings in the Southern violence, said robots are necessary because they could help to reduce fatalities explosive disposal missions. "If we'd had high-tech robotics to carry out deadly missions, people and authorities would not have died," he said.

To accomplish this new technological mission, participants agreed that academic institutions play a crucial role in developing new innovations because they act as centres of "know how" bringing together scholars and experts, Sompong said.

"Education institutions have performed tonnes of research but have no chance to apply their studies [in real situations]," he said.

The DTI director-general said he sees potential for knowledge transfers between these institutions and his agency.

"Their knowledge needs to be transferred and applied to the DTI's work. By doing this, they have an opportunity to further develop their technology and it saves time for us to conduct research on the robots," he said.

In addition to educational institutions, the industrial sector also has the potential to contribute to robotics projects.

To pioneer useful robots, industrial stakeholders need to get involved in terms of manufacturing, said Djitt Laowattana, lecturer at King Mongkut's University of Technology Thon Buri and founder and director of the Institute of Field Robotics (FIBO).

Djitt said industry is important because of its expertise in effectively managing resources in manufacturing and, especially, marketing and distribution.

The DTI knows how to invent technology but does not specialise in managing resources and budgets, he said. The government's support is required to entice the public sector to become more involved in robotics development, he added.

The government should catalyse the industry by introducing a "local materials" requirement to promote companies to use components available in the country, rather than imported ones, Djitt said, adding companies that utilise local materials should get government incentives. That would encourage others to adopt more technology and robotic components made in Thailand, he said.

When robots are produced and sold on a large scale, the lecturer said, the robotics industry would increasingly grow, leading innovators and manufacturers to become eager to help to produce defence systems contributing to national security.

"I just hope that future robots answer the needs of defence suppliers. [We should] not just launch [the idea] and then put it on a shelf after our lengthy discussion today," Sompong said. "And I just hope that the bomb retrieval robots will eventually be practical and meet international standards."

Press Trust of India

India to become full member of Missile Technology Control Regime

Monday, 27 June 2016

Section: general

New Delhi - In its first entry into any multilateral export control regime, India will today join the Missile Technology Control Regime (MTCR) as a full member, three days after it failed to get NSG membership due to stiff opposition from China and a few other countries.
"We applied for the membership of MTCR last year and all the procedural formalities have been completed. Tomorrow, Foreign Secretary S Jaishankar will sign the document of accession into MTCR in the presence of Ambassadors of France, Netherlands and Luxembourg," External Affairs Ministry spokesperson Vikas Swarup said.

Significantly, China, which stonewalled India's entry into the 48-nation Nuclear Suppliers Group (NSG) at the just- concluded Seoul plenary, is not a member of 34-nation MTCR.

Since its civil nuclear deal with the US, India has been trying to get into export control regimes like NSG, MTCR, the Australia Group and the Wassenaar Arrangement that regulate the conventional, nuclear, biological and chemicals weapons and technologies.

India's case in MTCR was opposed last year by Italy which is not happy with New Delhi over the marines dispute. However, after both marines, accused of murdering two fishermen off the Kerala coast in 2012, were allowed to return, the Italians have softened their opposition.

India's efforts to get into the MTCR also got a boost after it agreed to join the Hague Code of Conduct, dealing with the ballistic missile non- proliferation arrangement, earlier this month.

MTCR membership will enable India to buy high-end missile technology and also enhance its joint ventures with Russia.

The aim of the MTCR is to restrict the proliferation of missiles, complete rocket systems, unmanned air vehicles and related technology for those systems capable of carrying a 500 kilogramme payload for at least 300 kilometres, as well as systems intended for the delivery of weapons of mass destruction (WMD).

India to get access to almost 99% of U.S. defence technologies

Monday, 27 June 2016

Section: general

Washington - India will be the only country outside Washington's formal treaty allies that will gain access to almost 99 per cent of latest U.S.'s defence technologies after being recognised as a 'Major Defence Partner', a senior Obama administration official has said.
"India [now] enjoys access to [defence] technologies that is on a par with our treaty allies. That is a very unique status. India is the only other country that enjoys that status outside our formal treaty allies," the official told PTI explaining what 'Major Defence Partner' status means for India.

Early this month, after a meeting between U.S. President Barack Obama and Prime Minister Narendra Modi at the White House, the U.S., in a joint statement, recognised India as a 'Major Defence Partner'

"We were looking for something unique. This language you would not find in any arms transfer legislation or any of our existing policies. This is new guidance and new language that is intended to reflect the unique things that we have done with India under our defence partnership," the senior administration official said.

"This is intended to solidify the India-specific forward leaning policies for approval that the [U.S.] President and [Defence] Secretary [Ashton] Carter...and our export control system have implemented in the last eight years," the official said.

Under this recognition India would receive licence-free access to a wide range of dual-use technologies in conjunction with steps that New Delhi has committed to taking to advance its export control objectives.

Acknowledging that the impression in New Delhi was that India was not getting access to the kind of technology it needed from the U.S., the official said it was a constant source of discussion.

"[In reality], less than one per cent of all exports [requests] are denied [to India]. They are not denied because of India. They are denied because of global U.S. licencing policies. We do not share certain technologies with anybody in the world," the official asserted.

The perception in India that the denial of such technologies is reflective of India-U.S. relationship is far from the truth, the official has said.

According to the official, India being recognised as a "major defence partner puts it on par with our treaty allies." Inside the American bureaucratic system, such a recognition removes a number of major export control hurdles for India.

The category of 'Major Defence Partner' was created specifically for India, observed Ashley Tellis, of Carnegie Endowment for International Peace, a top American think-tank.

"It was meant to recognise that although India will not be an alliance partner of the United States, the administration seeks to treat it as such for purposes of giving it access to advanced technologies of the kind that are reserved for close US allies," Mr. Tellis told PTI.

"The U.S. expects that bilateral defence ties will only grow in the years ahead, that India and the United States will continue to work together especially regarding maritime security, that India will eventually be admitted to global non-proliferation regimes, and that it will sign the foundational agreements," he said in response to a question.

"As these developments materialise, India's access to U.S. technology will also increase, and the "major defence partner" moniker is intended to signal to both the outside world and to the U.S. bureaucracy

that oversees licensing that India is viewed as a unique collaborator and will be treated as such where access to advanced technologies are concerned," Mr. Tellis said.

Calling India a "Major Defence Partner" is "more a term of art than a technical designation", noted Richard M. Rossow, Wadhwani Chair in U.S. India Policy Studies at the Centre for Strategic and International Studies, another top American think-tank.

"It certainly captures what is emerging as a unique relationship, exhibited by programs such as the Defence Technology and Trade Initiative [DTTI] and the establishment of a dedicated 'India Rapid Reaction Cell' inside the Pentagon. Neither exists for a country other than India," he said.

"But the term 'Major Defence Partner' does not automatically trigger a specific process or program in the U.S. system. Our two countries are feeling their way around the contours of our defence relationship," Mr. Rossow told PTI.

"India desires advanced U.S. technology today, while the U.S. would like more clarity on the specific operations India may be willing to undertake in the future to contribute to regional security. It is a process that has seen great progress, which we hope will carry over into the next U.S. administration," Mr. Rossow said in response to a question.

Over the last one decade the defence trade between India and the U.S. has increased from being almost non-existent to more than $14 billion. This is expected to increase manifold as India embarks on a major defence modernisation drive.

Times of Israel

CyberArk eyes expansion in Asia

Monday, 27 June 2016

Byline: Shoshanna Solomon

Section: general

Jerusalem - Petah Tikva-based CyberArk, Israel's second-largest public cybersecurity company, plans to target the Asian and Latin American markets and mid-sized customers in the longer term to boost growth, Udi Mokady, president and chief executive officer of CyberArk, said in an interview.
Speaking with reporters last week at the sidelines of a cybersecurity conference in Tel Aviv, Mokady said enterprise customers are still the main focus of the company and CyberArk is still just "scratching the

surface" of the potential of these companies.But in the longer term the firm is also "looking at ways to address also the mid-market as part of our strategy."

CyberArk is a cybersecurity company that specializes in protecting "privileged accounts" on corporate servers. Privileged accounts are computer system user accounts that have extra privileges so that owners of those accounts can control important aspects of a server or network. Large computer systems, especially those that have been around for years, usually contain many such accounts that are no longer in use - either because they were set up specifically for certain no-longer relevant missions or because they belonged to former employees. These accounts are especially vulnerable to hacker accounts, as they aren't watched too closely.

CyberArk chokes off the possibility that privileged accounts will be abused by identifying and cutting off access to the accounts. The system sets up a policy on user accounts that forces users to change passwords on a regular basis, including dormant privileged accounts. In addition, the system sets up a "safe zone" for data to be managed when accessed from an account.

"We found that even though we were targeting enterprise, we got pull from mid-market -- universities, credit unions, law firms, things we weren't necessarily targeting, and so it shows us there is an opportunity and we are looking for ways to address that in 2017 and beyond," Mokady said in the interview. "Right now it is very much enterprise-focused."

The company, which held an initial public offering of shares on the Nasdaq in 2014, saw its shares surge as corporations flocked to buy security software amid higher levels of data breaches worldwide.

Today CyberArk, the largest Israeli public information security company in both revenue and in market capitalization, has more than 2,600 customers globally, of which more than 40% are Fortune 100 customers, according to data from a May 2016 presentation.

Revenues grew over 50 percent in 2014 and 2015, and in the first quarter of the year revenue jumped 43% to around $47 million compared to the same quarter a year earlier. Net income for the first quarter of 2016 rose to $4.3 million from $4.2 million in the same quarter in 2015. CyberArk in May forecast total revenue to rise by around 30% in 2016 to a range of $209 million to $211 million.

The company is also looking to increase its presence in the Asia Pacific, Mokady said. Last year the Americas accounted for 61% of its revenues while Europe, Middle East and Africa accounted for 31 percent. Just around 8% of sales were in Asia Pacific and Japan, according to the presentation. "We want to bring it much higher," Mokady said. "We want it to be toward the teens in the long term. The opportunity is tremendous." Latin America is also an opportunity for growth, he said. "They have the same problems, the same IT infrastructure, the same weaknesses."

Even as the company has posted strong results, its share price has has declined about 26% in the past year amid concerns that enterprise spending in cybersecurity software has started to slow, lackluster

results from peers and on worries about too-high valuations in the sector. The company has a market capitalization of about $1.61 billion, according to data compiled by Bloomberg.

CyberArk's share decline spurred speculation in January that the company would become an acquisition target for Israel's Check Point Software Technologies Ltd.

Mokady shrugged off the possibility of a company sale even as he sees the possibility of some consolidation in the industry among the smaller companies. "CyberArk is a buyer," he said. "We are going for it and being acquisitive. Naturally in any step of the way we will do what is right for the shareholders. But left alone, we are building it big. "

The company has made two acquisitions, Viewfinity, Inc., a Waltham, Massachusetts-based provider of Windows privilege management and application control software, for $30.5 million in cash, and Israeli firm CyberIntel.

Acquisitions "is part of our growth strategy and we are very pleased with the first two," Mokady said. "There is appetite and willingness to do more but there is no pressure because we have such a huge organic opportunity."

Wall Street Journal

Russian Hack Said To Reach Beyond Democrats

Monday, 27 June 2016

Byline: Nicole Hong

Section: general

New York - The attack on the Democratic National Committee's computer network this past spring was part of a broader monthslong campaign by Russian hackers against groups with ties to U.S. politics, according to a new report.
Party officials and security researchers disclosed about two weeks ago that the DNC's system was compromised in April by two hacking groups with links to Russian intelligence services, one of the largest known breaches of a U.S. political organization.

On Sunday, cybersecurity firm SecureWorks Corp. concluded that one of the hacking groups, dubbed "Fancy Bear" in security circles, also targeted the emails of presumptive Democratic nominee Hillary

Clinton's campaign, as well as email accounts belonging to U.S.-based military spouses, political activists and journalists who wrote critically about Russia and others.

Over the past year or so, the hackers tried to penetrate nearly 4,000 individual email accounts, researchers said.

Researchers believe the hackers wanted access to email accounts as part of an intelligence-gathering operation, as opposed to stealing information for financial gain. In one tactic, the hackers sent out mass emails containing links that asked victims to reset their passwords.

Users at two dozen email addresses associated with the DNC and Mrs. Clinton's campaign clicked on the links, but SecureWorks says it is unclear whether information was accessed. Researchers previously said the hackers gained access to the DNC's chat systems and research files, including the party's opposition research on presumptive Republican nominee Donald Trump.

The DNC is "confident" that Russian government hackers were responsible for the breach and has "deployed the recommended technology" to secure their systems, said a senior DNC official.

A representative of the Russian government couldn't be reached for comment. In a previous statement, a Kremlin spokesman said: "I completely rule out the possibility of the government or government structures being involved in this."

A spokesman for the Clinton campaign didn't respond to a request for comment.

New York Magazine

I, Snowbot

Monday, 27 June 2016

Byline: Andrew Rice

Section: general

New York - Edward Snowden lay on his back in the rear of a Ford Escape, hidden from view and momentarily unconscious, as I drove him to the Whitney museum one recent morning to meet some friends from the art world. Along West Street, clotted with traffic near the memorial pools of the World Trade Center, a computerized voice from my iPhone issued directions via the GPS satellites above. Snowden's lawyer, Ben Wizner of the American Civil Liberties Union, was sitting shotgun, chattily

recapping his client's recent activities. For a fugitive wanted by the FBI for revealing classified spying programs who lives in an undisclosed location in Russia, Snowden was managing to maintain a rather busy schedule around Manhattan.
A couple nights earlier, at the New York Times building, Wizner had watched Snowden trounce Fareed Zakaria in a public debate over computer encryption. "He did Tribeca," the lawyer added, referring to a surprise appearance at the film festival, where Snowden had drawn gasps as he crossed the stage at an event called the Disruptive Innovation Awards. Wizner stopped himself mid- sentence, laughing at the absurdity of his pronoun choice: "He!" Behind us, Snowden stared blankly upward, his face bouncing beneath a sheet of Bubble Wrap as the car rattled over the cobblestones of the Meatpacking District.

Snowden's body might be confined to Moscow, but the former NSA computer specialist has hacked a work-around: a robot. If he wants to make his physical presence felt in the United States, he can connect to a wheeled contraption called a BeamPro, a flat-screen monitor that stands atop a pair of legs, five-foot-two in all, with a camera that acts as a swiveling Cyclops eye. Inevitably, people call it the "Snowbot." The avatar resides at the Manhattan offices of the ACLU, where it takes meetings and occasionally travels to speaking engagements. (You can Google pictures of the Snowbot posing with Sergey Brin at TED.) Undeniably, it's a gimmick: a tool in the campaign to advance Snowden's cause -- and his case for clemency -- by building his cultural and intellectual celebrity. But the technology is of real symbolic and practical use to Snowden, who hopes to prove that the internet can overcome the power of governments, the strictures of exile, and isolation. It all amounts to an unprecedented act of defiance, a genuine enemy of the state carousing in plain view.

We unloaded the Snowbot in front of the Whitney, where a small group had gathered to meet us for a private viewing of a multimedia exhibition by the filmmaker Laura Poitras. It was Poitras whom Snowden first contacted, anonymously, in 2013, referring to the existence of a surveillance system "whose reach is unlimited but whose safeguards are not." Their relationship resulted in explosive news articles and a documentary, Citizenfour -- work that won a Pulitzer and an Oscar and incited global outrage. But the disclosures came at a high price for their source. If Snowden couldn't come home, Poitras at least wanted him to share vicariously in the experience of her Whitney show, "Astro Noise," which took its name from an encrypted file of documents he had spirited out of the secret NSA site where he worked in Hawaii. So she had arranged a personal tour.

Outside an eighth-floor gallery, a crowd of Poitras's collaborators and Whitney curators clustered around the Snowbot as a white circle twirled on its monitor. Then, suddenly, the screen awoke and Snowden was there.

"Hey!" Wizner said, and the group erupted in awkward laughter. The famous fugitive was wearing a gray T-shirt, his face pallid and unshaven. (He calls himself "an indoor cat.") His voice sounded choppy, but some fiddling resolved the problem, and Poitras, soft-spoken and clad in black, made introductions. Snowden's preternaturally eloquent Hong Kong hotel-room encounter with Poitras and the Guardian journalists investigating his leaks formed the core of Citizenfour, but even some of those who worked on

the documentary had never met its protagonist. One of the cinematographers came forward and wrapped him in a hug.

"I don't have hands," Snowden apologized. "The most I can do is maybe ..."

He scooted forward.

Sitting in the same homemade studio he uses for his frequent speaking engagements, Snowden could control the robot's movements with his computer, maneuvering with uncanny agility, swiveling to make eye contact with people as they spoke to him.

Poitras began with the show's opening piece, a colorful array of prints that resembled modern abstracts but were actually found objects: visualizations of intercepted satellite signals that turned up in the vast trove of NSA documents. "The whole show, there's a lot of deep research that's going on behind it," she said. She led Snowden into a darkened gallery, where a spooky ambient soundscape was playing over video footage of a U.S. military interrogation. Momentarily disoriented, he careened into a bench. But Snowden quickly figured out how to navigate in the dark. When he came to parts of the exhibit that required complicated movements -- lying on a platform to take in the watchful night sky over Yemen, or craning to look at an NSA document through a slit in the wall -- the humans hoisted him into position.

"Wow, okay, I see it," Snowden said as one of Poitras's researchers held him up to view footage of a drone strike's aftermath. "This is a surreal experience for a number of reasons."

When the tour was over, Snowden held an impromptu discussion, likening his decision to become a dissident to a risky artistic choice. "There's always that moment where you step out and there's nothing underneath you," he said. "You hope that you can build that airplane on the way down, or if you don't, that the world will catch you. In my case, I've been falling ever since." Still, Snowden said he had no regrets. "I do have to say," he told Poitras, "that I will be forever grateful that you took me seriously."

As usual, though, when the questions turned to the details of his non-robotic existence, Snowden remained courteously evasive. "What's a day in the life now?" asked Nicholas Holmes, the Whitney's general counsel. "Do you go for walks in the park?"

"Well," the Snowbot replied, "I go for walks in the Whitney, apparently."

The idea that Snowden is still walking the American streets, virtually or otherwise, is infuriating to his former employers in the U.S.-intelligence community. Its leaders no longer make ominous jokes about wanting to put him on a drone kill list -- as former NSA and CIA director Michael Hayden did in 2013 -- but they still vilify him and maintain that he did real harm to America's safety and international standing. While Snowden's leaks revealed the NSA's controversial and possibly unconstitutional bulk collection of domestic internet traffic and telephone metadata, they also exposed technical details about many other classified activities, including overseas surveillance programs, secret diplomatic arrangements, and

operations targeting legitimate adversaries. The spy agencies warn that the public doesn't comprehend the degree of damage done to their protective capabilities, even as events like the Orlando nightclub massacre demonstrate the destructive reach of terrorist ideology. The fallout from Snowden's actions may have prompted a debate about security and privacy that even President Obama acknowledges "will make us stronger," but there has been no such reassessment, at least officially, of Snowden himself. He still faces charges of violating the federal Espionage Act, crimes that could carry a decades-long prison sentence.

When Snowden first revealed the NSA's surveillance -- and his own identity -- to the world three years ago this month, there was little reason to believe that he would be in a position to communicate much of anything in the future. The last person to leak classified information of such magnitude, Chelsea Manning, was sentenced to 35 years in prison. (Manning, who was held in solitary confinement while awaiting trial, has largely communicated to the public through letters.) Yet so far, to his own surprise, Snowden has managed to avoid the long arm of U.S. law enforcement by finding asylum in Russia. Leaving aside, at least for the moment, the ethics of his actions (and the internal contradictions of his residence in an authoritarian state ruled by a former KGB operative), Snowden's case is, in fact, a study in the boundless freedoms the internet enables. It has allowed him to become a champion of civil liberties and an adviser to the tech community -- which has lately become radicalized against surveillance -- and, in the process, the world's most famous privacy advocate. After he appeared on Twitter last September -- his first message was "Can you hear me now?" -- he quickly amassed some two million followers.

"I feel like we're sort of dancing around the leadership conversation," Snowden said to me recently as I sat with him at the ACLU offices. Over the past few months, we have encountered one another with some regularity, and while I can't claim to know him as a flesh-and-blood person, I've seen his intellect in its native habitat. He is at once exhaustively loquacious and reflexively self-protective, prone to hide behind smooth oratory. But occasionally, he has let down his guard and talked like a human being. "I'm able to actually have influence on the issues that I care about, the same influence I didn't have when I was sitting at the NSA," Snowden told me. He claims that many of his former colleagues would agree that the programs he exposed were wrongfully intrusive. "But they have no voice, they have no clout," he said. "One of the weirder things that's come out of this is the fact that I can actually occupy that role." Even as the White House and the intelligence chiefs brand him a criminal, he says, they are constantly forced to contend with his opinions. "They're saying they still don't like me -- tut-tut, very bad -- but they recognize that it was the right decision, that the public should have known about this."

Needless to say, it is initially disorienting to hear messages of usurpation emitted, with a touch of Daft Punk-ish reverb, from a $14,000 piece of electronic equipment. Upon meeting the Snowbot, people tend to become flustered -- there he is, that face you know, looking at you. That feeling, familiar to anyone who's spotted a celebrity in a coffee shop, is all the more strange when the celebrity is supposed to be banished to the other end of the Earth. And yet he is here, occupying the same physical space. The technology of "telepresence" feels different from talking to a computer screen; somehow, the fact that Snowden is standing in front of you, looking straight into your eyes, renders the experience less like

enhanced telephoning and more like primitive teleporting. Snowden sometimes tries to put people at ease by joking about his limitations, saying humans have nothing to fear from robots so long as we have stairs and Wi-Fi dead zones in elevators. Still, he is quite good at maneuvering on level ground, controlling the robot's movements with his keyboard like a gamer playing Minecraft. The eye contact, however, is an illusion--Snowden has learned to look straight into his computer's camera instead of focusing on the faces on his screen.

Here's the really odd thing, though: After a while, you stop noticing that he is a robot, just as you have learned to forget that the disembodied voice at your ear is a phone. Snowden sees this all the time, whether he is talking to audiences in auditoriums or holding meetings via videoconference. "There's always that initial friction, that moment where everybody's like, 'Wow, this is crazy,' but then it melts away," Snowden told me, and after that, "regardless of the fact that the FBI has a field office in New York, I can be hanging out in New York museums." The technology feels irresistible, inevitable. He's the first robot I ever met; I doubt he'll be the last.

Wizner, the head of the ACLU's Speech, Privacy, and Technology Project, says that Snowden asked him to do some research on telepresence in their first conversation, back when he was still very much on the lam. Now that his situation has stabilized -- at least for the time being -- he and Snowden's small coterie of advisers are discussing ways they might use it for a widening range of purposes. Glenn Greenwald, one of Snowden's original journalistic collaborators, jokingly talks about taking the Snowbot on the road. "I would love to let it loose in the parking lot of Fort Meade," where the NSA is headquartered, he said. "Or to randomly go into grocery stores." More seriously, Snowden's advisers are in discussions about a research fellowship at a major American university. Already, the Snowbot has twice taken road trips to Princeton University, where he has participated in wide-ranging discussions about the NSA's capabilities with a group of renowned academic computer-security experts, rolling up to cryptographers during coffee breaks and dutifully posing for selfies.

For larger gatherings, Snowden usually dispenses with the robot, addressing audiences from giant screens. (He often opens with an ironic reference to Big Brother.) He is scheduled to make more than 50 such appearances around the world this year, earning speaking fees that can reach more than $25,000 per appearance, though many speeches are pro bono. Besides allowing Snowden to make a good living, his virtual travels on the public- lecture circuit are part of a concerted campaign to situate him within a widening zone of political acceptability. "One of the things we were trying to do is to normalize him," says Greenwald. "Normalize his life, normalize his presence." In 2014, Snowden joined Poitras and Greenwald on the board of the Freedom of the Press Foundation, a San Francisco nonprofit, and last year he was elected chairman. It serves as a base for his advocacy and gives him access to a staff of technologists with whom he has been working on encryption projects, tools intended to allow journalists to communicate with "people that live in situations of threat" -- in other words, people like Snowden himself.

Through a network of intermediaries -- chief among them Wizner, who acts as his advocate, gatekeeper, and talent agent in the United States -- Snowden is able to establish contact with almost anyone he

desires to meet. "Ed's now getting a lot of people on the phone, and it's broadening his horizons," says the author Ron Suskind, who has spoken with him on several occasions and recently had him lecture to a class he and Lawrence Lessig were teaching at Harvard Law School. Snowden also recently spoke to Amal Clooney's law class at Columbia, starred in an episode of the Vice show on HBO, and published a manifesto on whistle-blowing on the Intercept, the website Poitras and Greenwald started with the billionaire Pierre Omidyar. And he has been maintaining his presence on Twitter, where he has been playfully talking up Oliver Stone's forthcoming film, Snowden, which will star Joseph Gordon-Levitt.

The biopic's September release date matches up with Wizner's timetable for mobilizing a clemency appeal to Obama. "We're going to make a very strong case between now and the end of this administration that this is one of those rare cases for which the pardon power exists," Wizner said. "It's not for when somebody didn't break the law. It's for when they did and there are extraordinary reasons for not enforcing the law against the person." He says that while no single event is likely to shift opinion in Washington, Snowden's activities work "in the aggregate" to further his cause.

One thing Snowden refuses to do, however, is apologize. If anything, the last three years have turned him more strident. Whereas he once espoused a fuzzy dorm-room libertarianism -- "some of it was kind of rudimentary," Greenwald recalls -- today he offers a more traditional leftist critique of the "deep state." On Twitter, he has been admiring of Bernie Sanders, acerbic about Hillary Clinton's foreign policy, and bitingly sarcastic about her handling of classified emails. In February, he tweeted: "2016: a choice between Donald Trump and Goldman Sachs." He sees himself as part of a hacktivist movement, and he took pride when the anonymous source behind the massive cache of offshore banking data known as the Panama Papers cited Snowden's example. In his Intercept essay, he called such leaking "an act of resistance."

WNYC recently staged a sold-out Friday-night event at the Brooklyn Academy of Music, not far from Fort Greene Park, where some artists surreptitiously erected a Snowden bust last year. At the appointed time, the fugitive appeared on a screen at the front of an ornate opera hall. It was around 2:30 a.m. in Moscow, but Snowden looked wide-awake, wearing an open-collared shirt and blazer and his customary stubble. "In an extraordinary and unpredictable way," he told the audience, "my own circumstances show there is a model that ensures that even if we're left without a state, we aren't left without a voice."

When Snowden went public, one of the first people he sought out was a historical antecedent: Daniel Ellsberg, the military analyst who leaked the Pentagon Papers. He, too, was briefly a fugitive and faced Espionage Act charges, until they were dropped because of the illegal retaliatory actions of President Nixon. Now 85, Ellsberg was eager to talk to Snowden and they connected over an encrypted chat program.

"I had the feeling that, as I suspected from the beginning, we really were kindred souls," Ellsberg told me.

Ellsberg, mindful of Manning's experience, advised Snowden to give up any thought of returning home. Snowden was inclined to agree. From the beginning, he had spoken fatalistically about the consequences of his actions. "All my options are bad," Snowden acknowledged in his first interview in Hong Kong, which was published in the Guardian. If the American government didn't grab him, the Chinese might, just to find out what he knew. He hinted that the CIA might even try to kill him, either directly or through an intermediary like a triad gang. "And that's a fear I'll live under for the rest of my life, however long that happens to be," Snowden said at the time.

"He didn't have a plan," says Wizner. Snowden assumed that he would probably be silenced in one way or another, so he worked with a sympathetic programmer in the United States to design a website, supportonlinerights.com, which was to contain a letter addressed to the public. But instead, he more or less got away with it. After a nervy flight and an agonizing five-week wait in limbo at the Moscow airport, he was granted temporary asylum in Russia by President Vladimir Putin. Photos soon appeared in the Russian media showing Snowden pushing a grocery cart and looking slyly over his shoulder on a riverboat ride. It was an uneasy deliverance, though, one seemingly subject to Putin's unpredictable geopolitical power considerations.

Snowden argues that he was put in Russia by the U.S. government, which canceled his passport while he was en route to Ecuador, trapping him in Moscow during a layover. But to critics, his dependence on Putin is discrediting. "I am not saying that he is a Russian spy, but he is in a tough spot," says journalist Fred Kaplan, author of the recent book Dark Territory: The Secret History of Cyber War. "He is in a position where, because of his captive status, he can't really say anything that terribly critical about his hosts, who happen to be some of the most sophisticated and intrusive cyberespionage hackers in the world." Many in the intelligence community darkly speculate about the nature of Snowden's accommodation with the FSB, the Russian security service, which is not renowned for its hospitality or respect for civil liberties.

Although Snowden acknowledges that he was approached by the FSB, he claims he has given them no information or assistance, and he vehemently denies he is anyone's puppet. He cheered the release of the Panama Papers, which contained voluminous evidence of corruption in Putin's inner circle. "I have called the Russian president a liar based on his statements on surveillance, in print, in the Guardian," he said with an uncharacteristic flash of annoyance, when I asked whether he felt any constraints in discussing Russia. "I have criticized Russia's laws on this, that, and the other. It's just frustrating to get the question because it's like, look, what do I have to do?"

Snowden seems determined to refute predictions that he would end up broken, like so many whistle-blowers before him, or drunk and disillusioned, like a stereotypical Cold War defector. (He has claimed that he drinks nothing but water.) "People think of Moscow as being hell on earth," he said during his Whitney visit. "But when you're actually there, you realize it's not that much different than other European cities. Their politics are wildly different, and of course really they're problematic in so many ways, but the normal people, they want the same things." He says he does his own shopping and takes

the metro. Family members come to visit. His longtime girlfriend, Lindsay Mills, reunited with him in Moscow and has posted Instagram snapshots of her life there.

Last year, before Halloween, Mills posted a Photoshopped picture that posed the couple in front of FBI headquarters, with Snowden costumed as the capped protagonist of Where's Waldo? As improbable as it may sound, he has told confidants that he doesn't think the U.S. government has managed to pin down his exact whereabouts. He says he has designed his new life around his unique "threat model," minimizing his vulnerability to tracking by giving up modern conveniences like carrying a phone. "He does not believe that he's shadowed all the time by the CIA," says Ellsberg, who has been in regular contact. "But he does believe that he is in the sights of the FSB all the time, partly to keep him safe." Snowden is most at ease when he's on the internet, an environment he feels he can control. As a former systems engineer, he has been able to construct back-end protections that allow him to feel confident that he can evade locational detection, even when he is using the internet like a civilian. He has sometimes chatted via video on Google Hangouts.

Snowden is more wary about in-person meetings, typically conducting them in hotels like the Metropol near Red Square. More than a year after they began speaking, Ellsberg finally had the opportunity to meet Snowden in person, when he visited Moscow with an informal goodwill delegation that also included the actor John Cusack and the leftist Indian author Arundhati Roy. At the appointed time, Snowden called and said to meet him in the lobby of their hotel. Cusack took the elevator downstairs, and Snowden surprised him by getting on at the fourth floor. When they returned to the room, Ellsberg greeted Snowden by saying, "I've been waiting 40 years for someone like you."

Two days of marathon bull sessions and room-service dining ensued. Ellsberg tried -- unsuccessfully -- to get confirmation of some long-held suspicions about the extent of the NSA's spying on Americans. Periodically, Snowden would point to the ceiling, to remind the room that others were probably listening. Cusack and Roy later recounted the conversation in a 13,000-word essay, writing that when the meeting was over, Ellsberg lay down "on John's bed, Christ-like, with his arms flung open, weeping for what the United States has turned into -- a country whose 'best people' must either go to prison or into exile."

The notion that Snowden has become, to some, a sort of mythic figure -- the Oracle of the Metropol -- is profoundly annoying to the people who actually hold the nation's intelligence secrets. "I'd love to see him come back to the U.S. and take his medicine," says Robert Litt, general counsel for the Office of the Director of National Intelligence, who has been deeply involved in both the legislative fallout from the NSA revelations and internal government discussions over the potential prosecution of Snowden. Litt says he sees the consequences of Snowden's actions on extremist message boards, which now exhort jihadis to use encryption. "It cannot be disputed," he told me, "that this has had immeasurable impact."

Snowden believes that officials like Litt are merely trying to scare the public into acquiescence. Last October, the two had a showdown of sorts when they spoke back-to-back at a conference at Bard College. "Each time we have an election, it's like another round of a game," Snowden told the students.

Using a livecasting program designed for gamers that allows him to project illustrations, he filled the auditorium screen with an image of George W. Bush shaking hands with Obama. "The policies of one president become the policies of another." Then he played a video clip of the cleric Anwar al-Awlaki's son, a 16-year-old American citizen killed by a drone strike in Yemen. He cited a leaked 2015 email in which Litt addressed the hostile legislative climate, recommending "keeping our options open" for a change "in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."

"Surveillance is ultimately not about safety," Snowden said. "Surveillance is about power. Surveillance is about control."

Litt opened his remarks by joking that he could sympathize with the act that went on Ed Sullivan after the Beatles. "I can hear the NSA's opinion any day," one student stage-whispered, as he and many others got up to head for the exits. Litt called after them, saying he was "disappointed" with the disdain "given that this is an academic environment." He then elaborated on the ominous sentiment expressed in his email.

"Every time something bad happens, the finger gets pointed at the intelligence community," Litt said. "There is a pendulum that swings back and forth, in terms of the public view of the intelligence community, between, 'You mean you're doing what?' and 'Why didn't you protect us?' And that's a pendulum that's going to swing again."

While much of Washington remains hostile to him, Snowden is far more hopeful about Silicon Valley and is increasingly focusing his efforts on influencing technology and the people who make it. "Like me, they grew up with this stuff," he told me. "They remember what the internet was like before everybody felt it was being watched."

The Snowden leak "was like a gut punch for people across Silicon Valley," says Chris Sacca, a venture capitalist who invested early in Twitter and Uber and who now appears on the television show Shark Tank. Sacca was personally friendly with Obama, raising large sums for his 2012 campaign, but was shocked when he discovered the extent of the NSA's spying and has since become a vocal Snowden supporter. Last November, Sacca did an admiring interview with Snowden at the Summit at Sea, an invite-only weekend of seminar talks and techno dancing aboard a cruise ship, which was attended by the likes of Eric Schmidt, chairman of Alphabet, and Travis Kalanick, CEO of Uber. "After fielding over an hour of tough questions," Sacca says, "he got a resounding standing ovation from the room."

Even as Snowden captivated the audience on the boat, though, terrorists were mounting a bloody coordinated attack in Paris. The pendulum was swinging back. At first, Wizner says, Snowden was shaken -- he worried that the attacks had wiped out all of his progress. Almost immediately, anonymous security sources blamed encryption for giving cover to the attackers. (Subsequent reports suggest they may have been more reliant on primitive tactics, like using burner phones.) "They dragged out all the old CIA directors, the line of disgrace, to suddenly try to reclaim a halo," Snowden told me. "It did look really

exploitative." For three weeks, he went quiet, posting just once to Twitter, quoting Nelson Mandela about triumphing over fear. Meanwhile, Syed Farook and Tashfeen Malik attacked in San Bernardino, and Trump called for a ban on Muslim immigration.

Wizner advised his client to be patient. Snowden sometimes says he thinks of his existence like a video game: a series of challenges that culminate in a final screen, where you either win or it's game over. But political outcomes are never so final -- it's an iterative process. In February, when Apple announced it was refusing to break into Farook's iPhone for the FBI, Snowden was suddenly scoring points again. ("The @FBI is creating a world where citizens rely on #Apple to defend their rights," he tweeted, "rather than the other way around.") In an open letter, Tim Cook, Apple's chief executive, talked the way Snowden does about privacy, encryption, and government "overreach." The next day, Snowden spoke at Johns Hopkins University, where hundreds of shivering students lined up to get into a packed auditorium. "This is a case that's not about San Bernardino at all; it's not a case that's about terrorism at all," Snowden warned. "It's about the precedent."

Litt believes that, besides giving information to enemies, Snowden's disclosures have also had a radicalizing effect in the private sector. "The technology and communications community has moved from a position of willingness to cooperate," he told me, "to an attitude that ranges from neutrality to outright hostility, which is an extremely bad thing." Recently, Snowden has been working with technical experts who are mobilizing to fortify the internet's weak spots, both through collaborations with academic researchers and back-channel conversations with employees at major tech companies.

In all of these conversations, Snowden is operating on the assumption that a truly private space on the internet could be easier to create than to legislate -- that it may be more fruitful to coax programmers to invent something that is difficult to hack than it would be to try to reshape the entire national-security bureaucracy so it stops trying. "I'm regularly interacting with some of the most respected technologists and cryptographers in the world," Snowden said. "I believe that there's actually a lot more influence that results from those sorts of conversations, because so much of technology is an expert game."

The aspect of the Snowden leaks that most outraged technology experts was not the NSA's communications surveillance but its efforts to undermine encryption, which had broad impacts on computer security. That news has "created a period of innovation" in encryption, says Moxie Marlinspike, the San Francisco-based security specialist who developed Signal, the messaging program that Snowden likes to use to communicate. Marlinspike has become friendly with Snowden, whom he met in Moscow, where they had a lengthy discussion about the trade- offs between security and usability. (Snowden is always seeing holes hackers can poke through; Marlinspike wants to make encryption accessible to laypeople.) In April, WhatsApp, which is owned by Facebook, announced that it had integrated the Signal protocol Marlinspike developed, allowing it to offer end-to-end encryption. Those sorts of technical decisions, like Apple's strengthened encryption standards, affect the privacy of millions of customers.

But Snowden is skeptical of the motives of tech companies. "Corporations aren't friends of the people, corporations are friends of money," he said. He prefers to collaborate with academics and hacktivists, some of whom are helping him with projects he is developing for the Freedom of the Press Foundation. It already manages SecureDrop, a system for anonymously leaking documents, and the nonprofit's technical staff is working with Snowden to develop other programs tailored to protect journalists and whistle-blowers. "His goal with us is to start designing and prototyping what the tools of the future will look like," says Trevor Timm, the foundation's executive director. One of Snowden's priorities, unsurprisingly, is improving the security of videoconferencing.

About once a week, the team meets on a beta-stage video platform, where they discuss the painstaking work of testing their technology, a probing process called "dogfooding." As a prime target for hacking attacks, Snowden is in a unique position to appreciate extreme-threat models. He often comes up with exotic problems to solve and is able to bring in outside minds for confidential consultations. "We're building small projects," Snowden says, but he can't help but see larger applications. He talks enthusiastically about virtual reality, which could soon supplant videoconferencing. "In five years this shit's going to blow your mind," Snowden told me. But he also sees potential dangers. "Suddenly, you've got every government in the world sitting in every meeting with you."

Snowden is especially concerned about the monitoring power of Facebook, which acquired Oculus VR, the virtual-reality headset maker, for $2 billion. "What if Facebook has a copy of every memory that you ever made with someone else in these closed spaces?" he asked rhetorically. "We need to have space to ourselves, where nobody's watching, nobody's recording what we're doing, nobody's analyzing, nobody's selling our experiences."

It is clear that in virtual reality, Snowden sees more than just a work tool. "Right now, the technology is not quite there, but this is the first step," the Snowbot told Peter Diamandis, the space entrepreneur and Singularity University co-founder, in an interview at this year's Consumer Electronics Show. "I have someone who is very close to me," Snowden explained, "who was the victim of a serious car accident, and because of that they can't travel." Virtual reality could bring them together. Or it could allow him to visit home for Thanksgiving, overcoming what he calls "the tyranny of distance."

More than one person told me that, after talking to Snowden for hours on end, they got the sense that he is lonely. His conversation is preoccupied with the theme of escape. He recently collaborated on a track with a French musician, delivering a spoken-word monologue on surveillance over an electronic beat, and recommended the title: "Exit."

Snowden sometimes says that although he lives in Russia, he does not expect to die there, and he told me he is optimistic that he will find a way out, somehow. Maybe some Scandinavian country will offer him asylum. Maybe he can work out some kind of deal -- whether outright clemency or a plea bargain -- with the Justice Department. Wizner has been working with Plato Cacheris, a well-connected Washington defense attorney, but so far, there have been no official signals that the Justice Department would be willing to offer the kind of lenient terms Snowden would accept. And a window may be

closing. He is unlikely to receive a more receptive hearing from Hillary Clinton, who has said he shouldn't be allowed to return without "facing the music." As for Donald Trump: He has called Snowden a "total traitor" and suggested he should be executed. "If I'm president," he predicted last year, "Putin says, 'Hey, boom -- you're gone.'?"

So the comparatively thoughtful Obama may be Snowden's best hope, but even Snowden's allies concede that they doubt the outgoing president has the inclination to offer a pardon. "There is an element of absurdity to it," Snowden told me. "More and more, we see the criticisms leveled toward this effort are really more about indignation than they are about concern for real harm." He says he would return and face the Espionage Act charges if he could argue to a jury that he acted in the public interest, but the law does not currently allow such a defense. "These people have been thinking about the law for so long that they have forgotten that the system is actually about justice," Snowden said. "They want to throw somebody in prison for the rest of his life for what even people around the White House now are recognizing our country needed to talk about."

Earlier this year, Snowden was buoyed by an invitation from an unexpected source. David Axelrod, the president's former top political strategist, asked him to appear at the institute he now runs at the University of Chicago. Beforehand, they had a video chat. "The president of the United States' closest advisers," Snowden told me later, "are now introducing me and sharing the stage with me in ways that aren't actually critical. I'm not saying this to build myself up. I'm talking about the recognition by even the people who have the largest incentives to delegitimize me as a person, that maybe we overreacted, maybe this is a legitimate conversation that we need to have."

Axelrod asked Geoffrey Stone, a liberal law professor who is friendly with Obama, to moderate the public talk. Stone is a member of the ACLU's National Advisory Council and the author of a book titled Top Secret: When Our Government Keeps Us in the Dark, but he also served on Obama's commission to review the NSA's surveillance programs, an experience that gave him access to classified information and a dim view of Snowden. "My view is that he cannot be granted clemency, because he did commit a criminal offense and it did considerable harm," Stone told me. "The people who are celebrating Snowden have no understanding of the harm, for the reason that the people in the intelligence world can't really explain the harm to them." Snowden considered Stone's position to be "an example of regulatory capture," proof of the seductive power of security clearances. Secret knowledge, Snowden says, "is a very intoxicating thing."

Still, Snowden was looking forward to the debate, if only because it illustrates his progress. Wizner, who considered the Axelrod relationship important to his future clemency push, attended the May event in person. "We've gone from the president saying 'We're not going to scramble jets for a 29-year-old hacker' to talking with the president's rabbi,'?" Wizner said backstage as event staff set up computers and projection equipment. "That's a good journey for us."

Axelrod shambled in, looking sleepy-eyed as always, as students filled the auditorium and Wizner texted last-minute instructions to his client over Signal. "Whatever you think about Edward Snowden and his

actions, and the adjectives range from traitor to hero," Axelrod said by way of introduction, "he has indisputably triggered a really vital public debate about how we strike a balance between civil liberties and security." He sat down in the front row as Snowden's bashful grin filled a large screen.

Snowden had already done one event that day, a cybersecurity conference in Zurich, and he seemed weary as Stone probed for logical weaknesses. The law professor asked when it was appropriate for "a relatively low-level official in the national-security realm to take it upon himself to decide that it is in the national interest to disclose the existence of programs that have been approved ... To decide for himself that 'I think they're wrong.'?" Snowden gave his usual homilies about the Constitution, whistle-blowing, and civil disobedience. "Do we want to create a precedent that dissidents should be volunteering themselves not for the 11 days in jail of Martin Luther King or the single night of Thoreau," he asked, "but 30 years or more in prison, for what is an act of public service?"

Stone pointed out that Congress could pass a law allowing defendants to make a whistle-blowing defense in Espionage Act cases but shows no signs of doing it. "You believe in democracy," Stone said. "But democracy doesn't agree with you." The professor jabbed and Snowden weaved, setting his jaw and taking swigs from a big plastic water bottle. But when the floor opened for questions, it was clear who had won the audience. One student after another got up to offer Snowden praise.

"Did you expect to become a celebrity in this way?" one asked.

"If you go back to June 2013," Snowden said, "I said, 'Look, guys, stop talking about me, talk about the NSA.'?" But he added, "Our biology, our brains, the way we relate to things, is about character stories. So they simply would not let me go."

Axelrod watched impassively, his fingers tented under his nose. The full effect of Snowden's performance did not become clear until a few weeks later, when Axelrod had Eric Holder -- the former attorney general, once Snowden's chief pursuer -- on his podcast, The Axe Files. Holder allowed that Snowden "actually performed a public service," while Axelrod calmly presented Snowden's arguments.

"I think there has to be a consequence for what he has done," Holder replied. "But I think, you know, in deciding what an appropriate sentence should be, I think a judge could take into account the usefulness of having had that national debate."

Holder's concession made international headlines. It didn't mean anything legally, but symbolically it spoke volumes. Political realities were starting to come into alignment with Snowden's virtual ones. From his computer in Moscow, Snowden tweeted:

2013: It's treason!

2014: Maybe not, but it was reckless

2015: Still, technically it was unlawful

2016: It was a public service but

2017:

Montreal Gazette
Security specialists at forefront of cyber battle
Wednesday, 29 June 2016
Byline: Karen Seidman

Montreal - The huge "threat detection" screen at the front of the Montreal Cyber Intelligence Centre is ablaze with blinking lights, but none of the eight or so Deloitte employees manning the restricted centre seem particularly alarmed. Cyber attacks are routine for this gang of cybersecurity specialists, who try to keep the world safe from Internet thugs while hunkered down in their state-of-the art facility in downtown Montreal.
Another jumbo screen is monitoring brute-force logins as it keeps track of the "cyber kill chain" that aims to identify and prevent cyber intrusions. Despite the violent terminology casually shared between the co- workers, the room hidden behind a facial-recognition security system in the professional services firm's gleaming new downtown tower houses an unflappable team of hackers and risk experts hired to minimize casualties.

For there is no doubt about it, this is a modern-day war room in a cutting-edge battle that the general says we are losing. Badly.

That would be Robert Masse, leader of Deloitte's cyber risk services in Montreal and the incident response team across Canada, who spends his days trying to outsmart the increasingly sophisticated cyber criminals who are ready to pounce when they detect any vulnerabilities in the system.

"Companies are being attacked all the time," Masse said in an interview during a tour Tuesday which offered a glimpse into the workings of a cybersecurity centre. "We are really on the front lines of a cyber war."

The team he works with - about 70 in total across the three Canadian Cyber Intelligence Centres in Calgary, Montreal and Toronto - help companies monitor their systems for attacks 24/7. Deloitte has 15 such centres globally.

Vigilance is everything when the threat landscape and attack surface are so massive, as it is with the ubiquitous Internet, yet Deloitte's own research shows that only 36 per cent of businesses have effective procedures and technologies in place to protect critical assets.

"There are so many vulnerabilities that it's a free-for-all," Masse said. "People can't keep up with the sheer volume of attacks. We are losing the war."

One of the ways Deloitte helps companies protect themselves is by going into attack mode and launching advanced two- to threemonth campaigns to break into a company's system to reveal weaknesses. Their track record? One hundred per cent.

They won't ever use the word "foolproof" when discussing cybersecurity and who is vulnerable:

Banks, the U.S. National Security Agency, big business, small business, governments, everyone.

Attackers no longer even care about obtaining credit card information or other proprietary information in an attack; it's enough to get into a company's system, encrypt any operating information with ransomware and demand payment in Bitcoins. These ransomware attacks are reaching epidemic proportions, according to Masse, and affect both individuals and corporations in an important way.

And companies are quietly paying thousands of dollars to get their systems back up and running. Everyone is encouraged not to pay, but many have no choice. And the culprits do subsequently release the information because it's important to their business model; they even offer 24/7 customer service.

There are typically two kinds of attacks: a commodity attack or a targeted attack (increasingly popular, this is when attackers create a weaponized document, like an email that appears to come from a colleague but which allows an attacker to bypass the cybersecurity defences of a company once an attachment is opened).

Motives include financial gain, hacktivism for political or ideological purposes, and information for personal gain (like bringing down a competitor).

To show the hacker mentality, Deloitte consultant Sarantos Tsikinis detailed a commodity attack on a women's shoe and accessories company based on a real case they handled.

Using a botnet, a collection of many computers known as zombies, the attacker begins his reconnaissance, similar to checking every lock in a neighbourhood you might want to rob. He launches port scans to see which ports are open. When he finds a form on a login page, he knows many websites don't use form validation, which allows him to enter special characters that break the code and enable him to enter his own code.

That was the key left under the doormat.

"He can now interact directly with the web server and see data that is useful to him," said Tsikinis. It doesn't take much poking around before he finds a password and he can then generate a TCP connection which gives him entry through a back door.

Voila, there is a list of clients and their emails and passwords. Doesn't sound like much, but considering that the vast majority of people reuse their passwords (heck, Facebook founder Mark Zuckerberg was hacked because he did this) and the website had some 5 million users, it could be important. Masse can't stress enough that reused passwords are the premier vulnerability.

"This turns out to be a big breach and he gets all the credit card information, which he then sold," said Tsikinis.

What Deloitte offers its clients, he said, are the right barriers to slow down attackers and make it easier to thwart attacks.

Still, he and Masse emphasize that no business is immune. Masse calls it "asymmetrical warfare": the bad guys have to be right once, while the good guys have to be right 100 per cent of the time to defend themselves.

The Hindustan Times
Modi govt gets cracking on cyber espionage
Wednesday, 29 June 2016

New Delhi - It is not just sensitive data that cyber spies are looking to access but the possibility of terror groups using hackers to target vital security and infrastructure installations has spooked the security establishment.
Amid threats of hackers orchestrating attacks on nuclear or power stations, the government is for the first time framing a comprehensive policy to deal with cyber espionage and other threats related to it, highly placed sources in security establishment said.

The framework that explores the possibility of setting up a panel of experts who can work closely with the security establishment is the Prime Minister's Office.

Making changes in existing laws to keep pace with changing dynamics of the cyber threat is also being worked out.

Strengthening the cyber security workforce and upgrading infrastructure to combat the threat is part of the mechanism being planned.

"It requires inter- ministerial consulit's the biggest security challenge and the threat will only be more in days in future.

Sources say there is also a big jump in the alerts regarding hacking that are being shared with the Ministry of Home Affairs (MHA) as they have could have direct implications on national security.

Last month, a global cyber security firm that a cyber espionage group ' Suckfly' targeted high profile government and commercial organisations.

According to other reports another cyber spy group ' Danti' has access to Indian government organisations.

The PM has also suggested that countering the menace on the virtual world experts in the field have to be roped in at the earliest.

Later, this core team could involve officials on the grassroots level to be part of the team that focuses on the cyber space.

It needs to be worked out who will be the nodal body. The Intelligence Bureau and home ministry will definitely have an important role. It requires huge capital since top technology needs to be used," said a government official.

Sources in intelligence agencies currently dealing with cyber threats say Strengthening the cyber security workforce and upgrading infrastructure is part of the mechanism being planned

Experts to be roped in as part of specialised wing Infrastructure to be revamped Danger of cyber espionage increasing. Terror attacks through cyber space a possibility now The framework that explores the possibility of setting up a panel of experts who can work closely with the security establishment is being closely monitored by the Prime Minister's Office Strengthening the cyber security work force and upgrading infrastructure to combat the threat is part of the mechanism being planned.

South China Morning Post
New rules to control mainland app market
Wednesday, 29 June 2016
Byline: Nectar Gan and He Huifeng

Beijing - Internet authorities are tightening their grip on the rapidly growing app market, with new rules demanding that all app providers on the mainland adopt real-name registration for users and keep their user activity logs for 60 days.
The new rules from the Cyberspace Administration of China also aim to rein in excessive access of users' personal data by app -providers.

The new regulation applies to the provision of "information services through mobile internet apps as well as ... app store services on the Chinese mainland" . It is unclear if the new regulation would affect overseas users of Chinese apps.

The administration said the regulation, which will take effect from August 1, was introduced to curb the dissemination of "illegal information" and violations of users' rights through mobile apps.

"Lawbreakers exploit a handful of apps to disseminate violent, terrorist, obscene and pornographic information and rumours against the law," an unnamed CAC official said in a statement on the agency's website.

The administration estimated there were more than four million apps available through online stores on the mainland. According to research firm Analysys International, WeChat, QQ, Alipay, Taobao and Tencent Video were among the most popular last month in terms of number of -active users. Alibaba, which operates Alipay and Taobao, owns the South China Morning Post.

Under the new regulation, users will still be allowed to adopt a public alias but not before registering their real identities with the app providers. App providers must verify those identities by mobile phone numbers or other means.

Providers should issue warnings, restrict access, suspend updates or shut down accounts of users who publish "illegal information" and content.

App store operators, meanwhile, will be required to vet the apps' security and compliance with the law.

App providers will also need the explicit consent of users to gain access to their geographic -location and contact list, record video and audio through their mobile devices, or activate or bundle unnecessary functions with their services.

Beauty app founder Qi Shudan said the regulation would likely have a bigger impact on apps that had many commenters. "It will have little effect on apps of our kind that are only for business and commerce," Qi said.

A Guangzhou-based app operator, who refused to be named, said the rule on activity logs was a warning to "all internet users not to make improper comments on social or political issues because every word you type will be -recorded and handed in to the authorities".

"Many users like to comment on social and political news on live-streaming and news apps. Now they will need to think twice before making any comment that authorities could claim spurred public scares or rumours," he said.

"Such rules only put further limits on freedom of speech."

The authorities have ramped up online real-name registration since last year, implementing it for instant messaging services, Twitter-like microblogs, online forums and other websites.

On Monday, a controversial cybersecurity bill was also presented to the national legislature for a second reading.

Kyodo News
Japan, U.S., S. Korea hold joint missile-tracking exercise in Hawaii (Canada)

Wednesday, 29 June 2016
Byline: Staff reporter

Washington - The naval forces of the United States, South Korea and Japan concluded an eight-day, trilateral missile-tracking exercise off Hawaii on Tuesday, amid continuing ballistic missile launches by North Korea that have increased tension in the Asia-Pacific region.
This year's "Pacific Dragon," the third since the biennial exercises began in 2012, "featured a coordinated live ballistic target tracking event where each nation's Aegis Ballistic Missile Defense System capabilities were tested and improved," the U.S. 3rd Fleet said in a press statement.

The exercise, which was held off the coast of Kauai island, partly involved the Japanese Maritime Self-Defense Force's Chokai, an Aegis destroyer with the capability to intercept ballistic missiles, and two South Korean destroyers with like capability.

"While there were no missiles fired, all participants strengthened interoperability, communication channels, data collection and capabilities assessments," the statement said.

It said they shared tactical data link information on the basis of a memorandum of understanding on sharing and safeguarding classified information on North Korea's nuclear and missile programs that was signed in December 2014.

During the exercise, North Korea carried out two test firings of its Musudan intermediate-range ballistic missile in violation of U.N. Security Council resolutions, claiming success after one of them flew 400 kilometers and reaching an altitude of more than 1,000 km.

The missile has a potential range of between 2,500 and 4,000 km, which would cover not only any target in Japan and South Korea, but could also even reach U.S. military bases on the Pacific island of Guam.

North Korea, through its official media, reacted angrily to the trilateral exercise, calling it a "provocation" and vowing to "bolster in a sustainable manner the capabilities for preemptive nuclear attack to pose a constant threat to the enemies."

The trilateral exercise came ahead of the Rim of the Pacific, or RIMPAC, exercise that starts Thursday and will last through Aug. 4, in and around the Hawaiian islands and southern California, involving the same three countries.

This year's RIMPAC, the world's largest international maritime exercise, also involves Australia, Britain, Brunei, Canada, Chile, Colombia, Denmark, France, Germany, India, Indonesia, Italy, Malaysia, Mexico, the Netherlands, New Zealand, Norway, China, Peru, the Philippines, Singapore, Thailand and Tonga.

Times of Israel

Israel to hold cybersecurity conference in Beverly Hills (Canada).
Wednesday, 29 June 2016
Byline: Shoshanna Solomon

Jerusalem - Cybertech, the organizer of Israel's largest cybersecurity conference, will hold its first event in Beverly Hills on Thursday, June 30, in partnership with Israel's Los Angeles consulate general and the City of Beverly Hills.
"In the face of new threats we encounter daily, individuals, organizations and states are required to produce innovative, unique solutions to strengthen the resilience of sensitive communication systems they rely on every day," Amir Rappaport, the chief executive of Cybertech, said in an emailed statement. "For this purpose, it is essential to be aware of the latest developments in the cyber defense market."

The collaboration between the City of Beverly Hills and Israel is a direct result of an agreement signed in 2014 by California Governor Edmund Brown and Israeli Prime Minister Benjamin Netanyahu for cooperation in projects and research.

The intention of the collaboration with the City of Beverly Hills is "to promote professional cooperation and trade partnerships in areas such as cybersecurity, water innovation, and public safety," the statement said.

"Israel is second only to the United States in global private investment in cybersecurity firms, with half a billion dollars flowing to the sector annually," David Siegel, consul general of Israel to the Southwest United States, said in the statement. "This conference will create new groundbreaking opportunities for both our countries."

Cybertech Beverly Hills will include panel discussions on cyber-crime investigations, financial technology, media and entertainment and critical infrastructure. The event will also hold an exhibition of new technologies from Israeli and US start-ups and companies, including Palo Alto Networks, CyberArk and Fortscale.

Cybertech has held cyber solutions events in Tel Aviv, Singapore and Toronto. Its Tel Aviv event, one of the largest in the field outside the US, has over 12,000 participants annually from over 50 countries, the statement said.

Voice of America
US Increasingly Focused on Social Media to Weigh Terror Threats
Wednesday, 29 June 2016
Byline: Chris Hannas

Washington - The United States government has become increasingly focused on the idea of examining social media posts in order to make determinations about who represents a security threat to the country.
The latest example is a proposal from the Customs and Border Protection arm of the Department of Homeland Security to ask foreign travelers to disclose information about their accounts on services like Facebook and Twitter.

It would appear as an optional question on the form people fill out either upon arrival or presubmit online with information such as their name, address, phone number and the names of countries they have visited since 2011. It would also only apply to travelers from the 38 countries allowed visa-free entry into the U.S.

"Collecting social media data will enhance the existing investigative process and provide DHS greater clarity and visibility to possible nefarious activity and connections by providing an additional tool set which analysts and investigators may use to better analyze and investigate the case," the proposal says.

Customs and Border Protection is asking the Office of Management and Budget for permission to add the question and says it would affect an estimated 24 million people. There is a 60-day comment period for the public to weigh in.

Meanwhile, members of Congress have been busy during their current session drafting bills involving examining social media posts for terror links.

Senator John McCain sponsored one of several bills that would require the Department of Homeland Security to look at internet activity and social media profiles of anyone applying for admission to the U.S.

"It is unacceptable that Congress has to legislate on this, and that it wasn't already the Department of Homeland Security's practice to take such commonsense steps when screening individuals entering this country," McCain said.

A bill from Senators Martin Heinrich and Jeff Flake specifies that DHS "may search open source information, including internet and social media postings, of an alien who applies for a visa to enter the United States."

"It should be crystal clear to those inside and outside of DHS that the agency has the authority to review publicly available social media posts when vetting visa applications," Flake said.

The proposals do not seem to address the accounts of anyone who has set their posts to be private.

"Reviewing the public social media posts of an individual seeking a U.S. visa is just common sense in the digital world we live in today," Heinrich said.

Senator Chuck Schumer has proposed a different tactic to alert authorities to potential terrorists. He wants to use the Justice Department's existing Rewards for Justice program to pay people who submit a tip about a social media post that leads to the arrest of someone planning an attack in the U.S.

"We are in a time when a terrorist a world away can corrupt a disaffected youth -- and with just a few posts or tweets, can push them to plan or carry out acts of terror," Schumer said. "We need the public's eyes to alert authorities if they see someone they know writing things they know spell trouble."

He wants the awards to range from $25,000 to $25 million.

In the House of Representatives, Congressman Stephen Fincher is focusing on keeping those serving time in federal prisons from becoming radicalized and posing a threat when they are released. His bill calls for anyone who wants to volunteer in the prisons to divulge their social media accounts as part of a background check for possible links to terrorism.

"Over the years, our federal prisons have become a breeding ground for radicalization," Fincher said. "By allowing volunteers to enter the system without first having to undergo a comprehensive background check, some of the most vulnerable members of society have become susceptible to radicalization."

Washington Free Beacon
State Department Report Says Chinese Cyber Attacks 'Ongoing'
Wednesday, 29 June 2016
Byline: Bill Gertz

Washington - Chinese cyber attacks against American firms are "ongoing" and the use of covert cyber tools and methods by Beijing hackers led to a statistical decline in cyber activities, according to an internal State Department security report.
The report by the State Department-led Overseas Security Advisory Council, or OSAC, a public-private partnership, challenges the findings of a recent study by the private cyber security firm FireEye that says the decline in the number of Chinese-origin cyber attacks indicated China has cut back from large-scale cyber attacks.

"While media reporting has emphasized this alleged decrease in malicious activity, cases of Chinese espionage campaigns against the U.S. private sector are ongoing," the report said, adding that "OSAC constituents should remain aware that China is still considered a highly capable and motivated cyber threat actor."

The three-page report highlighting ongoing Chinese cyber threats is a setback for White House efforts to portray President Obama's September 2015 deal with China to curb cyber economic espionage as a diplomatic breakthrough.

Since the deal, various private security firms offered differing assessments of whether China is curtailing large-scale cyber attacks, the report said.

The report notes that Chinese cyber attacks in 2015 were particularly damaging. "At a higher level, paramount attacks against various U.S. organizations continued in 2015 and Chinese hackers exceeded other nation-state actors for consistency, volume, and severity of cyber attacks during the past year," the report, dated June 27, says.

"This included intrusions into healthcare systems Anthem and Premera, and the Office of Personnel Management, collectively compromising the sensitive data of over 100 million U.S. citizens."

Until the OSAC report, senior U.S. intelligence officials have sought to hedge their conclusions about the September agreement, stating publicly that it is not clear whether China is curbing cyber intrusion activity.

According to the OSAC report, the large- scale attacks in 2015 "suggests some China-based hacking groups may have shifted their focus from data theft for economic gain to national security interests and personally identifiable information (PII)."

According to OSAC, Chinese cyber attacks also have been focused on "continuously leveraging U.S. network infrastructure for offensive operations."

"Actors have been observed using servers of small businesses in the U.S. to plan and execute attacks against manufacturing firms, financial organizations, and the technology sector," the report said.

Rick Fisher, a China specialist, said China's Communist Party leaders see no current positive or negative inducement to halting the use of cyberspace for global intelligence gathering that can be used to prepare attacks on cyber-electronic infrastructures.

"American verbal argument or political pressure is not going convince the [Chinese Communist Party] leadership to stop waging its global cyber war," said Fisher, a senior fellow at the International Assessment and Strategy Center.

"Washington has been trying to engage the Chinese on its cyber war for nearly 20 years and has basically gotten nowhere," he noted.

The FireEye report was based on a study of network intrusions and compromises from China-based cyber actors since mid-2014. It tracked 262 cases to Beijing hackers carried out in 26 countries. The majority of the attacks took place against U.S. information networks.

The targets included aerospace companies, healthcare providers, manufacturers, including those building semiconductors and chemical compounds, along with media, software, and technology firms.

"Chinese targeting (and in some cases, successful stealing) of data from various public and private sector organizations is assessed to serve military, security, and economic interests equally," the report says. "This ambiguity makes it difficult for analysts to characterize the objective of recent Chinese cyber espionage operations."

OSAC analysts said the attention given to the FireEye study is based in part on a sharp decrease in the number of detected cyber attacks compared to the larger number of cyber intrusions logged by researchers three years ago.

The apparent decline in Chinese cyber activities was attributed to the Justice Department's high-profile indictment of five PLA military hackers in 2014, and the September 2015 meeting between Obama and Chinese leader Xi Jinping when the informal accord was struck calling for both governments not to engage in or "knowingly support" cyber economic espionage.

"While interpreted by some as nothing more than a political maneuver, other analysts believe the 2015 agreement may have somewhat influenced the decrease in malicious intrusions conducted by China-based groups," the OSAC report said.

However, the cutback could be the result of FireEye's lack of visibility of more recent Chinese cyber activities or the computer forensic investigators' inability to detect new cyber attack methods used by the Chinese.

"Public exposures [of Chinese hacking] have prompted some observed China-based hacking groups to develop new tools and incorporate anti-detection techniques into their offensive cyber operations," the report said.

Contrasting FireEye's assessment of a decline, the OSAC report said multiple studies confirm that "China-based network intrusions are still ongoing, only a fraction of which may be detected by researchers."

The council report also said the cyber security firm CrowdStrike reported three weeks after the Obama-Xi agreement that China was continuing cyber attacks on U.S. organizations.

Most of the targeted companies were engaged in technology or the pharmaceutical industries, an indication the goal is theft of American intellectual property.

The CrowdStrike report concluded that the U.S.-China agreement was ineffective, and that if the Chinese government were abiding by the agreement it would have controlled the central group of Chinese hackers behind the continued attacks.

The decline of attacks seen in metrics has not diminished the threat, the OSAC report said, noting, "China remains a serious cyber threat actor to U.S. firms."

China's hacking community is made up of government and military hackers, those who engage in cyber attacks on a contract basis, so-called "hacktivists," and criminals.

The report said competing interests between the groups has made it difficult for analysts to determine if there is a "top-down direction" for Chinese cyber attacks. The various cyber actors also "may mask continued attempts of cyber espionage," the report noted.

The OSAC report warned American companies to remain up to date in understanding ongoing Chinese network compromises against both private and public entities.

"Employing multi-layered network defense and detection systems, maintaining regular updates, and mandating employee cyber threat awareness programs can help OSAC constituents defend against threats of cyber espionage, crime, and other malicious network activity," it said.

Fisher, the China specialist, said the United States will not dissuade China from aggressive cyber attacks until Beijing is made to pay a price for digital aggression.

An initial step would be for the United States and NATO members to join together in expelling all Chinese nationals studying abroad in the field of computer science. Another would be to embargo all Chinese computer hardware and software from those countries, Fisher suggested.

"Chinese electronic infrastructure leaders like Huawei and computer manufacturers like Lenovo have long been identified by U.S. government agencies as cyber espionage threats so the justification for such an embargo exists already," he said.

BBC News
CIA taps huge potential of digital technology
Wednesday, 29 June 2016
Byline: Gordon Corera

London - At CIA headquarters in Langley, the office of the director of digital innovation sits next to the agency's in-house museum filled with artefacts from its history.
Featuring heavily are gadgets such as early secret cameras and bugging devices that would not appear out of character in a Hollywood film.

The line-up makes the point that even though the CIA is an intelligence agency whose central mission has been to recruit people to provide secrets, technology has always had a crucial role.

Andrew Hallman - who runs the recently created Directorate of Digital Innovation - has the job of making sure that the new digital world works to the CIA's advantage rather than disadvantage.

A major focus of Mr Hallman's effort is to use data to provide insights into future crises - developing what has been called "anticipatory intelligence".

This means looking for ways in which technology can provide early warning of, say, unrest in a country.

"I think that's a big growth area for the intelligence community and one the Directorate of Digital Innovation is trying to promote," Mr Hallman says.

The volume and variety of data produced around the world has grown exponentially in recent years - a process about to accelerate as more and more items as well as people are connected up in the so-called internet of things.

The ambition is to take this wealth of data and combine it with analytical models fine-tuned with insights from social sciences to spot where an issue such as food scarcity might be emerging and might, in turn, lead to instability in a region.

This might also involve looking at social media to perform "sentiment analysis" that can help understand if the mood in a population is turning sour.

The idea would be to spot a major change, such as the so-called Arab spring, as early as possible and provide policymakers with the kind of advanced warning they often crave and which intelligence agencies are sometimes criticised (fairly or unfairly) for failing to deliver.

These are often the kind of events not susceptible to the traditional intelligence gathering spies normally carry out - the emergence of protest groups in the Middle East was not a secret locked in a safe or in the mind of a leader that could be stolen or enticed out.

But the techniques of big data, some believe, may offer answers.

Mr Hallman, crisp in both words and appearance, is careful to explain this will not provide a crystal ball that can predict "point events" - for instance that the breakdown of order will happen on a particular day - but, instead, will point to a social or economic system becoming more fragile than might be superficially apparent.

More broadly, the directorate aims to change the culture as well as the structure of the CIA - bringing in technology and integrating it into every part of the agency's work.

The CIA has 10 mission centres where analysts and operators work together on either parts of the world or issues (with centres for Africa, the Near East, Counterterrorism, and Weapons and Counter-proliferation).

Digital officers will integrate into these and bring with them expertise in cyber-techniques, data sciences and software development.

The aspiration is that where some new technological innovation is pioneered in one mission centre, the Directorate for Digital Innovation will see if it can be pushed out to other centres.

Developing expertise in open-source (publicly available) information is another priority - in the past this was something of a sideshow at an agency that focused on "secrets" - but such information can often help focus on what really is secret and what can be obtained by other means, especially as the definition of open source expands rapidly from the past, when it largely meant foreign news and media.

This might involve understanding how a group such as so-called Islamic State (IS) uses social media and working out what options there are to address it.

Data is also changing the sharp end of human intelligence.

The head of Britain's MI6, Alex Younger, has described a high-stakes arms race in technology.

Spy agencies can use data to improve the way they find the secrets and people they are after.

But foreign security services can also use data to track down intelligence officers and identify them, using the digital exhaust we all leave in our wake in the modern world (one reason for the neuralgic reaction within the US government to the cyber-theft of vetting information from the Office of Personnel Management last year, which could be used to identify spies).

This poses fundamental challenges to the old concepts of operating clandestinely and "undercover".

"It is an existential challenge, which we are looking at very closely," Mr Hallman says.

He stresses though that the issue of how far data enables or restricts spy agencies will ultimately depend on their ability to adapt.

"That's entirely on us and how aggressively we can pursue both avenues," he says.

Intelligence officers in the field will need to become much more technologically adept rather than relying on the kind of human wiles and guile so highly prized in the past.

"Operators have to figure a way to enable them both to operate clandestinely and have at their fingerprints with them the digital capability to extend their reach," says Mr Hallman.

Human intelligence and cyber-espionage are increasingly merging.

This means agencies such as the National Security Agency (which focuses on cyber-espionage) and CIA (which focuses on human intelligence) will need to work together much more, something the US intelligence community has sometimes struggled to do.

This new world of digitally enabled espionage will also require a different model of working with the private sector where cutting-edge technology is being developed (the private sector pioneers many of the big data analytics to try to extract value or sell advertising from the information they collect).

Previously, by the time a company brought in a product to meet a need at CIA, it might already be out of date.

"We used to try to make long strides to catch up with the state of the art," Mr Hallman says, "but we need instead to ride a crest of innovation."

The relationship with Silicon Valley, he acknowledges, has been affected by the allegations of former NSA contractor and whistle-blower Edward Snowden.

A business partner of Twitter recently said it would no longer provide services to the US intelligence community.

But Mr Hallman says the levels of suspicion are not uniform.

"There are a lot of great parties in Silicon Valley who understand our values well, but there are some sectors that do not understand the intelligence world," he says.

Part of his job is to change that.

"I'm an optimist - I think we will eventually build that trust," he says.

He points to the working relationship between the intelligence community and Amazon Web Services to provide cloud computing as an example of what the relationship could look like.

Back out in the corridor are historical examples of technology developed initially for espionage - early photocopiers and tiny Minox cameras - all once cutting-edge but now ubiquitous.

Now, spy agencies are learning that maintaining the edge on which they rely will require new ways of working.

New York Times
New Line on Customs Forms May Seek Social Media Data
Wednesday, 29 June 2016
Byline: Ron Nixon

Washington - The federal government has proposed adding a line to forms filled out by visitors to the United States that would ask them to voluntarily disclose their social media accounts, a step that it said would help in screening for ties to terrorism.
Visitors entering the country under the Visa Waiver Program, which allows citizens of some countries to visit up to 90 days without a visa, would not be required to list their social media accounts, and the forms would not ask for passwords. But Customs and Border Protection, which announced the proposal last week in the Federal Register, said the social media information would give it extra investigative tools.

"Collecting social media data will enhance the existing investigative process and provide D.H.S. greater clarity and visibility to possible nefarious activity," the border agency said, referring to the Department of Homeland Security, its parent organization.

The proposal comes after Congress passed legislation last year to add restrictions to the Visa Waiver Program. The legislation was a response to the November terrorist attacks in Paris, which led to fears that European-born or naturalized citizens with terrorist ties could enter the United States without being properly vetted.

Legislation pending in Congress would require the Department of Homeland Security to collect social media information from foreign visitors. The bills were spurred by the terrorist attack in San Bernardino, Calif., in December. The couple who carried out the assault had exchanged private messages online discussing their commitment to jihad and martyrdom, law enforcement officials said, but they did not post any public messages about their plans.

Representative Vern Buchanan, Republican of Florida, who has introduced one of the bills requiring social media information, called the Customs and Border Protection proposal "lame."

"Voluntary disclosure won't keep anyone safe," Mr. Buchanan said. "If we want to win on the digital battlefield, mandatory screening is required."

Mr. Buchanan's bill would direct the Department of Homeland Security to review all public records, including Facebook and other forms of social media, before admitting foreign travelers.

The department said that while it does not consistently examine social media accounts of applicants for visas or immigration, it has a list of nearly three dozen situations in which social media can be examined to screen applicants.

Four pilot projects are underway in the department to examine the use of social media among applicants for immigration benefits. One of the projects, which began in December and runs through this month, screens the social media accounts of applicants for so-called fiancé visas, the program under which one of the San Bernardino attackers entered the United States.

Fox News
Huge number of successful cyberattacks at one federal agency, report reveals
Wednesday, 29 June 2016
Byline: George Russell

Washington - In 2014, a single U.S. government agency was hit with a blizzard of more than 1,370 external attacks on its most vital computer systems, with three out of every eight incidents resulting in a loss of data, according to a new report by the watchdog Government Accountability Office, suggesting hackers have been far more successful at getting at sensitive government information than previously disclosed.
The highly besieged agency was not named in the report, which was given to government officials in May and made public last week. GAO officials declined to provide the name of the agency in response to an additional query from Fox News.

The eye-opening number of data leaks that resulted from the attacks - - 516 "incidents" in all -- is barely mentioned in the 94-page GAO report.

It is mostly buried in the fine print of an information diagram on page 24 of the wordy and technical document.

The fact that the data losses all came from one agency is mentioned only in a footnote to the diagram, and the extraordinary success rate of the attacks has to be calculated from figures speckled on the previous page.

Fox News calculations of the success rate and number of attacks were subsequently affirmed by GAO officials.

The specific nature and importance of the torrent of data losses was not revealed.

A one-page executive summary of the GAO report that is the most likely portion to be read by policymakers or the general public makes no mention of data losses, or of the high success rate of attacks that caused them, or of the focus of the attacks on a single agency.

The high rate of attacks and successes in 2014 has particular significance for U.S. cybersecurity, however.

It was 2014 when the Obama administration revealed one of the worst losses of cyber-information in history had taken place, with the theft of 4.2 million personnel files of past and former U.S. federal civil servants from its Office of Personnel Management (OPM) by China-based intruders.

That loss was subsequently expanded in revelations a month later by 21.5 million sensitive background files on federal civil servants and contractors, after another hack that year, also believed to come from China, removed the huge quantities of sensitive personal information from a private background-checking firm.

On its website, OPM customarily refers to the losses as coming from only two "separate but related incidents" -- a far cry from the triple-digit data loss numbers stashed away in the GAO report.

A Fox News query to the White House Office of Management and Budget, which oversees the effectiveness of cybersecurity across the federal system, yielded no additional information about the figures in the carefully-groomed GAO report.

The computer assault information, along with much of the other information in the GAO document, came from the self-reporting of a swarm of 24 U.S. federal agencies that responded to a survey asking, among other things, about their "high-impact" federal information systems and cyberattacks.

The GAO audit, which took place between February 2015 and May 2016, came at the request of a trio of U.S. senators: Ron Johnson, R-Wis., chairman of the Senate Homeland Security and Government Affairs Committee; Thomas Carper, D-Del., the committee ranking member; and Susan Collins, R-Maine.

According to the report, 18 federal agencies have such "high-impact" systems, defined dramatically but opaquely as those where "the loss of confidentiality, integrity, or availability can have a severe or catastrophic adverse effect on organizational operations, assets or individuals."

During 2014, only 11 of the 18 reported 2,267 cyberattacks on their "high-impact" facilities; another three failed to provide any specific numbers of such assaults.

Virtually all of the agencies designated "nations" -- meaning foreign ones -- as the most serious and frequently-occurring source of the threat.

The GAO report may be highly circumspect about the success of high- impact attacks, but it is far more forthright in noting that cross- government authorities it included in the audit -- including the Office of Personnel Management -- had lots of guidance on how to protect themselves, but even now are still not doing enough to make sure the guidance was followed.

It noted, among other things, that OPM and other agencies had not done well in tracking whether special security training for employees in sensitive roles had been carried out, and none of them had fully completed remedial plans to correct "identified weaknesses" in their high-impact systems security.

For its part, OPM pushed back in a rebuttal that other means than directly tracking the completion of training were more effective and appropriate, especially for contractors, a conclusion that the GAO report did not accept.

OPM also argued that it had made further improvements to its security controls after the GAO audit was done that were not included in the report. GAO's answer: The document "reflects the state of information security at the time of our review."

The fact is that the entire Obama administration is still in the throes of carrying out a sweeping revamp of cybersecurity strategy that, according to some critics, is still far from a coherent answer to the active and still growing cyber- threat.

The senators who sparked the latest report may soon be focusing on some of those shortcomings. They are preparing to look further into the issues raised in the GAO document, which include the muffled and unsettling question of those hundreds of data losses.

The Guardian (London)
Devon schoolboy admits hacking sites but denies airline bomb hoaxes
Tuesday, 28 June 2016
Byline: Steven Morris

London - A schoolboy from Devon launched cyber-attacks on websites across the globe as part of a campaign for animal rights, a court has heard.
Among the 16-year-old boy's targets were SeaWorld Orlando in Florida and a town in Japan where dolphin hunting takes place, Plymouth youth court was told.

The teenager, who was 15 at the time, targeted sites in Africa, Asia, Europe and North America, but he denied sending tweets to two airlines claiming bombs were on board their planes.

He admitted three charges of performing an act to hinder access to a programme under the Computer Misuse Act 1990. The offences relate to distributed denial of service attacks, which involve overwhelming a website with traffic, often taking it offline.

The boy denied two further charges of sending bomb hoaxes to American Airlines and Delta Air Lines. Wearing a grey suit and a tie, he sat next to his mother in court on Tuesday as a trial on those alleged offences began.

The district judge, Diane Baker, told the court the defendant was "a very intelligent young man" who could follow the case "far better than a lot of people in this courtroom".

Ben Samples, prosecuting, claimed the teenager tweeted bomb hoaxes to two US airlines on 13 February 2015. The tweets read: "One of those lovely Boeing airplanes has a nice tick tick tick. Hurry gentleman the clock is ticking." They decided there was no credible threat but the FBI was alerted and they referred the matter to the UK authorities.

British police traced the boy to his home in Plymouth and his laptop was seized from his bedroom, the court heard.

Giving evidence, the boy said he carried out cyber-attacks because he supports animal rights. He said he communicated with hackers but claimed he was just "messing around".

Denying the plane bomb hoaxes, he said: "I feel like I have been stitched up by I don't know who. I don't know why they have done this to me."

Asked by his lawyer, Ken Papenfus, what his general view was of bomb hoaxes, he replied: "It is a really easy way of getting into trouble. It just scares people like something is going to happen when it is not."

He originally admitted making the bomb hoaxes, believing he would get a caution, but told his parents when he left the police station that he did not make the threats. Of his confession, he said: "I was young and scared."

The judge will deliver her verdict on the bomb hoax charges next week.

The Intercept
The Hunter
Tuesday, 28 June 2016
Byline: Peter Maass

Washington - The message arrived at night and consisted of three words: "Good evening sir!"
The sender was a hacker who had written a series of provocative memos at the National Security Agency. His secret memos had explained -- with an earthy use of slang and emojis that was unusual for an operative of the largest eavesdropping organization in the world -- how the NSA breaks into the digital accounts of people who manage computer networks, and how it tries to unmask people who use Tor to browse the web anonymously. Outlining some of the NSA's most sensitive activities, the memos were leaked by Edward Snowden, and I had written about a few of them for The Intercept.

There is no Miss Manners for exchanging pleasantries with a man the government has trained to be the digital equivalent of a Navy SEAL. Though I had initiated the contact, I was wary of how he might respond. The hacker had publicly expressed a visceral dislike for Snowden and had accused The Intercept of jeopardizing lives by publishing classified information. One of his memos outlined the ways the NSA reroutes (or "shapes") the internet traffic of entire countries, and another memo was titled "I Hunt Sysadmins." I felt sure he could hack anyone's computer, including mine.

Good evening sir!

The only NSA workers the agency has permitted me to talk with are the ones in its public affairs office who tell me I cannot talk with anyone else. Thanks to the documents leaked by Snowden, however, I have been able to write about a few characters at the NSA.

There was, for instance, a novelist-turned-linguist who penned an ethics column for the NSA's in-house newsletter, and there was a mid-level manager who wrote an often zany advice column called "Ask Zelda!" But their classified writings, while revealing, could not tell me everything I wanted to know about the mindset of the men and women who spy on the world for the U.S. government.

I got lucky with the hacker, because he recently left the agency for the cybersecurity industry; it would be his choice to talk, not the NSA's. Fortunately, speaking out is his second nature. While working for the NSA, he had publicly written about his religious beliefs, and he was active on social media. So I replied to his greeting and we began an exchange of cordial messages. He agreed to a video chat that turned into a three-hour discussion sprawling from the ethics of surveillance to the downsides of home improvements and the difficulty of securing your laptop. "I suppose why I talk is partially a personal compulsion to not necessarily reconcile two sides or different viewpoints but to just try to be honest about the way things are," he told me. "Does that make sense?"

The hacker was at his home, wearing a dark hoodie that bore the name of one of his favorite heavy metal bands, Lamb of God. I agreed not to use his name in my story, so I'll just refer to him as the Lamb. I could see a dime-store bubble-gum machine behind him, a cat-scratching tree, and attractive wood beams in the ceiling. But his home was not a tranquil place. Workmen were doing renovations, so the noise of a buzz saw and hammering intruded, his wife called him on the phone, and I could hear the sound of barking. "Sorry, my cats are taunting my dog," he said, and later the animal in question, a black-and-white pit bull, jumped onto his lap and licked his face.

The Lamb wore a T-shirt under his hoodie and florid tattoos on his arms and smiled when I said, mostly in jest, that his unruly black beard made him look like a member of the Taliban, though without a turban. He looked very hacker, not very government.

When most of us think of hackers, we probably don't think of government hackers. It might even seem odd that hackers would want to work for the NSA -- and that the NSA would want to employ them. But the NSA employs legions of hackers, as do other agencies, including the FBI, CIA, DEA, DHS, and

Department of Defense. Additionally, there are large numbers of hackers in the corporate world, working for military contractors like Booz Allen, SAIC, and Palantir. The reason is elegantly simple: You cannot hack the world without hackers.

In popular shows and movies such as "Mr. Robot" and "The Matrix," hackers tend to be presented as unshaven geeks loosely connected to collectives like Anonymous, or to Romanian crime syndicates that steal credit cards by the millions, or they are teenagers who don't realize their online mischief will get them into a boatload of trouble when Mom finds out.

The stereotypes differ in many ways but share a trait: They are transgressive anti-authoritarians with low regard for social norms and laws. You would not expect these people to work for The Man, but they do, in droves. If you could poll every hacker in the U.S. and ask whe---ther they practice their trade in dark basements or on official payrolls, a large number would likely admit to having pension plans. Who knows, it could be the majority.

This may qualify as one of the quietest triumphs for the U.S. government since 9/11: It has co-opted the skills and ideals of a group of outsiders whose anti-establishment tilt was expressed two decades ago by Matt Damon during a famous scene in Good Will Hunting. Damon, playing a math genius being recruited by the NSA, launches into a scathing riff about the agency serving the interests of government and corporate evil rather than ordinary people. Sure, he could break a code for the NSA and reveal the location of a rebel group in North Africa or the Middle East, but the result would be a U.S. bombing attack in which "1,500 people that I never met, never had a problem with, get killed." He turns down the offer.

In recent years, two developments have helped make hacking for the government a lot more attractive than hacking for yourself. First, the Department of Justice has cracked down on freelance hacking, whether it be altruistic or malignant. If the DOJ doesn't like the way you hack, you are going to jail. Meanwhile, hackers have been warmly invited to deploy their transgressive impulses in service to the homeland, because the NSA and other federal agencies have turned themselves into licensed hives of breaking into other people's computers. For many, it's a techno sandbox of irresistible delights, according to Gabriella Coleman, a professor at McGill University who studies hackers. "The NSA is a very exciting place for hackers because you have unlimited resources, you have some of the best talent in the world, whether it's cryptographers or mathematicians or hackers," she said. "It is just too intellectually exciting not to go there."

Revealingly, one of the documents leaked by Snowden and published by The Intercept last year was a classified interview with a top NSA hacker (not the Lamb) who exulted that his job was awesome because "we do things that you can't do anywhere else in the country ... at least not legally. We are gainfully employed to hack computers owned by al-Qa'ida!" Asked about the kind of people he works with at the NSA, he replied, "Hackers, geeks, nerds ... There's an annual event for hackers in Las Vegas called DEF CON, and many of us attend. When there, we feel as though we are among our bretheren! [sic] We all have a similar mindset of wanting to tear things apart, to dig in, to see how things work."

In 2012, Gen. Keith Alexander, the NSA director at the time, even attended DEF CON wearing blue jeans and a black T-shirt that bore the logo of the Electronic Frontier Foundation, an anti-surveillance organization that is beloved by hackers and other good citizens of the world. To coincide with Alexander's visit, the NSA had created a special webpage to recruit the hackers at DEF CON. "If you have a few, shall we say, indiscretions in your past, don't be alarmed," the webpage stated. "You shouldn't automatically assume you won't be hired." Alexander's personal pitch was even more direct: "In this room right here is the talent we need."

If you are willing to become a patriot hacker, Uncle Sam wants you.

As s a teenager, the Lamb was a devout Christian who attended church two or three times a week, yet he also participated in online forums for Satanists and atheists. He wanted to learn what others believed and why they believed it, and he wanted to hear their responses to questions he raised. If his beliefs could not withstand challenges from opposing ones, they might not be worth keeping.

"As a Christian, I believe the Bible, and one of the things it says is if you seek the truth, you should find it," he told me. "If I started to come across facts that contradicted what I believed and contradicted the way that I thought about things, I had to be open to confronting them and determining how I would integrate them into my life and my thought system."

Before he became a hacker, the Lamb had the restless spirit of one. After high school, he attended a Christian university for a year but dropped out and joined the military as a linguist. He was assigned to the NSA, and although he told me his computer skills were modest at the time, he was intrigued by the mysteries inside the machines. "I started doing some basic computer training, like 'Oh, here's how computers talk to each other and network' and that sort of stuff," he said. "I enjoyed that far more than trying to maintain a language that I rarely used."

He devoured books on computers and experimented on his own time, using an application called Wireshark to see how network data was moving to and from his own computer. He picked up a bit of programming knowledge, and he asked agency veterans for tips. As he wrote in one of his memos, "If you want to learn crazy new things ... why not walk around NSA, find people in offices that do things you find interesting, and talk to them about how they do what they do."

Like Snowden, he did not need a formal education to succeed. Snowden, after all, dropped out of high school and mastered computers through self-education. As an NSA contractor, he rose to a position that gave him access to broad swaths of the agency's networks. While Snowden was a systems administrator, the Lamb became an expert in network analysis and was well-versed in the crucial trick of shaping traffic from one place to another -- for instance, sending it from an ISP in a foreign country to an NSA server.

The Lamb's work was important, but his memos are remarkably irreverent, even cocky. I've read a fair number of NSA documents, and not one contains as much hacker and internet lingo as his; he used

words like "skillz" and "internetz" and "ZOMG!" and phrases like "pwn the network" and "Dude! Map all the networks!!!" Some of what he wrote is just cheerily impudent, like the opening line of one memo: "Happy Friday my esteemed and valued intelligence Community colleagues!" Another memo began, "Welcome back, comrade!"

While poking gentle fun at the government hackers he worked with, the Lamb dismissed the amateur hackers on the outside. He identified himself and his highly trained colleagues at the NSA as a breed apart -- a superior breed, much in the way that soldiers look down on weekend paintballers. Perhaps this shouldn't be altogether surprising, because arrogance is one of the unfortunate hallmarks of the male-dominated hacker culture. At the NSA, this hubris can perhaps serve as an ethical lubricant that eases the task of hacking other people: They are not as special as you are, they do not have the magical powers you possess, they are targets first and humans second.

As the Lamb wrote in one of his memos, "When I first went to Blackhat/Defcon, it was with the wide-eyed anticipation of 'I'm going to go listen to all of the talks that I can, soak up all of the information possible, and become a supar-1337-haxxor.' What a let-down of an experience that was. You find the most interesting topics and briefings, wait in lines to get a seat, and find yourself straining your ears to listen to someone that has basically nothing new to say. Most of the talks get hyped up exponentially past any amount of substance they actually provide."

When I asked the Lamb where he was in the hierarchy of hackers at the NSA, he just smiled and said, "I got to the point where more people would ask me questions than I asked other people questions." He would not delve into the classified specifics of his job -- he despises Snowden for leaking classified information -- but I knew a lot through his memos.

Although network analysis, the Lamb's area of expertise, is interesting from a technical perspective, he was one step removed from the most challenging and menacing type of government hacking -- executing finely tuned attacks that infiltrate individual computers. Nonetheless, he offered this characterization of his NSA work: "They were just ridiculously cool projects that I'll never forget." One of the quandaries of technology is that "cool" does not necessarily mean "ethical." Surveillance tools that are regarded as breakthroughs can be used to spy on innocent people as well as terrorists. This is a key part of the debate on the NSA, the concern that its formidable powers are being used, or can be used, to undermine privacy, freedom, and democracy.

The Lamb's memos on cool ways to hunt sysadmins triggered a strong reaction when I wrote about them in 2014 with my colleague Ryan Gallagher. The memos explained how the NSA tracks down the email and Facebook accounts of systems administrators who oversee computer networks. After plundering their accounts, the NSA can impersonate the admins to get into their computer networks and pilfer the data flowing through them. As the Lamb wrote, "sys admins generally are not my end target. My end target is the extremist/terrorist or government official that happens to be using the network ... who better to target than the person that already has the 'keys to the kingdom'?"

Another of his NSA memos, "Network Shaping 101," used Yemen as a theoretical case study for secretly redirecting the entirety of a country's internet traffic to NSA servers. The presentation, consisting of a PowerPoint slideshow, was offbeat at times, with a reference to throwing confetti in the air when a hack worked and jokey lines like, "The following section could also be renamed the 'I'm pulling my hair out in the fetal position while screaming "Why didn't it work?!"' section." The Lamb also scribbled a hand-drawn diagram about network shaping that included a smiley face in the middle next to the phrase, "YEAH!!! MAKE DATA HAPPEN!" The diagram and slideshow were both classified as top secret.

His memos are boastful, even cackling. At the end of one of the sysadmin memos, the Lamb wrote, "Current mood: scheming," and at the end of another, "Current mood: devious." He also listed "juche-licious" as one of his moods, ironically referring to the official ideology of North Korea. Another memo he wrote, "Tracking Targets Through Proxies & Anonymizers," impishly noted that the use of identity-obscuring tools like Tor "generally makes for sad analysts" in the intelligence community; this was followed by a sad face emoji. The tone of his classified writing was consistent with some of his social media posts -- the Lamb's attitude, in public as well as in private, was often outspoken and brash.

What if the shoe was on the other foot, however? When I wrote about the sysadmin memos in 2014, I wondered how their author would feel if someone used the same devious rationale to hack his computer and his life. Nearly two years later, I had the chance to find out.

"If I turn the tables on you," I asked the Lamb, "and say, OK, you're a target for all kinds of people for all kinds of reasons. How do you feel about being a target and that kind of justification being used to justify getting all of your credentials and the keys to your kingdom?"

The Lamb smiled. "There is no real safe, sacred ground on the internet," he replied. "Whatever you do on the internet is an attack surface of some sort and is just something that you live with. Any time that I do something on the internet, yeah, that is on the back of my mind. Anyone from a script kiddie to some random hacker to some other foreign intelligence service, each with their different capabilities -- what could they be doing to me?"

He seemed to be putting the blame for NSA attacks on the victims -- if they were too dimwitted to protect themselves from hunters like him, it was their fault. "People don't want to think about being targets on the internet, in spite of the fact that at this point in the game, everybody is," he added. "Every country spies."

He was dead serious, no smiles any longer. "As much as we'd like to say we will all beat our swords into plowshares and become a peaceful people, it's not going to happen," he continued. "Intelligence agencies around the world are being asked questions by their governments, and government officials don't want to hear, 'That's hard to solve.' They just say, 'Can you solve this and can you get me the intel I'm asking for?' Which is nation agnostic, whether that's the NSA, the FSB, the PLA or whoever."

The Lamb's political ideology evoked the cold-blooded realpolitik of Henry Kissinger. There is the idyllic digital world we would like to live in, there is the dog-eat-dog digital world we actually live in -- and the Lamb, as I understood it, was intensely focused on winning in the latter.

"You know, the situation is what it is," he said. "There are protocols that were designed years ago before anybody had any care about security, because when they were developed, nobody was foreseeing that they would be taken advantage of. ... A lot of people on the internet seem to approach the problem [with the attitude of] 'I'm just going to walk naked outside of my house and hope that nobody looks at me.' From a security perspective, is that a good way to go about thinking? No, horrible ... There are good ways to be more secure on the internet. But do most people use Tor? No. Do most people use Signal? No. Do most people use insecure things that most people can hack? Yes. Is that a bash against the intelligence community that people use stuff that's easily exploitable? That's a hard argument for me to make."

But it wasn't a hard argument for me to make, so I tried. Back in the 1990s, in the early days of the web, the uses and hopes for the internet were thought to be joyous and non-commercial. The web would let us talk to one another and would decentralize power and revolutionize the world in good ways. Those were the years when the Lamb spent hours and hours in chatrooms with Satanists and atheists -- just the sort of connect-us-to- each-other activity that made everyone so excited about the future. At the time, few people thought the internet would become, as Bruce Schneier describes it, a surveillance platform. So I asked whether the Lamb felt conflicted, as Snowden did, working for an organization that turned the web further and further away from its original potential as a global platform for speaking and thinking freely.

He responded by noting that he is, by nature, a defiant type and attracted to hard problems. That's how, without a lot of formal instruction, he became an NSA hacker -- he was curious about how computers worked and he wanted to figure them out. "Technically challenging things are just inherently interesting to me," he said. "If you tell me, 'This can't be done,' I'm going to try and find a way to do it."

I mentioned that lots of people, including Snowden, are now working on the problem of how to make the internet more secure, yet he seemed to do the opposite at the NSA by trying to find ways to track and identify people who use Tor and other anonymizers. Would he consider working on the other side of things? He wouldn't rule it out, he said, but dismally suggested the game was over as far as having a liberating and safe internet, because our laptops and smartphones will betray us no matter what we do with them.

"There's the old adage that the only secure computer is one that is turned off, buried in a box ten feet underground, and never turned on," he said. "From a user perspective, someone trying to find holes by day and then just live on the internet by night, there's the expectation [that] if somebody wants to have access to your computer bad enough, they're going to get it. Whether that's an intelligence agency or a cybercrimes syndicate, whoever that is, it's probably going to happen."

The Lamb was comfortable with the side he joined in the surveillance wars, and this sets him apart from the most common stereotypes of the men and women who devote their lives to spying on others.

Spies who do nothing but eavesdrop, slipping into computers and conversations without a trace, have a reputation in popular culture of being troubled in ways that conventional spies are not. Think of Gene Hackman in The Conversation, or Ulrich Mühe in The Lives of Others -- these surveillers are haunted, as it seems they should be. Conventional spies are seen as journeying into hostile lands and committing heroic or devious acts; they are men and women of action, not thought. But the people who watch, listen, or hack are not as distracted by danger or adrenaline. They mostly labor in tranquility, in temperature-controlled offices without windows, risking bodily harm no worse than carpal tunnel syndrome, and they have an abundance of time to think about the lurking that is their occupation and the people on whom they practice it.

I have a bias against the watchers, I suppose. I have been concerned about the bureaucracies of surveillance since the 1980s, when I was a student in the Soviet Union and felt like hunted prey. The telephone in the dreary lobby of my dormitory on the banks of the Neva River in Leningrad (now St. Petersburg) was assumed to be bugged, and if the KGB's devices weren't working, the dezhurnaya who sat nearby was sure to be listening. This was my anti-surveillance Rosebud, I guess. When I visited Russian friends, I stayed silent as I walked in their ill-lit stairwells, so that the accent of my Russian would not give away the fact a foreigner was visiting them. The walls had ears. This was one of the great contrasts between the Soviet Union and America, where I could speak to my friends without worrying about the government listening.

The Soviet Union is long gone, but in 2016 we live under the specter of far more surveillance than anything the KGB could have dreamed of with its rudimentary bugs and fearful informers. Not just government surveillance -- law enforcement can easily obtain our phone and internet records with a warrant from the nearly always compliant courts -- but corporate surveillance, too. It's not just Google and Facebook that might know more details about our lives and friends than the KGB could have imagined in its most feverish dreams of information dominance, but even Zipcar and Amazon.

There are precautions one can take, and I did that with the Lamb. When we had our video chat, I used a computer that had been wiped clean of everything except its operating system and essential applications. Afterward, it was wiped clean again. My concern was that the Lamb might use the session to obtain data from or about the computer I was using; there are a lot of things he might have tried, if he was in a scheming mood. At the end of our three hours together, I mentioned to him that I had taken these precautions--and he approved.

"That's fair," he said. "I'm glad you have that appreciation. ... From a perspective of a journalist who has access to classified information, it would be remiss to think you're not a target of foreign intelligence services."

He was telling me the U.S. government should be the least of my worries. He was trying to help me.

Reuters
Chinese economic cyber-espionage is diminishing, says U.S. official
Tuesday, 28 June 2016
Byline: Staff report

Washington - U.S. Assistant Attorney General John Carlin said on Tuesday that Chinese hacking activity appears to have declined since the Chinese government vowed last September to stop supporting the hacking of U.S. trade secrets.
The assertion supports findings released earlier this month from cyber security firm FireEye that breaches attributed to China- based groups had plunged by 90 percent in the past two years.

"Generally, people have seen a change in activity," Carlin said at the Center for Strategic and International Studies think tank in Washington.

But "there is debate about how long lasting" the apparent reduction in activity will be, Carlin said, adding that the private sector and U.S. intelligence officers were likely better positioned to assess hacking trends.

Carlin said that agreements on hacking activity with China and among the Group of 20 nations, both announced last year, were important to developing uniform international cyber norms.

Certain countries, such as North Korea, continue to be a "difficult actor" on cyber issues, he said.

Le Monde
Poutine renforce son arsenal antiterroriste
Wednesday, 29 June 2016
Byline: Isabelle Mandraud

Moscou - Les opérateurs Internet et de téléphonie devront conserver tous les échanges pendant six mois
A une cadence effrénée avant l'interruption de l'été, les députés de la Douma, la chambre basse du Parlement russe, ont adopté deux lois antiterroristes controversées que le Conseil de la fédération, l'équivalent du Sénat, s'apprête à son tour à entériner mercredi 29 juin. " Notre pays et notre société en ont besoin " , a déjà prévenu sa présidente, Valentina Matvienko. Présenté comme une réponse à l'attentat d'octobre 2015 contre un charter russe au-dessus du Sinaï, qui avait entraîné la mort de 224 passagers et membres d'équipage, ce Patriot Act version russe soulève l'inquiétude des organisations des droits de l'homme.

Réfugié en Russie depuis deux ans, le lanceur d'alerte Edward Snowden a également dénoncé sur Twitter un arsenal " Big Brother " , " qui constitue une violation inapplicable et injustifiable des droits " . " La surveillance de masse ne fonctionne pas , insiste l'ex-consultant qui a fui les Etats-Unis après avoir révélé l'ampleur des opérations d'espionnage menées par les services de renseignement américains. Ce texte va coûter de l'argent et de la liberté à chaque Russe sans améliorer la sécurité. "

Le paquet de mesures adoptées vise notamment à renforcer la surveillance des réseaux de communication. Les fournisseurs de service téléphonique et d'accès Internet seront dans l'obligation de conserver sur leurs serveurs les métadonnées - les caractéristiques d'un échange ou d'une connexion, telles que l'heure ou la durée - pendant trois ans, ainsi que tous les messages, appels et communications des utilisateurs pendant six mois. Sur demande des services russes, ils devront également fournir l'accès aux messageries cryptées.

Les lois Iarovaia - du nom de la députée Irina Iarovaia, membre du parti au pouvoir Russie unie, qui a porté ces textes - alourdissent considérablement la législation existante sur bien d'autres points. L'âge de la responsabilité pénale est abaissé à 14 ans. La " non- dénonciation " de crimes - une disposition de l'époque soviétique remise au goût du jour - pourra être punie d'un an de prison. Des peines jusqu'à sept ans de détention sont également prévues pour " justification publique du terrorisme " , y compris sur Internet, mais aussi pour " rébellion armée " ou " actes extrémistes " .

Or, sous cette dernière qualification assez large, plusieurs internautes ont récemment été condamnés pour avoir simplement partagé des publications sur les réseaux sociaux. Encourager par ce même biais à prendre part à " des troubles de masse " pourra aussi valoir cinq à dix ans de prison. Enfin, la loi bannit " le prosélytisme, le prêche et la prière en dehors des institutions religieuses reconnues " .

" Sérieux coup aux libertés "In extremis, la dernière version adoptée à la Douma a exclu la déchéance de la nationalité pour les binationaux travaillant pour des organisations internationales, ou l'interdiction de quitter le territoire pour des auteurs de crimes. " Le retrait des mesures les plus scandaleuses a peut-être été conçu pour que le public pousse un soupir de soulagement, mais, même écrémée, la loi Iarovaia porte un sérieux coup à la liberté d'expression et aux autres libertés fondamentales des Russes " , s'alarme Tania Lokchina, la représentante de l'ONG Human Rights Watch à Moscou.

A l'unisson, les opérateurs Internet et de téléphonie fustigent des mesures de surveillance qu'ils jugent inapplicables et dont le coût les amènerait " au seuil de la survie " . " Si nous devions prendre en compte le stockage des données, nous ne serions plus en mesure de payer des impôts sur bénéfices pendant au moins cent ans " , affirme Dmitri Solodovnikov, un représentant de MTS, le plus important opérateur de téléphonie mobile en Russie, cité par le quotidien Kommersant . Les nouvelles lois antiterroristes, que Vladimir Poutine doit parapher pour leur mise en application, sont les dernières prévues avant les élections législatives organisées le 18 septembre.

1. Yonhap English News

US, Korea hold cybersecurity cooperation talks

Saturday, 02 July 2016

Seoul - The United States and Korea held cybersecurity talks to boost cooperation in a wide range of areas, including tackling cyber hacking and other crimes, the State Department said.

Christopher Painter, the department's coordinator for cyber issues, led the U.S. delegation in the fourth U.S.-Korea Bilateral Cyber Consultations. His team also included officials from the National Security Council, and the departments of justice, defense and homeland security, the department said in a statement.

Led by International Security Affairs Ambassador Shin Maeng-ho, Korea's interagency team included officials from the National Police Agency, the Justice Ministry and the Korea Internet and Security Agency, the department said.

The talks "affirmed the benefits of a whole-of-government approach" between the two countries on cyber policy and reinforced cooperation "on a wide range of cyber issues including cooperation on cybersecurity of critical infrastructure, capacity building, information sharing, research and development, military-to-military cyber cooperation, cybercrime, international security issues in cyberspace," it said.

The meeting also reaffirmed shared principles that support an open, interoperable, secure, and reliable cyberspace, the department said.

2. New York Times

Loretta Lynch to Accept F.B.I. Recommendations in Clinton Email Inquiry

Saturday, 02 July 2016

Byline: Mark Landler

Washington - General Loretta E. Lynch, conceding that her airport meeting with former President Bill Clinton this week had cast a shadow over the federal investigation of Hillary Clinton's personal email account, said Friday that she would accept whatever recommendations career prosecutors and the F.B.I. director made about whether to bring charges in the case.

Ms. Lynch said she had decided this spring to defer to the recommendations of her staff and the F.B.I. because her status as a political appointee sitting in judgment on a politically charged case would raise questions of a conflict of interest. But the meeting with Mr. Clinton, she acknowledged, had deepened those questions, and she said she now felt compelled to explain publicly her reasoning to try to put the concerns to rest.

"People have a whole host of reasons to have questions about how we in government do our business," Ms. Lynch said at an Aspen Institute conference in Colorado. "My meeting on the plane with former President Clinton could give them another reason to have questions and concerns."

Though she insisted the 30-minute conversation was a purely social encounter, Ms. Lynch said, "I certainly wouldn't do it again."

The attorney general's response did little to quell a political tempest in Washington, with some Republicans calling for her to recuse herself from the case -- a step she said she was not going to take. Donald J. Trump, the presumptive Republican nominee, said the meeting had "opened up a Pandora's box." He cast doubt on whether it was entirely social, citing it as an example of how "the special interests are controlling your government."

For Democrats, already anxious about the political impact of the email investigation, the incident revived fears that Mr. Clinton could become a rogue actor in a campaign that has so far operated more smoothly than Mrs. Clinton's presidential bid in 2008.

Mr. Clinton, who was on a seven-state fund-raising swing for his wife, strode across the tarmac at the airport in Phoenix to greet Ms. Lynch after her plane landed there on Monday night. The attorney general joked that she should have acted more swiftly to keep him from boarding. Asked by a journalist to name one thing she wished her predecessor, Eric H. Holder Jr., had told her about her job, she replied, "Where the lock on the plane door was."

Still, Ms. Lynch said the episode was personally distressing because it stained the reputation of the Justice Department. "The fact that the meeting that I had is now casting a shadow over how people are going to view that work is something that I take seriously, and deeply and painfully," she said.

Even Ms. Lynch's explanation of how she planned to distance herself from the case -- without recusing herself -- required further clarification. "The case will be resolved by the team that's been working on it from the beginning," she said in Aspen. But a Justice Department spokeswoman, Melanie Newman, noted afterward that even if Ms. Lynch accepted the recommendation of her staff, she would be the one making the decision.

"She's the head of the department," Ms. Newman said, "and with that comes ultimate responsibility for any decision."

The White House declined to comment on Ms. Lynch's decision. President Obama "believes that this matter should be handled without regard to politics," the press secretary, Josh Earnest, said.

The F.B.I. is investigating whether Mrs. Clinton, her aides or anyone else broke the law by setting up a private email server for her to use as secretary of state. Internal investigators have concluded that the server was used to send classified information. For the Justice Department, the central question is whether the conduct met the legal standard for the crime of mishandling classified information.

Ms. Lynch, whom Mr. Clinton appointed to be a United States attorney in 1999, said that the meeting with the former president was unplanned and largely social, and did not touch on the email investigation.

"He said hello and we basically said hello, and congratulated him on his grandchildren, as people do," said Ms. Lynch, who was traveling with her husband. "That led to a conversation about those grandchildren."

For Mr. Clinton, who travels frequently by private jet, such airport socializing is common. Last month, he ran into Senator Orrin G. Hatch, the Utah Republican, after speaking at the funeral of Muhammad Ali in Louisville, Ky. The two chatted before their planes took off. He has also greeted Representative Paul D. Ryan, the House speaker, and Arnold Schwarzenegger, the former Republican governor of California, on the tarmac. And in Mobile, Ala., he chatted with Senator Ted Cruz, the Texas Republican who has called for Mrs. Clinton's imprisonment.

This meeting, however, created a particularly awkward situation for Ms. Lynch, a veteran prosecutor who was nominated from outside Washington's political circles. During her confirmation, her allies sought to contrast her with her predecessor, Mr. Holder, an outspoken liberal voice who clashed frequently with Republicans who accused him of politicizing the office.

Ms. Lynch's reassurance that she will not overrule her investigators is significant. When the F.B.I. sought to bring felony charges against David H. Petraeus, the former C.I.A. director, for mishandling classified information and lying about it, Mr. Holder stepped in and reduced the charge to a misdemeanor. That decision opened a deep -- and public -- rift.

Two other political appointees will review the findings of the email investigation before a final decision is made: John P. Carlin, the assistant attorney general for national security, and Deputy Attorney General Sally Yates. But both have also pledged to follow the recommendations of the career prosecutors and the F.B.I., Ms. Newman said.

The F.B.I. is expected to make a recommendation to the Justice Department in the coming weeks, though agents have yet to interview Mrs. Clinton. While some legal experts said they believed that criminal indictments in the case were unlikely, the investigation continues to cast a shadow over Mrs. Clinton's presidential campaign.

Beyond the day-to-day workings of the Justice Department, there is precedent for relying on career officials to make politically charged decisions. When the Justice Department was considering whether to recommend sanctions against former Bush administration lawyers who approved waterboarding, Mr.

Holder relied on his most senior career prosecutor to make the decision. No sanctions were recommended.

For Mrs. Clinton's presidential campaign, the incident in Phoenix resurrected questions about how the campaign would rein in her irrepressible husband.

With approval ratings among Democrats of over 60 percent, Mr. Clinton is one of his wife's most potent surrogates. He has traversed the country with a breakneck schedule, campaigning and raising money for Mrs. Clinton, traveling with a bare-bones staff and security detail.

Mr. Clinton and his chief of staff, Tina Flournoy, are in frequent contact with John D. Podesta, chairman of the Clinton campaign, and Robby Mook, the campaign manager. He often listens in on campaign conference calls from the family's home in Chappaqua, N.Y. But his unpredictable and sociable nature can also cause problems for his wife's candidacy.

David Axelrod, the former senior adviser to President Obama, said on Twitter that he took Mr. Clinton and Ms. Lynch "at their word" that they had not discussed the investigation, but added that it was "foolish to create such optics."

3. Politico.com

Senate says goodbye to the BlackBerry, at last

Saturday, 02 July 2016

Byline: Heather Caygle

Washington - The Senate is breaking up with BlackBerry, and it's for good this time.

The prehistoric smartphone, once a mainstay on Capitol Hill, will no longer be handed out to Senate staffers after the current supply runs out, according to a notice sent out Wednesday. Staffers were put on alert that since BlackBerry has decided to discontinue the device and there is a limited stock on the Hill, the chamber has no way to replenish the phones once they're gone.

"Once we have exhausted our current in-house stock, new device procurements will be limited, while supplies last, to warranty exchanges only," read a Sergeant at Arms note, first reported by Jim Swift.

While most Hill aides have long moved on to iPhones or Androids, there's a small, loyal band of staffers that just can't quit the dinosaur device.

Some Millennial Hill staffers may scoff at the sentimental attachment, but BlackBerry has proven its worth over the years. When an earthquake shook D.C. in 2011, BlackBerry messaging was the only service working while other carriers were overloaded and texts and calls wouldn't go through.

Currently, the Senate has a little more than 600 various BlackBerry models stockpiled, according to the Sergeant at Arms, and device support for current phones is expected to continue for the "foreseeable future."

4. Washington Post

Clinton, FBI meet in probe of email

Sunday, 03 July 2016

Byline: Matt Zapotosky, Anne Gearan

Washington - FBI agents interviewed Hillary Clinton for 3 1/2 hours Saturday morning - a signal that the investigation into her use of a private email account while she was secretary of state is drawing to a close.

Clinton campaign spokesman Nick Merrill said in a statement Saturday that Clinton "gave a voluntary interview this morning about her email arrangements while she was Secretary," and added, "She is pleased to have had the opportunity to assist the Department of Justice in bringing this review to a conclusion."

Asked if the interview, which took place at FBI headquarters, was businesslike and civil, Clinton told MSNBC that it was "both."

"It was something I had offered to do since last August," she said, according to a transcript provided by the network. "I've been eager to do it, and I was pleased to have the opportunity to assist the department in bringing its review to a conclusion."

As she has in the past, Clinton asserted that she "never received nor sent any material that was marked classified," although she said that some might have been retroactively branded classified during the process to prepare it for public release. She said she had "no knowledge" of the investigators' timeline.

The investigation is not over: Agents and prosecutors will now have to compare what the presumptive Democratic presidential nominee said Saturday to other evidence they have gathered, including from interviews with Clinton's aides. They will also have to analyze how the facts of the case apply to various laws that might have been violated.

But officials familiar with the probe and legal analysts have said a meeting with Clinton would be reserved for the end of the investigation.

"That's certainly a signal that they're wrapping things up," said Justin Shur, a former deputy chief of the Justice Department's public integrity section who is now in private practice at the MoloLamken firm.

A Justice Department spokesman declined to comment on the Clinton interview.

The past week has been tumultuous for Clinton and the government's investigation into whether her email system might have compromised classified information. On Monday, former president Bill Clinton had an impromptu meeting with U.S. Attorney General Loretta E. Lynch aboard Lynch's plane at an airport in Phoenix. Lynch asserted they did not discuss any pending investigations, but the conversation sparked an uproar - with some Republicans and Clinton rivals calling for a third party to be appointed to handle the case.

Referring to that meeting, Hillary Clinton told MSNBC that "hindsight is 20/20" and said her husband, like the attorney general, would probably not do it again.

On Friday, Lynch announced that she would accept recommendations from career prosecutors and FBI agents leading the probe - a decision that she said had been made before her meeting with Bill Clinton, but one that was surely meant to quiet criticism about the independence of the probe. While Lynch did not formally recuse herself from the investigation involving Hillary Clinton's email - saying that "would mean I wouldn't even be briefed on what the findings were" - she seemed to promise she would not veto whatever decision came from federal prosecutors handling the case.

It is not clear who precisely will be the ultimate decision-maker, if Lynch will serve as more of a rubber stamp. The attorney general said FBI Director James B. Comey would be among those involved.

The investigation is focused on whether classified information was mishandled because Clinton used a private email account when she was secretary of state. The State Department's inspector general has already issued a report highly critical of Clinton's email practices, asserting that she failed to seek legal approval to use a private server and that staffers would not have assented if they were asked. The inspector general also found that Clinton's email setup was "not an appropriate method" for preserving public records.

A Washington Post analysis of Clinton's publicly released correspondence found that Clinton wrote 104 emails that she sent using her private server while secretary of state that the government has since said contained classified information. But the review also found that using non- secure email systems to send sensitive information was widespread at the department and elsewhere in government and that Clinton's publicly released correspondence included classified emails written by about 300 other people inside and outside the government.

People familiar with the case have said previously that charges against Clinton seemed unlikely and that there was a particular void of evidence showing she intended to mishandle classified information, although they asserted investigators were still probing the matter aggressively. The interview with Clinton was always seen as critical. If the former secretary was untruthful with investigators, she could be charged with making false statements. That charge was contemplated in the case against retired Army general and former CIA director David H. Petraeus, although he ultimately pleaded guilty to a misdemeanor charge of mishandling classified information.

With the Republican and Democratic conventions looming later this month, timing has also become a complicating factor. Justice Department guidelines specifically warn prosecutors against selecting the timing of investigative steps for the purpose of affecting an election or helping a particular candidate or party.

5. Washington Post

Satellite imagery suggests China is secretly punishing North Korea

Saturday, 02 July 2016

Byline: Josh Rogin

Comment: Following North Korea's latest nuclear test, in January, trade over the China-North Korea border dropped dramatically, according to newly released satellite imagery. The revelation has led experts to conclude that Beijing has been quietly punishing Kim by cutting off the flow of funds to his regime.

There's no question that the China-North Korea relationship has been strained since Kim assumed power in 2011. Against Beijing's wishes, the young leader has revved up North Korea's pace of missile tests and detonated two nuclear devices, one in 2013 and then again this January. In 2013, Kim executed his uncle Jang Song Thaek, who had been China's main contact in Pyongyang.

After the latest nuclear explosion, which Pyongyang claimed was a hydrogen bomb, Secretary of State John F. Kerry publicly called on China to end "business as usual" with North Korea. Publicly, Beijing rejected being told by the United States how to handle its client state. Behind the scenes, it appears Beijing was doing just that.

"It is apparent that shortly after North Korea did the fourth nuclear test in January, China took unilateral measures to drastically curtail trade interaction along their border," said Victor Cha, director for Asian affairs at the National Security Council during the George W. Bush administration.

Cha, now at the Center for Strategic and International Studies (CSIS), led a team of researchers that procured and analyzed the new satellite imagery as part of their project Beyond Parallel, a website and database dedicated to demystifying what's going on inside the world's most secretive state. The project launched Thursday.

Cha's conclusion, that Beijing decided to punish North Korea after the nuclear test but didn't disclose that to the world, is backed up by anecdotal reports of Chinese officials telling Western interlocutors that President Xi Jinping had decided to "take action" against the Kim regime, behind the scenes, out of anger over the nuke test.

"It shows that China pursues things in their own way when it comes to North Korea, not because the U.S. or the U.N. tells them to," said Cha. "The good news is that they are squeezing them more than we were led to expect."

CSIS worked with imagery analysts at the commercial satellite firm DigitalGlobe to collect and examine satellite photos of several key trade-related areas on both sides of the China-North Korea border, including the Sinuiju railroad station and customs area on the North Korean side, the Dandong railroad station and customs area on the Chinese side, and the Sino-Korean Friendship Bridge that links the two countries.

They compared activity at the sites year over year, first by examining imagery from January and March of 2015 and then comparing that with imagery collected this February, just after the latest nuclear test. The images showed a "substantive reduction of economic activity on the Sino- North Korean border" as evidenced by a huge drop in the number of rail cars at the stations, trucks in customs areas, trucks on the bridge and undocked boats in the Yalu River.

At the Sinuiju rail station, most of the train cars appeared to be in storage early this year, with no engines attached to the freight cars. In the Sinuiju customs area, there were 111 trucks shown in the satellite image from January 2015, but in the February 2016 image, there were only five. On the Chinese side, there were 32 trucks spotted in the Dandong customs area in March 2015, but by this February there were only six.

Official trade data regarding North Korea is notoriously unreliable, and Cha said comprehensive data on economic activity over the China-North Korea border does not really exist. But his team has been briefing U.S. and South Korean government agencies on what they found, and he said both governments have shown interest in pursuing the research.

In March, China signed on to a new United Nations Security Council resolution imposing fresh sanctions on North Korea in response to the January nuclear test, showing that Beijing was in fact upset with Kim's actions. But the new data may show that Xi was much more upset than he let on and more than he wanted the rest of the world to know.

"The Chinese don't feel like they need to get credit for punishing North Korea and they don't want to be seen as [if] they are being pressured by the U.S. to do it," said Cha.

The question going forward is whether Chinese economic pressure on North Korea, which will surely hit at Kim's coffers, will compel the young ruler to think twice before his next dangerous provocation.

6. New York Times

F.B.I. Interviews Hillary Clinton Over Private Email Server

Sunday, 03 July 2016

Byline: Amy Chozick

Washington - The F.B.I. interviewed Hillary Clinton on Saturday morning for its investigation into whether she or her aides broke the law by corresponding through a private email server set up for her use as secretary of state, a controversy that has dogged her presidential campaign and provided fodder to her political rivals.

The voluntary interview, which took place over three and a half hours at F.B.I. headquarters in Washington, largely focused on the Justice Department's central question: Did the actions of Mrs. Clinton or her staff rise to the level of criminal mishandling of classified information?

It could take weeks or longer to reach a decision, but news that Mrs. Clinton, the Democratic Party's presumptive nominee, had been questioned in the J. Edgar Hoover Building three weeks before her party's convention quickly reverberated.

The Republican National Committee called the step "unprecedented," while Mrs. Clinton's expected opponent in the race for the White House, Donald J. Trump, wasted little time before weighing in.

"It is impossible for the FBI not to recommend criminal charges against Hillary Clinton," Mr. Trump wrote on Twitter on Saturday. "What she did was wrong!"

The interview had been weeks in the making as law enforcement officials and Mrs. Clinton's team coordinated schedules. Democrats also hoped that holding the interview on a holiday weekend might soften the anticipated storm. Shortly after the meeting, two black S.U.V.s were seen returning to Mrs. Clinton's house in the capital, but Mrs. Clinton herself stayed out of sight.

In a telephone interview with Chuck Todd on MSNBC after her meeting, Mrs. Clinton said: "I've been eager to do it, and I was pleased to have the opportunity to assist the department in bringing its review to a conclusion."

Accompanying Mrs. Clinton into the meeting were her lawyer David E. Kendall; Cheryl D. Mills and Heather Samuelson, longtime aides who are also lawyers; and two lawyers from Mr. Kendall's firm, Williams & Connolly, Katherine Turner and Amy Saharia.

Eight officials from the F.B.I. and the Department of Justice conducted the interview, according to a person who was familiar with the substance of the session but declined to be named because the meeting was private. This person characterized the meeting as "civil" and "businesslike."

Neither the campaign nor the F.B.I. would elaborate.

Although the interview on Saturday was an important step toward closure on the email issue, technical analysis of the material remains to be done and could stretch on for an indeterminate period.

The F.B.I. regularly interviews key figures before concluding an investigation, and such meetings are not an indication that it thinks the person broke the law.

While defense lawyers often advise clients against such interviews, Mrs. Clinton's campaign has been eager for her to cooperate, lest she give her opponents additional ammunition.

On Saturday, in a statement after the meeting, the Republican National Committee said that Mrs. Clinton "has just taken the unprecedented step of becoming the first major party presidential candidate to be interviewed by the F.B.I. as part of a criminal investigation surrounding her reckless conduct."

Mrs. Clinton has struggled to get beyond the issue, which came to light last year during a Republican-led congressional investigation into the aftermath of the Sept. 11, 2012, terrorist attack in Benghazi, Libya. More than 30,000 emails have since been made public.

After spending much of last summer insisting she did not need to apologize for keeping a private server in her home in Chappaqua, N.Y., because the practice was "allowed," Mrs. Clinton now frequently apologizes for the practice, saying it had been a "mistake."

The campaign has prioritized assisting the F.B.I., but it declined to cooperate with a State Department inspector general's audit of Mrs. Clinton's email practices.

Those findings, delivered to members of Congress in May, undermined some of Mrs. Clinton's initial statements defending her use of the server.

The report said there was "no evidence" that she had requested or received approval for the server, despite having "an obligation to discuss using her personal email account to conduct official business."

Federal law deems it a crime to "knowingly" mishandle classified information outside secure government channels or to permit the practice through "gross negligence."

None of the emails on Mrs. Clinton's private server were marked classified at the time they were sent or received, but the Central Intelligence Agency later determined that some contained material that would be considered "top secret."

Asked Saturday on MSNBC whether she had broken the law, Mrs. Clinton repeated her defense: "I never received nor sent any material that was marked classified."

There has been no indication that any sensitive information was compromised by Mrs. Clinton's use of a private server. But it has fed a perception that she was trying to hide information, and it has chipped away at data gauging Mrs. Clinton's trustworthiness. A Quinnipiac University poll released on Wednesday found that voters deemed Mr. Trump more honest and trustworthy than Mrs. Clinton, 45 percent to 37 percent.

"I have said that I'm going to continue to put forth my record, what I have stood for, do everything I can to earn the trust of the voters of our country," she told MSNBC when asked about being seen as less

trustworthy than Mr. Trump. "I know that's something that I'm going to keep working on, and I think that's, you know, a clear priority for me."

Mrs. Clinton's interview with the F.B.I. came amid controversy over a brief, unplanned meeting between her husband, former President Bill Clinton, and Attorney General Loretta E. Lynch, while both were at the Phoenix airport at the same time last week.

To avoid any appearance of political meddling, Ms. Lynch said on Friday that she would accept the recommendations of career prosecutors and the F.B.I. director on whether to bring charges in the matter. She said she had made that decision several months ago, before the criticism surrounding her meeting with Mr. Clinton.

She described the meeting as a casual conversation that did not touch on the investigation. But it added to Clinton campaign staff members' headaches over the email inquiry, which they had hoped to put behind them before the Democratic convention this month.

"I certainly wouldn't do it again," Ms. Lynch said of the meeting with the ex-president.

Find out what you need to know about the 2016 presidential race today, and get politics news updates via Facebook, Twitter and the First Draft newsletter.

Emmarie Huetteman contributed reporting.

7. Toronto Star

Data encryption hampering police work

Saturday, 02 July 2016

Byline: Alex Boutilier

Toronto - The growing popularity of programs that protect online privacy is creating a barrier for police and security agencies' ability to intercept and use data, documents obtained by the Star suggest.

Officials warned Public Safety Minister Ralph Goodale in November that encryption - the ability to mask communications so only the intended recipients can make sense of the message - is hindering their ability to use online communications in investigations.

"Canadians are increasingly using mobile phone networks, the Internet and other electronic means to communicate and execute transactions with each other," read the documents, heavily censored and stamped "secret."

"This has led to a significant gap between the technologies available for criminal exploitation and our means to enforce Canada's laws and keep Canadians safe."

Once a fringe set of complicated tools, encryption technology has become more and more mainstream, particularly after the disclosures of NSA whistleblower Edward Snowden. Journalists use encrypted emails to protect sources, businesses use encryption to protect their customers' transactions, and governments use encryption to protect sensitive information.

Because a number of companies have moved to encryption by default, plenty of Canadians are using encrypted messaging without even knowing it. If you've sent a text on an iPhone, you've used encryption.

Despite perfectly legal and appropriate uses, however, law enforcement has generally focused the encryption debate on the perceived advantages the technology gives to criminals to plot or cover their tracks.

The Star requested an interview with Goodale to discuss these issues, but the minister was unavailable over the past two weeks. His office noted that the minister recently addressed the encryption debate in a speech at the University of Regina.

"We need a thoughtful discussion about the legal framework that applies to new technologies. On the issue of encryption, for example, is absolute privacy the only 'public good' that needs to be safeguarded, or is there a point at which criminal or terrorist investigations should be properly and lawfully assisted?" the minister's prepared remarks read.

"And if so, where?"

Officials also flagged a number of other issues to Goodale in the documents, including data retention. Canada does not have an overarching law that requires companies to retain data for a certain period, meaning evidence sought by police could already be gone by the time they get around to asking for it.

The fact that many companies keep their data on foreign servers presents jurisdictional challenges. And a recent Supreme Court decision requiring police to obtain a warrant for users' "basic subscriber information" - things like address, Internet Protocol address, or phone numbers - have led to police complaints about increased paperwork.

"The issues outlined above are multi-faceted and inherently complex," the documents note.

"While it is possible to consider each issue separately, any solution would need to look to all issues collectively . . . To date, some work has been done to develop and advance solutions to address the issues highlighted above, however certain solutions are much more advanced than others."

Christopher Parsons, a researcher with Citizen Lab at the University of Toronto, suggested that there's little the government can do to prevent encryption in an age where every iPhone or WhatsApp message provides a high level of security.

"I think that really where the government has to explain things is, (for one) how could it possibly compel third parties who operate outside of the country and have invested so much on privacy and security, what are they going to do? I guess they can try to block Apple and iMessage, but that's not going to work," Parsons said in an interview Friday.

"And, moreover, people are gaining an appreciation slowly what encryption means. So it means that if you're using (messaging client) WhatsApp, it's actually pretty secure now to send your credit card information . . . You can send a password securely. These aren't bad things."

Parsons also questioned framing the debate around criminals and terrorists, rather than ordinary folks trying to protect their privacy.

"The majority of communications that are conducted using encryption are going to be fully lawful. So that means that there's an immediate proportionality issue," Parsons said.

"When we start framing things as we need access to the content to catch the bad guys, it really depends on what we're trying to do . . . I'm inherently suspicious."

8. Globe and Mail

Maximum-security terrorism inmate looks for 'Future Miss' on the Web

Saturday, 02 July 2016

Byline: Colin Freeze

Ottawa - In 2004, an Ottawa man helped to build a bomb that was being assembled in hopes of blowing up a packed nightclub in Britain.

When he was caught by the Mounties on the cusp of his 25th birthday, he became notorious as the first al-Qaeda-inspired extremist convicted in Canada.

Momin Khawaja's crime had once been unheard of in Canada.

Now, terrorism is a charge laid relatively routinely. At 37 years old, he is a prisoner of Millhaven Institution, kept in its maximumsecurity wing and he has spent years secluded from the wider world.

But now Mr. Khawaja is writing that he wants to become engaged. "My Future Miss: ... I'm interested in finding a girl I may marry," he has posted on an Internet site. He adds that "I have a life sentence, but I won't be in jail forever."

The personal ad has been posted on Canadian Inmates Connect.com, a site that emerged as controversial a few years ago after sex killer Luka Magnotta used it to look for prospective partners.

Mr. Khawaja may be seeking a love match, but he is glossing over some details about his own past.

"I've never killed an innocent human being or harmed women and children in any way," he writes. While he admits that he is doing time for terrorism, he says he had his reasons. "My offences stem from moral and financial support of the anti- Western occupation insurgency in places such as Iraq and Afghanistan."

Contacted by telephone, Mr. Khawaja told The Globe and Mail that he had an intermediary post a profile he put on the Internet last summer. He has had a pen pal or two since, but no serious romantic prospects have emerged.

But he is undaunted. "I have turned 37 ... but my heart and mind still feel like I'm young," he said.

He said he likes his chances because he has been out to improve himself. For example, he is taking science classes from Laurentian University. He also said he is studying religion more deeply. "I memorized the entire Koran in Arabic and its recitation," he said during the interview. "And, apart from that, I've studied Arabic etymology and morphology."

He insisted that correctional officials and prison-approved preachers have been teaching him what they call a "counternarrative." That's basically the difference between a fanatical version of Islam and a well-intentioned one where "one can be a productive member of society in line with Canadian values," he said.

Besides, he said, he really has no idea what terrorists are thinking these days.

"I know and understand a lot of these groups, such as ISIS, are using radical extremist ideology," he said. But he added that the group has no appeal for him and that its propaganda would be completely unfamiliar to him.

Back then, he was a young software engineer who fixed computers for the federal government's foreign service bureaucracy, after he had grown up in the Ottawa suburb of Orleans playing street hockey.

He took to corresponding by e-mail with twentysomething Muslims in Britain who were also of Pakistani heritage. Outraged by the U.S.-led military invasions of Afghanistan and Iraq, the British suspects and Mr. Khawaja journeyed together to their families' homeland. They enlisted in a terrorist training camp in the remote regions of Pakistan and returned home intent on striking a blow against the West.

Scotland Yard spotted the British cell starting to assemble a bomb made up of 600 kilograms of ammonium-nitrate fertilizer.

Mr. Khawaja popped into the frame after a flight to Heathrow Airport, where he was met by the British ringleader, to whom he showed pictures of a prototype detonator he had built.

Arrested by the RCMP after returning to Canada, Mr. Khawaja went on trial for wanting to use his device - which he had dubbed "the Hi-Fi Digimonster - to help the British cell remotely set off explosions.

The evidence showed that the intended targets would have probably been inside a shopping mall, or a packed nightclub, in London. One conspirator was caught on a wiretap saying the nightclub was a good target because "no one can even turn around and say, 'Oh, they were innocent, these slags dancing around ...' " The British conspirators were caught red-handed building the bomb.

Mr. Khawaja insisted that no one ever clued him in about specific targets. He said he only ever envisioned bombs going off in Afghanistan. "There is no chance that, if I had known for sure, with certainty, it would be used in the streets of Britain, that I would have ever supplied it to them."

Mr. Khawaja spent years warehoused in Canada's version of a supermax prison, Quebec's Special Handling Unit, where human contact - even hugging a family member - is mostly forbidden.

This made moving to Millhaven last year feel liberating for him.

"Having open visits with my family, sitting at a table with my mother and father, ... these are opportunities I didn't have," he said.

9. New York Times

Drone Strike Data Reveals Limits of Fighting Terrorists From Sky

Monday, 04 July 2016

Byline: Scott Shane

Washington - The promise of the armed drone has always been precision: The United States could kill just the small number of dangerous terrorists it wanted to kill, leaving nearby civilians unharmed.

But the Obama administration's unprecedented release last week of statistics on counterterrorism strikes underscored how much more complicated the results of the drone program have been.

It showed that even inside the government, there is no certainty about whom it has killed. And it highlighted the skepticism with which official American claims on targeted killing are viewed by human rights groups and independent experts, including those who believe the strikes have eliminated some very dangerous people.

"It's an important step -- it's an acknowledgment that transparency is needed," said Rachel Stohl, an author of two studies of the drone program and a senior associate at the Stimson Center, a research group in Washington. "But I don't feel like we have enough information to analyze whether this tactic is working and helping us achieve larger strategic aims."

More broadly, President Obama's move to open a window on the secret counterterrorism program takes place against a background of escalating jihadist violence that can be called up by a list of cities

that includes Paris; San Bernardino, Calif.; Brussels; Orlando, Fla.; Kabul, Afghanistan; Istanbul; Baghdad; and now Dhaka, Bangladesh.

Apart from the dispute over the number of civilian deaths, the notion that targeted drone strikes are an adequate answer to the terrorist threat appears increasingly threadbare.

"There's a massive failure of strategy," said Akbar S. Ahmed, a former Pakistani diplomat and the chairman of Islamic studies at American University in Washington. Drones have simply become one more element of the violence in countries like Pakistan and Yemen, not a way to reduce violence, he said.

Among young people attracted to jihadist ideology, "the line to blow yourself up remains horrifyingly long," he said. "That line should be getting shorter."

A senior Obama administration official, who spoke on the condition of anonymity to discuss the classified program, said the recent series of major terror attacks in urban areas had all been directed or inspired by the Islamic State.

The classified counterterrorism drone campaign, he said, has targeted other groups, notably Al Qaeda's old core in Pakistan, its branch in Yemen and the Shabab in Somalia. No attack in the West in the past year has been traced to those groups, suggesting that the strikes have been effective, he said. The drone strikes in Iraq, Syria and Afghanistan are, for the most part, carried out by the military in a separate program.

In Friday's release, the White House made public an executive order laying out policies to minimize civilian casualties in counterterrorism strikes and a plan to start making public the basic statistics on strikes each year.

At the same time, the Office of the Director of National Intelligence released the first official estimates of those killed during Mr. Obama's presidency in strikes outside the conventional wars in Iraq, Syria and Afghanistan. Though the announcement did not say so, the classified strikes took place in Libya, Pakistan, Somalia and Yemen, and the vast majority used missiles fired from unmanned drone aircraft, though a few used piloted jets or cruise missiles fired from the sea.

Since 2009, the government said, 473 strikes had killed between 2,372 and 2,581 combatants. They are defined as members of groups, like Al Qaeda and the Taliban, that are considered to be at war with the United States, or others posing a "continuing and imminent threat" to Americans.

In the most sharply debated statistics, the statement estimated that between 64 and 116 noncombatants had been killed. Officials said those numbers included both clearly innocent civilians and others for whom there was insufficient evidence to be sure they were combatants.

The numbers were far lower than previous estimates from the three independent organizations that track strikes based on news reports and other sources. The Long War Journal, whose estimates are lowest, counted 207 civilian deaths in Pakistan and Yemen alone. The security policy group New America

in Washington estimated a minimum of 216 in those two countries, and the London-based Bureau of Investigative Journalism estimated the civilian toll under Mr. Obama between 380 and 801.

With no breakdown by year or country, let alone a detailed strike-by-strike account, the Obama administration's new data was difficult to assess. For example, according to multiple studies by Human Rights Watch, Yemen's Parliament and others, an American cruise missile strike in Yemen on Dec. 17, 2009, killed 41 civilians, including 22 children and a dozen women. At least three more people were killed later after handling unexploded cluster munitions left from the strike.

If those 41 are included in the new official count, as appears likely, that would leave only 23 civilians killed in all other strikes since 2009 to reach the low-end American estimate of 64. By nearly all independent accounts, that number is implausibly low. Obama administration officials declined over the weekend to discuss any specific strikes or otherwise elaborate on the statistics.

Scott F. Murray, who retired from the Air Force as a colonel after 29 years, was a career intelligence officer involved in overseeing airstrikes in Iraq, Afghanistan and Syria. He said that while he had not been involved directly in the counterterrorist strikes outside those war zones, the civilian death estimates were "lower than I would have expected."

He said civilian deaths could result from multiple causes, including incomplete intelligence about the identities of people on the ground, equipment failure and human error.

Perhaps most often, Mr. Murray said, problems arise when civilians enter a target area before drone surveillance begins, or when a civilian suddenly enters the strike zone just before a strike.

"The night you choose to strike, it may be that the in- laws arrived earlier in the day or the children's birthday party is ongoing and you weren't watching when everyone arrived," Mr. Murray said. "Those are the things in war that drive you to drink. You never ever have perfect information."

Brandon Bryant, who worked on Air Force drone teams from 2006 to 2011 and has become an outspoken critic of the program, recalled one strike in 2007 targeting a local Taliban commander. As the Hellfire missile sped toward the small house, he said, a small child -- possibly frightened by the missile's sonic boom -- ran into the house and was killed.

"Those things are burned into my brain -- I can't really forget them," Mr. Bryant said. He added that he believed total civilian deaths were much higher than the administration's estimate because of officials' wishful thinking, rather than deliberate deception. "They're just deluding themselves about the impact," he said.

The senior administration official acknowledged the fear and frustration produced by the recent urban attacks and said Mr. Obama's strategy went far beyond drone strikes, incorporating the military battle against the Islamic State in Iraq and Syria, counter-messaging against jihadist groups, and support for allies facing the same enemies as the United States.

American officials strongly defend the necessity of targeted killing, and the president's executive order suggests that he believes the drone program will endure far beyond his presidency. But deaths from terrorism have risen sharply since 2011, according to the Global Terrorism Index, compiled annually by researchers, and there is worry inside and outside the government that the United States and its allies are winning battles but losing the ideological war.

Of particular concern is the possibility that the rash of attacks carried out in the name of the Islamic State is just the beginning -- not because the group is getting stronger but because it is getting weaker. As the United States and its allies uproot the Islamic State in Syria and Iraq, its supporters may turn to terrorism wherever they are, many terrorism experts believe. In most of those places, like the cities hit hardest in recent months, no drone strikes will be possible.

10. The Hindu

Cyber firm cautions mobile users against 'rogue' apps

Monday, 04 July 2016

Byline: Yuthika Bhargava

New Delhi - Cyber criminals are now turning to application stores, traditionally considered a safe destination for downloading mobile apps, to plant malware in phones.

Recently, cyber security solutions provider Symantec had detected an application on Google Play Store -- Beaver Gang Counter -- that masquerades as a score keeping app for a popular card game. However in reality, once installed on the device, this application secretly starts searching media files related to Viber. Once it finds them, it sends them to a remote server.

While applications are mostly verified before being published on the official Android store, some manage to slip past the store's upfront security checks.

"Viber is an extremely popular social media app with over 500 million installs on Google Play alone. The data stolen by the malware could be used for a number of nefarious purposes such as identity theft, blackmail, fraud, or pornography," Symantec said in a blogpost.

Symantec had alerted Google about this issue and in response they removed this app and developer from Google Play Store.

The discovery of this app, it added, demonstrated that having photos stolen from devices is also a risk Android users needed to be aware of. Some time ago, private photographs of some celebrities were leaked online, with reports suggesting that the attackers gained access to their Apple iCloud accounts.

"Mobile devices connect us to the world, storing our most personal and valuable information in digital form. However, this freedom complicates our security, and in fact mobile apps may present significant challenges to protecting our privacy. It might surprise you to learn that most threats to sensitive information on mobile devices are hidden in plain sight -- in apps," Ritesh Chopra, Country Manager, India, Norton by Symantec, said.

He added that many apps accessed or shared private, sensitive data without the users' knowledge or full understanding. Norton researchers recently found that globally, of the 10.8 million apps analysed by them, almost 3.3 million were classified as malware, a 230 per cent increase from 2014.

The study suggested that close to 40 per cent respondents granted permission to access their camera, bookmarks and browser history in exchange for free apps. "Thus, while apps are fun, boost your productivity and make your life easier, certain "rogue" apps can carry significant risks," Mr. Chopra added.

Meanwhile, a Google spokesperson said: "While we don't comment on specific apps, we can confirm that our policies are designed to provide a great experience for users and developers. That's why we remove apps from Google Play that violate those policies."

To stay protected from such mobile threats, Symantec recommends that users refrain from downloading apps from unfamiliar sites and install apps only from trusted sources. Besides, close attention should be paid to the permissions that apps request.

Users should avoid apps with a poor or non-existent reputation and any app that no one knows about should not be trusted. It is also important that mobile software, including anti-viruses are kept updated.

Earlier, Symantec had also found a bug in a popular local food and restaurant recommendation site Burrp, which ultimately allowed cyber criminals to take over users' system to encrypt files and later demand ransom to decrypt the same files. Most of the users who have been impacted by this attack are based in the U.S. and India.

11. Gulf News

Why the UAE needs more cyber-savvy people

Monday, 04 July 2016

Byline: Mariam M. Al Serkal

Dubai - UAE residents have to be more cyber-savvy when it comes to protecting their privacy online, recent research has revealed.

In a study carried out by Kaspersky Lab, experts discovered that while some UAE residents use extreme, but inadequate methods, the statistics show that other Internet users do not take the right precautions in protecting their information online. Some of these extreme methods even include hiding their devices from prying eyes.

David Emm, Principal Security Researcher from Kaspersky Lab said: "These findings demonstrate two extremes - one the one hand there are people who think they can keep their data safe by, for example, hiding their computers; but on the other hand there are still those who are simply not taking the necessary precautions online."

The research found that 25 per cent of Internet users in the UAE covered up their webcam, in an attempt to protect their privacy. Useful in itself, it is important to recognise that covering a webcam cannot prevent audio interception and protect users from being heard to by hackers or malicious groups.

"People need to become more cyber-savvy - with today's security solutions it's possible to protect yourself from cyberthreats, without having to go to the extreme lengths of hiding a computer," said Emm.

In addition, 17 per cent of those surveyed admitted that they try to avoid using popular websites like Google and Facebook because of the personal information they gather, despite the fact that it is normal practice for almost all websites to track users and collect some user data today.

Furthermore, only 23 per cent of Internet users in the UAE said they feel targeted online, and 23 per cent said that they do not think a security solution is necessary - raising questions about their online awareness and ability to protect themselves from harm.

Up to 31 per cent of people also said they tend to store sensitive data on devices that have no Internet access, mistakenly thinking that this will guarantee the protection of their data.

However, although this theory is grounded in logic, and is essential for securing backup data from the effects of a ransomware attack, even without an Internet connection it is possible for a device to be infected via a connected smartphone or USB stick.

12. Jerusalem Post

What does the future of terrorists on Twitter, Facebook look like?

Monday, 04 July 2016

Byline: Yonah Jeremy Bob

Jerusalem - Social media services like Facebook and Twitter have been immune to lawsuits for incitement and the negative impact of terrorists using their services until now.

With Public Security Minister Gilad Erdan attacking social media more aggressively than ever and Facebook responding more directly than ever on Sunday - is that about to completely change? Maybe.

But the road ahead is unclear and even with some new strategies, it will be like navigating a legal minefield of defenses that can insulate the platforms from any liability.

Until now it has been a bit quieter for Twitter in the legal sphere, certainly as compared to Facebook, and even more so compared to Facebook regarding terror in Israel. Facebook has already been in the legal crosshairs, but Twitter less so.

On October 26, 20,000 Israelis, through the NGO Shurat Hadin, sued Facebook in New York state court alleging that the social media platform is intentionally disregarding the widespread incitement and calls for murder of Jews being posted on its web pages by Palestinians.

A 76 page list of plaintiffs contended that "Facebook's refusal to remove the flood of extremist videos, statements and cartoons being posted by Palestinians is encouraging imminent violence and fanning the flames of the terrorist attacks that have overwhelmed Israel in the past month," demanding it self-monitor and block incitement against Israel.

Originally and until he died from his wounds, the lead plaintiff was Israeli-American Richard Lankin, who was a passenger on a Jerusalem bus on October 13 when Palestinian terrorists from East Jerusalem,

The plaintiffs, who other than Lankin and a small number of other Israeli-Americans already actually hurt, had a debatable chance to sue from the start since they have not yet been harmed and are not citizens.

The complaint acknowledged that Facebook has established some rules concerning the content it will prohibit, but then alleges these are not sufficient to block the incitement to violence nor adequately enforced by the company.

Also, the complaint recognizes that "Facebook has taken down some of the most extreme calls to murder," but again complains that this was "only after they were reported by Israelis." That particular lawsuit did not go after Twitter, but it is noteworthy that in February, the social media platform said it had suspended 125,000 terror-related accounts over several months.

The plaintiffs argue that Facebook is "far from a neutral or passive social media platform and cannot claim it is a mere bulletin board for other parties' postings."

They note that Facebook "utilizes sophisticated algorithms to serve personalized ads, monitor users' activities and connect them to potential friends" and claims it "has the ability to monitor and block postings by extremists and terrorists urging violence just as it restricts pornography."

The complaint seeks to overturn past precedent protecting internet service companies from liability for third party postings, claiming that the way Facebook operates, intentionally or not, it functionally has an active involvement in the users' pages.

Shurat Hadin's Facebook lawsuit always had an uphill battle as Facebook has beaten a wide range of lawsuits (most not even related to Israel) against it dating back to at least 2009, using the US Communications Decency Act (CDA) of 1996 to insulate it as an interactive-computer-service provider from liability for speech by third-party users of its services.

What all of that means is that publishers of content get to decide whether to publish content, so it is fair to hold them accountable for that content.

Facebook's unbeatable defense has been that both it and the online message boards which preceded it, are just conduits without knowledge of what content is being posted. It says this should also free them for liability of the posting and for responsibility to remove content, certainly at least until it has been informed by others of a violation of its rules.

Originally, Shurat Hadin hoped and still hopes that it could overcome this defense by arguing Facebook is a more dangerous tool for terrorists than was previously known and that it has greater abilities to detect and remove terror content than it has admitted.

This would mean essentially telling courts that even if Facebook was seen as the same as message boards until now, that it is now used by terrorists in a much more threatening way and should be put in a unique category.

Second, they hoped to argue that Facebook's advances in algorithms and society's better understanding of these algorithms show that it actually has the ability to find and remove terrorists' posts. This would contradict what was believed to be limitations on its abilities or the abilities of message board providers and again be an opening for holding Facebook liable even if it and message boards were insulated from liability in the past.

But this was only the beginning of lawyers analyzing how social media works and where it could be vulnerable to lawsuits to pressure it to cut-off terrorists from using their services.

At the beginning, the focus by advocates trying to fight anti-Israel terrorists (as opposed to ISIS which by far has the largest terror presence on the web) use of social media was Facebook and not Twitter for a few reasons.

First Facebook is used more than Twitter for posting videos and for larger and longer posts, so the terror incitement on Facebook broke through into the public's consciousness far more. Videos are less common on Twitter and posts are limited to 140 characters.

Observers have said this was particularly true in Israel and with the Palestinians where Facebook is used far more by the general public, and Twitter is used by a much smaller group of journalists and public officials. While no study has been done, some believe that Facebook being the typical tool of average

Israelis and Palestinians, as opposed to Twitter, is even more pronounced in this region than it is in the US where a greater number of average people use Twitter.

But then Tamara Fields, wife of a private American military contractor killed by a terrorist in Jordan in November, Reynaldo Gonzalez, father of Nohemi Gonzalez, who was murdered by ISIS terrorists in Paris in November and Shurat Hadin made a discovery, or connected some new dots.

They asked: what if social media is not looked at merely as a general tool for incitement by posting videos? What if it is looked at as giving "material support" to terrorists under the US Anti-Terrorism Act?

Using this concept, if banks could be sued in the US merely for being conduits of terrorists funds, even without being involved in terror themselves, social media providers could be sued as conduits for transmitting messages for using both Facebook and also Twitter for allowing networking, recruiting and publishing newsletters from Hamas' and other groups' Twitter accounts.

Once this approach was taken, it was apparent that Twitter could be included as violating the US's ATA and maybe both Twitter and Facebook could be beaten in court with the argument that defenses in the past under the CDA were only meant to protect from general incitement lawsuits, not from more serious ATA terrorism claims.

Put differently, Shurat Hadin asked itself, if Hamas agents cannot open a bank account or physically enter the US because it is a terrorist group, why should it be able to use social media services of US-based companies like Facebook and Twitter?

The first to sue was Fields in January in in a US federal court in Northern California, with her case recently being dismissed. Gonzalez sued on June 14 also in California.

Shurat Hadin is planning to file its own Twitter lawsuit on behalf of the families of Taylor Force, a former US military veteran murdered during a terrorist stabbing spree in Jaffo in March, and others in the very near future.

It says it is filing a few weeks after the other lawsuit to seek a more favorable jurisdiction than California, seen as too friendly to Silicon Valley, and to more fully address some of the potential legal defenses Twitter may attempt.

The ATA idea may have a better chance of working to get around the CDA law which has insulated Facebook and Twitter from incitement lawsuits, especially because there has been a conceptual jump to view the social media platforms not merely as message boards for terrorists, but as providing concrete material logistical support.

On the other hand, there are a variety of debates going on in Israel, the US and elsewhere about passing new legislation to hold Facebook and Twitter to a greater level of accountability or to build cyberspace back-doors for the government to enter to hunt down terrorist activity.

The fact that they are only debates and have not yet become new laws suggests that the CDA may still be an absolute defense against lawsuits until a new law actually passes.

Moreover, whereas a new law sponsored by Justice Minister Ayelet Shaked and Public Security Minister Gilad Erdan targets the social media platforms and may have a real chance of passing, support for legislation in the US is nowhere near the level needed for anything big to happen in the near future.

This means that the current lawsuits may raise public pressure on Facebook and Twitter, but even with their new approach, their chances of success are low without new legislation.

13. Gulf News

Mideast oil and gas sector faces wider cyberattacks

Monday, 04 July 2016

Byline: Naushad K. Cherrayil

Dubai - Concerns about cybersecurity are particularly high within the oil and gas industry, which faces a far wider spectrum of threats that are potentially more severe in comparison to other key industries.

According to Repository of Industrial Security Incidents (RISI) data, cyberattacks against oil and gas organisations in the Middle East make up more than half of the recorded instances. In parallel, in the US or other Western countries, they make up less than 30 per cent of the recorded instances.

Katharina Rick, partner and managing director at Boston Consulting Group (BCG), said that the rate of cyberattacks targeting companies in the regional oil and gas sector is notably high, especially compared to global figures.

In recent years, there has been a growing prevalence of cyberattacks in the region.

Cybersecurity firm Symantec reported that Trojan Laziok, an aggressive malware program, had attempted to steal data from energy companies around the world, some based in the Middle East last year. Remarkably, 25 per cent of the attempted cyberattacks targeted companies in the UAE versus 10 per cent in both Saudi Arabia and Kuwait and five per cent in both Oman and Qatar.

The dangers posed by large-scale threats are significant, given the physically expansive infrastructure of oil and gas production and distribution. For instance, the ramifications of a successful cyberattack on an oil and gas company in the Middle East could carry grave implications on national security. In most countries in the region, the oil and gas sector is the main source of income for the government and accounts for 60 to 70 per cent of fiscal spending resources.

This, of course, raises three pivotal questions -- Why are oil and gas companies in the Middle East more vulnerable to attacks? How can organisations that have fallen victim to cyberattacks ensure a quick recovery? And what can they do to fend off future attackers?

The reality is, she said that in recent years, companies in the region have invested heavily in newer IT infrastructure and solutions -- including multiple mobile devices connected to the oil and gas companies' networks.

According to Jebin George, senior research analyst at research firm International Data Corporation, IT spending by Middle East oil and gas sector is expected to grow to $1.83 billion in 2016 compared to $1.77 billion in 2015.

"Given their widespread popularity and ability to store sensitive or confidential data, mobile devices are increasingly turning into an open frontier for cyberattacks. In the Middle East and Africa, the situation is especially dire considering the region's high mobile phone penetration rates," Rick said.

Independent market research company eMarketer predicts that over 789 million people in the Middle East and Africa will own at least one mobile phone in 2019 -- and it is fair to assume that they will be bringing their device to work.

"In this day and age, inadequate boundary protection is a strong point of vulnerability. It can make it difficult to detect nefarious activity and can create avenues that allow outside parties to interface with systems and devices that directly support a company's control processes. It can also provide an easy access route to industrial control systems -- as most communication protocols for measuring and control devices are not as well encrypted as those for business communication systems," she said.

Another critical point of vulnerability is information flow enforcement. If false data is fed into the system or information is "siphoned off", most companies would likely never know that for a fact -- it could even go completely undetected. There is wide speculation that the colossal malware attack on oil giant Saudi Aramco's systems in 2012 was actually a cover-up for earlier information flow breaches.

"Insufficient control of information flows can allow attackers to establish unsanctioned and damaging commands and controls with potentially severe consequences for the physical infrastructure, the value of national assets and personal safety and health," Rick said.

The potential points of attack are plenty. Transactions in the oil and gas arena are broad in scope and range from sensitive information on well sites to end-user consumption at the pumps.

She said that governments in the region, including those of Saudi Arabia and Qatar, have crafted multi-phased national cyber security strategies and developed related policies and frameworks, focusing specific attention on critical infrastructure and national interests.

14. Khaleej Times

Users warned of ransomware attacks

Monday, 04 July 2016

Byline: Abdul Basit

Dubai - There is no silver bullet when it comes to ransomware protection and it can only be tackled by a holistic, multi-layered approach, according to security solution provider Trend Micro.

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

Ransomware attacks have increased manifold during the past year. No one is immune to it, neither big nor small businesses. Even home users are not spared.

Trend Micro has blocked more than 100 million ransomware threats for their customers in the past six months alone, with 99 per cent of threats blocked from email and web traffic. Recognising the growth and impact of ransomware, the company has taken a holistic approach to defend customers against ransomware.

"Trend Micro is assessing the threat of ransomware and acting to protect against it," Trend Micro CEO Eva Chen said.

Trend Micro says ransomware readiness assessment helps businesses of all sizes understand vulnerabilities in their security posture and provides action that can be taken.

Ransomware removal tools help both consumers and businesses that have been impacted by ransomware to recover data.

"We understand this pervasive form of cyberattack can be debilitating to enterprises, regardless of size or industry, and can cause grave amounts of stress and costs to consumers. Trend Micro business and consumer products have been tuned to deliver the best protection against ransomware. Our ransomware recovery tools and phone hotlines leverage the threat expertise within Trend Micro to deliver always-on support and help customers to prepare for the possibility of an attack, or quickly if they've already been hit," Chen explained.

Trend Micro delivers enhanced visibility of how ransomware impacts an organisation - identifying ransomware delivered through email, malicious URLs, a network breach or server compromise. This enables incidents to be investigated and resolved more rapidly, and enables ransomware trends to be tracked over time so that an organisation's overall security posture can be improved.

"Trend Micro is offering stronger solutions to combat ransomware," said John Dickson, director of IT infrastructure, RNDC. "Offering an all-inclusive solution and custom hotline to any enterprise customer

or consumer dealing with ransomware along with upgrades to existing products will help further protect customers in this digital age."

Doug Cahill, senior analyst covering cybersecurity at ESG, said: "The bottom line is that it's more important than ever to have a multi-layered approach for enterprise security."

Cahill added: "Trend Micro offers a set of security controls to protect enterprises from ransomware, providing the visibility required to understand how they are being impacted and how they can respond to improve their security posture. Their knowledge of the complexity and sophistication of ransomware brings a level of expertise that helps organisations mitigate the risk associated with this threat."

1. South China Morning Post

Warning to online news sites on social media sources

Tuesday, 05 July 2016

The powerful internet censorship body has further tightened its grip on online news reports by warning all news or social network websites against publishing news without proper verification, according to state media reports.

The instruction, issued by the Cyberspace Administration of China, came only a few days after Xu Lin, formerly the deputy head of the organisation, replaced his boss, Lu Wei, as the top gatekeeper of internet affairs.No website is allowed to report public news without specifying the sources, or report news that quotes untrue originsCyberspace Administration of China.

Xu is seen as a key supporter of President Xi Jinping.

The cyberspace watchdog said online media could not report any news taken from social media websites without approval.

"All websites should bear the key responsibility to further streamline the course of reporting and publishing of news, and set up a sound internal monitoring mechanism among all mobile news portals [and] Weibo or WeChat," Xinhua reported the directive as saying.

"It is forbidden to use hearsay to create news or use conjecture and imagination to distort the facts," it said.

The report said a number of news portals, including 163.com, Sina.com, Qq.com, Ifeng.com and Caijing.com.cn had been punished and given warnings for fabricating news before distributing it, the report said, without giving any details about the penalty.

The government already exercises widespread controls over the internet, including blocking popular foreign websites such as Google and Facebook.

It says the measures are needed to ensure security in the face of rising threats, such as terrorism, and also to stop the spread of damaging rumours.

2. Washington Free Beacon

Obama's Green Policies Threaten America's Energy Security

Tuesday, 05 July 2016

Byline: Bill Gertz

Washington - The threat of a devastating cyber attack on the U.S. electrical grid is increasing due to the Obama administration's politically correct policies that spend vast sums on green and smart grid technologies while failing to secure power grids from cyber attack.

A report by the Manhattan Institute, a New York think tank, warns that the push to integrate wind and solar electrical power into the $6 trillion electric utility system has created new vulnerabilities that other nations could exploit in a future cyber war.

"Electric grids have always been vulnerable to natural hazards and malicious physical attacks," writes Mark Mills, a physicist and engineer who authored the Manhattan Institute report. "Now the U.S. faces a new risk- -cyber attacks--that could threaten public safety and greatly disrupt daily life."

The U.S. electrical power network is not made up of a single grid, but a complex web of eight regional "supergrids" linked to thousands of local grids. Under a drive for improved efficiency, government policymakers and regulators in recent years have spent tens of billions of dollars on so- called "smart grid" technology. But the efficiency drive has not been matched with new technology that will secure grids against cyber attacks.

Utility owners also have resisted improving cyber security over concerns doing so would increase operating costs and force unpopular rate hikes. Yet the failure to take steps now to deal with future threats could prove catastrophic.

The threat, according to the report, is not the current state of security but the future use of greener and smarter electric grids, interconnected and linked to the Internet. "These greener, smarter grids will involve a vast expansion of the Internet of Things that greatly increases the cyber attack surface available to malicious hackers and hostile nation-state entities," the report warns, adding that cyber attacks overall have risen 60 percent annually over the past six years and increasingly include the targeting of electric utilities.

A recent survey by Cisco Systems revealed that 70 percent of electric utility security managers suffered at least one security breach.

Unfortunately, Obama's liberal agenda forced government policymakers and regulators to promote green and smart grid technologies while spending relatively trivial amounts to secure those grids from cyber attacks.

"Greater grid cyber security in the future means that policymakers must rethink the deployment of green and smart grids until there are assurances that security technologies have caught up," the report recommends.

Part of the problem for grid security is that power networks are controlled by the private sector utilities. Government can and must provide intelligence and warning of cyber threats. But grid security is the

responsibility of industry and there is an urgent need for the private sector to do more to defend the country from a future devastating blackout.

Further, the government and electric companies appear to be playing down the danger, claiming cyber attacks are less likely than squirrels eating electrical cables, or tree limbs shorting out wires.

This attitude was reflected in a controversial Department of Homeland Security Report produced in January that concluded the threat of a damaging or disruptive cyber attack on the electric infrastructure was low. The study was an embarrassing reminder that the federal government is ill-prepared for future dangers. A month before the DHS report, Russian hackers took down portions of Ukraine's power grid in what has been called the first known cyber attack on an electricity infrastructure.

The problem of grid security has been made worse by the past seven years of administration policies that subordinated building up security against cyber attacks to integrating environmental technologies. The liberal worldview mistakenly has placed climate change as a greater national security threat than future cyber attacks from nation states.

According to the Manhattan report, wind and solar power will be unable to meet the country's 24/7 energy demands for the foreseeable future. Yet programs to develop these energy sources received over 75 percent of all new generating capacity, with some $150 billion invested by the federal government on green and smart grid programs. By contrast, the Energy Department spent $150 million on cyber security research and development.

Blackouts have occurred in the past, mainly after hurricanes. One non-natural disaster was the August 2003 blackout that affected New York City and the Northeast. That power outage put 50 million people in the dark for two days, and caused $6 billion in damage. The cause was a combination of a software glitch and human error that resulted in a localized power outage in Ohio cascading into a widespread regional power disruption.

According to the Manhattan Institute study, Lloyd's estimates that the damage from a worst-case cyber attack that causes a widespread blackout would cost between $250 billion and $1 trillion.

The coming danger will involve sophisticated nation state cyber attacks. U.S. Cyber Command chief Adm. Mike Rogers announced in March that it is a matter of "when, not if" a foreign power will attack critical U.S. infrastructures.

Peter Pry, a former CIA officer and grid security advocate, says the report correctly identified the contradiction between Obama administration's green agenda and the need to protect the nation's energy security.

"The 'war on coal' and other hydrocarbon sources of energy, and the Obama administration's environmental obstacles to development of nuclear power, is making the nation less safe," said Pry, executive director of the Task Force on National and Homeland Security.

Coal-fired electric plants and potentially nuclear power provide the country with the most resilient source of electric power. But the administration's push to phase them out and replace them with wind and solar energy generation is not only technologically unrealistic. It will reduce national electrical supplies at a time when demand is increasing sharply.

The result will be both increase costs for electric power and increase risks to national survival in the aftermath a major cyber attack.

"The increased risks to the national electric grid and national security by Obama's green agenda, driven by the alleged threat from climate change, is even more true for greater threats to the grid posed by natural and manmade electromagnetic pulse (EMP)," Pry said. "These threats and cyber are here and now, while climate change--if this scientifically dubious threat occurs at all--is in the future."

Mills, the Manhattan Institute researcher, told the Washington Free Beacon that cyber security "is the existential challenge of the Internet, but so far mainly about private info and financial data."

"Meanwhile, the so-called smarter grid and green power both require a vast increase of Internet connectivity bolted onto our electrical grids," he said. "What in the world makes green pundits think that rapidly expanding and exposing our critical grid infrastructure to the Internet is a good idea to rush into?"

3. Pajhwok Afghan News

Drone kills 30 Taliban, IS militants in Nangarhar

Tuesday, 05 July 2016

Byline: Zeerak Fahim

Jalalabad - Drone strikes killed 30 Islamic State and Taliban militants, including two key commanders, and injured another three Taliban fighters in eastern Nangarhar province, officials said on Monday.

Nangarhar police spokesman Hazrat Hussain Mashriqiwal told Pajhowk Afghan News the drone strikes took place last night in Achin, Momand Dara and Khogyani districts.

A Daesh commander named Sajid was among 19 others killed in the strikes in Achin's Pekha area, he said, adding the dead included some Pakistani rebels. He said Sajid had been spearheading a 50-member armed group.

The governor's spokesman, Attaullah Khogyani, said Sajid was a resident of Pakistan's Orakzai tribal region and he led the latest attacks in Kot district. He said dead included Sajid's nephew as well.

Sher Aqa Faqiri, the 201 Selab Military Corps spokesman, said the drone targeted hideouts of Daesh militants and destroyed their weapons and ammunition.

Officials said a Taliban commander Sabir Kuchi was killed along with nearly a dozen fighters in a drone strike in the Khogyani district. Another three were injured, they said.

Mashriqiwal said commander Sabir Kuchi was living in Kot district and he was considered among key Taliban commanders. Sabir had been involved in a series attacks, he said.

A resident of Khogyani district, Obaidullah, said Sabir Kuchi was travelling in a convoy of vehicles with his fighters when came under attack from the air. He said it was being rumoured that Sabir had been killed in the attack.

4. Montreal Gazette

Montreal man charged with posting hate messages on social media, threatening Justin Trudeau

Tuesday, 05 July 2016

Byline: Paul Cherry

Montreal - A Verdun resident has been charged with posting hate messages on social media, while also uttering threats toward Prime Minister Justin Trudeau.

Jacques Roy, 47, appeared before a Quebec Court judge on Saturday after he turned himself in to the Montreal police on June 30, said Montreal police spokesperson Constable Jean-Pierre Brabant. Roy was released after agreeing to follow a series of conditions, and his case is scheduled to return to court on Oct. 3.

Brabant said the investigation began on March 26 after someone contacted the Montreal police and reported statements they had read on a social media page. The police investigated and found statements that were hateful toward Muslims, Islam and people from Syria. The author of the statements included Trudeau in some of what he posted, Brabant said.

An arrest warrant was issued on June 16 and the Montreal police were able to contact Roy for the first time last week. He agreed to turn himself in, with a lawyer, and was detained before he appeared in court.

The arrest warrant was made public at the Montreal courthouse over the weekend. In the warrant, Roy is accused of "encouraging hatred against an identifiable group." The charges are based on statements Roy allegedly made between Feb. 1 and March 26, in a manner "other than a private conversation." He is also accused of criminal harassment and uttering a threat toward Trudeau and "a member of his family" within the same time frame.

In February 2013, Roy was charged with assaulting a police officer. The charged was placed under a stay of proceedings the day after it was filed. On that same date, Roy pleaded guilty to willfully obstructing police in the execution of their duty. He was sentenced to one year of probation. Later on, in November 2013, Roy pleaded guilty to drug possession, and his sentence involved an unconditional discharge.

5. The Guardian (London)

Companies must 'take the fight to the criminals' to tackle cybercrime

Tuesday, 05 July 2016

Byline: Rob Davies

London - British firms must "take the fight to the criminals" to prevent a rising tide of cyber-attacks by sophisticated organised crime gangs, according to a report.

In a joint report, telecoms group BT and consulting firm KPMG called on companies to address the "industrialisation of cybercrime", warning against the danger of overplaying the more high- profile threat of lone hackers.

The report warns that today's cybercriminal often works for complex operations akin to businesses, with human resources divisions and budgets for research and development.

Some are so sophisticated that they are able to hijack senior executives' email accounts and fake correspondence to convince junior company employees to approve transactions. In one such case, the scam led to one company agreeing to pay out $18.5m (£13.9m) to criminals in the Asia-Pacific region, BT and KPMG said, without identifying the company.

Businesses must work with law enforcement against such operations, the report said, and should consider launching their own pre-emptive attacks against cybercrime networks.

Mark Hughes, chief executive of cybercrime at BT, said it was vital that companies "take the fight to the criminals". "The industry is now in an arms race with professional criminal gangs and state entities with sophisticated tradecraft," he said.

"The twenty-first century cybercriminal is a ruthless and efficient entrepreneur supported by a highly developed and rapidly evolving black market. Businesses need to not only defend against cyber- attacks but also disrupt the criminal organisations that launch those attacks."

But Hughes said the industry's efforts to tackle the problem are being hampered by a lack of graduates with the right skills to work in cyberdefence. BT has identified cybersecurity as a huge potential growth area, with revenues from its cybersecurity division increasing at more than 10% a year.

In April, the telecoms giant announced plans to hire 900 people for its already 2,500-strong security team to cope with growing demand.

The BT-KPMG report found that while 97% of firms have suffered a cyber-attack, only a fifth of technology chiefs at those firms felt well enough equipped to deal with organised cybercrime.

The skills deficit persists despite the importance of cybersecurity to major corporations being underlined by several high-profile security breaches.

Broadband and telecoms provider TalkTalk lost more than 100,000 customers and faced a bill of at least £60m in the wake of a cyber-attack last year that saw thousands of users' data harvested.

Ashley Madison - a US dating website aimed at people looking for extra-marital affairs - was hit by an attack that saw thousands of users' dating profiles leaked online.

6. The Hill

Wikileaks publishes Clinton war emails

Tuesday, 05 July 2016

Byline: Tom Devaney

Washington - WikiLeaks on Monday published more than 1,000 emails from Hillary Clinton's private server during her time as secretary of State about the Iraq War.

The website tweeted a link to 1,258 emails that Clinton, now the presumptive Democratic presidential nominee sent and received. They stem from a trove of emails released by State Department in February.

WikiLeaks combed through the emails to find all the messages that reference the Iraq War.

The development comes after WikiLeaks founder Julian Assange said last month the website had gathered "enough evidence" for the FBI to indict Clinton.

"We could proceed to an indictment, but if Loretta Lynch is the head of the [Department of Justice] in the United States, she's not going to indict Hillary Clinton," Assange told London- based ITV. "That's not possible that could happen."

7. Wall Street Journal

What's Next for the U.S. and China in Cybersecurity

Tuesday, 05 July 2016

Byline: Staff report

Interview - It took the threat of sanctions and a flurry of last- minute negotiations to get China to sit down for serious talks about cybersecurity with the U.S. Now comes the hard part.

Chinese President Xi Jinping's announcement last fall that Beijing would stop state sponsorship of hacking for commercial gain caught many by surprise. By multiplerecentaccounts, China has stayed true to its word. But in the area military types increasingly refer to as the "fifth domain" -- after land, sea, air and space -- of warfare, a cloud of questions large and tiny still loom over relations between the world's great powers

One emerging expert on the uncertain business of cyberpolitics is Carnegie Endowment for International Peace researcher Tim Maurer, who visited Beijing in late June to meet with Chinese cybersecurity scholars. China Real Time picked Mr. Maurer's brain on next steps for the U.S. and China, Beijing's ambitions for managing the internet and the cybersecurity threat that worries him the most. Here are excerpts edited for length and clarity:

WSJ: After the agreement between Obama and Xi, what's the next cybersecurity question for the U.S. and China?

Tim Maurer; Now that we have an agreement, there's a bigger strategic discussion that will continue to play out around the future of the internet and the issue of sovereignty. Topics like cloud storage and the role that multinational companies play still need to be resolved, and we still haven't seen a resolution to some of the security issues, like backdoors and other supply-chain integrity questions, that were raised by [NSA leaker Edward] Snowden and are a concern for both countries.

China's ?is big on this idea of Internet sovereignty-that national borders and national laws should extend into cyberspace. What does Beijing have to do to overcome political opposition in the U.S. and other countries and make that a reality?

There's a trade-off involved for the Chinese government, I think, between security and growth.China in and of itself is a huge market and is capable of satisfying a lot of Chinese companies. But? for global companies like Alibaba, Huawei and ZTE, ?the biggest growth opportunities are probably beyond China. This notion of technological sovereignty implies certain changes to the internet at several layers -- whether it's physical infrastructure, applications or control of content -- that will increase the cost of doing business globally ?through the internet. If you look at G20 economies, the internet actually accounts for a larger share of the economy in China than in the U.S.

WSJ: Where do the U.S. and China stand on question of establishing norms of behavior in cyberspace?

Maurer: There are disagreements over definitions of terms like "international wrongful act" and how norms will apply in a military context, but the major tension is over whether there should be a treaty. Russia and China are pushing for one. The U.S. and other Western governments are pushing for voluntary norms instead.

WSJ: Why not have a treaty? What do voluntary norms accomplish?

Maurer: There's been a gradual trend away from treaties and conventions the past few decades. One concern is that you undermine international law when you create treaties that are ineffective. That doesn't mean you can't have one, but there are lots of technical issues around issues like verification and enforcement. How do you determine when a violation has taken place, and how do you punish it? With voluntary norms, the idea is to to develop a standards of acceptable behavior that state actors will adhere to because it's in their self-interest to be a part of the community, to maintain access to shared information and resources.

WSJ: What will it take to get everyone to agree?

Maurer: There's already been significant progress in the last two or three years. Some people say there won't be much more progress until there's a major cyberattack. I think something else that might create movement is a growing threat from nonstate actors, like cybercriminals or terrorists, which is already happening.

WSJ: When you survey the variety of cybersecurity threats out there, what is the biggest concern you have?

Maurer: Probably the biggest concern is with the integrity of data. The vast majority of hacking incidents so far have been relatively unsophisticated stealing of data, which is the low-hanging fruit. In most instances, that's because defenses are so bad -- including at the government level. But now you're starting to see increasingly sophisticated malware, and there's a concern about hackers not just stealing data, but altering it

We haven't seen a lot of these attacks yet, but they are hard to detect and the potential damage is quite large, particularly in the financial sector. Electrical grids are confined to individual countries, but financial markets are highly interconnected. Imagine what would happen if people started losing faith in the integrity of financial data. It could have a domino effect. This is one area where we think there is potential for cooperation between states like the U.S., China and Russia.

8. Business In Vancouver

Canadian companies are woefully behind when it comes to cyber security

Monday, 04 July 2016

Byline: Albert Van Santvoort

Vancouver - A survey of 2,200 companies across 18 countries has found that Canadian companies are among the least equipped to deal with cyber threats.

The study ranks 18 countries based on the per cent of businesses that are adopters of effective modern cyber security procedures and technology. On a list of 18 countries Canada was number 15, ahead of only the Netherlands, Japan and the United Arab Emirates.

"We're moving from theft, which is costly, to potential catastrophe. There are forces at play now that aren't satisfied with just stealing your money, they want to destroy your entity. You can either start taking these threats seriously, or start looking for a hole to crawl into. Ignorance is no longer bliss," said Steve Duplessie, founder and senior analyst at the computer consulting firm Enterprise Strategy Group, in a press release.

The technology market research firm Vanson Bourne was contracted by the data storage company EMC (NYSE:EMC) to conduct the study. Vanson Bourne surveyed 100 Canadian companies and found that the majority of companies were "laggards" when it comes to adopting appropriate cyber security technologies.

Vanson Bourne found that 52% of Canadian companies surveyed had experienced unplanned system downtime sometime over the last 12 months. On average the unplanned downtime cost Canadian companies $414,000.

The survey also found that 34% of respondents suffered data loss in the last 12 months, which cost companies an average of $799,000.

Out of the instances of data loss or system down time 29% were a result of a security breach.

"I think CEOs themselves don't understand the ramifications of having little or no security on the cyber side. There was a recent study in the states that said 90% of CEOs don't seem to feel cyber security is their responsibility, and of course they're dead wrong," said Dale Jackaman, president of Vancouver-based Amuleta Computer Security.

According to Jackaman, Canada is "dead last" when it comes to cyber security in the western world. Jackaman, who originally started Amuleta as a cyber security firm to help businesses, had to change his entire business model because of a lack of demand from Canadian companies.

9. Yorkshire Post

I Spy: GCHQ reaches out to Mumsnet generation in new recruitment drive

Monday, 04 July 2016

Byline: Staff report

Scarborough - The director of GCHQ has announced a multi-million pound investment to transform a Yorkshire base into the North of England's training hub as the spy agency looks to recruit more middle-aged women from the Mumsnet generation.

The £42m package was outlined yesterday by Robert Hannigan, the director of the UK's Government Communications Headquarters, on a visit to its base on the outskirts of Scarborough.

The base is to be the training and skills hub of the northern network of GCHQ, the intelligence and security organisation which monitors radio and signals communications and protects against a wide range of threats, from terrorism and cyber crime to child sex exploitation and hacking.

Along with MI5 and MI6, there will be an emphasis on recruiting more women, especially those who middle-aged and also mid-career, dubbed "Jane Bonds", and the organisation has used Mumsnet for that purpose.

Of the £42m that is being invested in the next four years, £30m will go towards the base's infrastructure - modernising and improving the current environment - and £12m to skills training.

The current staff of about 200 will also be "upskilled".

During yesterday's visit, Mr Hannigan opened the Alan Turing Training and Innovation Centre (the ATTIC), a transformation of some of the existing main block into bright, airy training rooms.

Earlier, 94-year-old Sister Pamela Hussey cut the ribbon on a new museum showcasing the base's proud history.

Sister Hussey, who signed up to be a Wren in 1942, was a station operative during the Second World War, and was part of the team who intercepted radio messages from German U-boats.

Scarborough's role was fundamental in the conflict - the sinking of the Bismarck was down to messages which had been picked up at the North Yorkshire listening base.

In front of an audience of current staff and 30 or so guests, including dignitaries and GCHQ veterans, Mr Hannigan said the Scarborough base, since its inception early last century, had been one of the "collection sites - the crown jewels of intelligence gathering". The amazing work it had done throughout the last century, in two world wars and the Cold War, was continuing.

"We will not be able to face the threats and conflicts without the right skills and talents," he said. "We need to redress the balance to 50-50 (only 35 per cent of employees are women).

"We need people with the right aptitude, attitude and passion."

The surveillance organisation is now broadening its reach away from just graduates and it is also looking to recruit young school leavers into apprenticeships.

The Scarborough base already runs cyber summer schools aimed at young people who have an interest in science and technology.

Of the upcoming intake, which starts on July 11, there are 18 men and 14 women, reflecting a greater emphasis on recruiting both sexes.

The ATTIC Centre is named after the Second World War codebreaker who, after ground-breaking work by Polish mathematicians, cracked the Enigma code which had been developed by the Germans.

A short walk away from the new centre, the new "Y" Museum houses an Enigma machine and several other artefacts.

Sister Hussey, a nun since shortly after the war who now lives in a community in Harrogate, recalled about working in the underground bunker above which the museum now stands.

She said: "There were rows and rows of tables, the Wrens at one end, the sailors at the other, all with headphones on for hours and hours - but they used to throw paper planes at us.

"It was deadly serious work, though ... work which the spy organisation is hoping today's women will take up, for the country's sake."

1. Los Angeles Times

Chinese man gets prison for his role in hacking plot (Canada)

Thursday, 14 July 2016

Byline: Matt Hamilton

Los Angeles - A Chinese national was sentenced Wednesday to nearly four years in prison for plotting with Chinese military officers to hack computers belonging to U.S. defense contractors such as Boeing Co. and obtain trade secrets involving designs of American military aircraft.

In addition to the prison term, U.S. District Judge Christina A. Snyder ordered Su Bin, a 51-year-old man who is also known as Stephen Subin and Stephen Su, to pay a $10,000 fine.

Bin, who operated an aviation and aerospace company in Canada, pleaded guilty March 23 to a federal conspiracy charge of gaining unauthorized access to a protected computer.

He was arrested in British Columbia in 2014, and he waived extradition to the U.S. in February 2016.

Starting in 2008 and continuing until 2014, Bin informed military officers in China about what sites to hack and which files to steal, and he advised his co-conspirators on which information was significant, according to the U.S. attorney's office in Los Angeles.

Bin did not get any money from the scheme, but he admitted that he entered into the plot in order to profit.

One of the companies targeted in the conspiracy was Chicago-based Boeing, whose computer servers in Orange County stored detailed files on the C-17 military aircraft. Bin admitted that sensitive military information was accessed on the servers and sent to China, according to a plea agreement filed in the Central District of California.

Bin and his co-conspirators also handled data related to the F-22 and F-35 fighter jets, both made by Lockheed Martin Corp., according to court papers.

As part of the conspiracy, Bin reviewed files and translated a technical flight test plan from English into Chinese. He and his co-conspirators also drafted and sent reports summarizing the information and technology gained from the hacking effort.

Prosecutors contended that although Bin may not have actually hacked American companies, he showed his conspirators which ones to target and what to pilfer.

"Su Bin's sentence is a just punishment for his admitted role in a conspiracy with hackers from the People's Liberation Army Air Force to illegally access and steal sensitive U.S. military information," said John P. Carlin, the assistant attorney general for national security.

Defense attorney Robert J. Anello asked the judge to impose a 30-month sentence, arguing that the offense "was an aberration in a lifetime of generosity and kindness."

Anello also told the judge that Bin would be "permanently saddled with this conviction" and pointed out that such a conviction would hamper his future efforts at doing business.

The lawyer wrote: "He is sorry for his actions."

2. Wall Street Journal

Power Grid Left Exposed to Sabotage

Thursday, 14 July 2016

Byline: Rebecca Smith

New York - An early morning passerby phoned in a report of two people with flashlights prowling inside the fence of an electrical substation in Bakersfield, Calif. Utility workers from Pacific Gas & Electric Co. later found cut transformer wires.

The following night, someone slashed wires to alarms and critical equipment at the substation, which serves 16,700 customers. A guard surprised one intruder, who fled. Police never learned the identities or motive of the burglars.

The Bakersfield attacks last year were among dozens of break-ins examined by The Wall Street Journal that show how, despite federal orders to secure the power grid, tens of thousands of substations are still vulnerable to saboteurs.

The U.S. electric system is in danger of widespread blackouts lasting days, weeks or longer through the destruction of sensitive, hard-to- replace equipment. Yet records are so spotty that no government agency can offer an accurate tally of substation attacks, whether for vandalism, theft or more nefarious purposes.

Most substations are unmanned and often protected chiefly by chain-link fences. Many have no electronic security, leaving attacks unnoticed until after the damage is done. Even if there are security cameras, they often prove worthless. In some cases, alarms are simply ignored.

The vulnerability of substations was revealed in a Journal account of a 2013 attack on PG&E's Metcalf facility near San Jose, Calif. Gunmen knocked out 17 transformers that help power Silicon Valley; a blackout was narrowly averted. The assailants were never caught.

The following year, the Federal Energy Regulatory Commission, which regulates the country's interstate power system, began requiring that utilities better protect any substation that could disable parts of the U.S. grid if attacked.

FERC's new rule, however, doesn't extend to tens of thousands of smaller substations, including Metcalf and the one in Bakersfield. Security experts say a simultaneous attack on several of these substations also could destabilize the grid and cause widespread blackouts.

Gerry Cauley, head of the North American Electric Reliability Corp., -- which writes standards for the grid -- was asked at a FERC hearing in June on grid security what kept him up at night. He said the prospect of "eight or 10 vans going to different sites and blowing things up." Recovery from a coordinated attack, he said, could take weeks or months.

The Metcalf substation, while undergoing security upgrades, was hit again in August 2014. Intruders cut through fences and burglarized equipment containers, triggering at least 14 alarms over four hours. Utility employees didn't call police or alert guards, who were stationed at the site, according to a state inquiry.

Three days after the break-in, Stephanie Douglas, PG&E's senior director of corporate security, sent a memo to the utility's president saying security was in a fail mode, and her department lacked clout and resources: She had 26 full-time jobs to protect 900 substations, as well gas pipelines and other utility assets.

Ms. Douglas, no longer with PG&E, declined an interview request. PG&E spokesman Matt Nauman said the utility has responded with a $200-million program that includes better security equipment, more training and hiring.

The sprawling U.S. electric system is regulated by government but mostly owned and operated by utility companies and grid operators that monitor electricity supply and demand every minute, every day. The system is always on -- and for years few thought anyone would try to turn it off.

The motive of most substation break-ins appears to be theft. Intruders and, potentially, terrorists also could be trying to hack into control systems through computer equipment in substations -- either to cause immediate damageor to gather information for later use.

"A substation is not an obvious target for criminals like a bank," said Joseph Weiss, a security consultant to utilities. "Common sense says they want to get into the electric system."

The U.S. power grid is like a giant puzzle that can be configured in different ways to deliver power where and when it is needed.

Major power sources -- gas-fired generators and nuclear-power plants, for example -- connect to substations that raise voltages to ferry electricity long distance over a network of power lines. At cities and other destinations, substations lower the voltage to safely deliver electricity to homes and businesses. Substation computers help grid operators control those electrical flows.

The grid was cobbled together during the electrification of the U.S. over the past 125 years. It is a fragile, interdependent system generally more vulnerable in summer when it is running closer to its limits. It is also at risk during low-demand periods, when power-plant operators and linemen perform maintenance. Fewer plants and transmission lines operating mean fewer options for delivering electricity during emergencies.

There is so much variability in the grid that what causes a catastrophe one day might not the next, which makes security issues complex. Small problems can quickly spiral out of control.

On Sept. 8, 2011, equipment problems and human error caused a large transmission line in Arizona to trip out of service. The grid is supposed to withstand the loss of any one line. On this day, electric current shifted to nearby lines and overloaded them; that overtaxed transformers at two small substations, which shut down defensively to prevent equipment damage, and disruptions spread.

San Diego was blacked out 11 minutes later. Traffic snarled. Flights were canceled. Raw sewage flowed into the ocean. Altogether, 2.7 million utility customers lost power in California, Arizona and Mexico.

Federal officials have long known about the vulnerability of electrical substations. A 1990 report from the federal Office of Technology Assessment warned that "virtually any region would suffer major, extended blackouts if more than three key substations were destroyed."

A 2012 report from the National Research Council of the National Academies of Sciences looked at different parts of the electric system and concluded that substations were "the most vulnerable to terrorist attack."

"We've known we had an issue for a long time and have been very slow to do anything about it," said M. Granger Morgan, a professor of engineering at Carnegie Mellon University who studied the San Diego blackout.

Security adviser James Holler said his company, Abidance Consulting, inspected nearly 1,000 substations over the past year for utilities in 14 states. "At least half had nothing but a padlock on the gate," he said. "No cameras. No motion sensors or alarms."

One utility lost a set of substation keys that were in a truck stolen for a joy ride. After the truck and keys were recovered, Mr. Holler said, the utility didn't change the substation locks.

Richard Donohoe, director of security for the consulting firm Black & Veatch, said the security departments of utility companies are often so low in the pecking order that "the rest of the organization ignores them half the time."

After the attack on the Metcalf substation, FERC required better protection for individual substations "that if rendered inoperable or damaged could result in widespread instability," or cascading blackouts in any of the three separate sections of the U.S. power grid.

That is a high bar. Utility experts aren't sure how many substations the new rules cover but estimate it is fewer than 350 out of approximately 55,000. They say more protections are needed at smaller substations that could trigger blackouts if attacked in combination.

The exact combinations depend on energy demand and the direction of electricity flow. In spring, for example, hydroelectric power plants send electricity from the Pacific Northwest to California. In winter, electricity flows in the opposite direction, mostly from gas-fired and nuclear power plants in California and Arizona.

One security-focused nonprofit group called the Foundation for Resilient Societies has called for an analysis of the impact of simultaneous attacks, both physical and cyber.

Thomas Popik, chairman of the group, told FERC in June that existing grid protections were inadequate and his group believed the grid was "a battlefield of the future" that required military-type defenses for key infrastructure.

Michael Bardee, director of the Office of Electric Reliability at FERC, said the agency could do more to study security vulnerabilities at the thousands of substations not covered by the new rule. FERC expects a progress report on the new rule later this year.

"Clearly, there's some sense that as events go on we may need to re-evaluate the applicability of this standard," Mr. Bardee said, and possibly expand its reach.

The Vermont Electric Power Co. approved a $12 million program to beef up security at 55 locations after substations were penetrated more than a dozen times by thieves stealing copper during break-ins from 2012 through early 2014.

"We haven't seen a theft in over a year," said Kerrick Johnson, a spokesman. The utility installed more secure fencing and better security cameras.

Most utilities are reluctant to spend money on security unless under government orders. They must justify their expenses to regulatory agencies to pass on the costs to ratepayers, said John Kassakian, an emeritus professor of electrical engineering at the Massachusetts Institute of Technology.

Security upgrades generally include cameras, lights and motion sensors, as well as password- controlled doors and gates that electronically monitor entries and exits. Terror threats, Mr. Kassakian said, probably seem less pressing than spending to comply with federal environmental rules.

Utilities don't always report attacks despite a legal requirement to notify the Energy Department within six hours of any event that could interrupt electricity or if a break-in targets security systems.

No utility has been fined for failing to comply as far as he knew, said David Ortiz, deputy assistant secretary at the Energy Department: "I don't have an enforcement team."

The Journal found nine substation break-ins over the past two years where theft wasn't the apparent motive. The tally and details of the break-ins were gleaned from interviews and public records requests. The count included attacks affecting the federally owned Liberty substation in Buckeye, Ariz.

The substation, about 35 miles west of Phoenix, is a critical link in the southwest power corridor, delivering electricity to heat homes in northwestern states during winter and cool buildings in the southwest during summer.

On Nov. 5, 2013, someone slashed fiber-optic cables that serve Liberty, as well as the larger Mead substation near Hoover Dam. It took workers about two hours to re-establish proper communications and normal controls.

Liberty is operated by the Western Area Power Administration, which controls 17,000 miles of high-voltage power lines used by utilities serving 40 million people in 15 states. If this system suffered a catastrophic failure, it would take down other utilities with it, experts said.

Alarms signaling trouble at Liberty began ringing at a utility operations center inPhoenix 13 days after the communications outage. Dozens of alarms sounded over two days before an electrician was dispatched.

The electrician expected a false alarm. Instead, he found the perimeter fence sliced open and the steel door to the control building "peeled back like a sardine can," said Keith Cloud, the utility's head of security.

The substation's computer cabinets were pried open. The substation's security cameras proved useless: eight of 10 were broken or pointed at the sky, Mr. Cloud said. Most had been out of operation for a year or more.

Two months later, on Jan. 30, 2014, Liberty was hit again. Two men with a satchel cut the gate lock and headed to the control building. They left after trying, unsuccessfully, to cut power to a security trailer outfitted with cameras and blinking lights, which were installed after the first break-in.

This time, Mr. Cloud said, utility officials found 16 of 18 security cameras had failed. Most were installed after the first break-in and hadn't been properly programmed. Investigators retrieved a single fuzzy video from a thermal-imaging camera.

Mark Gabriel, WAPA's administrator, said the utility has "taken steps to improve our physical security program and processes," including creating the security department in 2013 that Mr. Cloud now heads.

A federal audit faulted WAPA in April for violations of security regulations, including broken or obsolete equipment, lax control over keys to critical substations and failure to install intrusion-detection systems.

Mr. Gabriel said WAPA spends a couple of hundred million dollars on capital improvements annually, which includes money for security improvements. "The bigger story is how that break-in and others in the industry changed the thinking," he said.

Mr. Cloud said he has received about $300,000 for security upgrades at a handful of WAPA's 328 substations, including Liberty. To protect the system's 40 most important substations and control centers, he said, he needs $90 million: "I don't have the authority or budget to protect my substations."

3. Washington Post

46-month sentence for businessman who helped Chinese military hackers (Canada)

Thursday, 14 July 2016

Byline: Matt Zapotsky

Washington - A businessman who admitted helping Chinese military officers as they hacked into the computer systems of U.S. defense contractors and stole significant information was sentenced Wednesday to three years and 10 months in prison, authorities said.

Su Bin, 51, a Chinese national who also went by Stephen Su and Stephen Subin, had pleaded guilty earlier this year to conspiring to gain unauthorized access to a protected computer and to violating the Arms Export Control Act. He had been accused of participating in a years-long plot to steal military technical data -- including details related to Boeing's C-17 military transport plane and other fighter jets produced for the U.S. military -- for the Chinese government.

Su's plea marked a first for someone involved with a Chinese government campaign of economic cyberespionage. Assistant Attorney General for National Security John P. Carlin said his sentence was "just punishment" for his crimes.

"These activities have serious consequences for the national security of our country and the safety of the men and women of our armed services," Carlin said in a statement. "This prison sentence reinforces our commitment to ensure that hackers, regardless of state affiliation, are held accountable for their criminal conduct."

Su, the owner of a company called Lode Technology, was initially arrested in Canada in July 2014, and he ultimately waived extradition and consented to come to the United States in February. As a part of his plea, he admitted that he told his co-conspirators, who were military officers in China, what people, companies and technologies to target in their cyber-intrusions and that he translated some stolen data from English to Chinese. He said he did so because he wanted to profit from selling the information that was taken.

Federal prosecutors in recent months have been aggressive about bringing cybercrime cases against foreign nationals who might seem unlikely to ever appear in U.S. courts. In March, the Justice Department indicted seven hackers associated with the Iranian government in connection with crimes

that included attacking U.S. banks' public websites from late 2011 through May 2013 and breaking into a computer system at a small dam in Rye, N.Y., in an apparent attempt to disrupt its operation.

4. Huffington Post Canada

CSIS Twitter Account Aims To Make Agency 'More Accessible'

Thursday, 14 July 2016

Byline: Mohamed Omar

Toronto - The Canadian Security Intelligence Service, or CSIS as it's affectionately called, is now on Twitter.

On Wednesday, the agency posted its first tweet to the social network.

"Yes, we're on Twitter. Now it's your turn to follow us," it said, invoking the hilarious topic of surveillance.

Users responded to the tweet while keeping up with the knee- slapping tone set by the agency. (A response tweet: 'loving the completely chill attitude regarding your charter busting surveillance of citizens. GREAT COMEDY GUYS')

The Communications Security Establishment welcomed them to the site and offered some advice.

CSIS director Michel Coulombe said in a statement that the Twitter account is a "step" in strengthening dialogue between the service and Canadians.

"The Canadian Security Intelligence Service recognizes that a modern organization needs to communicate using modern means," he said.

"Speaking publicly on the nature of our work isn't always easy, but we want CSIS to be more accessible, and want to help the public understand more about our work."

Is CSIS' first tweet as good as the CIA's debut? We'll leave that for you to decide. (Just kidding, they probably already know!) (Full report).

5. Al Jazeera

US: Chinese national jailed over military hacking (Canada).

Thursday, 14 July 2016

Washington - A Chinese businessman who pleaded guilty to hacking sensitive US military information was sentenced to nearly four years in prison, prosecutors have said.

Su Bin, 51, was charged on Wednesday with taking part in a years-long scheme by Chinese military officers to hack into the computer networks of aircraft manufacturer Boeing and other major US defence contractors.

In addition to a 46-month prison term, a US District Court judge in Los Angeles ordered Su to pay a $10,000 fine.

"Su Bin's sentence is a just punishment for his admitted role in a conspiracy with hackers from the People's Liberation Army Air Force to illegally access and steal sensitive US military information," John Carlin, assistant attorney general for national security, said in a statement.

"Su assisted the Chinese military hackers in their efforts to illegally access and steal designs for cutting-edge military aircraft that are indispensable to our national defence," he said.

In an August 2014 indictment, prosecutors said that Su travelled to the United States at least 10 times between 2008 and 2014 and worked with two unidentified co-conspirators based in China to steal the data. He was arrested in Canada in 2014 and later consented to US extradition.

The trio were accused of stealing plans relating to the C- 17 military transport plane and F-22 and F-35 fighter jets, and attempting to sell them to Chinese companies.

According to prosecutors, in pleading guilty Su admitted sending emails to his co-conspirators telling them which people, companies and technologies to target with their hacking, and translating the stolen material from English to Chinese.

Su admitted taking part in the crime for financial gain, prosecutors said. The Chinese government has repeatedly denied any involvement in hacking.

6. Canadian Press

Canada's e spies keep an eye on terrorists, foreign agents and 'The Good Wife'

Thursday, 14 July 2016

Byline: Jim Bronskill

Ottawa - It's among the most secretive agencies in Canada.

But one project officer at the Communications Security Establishment, the electronic spy service, was ``very excited'' about seeing the CSE portrayed in an April episode of the popular CBS television series ``The Good Wife.''

Internal emails obtained by The Canadian Press under the Access to Information Act reveal the drama about a Chicago law firm captured the attention of the CSE, which is usually preoccupied with monitoring terrorists and foreign agents.

``Just wanted to share something with you all,'' wrote the project officer, whose name was deleted for security reasons, the morning after the program aired.

``At our meeting last week we were talking about how nice it would be for TV shows to mention CSE ... well ... last night I was watching a show that I never watch, 'The Good Wife,' and CSE was mentioned about 2-3 times.

``I was very excited and thought it was funny that we were just talking about this.''

The episode took dedicated lawyers Alicia Florrick and Lucca Quinn to Toronto to help a whistleblower on the run from the U.S. National Security Agency, the CSE's American counterpart.

Much of the hour was devoted to clearly tongue-in-cheek references to Toronto as litter-free and the U.S. as a ``land of guns and gangs'' with inferior health care.

Surveillance of Florrick by the NSA added spooky intrigue to several instalments of the series, which ended its seven-year run in May. In Toronto, she and Quinn employ a little trickery to win safe haven for the American whistleblower.

The CSE comes across as a cubicle farm of tech- savvy young Canucks who, naturally, root for the Toronto Blue Jays.

The portrayal of the Canadian agency was fictional and ``done without input from CSE,'' said Ryan Foreman, a spokesman for the Ottawa-based spy service.

The project officer's comments stemmed from the CSE's increasing efforts to educate the public about the agency's ``vital work in helping protect Canadians and Canada's security,'' he said.

``In addition, as we are always looking to recruit the best and brightest to join our unique and talented workforce, more exposure through things like mentions in TV shows help further build awareness of CSE among potential job applicants.''

The agency has been thrust into the spotlight in recent years due to the disclosures about NSA surveillance, and some CSE operations, by real-life whistleblower Edward Snowden, a former U.S. spy contractor.

In turn, the CSE has tried to explain more about what it does, with obvious limits, to help shape public opinion.

Like the domestic Canadian Security Intelligence Service, the CSE even has a Twitter account. On Wednesday, the electronic spy service tweeted: ``It's nice when our vital work is noticed by Hollywood, but we're still holding out hope for a shout out in 'The Beachcombers.'''

It seems unlikely, unless the CSE has inside intelligence: the venerable Canadian show signed off in 1990.

7. Reuters

China likely hacked U.S. banking regulator: congressional report

Wednesday, 13 July 2016

Byline: Staff report

Washington - The Chinese government likely hacked computers at the Federal Deposit Insurance Corporation in 2010, 2011 and 2013 and employees at the U.S. banking regulator covered up the intrusions, according to a congressional report on Wednesday.

"Even the former Chairwoman's computer had been hacked by a foreign government, likely the Chinese," staff at the U.S. House of Representatives Committee on Science, Space and Technology said in the report.

The report was the latest example of how deeply Washington believes that Beijing has penetrated U.S. government computers. But while making the allegation that China was the culprit, the report does not provide specific evidence to support that conclusion.

China's embassy in Washington did not have immediate comment on the allegations. The FDIC, one of the United States' principal banking regulators that keeps confidential data on the biggest banks, did not have immediate comment.

The compromise of the FDIC computers had been previously reported in May and some lawmakers had mentioned China as a possible suspect, but the investigation for the first time cites an internal FDIC probe as pointing toward China.

It is often difficult to determine the identity of a malicious actor in cyberspace, although China is believed to have been behind a number of intrusions at other federal agencies in recent years.

The report follows accusations by the United States that China stole more than 21 million background check records from the federal Office of Personnel Management beginning in 2014.

China has long been a hacking adversary for the United States, although intelligence officials believe Beijing has decreased its hacking activity since signing a pledge with Washington last September to refrain from breaking into computer systems for the purposes of commercial espionage.

A source familiar with the FDIC's internal investigation said the areas of the regulator's network that were hacked suggested the intruders were seeking "economic intelligence."

The congressional staff report accused the FDIC of trying to cover up the hacks so as not to endanger the congressional approval of the regulator's chairman, Martin Gruenberg, who was nominated by President Barack Obama and confirmed by the U.S. Senate in November 2012. Gruenberg's predecessor, Sheila Bair, served in the post for five years until July 2011.

A witness interviewed by the staff said the FDIC's former chief information officer instructed employees not to disclose information about the foreign government's hack, the report said.

The witness said the hush order was to "avoid effecting the outcome of Chairman Gruenberg's confirmation by the U.S. Senate," according to the report. The report also provided details of data breaches in which FDIC employees leaving the regulator took sensitive documents with them.

The report said current officials at the FDIC have purposely concealed information about breaches that had been requested by Congress.

"The committee's interim report sheds light on the FDIC's lax cyber security efforts," said Lamar Smith, a Republican representative from Texas who chairs the House Science, Space and Technology Committee. "The FDIC's intent to evade congressional oversight is a serious offense."

Gruenberg is scheduled to testify on Thursday before the committee on the banking regulator's cyber security practices.

8. Reuters

Canadian intelligence agency CSIS joins Twitter 'to be more accessible'

Thursday, 14 July 2016

Byline: Staff report

Ottawa - Canada's main spy agency joined Twitter on Wednesday, announcing in a cheeky flip of the script: "Now it's your turn to follow us."

Canadian Security Intelligence Service Director Michel Coulombe said in a statement the agency wanted the public to have a better understanding of what it does.

"Speaking publicly on the nature of our work isn't always easy, but we want CSIS to be more accessible," he said.

Canada's ruling Liberals ran on an election platform last year to increase government transparency and oversight of the country's spy agencies, which have been accused of being overly secretive.

The agency by Wednesday afternoon had 2,247 followers and was following 17 accounts including the U.S Federal Bureau of Investigation and the Central Intelligence Agency.

The new account, @csiscanada, was not the spy agency's first foray into social media.

At least two other accounts, @csiscareers and its French-language counterpart, @carriereauscrs, have been around since September 2013, although they tweeted mostly recruitment messages.

Canada's other spy agency, the Communications Security Establishment, is already on Twitter.

In 2014, the CIA joined Twitter with a similar tongue-in-cheek announcement: "We can neither confirm nor deny that this is our first tweet."

9. Aviation Week website

MI5 Warns of Transport Security Threat

Wednesday, 13 July 2016

Byline: Angus Batey

London - Technologies designed to reduce costs of major public building programs may offer terrorists an unprecedented reconnaissance capability, the Security Service (MI5) has warned.

BIM (building information modeling) systems became mandatory for all centrally procured public construction schemes in the UK from the beginning of April: yet BIM cannot be fully secured, and failure to appropriately restrict access could lead to non-vetted workers obtaining classified building-security data.

The case for using BIM is clear. If different structural, mechanical and electrical plans are superimposed for the first time when building is already underway, delays and cost increases are inevitable. BIM brings all the design data together in a virtual environment, allowing different trades to align plans before construction begins.

"The trouble is, the resultant model is the most fantastic hostile reconnaissance tool you could look for," 'Paul' (identities of Security Service staff are not made public), the head of cross-cutting security knowledge at the MI5-run Centre for Protection of National Infrastructure (CPNI), told the Counter-Terror Expo in London earlier this year.

"On one project we're advising on at the moment, some 80,000 people have unfettered access to every layer of the model," Paul says. "Not one of them has been security-cleared, and 160 don't even work for the project any more, but haven't been removed from the access privileges of the system. Some of them left under a cloud: and if you left under a cloud you might just have a grievance against your ex-employer to either steal data from the model or inject bad data which could completely compromise the construction."

Configuration of a project's BIM systems can eliminate some of the most worrying problems, but decisions need to be taken early, and by people with a thorough understanding of the security implications. This does not always happen.

"We found one (project) recently where, if I was a lectern supplier, I would be allowed into the BIM model to click on the lectern, see what the spec was, and see if I had one to offer," Paul says. "But with how that BIM model has been set up, because the lectern is touching the stage I can also get the stage details; because the stage is touching the floor I get the floor details; because the floor is touching the wall I get the wall details; and as the wall is touching the locking mechanism on the door I get to see the lock details. Remember: I'm a lectern supplier."

These problems appear to arise because managers may have a limited view of what constitutes a potential security risk. For example, cybersecurity will be part of a robust BIM implementation, but even the best cyber defenses will not, on their own, address all of a project's potential BIM-related security problems.

Major infrastructure programs, such as rail stations or airport terminals, are not classified in the traditional sense, but that does not mean that every aspect of their design is appropriate for public release. The CPNI advises projects on security measures including suitable blast-protection technologies and the projected effectiveness of physical barriers. Making such data public could enable an attacker to circumvent the protection.

"(With) an airport terminal building, the roof is visible on Google Earth, and you can walk past and photograph it - so I'm not that concerned about its security in the BIM model," Paul says. "You can go to Heathrow Terminal 5 and admire the structure - it's beautiful. But the blast counts behind it no-one really should know about, and all the baggage- handling and access to control systems I wouldn't want anyone to know about either."

The answer is to cultivate better understanding and management of security risks, which in turn means reassessing all the security implications when granting wide-ranging BIM access to participants in major infrastructure projects. The CPNI has worked with the British Standards Institute to publish what Paul calls "the fastest ever British Standard", Publicly Available Specification 1192-5, which sets out advice on embedding BIM security-mindedness across different disciplines (physical, digital, human) and throughout the supply chain. Adhering to the standard will require new ways of thinking - even entirely new career fields.

"There is no way of doing BIM securely - you can only do it in a security-minded way," Paul says. "It involves the appointment of a new role, which I think will become a burgeoning profession, called the Built Assets Security Manager, who has got to identify that this plus that is greater than the sum of its parts."

10. National Post

CSIS tries to show it can be more 'accessible' with new Twitter account: 'Now it's your turn to follow us'

Wednesday, 13 July 2016

Byline: Stewart Bell

Ottawa - Canada's intelligence service posted its first Tweet on Wednesday, joining the Central Intelligence Agency and other secretive government organizations that have ventured into social media.

"Now it's your turn to follow us," the Canadian Security Intelligence Service wrote on its new @CSISCanada account. The handle @CSIS was already taken by the Centre for Strategic and International Studies.

Among the first to follow CSIS was the CIA, which joined Twitter in 2014 with the post, "We can neither confirm nor deny that this is our first tweet." The @CIA account is heavy on history rather than actual intelligence.

While CSIS already had a Twitter account for job openings, the new one appears to be an attempt to demystify the agency to Canadians who are sometimes wary of what it does in the name of national security.

"Speaking publicly on the nature of our work isn't always easy, but we want CSIS to be more accessible, and want to help the public understand more about our work," Director Michel Coulombe said in a statement.

Canada's signal's intelligence agency, the Communications Security Establishment, which has been Tweeting since April, welcomed CSIS to Twitter with what it called "some neighborly advice: 'password' is never a good password."

11. CTV Edmonton

'Now it's your turn to follow us', CSIS launches Twitter account

Wednesday, 13 July 2016

Byline: Julia Parrish

Edmonton - After more than 30 years, the Canadian Security Intelligence Service (CSIS) launched their first public social media account Wednesday.

In a Tweet sent out just before 9 a.m. MT, the organization's first tweet was sent out.

(Tweet from CSIS Canada: 'Yes, we're on Twitter. Now it's your turn to follow us'.)

The organization also released a statement from Michel Coulombe, Director of CSIS, saying the service "recognizes that a modern organization needs to communicate using modern means."

"A key element of the organization's vision is to communicate our role to Canadians, so they may attain a better understanding of CSIS.

Coulombe's statement went on to say: "Speaking publicly about the nature of our work isn't always easy, but we want CSIS to be more accessible, and want to help the public understand more about our work. Joining Twitter is one step in strengthening the dialogue with Canadians."

The account's initial Tweet was met with some ribbing online, with some users questioning whether the account was real, and another government organization issued their own response.

The official account for the Communications Security Establishment welcomed CSIS to Twitter, and offered some cheeky advice.

(CSE Tweet: 'Welcome to Twitter! Allow us to offer some neighbourly advice: "password" is never a good password!')

The service was officially established on July 16, 1984.

12. CTV.CA

CSIS joins Twitter: 'Now it's your turn to follow us'

Wednesday, 13 July 2016

Byline: Josh Elliott

Toronto - Here's one of the worst-kept secrets in the country: Canada's spy agency is on Twitter.

The Canadian Security Intelligence Service sent out its first tweet on Wednesday, urging Canadians to follow its new social media account.

"Now it's your turn to follow us," the tweet said.

Director of CSIS Michel Coulombe called it a way to be "more proactive" in helping the public understand the agency's role in keeping Canadians safe.

"Speaking publicly on the nature of our work isn't always easy, but we want CSIS to be more accessible, and want to help the public understand more about our work," Coulombe said in a statement on the CSIS website. "Joining Twitter is one step in strengthening that dialogue with Canadians."

13. Saudi Gazette

Kingdom among top progressive states in IT

Thursday, 14 July 2016

Byline: Staff Report

Riyadh - Saudi Arabia advanced to 33rd rank among 139 countries classified by the World Economic Forum as the top progressive states in the field of information technology and communication.

The Ministry of Communications and Information Technology said in a statement on Wednesday that according to the annual report of the World Economic Forum (https://www.weforum.org/reports/the-global-information-technology-report- 2016), the Kingdom has advanced two ranks in 12 months to reach 33rd position among 139 countries in terms of readiness to contain diverse networks of information technology.

The Kingdom came in the 8th place globally in terms of the efficiency in the use of information technology and communication by government and official bodies in the implementation of their work, and the extent to improve the quality of government services for the population in the information technology field.

It came in the 9th place globally in terms of the extent of the government's success in promoting the use of information technology and communication.

The Kingdom also ranked 15th in terms of broadband subscriptions for mobile computers per 100 inhabitants. It ranked 17th in the production of electricity (kilowatt/hour/per capita), and ranked 18th in the index of the quality of services being provided by the government in the field of internet.

This index deals with assessing the implementation of the government for internet services projects.

"The government is leading the way to increased networked readiness, promoting ICTs in the country," said the report.

The Global Information Technology Report 2016 features the latest iteration of the Networked Readiness Index (NRI), which represents a key tool in assessing countries' preparedness to reap the benefits of emerging technologies and capitalize on the opportunities presented by the digital transformation and beyond.

More particularly, the report assesses the factors, policies, and institutions that enable a country to fully leverage information and communication technologies (ICTs) for increased prosperity and crystallizes them into a global ranking of networked readiness at the country level in the form of the NRI.

Countries are assessed over four categories of indicators: (1) the overall environment for technology use and creation (political, regulatory, business, and innovation); (2) networked readiness in terms of ICT infrastructure, affordability, and skills; (3) technology adoption/usage by the three groups of stakeholders (government, the private sector, and private individuals); and (4) the economic and social impact of the new technologies. Whenever relevant, the Index looks at what the different actors in society, both private and public, can do to contribute to the country's networked readiness.

14. 45eNord.ca

Suivez les espions canadiens sur Twitter!

Wednesday, 13 July 2016

Byline: Journaliste maison

Ottawa - Le SCRS, l'agence canadienne de renseignement de sécurité, a souligné avec ironie le lancement de son compte Twitter en écrivant « Oui, on est sur Twitter. C'est maintenant à vous de nous suivre »...

?

Oui, on est sur Twitter. C'est maintenant à vous de nous suivre. https://t.co/dkaZg4b7OO

-- SCRS Canada (@scrscanada) 13 juillet 2016

Le Service canadien du renseignement de sécurité (SCRS) ou Canadian Security Intelligence Service en anglais (CSIS), est le principal service de renseignements du Canada.

Ses missions incluent le filtrage de sécurité, le terrorisme, la lutte à la prolifération des armes de destruction massive, l'espionnage et ingérence étrangère et les menaces pour la sécurité de l'information.

Le SCRS,dont les pouvoirs ont été accrus sous le règne des conservateurs, travaille à l'international en collaboration avec ses agences soeurs des États-Unis (CIA, FBI et NSA), de Grande-Bretagne (MI5), et d'Australie (les « five eyes »), ainsi que plusieurs autres pays.

Au plan national, le SCRS collabore avec le Commandement des Forces d'opérations spéciales du Canada (Forces canadiennes) et le Centre de la sécurité des télécommunications, tous deux sous le Ministère de la Défense nationale, ainsi qu,avec la avec la Gendarmerie royale du Canada, dont le ministère de tutelle est celui de la Sécurité publique.

Le directeur du Service canadien du renseignement de sécurité (SCRS), Michel Coulombe, en lançant le compte Twitter de l'agence, a déclaré « Le Service canadien du renseignement de sécurité reconnaît qu'une organisation moderne se doit de recourir à des moyens modernes pour communiquer. Un des éléments clés de la vision de l'organisation est de communiquer son rôle aux Canadiens pour qu'ils aient une meilleure compréhension de ses fonctions. »

Aix États-Unis, le compte Twitter de la CIA (Central Intelligence Agency), établi en 2014, a maintenant 1,43 Million d'abonnés qui suivent ainsi les activités de l'agence de renseignement américaine, et peuvent en outre poser des questions et obtenir des réponses.

« Il est primordial », a ajouté Michel Coulombe, »que le public comprenne le rôle souvent difficile que le SCRS joue pour assurer la sécurité du Canada et des Canadiens, et le SCRS doit s'efforcer de mieux l'en informer. Même s'il n'est pas toujours facile de parler publiquement de la nature du travail de ses employés, le SCRS veut être plus accessible et aider le public à mieux saisir son travail »

Et de conclure le patron de tous les espions canadiens en disant que « L'ouverture du compte Twitter est une des mesures prises pour renforcer le dialogue avec les Canadiens ».

Jakarta Post

Cyber Agency to be formed in August: Security Minister

Friday, 15 July 2016

Byline: News Desk

Section: general

Jakarta - The National Cyber Agency (BCN) is expected to be established in August 2016, Coordinating Minister for Political, Legal, and Security Affairs Luhut Binsar Pandjaitan stated.
"Probably, next month, the agency will be ready," Minister Pandjaitan said here, Thursday. The process of establishing the agency has reached its final stage, he added. The government had planned to set up the agency since 2015.

Earlier, Communication and Informatics Minister Rudiantara had stated that Minister Pandjaitan was coordinating to set up the agency.

The communication and informatics ministry has prepared the standardization process for the cyber agency in dealing with sectors, such as finance and banking, transportation, energy, and mineral resources. In the meantime, a cyber security expert recently said Indonesia urgently needs to establish the BCN.

Pratama Dahlian Persadha, former chairman of a team of the State Code Agency for Presidential Information Technology Security, said Indonesia was lagging behind neighboring countries, such as Malaysia and Singapore, in the area of cyber security.

"Singapore has already established a BCN since 2009, not to mention the United States, where President Obama has direct access to every matter related to cyber security," Pratama remarked.

Pratama, who is chairman of the Communication and Information System Security Research Center, said Indonesia is not like several European countries, with a small land territory and mono-ethnic nationality.

"Indonesia has several data on strategies and covert information, including about state secrets, which need to be safeguarded, to preserve the nation's pluralism and state integrity," he affirmed.

Currently, part of the data has been saved digitally. Without adequate protection, the data can become a potential threat, he pointed out.

"Later, the BCN's duty should be more than just to protect data. The main task of the BCN would be to secure Indonesia's cyberspace," he noted "The BCN should function on the similar lines as the armed forces in the cyber world," Pratama added.

Press Trust of India

Hafiz Saeed's Twitter account suspended

Friday, 15 July 2016

Section: general

New Delhi - The official Twitter account of Jamaat-ud-Dawa (JuD) chief Hafiz Saeed was suspended on Thursday.
The handle - @hafizsaeedlive was suspended by Twitter following complaints by Indian security agencies that it was being used to incite violence following the death of Kashmiri militant Burhan Wani in an encounter last week.

An accused in the 26/11 Mumbai attacks, Hafiz Saeed was seen earlier this week participating in a prayer meeting on Wani's death, along with Hizbul Mujahidren chief Syed Salahudeen.

On Wednesday night, Saeed launched an onslaught against India, following which the agencies approached Twitter to suspend his account.

Earlier too, Saeed's Twitter account was suspended following India's request. He created a new ID on Twitter in December 2015. Saeed reportedly has one more account which is maintained by his cyber team.

Arab News

'Spy tool' concerns as Pokémon mania grips Kingdom

Friday, 15 July 2016

Byline: Mohammed Al-Sulami

Section: general

Jeddah - As the global obsession with smartphone game Pokémon Go intensifies, many have taken to Twitter and social media sites to warn about the impact of the game on social life and the security of citizens and the country.
Pokémon Go works via GPS technology, using the phone camera to search for Pokémon characters and hunt them down.

While some claim the game could be a breach of privacy for users and their mobile phones, more serious concerns revolve around the possible threats to national security, as in the course of playing the game, sensitive sites, such as security buildings, houses of worship, foreigners' residential complexes, embassies, consulates and others may be photographed.

Many observers and commentators on social media warn that the game, like others, may also be penetrated by terrorist organizations who use it to contact youths and recruit them.

They are calling on authorities to closely examine such games and their potential danger to national security, as well as the possibility that they may become tools for terrorists, enemy countries or spy agencies wishing to collect data and information about sensitive locations.

Nayef Al-Subaie, an expert in technology, says the danger of these games is that they use live stream technology connected to the Internet and GPS, while those who play the game have limited understanding of where the stream is uploaded or what sites they may be led to during the game, "potentially embassies, consulates, military installations, oil refineries and our cities".

Such images may be used by foreign organizations, as was the case with the Baqeeq refinery, which was monitored by Al-Qaeda and attacked on Feb. 29, 2006, he said.

Naser Al-Qahtani, an electronic security expert, said these games can be easily accessed and used to spy on individuals, as well as infected with viruses. They can collect the largest possible amount of information and images from users around the world.

Information security experts have issued reminders that Saudi Arabia is constantly subjected to a large number of electronic attacks due to its special military, security and economic strength, which makes the game, and others of its kind, a cause for concern.

Hamed Al-Haddad, a citizen, says security authorities must intervene immediately to ban this game in the Kingdom until it is properly studied to identify any potential dangers, especially to society or the national security.

Other concerns about the game, says Masoud Al-Ali, are that it requests links to the users' personal information and e-mails, and its highly addictive nature causes users to lose touch with their surroundings and reality, and pay no attention to potential risks.

The game has caused global hysteria in the past few days, but it has yet to be introduced to the Arab markets. Saudis, however, were able to upload the game by using "proxies" and relocating to countries where the game already exists.

Some parents warn about the game, which pose potential hazards to their children because characters sometimes appear in dangerous places, such as the middle of a road or in suspicious sites. Some even hunt down the Pokémon characters using bicycles and cars, which may lead to accidents.

Ottawa Citizen

Aerospace firm owner sentenced for hacking

Friday, 15 July 2016

Byline: David Pugliese

Section: general

Ottawa - A Chinese man who ran an aerospace firm with offices in British Columbia has been sentenced to nearly four years in jail for stealing confidential information on a U.S. military transport aircraft and the F-35 stealth fighter.
Su Bin had pleaded guilty in federal court in Los Angeles to helping two Chinese military hackers. Among the targets of the hacking efforts was information on the U.S. F-22 and F-35 stealth fighters as well as Boeing's C-17 transport aircraft, which is also used by the Canadian Air Force.

In a plea agreement, Su admitted to conspiring with the two hackers in China to gain unauthorized access to computer networks in the U.S. between October 2008 and March 2014.

Su travelled to the U.S. on 10 occasions during that period, according to court documents.

He was arrested in Richmond, B.C., in June 2014 and a Canadian court ordered Su's extradition to the U.S. in September 2015.

The 51-year-old has been sentenced to three years and 10 months in jail. He was also fined $10,000.

Su, also known as Stephen Su and Steven Subin, is the owner of the aviation firm Lode Technology. Besides the office in Canada, it also had locations throughout China.

"Over the course of years, this defendant sought to undermine the national security of the United States by seeking out information that would benefit a foreign government and providing that country with information it had never before seen," U.S. prosecutor Eileen Decker said in a statement.

Su did not carry out the actual hacking, which was done by his two co-conspirators, both members of the People's Liberation Army in China.

Instead, Su's role was to identify technical data that the hackers could target, according to the charges filed by Decker.

Su also admitted translating the stolen information, which was then offered to Chinese aviation firms.

The theft of information on the C-17 aircraft made "important contributions to our national defence scientific research development," one of the Chinese military officers wrote in an email intercepted by the U.S.

itWorldCanada.com

Whistleblower Edward Snowden to keynote Toronto conference

Friday, 15 July 2016

Byline: Brian Jackson

Section: general

Toronto - The man that says he lives on the Internet will be the showcase speaker at SecTor, a Toronto-based security conference this year.
Edward Snowden, the former CIA employee and government contractor that leaked classified documents about a mass surveillance operation run by the National Security Administration (NSA), will be appearing at the conference via a video link from Russia, where he's been living under asylum since 2013. SecTor will be Snowden's first and only commercial conference appearance in North America this year, conference organizers say.

"Edward Snowden is not only one of the biggest names in cybersecurity, but his unique situation and cybersecurity experiences also make him one of the most important and influential," said SecTor co-

founder Brian Bourne in an email announcement. It's important to have him "appear in front of the Canadian IT community, so we engage and inspire today's security professionals and don't fall behind."

Snowden has been said to make his living off of speaking fees since fleeing the U.S. and leaking state secrets. Snowden's lawyer Ben Wizner once told the New York Times the fees can sometimes exceed $10,000 per appearance.

Snowden has also made appearances at conferences and gallery events via telepresence robot BeamPro, essentially a raised iPad on two wheels. He first used the robot at a TED talk in 2014.

Beyond NSA's clandestine mass surveillance operations that were leaked by Snowden, Canada's Communications Security Establishment (CSE) has also been the subject of some of his classified leaks. He's also said that Canada's intelligence gathering operations have the "weakest oversight" among western nations.

A Hollywood movie, directed by Oliver Stone and titled Snowden, is based the whistleblower's life and focuses on his choice to reveal state secrets.

SecTor begins in Toronto Oct. 17.

Globe and Mail

Man who stole military data sentenced

Friday, 15 July 2016

Byline: Mahnoor Yawar

Section: general

Ottawa - A Chinese citizen living in Vancouver who admitted helping Chinese military officers hack into the computer networks of U.S. defence contractors to steal classified information has been sentenced to 46 months in prison.
Su Bin, a 51-year-old multimillionaire businessman working in aviation, was convicted of participating in a years-long conspiracy to steal military technical data, including schematics related to Boeing's C-17 military transport plane as well as F-22s and F-35s.

According to a plea agreement released by U.S. prosecutors, Mr. Su admitted that he acted as a data scout to access sensitive military data on servers for U.S. defence contractors and sent relevant

information to China. He said he was motivated by the prospect of "commercial advantage and private financial gain."

In addition to the prison term, Mr. Su was ordered to pay a $10,000 (U.S.) fine by a District Court judge in Los Angeles for his part in the criminal hacking conspiracy, which took place from October, 2008, to March, 2014, while he resided in Canada with his family and took frequent trips across the border. In August, 2012, he bought a $2-million home in Richmond, B.C., with his wife.

"Su Bin's sentence is a just punishment for his admitted role in a conspiracy with hackers from the People's Liberation Army Air Force to illegally access and steal sensitive U.S. military information," John Carlin, the assistant attorney-general for U.S. National Security, said in a statement.

The sentencing is the first time the U.S. Department of Justice has highlighted allegations that Mr. Su and two co-conspirators e- mailed reports addressed to the headquarters for the Chinese People's Liberation Army, previously reported by The Globe and Mail in February.

The Globe also revealed that court filings in Canada described the co- conspirators as "Chinese military officers" who sent Mr. Su pictures of themselves with identifiable names and ranks. U.S. prosecutors have not charged or publicly identified these individuals.

Charges against Mr. Su were first announced in 2014, leading to his arrest in Canada on a U.S. warrant. He ultimately waived extradition to the United States, where he pleaded guilty to one count of conspiring to gain unauthorized access to a protected computer and to violate the Arms Export Control Act. As part of his plea deal, he negotiated a maximum five-year prison sentence with prosecutors.

When Mr. Su went to the United States, Canadian immigration authorities withdrew a bid launched to revoke his permanent resident status. Government officials could not be reached for comment on whether he will be authorized to return to Canada at the conclusion of his U.S. prison term.

Earlier this year, the Chinese government denied claims that a Canadian man detained in China was charged with espionage as retribution for proceedings against Mr. Su. Kevin Garratt and his wife, Julia, were arrested near the North Korean border, where they ran a coffee shop and did humanitarian work, weeks after Mr. Su's arrest in Vancouver. Ms. Garratt was released on bail in February, 2015, but has been barred from leaving the country or speaking to the media.

The Chinese government has repeatedly denied any involvement in hacking, but Mr. Su's cyber espionage efforts have been lauded by state-controlled media in China.

"On the secret battlefield without gunpowder, China needs special agents to gather secrets from the U.S. As for Su, be he recruited by the Chinese government or driven by economic benefits, we should give him credit for what he is doing for the country," said a March editorial in the Global Times, a publication with significant ties to the ruling Communist Party.

The editorial was headlined: "Su Bin deserves respect whether guilty or innocent."

With reports from Colin Freeze and Nathan VanderKlippe

Saudi Gazette

From the dark web to the 'open' web: What happens to stolen data

Friday, 15 July 2016

Byline: Michael Kassner

Section: general

Riyadh - The online black market is becoming a well-oiled and lucrative machine, thanks to the massive amount of stolen data flowing through the underground.
In any data breach, it's particularly interesting to note the number of individuals whose personal information was compromised. Case in point, the title of Zack Whittaker's June 9, 2016 article on TechRepublic sister site ZDNet: A hacker claims to be selling millions of Twitter accounts.

He writes, "A Russian seller, who goes by the name Tessa88, claimed in an encrypted chat on Tuesday to have obtained the database, which includes email addresses (and sometimes two per person), usernames, and plain-text passwords."

As compelling as that is, Thomas J. Holt, an associate professor of criminal justice at Michigan State University, is far more curious about what happens to the stolen data after the breach occurs. Holt's interest hearkens back to 2014 when he and fellow researchers made an intensive study of the underground path of stolen credit card information.

Holt recently decided to augment that information in his commentary on The Conversation titled Buying and selling hacked passwords: How does it work? "What happens after a breach?" asks Holt in the article. "What does an attacker do with the information collected? And who wants it, anyway?" He begins to answer these questions by saying more often than not, stolen data is sold via online black markets.

In what might be a surprise to some, Holt believes those selling stolen data use underground web forums remarkably similar to above ground retailers like Amazon--buyers and sellers can even rate each other and review previous negotiations (more on this later). Holt points out some of the differences.

As for those interested in buying stolen data, that happens in one of two places. "Most of the black markets operate on the so-called 'open' web, on sites accessible like most websites, using conventional web browsers like Chrome or Firefox," writes Holt. "They sell credit and debit card account numbers, as well as other forms of data including medical information."

Holt continues, "A small but emerging number of markets operate on another portion of the internet called the 'dark' web. These sites are only accessible by using specialized encryption software and browser protocols that hide the location of users who participate in these sites, such as the free Tor service."

Due to the nature of the product, sellers make every effort to remain incognito when it comes to receiving payments. The internet has been a big help in this regard. "Sellers accept online payments through various electronic mechanisms, including Web Money, Yandex, and Bitcoin," explains Holt. "Some sellers even accept real-world payments via Western Union and MoneyGram, but they often charge additional fees to cover the costs of using intermediaries to transfer and receive hard currency."

Holt next mentions that payments are made up front, with the release of stolen data taking a few hours to a few days. And, paying up front is why buyers want to know how the underground market rates the seller. If a deal goes wrong, it is doubtful either party will be calling the authorities.

"The parties operate anonymously, but have usernames that stay the same from transaction to transaction, building up their reputations in the marketplace over time," adds Holt. "Posting reviews and feedback about purchase and sale experiences promotes trust and makes the marketplace more transparent."

Holt says those who buy stolen information on underground black markets try to make as much money as quickly as possible. The bad guys do that by: Engaging in money transfers to acquire cash Buying goods with stolen credit card numbers Holding people's internet accounts (i.e., social media logins) for ransom Using the data to craft more targeted attacks on victims Padding legitimate account reputations using fake followers

Holt estimates the criminal buyers were able to net between $1.7 million and $3.4 million USD from 141 purchases on underground markets. "These massive profits are likely a key reason these data breaches continue," mentions Holt. "There is a clear demand for personal information that can be used to facilitate cybercrime and a robust supply of sources."

Holt points out that if the rating systems could not be trusted, buyers would more than likely refrain from providing funds before receiving their purchase. "Some computer scientists have suggested the approach [rigging the rating system] could disrupt the data market without the need for arrests and traditional law enforcement methods," explains Holt.

As to the success of the underground black markets, as Holt said earlier, they will continue to be successful as long as there are products to sell, and that seems assured with headlines like this from ZDNet: LinkedIn user? Your data may be up for sale.

Fars News Agency

Iran Unveils Home-Made Hi-Tech Batteries for Military, Industrial Purposes

Friday, 15 July 2016

Section: general

Tehran - Iran on Wednesday unveiled 7 home-made hi-tech military and 19 industrial batteries in a ceremony participated by First Vice-President Eshaq Jahangiri and Defense Minister Brigadier General Hossein Dehqan.
During the ceremony held in Tehran today, also the production line of hi- tech MF batteries and a CHP power plant with the capability of electricity and heat-generation were inaugurated.

Also today, the Iranian defense ministry plant which produces lithium batteries started production of batteries for bicycles, electric motorcycles, mobile cell phone chargers and computers.

Last month, the Iranian defense ministry unveiled three other home-made technological achievements.

The achievements include 1-MW national GPS system, robotic vacuum plasma coating and vacuum arc remelting furnace which have all been designed and built by Iranian researchers at Malek-e Ashtar University.

Elaborating on the new achievements, General Dehqan said that the 1-MW national GPS system is a reliable substitute for the GPS which can be used in critical conditions.

Also, the robotic vacuum plasma coating is one of the laboratorial equipment used in different research processes, turbines and jet engines that has the capability to resist high temperatures, he added.

General Dehqan also said that the vacuum arc remelting furnace can be used for melting and purification of titanium, remelting the super alloys and special steels and can be operated both manually and automatically.

In a relevant development in February, General Dehqan unveiled 4 products of the defense industry and inaugurated the production line of a key medicine that fights the effects of chemical elements.

The new achievements included 'Pars Kam' detector system that tracks chemical substances dangerous to health, a new system that can detect explosives and drugs, anti-strike and explosion-proof polymer coatings, a new generation of NBC protective clothes based on Travagzin membranes, as well as the production line of Obidoxime chloride medicine that fixes the effects of chemical substances on the body.

Speaking to reporters, Dehqan said the defense ministry will continue to design, invent and produce modern equipment and products for protection of its armed forces.

Also in February, the defense ministry had also unveiled 7 national geographic projects.

The projects included a remote defense lab - national spectral sensing, first unmanned smart hydrography Fajr 1 (Dawn 1), coastal development of Makran, production line of digital marine maps, digital geomorphology maps, magnetic marine measuring systems, climate database, and geographic data production line using drone images.

Minister Dehqan said, "The Fajr 1 hydrography is a remote control system, able to transmit data and image, GPS, measure depths, advance multibeam systems, and side scan sonar and radar data."

On the applications of digital maps of geomorphology system, he said they can be used in scientific and research projects, as well as in geography, environment, construction, development, agriculture, defense logistics, civil defense, and military affairs.

According to Dehqan, the database on climate will be used for military and defense purposes, including in tarmacs, military drills, and troop deployments.

Toronto Star

Federal documents could mask the scope of actual surveillance activities

Friday, 15 July 2016

Byline: Alex Boutilier

Section: general

Ottawa - "Clear gaps" in how the federal government reports invasive surveillance practices may hide the true scope of police activities, according to documents prepared for Canada's privacy watchdog.

Although the number of authorized wiretaps has "plummeted" since 2002, a January briefing for Privacy Commissioner Daniel Therrien suggests those numbers may mask police surveillance practices.

"It would be erroneous to infer from the drop in overall warrants issued that surveillance is affecting fewer individuals," reads the document, obtained under access to information law.

"While federal authorities issued just over a hundred surveillance warrants last year (2014), they issued 792 notifications of surveillance to individuals previously targeted. From this, one can conclude more and more individuals are being named as targets in a warrant application.

"With a single warrant from the Federal Court (police) may list dozens of individuals for surveillance targeting."

Public Safety is required to issue a report each year about the number of warrants sought to put individuals under surveillance - "wiretap" warrants that allow police extraordinary powers to keep tabs on individuals.

But police aren't just bugging the phones of bad guys anymore. New technology allows law enforcement agencies to conduct surveillance on a much wider scale.

The documents note that the decline in warrants "must also be kept in perspective against" newer surveillance powers that don't have to be publicly reported, including production orders for account information, warrants for GPS location devices and requests for "metadata."

Canada has also seen confirmed uses of "Stingray" technology, a device, called an IMSI catcher, that simulates a cellphone tower to force any mobile device in the area to connect to it. A recent Vice News investigation reported the RCMP has used IMSI catchers in public places for more than a decade, citing court documents.

The Star requested an interview with both Therrien and Public Safety Minister Ralph Goodale for this article. Neither was available Wednesday or Thursday.

But in an emailed response to the Star, a spokesman for Goodale said the minister is open to changing the system.

"Reporting is an important component of Canada's system accountability for security agencies," Scott Bardsley wrote.

"We're open to consideration in this review (of national security oversight) of how to improve these elements to better achieve our two objectives (of) ensuring that our police and security agencies are being effective ... and safeguarding the values, rights and freedoms of Canadians in a plural, open, democratic society."

Lisa Austin, a law professor at the University of Toronto specializing in privacy issues, said calls globally for transparency about police surveillance have increased, not just for wiretap warrants, but for any extraordinary powers for law enforcement snooping.

But it's not about pitting privacy rights against cops legitimately trying to do their jobs, Austin added.

"It's not about preventing access to the information that the state needs to pursue law enforcement or national security," Austin said Wednesday.

"I dislike it when the debate is about privacy versus law enforcement ... because the law has never been that. It's always been about balancing and accountability."

104 Number of applications or renewals for surveillance warrants in 2014, the most recent year Public Safety has released data.

0 Number of applications not approved in Federal Court.

45 Number of surveillance requests for drug trafficking, the most frequent offence where surveillance is sought, compared to 30 for terrorism.

14 Number of police convictionsin cases where surveillance was deployed.

The Advertiser

Surge in cyber sleuths

Friday, 15 July 2016

Byline: Lauren Ahwan

Section: general

Canberra - Students just halfway through their cyber security training are being snatched up by employers as the world struggles to meet the need for increased computer vigilance.
The demand for cyber security workers is expected to increase to six million globally by 2019, with a projected shortfall of 1.5 million workers, says the world's largest security software company Symantec.

University of NSW computer security, cybercrime and cyber terror associate professor Richard Buckland says employers are paying top dollar for workers - even those that are yet to complete their training. "At the moment, the shortage is so big that I don't think people need the piece of paper (qualification)," he says.

"I have (employers) coming up to me and saying, 'Give me your best students'. Well, I can't even give them my worst students because they all have jobs already and they're only in their second year (of a three or four year degree).

"Students who have just finished their first year are being snaffled up by the NSA (National Security Agency) or Google or Microsoft in the US.

"Some are working locally for the big banks." UNSW and the Commonwealth Bank recently launched a $1.6 million cyber security education and research centre, which includes a free online course that has already attracted 15,000 enrolments.

Box Hill Institute of TAFE offers a one-year Certificate IV in Cyber Security - believed to be the first vocational course in cyber security on offer in Australia.

Career changer Joseph Speziale, 31, is a marine engineer and one of the first to enrol in the vocational program."The thing I like most about cyber security is that it is not just limited to keeping your work computers safe - it's about making sure someone's phone won't do any damage, someone's laptop doesn't have a bug, but at the same time not restrict people from doing their job," he says.

NPR

NSA Boss Says U.S. Cyber Troops Are Nearly Ready

Friday, 15 July 2016

Byline: Victoria Mirian

Section: general

Washington - The director of the National Security Agency says his first few dedicated cyber troops will be operational by early fall but the nation can't wait for the full unit to be ready.
The military's Cyber Mission Force, which will eventually contain 6,200 people split into 133 teams, is the largest single unit dedicated to operating in computer networks. It's intended to both attack and defend computer systems around the world.

The U.S. Cyber Command ordered the creation of this dedicated cyber unit in 2012, and Adm. Michael Rogers, who is the director of the NSA and the Cyber Command, says the unit will reach what he called initial operating capability by Sept. 30.

"We find ourselves in a situation a little unusual in the military arena," Rogers told a crowd at the National Press Club Thursday. "As soon as we get a basic framework, we are deploying the teams and putting them against challenges."

Rogers likened it to sending a fighter squadron into action that only had five of its 24 aircraft. Because demand for cybersecurity exceeds capacity, Rogers said, the mission force will be put to work before the agency has time to finish building it.

He said he's trying to build the force, made up of both military personnel and civilians, even as his agency faces budget cuts. He said it'll be fully capable by Sept. 30, 2018.

"I just always feel like we're in a race to make sure we are generating capacity and capability, and that we are doing it faster than those who would attempt to do harm to us," Rogers said. "As you watch what opponents are doing, as I'm watching behaviors out on the net, it's almost visceral."

According to the Department of Defense, about half of the Cyber Mission Force teams will be assigned to protecting military networks from cyber intrusions. Another 20 percent will be dedicated to combat missions. About 10 percent will be assigned to national mission teams to protect the country's infrastructure, and the remaining fifth will be assigned to "support teams."

Rogers said he wants cyber to be integrated into the military and become a tool available to policymakers and operational commanders, as long as it's used legally. He said he's tried to stay mindful about the need to balance protecting the privacy and rights of individuals with the government's duty to protect citizens.

"I always tell [our workers], 'Don't ever forget that at the end, we're dealing with a choice that some human made on a keyboard somewhere else in the world,' " he said. "There was a man or woman on the other end of this."

SC Magazine

Maxthon browser vulnerable to Chinese cyberespionage and MitM attacks

Friday, 15 July 2016

Byline: Robert Abel

Section: general

New York - Researchers at Fidelis Cybersecurity and Poland-based Exatel found that the Maxthon browser sends sensitive data to a browser in Beijing and is prone to man-in-the-middle (MitM) attacks. The browser regularly sends a small encrypted file containing the user's entire browsing history, including Google searches, queries and a complete list of software installed on the user's computer, all without the prior authorization of the user, according to a recent report released by the firms.

The file is created as part of the Maxthon User Experience Improvement Program (UEIP), which is designed to understand users' needs to deliver better products and services. The program is supposed to be voluntary, but researchers found the information was being sent regardless of the user's decision to opt in or out of the program.

A Maxthon customer who opted out of the program noticed the file being sent and asked a representative on the company's official browser forum for clarification of the file's contents, to which the representative responded that the firm will "only collect basic data such as browser start condition and not the data that involves the user's privacy," according to screenshot of the conversation in the report.

"What adds irony to the whole matter, is that the creators of the browser inform on their website that it was created with the thought of ensuring security and privacy to the users in the light of scandals related to violation of the privacy by the American National Security Agency (NSA)," the report said.

Researchers said many users appear to be fond of the browser specifically because the creators don't share data with the NSA.

In addition, due to an error in the cryptographic architecture, the data which is transmitted may be intercepted and decrypted by any potential attacker, researchers said.

Using this information, if attackers obtained the user's email they could send a message, authenticated by its content, containing an attachment armed with a remote code execution exploit that could compromise the user's device, the report said.

The data collected could be analyzed for identifying targets based on the URLs users browse and applications on their devices which can be cross referenced with a vulnerability database to learn what sort of spearphishing attacks would work against them, Fidelis Cybersecurity Chief Security Officer Justin Harvey told SCMagazine.com via emailed comments.

"I personally believe it is possible that this information was being collected as a means of surveillance, for both foreign and domestic use cases," said Harvey.

Harvey also said that it's illegal to bypass the "Great Firewall" domestically in China and that people looking to use Facebook, Twitter, Google, or any other banned sites, need to use forbidden VPNs. The browser also provides a way for China to monitor citizens' Internet usage overseas, he added.

"Regardless of which network is being used, the way that the Maxthon browser is set up today, it will send their browsing history back to Maxthon's HQ," Harvey said. "How could the Chinese government not have access to this treasure trove of information?"

The browser is available for all major platforms in more than 50 languages and it is unclear how long Maxthon has been collecting this information.

New York Times

Limits on Privacy Board Face Challenge in Senate

Friday, 15 July 2016

Byline: Charlie Savage

Section: general

Washington - A leading Democrat in Congress is pushing back against an effort to impose new constraints on a civil liberties watchdog agency that investigates the nation's security programs. The agency, the Privacy and Civil Liberties Oversight Board, is a bipartisan five-member panel that Congress created after a recommendation by the commission that investigated the Sept. 11, 2001, terrorist attacks. Its members and staff have security clearances and a mandate to investigate government practices that affect individual rights.

The Senate and House intelligence committees have increasingly sought to impose new rules on the board's work, including a series of proposals in a pending intelligence authorization bill. But in a letter this week to Senate Intelligence Committee leaders, Senator Patrick J. Leahy, the top Democrat on the Judiciary Committee, demanded that the proposals be withdrawn.

Since the independent board began fully operating three years ago, it has produced a high-profile report about the once-secret National Security Agency program that collected bulk records of Americans'

phone calls. It called the program ineffective and illegal and said it should be shut down. Congress later did so by enacting the U.S.A. Freedom Act.

The oversight board also issued a report that brought to light new details about how the warrantless surveillance program authorized by the FISA Amendments Act worked. It is currently scrutinizing programs that operate under Executive Order 12333, which sets rules for espionage activities that Congress has left unregulated by statute.

In the letter, obtained by The New York Times, Mr. Leahy, Democrat of Vermont, described the provisions as "completely unacceptable" and "misguided." He deplored what he portrayed as an emerging pattern of efforts by the intelligence panels to undermine the oversight board's independence and authority. He also said any proposed changes to the board should go through the Judiciary Committee.

The dispute traces back to last spring, when the chairman of the oversight board at the time, David Medine, wrote an essay proposing that its mandate be broadened to also examine proposed targeted killing operations. In response, the two intelligence committees added a provision to the annual intelligence authorization law last year that barred the board from addressing covert activities.

The versions of this year's intelligence bill by the House and Senate committees would go further. For example, the Senate bill would limit the oversight board's jurisdiction to Americans' rights, not the privacy of foreigners.

That proposal comes at a time when the Obama administration has highlighted the privacy board's role in negotiations over a recently completed trans-Atlantic agreement for handling private data amid concern in Europe about using internet and technology companies based in America. Those concerns came after leaks by the former intelligence contractor Edward J. Snowden about National Security Agency surveillance programs.

In addition, the House version would change budgeting rules for the oversight board so that it would have to shut down if Congress did not act every year to reauthorize it to spend money. The versions in both chambers would require the board to tell the intelligence committees and the heads of intelligence agencies what it is investigating.

Mr. Medine, who stepped down as the board's chairman on July 1, said that the proposed changes were unwise in light of what was exposed by the Snowden leaks.

"The lesson from Snowden is how critical it is to have democratic debate and oversight of our intelligence community to give it credibility both nationally and internationally," he said. "Now we have the intelligence committees trying to undercut that and push the intelligence community back into the shadows again."

Senator Ron Wyden, Democrat of Oregon and an Intelligence Committee member, has also objected to provisions in the bill that would weaken the oversight board, as has a coalition of technology companies and privacy advocates.

The chairman of the Senate Intelligence Committee, Richard M. Burr, Republican of North Carolina, did not respond to a request for comment. But the chairman of the House Intelligence Committee, Representative Devin Nunes, Republican of California, pushed back.

"As is clear from the text of the bill, the Intelligence Authorization Act does not undermine Pclob in any way -- it simply establishes mechanisms to keep Congress fully informed of what the board is doing so Congress can exert proper oversight," Mr. Nunes said in a statement. Pclob is an acronym for Privacy and Civil Liberties Oversight Board.

He also portrayed the fear that Congress might not act each year to authorize the oversight board as "simply false," saying it could do so in a spending bill even if the annual intelligence authorization bill failed.

But Democratic leaders signaled openness to changing the bills. Senator Dianne Feinstein of California, the vice chairwoman of the Intelligence Committee, said in a statement, "We're aware of Senator Leahy's letter, and I'm happy to work with him to resolve his concerns." And Representative Adam B. Schiff of California, the top Democrat on the House Intelligence Committee, said he shared Mr. Leahy's concern.

Washington Free Beacon

State Department Farms Out Counter-ISIS Messaging Abroad

Thursday, 14 July 2016

Byline: Bill Gertz

Section: general

Washington - The State Department's latest effort to counter Islamic State propaganda and recruitment is relying on foreign states for strategic messaging, according to the department's public diplomacy official.
Richard A. Stengel, the undersecretary of state for public diplomacy, testified to Congress that the Obama administration believes other countries can better deal with terrorist information operations than the United States. He asserted that U.S. government propaganda is helping recruit terrorists.

"Our strategy is informed by a core insight: we are not always the best messengers for the message we want to deliver," Stengel told the House Foreign Affairs Committee on Wednesday. "Public statements from U.S. government officials condemning ISIL can easily be used by the enemy as a recruitment tool."

The latest approach to countering ISIS propaganda is the mission of the State Department's new Global Engagement Center, created in March.

The center replaced the troubled Center for Counterterrorism Communications earlier this year.

A six member panel of experts from the tech industry reviewed the operations of that center and concluded in December that the U.S. government should not be engaged in information operations against the Islamic terror group. The panel said it was concerned that the center lacked credibility in the Muslim world.

Critics contend that allowing foreign states, including Muslim majority countries, to take the lead in counter-terrorism messaging will result in promoting other forms of radical Islam, such as the Saudi variant known as Salafism, or the Egyptian-origin extremism of the Muslim Brotherhood.

President Obama in 2011 signed a secret directive that outlined U.S. policies to support the Muslim Brotherhood as an ideological alternative to al Qaeda, according to a State Department official.

Patrick S. Poole, a counterterrorism expert, criticized the State Department counter-ideology program as ineffective. The Center for Strategic Communications was a "disaster" and may have actually "legitimized terrorism," he said. Now, the new center has farmed out the mission to foreign states, Poole said.

"So basically we have foreign nationals running our information operations," Poole said. "It's an embarrassing testament to how ill-conceived and poorly executed the State Department's efforts have been under the Obama administration."

Stengel described the new counter-ISIS soft power initiative as "partner-driven messaging."

"Instead of direct messaging to potential ISIL sympathizers, much of our work focuses on supporting and empowering a global network of partners--from NGOs to foreign governments to religious leaders--who can act as more credible messengers to target audiences," he said.

Ultimately, Stengel said long-term success would result in a media environment "that does not require U.S. government messaging at all, because NGOs, local governments, partners, and credible voices are effectively drowning out ISIL's message of hate."

In the short term, the number of foreign fighters joining ISIS is declining sharply and media and social media activity by the terror group also has diminished.

A key focus is on what is called the Sawab Center, in Abu Dhabi in the United Arab Emirates, a Persian Gulf state, where U.S. officials work with Emiratis. So far nine social media campaigns using victims of terrorism and defectors to speak in favor of what Stengel said was "national pride."

The campaigns have averages of 125 million views on social media.

The Abu Dhabi center is being bolstered with similar "messaging centers" in Jordan, Nigeria, and Malaysia.

The center is using big data analytics to measure social media activity.

According to Stengel, anti-ISIS content online outnumbers pro-ISIS content by a ratio of six to one.

Under U.S. government prodding, Facebook and Twitter have been working to eliminate ISIS content and users from their services.

However, Stengel acknowledged that as terrorists are driven off of platforms like Twitter and Facebook, they are moving to new and more difficult to counter platforms, like Telegram, a cloud-based messaging and communications service that uses encryption.

Despite the signs of messaging progress, ISIS Islamic terror ideology is spreading to other parts of the world, Stengel said.

Committee Chairman Rep. Ed Royce, (R., Calif.) told the hearing the Internet is "awash" in ISIS propaganda, including gruesome videos of beheadings and other violent acts by ISIS terrorists.

Operating globally, ISIS operates a "virtual caliphate" to recruit members and propagandize.

"Using popular social media sites, ISIS can reach a global audience within seconds," Royce said.

Instead of urging fighters to travel to Syria and Iraq, ISIS is now telling overseas supporters to conduct attacks locally.

According to Royce, "more and more, the virtual caliphate is calling on its followers not to go to Syria, Iraq or Libya and take up arms--but to attack where they are at home. Orlando is a grim example of that."

An Islamic terrorist killed 49 people at an Orlando nightclub, pledging loyalty to the Islamic State during the attack.

ISIS had announced in June that the observance of Ramadan would be a time of global attacks in the United States and Europe. The Obama administration issued no warnings and took no additional security measures until after the Orlando shooting.

"Time is of the essence. If we don't come to grips with the virtual caliphate now, this struggle against Islamist terrorism will become more challenging by the day," Royce said.

Analysts say the Obama administration counter-ISIS ideology program has been hampered by the president's pro-Islam sympathies and his refusal to identify the threat from terrorism as based on radical Islam.

The president last month defended his reluctance to identify violent extremism as derived from Islam. "Calling a threat by a different name does not make it go away. This is a political distraction," he said.

However, other counterterrorism analysts say unless the nature of the terrorist threat is properly understood, efforts to defeat the threat will not be successful.

Under Obama foreign and security policies, Islamic terrorism has evolved from al Qaeda-style extremists conducting mass casualty attacks to more violent and deadly Islamic State- style attacks aimed at seizing and holding territory and then expanding both regional and globally.

Bloomberg View

Why the U.S. Pretends Drone Strikes Are Secret

Thursday, 14 July 2016

Byline: Eli Lake

Section: column

Column - One of the absurdities about the war on terror is that drone strikes are almost always highly classified by the U.S. government. It's hard to think of a more conspicuous state secret than a pilotless aircraft turning its target into a fireball. And yet, until recently, the Obama administration was reluctant to talk about this publicly in much detail.
This is starting to change. In May, President Barack Obama himself acknowledged the U.S. drone strike that killed Taliban leader Mullah Akhtar Mohammed Mansour. The acknowledgement was significant because he was killed in southwestern Pakistan, a country the U.S. does not consider an active combat

zone. Earlier this month, the White House released data for the first time on civilians it estimates have been killed in drone strikes outside of combat zones As one U.S. intelligence official told me Wednesday, the government is beginning to push the envelope on how much it can discuss about its drone strike operations in countries where the U.S. does not acknowledge the war it's fighting against al Qaeda and the Islamic State.

All of this openness at the end of Obama's second term is welcome. But it's fair to ask, what took so long? On Wednesday, CIA director John Brennan provided a part of this answer: The U.S. operates with the consent of governments where these strikes are happening. There's a catch though. "Sometimes these governments do not want to trumpet that cooperation and they want to keep it quiet," Brennan said. "But I will just caution people to think the United States just goes into airspace abroad without engaging with foreign governments."

We knew from sources like the diplomatic cables disclosed in 2010 by Wikileaks that some countries have acknowledged privately that they lie to their own populations about this issue. One such cable recorded Ali Abdullah Saleh, then president of Yemen, telling General David Petraeus, "We'll continue saying the bombs are ours, not yours."

Nonetheless, it's important Brennan went on the record about this. On the one hand, the request from foreign governments for this secrecy is understandable. None of these leaders would want to admit a super power was operating in his territory. This is particularly true in the Islamic world, where America and its drones are perceived by many as the tip of an imperial spear.

But Americans pay a price for this diplomatic discretion. It means an active American war in Libya, Pakistan, Somalia and Yemen is largely ignored in the public debate. When the U.S. finally does release its own information about these fields of battle, the delay raises suspicions. Many outside groups said the civilian casualty numbers released this month were too low to be believed.

Finally though, the U.S. does a disservice to the counterterrorism partners who requested the secrecy in the first place. The people in these countries know who is flying the drones. By pretending otherwise, their leaders forgo the chance to make the public case for U.S. airstrikes. Eventually that lie will catch up with even the most discreet dictators and threaten the quiet alliance that all this secrecy was supposed to protect in the first place.

Le Figaro

Daech confirme la mort d' « Omar le Tchétchène »

Friday, 15 July 2016

Byline: Thierry Portes

Section: general

Non identifié - Annoncée en mars comme « probable » par un responsable du Pentagone, qui l'avait reliée à un bombardement américain dans le nord-est de la Syrie, la mort d' « Omar le Tchétchène » , un important chef militaire de Daech d'origine géorgienne, a été confirmé jeudi par l'organisation terroriste.

The Hill Times
CSIS joins Twitter, hilarity ensues
Wednesday, 20 July 2016

The Canadian Security Intelligence Service (CSIS) started up a Twitter account last week, and had a little fun with people with its first tweet.
"Yes, we're on Twitter. Now it's your turn to follow us," it told the Twitterverse.

Social media users responded with good humour, generally. Ian Adam asked CSIS through Twitter, "And if you follow back, should I be really, really nervous?"

Things got a little more serious as writer and marketing consultant Karen Geier, under the handle Happy L'il Tree, wrote, "loving the completely chill attitude regarding your charter busting surveillance of citizens. GREAT COMEDY GUYS."

CSIS also received a tweet from the Communications Security Establishment (CSE) Canada, which said, "Welcome to Twitter! Allow us to offer some neighbourly advice: 'password' is never a good password!"

The U.S. Central Intelligence Agency (CIA) became an early follower of CSIS on Twitter. When the CIA joined Twitter in 2014, it tweeted, "We can neither confirm nor deny that this is our first tweet."

Canadian Press
Electronic spy agency mum on foreign info-sharing that could lead to torture
Wednesday, 20 July 2016
Byline: Jim Bronskill

OTTAWA - Canada's electronic spy agency won't say how often it shares information that could lead to someone being tortured in an overseas prison.
The Communications Security Establishment - which monitors threats from foreign terrorists and spies - has censored documents that spell out the figures, even though the RCMP and Canadian Security Intelligence Service have revealed such numbers in the past.

The reticence prompted Amnesty International Canada to say "much greater transparency" is needed from the Ottawa-based CSE.

"At stake is Canada's compliance with crucial international human rights obligations to prevent torture and ill- treatment," said Alex Neve, Amnesty's Canadian secretary general.

The secretive CSE has been thrust into the national spotlight in recent years due to leaks by Edward Snowden, the former spy contractor who worked for the National Security Agency, CSE's American counterpart.

It is also among a handful of Canadian agencies, including the RCMP, CSIS, the Canada Border Services Agency and National Defence, bound by a government instruction that allows it to share information with foreign partners - even when it means someone could be abused as a result of that exchange.

Public Safety Minister Ralph Goodale said earlier this year the Liberals will review the "troubling set of issues" raised by the foreign-sharing policy, enacted by the previous Conservative government.

A four-page 2010 federal framework document says when there is a "substantial risk" that sending information to - or soliciting information from - a foreign agency would result in torture, the matter should be referred to the responsible deputy minister or agency head.

In deciding what to do, the agency head will consider factors including the threat to Canada's national security and the nature and imminence of the threat; the status of Canada's relationship with - and the human rights record of - the foreign agency; and the rationale for believing that sharing the information would lead to torture.

Records obtained by The Canadian Press under the Access to Information Act offer a glimpse into how the CSE handled such cases in the first three months of 2015.

The quarterly report to CSE Chief Greta Bossenmaier, labelled Top Secret and for Canadian Eyes Only, told her the number of cases that required a "mistreatment risk assessment" and the level of risk associated with passing the information to others.

But those details were deleted from the publicly released version of the document.

Under the rules for deciding whether to share, the greater the risk, the higher the level of approval required. When the risk of mistreatment is low, a manager can decide. When the risk is substantial and cannot be managed - for instance, by seeking assurances from the foreign agency that someone will not be harmed - then the CSE chief or the defence minister must make the call.

The report says there were "no known instances" of a recipient country's non-compliance with conditions attached to information-sharing during the three months. But little else was disclosed.

The CSE faces "unique considerations" it must weigh when discussing details of assessments, said Christopher Williams, a senior spokesman for the intelligence agency. "With this in mind, we are not able to release the specific number you have requested without risking revealing insight into our capabilities."

However, the number and content of such assessments are reviewed by the independent watchdog who keeps an eye on the CSE, said Williams.

In addition, none of the requests in the three-month period involved a Canadian, all green-lighted information-sharing requests got the nod "to help mitigate foreign security threats," and requests are approved only after a thorough review, he added.

Amnesty's Neve said that when Canada shares intelligence information, there is a very real risk of contributing to torture.

The assessments are the safeguard meant to ensure that does not happen, he said.

"For Canadians to have any confidence that is the case we do, at a minimum, need details of how many assessments are being conducted, the breakdown of requests that are approved and denied, and some general information that conveys the basis for the decisions that have been reached."

New York Times
WhatsApp Is Briefly Shut Down in Brazil for a Third Time
Wednesday, 20 July 2016
Byline: Vinod Sreeharsha

Rio de Janeiro - For months, authorities in Brazil have sought access to digital data from WhatsApp to aid in criminal investigations. WhatsApp has repeatedly resisted the requests.
On Tuesday, the same clash erupted again, for the third time in less than a year. A Brazilian judge in a state criminal court in Duque de Caxias, in Rio de Janeiro, ordered a nationwide shutdown of WhatsApp after the popular messaging service, which is owned by Facebook, did not turn over user data requested by authorities as part of a criminal investigation. A few hours later, Brazil's Supreme Court overturned the order.

Despite the brevity of the episode, the case is part of a broader debate worldwide about when law enforcement officials and governments should have access to the digital data kept by tech companies. Many of the companies, like Apple and Microsoft, have said they are unwilling to turn over such data to authorities because doing so would infringe on the privacy rights of their customers. But authorities have argued that they need the data for security reasons.

In Brazil, WhatsApp faced two previous shutdowns -- one last December, and another in May -- for not turning over digital information. Both of those bans were also quickly overturned on appeal by higher court judges. In March, a Facebook executive was briefly taken into custody for refusing to comply with similar orders to turn over information from WhatsApp.

In the court ruling on Tuesday that ordered WhatsApp to be shut down, Judge Daniela Barbosa Assumpção de Souza said in a court statement that WhatsApp "cannot be offered to more than 100 million Brazilians without complying with the laws of the country, while failing to comply with judicial orders and obstructing criminal investigations."

"Especially when that activity leads to large profits, it is not credible that the company's representatives cannot appear before the court in order to comply with judicial decisions," the judge said.

Several previous requests had been made to Facebook for data, according to the court statement. The company is being fined 50,000 reais per day, or about $15,387, until it complies. Judge Barbosa also requested the company be investigated for obstruction of justice.

WhatsApp has end- to-end encryption of its communications, which makes it difficult to give third parties access to messages.

"As we've said in the past, we cannot share information we don't have access to," WhatsApp said in a statement.

After the Supreme Court overturned the lower court's order, the company said, "The Supreme Court swiftly rejected today's block, finding that it was disproportionate and violated people's fundamental freedom of expression."

Still, while the Supreme Court ruling referred to WhatsApp's nationwide shutdown, it did not address the merits of whether judges can require companies to provide data, suggesting the larger issue is far from settled.

Jan Koum, WhatsApp's chief executive, said in a Facebook post before the court order was overturned that "millions of people are cut off from friends, loved ones, customers and colleagues today, simply because we are being asked for information we don't have."

Access Now, a digital rights group, also called the initial court ruling disproportionate.

Peter Micek, global policy and legal counsel for Access Now, said in a statement, "Encryption keeps us safe, and companies need encouragement, not penalties, for taking steps like WhatsApp's end-to-end encryption that protects our data."

Jakarta Post
Pokemon Go could be used to detect secret info, minister warns
Wednesday, 20 July 2016
Byline: Marguerite Afra Sapiie

Jakarta - Defense Minister Ryamizard Ryacudu has warned players of Pokeman Go that their games may be used to detect the secretive information by foreign countries through smartphone cameras.

All media, including augmented reality game Pokemon, are susceptible to being used as surveillance tools since they can detect intelligence information without the awareness of the gamers, the minister said on Monday.

"We have to be very careful. [Secretive information] can be leaked through any form of media and channel, including this Pokemon Go game," Ryamizard said on Monday.

With the advance of technology, Ryamizard said there were now tools that could overhear people's conversations from a distance of 50 meters, adding that smartphone-based games might have similar abilities.

Last week, a statement from the Military Intelligence Division (BAIS) Cyber Taskforce circulated among the media, saying that people should not pay Pokemon Go in strategic locations, especially within military bases, to avoid intelligence information being leaked.

When playing the game, the players are unconsciously collecting information at locations through photos and videos captured on their smartphones, and the information could be employed by foreign intelligence bodies, the statement said.

Saudi Gazette
Daesh websites push young Saudis to join terror network
Wednesday, 20 July 2016

Jeddah - Many suspected Saudi militants have subscribed to Daesh ideas of an Islamic caliphate and wanted to participate in jihad in Iraq and Syria but they have not joined the terror group yet, according to Abdul Monem Al-Moshaweh, chairman of Assakeena Campaign.
He said some of these youths have adopted the takfiri ideology, which brands those who do not agree with it as infidels. "They have expressed their desire to contribute toward realizing the Islamic khilafat and to support weak Muslim communities," Al-Moshaweh said.

Speaking to Makkah Arabic daily, Al- Moshaweh said many militants joined the terrorist group in order to find out the truth or just to experience the thrill of fighting. "They did not listen to anti-terrorism awareness programs and media campaigns," he pointed out.

Al-Moshaweh said terrorist groups have found it easy to recruit young Saudis who subscribe to extremist views and believe in violence through their social networking websites.

However, Al-Moshaweh pointed out that some of these militants were ready for dialogue and discussions and could renounce their extremist thoughts either partly or fully. "We have found that terrorist groups influence these youths and turn them to armed terrorists."

He said the Kingdom's security agencies have been successful in defeating terrorism by cutting the link between terrorist leaders and their sympathizers. The Assakeena Campaign has been successful in changing the mindset of militants and bringing them back to the mainstream as responsible citizens.

The campaign has conducted dialogues with young Saudi men and women to convince them to change from the terrorist path.

"Most of them are convinced and wanted to change, but they fear for their safety," he said. "Many of them were influenced by extremist ideology propagated through websites."

He said the preemptive efforts of security forces were pivotal in foiling many terrorist operations across the Kingdom. "The two terrorists who killed their mother in Riyadh were prepared to carry out any acts of violence anywhere in the Kingdom," Al-Moshaweh said.

"An individual who can kill his mother will not hesitate to commit any crime," he pointed out. "In 2016, like 2013, terrorist groups succeeded in recruiting a large number of youths who were not linked to any of the terror networks."

Al-Moshaweh said: "Some of these youths say they don't have any connection to Daesh or Al-Qaeda. At the same time, they share the thoughts and views of these groups."

He said Assakina has given answers to four difficult questions on how to combat terror, especially after the recent terrorist attacks in the Kingdom.

Saudi Gazette
Insider corporate data theft big threat to digital business
Wednesday, 20 July 2016
Byline: Staff Report

Riyadh - Insider data theft and malware attacks top the list of the most significant concerns for enterprise security executives, a new report from Accenture and HfS Research reveals. Of those surveyed, a majority (69 percent) of respondents experienced an attempted or successful theft or corruption of data by insiders during the prior 12 months, with media and technology organizations reporting the highest rate (77 percent). This insider risk will continue to be an issue, with security professionals' concerns over insider theft of corporate information alone rising by nearly two-thirds over the coming 12 to 18 months. Additionally, the research shows that a budget shortage for hiring cybersecurity talent and well-trained employees is hindering the ability of organizations to properly defend themselves against these attacks.
The survey, "The State of Cybersecurity and Digital Trust 2016", was conducted by HfS Research on behalf of Accenture. More than 200 C-level security executives and other IT professionals were polled across a range of geographies and vertical industry sectors. The survey examined the current and future

state of cybersecurity within the enterprise and the recommended steps to enable digital trust throughout the extended ecosystem. The findings indicate that there are significant gaps between talent supply and demand, a disconnect between security teams and management expectations, and considerable disparity between budget needs and actual budget realities.

"Our research paints a sobering picture. Security leaders believe threats are not going away, in fact they expect them to increase and hinder their ability to safeguard critical data and establish digital trust," said Kelly Bissell, senior managing director, Accenture Security. "At the same time, while organizations want to invest in advanced cyber technologies, they simply don't have enough budget to recruit or train skilled people to use that technology effectively. To better manage this security problem, businesses will need to work in tandem with the extended enterprise ecosystem - business units, partners, providers and end users - to create an environment of digital trust."

Despite having advanced technology solutions, nearly half of all respondents (48 percent) indicate they are either strongly or critically concerned about insider data theft and malware infections (42 percent) in the next 12 to 18 months. When asked about current funding and staffing levels some 42 percent of respondents said they need more budget for hiring cybersecurity professionals and for training. More than half (54 percent) of respondents also indicated that their current employees are underprepared to prevent security breaches and the numbers are only slightly better when it comes to detecting (47 percent) and responding (45 percent) to incidents.

The report identified five significant gaps disrupting the ability of enterprises to effectively prevent or mitigate well-organized and targeted cyber attacks, including:

. Talent: Thirty-one percent list either lack of training or staffing budget as their single biggest inhibitor to combating attacks.

. Technology: Firewalls and encryption top the list of the most important technologies to combat cyber threats, but the largest increase in deployments anticipated in the next 12 to 18 months are in the areas of cognitive computing and AI (31 percent) and data anonymization (25).

. Parity: An enterprise is only as secure as its least secure partner, yet only 35-57 percent of all enterprises said they assess ecosystem partners for cyber integrity and preparedness, with BPO partners being the least vetted and credit partners being the most vetted.

. Budget: Seventy percent cite a lack of, or inadequate, funding for either cybersecurity technology or security talent, including training.

. Management: While 54 percent of respondents agree or strongly agree that cybersecurity is an enabler of digital trust for consumers, 36 percent believe that their executive management considers cybersecurity an unnecessary cost.

"While the gaps we identified can be overcome, they do collectively underscore the need for an inherently different approach, one that includes more robust risk management measures and the development of digital trust," said Fred McClimans, research vice president, Digital Trust and Cybersecurity, HfS Research. "There is an important opportunity to address these gaps by rethinking how digital trust and security can be holistically woven into the enterprise fabric through the integration of automation and AI solutions as well as through business partnerships and processes."

Reuters
Europe eyes Israeli technology for spotting lone-wolf terrorists online
Wednesday, 20 July 2016

Tel Aviv - European powers are trying to develop better means for pre-emptively spotting "lone-wolf" militants from their online activities and are looking to Israeli-developed technologies, a senior EU security official said on Tuesday.
Last week's truck rampage in France and Monday's axe attack aboard a train in Germany have raised European concern about self-radicalized assailants who have little or no communications with militant groups that could be intercepted by spy agencies.

"How do you capture some signs of someone who has no contact with any organization, is just inspired and started expressing some kind of allegiance? I don't know. It's a challenge," EU Counter-Terrorism Coordinator Gilles de Kerchove told Reuters on the sidelines of a intelligence conference in Tel Aviv.

Internet companies asked to monitor their own platforms' content for material that might flag militants had begged off, De Kerchove said. He said they had argued that the information was too massive to sift through and contextualize, unlike pedophile pornography, for which there were automatic detectors.

"So maybe a human's intervention is needed. So you cannot just let the machine do it," De Kerchove said. But he said he hoped "we will soon find ways to be much more automated" in sifting through social networks. "That is why I am here," he said of his visit to Israel. "We know Israel has developed a lot of capability in cyber."

Beset by Palestinian street attacks, often by young individuals using rudimentary weapons and without links to armed factions, Israeli security agencies that once focused on "meta data", or information regarding suspects' communications patterns, have refocused on social media in hope of gaining advance warnings from private posts.

Israeli officials do not disclose how far the technology has come, but private experts say the methods are enough to provide often basic alerts regarding potential attackers, then require follow-up investigation.

"Nine out of 10 times, the terrorist has contacts with others who provide support or inspiration, so meta data still applies," said Haim Tomer, a former Mossad intelligence division chief turned security consultant.

When it comes to true lone wolves, even a valedictory Facebook message can often be picked up by Israel, he said.

"But in such cases, it would be a low-level 'green alert', meaning the person should be looked at further, whereas a 'red alert' would warrant instant action. That leaves the security services to decide how to handle matters," Tomer said.

As De Kerchove was at pains to make clear to the conference, European standards of civil rights, such as privacy, make the introduction of intrusive intelligence-gathering technologies in the public sphere and aggressive police follow-ups difficult.

While Israel's emergency laws give security services more leeway, its intelligence minister, Yisrael Katz, called for cooperation with Internet providers rather than state crackdowns. He cited, for example, the encryption provided by messaging platform WhatsApp which, he said, could be a new way for militants to communicate and evade detection.

"We will not block these services," Katz told the conference. "What is needed is an international organization, preferably headed by the United States, where shared (security) concerns need to be defined, characterized."

Moscow Times
Cybercriminals Steal $21M from Russian Banks in 12 Months
Tuesday, 19 July 2016
Byline: Staff report

Moscow - Cybercriminals have stolen 1.37 billion rubles ($22 million) from Russian banks since last May, Russia's Central Bank announced Tuesday.
The figures come from a report marking the first-year anniversary of the Central Bank's cyber-space monitoring service FinCERT, created specifically to prevent the spread of cybercrime.

FinCERT recorded 20 major cyber attacks on Russian banks from May 2015 to June 2016, with criminals attempting to steal a total of 2.87 billion rubles ($45 million.)

Phishing websites and fake SMS and email messages claiming to be from FinCERT formed the basis of many of the attacks, along with ATM theft.

Roughly 100 million rubles ($1.5 million) has been stolen through ATMs and point-of-sale terminals since November 2015, using such as card reading devices at payment points in restaurants and stores.

FinCERT representatives warned holders of the national Mir payment card last month that the cards may be vulnerable to cyber attacks. The card was introduced to cut Russia's reliance on foreign firms like Visa and MasterCard.

The Central Bank and Ministry of Finance have also proposed changes in federal laws which would allow them greater powers to combat individual cases of cybercrime, according to the report.

The Guardian (London)
Turkey blocks access to WikiLeaks after Erdogan party emails go online
Wednesday, 20 July 2016
Byline: Staff report

Istanbul - Turkey has blocked access to the WikiLeaks website, the telecoms watchdog has said, after nearly 300,000 emails from president Recep Tayyip Erdogan's ruling Justice and Development party (AKP) were put online as Ankara grapples with the aftermath of a failed military coup.
The emails date from 2010 to 6 July this year. Obtained before the attempted coup, the date of their publication was brought forward "in response to the government's post-coup purges", WikiLeaks said on its website, adding that the source of the emails was not connected to the coup plotters or to a rival political party or state.

Turkey's telecommunications communications board said an "administrative measure" had been taken against the website - the term it commonly uses when blocking access to sites. Turkey routinely uses internet shutdowns in response to political events, which critics and human rights advocates see as part of a broader attack on the media and freedom of expression.

About 50,000 soldiers, police, judges and teachers have been suspended or detained since the attempted coup at the weekend, and Turkey's western allies have expressed concern over the crackdown's reach.

On Wednesday, it was also announced that Turkish academics have been banned from travelling abroad until further notice, according to state-run broadcaster TRT.

The report, which provided no details about the ban, came a day after the board ordered the resignation of 1,577 deans at all universities across Turkey. In a separate move on Tuesday the education ministry also revoked the licences of 21,000 teachers working in private institutions.

The government has accused a US-based Muslim cleric, Fethullah Gülen, of masterminding the attempted coup, in which more than 230 people were killed. Gülen denies the accusation.

The Courier (Leamington Spa)
GCHQ and Leamington charity aim to inspire girls to take up a career in cyber security
Wednesday, 20 July 2016

Leamington Spa - National security experts at GCHQ are working with a Leamington charity to offer a free cyber security course for teenage girls this summer.
The Smallpeice Trust is running the CyberFirst Futures residential course with GCHQ at Birmingham University from August 1 to 4, during which participants will gain an insight into the next generation of cyber security tools. The course will also test their skills in dealing with modern and advanced cyber defence scenarios.

Open to 16 and 17-year-old girls, those taking part in the four-day course will work closely with experts from GCHQ, the Smallpeice Trust and academia, gaining an insight into the importance of cyber security and getting first-hand experience of defending against a cyber-attack.

Chris Ensor from GCHQ said: "We want to develop a diverse, continuous flow of people with the right skills and knowledge to help protect the UK against future cyber-attacks.

"The reality is that our cyber security will become even more important as technology develops and the internet becomes all pervasive.

"It makes sense that we look to inspire and encourage a generation of young people into a career in cyber security who have grown up with the internet as an integral part of their lives and who have an innate understanding of the power of technology."

The UK now earns nearly £2 billion in cyber security exports and according to the last report on the strategy in 2014, there are 750 companies signed up to the Cyber-security Information Sharing Partnership for Industry and Government (CiSP). This emerging sector is driving the need for new recruits with good science, technology, engineering and mathematics (STEM) skills.

Dr Kevin P Stenson, chief executive at the Smallpeice Trust, said: "We've worked with GCHQ for many years on individual cyber security courses for 13 to 14-year-olds, but given the projected growth of career opportunities in cyber security and as the risk of cybercrime increases, it is now the ideal time for a national programme aimed at 16 to 17-year-olds to start."

Lebanon Daily Star
Dismantling of Israeli-tied networks hampered probe
Wednesday, 20 July 2016
Byline: Staff Report

Beirut - The head of the Parliament's telecoms committee said Tuesday that investigations into Lebanon's Israeli-tied internet setups were hampered due to their impromper dismantling by the army. "We were informed by the army that the dismantling of the equipment before experts arrived resulted in an error," MP Hasan Fadlallah told reporters.

The matter of illegal internet setups came to light in March when Telecommunications Minister Boutros Harb announced the discovery of unlicensed, low-cost internet networks across the country. He said Israel was using these setups to spy on Lebanon.

Four illegal networks have been discovered so far, in the Dinnieh highlands in north Lebanon, and in Ouyoun al-Simane, Faqra and Zaarour in Mount Lebanon.

Fadlallah announced that the committee has agreed to invite Finance Minister Ali Hassan Khalil and the president of the committee of cases at the Justice Ministry to a session to discuss the amount of financial losses from the state budget because of the illegal internet scandal.

These providers were buying bandwidth from abroad and selling it in Lebanon below official rates.

Fadlallah said that State Prosecutor Samir Hammoud informed them that the illegal internet case to proceeding according to judicial mechanisms.

Harb also said that he has provided Hammoud with information he had requested from the state-owned telecoms company Ogero. "We have made sure that the information was sent to him," Harb said.

Ogero has been at the center of the unlicensed internet scandal, with eight people so far arrested in the case and many more charged in absentia.

Three top Ogero officials are being questioned over "negligence that led to squandering public funds and evading taxes by allowing some people to set up unlicensed internet in the country.

"We will not allow for the illegal internet file to be hidden. We want the investigations to reveal those involved and to be punished. The judiciary is doing its work based on the legal requirements," Harb added during the news conference.

Fadlallah said that the next session will take hold place on Aug. 17, adding that the committee will continue discussions until the case is concluded.

CBC News
DND at the back of the drone line despite contractor pitches
Thursday, 21 July 2016
Byline: Murray Brewster

A total of 16 companies have come forward to express interest in providing the Canadian military with drones, but more consultation is in the offing, and it's likely other federal departments will be using the technology well before it arrives at National Defence.
The Trudeau government started browsing the defence marketplace earlier this year, asking contractors for information about what kind of systems were out there, when they are available and potential program options.

The absence of the capability has come up in presentations submitted to the current defence policy review undertaken in the spring by the Liberals.

The consultation paper that kicked off public feedback noted unmanned systems -- regardless of whether they are in the air, on land or under the sea -- have become "integral to modern military operations."

It also says unmanned aerial systems have been used with "great effect" on operations, including by Canada when the previous Conservative government leased drones from the Israelis.

That lease was dropped after Canada ended its Kandahar combat mission, and since then, troops and sailors have only experimented with micro-drones. The latest involves the recent $14-million purchase for the navy of the small RQ-21A Blackjack, which launches via cable system.

The government consultation paper made clear that pilotless planes "offer several advantages that manned aircraft cannot provide."

Even still, a spokesman for Public Services and Procurement Canada says the military is a long way from committing to anything, or even issuing a request for proposals.

"The (Joint Unmanned Surveillance and Target Acquisition System) project team is analyzing the information gathered, and will use it to develop detailed cost estimates and planning documents to help inform available options for this program," said Nicolas Boucher in an email.

It's conceivable that other federal departments will be operating drones before the military.

Last spring, Transport Canada issued a tender call for an unmanned aerial system to survey ice and oil spills in the Canadian Arctic.

The department is only looking for one drone, which would conceivably replace three manned, civilian turbo-prop aircraft that patrol the region.

The Fisheries Department also conducted its own test program on the West Coast in February.

And that is to say nothing about the explosion in commercially available drone technology.

However, National Defence's equipment acquisition guide, which was updated in May, does not foresee the military getting such a capability until at least 2026, a quarter century after the plan was first suggested.

Boucher's written response did not speak to the timeline, but did say that government needs more information to determine project risks, costs and potential economic benefits.

"Going forward, additional consultations will be required to further refine a strategy that addresses National Defence's short and long term needs," he said.

Drones first discussed in 2000

The request for information was at least third time the Canadian government has gone to industry looking for ideas over the last decade and a half.

The Defence Department first began pitching for the technology in September 2000, but the project didn't get any traction until 2003 when medium-altitude drones were leased for experimentation.

The military deployed French-manufactured Spewer remotely piloted planes during the early phases of the war in Afghanistan.

The former Conservative government even promised to create a drone squadron during the 2005 election, and soon after being elected, it implemented a $500-million acquisition program.

But a shortage of staff, which were reassigned to the CH-47F Chinook helicopter program, and political disagreements over whether the drones should be armed caused delays. The program is now estimated to be between $1 billion and $1.5 billion.

The Harper government, at the insistence of the Manley commission, temporarily acquired Heron remotely piloted surveillance planes to support troops during the latter half of the Kandahar combat mission, but the lease was handed over to the Australians after Canada withdrew in 2011.

To arm or not arm? That is the question

The air force has pushed for armed drones.

The country's top military commander, Gen. Jonathan Vance, publicly supported the notion last winter.

"If we are in operations against a force like ISIS, the surveillance piece is important but we also want to contribute to the strike," he said. "In my view, there's little point to having a UAV that can see a danger but can't strike it if it needs to."

But there are also critics who say while a drone strike capability is important, the Canadian government hasn't done enough homework, or put in place a legal framework of accountability for using the weapons.

London Free Press
'Exceedingly exceptional' break for far from 'normal criminal'
Thursday, 21 July 2016
Byline: Jane Sims

Stephen Solis-Reyes is, by all accounts, exactly what an Ottawa judge who dealt with him said he is: "not the normal criminal."
A London judge agreed Wednesday to lift a travel ban imposed on the Heartbleed Hacker, part of his conditional sentence for breaking into the federal tax collector's website in 2014, but not without telling the computer whiz the move is "exceedingly exceptional."

It pays to be good and Solis-Reyes - a Western University student serving house arrest for his crime, but nowfree to go to an elite international computer programming competition in California - is very, very good.

"It means a lot, for sure," Solis-Reyes said outside the London courthouse of the judge's decision. "I think he is expecting big things from me. He's expecting what I do in this competition is going to help society and help me in the future."

The 21-year old Londoner was convicted in May of four charges - two counts of mischief, unauthorized use of a computer and obstructing a police officer - for sending techno-shivers through the federal government in 2014.

That spring, as the income tax-filing deadline neared for Canadians, Canada Revenue Agency's website was breached by someone exploiting the so-called Heartbleed computer bug. About 900 social insurance numbers were stolen and the website had to be shut down, the tax deadline extended by a week and the RCMP began investigating.

The Crown ultimately dropped 13 other charges against the Londoner, who maintained he'd broken into the system only to demonstrate its vulnerability.

Soft-spoken, unfailingly polite, the computer science student who appeared in court Wednesday looks far younger than his age.

He's also super-brainy, the kind of guy who rattles off high 90s in his courses and writes computer code for fun. That passion has been both his curse, and his good fortune.

Recently, solis-reyes was named one of 10 finalists - the only one from North America - in an international, IBM- sponsored computer programming competition, Mastering the Mainframe, that drew 15,000 entries worldwide.

He's now been invited to san Francisco on sept. 14 to compete for four days. If finishes in the top two places, he goes to l as Vegas for two more days.

But solis-reyes is also serving an 18-month conditional sentence, after pleading guilty for demonstrating to the federal government - and the postal service in the Guernsey Islands, off the coast of France - just how vulnerable they were to the heartbleed computer virus.

In six seconds, he was able to breach revenue Canada's security and steal the social insurance numbers - not to use them, but to teach a lesson.

By the time the competition arrives, he will have done his four months of house arrest, but the rest of his sentence requires him to stay in Ontario.

So, all dressed up, with his suit hanging loosely on his thin frame, he waited patiently with his parents outside the courtroom for his chance to make a highly unusual request of a judge to vary his sentence.

Superior Court Justice Duncan Grace gave him the green light.

Grace said he was struck by the glowing comments of Justice Lynn ratushny when she sentenced him in May. she called him "a good person who made a very bad mistake."

"You are young. You have a bright future, a very bright future," ratushny said.

"I strongly recommend to any future employer they consider this young man's excellent potential and award him employment. He is a young man who has worked hard, who has exemplary values and I don't expect those values to change."

Assistant Crown attorney James spangenberg told Grace he spoke to the RCMP and solis-reyes's probation officer, who said he's done "very well" during his sentence. But the concern was the sentence would be difficult to enforce if he's unable to travel. "Allowing for travel would undermine that order," spangenberg said.

Defence lawyer Gordon Cudmore said the Ottawa judge's comments were clearly to encourage his client's future "to move forward" and not to crush his potential.

Grace agreed. He said the hearing "would have been short" if not for those comments at sentencing and the eloquent letter sent to him by solis-reyes, Last week, solis-reyes and his mother went to a tedious scheduling court, waiting all day for a chance to file his sentence variance request.

Grace oversees that court. "I noticed how politely you sat for the entire day," he said.

He also commented on the student's "extremely bright future," and how the conditional sentence was nothing out of the ordinary.

The judge was told solis-reyes was born in the United states and has both American and Canadian citizenships and is applyingfor reissue of both documents because the've expired.

Solis-reyes told Grace he was willing to travel with his Canadian documentation if necessary, but would need the U.s. paperwork if there were questions about his listed birthplace.

Grace said he still would have to consider what to do about travel documents, but had no questions about solis-reyes' character.

"I have every confidence you will represent yourself, your family and this country positively," the judge said.

Outside court, solis-reyes said he's grateful for the chance to compete and that his sentence has allowed him to work and go to school.

"Of course, it's a jail sentence, so it's not easy, but I think it's fair," he said.

"It's been difficult, but we're past the hard part and you have to pay the consequences and that's what I'm going to do and I'll go from there."

It's meant he can still hang on to his dreams. "I think I would like to find work at a nice company as a computer programmer and just write code because it's what I enjoy."

Then his eyes lit up. "I've always enjoyed programming and working with computers. It's something I've always wanted to do for a living and I have a chance to do it."

London Daily Telegraph
Teenager crashed world computer networks and sent Twitter bomb threats 'to be cool'

Thursday, 21 July 2016
Byline: Martin Evans

London - A teenage computer hacker, who shut down government networks across the world and sent bomb threats to US airlines, has been spared jail.
The 16-year-old, from Plympton in Devon, began targeting the systems of organisations and states he disagreed with when he was just 14.

Using a laptop computer in his bedroom, the schoolboy, who cannot be named for legal reasons, caused chaos targeting Iraq's ministry of foreign affairs, the department of agriculture in Thailand and China's security ministry. He also crashed computers in the Japanese town of Taiji, where an annual dolphin hunt takes place, and the Sea-World theme park in Florida.

He was arrested after using Twitter to send bomb hoaxes to American Airlines, Delta Air Lines and even the White House, telling them: "There's a nice tick-tick in one of those lovely Boeing planes. Hurry gentlemen, the clock is ticking. High quality." District Judge Diane Baker, sitting at Plymouth Youth Court, told the boy: "I think you got carried away by the fact you thought you were cool, you thought you were clever. You didn't think of what truly happens in the real world if you do these things. I don't think there would be any positive outcome for you going into a youth detention centre. I think it would destroy you."

Addressing the court, the teenager said: "I just want to say that I am really sorry for everything that I have done. I didn't really know how serious it was. I am sorry to my family."

He was convicted of three offences under the Computer Misuse Act and two under the Criminal Law Act, for the bomb hoaxes. He was given a twoyear youth rehabilitation order and a two-year supervision order and told to attend 120 hours' reparation and two courses.

The boy's mother was told to pay £620 in prosecution costs and his computer will be destroyed.

24 Heures (Suisse)
« Cette loi est un compromis entre sécurité et liberté individuelle »
Thursday, 21 July 2016
Byline: Florent Quiquerez

Berne - Nouveau préposé fédéral à la protection des données, Adrian Lobsiger défend la loi sur le renseignement
Sa nomination avait suscité quelques crispations sous la Coupole en mars dernier. D'aucuns s'inquiétaient de l'arrivée d'un ancien haut cadre de l'Office fédéral de la police (FedPol) au poste de préposé à la protection des données. A 55 ans, Adrian Lobsiger entame son mandat alors que les défis

ne manquent pas en matière de défense des libertés individuelles. Première bataille: la future loi sur le renseignement, en votation le 25 septembre. Interview.

Cette loi va-t-elle trop loin, comme l'estiment les opposants?

Je ne suis pas là pour faire peur aux gens. Mais il faut se rendre compte que chaque Etat a la possibilité de saisir les informations de ses citoyens. La différence entre un pays démocratique comme la Suisse et un régime autoritaire, c'est que la marge de manoeuvre et les possibilités données à l'Etat de droit sont ancrées dans la loi, qui détermine le cadre procédural et les instruments de recours auprès d'une justice indépendante. Le texte qui est soumis en votation est le produit d'une longue discussion, dont l'origine remonte aux attentats du 11 septembre 2001. Nous sommes au bout de ce processus.

Les libertés individuelles sont donc assez respectées?

Nos services ont été consultés tout au long du processus législatif. Le résultat obtenu aujourd'hui représente un compromis entre les besoins de sécurité et la défense des libertés individuelles. Nous avons été entendus et je peux vivre avec ce compromis. La question qui se pose maintenant est la suivante: est- ce qu'on préfère le statu quo ou un changement? La majorité du parlement veut ce changement, et je respecte ce choix. Si le citoyen veut aussi donner plus de pouvoirs aux services de renseignements, alors il doit voter en faveur de ce texte. S'il veut se contenter du droit en vigueur, il doit dire non. Dans ce cas, la discussion sera très probablement close pour longtemps.

Votre carrière à FedPol influence-t-elle votre position?

FedPol a été impliqué au tout début du processus. Mon prédécesseur s'est beaucoup engagé pour que cette loi sur les renseignements n'empiète pas trop sur les libertés individuelles. Il y a des garde-fous techniques, politiques et judiciaires. Pour obtenir le droit de surveiller quelqu'un, il faudra faire un grand travail de préparation et avoir de très bons arguments pour justifier la procédure. Si la loi est acceptée en votation populaire, le Conseil fédéral sera lié par ses déclarations selon lesquelles les autorisations porteront sur une dizaine de cas par année.

Le Conseil fédéral ne s'arrête pas là. Il projette une surveillance discrète pour lutter contre le terrorisme

Pour l'heure, c'est une décision de principe. Le gouvernement a donné mandat au Département compétent d'élaborer des libellés concrets. De notre côté, nous allons examiner si ces mesures sont proportionnées. Il faut toujours faire une pondération entre les libertés individuelles et l'intérêt de l'Etat. Il faut toutefois relativiser la portée de ce projet. Il n'est pas du tout comparable à la loi sur le renseignement. Ici, il s'agit plutôt de propositions qui doivent compléter le système préventif policier.

Autre domaine, la mobilité. Avec les projets de vignette électronique ou le SwissPass des CFF, on saura bientôt tout de nos déplacements

Souvent, les prestataires de ce genre de services ne sont pas prêts à supprimer les données de leurs clients, car ils se disent - selon le credo de big data - qu'ils pourraient en avoir besoin pour un développement futur. Pour moi, c'est important de savoir ce que les entreprises cherchent à faire dans l'immédiat, et quelles sont les différentes étapes prévues ensuite. De mon côté, les choses sont claires: si les explications fournies par l'entreprise ne sont pas convaincantes, alors je demande la destruction des données.

A l'heure d'Internet, votre combat pour la protection des données n'est-il pas voué à l'échec?

Je ne pense pas que l'importance de la sphère privée a diminué parce que nous nous trouvons dans une révolution numérique. Avoir une sphère privée, c'est un besoin inhérent à l'être humain. Rappelons-nous les réactions publiques aux révélations d'Edward Snowden.

Mais cette liberté individuelle, existe-t- elle encore?

Bien sûr! Je dirais même que la révolution numérique lui donne un nouveau souffle. Internet, c'est aussi un endroit où les gens peuvent se rassembler pour réclamer ou défendre leurs droits, c'est-à-dire leur autodétermination et le respect de la sphère privée. Regardez ce qui se passe dans le monde. Les organisations qui ont le plus de problèmes avec les opinions libres sur Internet, ce sont les régimes autoritaires. Finalement, les choses n'ont pas vraiment changé avec le progrès technologique. Les gens n'aiment pas être manipulés ou surveillés par n'importe quel pouvoir, qu'il soit étatique ou économique.

Il y a aussi un besoin sécuritaire qui se fait au détriment de cette liberté

Vous avez raison, et c'est justement là que nous entrons en jeu. Le préposé fédéral, mais aussi les préposés cantonaux, doivent sensibiliser la population. Nous devons expliquer avec des mots simples quels sont les défis en matière de protection des données, et pointer du doigt les applications qui pourraient enfreindre les libertés individuelles.

The Hindu
Big Brother is now keeping watch on social media too
Thursday, 21 July 2016
Byline: Anuradha Raman

New Delhi - On July 19, when the Supreme Court asked Congress vice- president Rahul Gandhi to apologise for his comments on the RSS, the two- year-old New Media Wing under the Information and Broadcasting Ministry, described as the online eyes and ears of the Government came up with this finding: 44 per cent respond positively to the SC admonishing Rahul Gandhi.
The team also made the following observation: positive response (in favour of the SC and the RSS as well as against Mr. Gandhi), is 44 per cent. The responses are graded as positive, negative and neutral (posts which state things as they are).

Twitter, Facebook, blogs and YouTube are the mining ground for information on which responses are graded as positive, negative and neutral, giving an insight to senior government officials on the mood in the social media on a daily basis. Sometimes, special requests are made by Ministries to understand the responses to new initiatives of the government.

The analysis, seen by The Hindu, has sparked off questions in the Ministry about whether the New Media Wing mines data for the BJP-led NDA Government or the BJP/RSS. Officials not wishing to come on record said there were no parameters drawn for analysis of social media trends as the Wing is relatively new. "The mandate of the Wing is not clear. We analyse trending topics and put it across to our seniors," said an official.

In the last few days, topics that have been picked up on the basis of their traction on Twitter, Facebook, Google Hangouts and YouTube video posts have revolved around Mr. Gandhi, Navjot Singh Sidhu, gagging of the media in Jammu and Kashmir and the beginning of the monsoon session of Parliament, and the responses have been analysed by Oracle's Social Relationship Manager tool and Meltwater and shared with senior officials in the I&B Ministry, PMO and concerned ministries and Intelligence agencies.

Top Influencers are listed in accordance with the followers they command on Twitter. Director General of the Press Information Bureau (PIB) Frank Noronha directed this correspondent to speak to an official in the Information and Broadcasting Ministry. The New Media Wing and the Electronic Media Monitoring Centre, (EMMC) together keep a watch online and on television channels.

The PIB sends press clippings every day to senior officials of the Government of India. At one place, the Wing which works with the Government to promote its activities even analyses the impact of an event on the BJP party --making it the first time, a government's wing has associated its activity with a political party. Sample this: For resignation of Sidhu on July 18, the positive response in favour of (BJP and against Sidhu) is 34 per cent, negative is 17 cent and neutral is 49 per cent. Significantly, the neutral position has larger numbers than positive or negative responses.

On the other hand, the analysis titled, Social Media Analytics on newspaper seizure in parts of J&K, threw up the following results: three per cent respond positively; 28 per cent negatively and 69 per cent maintain neutral positions. Some officials in the PIB said the Government should have cautioned about the adverse fallout of gagging the media instead of allowing status quo for three days.

Islamic Republic News Agency
Cyber security operation center launched in Isfahan N-zone
Thursday, 21 July 2016

Tehran - Iran's Atomic Energy Organization has launched a cyber security operation center in the nuclear zone of Isfahan.

This center has been launched in order to address new threats and at the same time to enhance the safety and security levels of the nuclear site in Isfahan, said Asghar Zare'an, Deputy Head of Iran's Atomic Energy Organization in the inauguration ceremony on Wednesday.

'Presently, the issues of cyber security, the information technology and industrial control systems, tend to constitute the main priorities of the enemy,' he said.

The enemy tries by deploying malwares sabotage the industrial development of the country and damage our infrastructures, he said.

According to Zare'an similar cyber security operation centers are going to be launched with the priority given first to Arak, Natanz and Boushehr nuclear sites.

'The enemy pays special attention to this method of industrial sabotage as it is done covertly and tends to inflict greater damages while it is less costly,' he said.

Direction informatique (site web)
Darktrace repêche un ancien agent du SCRS
Wednesday, 20 July 2016
Byline: Dominique Lemoine

Toronto - Darktrace s'implante au Canada avec l'ouverture d'un bureau à Toronto et nomme à la tête de sa direction au Canada un ancien agent de renseignements au service du Canada (SCRS) et de l'Angleterre (MI5), David Masson.
Cette multinationale se spécialise en produits de cybersécurité pour les entreprises. Elle a été fondée en 2013 à Cambridge en Angleterre et elle serait née d'une collaboration entre des mathématiciens de l'Université Cambridge et d'anciens agents du MI5, le service de renseignement responsable de la sécurité intérieure au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord.

L'approche de Darktrace miserait notamment sur l'apprentissage automatique (ou machine learning en anglais) pour reconnaître le comportement normal d'un utilisateur, d'un réseau ou d'un appareil informatique et pour pouvoir détecter une anomalie de comportement qui trahirait une attaque ou intrusion, plutôt que sur la surveillance d'attaques connues.

Cette méthode basée sur la surveillance du trafic réseau et sur la veille informatique serait inspirée de la biologie du système immunitaire humain et elle viserait la protection des données internes des organisations des secteurs de la finance, du manufacturier, de services professionnels et publics, de la santé, de l'énergie, du transport, du détail et des télécommunications.

Yonhap News Agency
Gov't bolsters countermeasures to deter N.K. cyberattacks
Friday, 22 July 2016
Byline: Staff reporter

Seoul - South Korea is beefing up its governmentwide countermeasures to prevent possible cyberattacks by North Korea, officials said Friday.
The Ministry of Science, ICT and Future Planning said the number of cyberattacks by North Korea more than doubled in the first half of this year.

The cyberattacks "are judged as a part of North Korean provocations to trigger public anxiety" in South Korea, the ministry said.

Last month, South Korean police said North Korea hacked into more than 140,000 computers at 160 South Korean firms and government agencies. About 42,000 documents were suspected to have been stolen, including defense-related information.

The ministry urged people to install antivirus software and avoid opening suspicious emails.

South Korea has been on high alert against hacking attacks by North Korea following the North's fourth nuclear test in January and a series of missile launches in recent months.

Huffington Post
Where Is The Accountability For Ottawa's Communications Spies?
Friday, 22 July 2016
Byline: Monia Mazigh

Commentary: The Communications Security Establishment (CSE) Commissioner report has been just released. For those who don't know what the CSE is, it is the agency related to the Department of National Defence that spies on communications received from abroad.
In their own words, their work focuses on "collecting foreign signals intelligence in support of the Government of Canada's priorities, and on helping protect the computer networks and information of greatest importance to Canada." It is important to emphasize that CSE is not supposed to spy on communication of Canadians in Canada or abroad.

In that regard, the commissioner's mandate is mainly to review CSE activities and their compliance with the law, and in the case of complaints, to undertake investigation. However, the commissioner report, which is supposed to be an independent exercise conducted by a review body, seems more and more like a self-congratulatory document where criticism directed at the CSE or its activities is hard to find. The situation can be compared to a professor rating her own students in a national competition. Of

course, she would like them to pass, and of course she would be lenient in marking. Rather, in such circumstances we need a professor from a different school, and the students' names should be hidden.

In previous years, two main problems became clear to the public in regard to CSE activities:

The stipulations protecting the privacy of Canadians are not always respected, as CSE was reminded by Privacy Commissioner Daniel Therrien.

The lack of safeguards when it comes to information sharing with other agencies -- the Canada Security Intelligence Agency (CSIS), for example.

Indeed, in defence of the CSE's activities, Minister of National Defence Harjit Sajjan recently minimized the amount of information revealed through metadata, usually collected by CSE during its operations. Metadata, or data on data, shouldn't be of a privacy concern for Canadians, according to minister Sajjan.

But the reality is that through the records of Internet and phone communications, even without revealing the identity of the user, much information can still be inferred and shared with other foreign agencies. There exists today a whole range of science fields and theories that can extract patterns about people behaviours without knowing their identities.

The report claims that the commissioner's office "is monitoring 14 active recommendations that CSE is working to address -- 10 outstanding recommendations from previous years and four from this year," and that the privacy issue about sharing foreign intelligence is also being looked into. Nevertheless, we can't know for sure how this is being done and if there is any proposed legislation to be submitted soon. The report doesn't tell us.

It seems from the report that, in general, the commission recommends that the minister should always be informed about controversial issues, but no specific mechanism is suggested to deal with the identified problems. The issue of transparency becomes a matter of blind trust in the hands of the minister of national defence.

Leaving it up to the minister in charge to decide what is acceptable and what is not, or what is lawful and what is not, is far from a democratic and accountable model. We need review mechanisms with the necessary autonomy, independence and structure to create true accountability.

For instance, the ambiguous relationship between CSE and CSIS, described in the report, can't be investigated by any review body. There are currently agencies to oversee respectively CSIS (SIRC) and the CSE (the office of the CSE commissioner), but there is no "super-SIRC" to oversees them both and launch investigations on both of them. The parliamentary oversight presented by the government in Bill C-22 isn't clear if this aspect will be included in its mandate.

As of yesterday, it was reported that CSE won't even reveal the number of times it shared information that could lead to someone being tortured in foreign prisons. The greater the risk of mistreatment (please note how the word "torture" isn't even used), the higher level of bureaucratic or political intervention is required.

Once again, it is up to the minister or a high-level bureaucrat to take that decision, and that risks him or her making a mistake in their assessment. If that happens, Canada will become collateral damage like it has in the past.

New Straits Times
Govt to improve security in airports
Friday, 22 July 2016
Byline: Fazleena Aziz

Sepang - The government will soon introduce a new mechanism to boost security in airports, especially at boarding gates.
Deputy Transport Minister Datuk Abdul Aziz Kaprawi said the mechanism would take into consideration existing operational procedures.

He said that given the increased terror threats globally, especially in transportation hubs, upgrading security was paramount to ensure people's safety.

Aziz said ministry secretary-general Datuk Seri Saripuddin Kasim had been directed on Wednesday to draw up details of the new mechanism through a committee, which would include agencies and departments.

"Some of the issues that pose obstacles, in terms of beefing up security, which we will have to consider, are airport design, businesses and visitors sending off their loved ones.

"But we have to increase security and safety in airports as the threat is real, especially in light of the attacks in Brussels and Istanbul."

He said this after opening the 13th Steering Committee Meeting of Cooperative Aviation Security Programme Asia-Pacific Region (CASP-AP) 2016 yesterday.

Aziz, however, said Kuala Lumpur International Airport complied with International Civil Aviation Organisation (ICAO) security standards, adding that the last audit was done in 2012, while the next audit was due next year.

He said he wanted the Department of Civil Aviation (DCA) to come up with stricter measures to screen potential staff and those working in airports to minimise insider threats.

As most contract workers could also be foreigners, proper screening was vital to ensure no one slipped through the system, he added.

Earlier, he said insider threats could come in the form of former employees, current employees, contract workers or partners who had inside knowledge of the industry.

He said such threats were capable of exploitation, tampering, fraud, espionage, theft and sabotage.

Cyber threats to computer systems were also a matter of concern with increasing reliability on technology, he said, adding that such attacks could cause disruptions.

It was reported that the government was considering a cabinet proposal to allow only passengers to enter terminals in major airports to boost security.

Deputy Prime Minister Datuk Seri Dr Ahmad Zahid Hamidi had said Transport Minister Datuk Seri Liow Tiong Lai had been instructed to work out this proposal with Malaysia Airports Holdings Bhd.

Present yesterday were DCA director of aviation security Abdul Rahmat Mahat and ICAO Asia and Pacific Office regional officer Ross Lockie.

Voice of America
Russian Agent Sentenced for Illegally Exporting US High-tech Gear
Friday, 22 July 2016

New York - A federal court in New York on Thursday sentenced an admitted agent of the Russian government to 10 years in prison and ordered him to forfeit $500,000 in profit he'd gained from his criminal activity, which focused on acquiring and secretly shipping abroad high-tech microelectronics for Russian military equipment.
Alexander Fishenko pleaded guilty to all 19 charges brought by the Department of Justice. U.S. officials said a company that Fishenko had founded shipped $50 million worth of electronic products to Russia between 2002 and 2012, all in defiance of a government licensing system meant to control such exports.

"These commodities have applications and are frequently used in a wide range of military systems," U.S. officials said, "including radar and surveillance systems, missile guidance systems and detonation triggers."

Charges against Fishenko, who has both American and Russian citizenship, included conspiracy, illegally exporting controlled products, conspiring to launder money and obstruction of justice. He was indicted in October 2012, along with 10 other individuals and two corporations, both of which Fishenko

controlled. Three of the people remain at large, but the others either have pleaded guilty or been convicted in court.

To evade export controls on high-tech products manufactured in the United States, officials said, Fishenko and his co-conspirators gave false information about who was buying the electronic components, concealed the fact they were exporters and falsely described the devices on records submitted to the U.S. Department of Commerce.

Ultimate recipients of the electronic components acquired by Fishenko's companies, known as ARC and Apex, included a research unit for the Russian internal security agency FSB, a Russian entity that builds air and missile defense systems, and another that produces electronic warfare systems for the Russian Ministry of Defense.

Assistant Attorney General John Carlin said prosecuting those who violate U.S. export laws is "an important part of our national security framework ... protecting national assets from ending up in the hands of our potential adversaries."

Politics.co.uk
Boris Johnson once outed MI6 spy 'for a laugh'
Wednesday, 20 July 2016
Byline: Adam Bienkov

London - There was some nervousness in the Foreign Office when it was announced that Boris Johnson had been made foreign secretary.
Part of Johnson's new role involves overseeing MI6. This is a highly sensitive and delicate task which some within his department worry he is unsuited for.

It now appears there is good reason for them to feel uneasy.

In 2001, while editor of the Spectator, Johnson published a piece suggesting that a former friend and colleague had worked for the secret service.

On the front page of the magazine, Johnson splashed the headline "Who was Smallbrow?" Inside, Boris published an article naming Agent Smallbrow as then Sunday Telegraph editor Dominic Lawson.

The allegation was based on a controversial book by renegade spy Richard Tomlinson which had been published in Russia. Tomlinson claimed that Lawson had provided cover for MI6 agents working in Eastern Europe.

Lawson, who denies ever having been an agent, was furious. He told Johnson's biographer Sonia Purnell that the former mayor had put the lives of journalists at risk.

"He knew me, we were friendly - it was intensely annoying. And apart from anything else, if you're running a newspaper with foreign correspondents in strange parts of the world, as I was then, it's potentially a physical threat to them if it's believed that they're working for British intelligence. You can imagine how angry I was."

Johnson was unrepentant, however.

"I rang him up, but there was just this sense of "Never mind, Dommers, I just did it for a laugh. And the thing about Boris is that because in some strange way he is adorable, one forgives him. It's not just women; men too fall for that charm."

Johnson's responsibilities as foreign secretary appear to have been significantly diminished from his predecessors, with responsibility for Brexit negotiations and future trade deals passed to other departments by Theresa May.

A piece by Adam Boulton in this week's Sunday Times also claimed that responsibility for MI6 was "being quietly shifted to the prime minister and National Security Council".

However, the Foreign Office strongly denied this yesterday, telling Politics.co.uk that there were no plans to strip the department of responsibility for the secret service.

"As has been long standing practice, responsibility for SIS and GCHQ lies with the foreign secretary. This has not changed and will not change," a spokesperson said.

The Daily Beast
How the Real Edward Snowden Helped Write the Ending to Oliver Stone's 'Snowden'
Friday, 22 July 2016
Byline: Jen Yamato

Washington - The NSA's worst nightmare made his San Diego Comic-Con debut by way of video chat, moments after the first public screening of Oliver Stone's Snowden.
"The FBI actually gets a copy of this talk because we're going through Google Hangouts, which unfortunately has a sort of built-in surveillance capability," joked Edward Snowden, his face peering down on a theater full of critics and journalists. He joined Stone and stars Joseph Gordon-Levitt and Shailene Woodley from Moscow, his home for the foreseeable future, "live--from the internet."

Snowden tracks the NSA analyst as he wrestles with the decision to blow the lid off of the U.S. government's top-secret global surveillance program, an act that made him persona non grata in America and changed history. The telling of this historic expose, co-scripted by Stone and Kieran Fitzgerald, is authorized by Snowden, who appears as himself in the final coda.

After a dazzling thriller of a finale right out of a spy flick (which, yes, involves a certain Rubik's cube), Stone's larger aims materialize. News footage of President Obama, seen earlier labeling Snowden a "29-year-old hacker," is used to pose a question--the question--seemingly to the President as much as the public at large: Is Edward Snowden a spy or a whistleblower? A traitor or a hero?

Snowden makes its official world premiere in September at the Toronto Film Festival, so bringing a tech-oriented political thriller to a July geekfest filled with superhero fans in spandex cosplay was a curious move. But its official release, timed for a fall Oscar berth, is not slated until September 16th. Thursday at Comic-Con, on the same night Donald Trump accepted the Republican presidential nomination, Stone's film highlighted the fact that Obama still has time to pardon Snowden before he leaves office.

The opportunistic move of sneaking Snowden into the annual pop culture convention appearance worked. Stone grabbed plenty of attention for Snowden by likening Pokémon Go to a form of totalitarianism during a panel earlier in the day. But that evening, he told The Daily Beast he's not banking on Obama rescuing Snowden from perma-exile. I asked if the President is likely to even see the film any time soon. "I hope so," Stone said. "I hope so, but I'm holding no hopes on it."

Live from the internet, Snowden explained why he got involved in a major motion picture retelling of his life. "When there is enough in the public record you don't really get to decide if a movie gets made," he said. Stone was the right director to bring his story to the screen, he said, because "nobody tells Oliver what to do, and that's not the case with a lot of studios. That's a distinguisher that I hope shows through in the final message."

He decided to appear in the movie after Stone flew out to film him for bonus materials, he said. In the film, he professes his newfound purpose while seated at a laptop bearing a sticker for the Electronic Frontier Foundation, a nonprofit organization dedicated to "defending civil liberties in the digital world."

According to Stone, it took nine takes to nail Snowden's scene--the same number of takes it took Trump to film his deleted cameo in Stone's Wall Street: Money Never Sleeps. "I once directed Donald Trump," Stone smiled to the crowd. "It was a hard day. The difference between Donald and Ed--and this is true, I love the man in a weird way--after every take [Trump] jumped up and said, 'Wasn't that great?'"

"The confidence is unbelievable, and that's what's allowing him to run," Stone continued. "I had to say, 'Donald, I think it's great but you know what? I think we can go a little bit better here.'"

Stone also revealed that Snowden made a major contribution to the scripting of the film's climax--a nail-biter that depicts exactly how Snowden managed to get away with the stolen files he would eventually release to the world. In the movie, Snowden anxiously downloads files upon files of documents and hides the SD card inside a Rubik's cube.

After much suspense, he manages to smuggle the cube out through security, smiling his relief into the open air.

Only that's not how he really did it.

"We don't know," Stone admitted. "None of us know. He's the only one who knows and one day he may reveal. It was Ed's idea, his suggestion. We responded to it and ran with it. But it was a good idea. Thank you."

Snowden did not divulge how that scene really unfolded, but he confirmed that life as an international fugitive isn't all that terrible. "I can confirm that I'm not living in a box," he said. "I actually live a surprisingly free life."

"This was not the most likely outcome," he added. "I didn't actually expect to make it out of Hawaii. I thought it was incredibly risky... I never thought I would be saved. But I thought the stories might still be able to get out there."

He slammed the U.S. government, which cancelled his passport and made travelling impossible in the wake of the leak, for threatening trade sanctions against countries that offered him asylum.

"Particularly in the case of Ecuador, they literally got a direct threat, I believe from John Kerry, to revoke trade preferences," he said. "Trade preferences were basically the thing keeping their economy alive--literally, for broccoli farmers and rose farmers. These are impoverished, indigenous farmers, and they were like, 'We're going to make sure these people's families can't eat if you defend this guy's human rights.'"

"But this is not a criticism about the United States specifically, although that's heinous in terms of foreign policy," he continued. "This is truly about the nature of power."

Earlier in the day, Snowden and Andrew "Bunnie" Huang unveiled plans for a device that would prevent the outside surveillance of cell phones. "We're not doing productization, we're not doing sales, we're not setting up a company or anything like that," Snowden clarified. "Just saying anybody who wants to do this, here are our findings."

"I love my country. I love the things that we try to do," he declared. "I have serious policy disagreements with some agencies of government, particularly senior officials. The working level guys by and large are good people trying to do the best they can. But they're often ordered more or less to do bad things, for what they believe to be a good reason."

Speaking from exile in Russia, Snowden seemed content given the circumstances. "I don't have to worry about that anymore."

Bangkok Post
Police bust international hacking suspects
Friday, 22 July 2016

Bangkok - A Russian man and an Uzbek woman were busted by tourist police for their alleged involvement in a transnational hacking scam in which more than 50 people in several countries lost a total of one billion baht, police said.
Surachet Hakphan, commander of the Tourist Police Division, said police arrested Dmitry Ukrainskiy, a 44-year-old Russian, and Olga Komova, a 25-year-old Uzbekistan national, both of whom were wanted by US authorities for hacking into a personal financial database.

More than 50 people from various countries, including the US, Australia, Japan and Britain, were swindled out of more than one billion baht by the two suspects, he added. The police, however, declined to say where the suspects were arrested.

Pol Maj Gen Surachet said the US Federal Bureau of Investigation (FBI) had sought assistance from Thai police to track the two suspects belonging to a computer hacking network as authorities believed Mr Ukrainskiy and Ms Komova were hiding out in Thailand.

Since 2014, US authorities found that financial transactions believed to be carried out by the hacking network were made from several countries to Thailand. A police team was set up to search for the two suspects, Pol Maj Gen Surachet said.

Police found that Mr Ukrainskiy was running a yacht charter business in Pattaya and Ms Komova was working at a hotel in Koh Chang in Trat, he said.

Police said the suspects told investigators they used software that allowed them to gain access to a private computer system and stole the victims' financial information.

The Anti-Money Laundering Office had seized more than one billion baht and frozen more than 50 bank accounts from the network, Pol Maj Gen Surachet said. Meanwhile, a 50-year-old Turkish national has been arrested for robbery, police said.

Abdullah Alp Kaya, who was wanted on an arrest warrant issued by the Southern Bangkok Criminal Court on Wednesday, was caught yesterday at a coffee shop in the Terminal 21 shopping mall on Sukhumvit Road, Lumpini police said.

Investigators said people lodged complaints with police that their notebook computers, tablets, and smartphones were stolen when they were spending time at coffee shops at department stores in Bangkok.

Police said Mr Kaya admitted to police that he had stolen notebook computers and other gadgets from unsuspecting customers.

The Guardian (London)
Surge in cybercrime figures prompts police call for awareness campaign
Friday, 22 July 2016
Byline: Alan Travis

London - Police chiefs have called for a national campaign on online fraud and other cybercrime on the scale of last century's seatbelt and drink-driving campaigns in the wake of figures showing that one in 10 adults have been victims of such offences in the past year.
Chris Greany, City of London police's economic command head, said that with around 1m cases reported in the last year to Action Fraud alone, it was not possible for all cases to be investigated.

On Thursday the Office for National Statistics said there had been more than 5.8m incidents of cybercrime in the past year, far more than previously thought and enough to nearly double the headline crime rate in England and Wales.

The first official estimate of the true scale of online shopping scams, virus attacks, theft of bank details and other online offences was much higher than an initial ONS estimate in October last year, which put the annual figure at 3.8m, or 40% of all crimes.

Greany said fraud now cost an estimated £193bn each year, and with half of all crimes against people in the UK committed from abroad it was becoming more challenging for police to tackle.

"Law enforcement agencies are becoming increasingly successful at targeting the most serious offenders; however, the scale of the challenge is such that prevention, and helping businesses and individuals protect themselves, is the only long-term way of combating the escalating threat," he said. "That includes all industries taking proper steps to protect their customers from becoming victims of fraud."

Greany endorsed a call for a national fraud and cybercrime campaign on a par with the seatbelt and drink-drive campaigns of the 1980s and 90s to create a more internet-savvy society.

Deputy chief constable Peter Goodman, the National Police Chiefs Council lead on cybercrime, said digital crime was no longer a curiosity or a new specialism in policing. "The priorities for law enforcement are to make the UK a hostile place for cyber-criminals to operate, improve the response to victims and develop capabilities in local forces. Transforming our response to these crimes is a challenge but it is a priority for investment in policing," he said.

In March the Metropolitan police commissioner, Sir Bernard Hogan-Howe, faced criticism when he suggested that bank customers who were victims of online fraud should not be refunded by banks if they had failed to protect themselves from cybercrime.

The ONS says one in 10 adults have been victims of cybercrime in the past year. The chance of being a victim is the same regardless of social class or whether someone lives in a deprived or affluent, urban or rural area.

The 5.8m offences were made up of 3.8m fraud offences, including 2.5m incidents of bank and credit card fraud, and 2m computer misuse offences, including 1.4m virus attacks. The remaining 600,000 estimated offences related to unauthorised access to personal information, such as hacking of email, social media or other online accounts.

The latest overall figures, excluding online crime, in the 12 months to March 2015 show there were an estimated 6.3m offences - 6% fewer than in the previous year.

Police crime figures show that the murder rate rose by 34 to 571, the highest in five years. This is still far below the peak in 2002-03, when 1,047 homicides were recorded, but the recent rise is one of the more authoritative indicators that Britain is experiencing an increase in violence. The 96 deaths at Hillsborough in 1989 will be added to the official homicide figures and included in the next set of figures after the inquests finished in April.

Knife crime offences rose by 10% in the past year and gun crime increased by 4% over the same period.

Incidents of harassment, including new categories of offence such as malicious communications online, social media abuse and revenge porn, have risen 90%, from 82,000 to 156,000.

The police figures also show a 27% rise in offences against the person and a 21% increase in sexual offences. Those figures include a 22% increase in reported rapes from 29,300 to 35,798. By contrast, the crime survey shows no significant change in the proportion of adults who say they had been a victim of a sexual assault in the past year. The ONS said the 21% increase in sexual offences reflected both an improvement in police recording of the offences and a greater willingness of victims to come forward.

But the overall picture of all crime - excluding the 5.8m online offences - according to the crime survey of England and Wales, which is regarded as the best measure of crime trends, shows a 6% fall to 6.3m offences involving adult victims in the 12 months to March 2016.

The long- term trends in "traditional" crimes such as burglary, car thefts and criminal damage show that the fall in crime since its 1995 peak has slowed down since 2005. The crime survey found there had been no change in the overall level of violent crime compared with the previous year.

The online crime numbers give the first official snapshot of the scale of the threat from online attacks and scams. However, ONS statisticians said it would be "misleading to conclude that this means actual crime levels have doubled, since the survey previously did not cover these offences".

The first estimate is based on a 9,000-strong sample size from six months of interviews from the crime survey. Only when the ONS has 12 months of data in January will the online crime figures be incorporated into the headline crime rate.

Separate Home Office figures for police officer numbers show they fell by a further 3,126 last year to 124,000 - the lowest level since 2003.

Andy Burnham, the shadow home secretary, said: "At long last, we have the true picture of crime in England and Wales and it puts the former home secretary's record in a new light.

"Our new PM [Theresa May] was fond of saying that crime is falling but, as people can see, crime has moved online and until now the official statistics haven't shown that. Her complacent claims do not read well alongside these worrying increases in violent crime, sexual crime and homicide.

"The only conclusion that can be drawn is that it is the wrong time to be cutting the police. The PM promised real-terms protection but has failed to deliver it. Now that decision is entirely within her hands, she must honour the promise that she made and protect frontline policing," he said.

The policing minister, Brandon Lewis, said: "As crime falls, we know that it is also changing. Fraud and cyber-offences are not a new threat and the government has been working to get ahead of the game, committing to spend £1.9bn on cybersecurity and cybercrime over the next five years. We have also established the joint fraud taskforce, bringing together law enforcement and the banking sector, while Action Fraud, the National Fraud Intelligence Bureau and the National Crime Agency are working to improve our response.

"We welcome today's experimental ONS figures on fraud and cybercrime - offences which we have always known were happening but were previously unable to quantify. Having an accurate national picture will be crucial to inform future action."

New York Times
Pyongyang Radio Revives Coded Broadcasts for Spies
Friday, 22 July 2016
Byline: Choe Sang-Hun

Seoul - In an era of sophisticated spycraft, North Korea appears to be returning to the days of shortwave radio.

The North broadcast a series of seemingly random numbers on Pyongyang Radio twice recently, an eerie reminder of the days when the North encrypted messages to its spies in South Korea.

In the latest episode last Friday, an announcer read what she described as "a mathematics review assignment for investigative agent No. 27," engaged in a "distance learning" program.

"Turn to Page 459, No. 35; Page 913, No. 55; Page 135, No. 86," she said, continuing to cite numbers for 14 minutes.

Decades ago, it was not unusual for late-night radio listeners in the South to hear mysterious numbers arriving on static- filled signals from the North. The South Korean government in Seoul tried to block the signals and barred its citizens from listening.

Kim Dong-sik, a former intelligence officer for North Korea, said he used to listen for such broadcasts at midnight each night to check whether his spymasters had a message for him. Mr. Kim was caught by the South in 1995 after a gun battle with South Korean agents and police officers.

"When I arrived in the South, I had five different call signs assigned to me," said Mr. Kim, who now works as a senior analyst at the Institute for National Security Strategy, a think tank run by South Korea's National Intelligence Service. "Each night, I listened for my call signs."

The June 24 and July 15 broadcasts, confirmed by the South Korean government on Wednesday, were the first such coded messages in 16 years, leaving intelligence officials and analysts puzzled by the North's motives.

The broadcasts come amid concerns about the North, which has raised tension with the United States and its allies by conducting a series of missile tests and has issued bold claims of advances in its quest for a nuclear-tipped long-range missile.

North Korea has reacted strongly to a plan by the United States to deploy an advanced missile defense system in the South. This week, it fired three ballistic missiles, saying that they were used in simulated tests to detonate nuclear warheads over seaports and airfields in the South, where American reinforcements are supposed to arrive in the event of a war.

The tests defied a new round of sanctions that the United Nations Security Council imposed against the North after a nuclear test in January and a long-range rocket launch in February.

Jeong Joon-hee, a government spokesman for South Korea, has called the resumption of the broadcasts "seriously regrettable" but declined to comment on any motives. "The North should abandon its old ways," he said.

South Korea itself has resorted to old-school propaganda in recent years, resuming loudspeaker and radio broadcasts into the North and juicing them up with synthesized Korean music known as K-pop.

Some analysts said the North's use of a bygone encryption tool was rekindling old fear among South Koreans of an escalation in psychological warfare. North Korea stopped sending out such coded messages by shortwave radio after the Koreas held a summit meeting in 2000, agreeing to de-escalate the Cold War- era intrigue on the divided peninsula.

Since then, the North is believed to have adopted more sophisticated methods of communication. When the South's intelligence service announced the capture of a spy ring in 2011, it said that the officers contacted the North through steganography, a technique for encrypting a message into a text, image or video file delivered online.

Mr. Kim, the analyst and former spy, said the broadcasts should be taken seriously. He said the North appeared to be bolstering its espionage operations since 2009, when it created the General Bureau of Reconnaissance by merging various party and military agencies in charge of sending spies to the South.

Washington blacklisted the bureau after North Korean hackers were accused of wreaking havoc on the computer network of Sony's movie studio in 2014.

At a time when the counterintelligence authorities use sophisticated technology to monitor the digital communication of espionage suspects, "the old number broadcasts are still a dependable and preferable means of communication for spies," Mr. Kim said.

"We should assume that the North is using the radio broadcasts to communicate with its agents here or is at least using them to train spies," he added.

He recalled that when he was training in the 1980s, he spent countless hours listening to tape- recorded broadcasts and copying the numbers to master a so-called numbers station technique of encrypted communication.

Mr. Kim said he and his handlers in the North used an agreed-upon book -- "Whale Hunt," a popular novel in the South -- to decipher one another's codes. As in the broadcast on Friday, a typical five-digit combination started with a three-digit page number. The remaining two digits pointed at two Korean characters in the text of the page.

The two Koreas still accuse each other of spying. The North is holding at least four South Koreans, some of them sentenced to a labor camp for life, on charges of espionage.

In recent years, the South's intelligence service has arrested people it deemed spies as they entered the country disguised as refugees. Last week, prosecutors said they arrested two South Korean men on

charges of spying for the North. They released closed- circuit video of counterespionage officers overpowering a suspect at an internet cafe.

The men used encrypted emails to contact their handlers in the North, the prosecutors said.

Mr. Kim said that during his days as a spy, the radio was a main tool of communication.

"If there was a certain song broadcast by Pyongyang Radio at an agreed-upon hour, that meant that there was something wrong and I should immediately abort my mission," he said. "If not, it was all clear."

Gulf News
Beware ransomware attacks on your PC
Friday, 22 July 2016
Byline: Faisal Masudi

Dubai - Ransomware, a relatively new kind of cyber attack where criminals demand money for decrypting files they have taken control over, is increasingly targeting ordinary consumers -- including those in the UAE -- a new study said on Wednesday.
Security firm Symantec said in its latest research the average ransom demanded by attackers jumped to $679 (Dh2,491), up from $294 (Dh1,078) at the end of 2015.

The "Internet Security Threat Report (ISTR) Special Report: Ransomware and Businesses 2016" revealed consumers make up 57 per cent of ransomware victims.

The majority of ransomware variants are designed to attack Windows computers and ordinary home users continue to be one of the biggest victim groups, it added. Meanwhile, employees at organisations make up 43 per cent of ransomware victims.

According to Symantec's 2016 ISTR, the UAE experienced the fourth highest rate in ransomware attacks in the Middle East and Africa region, added Hussam Sidani, regional manager for Gulf, Symantec.

Furthermore, ransomware attacks grew by 44 per cent year-on-year in the UAE in 2015. "In 2015, we saw an average of 28 attacks per day and 10,279 total attacks on UAE-based organisations," Sidani said.

"Additionally, given the strong uptake of smartphones and tablets, we're seeing more mobile devices coming under attack, with attackers encrypting files, and anything else an owner will pay to recover.

"The UAE has one of the highest penetration of smartphones in the world and users enjoy great connectivity here. This can make them a very lucrative target for ransomware."

Sidani explained that one of the most common methods to spread ransomware, and malware in general, is through malicious spam email. These spam emails pose as an important email from a well-known organisation, such as a shipping or utility company. However, as soon as the user opens the malicious attachment or link, malware will be installed on their device or computer. Following this, the user's important files will be encrypted and they will receive a message demanding a ransom to release the files.

Victims can be asked to send ransom money via a payment link or by handing over their credit card information. However, Symantec's recommendation is not to pay the ransom.

"While we recognise that some organisations may feel that paying the ransom is their only option, there is no guarantee that this will recover their data. Attackers may not send a decryption key, could poorly implement the decryption process and damage files, and may deliver a larger ransom demand after receiving the initial payment."

Don't click links in unsolicited email or social media messages, particularly from unknown sources. Use strong and unique passwords for your accounts and devices, and update them on a regular basis.

When installing a network-connected device, or downloading a new app, review the permissions to see what data you're giving up. Disable remote access when not needed. Antivirus-only security is no longer enough to combat security threats like ransomware. Protect your data with a multi-platform solution and back up your computer and devices on a regular basis.

New York Times
Snowden to Help Develop a Safer Phone for Journalists
Friday, 22 July 2016
Byline: John Markoff

Cambridge, Mass. - The former National Security Agency contractor Edward J. Snowden said Thursday that he planned to help develop a modified version of Apple's iPhone for journalists who are concerned that they may be the target of government surveillance.
The announcement was made during a one-day conference on "Forbidden Research" held at the Massachusetts Institute of Technology's Media Lab.

Mr. Snowden, who spoke via a video connection from Russia, where he is living in exile, said he was working with Andrew Huang, a computer hacker known as Bunnie who studied electrical engineering at M.I.T., to see if it would be possible to modify a smartphone to alert journalists working in dangerous environments to electronic surveillance.

Mr. Snowden, who is a board member of a nonprofit group called the Freedom of the Press Foundation, said he was concerned that cellphones and smartphones serve as tracking devices that automatically

create electronic dossiers that give third parties, including governments, detailed information on location.

As an example of the dangers of location data, he cited the mortar attack in 2012 by the Syrian government that killed Marie Colvin, an American journalist who was reporting in Homs, Syria, for The Sunday Times of London.

"The radio frequency emissions of her communications that she used to file those news reports were intercepted by the Syrian Army," he said.

He said it was increasingly difficult for users to trust their smartphones. They may be tampered with by malware programs, causing them to transmit location information even when the user may believe that the device has been placed into a safe "airplane mode."

Mr. Huang said the project was still experimental, but he hoped it would provide journalists with modified phones that would come in a special case with a separate display that would provide an alert when the phone was active and transmitting data at improper times.

The conference focused on issues raised by computer hacking, as well as controversial scientific research in areas such as genetic engineering and geoengineering.

Also at the conference, Reid Hoffman, one of the founders of LinkedIn, which recently agreed to be acquired by Microsoft for $26 billion, announced that he planned to offer a $250,000 "Disobedience Prize" aimed at promoting positive social change and opposing injustice.

"It will go to a person or group engaged in what we believe is excellent disobedience for the benefit of society. The disobedience that we would like to call out is the kind that seeks to change society in a positive way, and is consistent with a set of key principles," wrote Joichi Ito, director of the M.I.T. Media Lab, in a web posting about the prize. The timing of the award has not yet been determined.

In separate panels, biologists and climate scientists explored the risks and rewards of scientific research that might have unexpected consequences.

Kevin Esvelt, a biologist who is director of the Sculpting Evolution research group at the M.I.T. Media Lab, spoke about new, easily accessible genetic engineering technologies that might be used to preserve species that are at risk of extinction, and alternatively to eradicate pests that threaten human populations by spreading disease.

He described a discussion scientists had on Wednesday with residents of Martha's Vineyard about the use of advanced genetic engineering techniques to introduce a type of mouse that had been modified to be unable to carry Lyme disease. The idea would be to break the transmission of the disease to ticks and then to humans.

He said that before beginning the experiment, the scientists engaged the community to discuss potential risks.

Scientists on several panels acknowledged that it was impossible to be certain about unforeseen effects from new engineering techniques.

"What we're worried about is something that we do that could be very attractive in the short term but have some triggering mechanism or some slow events that occur far in the future," said George Church, a Harvard geneticist who is exploring genetic engineering techniques to revive extinct species.

Gulf News
Lack of funds and training hamper cybersecurity
Friday, 22 July 2016
Byline: Staff Report

Dubai - Poor funding and lack of skilled staff remain serious challenges for global business IT security, according to a new survey by Accenture and HfS Research.
And insider data theft and malware attacks are the most significant threats, with 69 per cent of survey respondents saying they had suffered attempted or successful theft or corruption of data by insiders in the previous 12 months.

The survey, The State of Cybersecurity and Digital Trust 2016, polled 200 security executives and IT professionals in different countries and in different sectors.

Findings indicate that there are significant gaps between talent supply and demand, a disconnect between security teams and management expectations, and considerable disparity between budget needs and actual budget realities.

"Our research paints a sobering picture. Security leaders believe threats are not going away, in fact they expect them to increase and hinder their ability to safeguard critical data and establish digital trust," said Kelly Bissell, senior managing director, Accenture Security. "At the same time, while organisations want to invest in advanced cyber technologies, they simply don't have enough budget to recruit or train skilled people to use that technology effectively."

"While the gaps we identified can be overcome, they do collectively underscore the need for an inherently different approach, one that includes more robust risk management measures and the development of digital trust," said Fred McClimans, research vice president, Digital Trust and Cybersecurity, HfS Research.

London Times
One in ten become victims of cybercrime
Thursday, 21 July 2016
Byline: Richard Ford

London - One in ten adults have been victims of fraud or computer misuse offences, according to official figures published today.
An estimated 5.8 million fraud and cyberoffences are committed annually, pushing the overall crime figures in England and Wales to more than 12 million.

The first official estimate of the scale of online shopping scams, virus attacks, ticket frauds, computer hacking and theft of bank details along with credit and bank card fraud shows that fraud is the most common crime experienced by the public.

The chance of being a victim of victim of fraud is the same regardless of class, region and whether a person lives in a rural or urban area, according to the Crime Survey of England and Wales.

Official crime figures from the Office for National Statistics (ONS) showed that excluding fraud and cybercrime, there were 6.3 million crimes in the 12 months to March 2016, a fall of 6 per cent.

Separate police-recorded crime figures for murder rose by 34 to 571 homicides, the highest level for five years

Police figures also showed a 27 per cent rise in offences against the person and a 21 per cent increase in sexual offences. Statisticians said the rise in both types of offences was due to better recording practices by the police and that the increase in sex crimes was also due to a willingness of more victims to report offences.

Incidents of revenge porn and harassment, including online abuse, accounted for almost half the rise in personal violence.

The confirmation of the high volume of online crime provides the first official snapshot of the scale of threat from online attacks and scams.

Statisticians said "it would be misleading to conclude that this means actual crime levels have doubled, since the survey previously did not cover these offences".

The first estimate is based on a 9,000 sample size from six months of interviews from the survey.

Only when the ONS has 12 months of data in January will the online crime figures be incorporated into the headline crime rate for England and Wales.

The 3.8 million frauds included 2.5 million bank and credit account cases plus one million sales, tickets and computer software service frauds.

There were a further 0.1 million incidences involving lottery scams and frauds linked to dating sites.

Of the two million computer misuse incidents, 1.4 million involved computers being infected with viruses and 0.6m incidents of hacking of e-mail, social media or other online accounts.

The Intercept
Edward Snowden's New Research Aims to Keep Smartphones From Betraying Their Owners
Thursday, 21 July 2016
Byline: Micah Lee

Washington - In early 2012, Marie Colvin, an acclaimed international journalist from New York, entered the besieged city of Homs, Syria, while reporting for London's Sunday Times. She wrote of a difficult journey involving "a smugglers' route, which I promised not to reveal, climbing over walls in the dark and slipping into muddy trenches." Despite the covert approach, Syrian forces still managed to get to Colvin; under orders to "kill any journalist that set foot on Syrian soil," they bombed the makeshift media center she was working in, killing her and one other journalist and injuring two others.
Syrian forces may have found Colvin by tracing her phone, according to a lawsuit filed by Colvin's family this month. Syrian military intelligence used "signal interception devices to monitor satellite dish and cellphone communications and trace journalists' locations," the suit says.

In dangerous environments like war-torn Syria, smartphones become indispensable tools for journalists, human rights workers, and activists. But at the same time, they become especially potent tracking devices that can put users in mortal danger by leaking their location.

National Security Agency whistleblower Edward Snowden has been working with prominent hardware hacker Andrew "Bunnie" Huang to solve this problem. The pair are developing a way for potentially imperiled smartphone users to monitor whether their devices are making any potentially compromising radio transmissions. They argue that a smartphone's user interface can't be relied on to tell you the truth about that state of its radios. Their initial prototyping work uses an iPhone 6.

"We have to ensure that journalists can investigate and find the truth, even in areas where governments prefer they don't," Snowden told me in a video interview. "It's basically to make the phone work for you, how you want it, when you want it, but only when."

Huang made a name for himself by using a technique known as reverse engineering to hack into Microsoft's Xbox and other hardware devices locked down using various forms of encryption, and Snowden said he's been an invaluable research partner.

"When I worked at the NSA, I worked with some incredibly talented people," Snowden said, "but I've never worked with anybody who had such an incredible outpouring of expertise than I have with Bunnie."

Snowden and Huang presented their findings in a talk at MIT Media Lab's Forbidden Research event today and published a detailed paper.

Location Privacy and Smartphones

Smartphones come with a variety of different types of radio transmitters and receivers: cellular modems (for phone calls, SMS messages, and mobile data), wifi, bluetooth, and others. But using any of these radios could leak your physical location to an adversary who is watching the airwaves.

Journalists and activists use their phones to communicate with sources and colleagues, post updates and livestream to social media, and accomplish countless other networked tasks. If they need to keep their location secret, for example in a war zone, they need to turn off all of the radios within their phones. Even so, phones can still be vital tools even when offline; internet access is not needed to take photographs, record video or audio, take notes, use certain maps, or manage schedules.

Snowden and Huang have been researching if it's possible to use a smartphone in such an offline manner without leaking its location, starting with the assumption that "a phone can and will be compromised." After all, journalists and activists are often under-resourced and face off against well-funded intelligence services. They also, necessarily, use their phones to talk to, and open documents from, a wide variety of sources, leaving them especially vulnerable to targeted phishing, or "spearphishing," attacks, where an attacker baits a victim into opening an enticing document that actually contains an exploit.

The research is necessary in part because the most common way to try to silence a phone's radio -- turning on airplane mode -- can't be relied on to squelch your phone's radio traffic. "Malware packages, peddled by hackers at a price accessible by private individuals, can activate radios without any indication from the user interface," Snowden and Huang explain in their blog post. "Trusting a phone that has been hacked to go into airplane mode is like trusting a drunk person to judge if they are sober enough to drive."

Introspection Engine

Since a smartphone can essentially be made to lie about that state of its radios, the goal of Snowden and Huang's research, according to their post, is to "provide field-ready tools that enable a reporter to observe and investigate the status of the phone's radios directly and independently of the phone's native hardware." In other words, they want to build an entirely separate tiny computer that users can attach to a smartphone to alert them if it's being dishonest about its radio emissions.

Snowden and Haung are calling this device an "introspection engine" because it will inspect the inner-workings of the phone. The device will be contained inside a battery case, looking similar to a smartphone with an extra bulky battery, except with its own screen to update the user on the status of the radios. Plans are for the device to be able to sound an audible alarm and possibly also to come equipped with a "kill switch" that can shut off power to the phone if any radio signals are detected. "The core principle is simple," they wrote in the blog post. "If the reporter expects radios to be off, alert the user when they are turned on."

The introspection engine also must fit a number of design goals, including: It should be entirely open source, with open hardware, to make it easy for experts to inspect; it should operate in a separate "security domain" than the phone. Basically, the introspection engine should work even if the phone is hacked and actively lying to you; it should have a simple and intuitive user interface and require no special training to use; it should be usable on a daily basis with minimal impact on workflow.

Introspection engines don't exist yet, and the research Snowden and Huang presented today is only the beginning. In order to begin work on a prototype, the pair needed to pick a specific model of smartphone to target. They chose the 4.7-inch iPhone 6, based on their understanding of "the current preferences and tastes of reporters." However, introspection engines could be designed for any model phone.

Jacking Into the iPhone

Huang, an American who currently lives in Singapore, traveled to the metropolis of Shenzhen, China, to explore the electronics markets of Hua Qiang, which he described as "ground zero for the trade and practice of iPhone repair." While there, he bought spare parts and repair manuals that contained detailed blueprints of the target device.

Using information gleaned from these manuals, Snowden and Huang discovered that the iPhone's logic board has several test points designed by the manufacturer that can be exploited to learn the status of various on-board radios. These test points, which are built-in to many consumer devices, are crucial to improving customer experience. When a customer returns a defective device, engineers rely on them to determine the cause of the defect.

Snowden and Huang discovered 12 test points that could be used to monitor the status of the cellular radios, the GPS radio, and the wifi and bluetooth radios. While they didn't find a test point to monitor the Near Field Communication chip, the part that makes Apple Pay possible, they discovered that they could disconnect its antenna, vastly reducing its range.

They don't think that modifying an iPhone 6 to install an introspection device could be done by just anyone, but "any technician with modest soldering skills can be trained to perform these operations reliably in about 1-2 days of practice on scrap motherboards."

Supply Chain

The next step is to develop a working prototype, which Snowden and Bunnie hope to complete over the next year. Their blog post says that the project is currently operating on a "shoestring budget" and "donated time."

If it proves successful, they may seek funding through the Freedom of the Press Foundation to develop and maintain a supply chain. The nonprofit, of which both Snowden and I are board members, could then distribute iPhones that have been modified to include introspection devices to journalists who work in dangerous environments to use in the field.

Lebanon Daily Star
Touch witness completes testimony at STL
Friday, 22 July 2016
Byline: Susannah Walden

Beirut - Protected witness PRH 705 completed his testimony Thursday as the designated representative of the MTC touch cellular network at The Special Tribunal for Lebanon. Touch is one of Lebanon's two GSM networks, the second of which, Alfa has been represented by PRH 707 - another protected witness. Both networks turned over reams of extensive records concerning billingrecords, call logs and coverage maps at the request of investigators.
Prosecutors have built much of their case against the five defendants accused of conspiring to assassinate former Prime Minister Rafik Hariri on this telecommunications data. Prosecutors argue that the data can be used to retrace the movements of the defendants.

Defense attorney Thomas Hannis, representing the interests of Salim Ayyash, completed his cross-examination of the witness by clarifying comments about some of the documents handed over by the network.

The records were a source of debate at the trial, as defense attorneys contested submitting documents into evidence if the witness could not personally attest to their origin.

Hannis had previously voiced his doubt at a May appearance of PRH 705. "This witness has been placed in a very difficult position. He's speaking for the community," he said. "We have a concern that we won't be able to have fair trial for our clients if we're not able to have a meaningful cross-examination of the underlying sources of evidence."

The final appearance of PRH 705 focused on clarifications. "I apologize your honor, this may seem detailed and fiddly, but it won't take long and may be important for our submission later on," Hannis said.

After the lunch recess, Prosecutor Fabia Wong took over to ask the witness several questions on records submitted concerning cellphone handsets that prosecutors allege were used by the deceased Hezbollah commander Mustafa Badreddine. Legal proceedings against Badreddine were halted after an Appeals Chamber found there was sufficient evidence that he was killed in Syria in May.

The investigation into controversial telecommunications data will continue with further testimony from Alfa representative PRH 707, however Thursday's session ended PRH 705 contribution for the time being.

Judge David Re, the Trial Chamber president, highlighted the weight the telecommunications evidence has carried in the proceedings as PRH 705's testimony concluded.

"[There was a] considerable amount of interest in what you had to say based on the number of questions from the counsel and the bench itself. You're free to go ... As they say, don't call us, we'll call you," he said.

Yonhap News Agency
Gov't bolsters countermeasures to deter N.K. cyberattacks
Friday, 22 July 2016
Byline: Staff reporter

Seoul - South Korea is beefing up its governmentwide countermeasures to prevent possible cyberattacks by North Korea, officials said Friday.
The Ministry of Science, ICT and Future Planning said the number of cyberattacks by North Korea more than doubled in the first half of this year.

The cyberattacks "are judged as a part of North Korean provocations to trigger public anxiety" in South Korea, the ministry said.

Last month, South Korean police said North Korea hacked into more than 140,000 computers at 160 South Korean firms and government agencies. About 42,000 documents were suspected to have been stolen, including defense-related information.

The ministry urged people to install antivirus software and avoid opening suspicious emails.

South Korea has been on high alert against hacking attacks by North Korea following the North's fourth nuclear test in January and a series of missile launches in recent months.

Huffington Post
Where Is The Accountability For Ottawa's Communications Spies?
Friday, 22 July 2016
Byline: Monia Mazigh

Commentary: The Communications Security Establishment (CSE) Commissioner report has been just released. For those who don't know what the CSE is, it is the agency related to the Department of National Defence that spies on communications received from abroad.
In their own words, their work focuses on "collecting foreign signals intelligence in support of the Government of Canada's priorities, and on helping protect the computer networks and information of greatest importance to Canada." It is important to emphasize that CSE is not supposed to spy on communication of Canadians in Canada or abroad.

In that regard, the commissioner's mandate is mainly to review CSE activities and their compliance with the law, and in the case of complaints, to undertake investigation. However, the commissioner report, which is supposed to be an independent exercise conducted by a review body, seems more and more like a self-congratulatory document where criticism directed at the CSE or its activities is hard to find. The situation can be compared to a professor rating her own students in a national competition. Of

course, she would like them to pass, and of course she would be lenient in marking. Rather, in such circumstances we need a professor from a different school, and the students' names should be hidden.

In previous years, two main problems became clear to the public in regard to CSE activities:

The stipulations protecting the privacy of Canadians are not always respected, as CSE was reminded by Privacy Commissioner Daniel Therrien.

The lack of safeguards when it comes to information sharing with other agencies -- the Canada Security Intelligence Agency (CSIS), for example.

Indeed, in defence of the CSE's activities, Minister of National Defence Harjit Sajjan recently minimized the amount of information revealed through metadata, usually collected by CSE during its operations. Metadata, or data on data, shouldn't be of a privacy concern for Canadians, according to minister Sajjan.

But the reality is that through the records of Internet and phone communications, even without revealing the identity of the user, much information can still be inferred and shared with other foreign agencies. There exists today a whole range of science fields and theories that can extract patterns about people behaviours without knowing their identities.

The report claims that the commissioner's office "is monitoring 14 active recommendations that CSE is working to address -- 10 outstanding recommendations from previous years and four from this year," and that the privacy issue about sharing foreign intelligence is also being looked into. Nevertheless, we can't know for sure how this is being done and if there is any proposed legislation to be submitted soon. The report doesn't tell us.

It seems from the report that, in general, the commission recommends that the minister should always be informed about controversial issues, but no specific mechanism is suggested to deal with the identified problems. The issue of transparency becomes a matter of blind trust in the hands of the minister of national defence.

Leaving it up to the minister in charge to decide what is acceptable and what is not, or what is lawful and what is not, is far from a democratic and accountable model. We need review mechanisms with the necessary autonomy, independence and structure to create true accountability.

For instance, the ambiguous relationship between CSE and CSIS, described in the report, can't be investigated by any review body. There are currently agencies to oversee respectively CSIS (SIRC) and the CSE (the office of the CSE commissioner), but there is no "super-SIRC" to oversees them both and launch investigations on both of them. The parliamentary oversight presented by the government in Bill C-22 isn't clear if this aspect will be included in its mandate.

As of yesterday, it was reported that CSE won't even reveal the number of times it shared information that could lead to someone being tortured in foreign prisons. The greater the risk of mistreatment (please note how the word "torture" isn't even used), the higher level of bureaucratic or political intervention is required.

Once again, it is up to the minister or a high-level bureaucrat to take that decision, and that risks him or her making a mistake in their assessment. If that happens, Canada will become collateral damage like it has in the past.

New Straits Times
Govt to improve security in airports
Friday, 22 July 2016
Byline: Fazleena Aziz

Sepang - The government will soon introduce a new mechanism to boost security in airports, especially at boarding gates.
Deputy Transport Minister Datuk Abdul Aziz Kaprawi said the mechanism would take into consideration existing operational procedures.

He said that given the increased terror threats globally, especially in transportation hubs, upgrading security was paramount to ensure people's safety.

Aziz said ministry secretary-general Datuk Seri Saripuddin Kasim had been directed on Wednesday to draw up details of the new mechanism through a committee, which would include agencies and departments.

"Some of the issues that pose obstacles, in terms of beefing up security, which we will have to consider, are airport design, businesses and visitors sending off their loved ones.

"But we have to increase security and safety in airports as the threat is real, especially in light of the attacks in Brussels and Istanbul."

He said this after opening the 13th Steering Committee Meeting of Cooperative Aviation Security Programme Asia-Pacific Region (CASP-AP) 2016 yesterday.

Aziz, however, said Kuala Lumpur International Airport complied with International Civil Aviation Organisation (ICAO) security standards, adding that the last audit was done in 2012, while the next audit was due next year.

He said he wanted the Department of Civil Aviation (DCA) to come up with stricter measures to screen potential staff and those working in airports to minimise insider threats.

As most contract workers could also be foreigners, proper screening was vital to ensure no one slipped through the system, he added.

Earlier, he said insider threats could come in the form of former employees, current employees, contract workers or partners who had inside knowledge of the industry.

He said such threats were capable of exploitation, tampering, fraud, espionage, theft and sabotage.

Cyber threats to computer systems were also a matter of concern with increasing reliability on technology, he said, adding that such attacks could cause disruptions.

It was reported that the government was considering a cabinet proposal to allow only passengers to enter terminals in major airports to boost security.

Deputy Prime Minister Datuk Seri Dr Ahmad Zahid Hamidi had said Transport Minister Datuk Seri Liow Tiong Lai had been instructed to work out this proposal with Malaysia Airports Holdings Bhd.

Present yesterday were DCA director of aviation security Abdul Rahmat Mahat and ICAO Asia and Pacific Office regional officer Ross Lockie.

Voice of America
Russian Agent Sentenced for Illegally Exporting US High-tech Gear
Friday, 22 July 2016

New York - A federal court in New York on Thursday sentenced an admitted agent of the Russian government to 10 years in prison and ordered him to forfeit $500,000 in profit he'd gained from his criminal activity, which focused on acquiring and secretly shipping abroad high-tech microelectronics for Russian military equipment.
Alexander Fishenko pleaded guilty to all 19 charges brought by the Department of Justice. U.S. officials said a company that Fishenko had founded shipped $50 million worth of electronic products to Russia between 2002 and 2012, all in defiance of a government licensing system meant to control such exports.

"These commodities have applications and are frequently used in a wide range of military systems," U.S. officials said, "including radar and surveillance systems, missile guidance systems and detonation triggers."

Charges against Fishenko, who has both American and Russian citizenship, included conspiracy, illegally exporting controlled products, conspiring to launder money and obstruction of justice. He was indicted in October 2012, along with 10 other individuals and two corporations, both of which Fishenko

controlled. Three of the people remain at large, but the others either have pleaded guilty or been convicted in court.

To evade export controls on high-tech products manufactured in the United States, officials said, Fishenko and his co-conspirators gave false information about who was buying the electronic components, concealed the fact they were exporters and falsely described the devices on records submitted to the U.S. Department of Commerce.

Ultimate recipients of the electronic components acquired by Fishenko's companies, known as ARC and Apex, included a research unit for the Russian internal security agency FSB, a Russian entity that builds air and missile defense systems, and another that produces electronic warfare systems for the Russian Ministry of Defense.

Assistant Attorney General John Carlin said prosecuting those who violate U.S. export laws is "an important part of our national security framework ... protecting national assets from ending up in the hands of our potential adversaries."

Politics.co.uk
Boris Johnson once outed MI6 spy 'for a laugh'
Wednesday, 20 July 2016
Byline: Adam Bienkov

London - There was some nervousness in the Foreign Office when it was announced that Boris Johnson had been made foreign secretary.
Part of Johnson's new role involves overseeing MI6. This is a highly sensitive and delicate task which some within his department worry he is unsuited for.

It now appears there is good reason for them to feel uneasy.

In 2001, while editor of the Spectator, Johnson published a piece suggesting that a former friend and colleague had worked for the secret service.

On the front page of the magazine, Johnson splashed the headline "Who was Smallbrow?" Inside, Boris published an article naming Agent Smallbrow as then Sunday Telegraph editor Dominic Lawson.

The allegation was based on a controversial book by renegade spy Richard Tomlinson which had been published in Russia. Tomlinson claimed that Lawson had provided cover for MI6 agents working in Eastern Europe.

Lawson, who denies ever having been an agent, was furious. He told Johnson's biographer Sonia Purnell that the former mayor had put the lives of journalists at risk.

"He knew me, we were friendly - it was intensely annoying. And apart from anything else, if you're running a newspaper with foreign correspondents in strange parts of the world, as I was then, it's potentially a physical threat to them if it's believed that they're working for British intelligence. You can imagine how angry I was."

Johnson was unrepentant, however.

"I rang him up, but there was just this sense of "Never mind, Dommers, I just did it for a laugh. And the thing about Boris is that because in some strange way he is adorable, one forgives him. It's not just women; men too fall for that charm."

Johnson's responsibilities as foreign secretary appear to have been significantly diminished from his predecessors, with responsibility for Brexit negotiations and future trade deals passed to other departments by Theresa May.

A piece by Adam Boulton in this week's Sunday Times also claimed that responsibility for MI6 was "being quietly shifted to the prime minister and National Security Council".

However, the Foreign Office strongly denied this yesterday, telling Politics.co.uk that there were no plans to strip the department of responsibility for the secret service.

"As has been long standing practice, responsibility for SIS and GCHQ lies with the foreign secretary. This has not changed and will not change," a spokesperson said.

The Daily Beast
How the Real Edward Snowden Helped Write the Ending to Oliver Stone's 'Snowden'
Friday, 22 July 2016
Byline: Jen Yamato

Washington - The NSA's worst nightmare made his San Diego Comic-Con debut by way of video chat, moments after the first public screening of Oliver Stone's Snowden.
"The FBI actually gets a copy of this talk because we're going through Google Hangouts, which unfortunately has a sort of built-in surveillance capability," joked Edward Snowden, his face peering down on a theater full of critics and journalists. He joined Stone and stars Joseph Gordon-Levitt and Shailene Woodley from Moscow, his home for the foreseeable future, "live--from the internet."

Snowden tracks the NSA analyst as he wrestles with the decision to blow the lid off of the U.S. government's top-secret global surveillance program, an act that made him persona non grata in America and changed history. The telling of this historic expose, co-scripted by Stone and Kieran Fitzgerald, is authorized by Snowden, who appears as himself in the final coda.

After a dazzling thriller of a finale right out of a spy flick (which, yes, involves a certain Rubik's cube), Stone's larger aims materialize. News footage of President Obama, seen earlier labeling Snowden a "29-year-old hacker," is used to pose a question--the question--seemingly to the President as much as the public at large: Is Edward Snowden a spy or a whistleblower? A traitor or a hero?

Snowden makes its official world premiere in September at the Toronto Film Festival, so bringing a tech-oriented political thriller to a July geekfest filled with superhero fans in spandex cosplay was a curious move. But its official release, timed for a fall Oscar berth, is not slated until September 16th. Thursday at Comic-Con, on the same night Donald Trump accepted the Republican presidential nomination, Stone's film highlighted the fact that Obama still has time to pardon Snowden before he leaves office.

The opportunistic move of sneaking Snowden into the annual pop culture convention appearance worked. Stone grabbed plenty of attention for Snowden by likening Pokémon Go to a form of totalitarianism during a panel earlier in the day. But that evening, he told The Daily Beast he's not banking on Obama rescuing Snowden from perma-exile. I asked if the President is likely to even see the film any time soon. "I hope so," Stone said. "I hope so, but I'm holding no hopes on it."

Live from the internet, Snowden explained why he got involved in a major motion picture retelling of his life. "When there is enough in the public record you don't really get to decide if a movie gets made," he said. Stone was the right director to bring his story to the screen, he said, because "nobody tells Oliver what to do, and that's not the case with a lot of studios. That's a distinguisher that I hope shows through in the final message."

He decided to appear in the movie after Stone flew out to film him for bonus materials, he said. In the film, he professes his newfound purpose while seated at a laptop bearing a sticker for the Electronic Frontier Foundation, a nonprofit organization dedicated to "defending civil liberties in the digital world."

According to Stone, it took nine takes to nail Snowden's scene--the same number of takes it took Trump to film his deleted cameo in Stone's Wall Street: Money Never Sleeps. "I once directed Donald Trump," Stone smiled to the crowd. "It was a hard day. The difference between Donald and Ed--and this is true, I love the man in a weird way--after every take [Trump] jumped up and said, 'Wasn't that great?'"

"The confidence is unbelievable, and that's what's allowing him to run," Stone continued. "I had to say, 'Donald, I think it's great but you know what? I think we can go a little bit better here.'"

Stone also revealed that Snowden made a major contribution to the scripting of the film's climax--a nail-biter that depicts exactly how Snowden managed to get away with the stolen files he would eventually release to the world. In the movie, Snowden anxiously downloads files upon files of documents and hides the SD card inside a Rubik's cube.

After much suspense, he manages to smuggle the cube out through security, smiling his relief into the open air.

Only that's not how he really did it.

"We don't know," Stone admitted. "None of us know. He's the only one who knows and one day he may reveal. It was Ed's idea, his suggestion. We responded to it and ran with it. But it was a good idea. Thank you."

Snowden did not divulge how that scene really unfolded, but he confirmed that life as an international fugitive isn't all that terrible. "I can confirm that I'm not living in a box," he said. "I actually live a surprisingly free life."

"This was not the most likely outcome," he added. "I didn't actually expect to make it out of Hawaii. I thought it was incredibly risky... I never thought I would be saved. But I thought the stories might still be able to get out there."

He slammed the U.S. government, which cancelled his passport and made travelling impossible in the wake of the leak, for threatening trade sanctions against countries that offered him asylum.

"Particularly in the case of Ecuador, they literally got a direct threat, I believe from John Kerry, to revoke trade preferences," he said. "Trade preferences were basically the thing keeping their economy alive--literally, for broccoli farmers and rose farmers. These are impoverished, indigenous farmers, and they were like, 'We're going to make sure these people's families can't eat if you defend this guy's human rights.'"

"But this is not a criticism about the United States specifically, although that's heinous in terms of foreign policy," he continued. "This is truly about the nature of power."

Earlier in the day, Snowden and Andrew "Bunnie" Huang unveiled plans for a device that would prevent the outside surveillance of cell phones. "We're not doing productization, we're not doing sales, we're not setting up a company or anything like that," Snowden clarified. "Just saying anybody who wants to do this, here are our findings."

"I love my country. I love the things that we try to do," he declared. "I have serious policy disagreements with some agencies of government, particularly senior officials. The working level guys by and large are good people trying to do the best they can. But they're often ordered more or less to do bad things, for what they believe to be a good reason."

Speaking from exile in Russia, Snowden seemed content given the circumstances. "I don't have to worry about that anymore."

Bangkok Post
Police bust international hacking suspects
Friday, 22 July 2016

Bangkok - A Russian man and an Uzbek woman were busted by tourist police for their alleged involvement in a transnational hacking scam in which more than 50 people in several countries lost a total of one billion baht, police said.
Surachet Hakphan, commander of the Tourist Police Division, said police arrested Dmitry Ukrainskiy, a 44-year-old Russian, and Olga Komova, a 25-year-old Uzbekistan national, both of whom were wanted by US authorities for hacking into a personal financial database.

More than 50 people from various countries, including the US, Australia, Japan and Britain, were swindled out of more than one billion baht by the two suspects, he added. The police, however, declined to say where the suspects were arrested.

Pol Maj Gen Surachet said the US Federal Bureau of Investigation (FBI) had sought assistance from Thai police to track the two suspects belonging to a computer hacking network as authorities believed Mr Ukrainskiy and Ms Komova were hiding out in Thailand.

Since 2014, US authorities found that financial transactions believed to be carried out by the hacking network were made from several countries to Thailand. A police team was set up to search for the two suspects, Pol Maj Gen Surachet said.

Police found that Mr Ukrainskiy was running a yacht charter business in Pattaya and Ms Komova was working at a hotel in Koh Chang in Trat, he said.

Police said the suspects told investigators they used software that allowed them to gain access to a private computer system and stole the victims' financial information.

The Anti-Money Laundering Office had seized more than one billion baht and frozen more than 50 bank accounts from the network, Pol Maj Gen Surachet said. Meanwhile, a 50-year-old Turkish national has been arrested for robbery, police said.

Abdullah Alp Kaya, who was wanted on an arrest warrant issued by the Southern Bangkok Criminal Court on Wednesday, was caught yesterday at a coffee shop in the Terminal 21 shopping mall on Sukhumvit Road, Lumpini police said.

Investigators said people lodged complaints with police that their notebook computers, tablets, and smartphones were stolen when they were spending time at coffee shops at department stores in Bangkok.

Police said Mr Kaya admitted to police that he had stolen notebook computers and other gadgets from unsuspecting customers.

The Guardian (London)
Surge in cybercrime figures prompts police call for awareness campaign
Friday, 22 July 2016
Byline: Alan Travis

London - Police chiefs have called for a national campaign on online fraud and other cybercrime on the scale of last century's seatbelt and drink-driving campaigns in the wake of figures showing that one in 10 adults have been victims of such offences in the past year.
Chris Greany, City of London police's economic command head, said that with around 1m cases reported in the last year to Action Fraud alone, it was not possible for all cases to be investigated.

On Thursday the Office for National Statistics said there had been more than 5.8m incidents of cybercrime in the past year, far more than previously thought and enough to nearly double the headline crime rate in England and Wales.

The first official estimate of the true scale of online shopping scams, virus attacks, theft of bank details and other online offences was much higher than an initial ONS estimate in October last year, which put the annual figure at 3.8m, or 40% of all crimes.

Greany said fraud now cost an estimated £193bn each year, and with half of all crimes against people in the UK committed from abroad it was becoming more challenging for police to tackle.

"Law enforcement agencies are becoming increasingly successful at targeting the most serious offenders; however, the scale of the challenge is such that prevention, and helping businesses and individuals protect themselves, is the only long-term way of combating the escalating threat," he said. "That includes all industries taking proper steps to protect their customers from becoming victims of fraud."

Greany endorsed a call for a national fraud and cybercrime campaign on a par with the seatbelt and drink-drive campaigns of the 1980s and 90s to create a more internet-savvy society.

Deputy chief constable Peter Goodman, the National Police Chiefs Council lead on cybercrime, said digital crime was no longer a curiosity or a new specialism in policing. "The priorities for law enforcement are to make the UK a hostile place for cyber-criminals to operate, improve the response to victims and develop capabilities in local forces. Transforming our response to these crimes is a challenge but it is a priority for investment in policing," he said.

In March the Metropolitan police commissioner, Sir Bernard Hogan-Howe, faced criticism when he suggested that bank customers who were victims of online fraud should not be refunded by banks if they had failed to protect themselves from cybercrime.

The ONS says one in 10 adults have been victims of cybercrime in the past year. The chance of being a victim is the same regardless of social class or whether someone lives in a deprived or affluent, urban or rural area.

The 5.8m offences were made up of 3.8m fraud offences, including 2.5m incidents of bank and credit card fraud, and 2m computer misuse offences, including 1.4m virus attacks. The remaining 600,000 estimated offences related to unauthorised access to personal information, such as hacking of email, social media or other online accounts.

The latest overall figures, excluding online crime, in the 12 months to March 2015 show there were an estimated 6.3m offences - 6% fewer than in the previous year.

Police crime figures show that the murder rate rose by 34 to 571, the highest in five years. This is still far below the peak in 2002-03, when 1,047 homicides were recorded, but the recent rise is one of the more authoritative indicators that Britain is experiencing an increase in violence. The 96 deaths at Hillsborough in 1989 will be added to the official homicide figures and included in the next set of figures after the inquests finished in April.

Knife crime offences rose by 10% in the past year and gun crime increased by 4% over the same period.

Incidents of harassment, including new categories of offence such as malicious communications online, social media abuse and revenge porn, have risen 90%, from 82,000 to 156,000.

The police figures also show a 27% rise in offences against the person and a 21% increase in sexual offences. Those figures include a 22% increase in reported rapes from 29,300 to 35,798. By contrast, the crime survey shows no significant change in the proportion of adults who say they had been a victim of a sexual assault in the past year. The ONS said the 21% increase in sexual offences reflected both an improvement in police recording of the offences and a greater willingness of victims to come forward.

But the overall picture of all crime - excluding the 5.8m online offences - according to the crime survey of England and Wales, which is regarded as the best measure of crime trends, shows a 6% fall to 6.3m offences involving adult victims in the 12 months to March 2016.

The long- term trends in "traditional" crimes such as burglary, car thefts and criminal damage show that the fall in crime since its 1995 peak has slowed down since 2005. The crime survey found there had been no change in the overall level of violent crime compared with the previous year.

The online crime numbers give the first official snapshot of the scale of the threat from online attacks and scams. However, ONS statisticians said it would be "misleading to conclude that this means actual crime levels have doubled, since the survey previously did not cover these offences".

The first estimate is based on a 9,000-strong sample size from six months of interviews from the crime survey. Only when the ONS has 12 months of data in January will the online crime figures be incorporated into the headline crime rate.

Separate Home Office figures for police officer numbers show they fell by a further 3,126 last year to 124,000 - the lowest level since 2003.

Andy Burnham, the shadow home secretary, said: "At long last, we have the true picture of crime in England and Wales and it puts the former home secretary's record in a new light.

"Our new PM [Theresa May] was fond of saying that crime is falling but, as people can see, crime has moved online and until now the official statistics haven't shown that. Her complacent claims do not read well alongside these worrying increases in violent crime, sexual crime and homicide.

"The only conclusion that can be drawn is that it is the wrong time to be cutting the police. The PM promised real-terms protection but has failed to deliver it. Now that decision is entirely within her hands, she must honour the promise that she made and protect frontline policing," he said.

The policing minister, Brandon Lewis, said: "As crime falls, we know that it is also changing. Fraud and cyber-offences are not a new threat and the government has been working to get ahead of the game, committing to spend £1.9bn on cybersecurity and cybercrime over the next five years. We have also established the joint fraud taskforce, bringing together law enforcement and the banking sector, while Action Fraud, the National Fraud Intelligence Bureau and the National Crime Agency are working to improve our response.

"We welcome today's experimental ONS figures on fraud and cybercrime - offences which we have always known were happening but were previously unable to quantify. Having an accurate national picture will be crucial to inform future action."

New York Times
Pyongyang Radio Revives Coded Broadcasts for Spies
Friday, 22 July 2016
Byline: Choe Sang-Hun

Seoul - In an era of sophisticated spycraft, North Korea appears to be returning to the days of shortwave radio.

The North broadcast a series of seemingly random numbers on Pyongyang Radio twice recently, an eerie reminder of the days when the North encrypted messages to its spies in South Korea.

In the latest episode last Friday, an announcer read what she described as "a mathematics review assignment for investigative agent No. 27," engaged in a "distance learning" program.

"Turn to Page 459, No. 35; Page 913, No. 55; Page 135, No. 86," she said, continuing to cite numbers for 14 minutes.

Decades ago, it was not unusual for late-night radio listeners in the South to hear mysterious numbers arriving on static- filled signals from the North. The South Korean government in Seoul tried to block the signals and barred its citizens from listening.

Kim Dong-sik, a former intelligence officer for North Korea, said he used to listen for such broadcasts at midnight each night to check whether his spymasters had a message for him. Mr. Kim was caught by the South in 1995 after a gun battle with South Korean agents and police officers.

"When I arrived in the South, I had five different call signs assigned to me," said Mr. Kim, who now works as a senior analyst at the Institute for National Security Strategy, a think tank run by South Korea's National Intelligence Service. "Each night, I listened for my call signs."

The June 24 and July 15 broadcasts, confirmed by the South Korean government on Wednesday, were the first such coded messages in 16 years, leaving intelligence officials and analysts puzzled by the North's motives.

The broadcasts come amid concerns about the North, which has raised tension with the United States and its allies by conducting a series of missile tests and has issued bold claims of advances in its quest for a nuclear-tipped long-range missile.

North Korea has reacted strongly to a plan by the United States to deploy an advanced missile defense system in the South. This week, it fired three ballistic missiles, saying that they were used in simulated tests to detonate nuclear warheads over seaports and airfields in the South, where American reinforcements are supposed to arrive in the event of a war.

The tests defied a new round of sanctions that the United Nations Security Council imposed against the North after a nuclear test in January and a long-range rocket launch in February.

Jeong Joon-hee, a government spokesman for South Korea, has called the resumption of the broadcasts "seriously regrettable" but declined to comment on any motives. "The North should abandon its old ways," he said.

South Korea itself has resorted to old-school propaganda in recent years, resuming loudspeaker and radio broadcasts into the North and juicing them up with synthesized Korean music known as K-pop.

Some analysts said the North's use of a bygone encryption tool was rekindling old fear among South Koreans of an escalation in psychological warfare. North Korea stopped sending out such coded messages by shortwave radio after the Koreas held a summit meeting in 2000, agreeing to de-escalate the Cold War- era intrigue on the divided peninsula.

Since then, the North is believed to have adopted more sophisticated methods of communication. When the South's intelligence service announced the capture of a spy ring in 2011, it said that the officers contacted the North through steganography, a technique for encrypting a message into a text, image or video file delivered online.

Mr. Kim, the analyst and former spy, said the broadcasts should be taken seriously. He said the North appeared to be bolstering its espionage operations since 2009, when it created the General Bureau of Reconnaissance by merging various party and military agencies in charge of sending spies to the South.

Washington blacklisted the bureau after North Korean hackers were accused of wreaking havoc on the computer network of Sony's movie studio in 2014.

At a time when the counterintelligence authorities use sophisticated technology to monitor the digital communication of espionage suspects, "the old number broadcasts are still a dependable and preferable means of communication for spies," Mr. Kim said.

"We should assume that the North is using the radio broadcasts to communicate with its agents here or is at least using them to train spies," he added.

He recalled that when he was training in the 1980s, he spent countless hours listening to tape- recorded broadcasts and copying the numbers to master a so-called numbers station technique of encrypted communication.

Mr. Kim said he and his handlers in the North used an agreed-upon book -- "Whale Hunt," a popular novel in the South -- to decipher one another's codes. As in the broadcast on Friday, a typical five-digit combination started with a three-digit page number. The remaining two digits pointed at two Korean characters in the text of the page.

The two Koreas still accuse each other of spying. The North is holding at least four South Koreans, some of them sentenced to a labor camp for life, on charges of espionage.

In recent years, the South's intelligence service has arrested people it deemed spies as they entered the country disguised as refugees. Last week, prosecutors said they arrested two South Korean men on

charges of spying for the North. They released closed- circuit video of counterespionage officers overpowering a suspect at an internet cafe.

The men used encrypted emails to contact their handlers in the North, the prosecutors said.

Mr. Kim said that during his days as a spy, the radio was a main tool of communication.

"If there was a certain song broadcast by Pyongyang Radio at an agreed-upon hour, that meant that there was something wrong and I should immediately abort my mission," he said. "If not, it was all clear."

Gulf News
Beware ransomware attacks on your PC
Friday, 22 July 2016
Byline: Faisal Masudi

Dubai - Ransomware, a relatively new kind of cyber attack where criminals demand money for decrypting files they have taken control over, is increasingly targeting ordinary consumers -- including those in the UAE -- a new study said on Wednesday.
Security firm Symantec said in its latest research the average ransom demanded by attackers jumped to $679 (Dh2,491), up from $294 (Dh1,078) at the end of 2015.

The "Internet Security Threat Report (ISTR) Special Report: Ransomware and Businesses 2016" revealed consumers make up 57 per cent of ransomware victims.

The majority of ransomware variants are designed to attack Windows computers and ordinary home users continue to be one of the biggest victim groups, it added. Meanwhile, employees at organisations make up 43 per cent of ransomware victims.

According to Symantec's 2016 ISTR, the UAE experienced the fourth highest rate in ransomware attacks in the Middle East and Africa region, added Hussam Sidani, regional manager for Gulf, Symantec.

Furthermore, ransomware attacks grew by 44 per cent year-on-year in the UAE in 2015. "In 2015, we saw an average of 28 attacks per day and 10,279 total attacks on UAE-based organisations," Sidani said.

"Additionally, given the strong uptake of smartphones and tablets, we're seeing more mobile devices coming under attack, with attackers encrypting files, and anything else an owner will pay to recover.

"The UAE has one of the highest penetration of smartphones in the world and users enjoy great connectivity here. This can make them a very lucrative target for ransomware."

Sidani explained that one of the most common methods to spread ransomware, and malware in general, is through malicious spam email. These spam emails pose as an important email from a well-known organisation, such as a shipping or utility company. However, as soon as the user opens the malicious attachment or link, malware will be installed on their device or computer. Following this, the user's important files will be encrypted and they will receive a message demanding a ransom to release the files.

Victims can be asked to send ransom money via a payment link or by handing over their credit card information. However, Symantec's recommendation is not to pay the ransom.

"While we recognise that some organisations may feel that paying the ransom is their only option, there is no guarantee that this will recover their data. Attackers may not send a decryption key, could poorly implement the decryption process and damage files, and may deliver a larger ransom demand after receiving the initial payment."

Don't click links in unsolicited email or social media messages, particularly from unknown sources. Use strong and unique passwords for your accounts and devices, and update them on a regular basis.

When installing a network-connected device, or downloading a new app, review the permissions to see what data you're giving up. Disable remote access when not needed. Antivirus-only security is no longer enough to combat security threats like ransomware. Protect your data with a multi-platform solution and back up your computer and devices on a regular basis.

New York Times
Snowden to Help Develop a Safer Phone for Journalists
Friday, 22 July 2016
Byline: John Markoff

Cambridge, Mass. - The former National Security Agency contractor Edward J. Snowden said Thursday that he planned to help develop a modified version of Apple's iPhone for journalists who are concerned that they may be the target of government surveillance.
The announcement was made during a one-day conference on "Forbidden Research" held at the Massachusetts Institute of Technology's Media Lab.

Mr. Snowden, who spoke via a video connection from Russia, where he is living in exile, said he was working with Andrew Huang, a computer hacker known as Bunnie who studied electrical engineering at M.I.T., to see if it would be possible to modify a smartphone to alert journalists working in dangerous environments to electronic surveillance.

Mr. Snowden, who is a board member of a nonprofit group called the Freedom of the Press Foundation, said he was concerned that cellphones and smartphones serve as tracking devices that automatically

create electronic dossiers that give third parties, including governments, detailed information on location.

As an example of the dangers of location data, he cited the mortar attack in 2012 by the Syrian government that killed Marie Colvin, an American journalist who was reporting in Homs, Syria, for The Sunday Times of London.

"The radio frequency emissions of her communications that she used to file those news reports were intercepted by the Syrian Army," he said.

He said it was increasingly difficult for users to trust their smartphones. They may be tampered with by malware programs, causing them to transmit location information even when the user may believe that the device has been placed into a safe "airplane mode."

Mr. Huang said the project was still experimental, but he hoped it would provide journalists with modified phones that would come in a special case with a separate display that would provide an alert when the phone was active and transmitting data at improper times.

The conference focused on issues raised by computer hacking, as well as controversial scientific research in areas such as genetic engineering and geoengineering.

Also at the conference, Reid Hoffman, one of the founders of LinkedIn, which recently agreed to be acquired by Microsoft for $26 billion, announced that he planned to offer a $250,000 "Disobedience Prize" aimed at promoting positive social change and opposing injustice.

"It will go to a person or group engaged in what we believe is excellent disobedience for the benefit of society. The disobedience that we would like to call out is the kind that seeks to change society in a positive way, and is consistent with a set of key principles," wrote Joichi Ito, director of the M.I.T. Media Lab, in a web posting about the prize. The timing of the award has not yet been determined.

In separate panels, biologists and climate scientists explored the risks and rewards of scientific research that might have unexpected consequences.

Kevin Esvelt, a biologist who is director of the Sculpting Evolution research group at the M.I.T. Media Lab, spoke about new, easily accessible genetic engineering technologies that might be used to preserve species that are at risk of extinction, and alternatively to eradicate pests that threaten human populations by spreading disease.

He described a discussion scientists had on Wednesday with residents of Martha's Vineyard about the use of advanced genetic engineering techniques to introduce a type of mouse that had been modified to be unable to carry Lyme disease. The idea would be to break the transmission of the disease to ticks and then to humans.

He said that before beginning the experiment, the scientists engaged the community to discuss potential risks.

Scientists on several panels acknowledged that it was impossible to be certain about unforeseen effects from new engineering techniques.

"What we're worried about is something that we do that could be very attractive in the short term but have some triggering mechanism or some slow events that occur far in the future," said George Church, a Harvard geneticist who is exploring genetic engineering techniques to revive extinct species.

Gulf News
Lack of funds and training hamper cybersecurity
Friday, 22 July 2016
Byline: Staff Report

Dubai - Poor funding and lack of skilled staff remain serious challenges for global business IT security, according to a new survey by Accenture and HfS Research.
And insider data theft and malware attacks are the most significant threats, with 69 per cent of survey respondents saying they had suffered attempted or successful theft or corruption of data by insiders in the previous 12 months.

The survey, The State of Cybersecurity and Digital Trust 2016, polled 200 security executives and IT professionals in different countries and in different sectors.

Findings indicate that there are significant gaps between talent supply and demand, a disconnect between security teams and management expectations, and considerable disparity between budget needs and actual budget realities.

"Our research paints a sobering picture. Security leaders believe threats are not going away, in fact they expect them to increase and hinder their ability to safeguard critical data and establish digital trust," said Kelly Bissell, senior managing director, Accenture Security. "At the same time, while organisations want to invest in advanced cyber technologies, they simply don't have enough budget to recruit or train skilled people to use that technology effectively."

"While the gaps we identified can be overcome, they do collectively underscore the need for an inherently different approach, one that includes more robust risk management measures and the development of digital trust," said Fred McClimans, research vice president, Digital Trust and Cybersecurity, HfS Research.

London Times
One in ten become victims of cybercrime
Thursday, 21 July 2016
Byline: Richard Ford

London - One in ten adults have been victims of fraud or computer misuse offences, according to official figures published today.
An estimated 5.8 million fraud and cyberoffences are committed annually, pushing the overall crime figures in England and Wales to more than 12 million.

The first official estimate of the scale of online shopping scams, virus attacks, ticket frauds, computer hacking and theft of bank details along with credit and bank card fraud shows that fraud is the most common crime experienced by the public.

The chance of being a victim of victim of fraud is the same regardless of class, region and whether a person lives in a rural or urban area, according to the Crime Survey of England and Wales.

Official crime figures from the Office for National Statistics (ONS) showed that excluding fraud and cybercrime, there were 6.3 million crimes in the 12 months to March 2016, a fall of 6 per cent.

Separate police-recorded crime figures for murder rose by 34 to 571 homicides, the highest level for five years

Police figures also showed a 27 per cent rise in offences against the person and a 21 per cent increase in sexual offences. Statisticians said the rise in both types of offences was due to better recording practices by the police and that the increase in sex crimes was also due to a willingness of more victims to report offences.

Incidents of revenge porn and harassment, including online abuse, accounted for almost half the rise in personal violence.

The confirmation of the high volume of online crime provides the first official snapshot of the scale of threat from online attacks and scams.

Statisticians said "it would be misleading to conclude that this means actual crime levels have doubled, since the survey previously did not cover these offences".

The first estimate is based on a 9,000 sample size from six months of interviews from the survey.

Only when the ONS has 12 months of data in January will the online crime figures be incorporated into the headline crime rate for England and Wales.

The 3.8 million frauds included 2.5 million bank and credit account cases plus one million sales, tickets and computer software service frauds.

There were a further 0.1 million incidences involving lottery scams and frauds linked to dating sites.

Of the two million computer misuse incidents, 1.4 million involved computers being infected with viruses and 0.6m incidents of hacking of e-mail, social media or other online accounts.

The Intercept
Edward Snowden's New Research Aims to Keep Smartphones From Betraying Their Owners
Thursday, 21 July 2016
Byline: Micah Lee

Washington - In early 2012, Marie Colvin, an acclaimed international journalist from New York, entered the besieged city of Homs, Syria, while reporting for London's Sunday Times. She wrote of a difficult journey involving "a smugglers' route, which I promised not to reveal, climbing over walls in the dark and slipping into muddy trenches." Despite the covert approach, Syrian forces still managed to get to Colvin; under orders to "kill any journalist that set foot on Syrian soil," they bombed the makeshift media center she was working in, killing her and one other journalist and injuring two others.
Syrian forces may have found Colvin by tracing her phone, according to a lawsuit filed by Colvin's family this month. Syrian military intelligence used "signal interception devices to monitor satellite dish and cellphone communications and trace journalists' locations," the suit says.

In dangerous environments like war-torn Syria, smartphones become indispensable tools for journalists, human rights workers, and activists. But at the same time, they become especially potent tracking devices that can put users in mortal danger by leaking their location.

National Security Agency whistleblower Edward Snowden has been working with prominent hardware hacker Andrew "Bunnie" Huang to solve this problem. The pair are developing a way for potentially imperiled smartphone users to monitor whether their devices are making any potentially compromising radio transmissions. They argue that a smartphone's user interface can't be relied on to tell you the truth about that state of its radios. Their initial prototyping work uses an iPhone 6.

"We have to ensure that journalists can investigate and find the truth, even in areas where governments prefer they don't," Snowden told me in a video interview. "It's basically to make the phone work for you, how you want it, when you want it, but only when."

Huang made a name for himself by using a technique known as reverse engineering to hack into Microsoft's Xbox and other hardware devices locked down using various forms of encryption, and Snowden said he's been an invaluable research partner.

"When I worked at the NSA, I worked with some incredibly talented people," Snowden said, "but I've never worked with anybody who had such an incredible outpouring of expertise than I have with Bunnie."

Snowden and Huang presented their findings in a talk at MIT Media Lab's Forbidden Research event today and published a detailed paper.

Location Privacy and Smartphones

Smartphones come with a variety of different types of radio transmitters and receivers: cellular modems (for phone calls, SMS messages, and mobile data), wifi, bluetooth, and others. But using any of these radios could leak your physical location to an adversary who is watching the airwaves.

Journalists and activists use their phones to communicate with sources and colleagues, post updates and livestream to social media, and accomplish countless other networked tasks. If they need to keep their location secret, for example in a war zone, they need to turn off all of the radios within their phones. Even so, phones can still be vital tools even when offline; internet access is not needed to take photographs, record video or audio, take notes, use certain maps, or manage schedules.

Snowden and Huang have been researching if it's possible to use a smartphone in such an offline manner without leaking its location, starting with the assumption that "a phone can and will be compromised." After all, journalists and activists are often under-resourced and face off against well-funded intelligence services. They also, necessarily, use their phones to talk to, and open documents from, a wide variety of sources, leaving them especially vulnerable to targeted phishing, or "spearphishing," attacks, where an attacker baits a victim into opening an enticing document that actually contains an exploit.

The research is necessary in part because the most common way to try to silence a phone's radio -- turning on airplane mode -- can't be relied on to squelch your phone's radio traffic. "Malware packages, peddled by hackers at a price accessible by private individuals, can activate radios without any indication from the user interface," Snowden and Huang explain in their blog post. "Trusting a phone that has been hacked to go into airplane mode is like trusting a drunk person to judge if they are sober enough to drive."

Introspection Engine

Since a smartphone can essentially be made to lie about that state of its radios, the goal of Snowden and Huang's research, according to their post, is to "provide field-ready tools that enable a reporter to observe and investigate the status of the phone's radios directly and independently of the phone's native hardware." In other words, they want to build an entirely separate tiny computer that users can attach to a smartphone to alert them if it's being dishonest about its radio emissions.

Snowden and Haung are calling this device an "introspection engine" because it will inspect the inner-workings of the phone. The device will be contained inside a battery case, looking similar to a smartphone with an extra bulky battery, except with its own screen to update the user on the status of the radios. Plans are for the device to be able to sound an audible alarm and possibly also to come equipped with a "kill switch" that can shut off power to the phone if any radio signals are detected. "The core principle is simple," they wrote in the blog post. "If the reporter expects radios to be off, alert the user when they are turned on."

The introspection engine also must fit a number of design goals, including: It should be entirely open source, with open hardware, to make it easy for experts to inspect; it should operate in a separate "security domain" than the phone. Basically, the introspection engine should work even if the phone is hacked and actively lying to you; it should have a simple and intuitive user interface and require no special training to use; it should be usable on a daily basis with minimal impact on workflow.

Introspection engines don't exist yet, and the research Snowden and Huang presented today is only the beginning. In order to begin work on a prototype, the pair needed to pick a specific model of smartphone to target. They chose the 4.7-inch iPhone 6, based on their understanding of "the current preferences and tastes of reporters." However, introspection engines could be designed for any model phone.

Jacking Into the iPhone

Huang, an American who currently lives in Singapore, traveled to the metropolis of Shenzhen, China, to explore the electronics markets of Hua Qiang, which he described as "ground zero for the trade and practice of iPhone repair." While there, he bought spare parts and repair manuals that contained detailed blueprints of the target device.

Using information gleaned from these manuals, Snowden and Huang discovered that the iPhone's logic board has several test points designed by the manufacturer that can be exploited to learn the status of various on-board radios. These test points, which are built-in to many consumer devices, are crucial to improving customer experience. When a customer returns a defective device, engineers rely on them to determine the cause of the defect.

Snowden and Huang discovered 12 test points that could be used to monitor the status of the cellular radios, the GPS radio, and the wifi and bluetooth radios. While they didn't find a test point to monitor the Near Field Communication chip, the part that makes Apple Pay possible, they discovered that they could disconnect its antenna, vastly reducing its range.

They don't think that modifying an iPhone 6 to install an introspection device could be done by just anyone, but "any technician with modest soldering skills can be trained to perform these operations reliably in about 1-2 days of practice on scrap motherboards."

Supply Chain

The next step is to develop a working prototype, which Snowden and Bunnie hope to complete over the next year. Their blog post says that the project is currently operating on a "shoestring budget" and "donated time."

If it proves successful, they may seek funding through the Freedom of the Press Foundation to develop and maintain a supply chain. The nonprofit, of which both Snowden and I are board members, could then distribute iPhones that have been modified to include introspection devices to journalists who work in dangerous environments to use in the field.

Lebanon Daily Star
Touch witness completes testimony at STL
Friday, 22 July 2016
Byline: Susannah Walden

Beirut - Protected witness PRH 705 completed his testimony Thursday as the designated representative of the MTC touch cellular network at The Special Tribunal for Lebanon. Touch is one of Lebanon's two GSM networks, the second of which, Alfa has been represented by PRH 707 - another protected witness. Both networks turned over reams of extensive records concerning billingrecords, call logs and coverage maps at the request of investigators.
Prosecutors have built much of their case against the five defendants accused of conspiring to assassinate former Prime Minister Rafik Hariri on this telecommunications data. Prosecutors argue that the data can be used to retrace the movements of the defendants.

Defense attorney Thomas Hannis, representing the interests of Salim Ayyash, completed his cross-examination of the witness by clarifying comments about some of the documents handed over by the network.

The records were a source of debate at the trial, as defense attorneys contested submitting documents into evidence if the witness could not personally attest to their origin.

Hannis had previously voiced his doubt at a May appearance of PRH 705. "This witness has been placed in a very difficult position. He's speaking for the community," he said. "We have a concern that we won't be able to have fair trial for our clients if we're not able to have a meaningful cross-examination of the underlying sources of evidence."

The final appearance of PRH 705 focused on clarifications. "I apologize your honor, this may seem detailed and fiddly, but it won't take long and may be important for our submission later on," Hannis said.

After the lunch recess, Prosecutor Fabia Wong took over to ask the witness several questions on records submitted concerning cellphone handsets that prosecutors allege were used by the deceased Hezbollah commander Mustafa Badreddine. Legal proceedings against Badreddine were halted after an Appeals Chamber found there was sufficient evidence that he was killed in Syria in May.

The investigation into controversial telecommunications data will continue with further testimony from Alfa representative PRH 707, however Thursday's session ended PRH 705 contribution for the time being.

Judge David Re, the Trial Chamber president, highlighted the weight the telecommunications evidence has carried in the proceedings as PRH 705's testimony concluded.

"[There was a] considerable amount of interest in what you had to say based on the number of questions from the counsel and the bench itself. You're free to go ... As they say, don't call us, we'll call you," he said.

Chronicle-Herald (Halifax)
Legal experts mull risks to privacy
Saturday, 23 July 2016

Halifax - Cyber-crime and privacy issues top the agenda at the International Society for the Reform of Criminal Law annual conference in Halifax this week.
It is the first time the conference, slated to run Sunday through Thursday has been held east of Montreal.

Judges, lawyers, legislators and law enforcement officials from around the globe will weigh in on the difficult balance between the rights of the individual and society's collective security, said Hon. Justice Michael MacDonald, Supreme Court of Nova Scotia, who is co-chairing this year's conference along with Supreme Court Justice Thomas Cromwell.

"It's a huge challenge in the face of technology that's changing at warp speed," MacDonald said.

"The Internet is changing our lives daily and it's a challenge at the best of times to find that right balance between protecting your and my privacy with the need to protect society," he said.

While judges are loath to give police the right to hack anyone's account without good reason, with the Internet changing life in almost every way, the justice system has to act appropriately to make sure the use of the Internet as an instrument of crime is minimized, MacDonald said.

One of the biggest challenges is that of the principle of open court, he said.

"In Nova Scotia and Canada and all leading democracies we value our open courts principle, which means everything that happens must be open to the public and the public must be able to scrutinize to make sure justice is administered properly," MacDonald said.

The problem is that information that can be gathered through open court principle can be manipulated for malicious purposes, he said, recalling his law practice in the 1970s, when a messy divorce case might yield personal details about children or other vulnerable people.

Those same details, online, could be Googled and exploited, MacDonald said.

"We have a need to balance the requirement to preserve the open court principle but at the same time, to protect vulnerable people who could be abused by this same open court system," he said.

Caught in middle of the tug-of-war between individual privacy and collective security, law enforcement and the justice system have to weigh all the angles.

On the downside, there's cyber-stalking, cyber-bullying and internet luring.

On the upside, the Internet provides new investigative tools for solving these crimes and others, MacDonald said.

Parliament has enacted statutory measures to protect the identities of witnesses in criminal matters, with limited provision under the criminal code for in-camera testimony.

"Again, it's about fitting the proper balance between protecting your individual privacy when using the internet and protecting society by arming law enforcement officials with sufficient tools to trace and to solve crimes that are happening on the Internet," MacDonald said.

Serious criminal activities like hacking and extortion are threatening institutions that would have previously been impervious to digital attack, said attorney Don Sorochan, secretary-treasurer to the international society.

The conference has made a difference for countries with participants attending it over the years.

"They've taken what they've learned (home) and we've seen changes flowing from that a few years later," Sorochan said.

Canadian Press
Banks eye biometrics to boost security
Saturday, 23 July 2016
Byline: Alexandra Posadzki

Toronto - In the not-too-distant future, your bank will be able to prevent fraud by learning how you type, your car will unlock when it senses the electrical activity of your heart and the security system at your office will recognize your facial features.
That's according to experts in the field of biometrics, which identifies a person by measuring unique characteristics such as their fingerprints, their retinas or their voice.

But these types of distinctive identification authentication processes offer more than the promise of a higher degree of security than traditional passwords.

Biometrics will also free consumers from the need to memorize a myriad of characters - a convenience that will appeal to anyone who needs to access a secure computer or network regularly. "People are having to jump through more and more hoops to create a secure authentication," says Karl Martin, founder of Nymi, a Toronto-based startup that created a wristband that can identify its wearer based on their electrocardiogram, or the electrical activity of their heart.

"How many times a day do you have to prove who you are, whether it be through a password or a biometric or other means?" Banks - and the financial services industry, more broadly - have been one of the quickest adopters of biometrics technology, given their strong need for security and identity verification, says Bianca Lopes, director of strategy at Bio- Connect.

"They're inherently wired and regulated to protect the customer with things like know-your-client and anti-money laundering rules," says Lopes, whose company helps businesses integrate biometrics technologies across various channels.

Royal Bank is currently testing technologies such as iris scanning, face recognition, speech recognition and fingerprint scans - and is expecting to roll out the features to customers in 2017.

Martin says Nymi has completed successful pilot projects alongside RBC and TD Bank to test how its wristband can be used to verify purchases, while MasterCard recently launched a service that allows users to verify their identities with their smartphones by taking a selfie or using a fingerprint scanner.

Notably, it's the popularity of the fingerprint scanner on Apple iPhones that's made consumers more comfortable and familiar with biometrics, says Dennis Gamiello, vice-president of identity solutions at MasterCard. "Fortunately, Apple and some of the other digital players that have introduced (biometric) capabilities are in some ways helping train the consumers for us."

Biometrics can also identify users based on how they behave - for instance, their typing patterns or the way that they swipe across the screen on a mobile device.

"The way that you actually interact with the phone, the way that you swipe the phone ... it's fairly unique to you," explains Eddy Ortiz, RBC's vice-president of innovation and solution acceleration. In the future, behavioural biometrics could even be used to detect if a fraudster has somehow gained access to your bank account, Lopes adds.

While identity verification is important, the capabilities of biometrics go beyond that function, notes Martin. The technology can also be used to create personalized environments - by setting the thermostat to your preferred temperature, for example - at your home, the office or a commercial space.

"We're looking at how can identity be used to create completely personalized experiences," says Martin, pointing to cars as an example.

"You may have a shared vehicle but you have preferences in terms of the seat height and position and the steering wheel and entertainment and all of those things." Experts concede that while biometrics can beef up security, improve convenience and create personalized environments, for some users the technologies may evoke scenes from the popular science fiction film Minority Report - a Tom Cruise

mystery-thriller that features a future of nearly boundless technological advancements designed to protect its citizenry.

"There will be consumers who get creeped out," says Krista Jones, head of work and learning at the MaRS Discovery District.

Ultimately, though, the technology gives consumers a greater guarantee that their private information will be kept safe, she adds. "We have an opportunity to craft this in such a way that the privacy of the consumer is at the heart of this."

Canadian Press
StatsCan wants its freedom from central federal IT department: documents
Saturday, 23 July 2016

Ottawa - The country's chief statistician believes Statistics Canada must have complete control of its own digital systems rather than having to turn to the federal government's central IT department. Workers at the statistics agency were told earlier this year that it was antithetical having someone else look after IT services when the Liberals vowed during the election to make Statistics Canada more independent from the federal government.

The details are contained in documents obtained by The Canadian Press under the Access to Information Act that included speaking notes for chief statistician Wayne Smith.

"Dependence on another party for informatics services impedes our ability to deliver our programs, to innovate and transform, (and) to better address new and emerging data needs," Smith's speaking notes read.

"As such, this dependence is incoherent with the notion of independence, not to mention protection of the confidentiality of respondent data."

Shared Services Canada and the statistics agency have had a rocky relationship amid outages and sluggish systems critical to Statistics Canada's mandate.

Smith also wrote in response to a staff question that "programs have suffered and continue to suffer delays" since Statistics Canada handed over oversight of its systems to Shared Services Canada, creating "challenges in terms of reliability, timeliness, effectiveness and affordability of IT architecture."

A spokeswoman for Shared Services Canada said in an email that the IT department is working with Statistics Canada to "ensure its operational needs are met."

Stephanie Richardson said Shared Services Canada has proposed moving Statistics Canada systems to a new "world-class" data centre "in order to reduce incidents."

Washington Post
Clinton campaign -- and some cyber experts -- say Russia is behind email release
Monday, 25 July 2016
Byline: Tom Hamburger, Ellen Nakashima

Washington - A top official with Hillary Clinton's campaign on Sunday accused the Russian government of orchestrating the release of damaging Democratic Party records to help the campaign of Republican Donald Trump - and some cybersecurity experts agree.
The extraordinary charge came as some national security officials have been growing increasingly concerned about possible efforts by Russia to meddle in the election, according to several individuals familiar with the situation.

Late last week, hours before the records were released by the website WikiLeaks, the White House convened a high-level security meeting to discuss reports that Russia had hacked into systems at the Democratic National Committee.

Although other experts remain skeptical of a Russian role, the hacking incident has caused alarm within the Clinton campaign and also in the national security arena. Officials from various intelligence and defense agencies, including the National Security Council, the Department of Defense, the FBI and the Department of Homeland Security, attended the White House meeting Thursday, on the eve of the email release.

If the accusation is true, it would be the first time the Russians have actively tried to influence an election in this manner, analysts said.

Clinton's campaign chief, Robby Mook, told ABC News on Sunday that "experts are telling us that Russian state actors broke in to the DNC, took all these emails and now are leaking them out through these Web sites. ... It's troubling that some experts are now telling us that this was done by the Russians for the purpose of helping Donald Trump."

Trump campaign officials rejected the suggestion as absurd.

The most sensational revelation so far in the emails is that officials at the supposedly impartial DNC were in fact helping Clinton during the primary. One email written May 5 to Luis Miranda, the national communications director for the DNC, from another party official suggests that the party could help Clinton by raising questions about Sanders's faith. Other emails generally disparaged Sanders and indicated a preference for Clinton.

The emails have infuriated Sanders supporters, who have repeatedly accused the DNC of improperly helping the Clinton campaign during the primary. The episode prompted the resignation Sunday of DNC Chairwoman Debbie Wasserman Schultz.

"They said they were neutral, which we knew not to be true," said Sanders campaign manager Jeff Weaver. "Now we have evidence in black and white that they were trying to put out negative stories about Bernie Sanders. People are very angry about these leaks, and rightfully so. There's no doubt about that."

Beyond Mook, DNC and Clinton campaign officials have not responded to requests for comment Friday as reporters and unnerved campaign staff tried to assess the damage caused by the release, which comes just as the party holds a nominating convention in Philadelphia designed to project unity after a bitter primary season.

The emails were released Friday on Twitter by WikiLeaks. The document dump follows a report last month by The Washington Post that Russian government hackers had penetrated the computer network of the DNC, gaining access to an entire database of opposition research, among other material.

Other emails offered details of perks provided to party donors attending the convention and other events involving Democratic officials.

On Sunday, Mook and others noted that Trump has taken positions in the campaign that seem to align with those held by Russian President Vladimir Putin. He cited Trump's recent statement on NATO - that he might not provide assistance to member states that hadn't contributed their financial share - as a sign that the Republican nominee is taking positions favorable to Putin.

"I think when you put all this together, it's a disturbing picture and voters need to reflect on that," Mook told CNN in an interview Sunday.

Trump's campaign chairman, Paul Manafort, flatly denied the insinuation, calling Mook's comments "pure obfuscation" on ABC's "This Week."

"What they don't want to talk about is what's in those emails," Manafort said.

Last month, the forensic firm CrowdStrike said two competing Russian intelligence hacker groups penetrated the DNC's computers. In the past 24 hours, cybersecurity experts have said that the email cache released by WikiLeaks on Friday appears to have been given to the anti-secrecy group by Russian intelligence.

Thomas Rid, a professor at King's College London, said in an interview that in a private chat on Twitter on Saturday, he communicated with the entity that claimed to have released the email cache to WikiLeaks.

The party, which calls itself Guccifer2, last month claimed responsibility for the DNC hack. Several independent analysts have concluded that Guccifer2, who claimed to be Romanian, is likely linked to Russia.

"We've been looking at this very closely from both the technical and non-technical spheres," said Richard Barger, chief information officer for ThreatConnect, a cyber-intelligence software firm. "Based on our analysis, we strongly feel Guccifer2 is linked to a Russian information operations campaign and is not the independent Romanian hacker that he claims to be."

The apparent link to Russian intelligence raises troubling implications for U.S. foreign relations and national security. Russia has not to date tried to interfere in U.S. elections, analysts say. But if this is a deliberate effort by the Kremlin to meddle, it is worrisome, they say.

Michael G. Vickers, who served as undersecretary of defense for intelligence from 2011 to 2015, said an effort by the Russians to release intelligence in advance of a U.S. election is likely unprecedented.

"What is really new here is the attempt to influence the politics of the United States. That is the problem," he said.

Vickers said that the Russians have attempted to influence elections in states closer to their border but that seeking to do so in the United States would represent a historic and significant change, even in an era when Russian intelligence gathering has become more aggressive.

Because he is no longer in government service, Vickers said he had no direct knowledge of the forensic evidence in the DNC email case. However, he said that "people who have looked at it have said it looks like groups that have been tied to Russian intelligence."

Fiona Hill, a former Russia expert on the National Intelligence Council, said putting the emails out on WikiLeaks for the world to see is consistent with her view of the modus operandi of Putin and Russian intelligence.

"They're doing what they do best," said Hill, now a Brookings Institution senior fellow. "They would not be doing their jobs as intelligence officers if they were not trying to outsmart their main opponent and to have influence on their politics."

But, Rid pointed out, "what we don't know is whether this is a top-down order or not."

Russian Embassy officials did not respond to a request for comment Sunday. In the past, Russian officials denied any involvement with the hack.

"I completely rule out a possibility that the [Russian] government or the government bodies have been involved in this," Dmitry Peskov, the Kremlin's spokesman, told the Reuters news agency in Moscow.

One U.S. official, who like others interviewed for this report spoke on the condition of anonymity, said the email dump "would be the worst possible way to influence an election. It just seems a little clumsy. It just seems a very odd way of going about it."

WikiLeaks is nonetheless an ideal venue for gaining exposure, other analysts say. The site, cofounded in 2006 by Julian Assange, promotes itself as an anti-secrecy organization and promises leakers' anonymity.

"If you're the Russians and you want to leak information for maximal effect, WikiLeaks is a great platform for that," said one analyst, who spoke on thecondition of anonymity because his work involves studying Russian intelligence and he did not want to draw attention to himself.

Russia has intervened in other countries' elections. For instance, in Ukraine in 2004, a Russian hacker group calling itself Cyber Berkut claimed it hacked and disabled the electronic vote-counting system of the Ukraine central election commission three days before the presidential election. The election followed the toppling of a pro-Moscow leader, a move that set off Russia's invasion and annexation of Crimea.

Analysts have attributed the hack to the GRU, one of the same Russian military intelligence services said to have hacked the DNC. They said that the agency created Cyber Berkut, which portrayed itself as an independent hacktivist group but in reality was used to further Moscow's political interests in Ukraine.

Likewise, French authorities say a cyberattack last year on the French television network TV5Monde was carried out by Russian hackers. A group posing as being linked to the Islamic State and calling itself "Cyber Caliphate" posted jihadist propaganda on the station's website - an apparent effort to deflect suspicion away from Russia - and plunged the network's TV channels into darkness. Again, it was the GRU that was said to be behind the attack, the French authorities said. Some analysts said they believed the attack was Russian retaliation against France for backing out of a deal to sell helicopter carriers to Russia because of Moscow's aggression in Ukraine.

Within 24 hours of the news breaking of the Russian hack of the DNC, files that purported to be from the servers began to appear online. Guccifer2 claimed credit for the hack and portrayed itself as independent of Russia. But a number of independent experts pointed to evidence that Guccifer2 appeared to be linked to Russia and said they believed Guccifer2 was trying to deflect blame from Russia.

The Post has previously reported that Trump has had a long-standing interest in Russia. In addition, The Post found that Manafort has multi- million dollar financial ties to oligarchs in the former Soviet Union.

Atlantico (site web)
Comment Edward Snowden conçoit un prototype de coque anti- espionnage pour iPhone
Monday, 25 July 2016
Byline: Journaliste maison

Non identifié - Le lanceur d'alerte américain Edward Snowden a conçu une coque qui devrait permettre aux journalistes, activistes et défenseurs des droits de l'homme de se protéger de l'espionnage des gouvernements.
Edward Snowden , l'informaticien qui a dénoncé en 2013 les programmes de surveillance de masse menés par les gouvernements américains et britanniques, continue son combat contre l'espionnage.

Quelques jours avant de faire éclater le scandale, Snowden avait demandé à ses avocats qu'il avait rencontrés à Hong Kong de placer leurs téléphones au réfrigérateur afin d'empêcher toute tentative de mise sur écoute . En effet, l'habitacle métallique servait de brouilleur d'ondes.

Snowden a décidé de rendre la vie plus facile aux personnes qui comme lui, ont dû se dépêtrer de l'emprise invisible mais bien réelle de la surveillance gouvernementale : à l'occasion d'une conférence menée le 21 juillet 2016 au MIT Media Lab , célèbre sommet dédié à la l'éthique technologique se déroulant au département universitaire de Cambridge, dans le Massachusetts, il est intervenu en visioconférence depuis la Russie où il est exilé depuis trois ans, rapporte le site Wired.

Mode avion inefficace contre les hackeurs

Il a ainsi fait part de son intention de dévoiler un concept de coque pour iPhone capable d'empêcher un gouvernement de géolocaliser son porteur, entre autres, relate Le Monde informatique. "Les smartphones, bien qu'incroyablement utiles, sont également de parfaits terminaux d'espionnage. Les gouvernements peuvent surveiller la localisation d'un utilisateur au travers des signaux radio du téléphone et peuvent mettre les journalistes, activistes et défenseurs des droits de l'homme en danger" , s'est exprimé Snowden dans un article .

Pour ce projet, l'informaticien s'est associé au hackeur Andrew "Bunnie" Huang , célèbre pour ses expérimentations sur Xbox, la console de jeux de Microsoft. Dans un rapport, les deux hommes précisent que le mode avion est loin de pouvoir vous parer contre la surveillance : "croire au mode avion d'un téléphone hacké équivaut à laisser une personne ivre juger de sa capacité à conduire", indiquent-ils.

En effet, le mode avion ou éteindre son téléphone ne sont pas des moyens infaillibles. Le mode avion pourrait ne pas vraiment couper les radios et il serait également possible de "faussement" éteindre un mobile en répliquant un écran d'extinction, détaille Les Numériques.

Véritable utilité

Selon Numerama, cette coque de smartphone comporterait un oscilloscope miniature permettant de surveiller en permanence l'activité électrique du circuit utilisé par le modem sans fil, et ainsi détecter toute utilisation de ce modem alors que le mobile est censé être en mode avion et donc ne plus émettre ni recevoir aucune donnée. Une alerte est alors donnée à l'utilisateur du mobile, avant que celui-ci ne s'éteigne afin de se protéger de l'intrusion, précise Mashable.

Un premier exemplaire devrait être disponible d'ici un an et mis en production si Snowden et Huang obtiennent les financements suffisants. Les plans et codes sources seront rendus publics, et de nouvelles améliorations devraient être dévoilées afin de garantir un peu plus la confidentialité des données mobiles.

Cet outil devrait trouver son public, quand on sait que la menace d'espionnage est réelle pour certains. Par exemple, en 2012, la reporter américaine Marie Colvin qui couvrait le conflit syrien avait été tuée dans un bombardement à Homs. Une action en justice avait révélé par la suite que le gouvernement syrien l'avait assassinée en traçant ses communications téléphoniques pour la localiser .

New York Times
In Hacking, Russia Is Accused of Playing in American Politics
Monday, 25 July 2016
Byline: David E. Sanger, Nicole Perlroth

Washington - An unusual question is capturing the attention of cyberspecialists, Russia experts and Democratic Party leaders in Philadelphia: Is Vladimir V. Putin trying to meddle in the American presidential election?
Until Friday, that charge, with its eerie suggestion of a Kremlin conspiracy to aid Donald J. Trump, has been only whispered.

But the release on Friday of some 20,000 stolen emails from the Democratic National Committee's computer servers, many of them embarrassing to Democratic leaders, has intensified discussion of the role of Russian intelligence agencies in disrupting the 2016 campaign.

The emails, released first by a supposed hacker and later by WikiLeaks, exposed the degree to which the Democratic apparatus favored Hillary Clinton over her primary rival, Senator Bernie Sanders of Vermont, and triggered the resignation of Debbie Wasserman Schultz, the party chairwoman, on the eve of the convention's first day.

Proving the source of a cyberattack is notoriously difficult. But researchers have concluded that the national committee was breached by two Russian intelligence agencies, which were the same attackers behind previous Russian cyberoperations at the White House, the State Department and the Joint Chiefs of Staff last year. And metadata from the released emails suggests that the documents passed through

Russian computers. Though a hacker claimed responsibility for giving the emails to WikiLeaks, the same agencies are the prime suspects. Whether the thefts were ordered by Mr. Putin, or just carried out by apparatchiks who thought they might please him, is anyone's guess.

On Sunday morning, the issue erupted, as Mrs. Clinton's campaign manager, Robby Mook, argued on ABC's "This Week" that the emails were leaked "by the Russians for the purpose of helping Donald Trump" citing "experts" but offering no other evidence. Mr. Mook also suggested that the Russians might have good reason to support Mr. Trump: The Republican nominee indicated in an interview with The New York Times last week that he might not back NATO nations if they came under attack from Russia -- unless he was first convinced that the countries had made sufficient contributions to the Atlantic alliance.

It was a remarkable moment: Even at the height of the Cold War, it was hard to find a presidential campaign willing to charge that its rival was essentially secretly doing the bidding of a key American adversary. But the accusation is emerging as a theme of Mrs. Clinton's campaign, as part of an attempt to portray Mr. Trump not only as an isolationist, but also as one who would go soft on confronting Russia as it threatens nations that have shown too much independence from Moscow or, in the case of Lithuania, Latvia and Estonia, joined NATO.

Mr. Trump has also said he would like to "get along with Russia" if he is elected, and complimented Mr. Putin, saying he is more of a leader than President Obama. Mr. Putin has in turn praised Mr. Trump. But Trump campaign officials on Sunday strongly rejected any connections between their candidate and efforts to undermine the Democrats.

"Are there any ties between Mr. Trump, you or your campaign and Putin and his regime?" George Stephanopoulos, of "This Week," asked Paul Manafort, Mr. Trump's campaign chairman.

"No, there are not," Mr. Manafort shot back. "That's absurd. And, you know, there's no basis to it."

One of Mr. Trump's sons, Donald Trump Jr., was more definitive, charging the Clinton camp with a smear campaign. "I can't think of bigger lies," he said on CNN. The younger Mr. Trump mockingly suggested that Mr. Mook's "house cat at home once said this is what happened with the Russians."

It may take months, or years, to figure out the motives of those who stole the emails, and more important, whether they were being commanded by Russian authorities, and specifically by Mr. Putin. But the theft from the national committee would be among the most important state-sponsored hacks yet of an American organization, rivaled only by the attacks on the Office of Personnel Management by state-sponsored Chinese hackers, and the attack on Sony Pictures Entertainment, which Mr. Obama blamed on North Korea. There, too, embarrassing emails were released, but they had no political significance. The WikiLeaks release, however, has more of a tinge of Russian-style information war, in which the intent of the revelations is to alter political events. Exactly how, though, is a bit of a mystery, apart from embarrassing Democrats and further alienating Mr. Sanders's supporters from Mrs. Clinton.

Evidence so far suggests that the attack was the work of at least two separate agencies, each apparently working without the knowledge that the other was inside the Democrats' computers. It is unclear how WikiLeaks obtained the email trove. But the presumption is that the intelligence agencies turned it over, either directly or through an intermediary. Moreover, the timing of the release, between the end of the Republican convention and the beginning of the Democratic one, seems too well planned to be coincidental.

Mr. Trump himself leapt on the news after the WikiLeaks release on Saturday. In a Twitter message he wrote: "Leaked emails of DNC show plans to destroy Bernie Sanders. Mock his heritage and much more. On-line from Wikileakes, really vicious. RIGGED."

The experts cited by Mr. Mook include CrowdStrike, a cybersecurity firm that was brought into the Democratic National Committee when officials there suspected they had been hacked.

In mid-June the company announced that the intruders appeared to include a group it had previously identified by the name "Cozy Bear" or "APT 29" and been inside the committee's servers for a year. A second group, "Fancy Bear," also called "APT 28," came into the system in April. It appears to be operated by the G.R.U., the Russian military intelligence service, according to federal investigators and private cybersecurity firms. The first group is particularly well known to the F.B.I.'s counterintelligence unit, the C.I.A. and other intelligence agencies. It was identified by federal investigators as the likely culprit behind years of intrusions into the State Department and White House unclassified computer system.

Russian intelligence agencies went to great lengths to cover their tracks, investigators found, including meticulously deleting logs, and changing the time stamps of the stolen files.

Officials at several other firms that have examined the code for the malware used against the Democratic National Committee and the metadata of the stolen documents found evidence that the documents had been accessed by multiple computers, some with Russian language settings. Moscow has outsourced politically motivated hacking to outside groups in the past. A crippling attack on Estonia in 2007, for example, was attributed to the pro-Kremlin Nashi youth organization. Intelligence officials and security researchers believe this outsourcing is done, in part, to preserve a measure of plausible deniability.

Intrusions for intelligence collection are hardly unusual, and the United States often does the same, stealing emails and other secrets from intelligence services and even political parties. But the release to WikiLeaks adds another strange element, because it suggests that the intelligence findings are being "weaponized" -- used to influence the election in some way. The story has another level of intrigue involving Mr. Manafort, Mr. Trump's campaign chairman. Working through his lobbying firm, Mr. Manafort was one of several American advisers to Viktor F. Yanukovych, the Russian-backed leader of

Ukraine until he was forced out of office two years ago. Mr. Yanukovych was a key Putin ally who is now in exile in Russia.

In April, asked on Fox News about his relationship with Mr. Yanukovych, Mr. Manafort said he was simply trying to help the Ukrainians build a democracy that could align more closely with the United States and its allies.

Gulf Times
Forum explores cyber challenges in Qatar
Monday, 25 July 2016

Doha - Global technology leader Lockheed Martin has joined hands with Hamad Bin Khalifa University (HBKU) and the University of Patras, Greece, to support the development of Qatar's national cyber security capabilities.
The announcement was made at the first International Cyber Security Technologies Round Table recently.

In line with Qatar National Vision 2030, the round table is part of Lockheed Martin's growing collaboration to support the country's national cyber security objectives.

The round table brought together a group of multi-national cyber experts from across academia and industry to support innovation and open discussions in this field of growing importance to Qatar and the greater GCC region.

The discussions also focused on the build-up of the next generation of cyber defenders. The outcome of the two-day round table will support the development of a comprehensive framework to cultivate the human-capital and educational framework necessary to solve future cyber challenges across diverse sectors of national importance.

Prof Amine Bermak, acting associate provost and ICT division co-ordinator, HBKU said: "Later this summer, we look forward to welcoming our first cohort of students to our new Master of Science in Cyber Security programme. We recognise the importance of collaborating with industry to provide our students with the skills of the future to solve some of the most pressing cyber challenges facing industry and government.The discussions that took place over the past few days will help us develop the talent pipeline in this area of critical national significance to Qatar."

Prof Dimitrios Serpanos from the University of Patras and director of the Industrial Systems Institute said: "The University of Patras is a leading European University in engineering, including electrical and computing, with strong activities in cyber security research. The participation and support to this round table demonstrates the commitment of the faculty to address the growing cyber security challenge to

academia, industry, and governments around the world. Bringing talent together with a global lens will bring the innovative approach we need to shape a more secure future."

Tom Milton, chief executive, Lockheed Martin Qatar, said: "We are excited to support a strong foundation of preparedness for the emerging cyber threats this region will face. Today's increasingly complex security environment requires dynamic collaboration with academia, industry, and government to execute Qatar's national cyber priorities."

According to him the round table was just the beginning. "Lockheed Martin looks forward to leveraging our global technology expertise to support Qatar's efforts to keep its networks and citizens safe from the emerging cyber challenges," he added.

Saudi Gazette
Corporate espionage key reason for cyber attacks in mining sector (Canada).
Monday, 25 July 2016
Byline: Staff Report

Dubai - With Saudi's mining sector to represent 10% of its non-oil revenue by 2030, and other countries like Oman and the UAE investing into latest technologies, the outlook for integrated IT platforms and cloud operations in the mining sector looks promising in the region. However, companies in the sector will have to be ready for the security challenges, these technological advances bring in.
According to a recent report by Trend Micro, the global leader in security software solutions, the mining industry is being targeted by cyber criminals. The security firm has been called in to investigate 17 incidents involving cyber-attacks on 22 entities operating in the sector since 2010.

The most recent attack was recorded in April 2016, when hackers leaked 14.8 GB of data from the Canadian mining corporation Goldcorp.

Though the report does not have major cases from the Middle East and Africa, companies in the region are not immune to these attacks. The UAE-based firm Minerals and Marine Assets Corporation (MAC) and Canadian company Nautilus were the victims of a targeted cyber scam, wherein Nautilus paid a $10-million deposit intended for MAC into an unknown bank account.

According to the report, the main reason for the attacks is corporate espionage among other motives like information theft and hacktivism. The mining industry is both a geopolitical and an economic target, as the data stolen through commercial espionage can have devastating effects on the targeted firm's operations, finances, and market standing, as well as detrimental consequences on the host country's economy.

The prime target for data theft in the mining sector is information about a mine's pricing, which can help a competitor hijack a sales deal by outbidding the competition or a buyer negotiate a better purchase

price or change the terms of a takeover bid. Customer information is another prime target for data theft, competitors can use the stolen information to hijack future sales. The study says cybercriminals also target Intellectual property (IP) data, such as production methods, mineral processing methods, chemical formulae and custom software.

According to Trend Micro, the competitive global market for commodities and manufactured goods, the reliance on natural resources for economic development and fluctuating geopolitical climates have contributed to making mining industry a target of cyber espionage campaigns, and in extreme cases disruptive and destructive cyber-attacks.

Gulf News
Keeping up with next-generation datacentres
Monday, 25 July 2016
Byline: Jyoti Lalchandani

Dubai - The datacenter represents the beating heart of the modern business. It is where information flows in and out of the organisation, ultimately helping to support business functions, create competitive advantage, and drive revenue. And with the emergence of various new trends and innovations, the datacenter has been going through a continuous process of transformation over the past few years.
IT applications and services are critical elements that represent the lifeblood that flows through the datacenter to support the way in which organisations interact with their customers, deliver new products and services, and improve the productivity of their employees. Datacenters are continually being tasked with delivering workloads in the most cost-effective and efficient manner, and organisations must now look to drive greater efficiencies in their operations to provide the agility required to meet future business demand.

So what needs to happen? Well, the traditional manner of provisioning services via hardware and software needs to radically change in order to keep pace with the digital transformation that is rapidly shaping today's business landscape. Past technologies have introduced increased levels of optimisation within the datacenter, but is this enough? Most corporate datacenters were built on the assumption that technology enhancements and workloads occur at a steady and predictable pace, but that is not the rate of change we are currently experiencing.

IDC believes that CIOs must also consider whether their current technology platforms are capable of supporting the agility and scale expectations that businesses now demand. And how can the IT department manage these expectations while simultaneously facilitating greater levels of innovation? These are just some of the challenges facing IT executives today. And in order to address these challenges, the datacenter needs to evolve and keep pace with the dynamic trends that are shaping the external market.

New technologies should be implemented not only to reduce complexity and costs, but also to redefine the way in which the IT department provisions services for consumption. The concept of next-generation datacenters has been around for a while, where initially the main tasks were to rationalise, consolidate, and standardise the IT environments. While many organisations are progressing along this path, the next wave of change beyond virtualisation needs to address the provisioning of IT as a service (ITaaS) by moving away from the current silo-based approach.

With each passing year, it appears that the competitive environment requires businesses to deliver applications faster and improve productivity, whilst simultaneously reducing costs. The costs associated with provisioning, monitoring, and managing servers have escalated, challenging organisations to seek out new systems and tools that can help them lower the overall cost of it operations, including -- among others -- converged systems, hyperscale cloud infrastructure, software-defined computing, OpenStack, modularity, and virtualisation.

We currently find ourselves in the midst of widespread digital transformation, with the endgame being the conversion of all business and IT operations into digital processes. This technology evolution is already placing intense demands on CIOs and the IT departments they manage. And adding to this pressure is the way in which end-user expectations for IT services are evolving; internal and external customers alike now expect to be able to access applications and data at anytime from anywhere and on any device.

What all this means is that the performance of business operations is now intrinsically linked to the datacenter and its accompanying server infrastructure. With this in mind, next-generation datacenters are focusing on the services they deliver and how they are delivered. And for all this to be effective, CIOs must develop a comprehensive understanding of how individual business units operate, as well as a clear picture of the end user's current and future needs. Indeed, IDC believes that such knowledge of individual workload characteristics will play a critical role in deciding which server technologies to adopt, maintain, and/or retire.

Given how essential IT applications and services are to the success of any modern business, the primary goal must now be to maximise application performance and efficiency. Some applications, such as large databases, will run best on a converged system that integrates hardware with software, while other applications will be better to run in a hosted service provider environment. It is ultimately the CIO's responsibility to sift through these options and weigh the pros against the cons to make the right decision.

But to help you along the way, IDC advises customers that are deploying next-generation applications with distinctly different operational characteristics to explore containers, software-defined computing, and disaggregated and compostable systems. On the other hand, customers with more traditional enterprise application needs may be better served by avoiding disaggregated and compostable systems, as those systems are not yet optimised for these workloads.

As businesses battle to maintain a modern infrastructure and keep their business goals in context, there is often a temptation to chase the latest innovation waves. But without a clear match between innovative new technologies and a useful business outcome, new technology for new technology's sake is never a good choice to make. That said, hot new emerging technologies such as containers, OpenStack, and software-defined computing are unlocking new opportunities for IT that can deliver tangible benefits -- to the right application.

Gulf News
Don't search for a magic bullet for cyber security
Monday, 25 July 2016
Byline: Dr. Robert Statica

Dubai - Governmental agencies shouldn't just rely on installing the latest software and hardware - they should take clear steps in training, process and practice to ensure they're protected from cyber attacks. Although there is no such thing as one solution fits all when it comes to cyber defence, there are certain steps that every government agency must employ to create a solid foundation on which they can start building their cyber defences.
Government agencies remain in the cross hairs of cyber attackers as hostile nation-states, terrorists, hackers for profit and campaigning organisations (hacktivism) focus on breaching their systems. Government cyber security professionals should always take a holistic approach to managing their defences and response procedures, but there are some key steps which are the building blocks of a strong defence.

Edward Snowden's data leakage and the WikiLeaks scandal have highlighted the danger of malicious disclosure, but more often than not the threat comes not from deliberate employee sabotage, but rather from ignorance or careless practice. Threats from hostile governments or sophisticated criminal organisations - dubbed 'Advanced Threats' by the industry - often use an initial employee mistake to embed themselves in a targeted department, gaining persistent access to a system and becoming increasingly difficult to detect.

So employee mistakes can have implications far beyond the immediate incident. It is therefore vital that all employees, whatever their seniority level, should be given continuous cyber-security awareness and counter-intelligence training, to avoid poor practice and minimise the possibility of a security breach. Employees are the most important part of the information system of an agency, but also its weakest link when it comes to cyber security and defence.

Likewise, public knowledge of software and hardware used in a department's network should be limited to a few trusted and vetted employees who have a real "need to know". If hostile actors understand a system's make-up in advance (as part of their pre-attack recognisance), then they can tailor their attacks to known vulnerabilities, giving them a headstart before they begin probing the system's defences directly.

This is why it's also vital to do a constant security vetting, and re-vetting, of outside vendors with access to the system, even if their role is relatively limited. Many times breaches of the vendor's networks or software and hardware products, lead to breaches of their customer networks and to data exfiltration, and many a time goes undetected by the customer.

Just as knowledge should be compartmented and firewalled, so should software. Patches, updates and fixes can often prove a 'Trojan horse' allowing malware to enter the system either causing direct damage, or creating an opening for future exploitation. They should therefore always be deployed in a 'sandbox', a virtual space, discrete from the main system which allows new software to be run isolated without risk of contamination of the main network.

Once vetted from the security, compatibility and functionality point of view, the patches or updates should be deployed to the main network in a staged upgrade push that would minimise the possibility of the entire network being down. To avoid unwitting disclosure of information all communications should be end-to-end encrypted - that means not just voice, but texts and files as well, both in transit and at rest.

Crucially, encryption systems should also sit on hardened hardware, the best algorithm in the world won't preserve your privacy if it's hosted on an insecure computer, cloud or mobile handset.

Lastly, but certainly not least, government cyber security professionals should constantly test the security of their systems through penetration testing. Knowing your network from the outside will provide invaluable information about the vulnerabilities (and sometimes even zero day exploits) of your systems. This is an ideal role for outside vendors who can bring in some of the best hacking expertise in the world, at far lesser expense than keeping it in- house.

External contractors also have the great advantage of being unbiased by the system; they won't overlook that crucial vulnerability because that's how the department has held its data for years, or because it's due to be resolved in next year's round of IT upgrades. They bring an honest perspective on how your system works from the outside.

Testing has to be a constant and iterative process: test, analyse, remediate (both through processes and upgrades), then test again.

There's never a magic bullet to defeating cyber threats, this is a constant battle, but through a combination of training, processes and judicious use of outside expertise government security professionals can help ensure their department doesn't become the subject of the next cyber attack newspaper headline.

La Presse+
Renseignements personnels Au voleur !
Monday, 25 July 2016
Byline: Ariane Krol

Editorial - Aussi incroyable que cela puisse paraître, les renseignements personnels que vous partagez avec une entreprise pourraient être piratés sans que vous en soyez jamais avisés. Plus pour longtemps, heureusement. Les vols de données devront bientôt être déclarés, prévoit un règlement actuellement à l'étude au ministère fédéral de l'Innovation. Reste à s'assurer que cela se fera avant tout dans l'intérêt des citoyens.
Pour l'instant, les Canadiens ont plus de chances d'être informés si leurs renseignements sont volés à une société américaine, comme Home Depot ou Target, que si la cible du piratage est une entreprise locale. La plupart des États américains exigent en effet que ces événements soient déclarés - certains sont d'ailleurs en train d'élargir cette obligation.

Chez nous, c'est à la discrétion des entreprises. Seuls les ministères et organismes du gouvernement fédéral doivent déclarer ces failles, comme Revenu Canada l'a fait en 2014. La Loi sur la protection des renseignements personnels numériques, adoptée il y a un an, vise à corriger cette lacune. Il était temps.

Les entreprises piratées ne sont pas les seules victimes, loin de là. Si vos renseignements personnels ont été compromis, vous risquez d'en subir les inconvénients.

Devoir changer son numéro d'identification personnel (NIP) ou sa carte ne prend pas trop de temps, mais se faire créditer des transactions frauduleuses peut se révéler laborieux. Et c'est sans compter le risque de vol d'identité. Que les consommateurs soient mis dans le coup afin de pouvoir prendre certaines précautions ou, à tout le moins, redoubler de vigilance est un minimum.

Autre avantage : cette obligation de divulgation devrait inciter les entreprises à mieux protéger les renseignements personnels qu'elles détiennent. Avoir à contacter des centaines ou des milliers de clients lésés alourdit la facture, déjà salée, avec laquelle doit composer une organisation touchée par une perte ou un vol de données. Sans oublier la perte de confiance et de revenus qui suivront, surtout si l'on apprend qu'elle a été négligente. L'effet ne sera pas instantané, mais à force de voir des entreprises échaudées, celles qui rechignent à investir en sécurité referont peut-être leurs calculs.

Ottawa a déjà tenu une première consultation. Une nouvelle version du règlement devrait bientôt être publiée pour commentaires. L'intérêt des citoyens doit demeurer en tête des priorités. Déjà, seuls les cas où il y un « risque réel de préjudice grave » doivent être divulgués. Les entreprises seraient donc malvenues de crier à la lourdeur bureaucratique. Avec tous les renseignements qu'elles récoltent à la moindre transaction (carte de crédit, courriel, numéro de téléphone, et bien plus avec les achats en ligne), on s'attend à ce qu'elles fassent le maximum pour en assurer la protection.

Al Jazeera
Iran destroys 100,000 'depraving' satellite dishes
Monday, 25 July 2016

Tehran - Authorities say the banned satellite dishes are morally damaging, despite high-level calls for reform of the law.
Iranian authorities have destroyed 100,000 satellite dishes and receivers as part of a widespread crackdown against illegal devices they say "deviate morality and culture".

Most of these satellite channels not only weaken the foundation of families but also cause disruptions in children's education and children who are under the influence of satellite have improper behaviour.

General Mohammad Reza Naghdi, the head of Iran's Basij militia, oversaw the destruction ceremony in Tehran on Sunday and warned of the impact that satellite television was having in the country.

"The truth is that most satellite channels... deviate the society's morality and culture," AFP news agency reported him as saying. "What these televisions really achieve is increased divorce, addiction and insecurity in society."

Naghdi said that a total of one million Iranians had already voluntarily handed over their satellite dishes to authorities.

Conservatives regularly denounce the channels as an attempt to corrupt Iranian culture and Islamic values.

Iranian police regularly raid neighbourhoods and confiscate dishes from rooftops, and under Iranian law, satellite equipment is banned and those who distribute, use, or repair them can be fined up to $2,800.

On Friday, Culture Minister Ali Jannati called for a revision of the law. "Reforming this law is very necessary as using satellite is strictly prohibited, but most people use it," Jannati said. "This means that 70 percent of Iranians violate the law" by owning satellite dishes, he added.

Naghdi criticised Jannati's comments and said those in charge of cultural affairs "should be truthful with people rather than following what pleases them".

"Most of these satellite channels not only weaken the foundation of families but also cause disruptions in children's education and children who are under the influence of satellite have improper behaviour," Naghdi said.

There are dozens of foreign-based Farsi satellite channels broadcasting mostly news, entertainment, films and series.

President Hassan Rouhani, whose four-year mandate ends in June 2017, has repeatedly said that the ban on satellite dishes is unnecessary and counterproductive.

New York Times
In D.N.C. Hack, Echoes of Russia's New Approach to Power
Tuesday, 26 July 2016
Byline: Max Fisher

Analysis - Of the questions raised by charges that Russia was involved in the release of hacked Democratic National Committee emails, at least one -- why would Russia do such a thing? -- can be answered with a little-noticed but influential 2013 Russian military journal article.
"The very rules of war have changed," Gen. Valery V. Gerasimov, the chief of the general staff, wrote in the Military-Industrial Courier.

The Arab Spring, according to General Gerasimov, had shown that "nonmilitary means" had overtaken the "force of weapons in their effectiveness." Deception and disinformation, not tanks and planes, were the new tools of power. And they would be used not in formally declared conflicts but within a vast gray between peace and war.

Those ideas would appear, the next year, in Russia's formal military doctrine. It was the culmination of a yearslong strategic reorientation that has remade Russian power, in response to threats both real and imagined, into the sort of enterprise that could be plausibly accused of using cyberattacks to meddle in an American presidential election.

'We are protecting our sovereignty'

Like so many military rethinks, what became known as the Gerasimov Doctrine began as an effort to solve a seemingly urgent problem.

Throughout the 2000s, popular uprisings in Eastern Europe and Central Asia overturned their pro-Kremlin leaders, replacing them with democratically elected governments more inclined to the West.

In Moscow, these "color revolutions," as well as the subsequent Arab Spring, were seen as a wave of hostile American operations, engineered to topple Russia's allies and weaken Russia itself.

Sergei Shoigu, the Russian defense minister, said in a 2014 speech that such uprisings were "used as an excuse to replace nationally oriented governments with regimes controlled from abroad."

The Kremlin felt encircled and threatened by what it took to be a vast American conspiracy whose ultimate goal, it concluded, was the subjugation or outright destruction of the Russian state.

In December 2011, thousands gathered in Moscow to protest legislative elections that had been marred by accusations of fraud. The demonstrations didn't come to much, but they engendered a fear among Russian leaders that they were next.

President Vladimir V. Putin, at a news conference in 2014, warned that the West was seeking to "defang" the Russian bear -- to remove its nuclear weapons so as to gain access to its natural resources.

"Once they've taken out his claws and his fangs, then the bear is no longer necessary," Mr. Putin said. "The issue is that we are protecting our sovereignty and our right to exist."

Russian military planners, apparently obsessed with such fears, concluded that their best defense would be to go on the offense. Believing that the Americans were already conducting a clandestine war through intelligence operations, media disinformation, and deniable proxy forces, they set out to do the same.

The phrase "hybrid war" -- a common label in the West for Russia's actions -- was first used by Russian analysts to describe the supposed American tactics they believed they were countering. They called their own strategy something different: "new generation war."

Projecting power beyond Russia's strength

Even before this doctrine became formalized, Russia had developed tools of coercion and subterfuge, providing a model for wider usage.

As Russian power has resurged under Mr. Putin, the country has often used asymmetrical methods to assert its interests, particularly in the former Soviet republics it still considers its "near abroad" and rightful zone of influence.

In 2007, amid tensions with the small Eastern European nation of Estonia, Russian media falsely reported that members of Estonia's Russian minority were being drugged and tortured by police, contributing to riots that injured several people and killed one. The next day, cyberattacks, attributed to a pre-Kremlin Russian group, forced many of Estonia's major institutions offline.

At no point, in the 2007 episode, did Russia commit an act of military aggression against its neighbor. Yet Estonian leaders say these actions were meant as a message: Even if their country had joined NATO and the European Union, Moscow was still the boss.

These sorts of tools allowed Russia to project power beyond its strength and, just as importantly, to assert its interests abroad despite Western military and political dominance.

To paraphrase Mark Galeotti, a New York University professor who studies Russia's military, this is a country whose economy is smaller than Canada's or South Korea's, yet is seeking a great power role akin to China or the United States. Traditional methods won't cut it.

Information struggle and Maidan technology

Russia deployed its "new generation war" to startling effect in early 2014, when, amid Ukraine's political crisis, it seized and subsequently annexed the Ukrainian region of Crimea.

While that action is most remembered for the "little green men" - - unmarked Russian special forces who seized key locations in a clandestine invasion -- there were subtler components as well.

Russian state news media flooded Crimea's airwaves with false stories about neo-Nazis taking over Ukraine and systematically attacking ethnic Russians, who are a majority in Crimea. As a result, many Crimeans welcomed the unmarked Russian troops, believing they were being saved from possible ethnic cleansing.

Dmitry Adamsky, an Israeli analyst, wrote in a 2015 report that this "information struggle" is central to Russia's new strategy.

This information war, he wrote, "comprises both technological and psychological components designed to manipulate the adversary's picture of reality, misinform it and eventually interfere with the decision-making process of individuals, organizations, governments and societies."

While this was especially visible in Crimea, Mr. Adamsky warned that it was also deployed in peacetime and against any target where Moscow seeks influence. It may be intended to pursue a "strategic goal," such as the weakening of pro-American political parties in Europe, or to simply foment a degree of instability that weakens adversaries.

Mr. Adamsky described this as a form of "subversion" that "aims to deceive the victim, discredit the leadership, and disorient and demoralize the population and the armed forces."

That sheds light on why Russia might want to release Democratic National Committee emails, whose greatest effect is creating a kerfuffle within Democratic politics. It's not as if the resignation of the party chairwoman, Debbie Wasserman Schultz, was some strategic Russian ambition.

While some observers say Moscow sees a potential friend in Donald J. Trump, it would also be well within Russian strategy to stir up trouble just to stir up trouble. This is what Mr. Adamsky calls "managed stability-instability" -- low-level confusion and disunity that Russia could perhaps one day exploit.

Russia has long seen itself as the victim of these very tactics, accusing Western governments of using vague "Maidan technology," named for the square where Ukraine's 2014 protests began, to create "managed chaos" in targeted countries. Embarrassing stories, such as the Russian doping scandal and the Panama Papers, are seen as American information warfare meant to weaken Moscow.

In this view, Kremlin leaders could see releasing internal Democratic emails as a tit-for-tat retaliation in the information struggle. Such a thing would make little sense in the Western conception of geopolitics.

But as Mr. Adamsky wrote in his 2015 study, Americans have long tried to conceptualize Russian strategy within Western ways of thinking, when it is anything but.

USA Today
It will be hard to prove Russians are behind DNC hack, experts say
Tuesday, 26 July 2016
Byline: Elizabeth Weise

Washington - Computer security researchers say it's difficult to definitively say the cyber theft of files from the Democratic National Committee was perpetrated by Russian hackers as some media outlets have reported.
"Just because you find an AK-47 at a crime scene doesn't mean a Russian pulled the trigger," said J.J. Thompson, chief executive of Rook Security, an Indianapolis-based firm.

On Friday, WikiLeaks released what it said were 19,252 emails and 8,034 attachments from leaders at the Democratic National Committee.

The documents, which the DNC has not dismissed as fraudulent, show antipathy toward Bernie Sanders, who had hoped to win the party's presidential nomination.

They infuriated Sanders supporters and led to U.S. Rep. Debbie Wasserman Schultz's announcement she would step down as the committee's chair.

On Sunday, Hillary Clinton's campaign manager, Robby Mook, said on ABC's This Week that the emails had been extracted by the Russians to help Donald Trump's campaign. To support his claim, Mook cited "experts."

Mook added to this charge Monday, telling reporters, "All we know right now is what experts are telling us," which is that "Russian state actors were feeding the emails to hackers for the purpose of helping Donald Trump."

In an article published Monday, The New York Times reported that researchers at CrowdStrike, an Irvine, Calif.-based cyber-security firm, had concluded the breach was the work of two Russian intelligence agencies, or people working for or with them.

CrowdStrike declined to comment for this article. However, in May and June it blogged that an analysis it had completed of the long- known intrusion into the DNC's computer network was the work of Russian intelligence-affiliated adversaries, one of whom it called Cozy Bear and the other Fancy Bear.

CrowdStrike said that it had run into both of these groups in previous attacks.

"Both adversaries engage in extensive political and economic espionage for the benefit of the government of the Russian Federation and are believed to be closely linked to the Russian government's powerful and highly capable intelligence services," Dmitri Alperovitch, the company's co-founder, wrote in its blog.

However, experts within the cyber-security world say it's extremely difficult to know exactly who is behind an attack without the kind of on-the-ground surveillance that only government agencies are able to provide.

The FBI said in a statement that it was investigating the intrusion into the DNC's computer network.

The Japan News
Govt to protect source code in economic deals
Tuesday, 26 July 2016
Byline: Staff reporter

The government has decided to include stipulations on protecting the confidential data of software in future economic deals it signs, aiming to curb China and other countries that have requested such data from companies, sources say.
The government intends to address the issue in economic partnership agreements and investment agreements when it signs them with other countries and regions, as advanced technologies such as the internet of things (IoT) and artificial intelligence play an ever-growing role.

At Monday's meeting of World Trade Organization member countries in Geneva, Japan was to propose that rules be established to prohibit WTO countries from making requests to divulge source code. The government ultimately aims to create a pact among countries and regions in favor of the idea.

The Trans-Pacific Partnership free trade agreement -- which was officially signed in February by Japan, the United States and 10 other countries -- prohibits signatories in principle from requesting private companies to disclose source code.

Revealing source code may leak a software creator's critical development know-how, which could not only threaten the intellectual property of developers, but also make it possible to remotely control devices connected to the internet.

Japan aims to include similar stipulations to those under the TPP in economic deals with other countries and regions. The government has been discussing the issue in talks with Colombia and the European Union over economic partnership agreements, and also plans to deal with it during negotiations on investment agreements with Ghana, Morocco and Tanzania.

The move has been driven by China, which has made requests that foreign countries operating in the country disclose source code for information-related and other products, citing security checks among other reasons. It has been reported that Russia and some developing countries have made similar requests.

CBS News
Kerry discusses DNC email hack with Russia's top diplomat
Tuesday, 26 July 2016
Byline: Staff report

Vientiane, Laos - Secretary of State John Kerry says he raised the email hack of the Democratic National Committee with Russia's top diplomat but stopped short of making any allegation about who might be responsible.
Kerry told reporters Tuesday he brought the matter up with Russian Foreign Minister Sergey Lavrov at a meeting in Laos and explained that the FBI was investigating. He did not, however, repeat allegations or echo suspicions that Russia was responsible for the hack and said he would not draw conclusions until the probe is complete. "I raised the question and we will continue to work to see precisely what those facts are," Kerry said. He would not say if Lavrov responded.

Asked about the allegations earlier, Lavrov scoffed, saying: "I don't want to use 4-letter words."

The FBI confirmed Monday that it was investigating the hack involving Democratic National Committee (DNC) emails.

A cache of more than 19,000 emails from Democratic party officials, were leaked Friday in advance of Hillary Clinton's nomination at the party's convention this week in Philadelphia, and they detail the acrimonious split between the Democratic National Committee and Clinton's former rival, Sen. Bernie Sanders, D- Vermont.

Although Wikileaks' posting of the emails Friday did not disclose the identity of who provided the private material, those knowledgeable about the breach said last month that Russian hackers had penetrated the DNC computer system. At the time, DNC Chairwoman Debbie Wasserman Schultz said the breach was a "serious incident" and a private contractor hired to sweep the organization's network had "moved as quickly as possible to kick out the intruders and secure our network."

The Hillary Clinton campaign has blamed the email leaks on Russia, reports CBS News' Julianna Goldman.

Clinton's campaign manager Robbie Mook accused Russian President Vladimir Putin of meddling in the U.S. election.

"What the experts said when this breach initially happened at the DNC was that they believed that it was Russian state actors who took these emails," Mook said.

"Russian state actors were feeding the emails to hackers for the purpose of helping Donald Trump," he continued.

But neither the Clinton campaign, the White House, nor lawmakers briefed on the hack definitively linked the leak to the Russian government on Monday.

Miami Herald
Bitcoin not money, Miami judge rules in dismissing laundering charges
Tuesday, 26 July 2016
Byline: David Ovalle

Miami - A Miami-Dade judge ruled Monday that Bitcoin is not actually money, a decision hailed by proponents of the virtual currency that has become popular across the world.
In a case closely watched in financial and tech circles, the judge threw out the felony charges against website designer Michell Espinoza, who had been charged with illegally transmitting and laundering $1,500 worth of Bitcoins. He sold them to undercover detectives who told him they wanted to use the money to buy stolen credit- card numbers.

But Miami-Dade Circuit Judge Teresa Mary Pooler ruled that Bitcoin was not backed by any government or bank, and was not "tangible wealth" and "cannot be hidden under a mattress like cash and gold bars."

"The court is not an expert in economics; however, it is very clear, even to someone with limited knowledge in the area, the Bitcoin has a long way to go before it the equivalent of money," Pooler wrote in an eight-page order.

The judge also wrote that Florida law -- which says someone can be charged with money laundering if they engage in a financial transaction that will "promote" illegal activity -- is way too vague to apply to Bitcoin.

"This court is unwilling to punish a man for selling his property to another, when his actions fall under a statute that is so vaguely written that even legal professionals have difficulty finding a singular meaning," she wrote.

The ruling was lauded by Bitcoin experts who believe the ruling will encourage the use of the virtual currency, and offer a roadmap to governments across the world that have struggled to understand and regulate it.

Espinoza's attorney, Rene Palomino, said the judge's order was "beautifully written."

"At least it gives the Bitcoin community some guidance that what my client did was not illegal," Palomino said. "What he basically did was sell his own personal property. Michell Espinoza did not violate the law, plain and simple."

A spokesman for the Miami-Dade State Attorney's Office said: "We are presently reviewing the court order to determine whether we will be appealing this decision."

Law enforcement has struggled to figure out how Bitcoin fits into illegal activities, and Espinoza's case was believed to be the first money-laundering prosecution involving the virtual currency.

The controversial virtual currency allows some users to spend money anonymously and it can be also be bought and sold on exchanges with U.S. dollars and other currencies.

The currency has gained popularity with merchants selling legitimate goods and services. In Miami, there are a few restaurants that accept the virtual currency -- and even a plastic surgeon.

Regulated services such as CoinBase, which operates similarly to PayPal, allow people to buy, sell and use the Bitcoins. But authorities have raised concerns about the currency being used in the anonymous black market.

Most notoriously, Bitcoins were used to traffic drugs in the now-shuttered Silk Road network. In an unrelated South Florida case, a Miramar man got 10 years in prison after using Bitcoins to buy Chinese-made synthetic heroin from a Canadian prisoner.

In Espinoza's case, Miami Beach detectives found him through a Bitcoin exchange site, LocalBitcoins.com, and told him they were going to use the currency to purchase stolen credit-card numbers.

The detectives met with Espinoza, 32, three times in person: on Lincoln Road, at an ice cream shop and in a hotel room.

Espinoza was arrested along with another man, Pascal Reid, who pleaded guilty to acting as an unlicensed money broker and was sentenced to probation. Under his unusual plea deal, he agreed to teach law enforcement about Bitcoin.

At a hearing in May, a defense expert, Barry University economics professor Charles Evans, testified that Bitcoin was not actually money.

No central government or bank backs Bitcoin, like the United States does the dollar. Government regulation of Bitcoin remains a messy hodgepodge from state to state, country to country. The IRS considers Bitcoin deals no more than bartering, he said.

"Basically, it's poker chips that people are willing to buy from you," said Evans, a virtual-currency expert who was paid $3,000 in Bitcoins for his defense testimony.

The judge's decision will help Bitcoin flourish in Miami and countries where banking system are tenuous, Evans said in an interview on Monday.

"Bitcoin is perfect for small-scale cross-border transactions and we are international in this area," Evans said. "If somebody from Venezuela needs a hammer, now that person can send Bitcoin to his cousin in Miami, that cousin can sell the Bitcoin, go buy the hammer and send it to Venezuela."

The ruling could also spark a push to tweak Florida law. Judge Pooler, in her ruling, said the state's money-laundering law that targets transactions that "promote" illegal activity requires a "much-needed update."

"Hopefully, the Florida Legislature or an appellate court will define 'promote' so individuals who believe their conduct is legal are not arrested," Pooler wrote.

Jerusalem Post
IDF bans 'Pokemon Go' app from all military bases amid security fears
Tuesday, 26 July 2016
Byline: Yaakov Lappin, Judy Siegel-Itzkovich

Jerusalem - Acting on concerns that soldiers on IDF bases playing Pokemon Go could download a lookalike application and inadvertently reveal sensitive data, the military this week banned all usage of the smart phone application on military property.
The decision was taken by the IDF's Security Division, which recently ordered all soldiers and officers to cease playing the game on base immediately.

The IDF Spokesperson Unit said in a statement that "a concern over the leaking of sensitive military information, such as photographs and base locations," drove the decision.

Military sources said they had become aware of another application that "looks and acts like the original [Pokemon Go] application, which causes data to be leaked out," adding that this was the real reason for banning the game.

It noted that "as part of the installation of the application, a device's camera is activated to enable the game's embedded reality, while location sensors, for orientation around an area, are also activated."

Meanwhile, with large numbers of people running around during daylight exposed to the sun trying to capture monsters for the Pokemon Go smartphone application, the Israel Cancer Association warns the public to protect itself from sunburn and the risk of skin cancer.

The relatively safe hours to go out are before 10 a.m. and after 4 p.m., the ICA cautions. Try to spend as much time in the shade, and wear a wide-brimming hat, sunglasses and light, longsleeved clothing and regularly apply sunscreen, the ICA warns. Drink water often to avoid heat prostration, and be aware of traffic dangers.

Nextgov.com
Spy Chief 'Excited' about Agency's Modernization Effort
Tuesday, 26 July 2016
Byline: Frank Konkel

Washington - Although CIA Director John Brennan admitted last week the agency's modernization effort has experienced pushback from some of its most tenured employees, he expressed excitement over how his agency has used technology to improve its data collection and analytic efforts.
The CIA made news two years ago for its deal with Amazon Web Services to lead the development of cloud computing capabilities for the intelligence community. Then, last year, the CIA stood up its first new directorate in more than 50 years, designed to improve agents' individual tech skills, improve data governance across the agency and to harness the power of big data.

Evidently, it hasn't been easy.

"I am very excited about where the agency is going," Brennan said at a July 19 Intelligence and National Security Alliance event. "Yes, a big organization that goes through a modernization is going to experience dislocations. And people who grew up in the organization over the last 20 or 30 years, it's like, 'oh, God what is Brennan doing now?' But I think the initial opposition in some quarters to this really has dissipated as we've been able to explain what the purpose is."

The goal, he continued, is "not to homogenize everybody," but to connect intelligence analysts and others in ways not possible in previous decades. Brennan said the decision to restructure was made out of necessity - the demands for signal intelligence and to feed policymakers' voracious appetites for situational information tied to international events.

A new directorate - headed by Deputy Director Andrew Hallman - is doing exactly that, helping integrate intelligence for consumption by CIA analysts and others across the IC.

"The organizational structure of the CIA was not optimally configured to give us that," Brennan said. "And I think this is going to allow us to have a better opportunity to ensure that the various regions of

the world have constant attention of CIA officers who are working together to identify what might be over the horizon."

Chief among them is the ability of analysts to pick up "early indicators" of global events, such as the recent flood of ISIL-inspired terrorist attacks or the attempted coup in Turkey. Brennan said getting those "advanced warnings" is "increasingly a challenge" meriting more resources.

Pravda
Russian FM Lavrov refuses to use 4-letter words in comments about Russian hackers
Tuesday, 26 July 2016
Byline: Staff report

Moscow - Russian Foreign Minister Sergei Lavrov said he could not exclude expletives from his comments about the Russian trace in the hacking of the US Democratic Party mail server. It was reported that Russian hackers could be involved in the recent cyber attack on the USA.
Last week, WikiLeaks published documents indicating that the party leadership was favoring Hillary Clinton in the fight for the right to become a candidate for US presidency to the detriment of Bernie Sanders.

"I would not like to use four-letter words," Lavrov said when asked to comment on the Russian track in the data leak.

The New York Times wrote with reference to computer security experts that the metadata of the documents of the Democratic National Committee contained traces of computers with Russian language settings.The traces were reportedly found in the code that was used to hack into the computer network of the national committee of the party.

In June, computer security experts told The Washington Post that the headquarters of the Democratic Party were infiltrated by hacker groups that were allegedly associated with Russia. Spokespeople for CrowdStrike clarified that it goes about such groups as Cozy Bear and Fancy Bear. According to the experts, the groups could be linked with the Russian FSB and the Central Intelligence Directorate (GRU).

The Kremlin has ruled out any involvement of Russian state structures in the hacking of computer networks of the Democrat Party. Later, lone hacker known as Guccifer 2.0 claimed responsibility for the attack. He promised that the hacked documents would be published on WikiLeaks.

On Monday, the head of the US Democratic National Committee (DNC), Debbie Wasserman Schultz, announced a decision to resign in connection with the scandal about the leak.

London Times

Judge appointed 'surveillance tsar' after police spy row
Tuesday, 26 July 2016
Byline: Neill Johnston

London - A leading judge has been appointed as the country's new "surveillance tsar" after a controversial row over police spying.
Lord Bracadale, who presided over the trials of Nat Fraser and Tommy Sheridan, is now being urged to "vigorously protect" the interests of the public and journalists.

The appointment comes after police were found to have spied on one of their own officers in an effort to uncover the source of media leaks, and was wel-comed by opposition parties after more than a year of delay in filling the role.

Liam McArthur, a Liberal Democrat MSP, said: "The fact that a commissioner is now in place will mean nothing unless he vigorously protects the interests of journalists and others who have had their communications data intercepted unlawfully. Units within Police Scotland played fast and loose with the rules to identify journalistic sources and in many respects seem to have ignored them altogether. This cannot be allowed to happen again."

Last year it emerged that Police Scotland had contravened the communications data code of practice.

Its counter corruption unit was found to have breached its requirement to seek judicial approval in trying to establish whether officers had leaked information to a newspaper about the original investigation into the murder of Emma Caldwell, a sex worker.

An independent inquiry is now likely to be carried out by an external force after a day of legal arguments before the investigatory powers tribunal in Edinburgh last week. The annual report of the UK's Office of Surveillance Commissioners for 2015-16, published earlier this month, raised concerns.

It said: "We are concerned that one police force in the United Kingdom finds itself in a different position to its counterparts across the border."

A Scottish government spokeswoman said: "Surveillance commissioners have held high judicial office, which provides strong assurance of independence and integrity in carrying out their functions. The interception of communications commissioner has commented on the robust and rigorous steps Police Scotland has now taken to ensure processes for all communications data applications are fully compliant with the code of practice." In 2012, Nat Fraser went on trial before Lord Bracadale for the murder of his wife Arlene in Elgin in 1998. He was found guilty by a majority verdict and sentenced to a minimum of 17 years imprisonment.

In 2010, Lord Bracadale presided over the trial of Tommy Sheridan, a former MSP, for perjury in a case involving News Group Newspapers. He was found guilty and sentenced to three years in prison.

Wall Street Journal
DNC Hack Prompts Allegations of Russian Involvement
Tuesday, 26 July 2016
Byline: Damian Paletta, Davelin Barrett

Washington - The theft and leak of embarrassing Democratic National Committee emails created a political firestorm at the party's convention and prompted Democratic allegations of involvement by the Russian government.
U.S. authorities said they were still investigating who perpetrated the hack, but cybersecurity experts said the email release resembled past examples of political interference that other countries have tied to Russia.

Russian officials have denied involvement in the DNC hack. U.S. national-security officials haven't drawn a conclusion in the matter but consider Russian intelligence the chief suspect, according to people familiar with the investigation.

Regardless of who is responsible, the release of the DNC emails created immediate political fallout with the resignation of Democratic Party chief Debbie Wasserman Schultz and led to maneuvering by Democrats and Republicans seeking to spin the controversy.

Multiple Democrats alleged the Russian government stole the emails and provided them to WikiLeaks for publication in an effort to help Republican presidential nominee Donald Trump win the November election, though they offered no proof. "I think that voters need to take a look at this," said Robby Mook, campaign manager for Democrat Hillary Clinton's campaign. "It's troubling if it's true."

Meanwhile, Mr. Trump has attempted to take political advantage of the development. "She worked very hard to rig the system," Mr. Trump said of Mrs. Clinton at a Virginia campaign appearance. "Little did she know that China, Russia one of our many many 'friends' hacked the hell out of us."

The November elections could have a profound impact on U.S.-Russia relations at a time when the countries are at odds over the Syrian civil war and other foreign-policy matters.

Mrs. Clinton has described Russian President Vladimir Putin as a "bully" who needs to be stood up to. Mr. Trump has said several times that the U.S. needs to work more closely with Russia--to help the U.S. disentangle itself from the Middle East-- and that the U.S. should rethink its alliance with members of the North Atlantic Treaty Organization, a group that has traditionally stood as a resistance to Russian interference.

Cybersecurity experts have said forensic evidence in the DNC breach and the leaked emails connects the operation to Russian actors.

"The Russian security services have long experience in trying to directly influence elections abroad," said Alexander Klimburg, a cyber expert at the Hague Center for Strategic Studies.

White House spokesman Josh Earnest said he couldn't verify the results of investigations by private firms and said the Federal Bureau of Investigation would determine whether to make the results of its investigation public.

He said there are "a variety of actors both state and criminal who are looking for vulnerabilities in the cybersecurity of the United States, and that includes Russia."

The FBI said it is still working "to determine the nature and scope of the matter. A compromise of this nature is something we take very seriously."

"We see the flood of inadequate and inappropriate allegations that has inundated the U.S. media. One can only be surprised by such childish groundless accusations that are far beyond reality," said Yury Melnik, press secretary at the Russian embassy in Washington.

Russian hackers have long targeted U.S. political entities and policy groups, including political parties and senior elected officials, according to U.S. officials. Alarming to some U.S. officials is the possibility that the DNC hack shows the Russians may be getting more aggressive and attempting to sway the U.S. political process.

"That foreign actors may be trying to influence our election--let alone a powerful adversary like Russia--should concern all Americans of any party," Rep. Adam Schiff, the top Democrat on the House Intelligence Committee, said Monday.

In June, CrowdStrike, a cybersecurity firm hired by the DNC, found that "two separate Russian-intelligence affiliated adversaries" had breached the DNC network in May.

CrowdStrike has labeled the alleged Russian hacking teams as COZY BEAR and FANCY BEAR.

COZY BEAR is believed to be the same team that successfully breached White House networks, the State Department, and the U.S. Joint Chiefs of Staff, among others. CrowdStrike has tied FANCY BEAR to past hacks targeting aerospace, military, energy, government and media sectors. CrowdStrike found that COZY BEAR was in the DNC's network since at least the summer of 2015, while FANCY BEAR entered in April 2016.

The officials said the case against Russian intelligence is partly circumstantial, based on similarities with past hacking behavior by what security experts call "advanced persistent threats"--terminology used to describe nation-state hackers.

"They use hacking for political effect and to shape opinion," said James Lewis, an expert on nation-state hacking practices and director of the strategic technologies program at the Center for Strategic and International Studies. "So let's just say it fits their [modus operandi]."

Not everyone is convinced the case has been cracked.

Steven Bongardt, a former FBI official now at the firm Fidelis Cybersecurity, said WikiLeaks has a history of getting documents from inside leakers, not foreign hackers, and said the emails could be the work of someone trying to disguise their handiwork behind the Russian hackers.

"The timing could indicate a disgruntled insider," said Mr. Bongardt.

Washington Post
The anxiety for Democrats: Are more leaks to come?
Tuesday, 26 July 2016
Byline: Tom Hamburger, Ellen Nakashima

Washington - The FBI warned the Clinton campaign and dozens of lawmakers in recent months that they were being targeted by hackers, according to people familiar with the discussions.
There is no evidence that those hacks were successful. But the FBI's warning came weeks before The Washington Post reported that Russian hackers had twice broken into computers at the Democratic National Committee, underscoring concerns of national security experts that foreign adversaries might be trying to influence the presidential election.

Those fears burst onto the public stage this week as Democrats gathered in Philadelphia for their national convention in the wake of Friday's release of thousands of damaging emails on the website WikLeaks. The embarrassing emails spurred the resignation of the party chairwoman and marred a carefully orchestrated opening of the Democrats' convention.

Activists and campaign officials, anxious about what leaks may be yet to come, also worried about the alleged involvement of the Russian government, with campaign officials suggesting that the Kremlin was releasing the documents to damage Clinton's candidacy. National security experts, while cautious about leaping to premature conclusions, warned of the possibility of a significant escalation in an ongoing information war.

If the Russians were behind the leaks, said former CIA director Michael Hayden, "they're clearly taking their game to another level. It would be weaponizing information." He added: "You don't want a foreign power affecting your election. We have laws against that."

On Monday, the FBI formally acknowledged that it is looking into the DNC hack. The agency has been probing the matter for months and on Monday said publicly that it will "investigate and hold

accountable those who pose a threat in cyberspace." The FBI announcement followed the stunning allegation by the Clinton campaign Sunday that the Russian government was behind the release of damaging documents on the WikiLeaks website as part of a ploy to help Republican nominee Donald Trump.

Trump's campaign manager, Paul Manafort, called the suggestions "absurd" and suggested that Democrats were looking to shift attention away from damaging information about the party's conduct during the primary campaign.

On Monday, fallout from the hack also reverberated at the Kremlin, where a spokesman declined to comment on the hack except to refer reporters to comments by Trump's son, Don Jr., calling the allegations part of a pattern of "lie after lie."

"Mr. Trump Jr. has already strongly responded" to the Clinton campaign's claims, the Russian spokesman said, according to the news agency Tass.

The founder of WikiLeaks and its current top editor, Julian Assange, told the Democracy Now radio show Monday that he would not discuss the source of the data.

"In relation to sourcing, I can say some things. (A), we never reveal our sources, obviously. That's what we pride ourselves on. And we won't in this case, either. But no one knows who our source is." Assange has said the release Friday was the first in a series.

U.S. law enforcement and intelligence experts acknowledge they are taking the claim seriously but cautioned Monday that they have reached no conclusions.

The FBI is focusing on the Russian military intelligence agency, the GRU, and investigating whether it was responsible for passing the emails to WikiLeaks, according to individuals familiar with the investigation.

The GRU is one of two Russian spy agencies that apparently compromised the DNC's computer systems, according to CrowdStrike, a cyber-firm that investigated the breach this spring on behalf of the DNC.

The GRU, which broke into the DNC's computers in late April, also stole opposition research files on Trump, according to CrowdStrike.

Another Russian spy agency, the FSB, or an affiliate, had penetrated the DNC's computers last summer and was monitoring DNC email and chat traffic, CrowdStrike said.

The FBI is trying to determine with certainty whether Russian intelligence passed the emails to WikiLeaks.

That line of inquiry probably will involve intelligence agencies such as the National Security Agency and the CIA, which might be able to pick up intercepts or gather intelligence overseas, according to intelligence experts.

A big question looming over the investigation is what, if anything, should be done if it is shown that Russian intelligence is responsible for the leak.

The email releases continued to cause anxiety among Democratic officials as the party gathered for its convention in Philadelphia.

Most unnerving to activists here is the uncertainty over what may come next.

Former Senate majority leader Thomas A. Daschle (D-S.D.) told The Post that his email account was hacked recently, but he said he had no indication that the hack originated overseas or was a matter of concern to law enforcement.

Former White House chief of staff William M. Daley, attending the convention, called the Russian hack of DNC emails "pretty frightening."

Given Russia's sophistication in this realm, Daley said that it would be reasonable to conclude that President Vladimir Putin and his government are behind the email leak in an effort to undermine Hillary Clinton's candidacy.

"I don't think anybody would be surprised if Putin would try to affect the election," Daley said in an interview Monday. "That's like the old 'Casablanca' -- there's gambling in the casino. It doesn't surprise me at all. Period. I think anybody who dismisses that is living in fairy land here."

Steve Elmendorf, a lobbyist and former aide to House Democratic leader Richard A. Gephardt (Mo.), said the link to Russia was particularly concerning and yet not surprising given its concerted effort to infiltrate various arms of the U.S. government.

Washington lobbyist Tony Podesta said he expects hacks of private information in the digital age.

"I assume that all private information is public -- it's the safest way to live," he said.

John Cordisco, a former member of the Pennsylvania House of Representatives and the current chairman of the Bucks County Democratic Party with long-standing ties to Democratic donors across the state, said the consequence of the breach is that any personal information transmitted through the Internet could become compromised.

"Anyone would be worried," he said about the chilling effect on donations.

Podesta cautioned party officials to be more careful about how they communicate about donors, given the risk of exposure.

"Everything you say can and will be used against you," he said with a grin.

While federal agencies would not discuss their response in any detail, former government intelligence officials offered insight in to what is happening. Michael G. Vickers, who served as undersecretary of defense for intelligence from 2011 to 2015, said the approach would probably include three steps involving multiple federal agencies.

First, there would be an effort by the FBI, assisted by other intelligence agencies, to nail down "attribution," the identity of the hackers, by looking for telltale bits of identifying code that are left when such breaches occur. Second, he said, there would be discussion among interagency experts "about the intelligence, the timing of the attack, and the release of the information." Was information collected just to gain intelligence, to influence policy or politics, or as a "destructive act"? Third, he said, there would careful deliberations about how to respond.

Vickers was at the Defense Department in 2014 when the most recent destructive cyberattack occurred, one against Sony Pictures apparently initiated by North Korea. Responses could range from a diplomatic wrist slap or warning to countermeasures. Of course, the federal investigators first need to determine that the hack was indeed conducted by the Russians.

In the case of Sony, the administration imposed economic sanctions on North Korea in response to the attack. Later, President Obama signed an executive order establishing a program that enables officials to impose economic sanctions specifically in response to significant cyber-incidents. That tool has not yet been used.

Yahoo News
Suspected Russian hack of DNC widens -- includes personal email of staffer researching Manafort
Tuesday, 26 July 2016
Byline: Michael Isikoff

Washington - Just weeks after she started preparing opposition research files on Donald Trump's campaign chairman Paul Manafort last spring, Democratic National Committee consultant Alexandra Chalupa got an alarming message when she logged into her personal Yahoo email account. "Important action required," read a pop-up box from a Yahoo security team that is informally known as "the Paranoids." "We strongly suspect that your account has been the target of state-sponsored actors."

Chalupa -- who had been drafting memos and writing emails about Manafort's connection to pro-Russian political leaders in Ukraine -- quickly alerted top DNC officials. "Since I started digging into

Manafort, these messages have been a daily oc----currence on my Yahoo account despite changing my p--a-ssword often," she wrote in a May 3 email to Luis Miranda, the DNC's communications director, which included an attached screengrab of the image of the Yahoo security warning.

"I was freaked out," Chalupa, who serves as director of "ethnic engagement" for the DNC, told Yahoo News in an interview, noting that she had been in close touch with sources in Kiev, Ukraine, including a number of investigative journalists, who had been providing her with information about Manafort's political and business dealings in that country and Russia.

"This is really scary," she said.

Chalupa's message is among nearly 20,000 hacked internal DNC emails that were posted over the weekend by WikiLeaks as the Democratic Party gathered for its national convention in Philadelphia. Those emails have already provoked a convulsion in Democratic Party ranks, leading to the resignation of DNC Chair Debbie Wasserman Schultz in the wake of posted messages in which she and other top DNC officials privately derided Bernie Sanders and plotted to undercut his insurgent campaign against Hillary Clinton.

But Chalupa's message, which had not been previously reported, stands out: It is the first indication that the reach of the hackers who penetrated the DNC has extended beyond the official email accounts of committee officials to include their private email and potentially the content on their smartphones. After Chalupa sent the email to Miranda (which mentions that she had invited this reporter to a meeting with Ukrainian journalists in Washington), it triggered high-level concerns within the DNC, given the sensitive nature of her work. "That's when we knew it was the Russians," said a Democratic Party source who has knowledge of the internal probe into the hacked emails. In order to stem the damage, the source said, "we told her to stop her research."

A Yahoo spokesman said the pop-up warning to Chalupa "appears to be one of our notifications" and said it was consistent with a new policy announced by Yahoo on its Tumblr page last December to notify customers when it has strong evidence of "state sponsored" cyberattacks. "Rest assured we only send these notifications of suspected attacks by state-sponsored actors when we have a high degree of confidence," wrote Bob Lord, the company's Chief Information Security Officer, in the Tumblr post.

Asked about charges by Clinton campaign manager Robby Mook that "Russian state actors" hacked the DNC in order to help Trump, who has made sympathetic comments about Russian President Vladimir Putin, Manafort on Sunday dismissed the charges in multiple television interviews as "absurd" and "crazy." The claims are "pure obfuscation on the part of the Clinton campaign," Manafort said on ABCs "This Week." "What they don't want to talk about is what's in those emails."

In mid-June, Democratic Party suspicions about the hackers seemed to be confirmed when CrowdStrike, an outside security firm retained by the DNC, reported that it traced the hackers to two separate units linked to Russia's security services: the FSB, Russia's equivalent of the FBI, and GRU, the country's

military intelligence agency. The company noted strong similarities between the attack on the DNC by the suspected GRU hackers and previous cyberintrusions of unclassified systems at the White House, the State Department and the offices of the Joint Chiefs of Staff. (After discovering the data breach, a DNC security source said its cyberexperts noted that the hackers' exfiltration of files took place "9 to 5, Moscow time.") An FBI official confirmed that the bureau has been investigating the breach for some time, and, according to one source familiar with the matter, Director James Comey has been personally briefed.

The extent of the damage was at first unclear. When they first authorized a public release of the CrowdStrike analysis, party officials said that the hackers had targeted oppo files on Donald Trump. But they told reporters that no personal information about donors had been penetrated. Party officials are no longer standing by those assurances. Two sources familiar with the breach said that the hackers' reach was far more widespread than initially thought and includes personal data about big party contributors and internal "vetting" evaluations that include embarrassing comments about their business dealings (as well as gossipy internal emails about the private affairs of DNC staffers). One newly posted email discusses a prospective DNC donor's offering to host a fundraiser with President Obama, noting that he had previously been convicted in a case involving allegations that he killed 50 horses, as part of an insurance fraud scheme. Party officials are bracing for more damaging document dumps after Labor Day. "They're having to do serious damage control with the donors right now," said a party official familiar with the matter.

There are also signs that the hackers have penetrated the personal email of some Clinton campaign staffers -- at least those who were in communication with senior DNC staff members. On May 6, John McCarthy, a DNC consultant who has since joined the Clinton campaign to do outreach to religious groups, sent an email to Chalupa from his personal Gmail account that was then forwarded to other party officials. McCarthy proposed arranging for religious leaders who have "condemned Trump for bringing out the worst in America" to stage a protest at the Republican National Convention. "It would be great to try and engage them and get them to do something at convention, etc. Maybe do a vigil at the Cleveland convention?" McCarthy wrote in the email, which included his personal cellphone number and which has now been posted as part of the WikiLeaks data dump.

There is still much that is not known about the DNC hack and how, if the Russians are indeed behind it, the emails found their way to WikiLeaks. Some commentators have noted that WikiLeaks founder Julian Assange has in the past hosted a talk show on RT, the Russian television network that serves as a propaganda arm for the Kremlin. (Assange, without providing specifics, recently claimed he will be posting more emails that will be damaging to Clinton and "provide enough evidence" to get her arrested.)

There are also signs that the Obama administration is taking the matter more seriously. The Washington Post reported Monday that White House officials convened a high-level security meeting last Thursday, hours before WikiLeaks began posting the emails, to review information about the DNC attack. Party officials are privately pushing the White House to publicly blame the Russians in the same way it blamed

North Korea for the cyberattack on Sony and China for intrusions into U.S. companies. "The last time somebody broke into the DNC, it led to the resignation of a president," said the Democratic Party security source, referring to the Watergate scandal. In some ways, the source insisted, the current cyberheist -- what some in party circles are already calling a "21st century Watergate" -- is even more sinister, the source said. "This is the Russians screwing with the integrity of our election process."

Wall Street Journal
White House to Issue New Policy for Cyberattack Responses
Tuesday, 26 July 2016
Byline: Damian Paletta

Washington - The White House as soon as Tuesday is expected to issue a new directive on how the government should respond to significant cyberattacks, two people familiar with the matter said, aiming to end confusion about the responsibilities of agencies involved in security breaches.
The new presidential policy directive is a response to the rapid escalation of cyberattacks by criminals and foreign governments that have stolen information from U.S. companies, citizens and government offices.

The policy has been in the works for months, but it will be released at a time when there is an acute focus on the damage caused by cyberattacks. Hackers last year broke into the Democratic National Committee's network and WikiLeaks began releasing some internal party emails several days ago. Some of the emails humiliated top DNC officials and led to an uproar at the party's convention in Philadelphia and the resignation of DNC chairwoman Debbie Wasserman Schultz.

A White House spokesman declined to comment.

The directive is expected to focus in part on how the government will coordinate its response to significant cyberattacks, the people familiar with the matter said.

Lawmakers and U.S. officials have said the government should clarify how it responds to cyberattacks following large-scale breaches at major U.S. companies, the State Department, the U.S. Office of Personnel Management, and even parts of the Pentagon. Hackers try and steal information for commercial reasons but also as a form of espionage, and the U.S. response to these incidents has varied.

There are numerous agencies that play a role in designing cybersecurity safeguards and responding to individual incidents.

The Federal Bureau of Investigation probes the hacks. The Department of Homeland Security is supposed to help protect civilian agencies and serve as a conduit between the government and business community. The National Security Agency has forensic tools that can determine who is behind certain breaches.

The Commerce Department plays a role in monitoring the development and sale of cyber weapons. U.S. Cyber Command has teams focused on offensive and defensive cyber tools. And a number of other agencies work with companies from a range of sectors, including banking and energy, to push them to have strong defenses.

The plethora of agencies involved in cybersecurity has led some companies to wonder who is in charge and who they should turn to when there is an attack.

NBC News
Why Experts Are Sure Russia Hacked the DNC Emails
Tuesday, 26 July 2016
Byline: Josh Meyer

New York - Many U.S. officials and cyber security experts in and out of government are convinced that state-sponsored Russian hackers are the ones who stole 20,000 emails from the Democratic National Committee and leaked them to the public just in time to disrupt the Democrats' national convention in Philadelphia.
Here's why the experts are so confident the Russians did it:

* GEOGRAPHY: At least one of the hacker groups attacking the DNC appeared to cease operations on Russian holidays, and its work hours aligned with a Russian time zone, cybersecurity company FireEye concluded in a report.

* LANGUAGE: The hackers also left an obvious digital fingerprint, one cybersecurity expert said, perhaps on purpose: a signature in Russia's Cyrillic alphabet.

* FORENSIC EVIDENCE: After a different batch of hacked Democratic emails was released last month, a wide spectrum of cyber-security experts concluded that it was the work of Russian intelligence agencies through previously known proxy groups known as COZY BEAR or APT 29, and FANCY BEAR or APT 28. "We've had lots of experience with both of these actors ... and know them well," according to the DNC's own contract cybersecurity firm, Crowdstrike, which blogged that one of the two groups had already gained illegal access to the White House, State Department and even the military's Joint Chiefs of Staff.

* MOTIVE: Given their mutual and very public bromance, Putin would much prefer a Trump presidency to a Clinton one and the timing suggests the leak was timed for maximum embarrassment to the Democrats and their presumptive nominee. Clinton campaign manager Robby Mook said the campaign was told by cyber experts that Russian hackers stole and released the emails to help Trump. "I don't think it's coincidental that these emails were released on the eve of our convention here," said Mook, "and I think that's disturbing."

* HISTORY: U.S. intelligence officials, including Director of National Intelligence James Clapper, said they had previously seen evidence of foreign hackers spying on U.S. presidential candidates, including some state-sponsored ones, and that such cyber-intrusions would become even more commonplace.

The main reason, however, is that the email hack is exactly the kind of thing Russian hackers can do, are supposed to do, and are used for by Putin and his aides, retired four-star Adm. James Stavridis told NBC News.

"It is certainly well known that the Kremlin uses Russian hackers for a variety of missions," said Stavridis, who led NATO from 2009 to 2013. "It is certainly well known that Russia possesses those kinds of capabilities. And it certainly seems sensible to assume that the Russians would rather have a Trump than a Clinton presidency."

"And as the saying goes, crime is so often where motive meets opportunity. And when you put those two elements together, I'd say it's a real possibility."

Like other cyber-experts, however, Stavridis said definitively proving such connections is virtually impossible. "I don't know the answer to that and I'm not sure anyone knows the answer to that except for a few individuals in the Kremlin."

(Stavridis, who now heads Tufts' University's Fletcher School of International Affairs, was mentioned as a possible Clinton running mate, but says he is a registered Independent.)

On Monday, Crowdstrike co-founder and CTO Dmitri Alperovitch declined to comment on the latest release of hacked emails and whether it confirmed his earlier assessment that the Russians were responsible.

"At this time, I don't have any new insights or commentary to share beyond the facts that I presented [earlier]," he told NBC News.

Trump campaign chairman Paul Manafort dismissed allegations of Russian complicity in the leak of DNC emails Monday, as the FBI announced that it is investigating what it called "a cyber intrusion involving the DNC and are working to determine the nature and scope of the matter."

"A compromise of this nature is something we take very seriously," said the FBI in a statement, "and the FBI will continue to investigate and hold accountable those who pose a threat in cyberspace."

Strait Times
Digital media the new frontier in war against terror
Tuesday, 26 July 2016
Byline: Farik Zolkepli

Putrajaya - Digital media is the new frontier in which the war against terrorism must be fought on, said Datuk Seri Najib Tun Razak. "It is the new battleground and its centrality cannot be overestimated. "We must seize the opportunity to convince the world that Muslims have nothing to do with the ideology of hatred and destruction," the prime minister said at the launch of the 36th Asean Chiefs of Police (Aseanapol) Conference on Tuesday.

Najib said Malaysia has initiated the Regional Digital Counter-Messaging Communications Centre to synchronise efforts to fight terrorism in Asean and beyond.

"It is vital that this centre uses the studies that illustrate why there is nothing "Islamic" about the state that shamefully declares itself as such.

"It is also vital that all authorities ensure that the message, which the centre puts out is solid, persuasive and real," he said.

Najib hoped that the conference would serve as useful platform for the sharing of expertise and exprience in all aspects of security.

New York Times
F.B.I. Examining if Hackers Gained Access to Clinton Aides' Emails
Tuesday, 26 July 2016
Byline: David E. Sanger

Washington - The F.B.I. investigation into the suspected state- sponsored Russian theft of emails and documents from the Democratic National Committee's computer networks has expanded to determine if aides and organizations considered close to Hillary Clinton were also attacked, according to federal officials involved in the investigation.
But so far, a sampling of senior Clinton aides at the Democratic National Convention in Philadelphia found none who said they had been notified by the F.B.I. or private investigators that their private emails had been compromised. At this point, law enforcement officials say, there is evidence only of attempts to gain access to those associates through "spear-phishing" attacks, often crude efforts to get someone to click on an email that releases malware into the computer.

The committee has said that Russia hacked into its computers and has been supported in its assertion by several private cybersecurity firms, including Crowdstrike, the company that investigated the committee's breach.

Two years ago, several Clinton aides who had worked at the State Department were notified that their accounts there had been broken into by one of the same Russian intelligence agencies, the Federal

Security Service, or F.S.B., suspected of getting into the committee's system. That hacking, which went largely undetected while Mrs. Clinton was secretary of state in President Obama's first term, gave the Russian intelligence services what one diplomat termed a road map of Mrs. Clinton's associates and frequent email partners.

Mrs. Clinton's private server while she was secretary of state, in Chappaqua, N.Y., would have been another obvious target. But last month the F.B.I. director, James B. Comey, said there was no "direct evidence" that Russia or any other power had "successfully hacked" into Mrs. Clinton's server. Still, he said, there was evidence that intruders had tried, and when Mr. Comey said any successful intruders were probably far too skilled to leave evidence of their intrusion behind, law enforcement officials said, he had the Russians in mind.

For years American intelligence agencies and the F.B.I. have tracked the operations here of two of the most sophisticated state-run hacking groups in the world, the G.R.U., Russia's military intelligence agency, and the F.S.B., the state security service and successor, twice removed, of the K.G.B. of the Soviet era.

The activities of the two groups in the United States and around the world have been tracked for so many decades that their successes and misadventures are the subject of movies and lore in both the United States and Russia. But since they turned to hacking techniques and sometimes cyberweaponry, the Obama administration has rarely protested in public about the group's boldest information-warfare attacks, in part to avoid retaliation.

The administration decided not to publicly identify the Russians as the power behind State Department, White House and Joint Chiefs of Staff intrusions. James R. Clapper Jr., the director of national intelligence, told Congress that the United States would not name or shame any country engaged in ordinary espionage -- of the kind the United States also does -- but should focus instead on setting norms against the theft of intellectual property and destructive attacks. For that reason, Mr. Obama has focused on agreements with China to protect corporate secrets.

Now some administration officials think they may have misunderstood Russia's intentions. After the public release of the emails and documents that brought down the chairwoman of the Democratic Party, Debbie Wasserman Schultz, and the threat by WikiLeaks to release more documents from this and other hacks, administration officials say they are in a strange new world in which Russia may be using the products of espionage to influence an American election.

Some outsiders agree. "There is nothing new in one nation's intelligence services using stealthy techniques to influence an election in another," Jack Goldsmith, a professor at Harvard Law School, wrote on the Lawfare blog on Monday. He noted that the United States had engaged in covert actions to influence elections in Indonesia, Italy, Chile and Poland during the Cold War.

But he added that "doing so by hacking into a political party's computers and releasing their emails does seem somewhat new." It could foretell an era of data manipulation, in which outsiders could tinker with votes, or voter data, or "lose" electronic ballots.

Federal officials say their investigation has been underway since the spring, when the committee notified the F.B.I. of the intrusion. The committee's suspicions were triggered by what appeared to be a relatively clumsy attack by the G.R.U. In the course of investigating that attack, the F.B.I. discovered an earlier, more sophisticated attack on the committee by the F.S.B., which is often in competition with the G.R.U.

But investigators say the committee was reluctant to cooperate deeply in the federal investigation, relying instead -- as many companies do -- on private investigators that they hired. The committee brought in Crowdstrike, which reported publicly in June that it had evidence that the hack began last summer.

Julian Assange, who founded WikiLeaks, argued to Richard Engel of NBC in an interview broadcast Monday that "there is no proof of that whatsoever" that Russia was behind the original hacking. "We have not disclosed our source, and of course, this is a diversion that's being pushed by the Hillary Clinton campaign."

Mr. Assange also said another round of emails to be released would provide "enough evidence" to indict her, but her campaign manager, Robby Mook, said, "He says a lot of things, so I'm not, I'm not going to pay attention to that."

Many cybersecurity firms that have examined the evidence released by Crowdstrike say Russia appears to be the source. Thomas Rid, a cyberexpert and author of "Rise of the Machines," noted in an article published on Vice's website that the intruders made several mistakes: "One leaked document included hyperlink error messages in Cyrillic," because the documents had been edited with Russian language settings, and other "metadata" was consistent with "identical fingerprints" found in attacks on the German Parliament. The Germans named one of Russia's intelligence agencies as the attacker in that case.

NBC News
WikiLeaks' Julian Assange: 'No Proof' Hacked DNC Emails Came From Russia
Tuesday, 26 July 2016
Byline: Alex Johnson

New York - WikiLeaks founder Julian Assange told NBC News on Monday that "there is no proof whatsoever" that his organization got almost 20,000 hacked Democratic National Committee emails from Russian intelligence -- adding it's what's in the emails that's important, not who hacked them.

In a Skype interview with Richard Engel for "NBC Nightly News," Assange rejected that it hadn't even been proven that it was WikiLeaks that published some email messages that have been analyzed in outlets like The New York Times.

Information in some DNC email messages led to the ouster of DNC Chairwoman Debbie Wasserman Schultz.

Three cybersecurity experts have told NBC News that the DNC's servers were hacked by Russian intelligence. But Assange said Monday that DNC servers have been riddled with security holes for years and that many sets of documents from multiple sources are now in public hands.

"The emails that we have released are different sets of documents to the documents of those [that] people have analyzed," he said.

"I have seen Hillary Clinton apologists talk -- or some experts talk -- about other material, and not the material that we have released," Assange said.

In any event, the provenance of the documents is irrelevant, Assange contended. What commentators should be focusing on is what the documents say about Clinton, Bernie Sanders and the Democratic Party.

"The real story is what these emails contain, and they show collusion at the very top of the Democratic Party" to derail Sanders' campaign, he said.

Would Hillary Clinton have won anyway?" Assange asked. "Maybe, maybe not. I think that it's completely up in the air now, and so the result of the nomination process has no political legitimacy."

Assange remains in exile in the Ecuadorian Embassy in London to avoid prosecution on sexual assault charges in Sweden. He denies the charges.

Politico
Edward Snowden weighs in on DNC leak
Monday, 25 July 2016
Byline: Caroline Kelly

Washington - Edward Snowden knows a thing or two about leaks.
The former CIA employee and government contractor weighed in on WikiLeaks' publication of thousands of emails by Democratic National Committee staffers, calling for greater transparency of government intelligence capabilities.

"To summarize: the US Intel Community should modernize their position on disclosure. Defensive capabilities should be aggressively public," he tweeted as one of a seven-tweet series earlier Monday morning.

Snowden, who now lives in asylum in Russia -- which has been widely accused of hacking the DNC's servers -- said more disclosure could give the U.S. government a greater ability to attribute blame for the DNC hack.

"If Russia hacked the #DNC, they should be condemned for it," Snowden tweeted, citing the way the FBI presented its findings related to the Sony hack in November 2014, which the agency attributed to North Korea. "Evidence that could publicly attribute responsibility for the DNC hack certainly exists at #NSA, but DNI traditionally objects to sharing," he later added.

The widespread knowledge of the formerly secret NSA data analysis program XKeyscore, which Snowed revealed in 2013, "makes following exfiltrated data easy. I did this personally against Chinese ops," he tweeted. Snowden criticized the NSA's penchant for secrecy, adding, "The aversion to sharing #NSA evidence is fear of revealing 'sources and methods' of intel collection, but #XKEYSCORE is now publicly known."

Snowden argued that publicizing the consequences of insidious data hacking clear is the best national defense. "Without a credible threat that USG can and will use #NSA capabilities to publicly attribute responsibility, such hacks will become common," he tweeted, adding, "This is the only case in which mass surveillance has actually proven effective. Though I oppose in principle, it is a mistake to ignore."

Yahoo News
Machines v. hackers: Cybersecurity's artificial intelligence future
Monday, 25 July 2016
Byline: Paul F. Roberts

New York - It's a common refrain after any recent high-profile breach into federal computers and corporate networks: There aren't enough skilled cybersecurity professionals to outwit criminal hackers. That message from officials, executives, and industry experts isn't just grousing, either. According to industry estimates, the US needs about 200,000 more workers to fill current cybersecurity roles. Globally, the gap is five times higher - an estimated 1 million workers.

The issue has become such a priority that President Obama made increasing the number of cybersecurity workers a key component of his multibillion-dollar Cybersecurity National Action Plan, which was introduced earlier this year. The White House said earlier this month it plans on boosting the federal cybersecurity workforce by 3,500 new hires by year's end.

But as businesses compete for scarce cybersecurity talent and policymakers weigh remedies for the digital security worker shortage, the ground underneath the profession is shifting.

Now, computers equipped with sophisticated learning algorithms are performing jobs that until recently required highly trained humans. Over time, experts say, the complexity of cybersecurity jobs performed by machines will increase, further reducing the demand for workers and changing the entire nature of cybersecurity work.

"If we fast forward ... I think we will see a diminished role for humans," says Amir Husain, an authority on artificial intelligence and chief executive officer of SparkCognition, a startup focused artificial intelligence.

In fact, Mr. Husain and others note, the use of artificial intelligence to do information security work is already happening. For example, antivirus companies have long relied on algorithms - not humans - to determine whether a given file is malicious or not, based on patterns identified in previous malicious files.

"Except in very rare cases, where you have an unknown threat, humans are not doing file analysis," he says.

Much of the investment that's going into the cybersecurity space to fuel the development of automation is directed at responding to cybersecurity incidents. Currently, humans are the ones who figure out how to respond to cyberattacks on networks, working to quickly block suspicious communications and analyze malicious behavior and software. But computers could perform the same functions -- and do it much more quickly than people behind the keyboard.

But computers could perform the same functions -- and do it much more quickly than people behind the keyboard.

In fact, the allure of machines quickly fixing vulnerabilities has led the Defense Advanced Research Projects Agency (DARPA), the Defense Department's technology lab, to organize the first-ever hacking competition that pits automated supercomputers against each other at next month's Black Hat cybersecurity conference in Las Vegas.

With the contest, DARPA is aiming to find new ways to quickly identify and eliminate software flaws that can be exploited by hackers, says DARPA program manager Mike Walker.

"We want to build autonomous systems that can arrive at their own insights, do their own analysis, make their own risk equity decisions of when to patch and how to manage that process," said Walker.

Technology firms large and small are already moving toward that goal. In May, IBM announced plans to train a new, cloud-based version of its Watson cognitive technology to detect cyberattacks and

computer crimes. As part of its training, IBM fed Watson a dictionary of information security-specific terms such as "exploit" and "dropper" and programmed it how to identify and respond to cybersecurity incidents.

Of course, cybersecurity isn't the only work that will be affected by artificial intelligence and automation. A recent analysis by the consulting firm McKinsey concluded that automation will "affect portions of almost all jobs to a greater or lesser degree, depending on the type of work they entail."

That study analyzed more 2,000 work activities across 800 different occupations and concluded that automation of work is already going beyond routine manufacturing activities and has the potential to transform sectors that "involve a substantial share of knowledge work."

The Register (UK)
Alleged hacker Lauri Love will learn his fate in September, says judge
Monday, 25 July 2016
Byline: Alexandr J. Martin

London - Lauri Love will not find out whether he will be extradited to the US until September, District Judge Nina Tempia said today at Westminster Magistrates' Court.
Judge Tempia will hand down her judgment on the US authorities' attempt to have Love handed to them for trial on Friday 16 September at 2pm.

There were more than 20 extradition hearings taking place in Westminster Magistrates' Court today, including that of Love. The 31-year-old is being sought on three indictments alleging he "carried out a series of cyber attacks against the websites and computer systems" of the US government, military, and private sector.

The allegations against Love concern his alleged activities during #OpLastResort, a series of online protests which followed the suicide of Aaron Swartz. Swartz was perceived to have been persecuted by the US government after being accused of hacking into academic library JSTOR.

If extradited and found guilty in the US, Love faces a maximum of 99 years' imprisonment.

Both the defence and prosecution delivered their final arguments this morning, in Court One of Westminster Magistrates' Court.

Love's lawyer, Ben Cooper, again argued that his client's extradition should be refused under the "forum bar" of section 83A of the Extradition Act 2003. This bar was introduced following the then-Home Secretary (and now Prime Minister) Theresa May blocking the extradition of Gary McKinnon to the United States because of the increased risk of suicide this posed to him.

It is a key part of Love's defence that he would be at risk of suicide if extradited. Professor Simon Baron-Cohen, director of the University of Cambridge's Autism Research Centre, said, in his view, "there is absolutely no question that [Love] has Asperger's [Syndrome]" as well as severe depression and aggressive anxiety-related eczema, and was at a "very high" risk of committing suicide if imprisoned within the US system.

Speaking to The Register, Nicole Powers of the Courage Foundation, an international group that supports "those who risk life or liberty to make significant contributions to the historical record" stated that the case is the first major test of the forum bar: "We're seeing if this law has teeth or whether it just paid lip-service to the outcry following the McKinnon case."

Peter Caldwell was the Crown Prosecution Service's barrister - the CPS represents requesting states in all extradition cases - and he argued that Love's threat to commit suicide was an attempt to spite the court. He recommended to Judge Tempia that she separate whatever influenced the Home Secretary to refuse Gary McKinnon's extradition from Love's case.

Appearing for Love, Cooper described Caldwell's efforts to downplay Love's health issues and suicide risk as "disgusting", noting that the defence had provided much evidence, including expert witness testimony, of Love's history of mental illness. He referenced the inadequacies of not just mental healthcare but healthcare in US prisons in general.

Love had a long history of mental illness, the court was told, including losing all of his hair when he was 15. He had been prescribed antidepressants on several occasions and referred to psychiatrists several times, said Cooper, and it was "impossible to predict the severity" of his reaction to extradition. At an earlier hearing, Love's father, the Reverend Alexander Love, a prison chaplain, had testified that he feared and believed his son would commit suicide if extradited to the US.

The prosecution said that Love was the source for much of the history of his mental health problems and that little existed, including his diagnosis of Asperger's Syndrome, before the extradition case had been opened.

Three separate indictments have been filed against Love, in New Jersey (PDF), the Eastern District of Virginia (PDF), and the Southern District of New York (PDF). While in England the allegations against Love would be prosecuted before a single court on a single indictment, in the US the three indictments require three separate court hearings.

Cooper argued that single venue and single prosecution in the UK would be preferable to the three prosecutions in the United States. It would be "more efficient... speedier... and enables the mental health considerations to be given full account," argued Cooper, who stated: "There's no good reason why an English prosecution would do anything to let down the complainants in this case."

The prosecution disagreed, stating that while much of the evidence was portable, "you may well find that certain details of the case may be readily available, but not all."

One issue regarded an informant witness whom it was known was prepared to assist the US in their prosecution, but it was not known whether they would be willing to help the UK. "There is no guarantee that the witness evidence would be available in the UK for a domestic prosecution," argued Caldwell, on behalf of the US authorities.

Cooper had noted the ease of transferring both digital evidence and witness evidence in the prosecution of Mustafa Al- Bassam and Ryan Ackroyd, who were members of the Lulzsec hacking crew. In the domestic prosecution of the UK-based members of Lulzsec, an informant witness, Hector Xavier Monsegur (AKA Sabu), the de facto leader of the group, had provided evidence.

Prosecution in the UK would be in the interest of the victims, argued Cooper, as the mental health factors affecting Love may compromise the prosecutions in the US, preventing the victims from accessing justice.

In the US Love would "surely be denied bail, as anyone who is extradited doesn't meet the criteria for bail as they have no ties to the country. As a matter of course he will be placed in jail and be unable to participate in his own defence, as well as being separated from his parents and support system," the Courage Foundation's Powers told The Register.

Once Judge Tempia hands down her eventual judgment, whichever side loses is very likely to appeal, thus sending the case to the High Court.

The Hindu
U.S., India may sign logistics pact
Tuesday, 26 July 2016
Byline: Special Correspondent

New Delhi - Taking forward the India-U.S. defence dialogue, senior U.S. defence officials are visiting India on Tuesday during which the logistics pact, the text for which has already been finalised, is in focus in addition to high technology cooperation.
U.S. Under Secretary of Defence for Acquisition, Technology & Logistics Frank Kendall will be in India on a three-day visit beginning on Tuesday, officials told The Hindu. While the focus will be on the evolving high technology and co-development projects under the Defence Technology and Trade Initiative (DTTI), the Logistics Exchange Memorandum of Understanding (LEMOA), a logistics agreement facilitating the exchange of fuel and supplies at each other's facilities, could be signed.

"The text has already been agreed. Signing it is just a formality," a senior official observed without specifically commenting on the status.

LEMOA is one of the three foundational agreements along with the Communications Interoperability and Security Memorandum of Agreement (CISMOA) and Basic Exchange and Cooperation Agreement for Geo-spatial Cooperation (BECA) which the U.S. has been pushing India to sign to further deepen defence and strategic cooperation.

Both sides have been negotiating the LEMOA and during U.S. Defence Secretary Ashton Carter's visit to India in April both sides announced in-principle agreement to conclude the pact. During Prime Minister Narendra Modi's visit to the U.S. last month the two leaders announced that the text of the agreement has been finalised.

The two sides have informally begun talks on the other two agreements and of them India has expressed particular reservations on BECA, informed sources said.

In addition the new projects agreed under DTTI along with cooperation in jet engine and aircraft carrier would be reviewed.

Sputnik (Russia)
Snowden Posts Document Alleging US Policy to Hack Foreign Political Parties
Monday, 25 July 2016

Washington - The US intelligence community allegedly authorized the hacking of foreign political parties, according to a 2010 national security document posted by whistleblower and former National Security Agency contractor Edward Snowden on Monday.
The document, originating from the Director of National Intelligence and dated July 16, 2010, purported to identify "foreign-based political organizations" allegedly targeted by US intelligence.

"Our government specifically authorized the hacking of political parties. Mistakes were made," Snowden said in a Twitter message.

Among them were Egypt's Muslim Brotherhood and National Salvation Front, the Pakistan Peoples Party, the Lebanese Amal group and the Indian Bharatiya Janata Party.

The document was released in the midst of a significant hack of the Democratic National Committee (DNC), in which dozens of emails were publicly released showing DNC efforts to obstruct candidate Bernie Sanders's presidential campaign to increase rival Hillary Clinton's chances to become the Democratic party's presidential candidate.

DNC and other US sources have claimed Russian responsibility for the hack.

In 2013, Snowden leaked a cache of intelligence documents revealing widespread US surveillance practices at home and abroad. Snowden is currently living in exile in Russia, and faces charges of espionage and theft of government property in the United States.

Gulf News
Kuwait starts applying new electronic media law
Tuesday, 26 July 2016
Byline: Staff Report

Kuwait - Kuwaiti Ministry of Information started the implementation of law No. 8/2016 to regulate electronic media, which was approved and published in the Official Gazette on Sunday. The new law is to regulate all web-based publications, including electronic news services, bulletins, websites of newspapers and televisions and the likes. Under the legislation, all these services must obtain a license from the government before they can operate.
The first article in the Electronic Media tackled the activity that includes publishing or broadcasting items and forms of a media service of electronic content that is produced, developed, upgraded, dealt with, broadcast, published or reached through the internet or any other communications network, Kuna reported on Monday.

The electronic media is considered one of the components of the information system in the country, and the freedom of its use is guaranteed for all according to the rules of this law, and there is no prior censorship on what is circulated of content via electronic sites and facilities.

The executive regulations of this law shall control polls carried out by licensed websites and electronic media facilities.

Kuwaiti Minister of Information and Minister of State for Youth Affairs Shaikh Salman Sabah Al Sabah asserted that Kuwait was among the first countries that have legislated a comprehensive electronic media law.

In a press statement during a tour to the electronic publishing department at the ministry, he said that the law will regulate electronic publishing, websites, blogs and social media in Kuwait He called on all electronic media outlets to abide by law 8/2016 as to contribute to the growth of the media sector. Moreover, the ministry called on all electronic media outlets to abide by law 8/2016, as contributors to the growth of the media sector.

The ministry also underscored how helpful these media outlets can be to staving off extremist ideologies, while espousing various virtues for the betterment of the nation. The law works to promote freedom of expression while ensuring unhindered access to information. It also aims to eliminate all impediments to the spread of information on electronic media outlets in a way that would conserve national values and interests.

The National (UAE)
Facebook and UK police fail to act on Islamophobic hate abuse online
Tuesday, 26 July 2016
Byline: Jonathan Gornall

London- Islamophobia on Facebook has been "much more prevalent than previously thought" and is "being used by groups and individuals to inflame religious and racial hate", according to research carried out by the UK's Birmingham City University.
With under-resourced police forces overwhelmed by the scale of the problem and social media companies ineffective at policing their platforms, Muslims should not ignore abuse but report it at every opportunity, says the author of a paper published on Monday in the International Journal of Cyber Criminology.

A nearly two- year study of 100 Facebook pages carried out between 2013 and 2014 revealed 494 instances of Islamophobic abuse. Many were posted under the umbrella of known far-right UK-based organisations such as the English Defence League and Britain First and clearly breached British anti-hate laws, yet escaped both censure by Facebook and prosecution by the police.

According to the paper, Islamophobia on Social Media: A Qualitative Analysis of Facebook's Walls of Hate, Muslim women in particular were targeted for abuse, singled out on 76 occasions in writing and in illustrations as a security threat because of the way they dressed.

Accusing Muslim women of being a security threat was one of five main themes of anti-Islamic abuse identified by Imran Awan, an associate professor in criminology at Birmingham. The other themes were saying that Muslims should be deported, that they were terrorists or rapists and that there was a war between "them and us".

Dr Awan accused Facebook of a "laissez-faire" attitude to anti-Islamic abuse and called on it to strengthen its community standards, which he dismissed as ineffectual and weak.

Although he recognised the police were under- resourced, he said high-profile prosecutions should be pursued and lengthy sentences imposed by the courts to "make an example" of offenders and discourage others.

It was, he told The National, also "a real worry and a shame that the number of people reporting these offences is really low ... people need to bombard Facebook with complaints when this sort of thing happens, so the company will be much more in tune with what's happening on its platform".

Many of the examples of abuse quoted in the paper are too offensive to repeat in print. One typical highly abusive post, published by the so-called "English Defence League Sikh Division", was entitled

"How Muslim scum celebrate Eid" and reported a supposedly true story about drink- driving involving Muslim youths from Pakistan.

With 93 "likes", the post attracted many hateful comments, including calls for the alleged culprits to be given lethal injections and the branding of all Muslims as "scum".

Dr Awan, who in 2014 addressed a conference in Abu Dhabi designed to promote peaceful coexistence in Muslim societies, is highly critical of Facebook's community standards, which he says leave plenty of scope for hate masquerading as humour.

According to the standards, "content that attacks people based on their actual or perceived race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability or disease is not allowed". However, Facebook does allow "clear attempts at humour or satire that might otherwise be considered a possible threat or attack. This includes content that many people may find to be in bad taste".

Images purporting to use humour are frequently used to spread anti-Islamic messages on Facebook. One example highlighted by the report shows two identical Qurans pictured side-by-side and captioned "Islams [sic] Quran" and "ISIS Quran", with the heading "Spot the difference?".

Another post, on the Facebook page of the group Britain First, which describes itself as "a patriotic political party", posed the seemingly innocuous question "What's a typical British breakfast?" but was clearly intended "to stoke up animosity without being so explicit that it would be obviously illegal", said Dr Awan. The quotes underneath the post - including "For breakfast it would be good to chop a Muslim's head off" - made clear its intent.

The study was carried out between January 2013 and November 2014 and Dr Awan fears that subsequent global events, including the migrant crisis and various terrorist attacks in European countries, will have provoked only more prejudice against Muslims on Facebook, which in turn will generate more hostility in the offline world. This, he says, makes it "all the more important that Facebook and the authorities respond robustly to the problem".

His fears appeared to be confirmed last month by the UK organisation Measuring Anti- Muslim Attacks which reported that incidents of anti-Islamic hate in the UK had increased by more than 300 per cent in 2015.

Last month Britain's National Police Chiefs' Council also reported that there had been a 57 per cent increase in reported hate crimes in the four days following the UK's referendum vote to leave the European Union. This followed a Brexit campaign centred on the issue of immigration.

Dr Awan said Brexit had without doubt "emboldened" those who held extreme racist and anti-Muslim views to express them on Facebook and elsewhere.

In May Facebook and other social media companies signed up to a new online code of conduct launched by the European Union, banning "all conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin".

That voluntary commitment remains at odds with Facebook's ongoing struggle "to balance giving people the power to express themselves whilst ensuring we provide a respectful environment", as Monika Bickert, the company's head of global policy management, put it at the launch of the code.

"I hope the code has an impact, but it is only voluntary and Facebook has to be prepared to take down posts," said Dr Awan. "Its community guidelines must be revisited and they need to be much more proactive."

It is, he acknowledged, a big task - Facebook has 1.6 billion users worldwide - "but on the other hand they make a lot of money, and they have a responsibility", he said.

"Yes, freedom of expression is paramount. But it must come with limits and responsibilities." By the time of publication Facebook had not responded to a request for comment.

Times of Israel
Biometric startup sees surge in demand as security woes weigh
Tuesday, 26 July 2016
Byline: Shoshanna Solomon

Jerusalem - The rise in terror attacks in Europe and elsewhere has generated a surge in interest in products that can keep areas safe from intruders.
"There is a rise in the need for security products because people realize they have to protect themselves in these kinds of situations," said Arie Melamed, chief marketing officer of the Israeli startup FST Biometrics, which has also witnessed a rise in demand for its identification technology.

The biometric identification technology uses a combination of facial recognition and behavioral and voice analytics to identify personnel of enterprises or government buildings from a distance and in motion, doing away with keys, codes or ID cards.

FST's system is based on prevention: it enables access only to those who are authorized to enter certain areas, freeing up security guards to focus their attention on the remaining people in the building who have to be checked.

"Why should you punish everyone with the checks?" Melamed said. "Why ask everyone at airports to come three hours earlier, for example, when you could be asking that only of people who are not

frequent fliers, for example. We don't have a magic wand for everything, but we can reduce the load on security people."

Government institutions and enterprises globally in the financial, corporate, health and real estate sectors are already using the technology to secure access for their employees in a nonintrusive manner, Melamed said, and protecting security sensitive areas from intruders.

FST, whose founder and CEO is a former head of Israeli intelligence Aharon Farkash and which has former Israeli prime minister Ehud Barak on its board, said earlier this month that its In Motion Identification (IMID) access system product makes more than 1.5 million identifications a month and has increased its customer base by 30 percent in the past year.

The company is also developing a mobile solution, Melamed said, and also one for situations in which there is no user cooperation -- for example in airports, stadiums or malls, where, unlike in an office building, creating a database of all regular users is more complicated. "We have the technology; we are still deciding if that is the direction we want to company to go," he said.

The applications of the technology don't all have to be grim, however. In Holland, the ICER Innovation Center uses FST's IMID technology to allow visitors, including King Willem-Alexander and Queen Maxima of the Netherlands, to gain personalized information about exhibits as they pass through interactive checkpoints.

New York Times
China Clamps Down on Online News Reporting
Monday, 25 July 2016
Byline: Michael Forsythe

Hong Kong - China has ordered several of the country's most popular internet portals to halt much of their original news reporting, in a move that could confine an even larger share of the journalism in the country to Communist-controlled mouthpieces ahead of an important party meeting next year.
The profit-driven portals, several of which are listed on United States stock exchanges, have in recent years expanded their investigative teams to increase readership among China's more than 600 million internet users by scooping the staid state-owned news media on stories about subjects including industrial pollution, tainted milk powder and even police brutality.

But on Monday, several news organizations reported that the Beijing office of China's internet regulator, the Cyberspace Administration of China, ordered the websites of a number of the companies, including Sina, Sohu, NetEase and Phoenix, to shut down or "clean up" several of their most popular online news features.

The announcement came within weeks of the surprise departure of the Cyberspace Administration's director, Lu Wei, and his replacement by an official who had served under President Xi Jinping in a previous position. Under Mr. Xi, media controls have tightened as the Communist Party has tried to squelch news that might put its governance in an unfavorable light.

In February, Mr. Xi visited three of the top state- run news organizations, telling their staffs in a highly choreographed tour that they existed to serve as propaganda messengers for the party. This month, a respected scholarly journal run by retired Communist Party cadres shut down after a quarter-century following the dismissal of its founding publisher.

The edict made public on Monday, which said the web portals were in "serious violation" of a 2005 internet regulation, came before a meeting next year of the Communist Party Congress. The party often puts in place controls on news before important events, such as the party conclave, held once every five years, which will pick a new group of senior leaders.

The news sites are run by China's biggest internet companies, which also operate social media platforms and produce some of the country's most popular online games. Sina, which runs a news aggregation service and publishes original reporting, also created Weibo, China's popular Twitter-like social media site. The companies are roughly the equivalent of the United States' largest internet companies, like Facebook, Twitter and Google, and their news sites combine articles from other outlets with original reporting and investigative journalism.

It is unclear whether the regulation will end all original reporting at the websites, where hundreds of millions of Chinese turn for their news. Monday's announcement mentioned specific features at four internet sites, which in recent years have attracted investigative reporters from newspapers such as Southern Weekend. It was among the first news organizations to face restrictions after Mr. Xi became head of the Communist Party in November 2012.

Wen Tao, who until last year was a reporter for "Serious Reporting" at Phoenix, one of the news features shut down by the new edict, said by telephone that in recent years the news portals had played a cat-and-mouse game with government internet censors, pushing the boundaries of censorship by publishing material without submitting it for approval and waiting to see if it was taken down by the authorities.

But Mr. Wen said that even in China, with its notorious army of censors, it was difficult for the government to control news in a market powered by hundreds of millions of readers hungry for news that goes beyond Communist propaganda.

"The flow of information cannot be stopped -- it's like a flood," Mr. Wen said. "You either need to discharge it or it will run rampant. The regulators are trying to use policies to block the holes."

Sun Xuyang, a former investigative reporter for Beijing News and Southern Metropolis Daily, was more pessimistic, saying by telephone that Monday's announcement was a signal that the space for original reporting was being eroded.

"There are no more illusions," Mr. Sun said.

The news sites targeted by the Cyberspace Administration include Sina's "News Geek," which this month published an article, later deleted, about a chemical contamination at a Beijing school, and "Landmark," run by NetEase, that last year scooped the official news media in reporting the arrest of the brother- in-law of a jailed former top official.

On Monday, the media or investor relations departments at Sina, Phoenix and NetEase did not respond to emails asking how the announcement would affect news operations. A spokeswoman for Sohu declined to comment, and the Cyberspace Administration of China did not immediately reply to questions faxed to its news office.

Globe and Mail
Why Russian hackers would meddle in U.S. politics
Thursday, 28 July 2016
Byline: Derek Burney and Fen Osler Hampson
Section: oped

That Russia is strongly believed to be behind the breach and leak of e-mails from the Democratic National Committee should not be a great surprise.
U.S. federal investigators had warned DNC officials earlier about the threat of such breaches. There have been similar kinds of attacks in the past. China, for example, was allegedly behind the cyberattack of the presidential campaigns of Barack Obama and John McCain in 2008.

What is new is that the stolen files were put into the public domain with the apparent intention of embarrassing Hillary Clinton and further dividing the Democratic Party between her supporters and those of her rival, Bernie Sanders.

The motive was likely directed more against Ms. Clinton than in support of any budding love affair between Russian President Vladimir Putin and Republican presidential nominee Donald Trump (who on Wednesday called on Russia to find Ms. Clinton's "missing" e-mails, essentially encouraging cyberspying by a foreign power).

As former U.S. ambassador to Russia Michael McFaul recently noted, Mr. Putin's dislike of Ms. Clinton is palpable. Her support for Ukraine and criticisms of Russia's parliamentary elections in 2011 was seen as unwelcome meddling in Russia's internal affairs. Mr. Putin's "a guy that remembers these things," Mr. McFaul said, "maybe that's another explanation for why they're seeking this tit for tat now."

We should expect more embarrassing revelations, especially if Russia, as some allege, was able to hack into Ms. Clinton's private e-mail servers, which she used when she was secretary of state.

Julian Assange, the founder of WikiLeaks, is also an all-too willing accomplice of Mr. Putin, such is his own personal dislike of Clinton.

But this is not just simply a titillating scandal in America's electoral silly season. It sadly points to a fundamental weakness in the United States' own cyberstrategy and its inability to deal effectively with autocrats who have outsized, imperial ambitions and terrorists who want to wreak havoc.

Cyberattacks are increasingly the cornerstone of Russia's regional and global military and political security strategy. They offset Moscow's economic weakness.

Russian pro-Kremlin groups initiated DDoS (distributed denial of service) attacks against Estonia, targeting its parliament, banks, government ministries and the media, after Estonia's spat with Russia

about the removal of a war memorial. Russian-sponsored DDoS attacks targeted Georgian websites, foreign ministry and media and even a pipeline concurrent with Russia's attack on Georgia in 2008.

Russia was also responsible for a major cyberintrusion against the power grid of the Ivano-Frankivsk region in Ukraine in 2015.

The attack, according to an online report by the SANS Institute, was highly co-ordinated and effective, leading to power outages for more than 80,000 customers.

Russia is not alone in playing this game. So do China and countries such as North Korea and Iran. The challenge is only going to get bigger. With the changing of guard in the United States, the whole world has one foot in the air. Mr. Putin and others are going to exploit the political vacuum.

And Mr. Trump is no better than Ms. Clinton on national security. His comments about NATO and the defence of frontline states such as Estonia, Lithuania or Latvia show both the limitations of his understanding of America's vital national security interests and his intellect.

Nor should Canadians, who are generally complacent about global pressures, think they are immune. Cyberattacks can and do happen here. A 2011 major attack against the Canadian government appears to have originated in China; it infiltrated three Canadian government departments and obtained classified information.

Cyberhackers have a distinct advantage because of the Internet's anonymity, the speed of attacks, and the strong incentives for states and other non-state actors to try to game the system.

The breach of DNC records is a wake-up call to us all, one that undermines trust in the Internet.

Russia, or China for that matter, cannot be given a free hand to disrupt at their discretion. There need to be reprisals, countermeasures and heightened vigilance to ensure that the openness of Western societies does not become a source of weakness or vulnerability against those who oppose our most basic values.

Derek Burney was Canada's ambassador to the U.S. from 1989-1993.

Fen Osler Hampson is a distinguished fellow and director of global security at the Centre for International Governance Innovation and Chancellor's Professor at Carleton University.

Politico
NSA could hold 'smoking gun' in DNC leak
Thursday, 28 July 2016
Byline: Josh Gerstein

Washington - The political world is intensely focused on the FBI investigation into the suspected Russian hacking of Democratic National Committee emails, but the real smoking gun that could link the hack to Moscow is more likely found in the vast data troves of the National Security Agency.
While private sector cybersecurity specialists have gathered evidence pointing to Russia as the source of the hack, the U.S. Government has unique abilities to confirm such a finding, including sometimes being able to identify specific foreign government agencies or even individuals as responsible for the hacking, experts said.

"Private firms are really good at forensics, but the federal government has other tools," former NSA Director Michael Hayden said in an interview Wednesday. "It's not just following the breadcrumbs to the actual crime. It's broader intelligence collection: what someone may have been planning, what they were planning to do with it after, fingerprints on how the information was forwarded ... It's not just forensics."

"It's the difference between being able to examine the crime scene and being able to conduct a wiretap," said former National Security Agency lawyer Susan Hennessey, now with the Brookings Institution. "You can learn a lot at the crime scene and maybe even solve the crime [but] intelligence authorities allow you to listen to people ... potentially gathering the kind of smoking gun evidence you need for this kind of attribution."

Whatever information the NSA has on the DNC hack is not likely to emerge from the spy agency directly but to be compiled by the FBI. Whether to call out the Russians directly will be up to the White House. Criminal charges are always a possibility, as well, although the chances of actually putting suspects on trial is remote.

At a cybersecurity conference in New York City Wednesday, FBI Director James Comey was mum about the DNC hack, but defended the value of the so-called name-and-shame appraoch.

"If we can't lock them up, we have to call them out," Comey said.

One very prominent former NSA contractor, Edward Snowden, has already said he believes that spy agency's snooping programs would "certainly" have spotted the DNC data as it made its way to Russia, if that's what happened. It's even possible the U.S. Government has some knowledge of internal Kremlin discussions about the hack, through surveillance or human sources, former intelligence officials say.

"Even if the attackers try to obfuscate origin, #XKEYSCORE makes following exfiltrated data easy. I did this personally against Chinese ops," Snowden tweeted Monday.

Records Snowden took from the NSA that have not yet been published show the spy agency hard at work trying to trace cyber intrusions and thefts, according to an author and journalist who had access to the archive of data Snowden copied while working for an NSA contractor in Hawaii.

"A lot of the stuff shows the NSA looking into the origins of some these attacks," said Jim Bamford, whose 1982 book "The Puzzle Palace" was the first widely read history of the agency. "One slide [in the Snowden collection] shows NSA ramping it up to plant up to a million or more implants in computers around the world. When you put an implant someplace it captures where something is coming from ... If you have a million of pieces of malware all around the world in key locations, it could trace back where an email came from."

The NSA will be able to compare signatures of the DNC hacks against a broader set of existing data than private security firms have access to, experts said.

In addition, the NSA may have intercepted and stored evidence of foreigners trying to get into the DNC systems, data being pulled out of those systems, or someone forwarding the data on to WikiLeaks, which released the emails and other records on the weekend before this week's Democratic National Convention.

Hayden declined to discuss the NSA's specific capabilities in this area, but said that sifting back through the recorded data is a frequent part of this kind of sleuthing. "It is routine for something that happens to then illuminate the data you already possessed in the past, whose meaning was not obvious," he said.

The NSA's ability to trace or, in government-speak, "attribute" cyberattacks has become pretty sophisticated, although it's far from perfect, experts said.

"They've been doing this ever since the beginning of the Internet," Bamford said. "That doesn't mean they can't be fooled, but NSA does a pretty good job of locating the origin or attribution of a lot of these attacks."

So far, President Barack Obama has been cautious about apportioning blame for the hack.

"I think the FBI's still investigating. I know the experts have attributed this to the Russians," Obama told NBC's "Today." "What we do know is the Russians hack our systems, not just government systems, but private systems, but what the motives were in terms of the leaks and all that, I can't say directly. What I do know is that Donald Trump has repeatedly expressed administration for Vladimir Putin."

One former U.S.national security official said he doubted Obama would have mentioned the Russians at all unless he had some official indication they were involved. "He wouldn't make a statement like that, even attributing to experts, without him having some reason to think it's true," said the ex-official, who spoke on condition he not be named.

A policy directive Obama issued Tuesday further clarifies how the U.S. Government responds to cyber incidents. The FBI is the key agency for on-the-ground "threat response," with the intelligence

community in a supporting role. Officially, the task of "providing attribution" appears to be assigned to the FBI.

An NSA spokesperson did not respond to a request for comment on the agency's role in the DNC investigation. A Director of National Intelligence official referred requests for comment to the FBI, which offered a statement confirming its ongoing probe.

"The FBI is investigating a cyber intrusion involving the DNC and are working to determine the nature and scope of the matter. A compromise of this nature is something we take very seriously, and the FBI will continue to investigate and hold accountable those who pose a threat in cyberspace," an FBI spokesperson said.

Pointing the finger at Russia publicly will be the easy part, though, compared to the question U.S. officials are certain will come next: How do you know that?

That's where things really get messy, because explaining how the U.S. Government zeroed in on suspects can expose sources and methods and compromise ability to do the same thing again in the future. Even publicly making the claim that a specific country did it can set in motion a series of events where revealing some sophisticated or sensitive U.S. capabilities get made public, experts say.

Intelligence officials got a vivid lesson to that effect when they publicly blamed North Korea for the 2014 hack into confidential files at Sony Pictures. Many in the private cybersecurity realm were skeptical and publicly challenged the U.S. attribution. The FBI eventually released more details information about the reasons for the attribution.

"Their credibility depended on it and essentially their hand got forced," Hennessey said.

If the Russians are culpable for the DNC hack (or hacks), detailing why the U.S. thinks that could limit our insight the next time Russia tries something similar.

"In a case where information was exchanged through a single channel, people who are sophisticated can determine that's how it was made public," Hennessey observed.

While many in the political world are breathless about the DNC hack and the possibilty of Russian involvement, those immersed in the world of intelligence don't find the act shocking or much different than things the U.S. has done over the years, vacuuming up information and using it for political advantage.

"We don't come in here with clean hands," Bamford said. "A lot of stuff is being intercepted all the time everywhere ...This goes on all the time. The only difference here is there was a publicized leak."

Washington Free Beacon
Experts: DNC Hack Shows Inadequate U.S. Security Against Russian Cyber Attacks
Wednesday, 27 July 2016
Byline: Reuben F. Johnson

Fort Lauderdale - Specialists who have studied Russia's cyber warfare capabilities said the Kremlin is responsible for the hacking and eventual release of 20,000 emails from the Democratic National Committee, adding that there is no sure way to stop these kinds of attacks from recurring.
Experts who spoke to the Washington Free Beacon cautioned that it is difficult to prove the connection between the hackers and the Russian government with a legal degree of certainty, but they said the evidence indicated Russian involvement.

Russia's intelligence services decided years ago to make cyber warfare a national defense priority, said Dr. David Stupples, director of the Centre for Cyber Security Sciences at City University London. They have become increasingly proficient in cyber operations as a result.

"From around 2007, Russia decided that information warfare was key to winning any world conflict, and that it was this area of capability and technology they decided would benefit from vastly increased military investment," Stupples said. "What made this decision easier was that Russia was also home to the largest numbers of some of the world's best hackers."

While the DNC is not a high-value military target, "there was still a threefold motivation to hack its system," Stupples said. "One was to demonstrate that Russia is on top of its game in this kind of shadowy warfare. Another was to embarrass the Democrats and undermine the presidential election process at a critical time. A third was to test U.S. security measures."

Testing U.S. defenses would reveal to Moscow how Washington might react in response to further provocations.

"The goal of testing U.S. security measures is not now, nor has it in the past--proved to be a difficult objective for Moscow," Stupples said. "The National Security Agency and FBI have long suspected that Russia had penetrated a significant number of sensitive U.S. infrastructure systems in order to test efficacy and document structure--not to mention steal military secrets."

The goal of Russia's cyber warfare activities is not just random disruption or embarrassing revelations, Stupples said in May at the European Electronic Warfare Symposium in Rotterdam.

"What Russia is doing is linking cyber attacking and hacking with its open information warfare methods--propaganda disguised as news programming, funding of NGOs, etc.--and in coordination with its military establishment's use of electronic warfare," Stupples said. "By employing all three methods together in an integrated pattern of activity Moscow can achieve what its military theorists call 'reflexive control'--in

other words warping your adversary's perceptions to the point where that adversary begins to unknowingly take wrong or damaging actions."

Russia has a distinct advantage in the cyber realm because it engages the services of non-governmental cyber crime entities, which masks its role in cyber attacks.

"This is what the U.S. and others of us do not have--proxy cyber warriors," said Stupples. "What the Russians are saying is that 'we will make these criminal organizations our partners--recruiting them to do cyber work for the Russian state.'"

The Kremlin promises its criminal partners it will "turn a blind eye to their attacking banks, disrupting commerce in the west, etc." as long as they make themselves available to do the odd job for Russia's intelligence services and military.

There are currently more than one million Russian programmers engaged in cyber crime, according to the United Kingdom and other NATO intelligence services. These programmers are affiliated with 40 Russian- based cyber crime rings. The United States and its partners could not feasibly match this level of manpower using only government agencies and employees.

The United States has maintained misplaced faith in international agreements or treaties as other state actors have raced ahead in developing cyber warfare capabilities, according to several experts. While Russia, China, North Korea, and other nations sign accords about cyber warfare, they use proxies to carry out prohibited operations and then blame them on criminal enterprises. "How do you prove which cyber attacks by a criminal gang were ordered by Moscow or Beijing and which were not?" asked one European expert.

The experts said no firewall or security scheme was ever going to be effective to acceptable levels against these kinds of attacks. The most effective deterrent, they said, was an offensive response more severe than the attack suffered.

"The U.S. administration not only continues to 'fight the last war' with ineffective measures, but it refuses to engage in reprisals against Moscow," said a cyber security specialist in Poland.

In 2008, a malware program named Agent.btz compromised some of the most sensitive U.S. military computer networks, including those of the NSA. The U.S. military's offensive cyber unit proposed counter measures that could be taken against the Russian government, which was thought to be responsible for the attack.

Senior administration officials turned down these suggestions, reasoning that the Russian operation was "an act of espionage and not an outright attack," according to the Washington Post. NATO specialists on electronic warfare said Russia exploits these ambiguities in U.S. policy.

According to Stupples, "Washington is now playing catch up" in a field where its adversaries have invested considerable resources.

The problem will only worsen with time, said another European expert, who said the current administration's refusal to confront Russia directly had only made the situation worse.

"Regardless of who wins this U.S. election, this issue needs to be addressed at the highest levels as soon as a new president takes office in January 2017."

Washington Post
Is there a Russian master plan to install Trump in the White House? Some intelligence officials are skeptical.
Thursday, 28 July 2016
Byline: Ellen Nakashima

Washington - The possibility that Russia is behind an information warfare operation to interfere in the U.S. election has sparked concern among administration officials, but it also generated skepticism that there is a Kremlin master plan to install Donald Trump in the White House, as some political operatives are now alleging.
Intelligence officials, who spoke on the condition of anonymity to discuss an issue under investigation, said there is little doubt that agents of the Russian government hacked the Democratic National Committee, and the White House was informed months ago of Moscow's culpability.

What is at issue now is whether Russian officials directed the leak of DNC material to the anti-secrecy group WikiLeaks -- a possibility that burst to the fore on the eve of the Democratic National Convention with the release of 20,000 DNC emails, many of them deeply embarrassing for party leaders.

The intelligence community, the officials said, has not reached a conclusion about who passed the emails to WikiLeaks.

"We have not drawn any evidentiary connection to any Russian intelligence service and WikiLeaks -- none," said one U.S. official. Doing so will be a challenge, in part because the material may not have been passed electronically.

Also unclear, the officials said, is the motivation, even if Russia is behind the leak. It may be that the Kremlin wishes to disrupt and discredit the U.S. political process without seeking any particular result.

Michael V. Hayden, former CIA director, said, "Frankly, I don't think they're motivated by thinking they can affect the election itself." He said the Russians, already masters at "information dominance" or using information as a political and military weapon, may be flexing their muscles "to demonstrate that they can -- not necessarily to make Trump win or Hillary lose."

If they are truly behind the email dump, he said, "they're taking their game to another level."

The email dump, current and former national security officials said, is highly troubling, regardless of its provenance. And it could warrant considering whether the elements of the electoral process should be raised to the level of "critical infrastructure," such as power grids and key financial systems, which merit special protection from cyberattacks, some officials said.

"We're not used to thinking of the election system as a critical infrastructure," said one senior administration official. "But I could make the case that it ought to be considered that. We ought to start talking about that."

Whoever shared the emails with WikiLeaks, the senior administration official said, "sure as hell didn't do that for our benefit."

And WikiLeaks co-founder Julian Assange promised Wednesday another significant release, but he did not specify when.

"There are more DNC emails and we will be publishing more related to Hillary Clinton's campaign," he told The Washington Post.

The WikiLeaks release -- and the prospect of more to come -- has presented the Obama administration with a fresh set of challenges that affect both national security and cybersecurity on top of a host of other damaging cyber-events. The North Korean hack of Sony Pictures Entertainment in 2014 represented the first time a foreign government hacker targeted an American company. It not only damaged computer systems, but attacked free speech by seeking to coerce the film studio into pulling a movie that poked fun at the North Korean supreme leader, Kim Jong Un.

And the Chinese hack of the Office of Personnel Management discovered in 2015 was so vast and disruptive, slowing down the security clearance process and raising significant counterintelligence issues, that U.S. officials considered it precedent-setting.

But an influence operation by Russia to interfere in a presidential election -- if that is what happened -- would be a bold move, even for President Vladimir Putin, analysts say. It would take what began ostensibly as traditional political espionage into a new category of information warfare.

"I'm deeply concerned because, if Russia is behind this, it would represent an unprecedented and alarming escalation of Russian willingness to interfere in our political process," said Rep. Adam B. Schiff, (Calif.), the ranking Democrat on the House Intelligence Committee. It would be an effort "to help pick a candidate who is favorable to an adversary."

Some of Trump's positions -- including raising questions about mutual defense among NATO members and potentially recognizing the Russian annexation of Crimea, a part of Ukraine -- would be applauded in Moscow, but the GOP candidate has said he has no connection to the Russian president.

Republican and Democratic lawmakers alike are calling on the administration to quickly figure out who is behind the leak -- and if it is the Russians, to call them out.

"Mr. Putin's Soviet-style aggression has escalated to levels that were unimaginable just a week ago," Sen. Ben Sasse (R-Neb.) said in a statement. "America is digitally exposed. The United States must take serious offensive and defensive actions now. Russia must face real consequences."

If it is Russia, Schiff said, the administration should absolutely say so. "They should make it known publicly and forcefully," he said. "Even if they're not able to lay out the evidence because it would disclose sources and methods, they should make the attribution."

The FBI, which has been investigating the hack for months, announced its involvement this week.

Forensic evidence linking the email dump by WikiLeaks to Russia came from a cyber-researcher and former Army intelligence analyst who on Tuesday concluded that the party that passed the material to WikiLeaks was part of a Russian information operation.

The party, who calls himself Guccifer 2.0 and who claimed to be Romanian, used a Russian company that provides a special type of service that helps mask the user's true location, said Rich Barger, chief information officer at the Arlington, Va.-based ThreatConnect. Barger analyzed communications between Guccifer 2.0 and journalists that were shared with him by the reporters. He traced information in the emails to the Russian service, called a virtual private network. Guccifer also used an Internet address associated with a number of Russian online scams, he said.

"Determining with confidence who was behind it -- if the Russians were the hackers, seeing them pass that data to WikiLeaks -- is probably much more difficult than attributing it to the initial hacker," said former National Security Agency Director Keith B. Alexander at an FBI cyber-conference at Fordham University this week. "That's a tough one -- especially because there are different ways of passing that information, not all electronic."

The larger question, Alexander said, is " 'Why did they do this? And what were they trying to influence?' That's the real issue."

Not everyone is convinced that the Russians, if they did it, meant to influence the election. "This is not Putin trying to help Trump," said Leo Taddeo, a former FBI special agent in charge of cyber and special operations in New York. "I think they were messaging Hillary Clinton, telling her that they can get in the way of her election if she doesn't show some flexibility in her position toward them."

Some analysts actually think Putin would see his interests better served by a President Clinton, who is well known in Moscow. "If I'm in the Kremlin, I'd love to see Hillary in office," said one former intelligence official. "She's incredibly predictable and not willing to do confrontation. Trump is both unpredictable and confrontational. As a game theory person, I'd much rather play poker against Hillary. I'd win every hand."

The Daily Dot
Russia begins collecting encryption keys while internet companies, like Facebook, stay silent
Thursday, 28 July 2016
Byline: Patrick Howell O'Neill

New York - Russia's Federal Security Service now has a means to collect encryption keys from internet companies that will decode otherwise unreadable data on the internet, it announced on Tuesday. The FSB announced the capability on its website but the actual order, which would detail the process, was not made public.

One month ago, Russia passed a sweeping surveillance bill requiring encryption backdoor access for the state, among other expansive new spying rules. The legislation specifically pointed out apps like WhatsApp (which is owned by Facebook), Viber, and Telegram. Noncompliance can result in a fine of 1 million rubles--or $15,000--but it's not clear how frequently that punishment can be levied.

WhatsApp, Viber, and Telegram representatives have repeatedly declined to comment on the new backdoor law in Russia.

Two weeks ago, Russian President Vladimir Putin ordered the FSB to produce the "encryption keys."

Russia's new surveillance reality is one of the most extreme moves in a global debate over encryption, privacy, and surveillance. What makes it even more incredible is the utter lack of transparency from the Russian government and businesses in the country.

"It's important, but we don't know what FSB actually suggested yet," Anton Nesterov, a Russian technologist, explained to the Daily Dot in an email.

Actually, no one seems to know what this new law means in the slightest. Or, more accurately, the people who do know are keeping mum.

To illustrate just how much we don't know, Nesterov has a long list of technical and legal questions he wants answered on the law:

In a way that it's written in the law, it's a disaster, and brings a lot of questions. Should SSL keys be shared? Ok, we can share SSL keys, but what about PFS?

Should it never be enabled, or we should patch openssl to keep track on session keys and then send billions of them to FSB? What about payment systems? I'm not sure if it's allowed by Visa/MasterCard rules to share encryption keys with a third party.

How can leaks be prevented? Passing keys allows authorities not only to decode transmitted everyone's information, including people who wasn't original target [sic], but also to perform active attacks, which can be a major problem.

Should we share keys at request or at the time we started using it? What's kind of transmitted data covered by this law? All kinds of data? Should we also share SSH keys, giving direct access to servers? Should we share VPN keys used by companies to connect to their internal networks?

These are the questions which should be answered by FSB decree, it's internal documents and practice.

The one organization that did provide comment on this situation struck a defiant tone. Tor, the American-based and funded anonymity network, is decentralized around the globe.

"We encourage people to try anonymous, decentralized services based on

Tor, like OnionShare to share files, or Ricochet for instant messaging," Tor representative Kate Krauss told the Daily Dot after the law was passed. "There is no data to retain and no central server to hack. Both are super easy to use and have a lot of fans."

The new "anti-terrorism" legislation was signed into law earlier this month by Putin.

The Daily Dot
Russia's rise to cyberwar superpower
Thursday, 28 July 2016
Byline: Patrick Howell O'Neill

New York - "The Russians are top notch."
Chris Finan is a former director of cybersecurity legislation in the Obama administration, an ex- director at DARPA for cyberwar research, and a former U.S. Air Force pilot and intelligence officer. When it comes to explaining Russia's place in the evolving world of cyberwar, he ranks the world's nations and firmly declares Russia's place in the top tier.

"They are some of the best in the world," Finan, now the CEO of the security firm Manifold Technology, says. "We're not talking North Korea or even China, who are really sloppy. The Russians are really good at covering their tracks."

Sometimes the best way to explain war is the language of sport. Cyberwar is no different. So we talk about who is best, worst, and most improved--everything short of handing out a trophy. We try to predict the future geopolitical games that seemed impossible yesterday and inevitable today.

In a flurry of action over the last decade, Russia has established itself as one of the world's great and most active cyber powers.

The focus this week is on the leak of nearly 20,000 emails from the Democratic National Committee. The culprit is alleged by many, including Democratic Party officials, to be Russia. The evidence-- plainly not definitive but clearly substantial--has found support among a wide range of security professionals. The Russian link is further supported by U.S. intelligence officials, who reportedly have "high confidence" that Russia is behind the attack.

The blame and the proof for the DNC hack will be debated for weeks and months beyond. Attributing cyberattacks is notoriously difficult, doubly so when the adversary is among the best in the world.

"To definitively attribute the breach at the DNC to a Russian actor is next to impossible," Leo Taddeo, former special agent in charge of the FBI's NY cybercrime division and now the chief security officer of Cryptzone, explains. "Unless we have a window into their side, we'll probably never definitively attribute this to Russia."

Beyond the forensic evidence that points to Russia, however, is the specter of President Vladimir Putin. Feeling encircled by the West and its expanding NATO alliance, the Kremlin's expected modus operandi is to strike across borders with cyberwar and other means to send strong messages to other nations that are a real or perceived threat.

This is not unique to Russia. The United States is extremely active and effective in the cyberdomain. The Americans spend billions of dollars annually to launch hundreds of cyberattacks every year. Furthermore, Washington has a long history of interfering in foreign elections and politics. And U.S. actors are often the chief suspects in unrest when the evidence is less than clear.

The most poignant such episode began in 2011, when protesters took to the Moscow streets to speak against Russian elections they deemed flawed or fixed--elections that put Putin into his third term as Russian president. You didn't hear much about it in the American press, but Putin accused then-Secretary of State Hillary Clinton of giving "the signal" and trying to "set the tone" that led to the demonstrations--an open charge of American politicians interfering in Russian elections.

To understand Russia's decade-long rapid rise in cyberwar, you have to look at Russia's number one perceived enemy: The West's North Atlantic Treaty Organization alliance and its slow but steady creep eastward toward Moscow, the capital city that the NATO alliance was originally built to defeat.

Sixteen years can seem like an eternity when it comes to the international sport of war.

"Russia is part of the European culture," Putin said 2000, the year he rose to the presidency. "And I cannot imagine my own country in isolation from Europe and what we often call the civilized world. So it is hard to visualize NATO as an enemy."

The newly minted head of state sought "more profound integration" with NATO, he said, including the possibility of joining the alliance if Russia "is regarded as an equal partner."

Whatever warmth existed between Russia and NATO disintegrated over the next few years. The Western alliance took in a dozen new member states since the end of the Cold War, a move seen by Russian leadership as an openly broken promise meant to take advantage of Moscow's post-Soviet weakness.

Russia's western-facing cyberwar exploded onto the world stage a decade ago when, in 2007, it smashed neighboring Estonia's national internet during nights of deadly riots sparked by disputes over the country's Soviet-occupied history and a bronze statue in Tallinn, Estonia's capital, that embodied it.

This Russian cyberattack opened a new era in war. Estonia, one of the world's most connected countries, was hit with a hammer that cut down the websites and servers of the country's leading newspaper, banks, police, parliament, national ministries, and the national emergency number.

"Attacking us is one way of checking NATO's defenses," Ene Ergma, speaker of the Estonian parliament in 2007, said. "They could examine the alliance's readiness under the cover of the statue protest."

The answer to that check: The alliance was not ready.

In an attempt to fix that failure, Estonia is now home to the cyber defense headquarters of NATO.

Despite the cyber defense center's existence, however, there's little feeling or evidence the Western alliance has a coherent and effective strategy against aggressive action from their Russian rivals.

After a massive amount of behind-the-scenes work and very public diplomatic efforts, China and the U.S. seemed to reach a detente that cooled an ongoing cyberwar between the two great powers. No such success has visited American-Russian relations.

"What the president has been able to do to restrain Chinese behavior has been effective," Finan, who worked on cybersecurity in the Obama White House, says. "Hacking private companies has really dropped off. We haven't had that kind of progress with Russia. We don't have the same type of leverage with Russia, and we need their help elsewhere. But [the DNC hack] has raised the stakes."

A year after Estonia's networks buckled, Russia's growing hammer in cyberspace dropped on another neighbor and former Soviet Republic nation it deemed a threat: Georgia.

Georgia ended up in a full blown war with Russia in 2008. But before a single shot was fired, denial-of-service attacks and defacements against targets like the website of the Georgian president--he was compared to Adolf Hitler on his own Georgian websites when hackers took control--set the stage for the traditional war that would begin a month later. Dozens of Georgian government, finance, and communications websites went down in the lead up to kinetic fighting.

When the shooting war began, the cyberattacks continued, marking the first time in history that the two domains of warfare coincided. In contrast to the relatively small on-the-ground fighting, the Russian-Georgian War has been called "quite historic and precedent setting," as David Hollis wrote in the Small Wars Journal, because Russia attacked Georgia on four fronts: Land, air, sea, and cyberspace.

Georgia is no Estonia, however; it was and is not nearly as connected a nation, so the effects paled in comparison to even the relatively small and contained shooting war. But it mattered.

"As tanks and troops were crossing the border and bombers were flying sorties, Georgian citizens could not access web sites for information and instructions," journalist Jon Oltsik wrote on Networked World. "From a U.S. perspective, imagine a 9/11 or Hurricane Katrina event if citizens had no idea what to do, emergency responders couldn't communicate, and utilities were cut off in a 200 mile radius outside of the disaster zone. This is the risk."

The message became increasingly clear: Cyberwar is a ready and effective tool in Russia's growing arsenal.

Part of what makes it such a potent tool is, once again, that attribution is difficult. Does this or that attack originate within Russia? That's often tough to say, but, even when that much is definitive, there remains the trouble of sorting through all the different cyberspace movers and shakers in Russia.

Some of the 2008 cyberattacks against Georgia were linked to a Russian criminal gang known as the Russian Business Network, or RBN. Pinning down the extra level of control and coordination between the Kremlin and the criminals for each specific incident can be a titanic task.

In this particular war, however, the links shined brightly.

Hackers took out Georgian news and government websites exactly in locales where the Russian military attacked, cutting out a key communication mode between the Georgian state and citizens directly in the path of the fight.

"It created panic and confusion in the local populace, further hindering Georgian military response," Hollis, a veteran of the U.S. Defense Department's cyberspace efforts, wrote in his 2011 study on the war.

The intimacy between the Russian state, private industry, and criminal underworld is notorious in cyberspace and beyond, to the top levels of Russian government and private industry.

"There is no doubt Russia uses these criminal organizations to mask their state-sponsored intelligence and military operations," Leo Taddeo, the former special agent in charge of the FBI's New York cybercrime division, says. Taddeo began his career in the Bureau focused on Russian organized crime.

"The Russian science and math programs are very good," Finan says. "They also have a ton of organized criminal groups that are frankly very innovative in their methods. Sometimes the state will outsource their work there."

Taddeo is convinced that Putin's ultimate goal in his alleged hack of the DNC is to knock back against NATO, the U.S., and the West in general.

"Putin and his senior leadership believe the main threat to Russia is the perception of a slow but steady encirclement of Russia by the U.S. and NATO," Taddeo argues. "Throughout the Obama administration, we have moved closer to Russia with advanced missile defense systems and the expansion of NATO bases. As such, the main strategic objective for Putin is to disrupt the U.S./NATO advance to their borders. This can not be overstated."

In the last year alone, the effects of this apparent agenda have been felt strongly in countries nearest to Russia that are either already in NATO or who flirt heavily with the alliance. After NATO conducted a naval exercise from Finnish territory for the first time ever earlier this year, hackers knocked the Finnish Ministry of Defense's website offline. Germany accused Russia of a cyberattack against a steel mill that caused "massive" damage.

The steel mill attack stands as only the second known incident in which hackers have caused physical damage. The first is Stuxnet, the American-Israeli cyberattack against Iranian nuclear facilities in 2007 and 2008.

The French television network TV5 Monde was knocked off the air for 18 hours in April 2015. The website was replaced by jihadist propaganda, but French authorities insisted Russian state-sponsored hackers were behind the attack. More to the point, they accused a group called Fancy Bear that American security experts believe is behind this year's hack of the Democratic National Committee.

When a Dutch commission concluded a Russian weapon destroyed a Malaysian airliner over war-torn Ukraine, Russian hackers targeted the investigation from start to finish.

In late 2015, Ukraine itself was the target of hackers who took control of a western Ukrainian power grid that knocked out power substations and launched a blackout for 230,000 Ukrainians.

Coming amid an ongoing armed struggle in Eastern Ukraine that heavily and continuously involved Russian soldiers and weapons taking and holding formerly Ukrainian soil, it was little surprise when the finger was pointed from Kiev to Moscow.

German intelligence backs Ukraine's blaming of Russia, but, as always, definitive proof remains elusive.

A year prior, just days before a Ukrainian presidential election, self-avowed pro-Moscow hackers crippled the country's national election commission digitally. Software, hard drives, routers, and backups were decimated.

In the middle of not only a civil war and armed conflict with Russia but also a political drama about the future of Ukrainian democracy, the country's election authorities being hamstrung and unable to offer real-time results may have sparked doubts about the legitimacy of a vote that was putting a more pro-Western and anti-Russian government in office in Kiev.

Ukraine's government and military have been the target of numerous cyberattacks since war broke out, putting it squarely on the front line of a new, hybrid conflict with Moscow. And although NATO has spoken about giving resources and defense aid to Ukraine, the progress has been slow so far.

The Kremlin's response to these accusations echoed their answer to nearly every charge leveled at them in the last decade. It's "absurd," Kremlin spokesman Dmitry Peskov said.

"The campaigns being monitored by the BfV [Germany's domestic intelligence agency] are generally about obtaining information, that is spying," Hans-Georg Maaßen, who leads BfV, said this year. "However, Russian secret services have also shown a readiness to carry out sabotage."

"Cyber- attacks carried out by Russian secret services are part of multi-year international operations that are aimed at obtaining strategic information," Maaßen said, also earlier this year. "Some of these operations can be traced back as far as seven to 11 years."

It's called "gray zone" combat, because cyberwar is saturated by such a dense fog that clear understanding or response can feel out of reach.

"The biggest problem in cyber remains deterrence," Toomas Hendrik Ilves, the Estonian president, said earlier this year. "We have been talking about the need to deal with it within NATO for years now."

In June, just prior to WikiLeaks public release of emails stolen during the DNC hack, Ilves said his biggest fear was the escalation of cyberattacks. If the DNC proves to be Russian work--or, more likely, if no absolute proof is forthcoming, but the the evidence and context continues to point that way--it won't be the first time high-level American politicians were hit by Russian hackers.

In 2014, hackers breached the White House's unclassified servers and accessed some (but not all) emails from President Barack Obama to staffers. The State Department was also breached, though Secretary of State Ashton Carter said the breach there was also limited to unclassified computers. One U.S. official called their adversaries "one of the most sophisticated actors we've ever seen."

Despite the decade-long rise in Russian cyberwar, the DNC hack is seen by many in the West as a blatant escalation beyond what the Kremlin has done previously.

"Everyone steals secrets," American political scientist P.W. Singer says. "Everyone. The difference is the dumping of them in ways designed to influence elections of foreign powers. It's akin to Putin's personal rise, viewing the processes of democracy as merely something to manipulate, not institutions to respect."

Russian actions on the internet extend beyond traditional hacking. Singer points to the country's dynamic troll factory system that influences social media; the international propaganda system, centered around Russia Today, aimed at influencing news; efforts to influence European politics and Brexit; and an information war focused on the U.S. election that fuels extremist support of Donald Trump.

"They literally invented [information warfare]," Singer says of the Russians. "They also have set up a wide apparatus to support it, some 75 different organizations, ranging from university programs to military units, studying the issue and operationalizing. Finally, the willingness to look at democracy as merely something to be manipulated gives a wider scope of activity they can do."

With the DNC breach as the latest cherry on top of what seems to be an endless onslaught of headline-making hacks, the potential responses vary widely.

Financial sanctions are seen by many as the most effective immediate tool to fight Russian action. Singer suggests retaliatory data dumps targeting the bank accounts of Putin and Russian oligarchs.

Acting chair of the DNC Donna Brazile, Trump, and Putin himself take a different lesson: Just don't use email--it's horribly insecure. Plenty of security experts agree, though the ubiquity of the medium make it tough to get rid of.

"The DNC breach really hits home on the evolution of the data breach from a sort of petty crime or adolescent act of vandalism to a professionalized tool of global influence being deployed by state-sponsored organizations carefully executing these acts in order to influence national elections with international consequences," says Danny Rogers, CEO of the security firm Teribium Labs.

It's the result of these breaches that remains the biggest question mark for Rogers.

"It remains to be seen throughout the election season whether this action is effective," he says, "or if it's a desperate attempt where there aren't stronger levers to pull."

Global Times
China stresses information age military capability
Thursday, 28 July 2016
Byline: Li Ruohan and Wu Gang

Beijing - China intends to become a strong information technology power, will beef up cyber security systems and will enhance its capability to win an "informationized war," the government stated in a document Wednesday.
The Central Committee of the Communist Party of China and the State Council jointly issued the "Outline of National IT Development Strategy" on Wednesday. The plans to steer the country's IT development for the next decade have for the first time included military development for the information age.

"To adapt to the recent changes in the national security situation ... information technology will resolutely become the direction of military modernization," the document states.

It also said the Chinese military needs to enhance real combat capability based on network information systems, which will focus on taking control of information in wartime.

Zhuang Rongwen, deputy director of the Cyberspace Administration of China, said the outline is the result of two years of cross-department work based on President Xi Jinping's emphasis on cyber security and IT development since Xi established and headed the Central Leading Group for Cyberspace Affairs in February 2014.

China is planning to make major breakthroughs in 5G technology by 2020. And by 2025, a leading global mobile communication network will be in place, ridding the country of reliance on overseas technology. Cyber security must be vastly improved, according to the outline released Wednesday.

Song Zhongping, a Beijing-based military expert, said China's military is still significantly far from a real informationized military.

"Presently China is not there yet, as most of the country's army are still mechanized forces," Song told the Global Times on Wednesday.

China needs to work on advanced Internet technologies to be a rule-maker instead of a game-player, so as to have a bigger say and to better protect its national defense and military information, he said. He added that an informationized military means connecting every soldier and every weapon among all troops so that when they are operating they are not only receivers of information but also contributors.

China established a Strategic Support Force at the end of last year, to go alongside the army, navy, air force and Rocket Force. Experts said the Strategic Support Force includes cyber war and space war troops.

"China has made remarkable progress in transforming mechanized forces to informationized forces, though it still has a long way to go to actualize the full informationization in all troops," Li Jie, another Beijing-based military expert, told the Global Times on Wednesday.

The biggest difficulty lies in the lack of informationization in the core technology and key equipment, such as large- scale combat platforms and warning systems, Li said. He added that the informationization of China's most advanced weapons still needs to be improved.

Xi calls for further reform

General Secretary of the Communist Party of China (CPC) Central Committee Xi Jinping on Tuesday called for the building of strong armed forces through military reform.

Xi presided over a group study seminar of the Political Bureau of the CPC Central Committee in Beijing, which focused on national defense and military reform.

Based on the reform plan, the general command of the People's Liberation Army (PLA) army, the PLA Rocket Force, and the PLA Strategic Support Force were established. The previous seven military area commands were regrouped into five theater commands, and the four military departments - staff, politics, logistics and armaments - were reorganized into 15 agencies.

With those reforms, the PLA has a system in which the CMC is tasked with the overall administration of the armed forces, while theater commands focus on combat preparedness, and various armed services pursue development, Xi added.

The Intercept
In Secret Battle, Surveillance Court Reined in FBI Use of Information Obtained From Phone Calls
Thursday, 28 July 2016
Byline: Jenna McLaughlin

Washington - Beginning over a decade ago, the country's surveillance court intervened to limit the FBI's ability to act on some sensitive information that it collected while monitoring phone calls.
The wrangling between the FBI and the secret court is contained in previously undisclosed documents obtained by the Electronic Privacy Information Center, or EPIC. The documents, part of an ongoing Freedom of Information Act lawsuit, were shared with The Intercept.

The documents reveal that the Foreign Intelligence Surveillance Court (FISA) told the FBI several times between 2005 and 2007 that using some incidental information it collected while monitoring communications in an investigation -- specifically, numbers people punch into their phones after they've placed a call -- would require an explicit authorization from the court, even in an emergency.

"The newly obtained summaries are significant because they show the power that the [Foreign Intelligence Surveillance Court] has to limit expansive FBI surveillance practices," Alan Butler, an attorney for EPIC, wrote in an email to The Intercept.

Additionally, The Intercept independently obtained sections of the FBI's 2011 Domestic Investigations and Operations Guide describing how the FBI currently deals with information it obtains after getting a court order for what's called a "pen register," or "trap and trace" on a target -- a capability built into the phone lines that records incoming and outgoing phone numbers for a particular phone. The 2011 guide is currently public but heavily redacted.

The Operations Guide, in addition to shedding light on how the FBI uses pen registers, reveals that the surveillance court's pushback more than a decade ago has become internal FBI policy.

During an investigation, the FBI is often interested in who a target is talking to -- what calls they make and receive, and where those calls physically originate.

By simply telling a judge the information is "relevant," the FBI can demand that a phone company, or email or other online provider, immediately hand over any and all "telephone numbers, email addresses, and other dialing, routing, addressing, or signaling information." That information can sometimes include locational data. They don't need to notify the target or demonstrate probable cause that he or she committed a crime to get it.

But the FBI's monitoring can end up getting more information than just phone numbers, though pen-register and trap-and- trace orders are not intended to get any "content" that would provide insight into the substance or subject of a communication.

For example, the numbers people punch into the phone after making a call can reveal financial or personal information -- like a credit card number, a social security number, a PIN, a prescription number, or any other type of response via automated telephone prompts. The "term of art" for this information is "post-cut-through dialed digits."

The FBI in the 2011 Domestic Investigations and Operations Guide has described the digits dialed after someone makes a call as "content."

Following the release of documents by NSA whistleblower Edward Snowden, many have described the secretive court as a "rubber stamp" because it rarely rejects a surveillance request. But there's nuance in what the judges have challenged or modified in response to requests over the years.

Between July and December in 2005, the surveillance court approved pen registers and trap-and-trace devices to target "at least 138" people.

However, one judge started asking the FBI more probing questions about what exactly it did with post-cut through dialing digits it "incidentally" obtained with those orders -- launching what Butler describes as an "open secret" fight between the Foreign Intelligence Surveillance Court and FBI over the information. The judge's request for a "memorandum of law" appears in the July 2006 Department of Justice report to Congress on its use of FISA pen registers, obtained by EPIC. Some of that pushback was documented by Wired in 2008.

In May 2006, the government told the court that it had the authority to collect that sensitive information, and would "in some cases ... specifically seek authority for secondary orders requiring a service provider to provide all dialing, routing, addressing or signaling information transmitted by a target telephone, which, in light of technological constraints, may include content and non-content digits alike," the report continues. (According to the Domestic Investigations and Operations Guide, the FBI agent requesting the pen register has to specifically ask for any additional dialing information following the first nine or 10 digits -- it isn't automatic.)

The government also insisted it wouldn't actually use that information in an investigation -- unless there's an emergency, that is, to prevent death, serious physical injury, or "harm to national security," though it's never made explicit what exactly that means.

Between January and June in 2006, the surveillance court modified some of the FBI's applications to stop it from using that information without additional permission, no matter the urgency.

The court "had made modifications to the government's proposed pen register orders," reads the biannual report to Congress obtained by EPIC. "Although the [FISA Court] has authorized the government to record and decode all post-cut-through digits dialed by the targeted telephone, it has struck the language specifically authorizing the government to make affirmative investigative use of possible content" unless permission is specifically granted by the court.

The surveillance court wasn't the only judicial body rejecting the FBI's requests to hold on to the additional dialing information. In July 2006, a magistrate judge in Texas denied an application for a pen register because filtering technology would not eliminate the additional content information. That led then-chief judge of the surveillance court, Colleen Kollar-Kotelly, to ask the government to respond to the Texas court, and explain how it might impact decisions in foreign intelligence investigations.

The government said the court should basically ignore the decision -- and take note of new revisions to the USA Patriot Act, which said the government could obtain "noncontent" dialing information. (Because there isn't technology that can reliably separate out content from noncontent when it comes to this type of dialing information, the law basically allows for all of it, the government argued.)

In 2006, the court had not yet written a formal decision on whether or not the government could keep getting this information -- let alone use it in an investigation.

But "most" of the judges continued to strike the "emergency" language from the FBI's requests, despite the government continuing to insist that "the proposed exception is reasonable under the Fourth Amendment" because its use is so rare.

By August 2006, the court asked the FBI to produce an entire report on how the dialing information obtained through pen registers is stored and kept in its databases. By 2007, the court reported that it modified 18 different government requests out of 98 within six months.

The secret court continued to delete language that would allow the government to use the post-cut-through dialed digits in an emergency -- and added a time limit on when it could come back to ask to use that content.

By 2011, the court's resistance appeared to enter into formal policy, according to the Domestic Investigations and Operations Guide section obtained by The Intercept. The FBI, the guide states, can never in these cases use information like credit card numbers or social security numbers obtained after dialing a phone number, "even in cases of emergency."

However, that exception still applies in criminal cases, according to the 2011 Operations Guide. "In an emergency," information obtained from the numbers people dial "may be used as necessary in criminal investigations to prevent immediate danger of death, serious physical injury, or harm to national security," reads the section on post-cut through dialing digits. And if the target is calling a bank, for example -- the FBI cannot get the account number from the call, but it can use the call as a lead and subpoena the bank for that information instead.

Butler points out that despite the FBI and the secret court's fight over the information, it is basically impossible to tell whether that information triggered investigative leads agents wouldn't have otherwise had without the pen register.

The FBI declined to comment on the previously redacted portions of the 2011 Domestic Investigations and Operations Guide obtained by The Intercept as well as the FOIA documents obtained by EPIC.

"The Domestic Investigations and Operations Guide establishes the FBI's internal rules and procedures, and describes the FBI's authority to use specific investigative tools as determined through the Constitution, U.S. statutes, executive orders, and the AG Guidelines for Domestic FBI Operations," Chris Allen, an FBI spokesperson, wrote in an email. "These rules are audited and enforced through a rigorous compliance mechanism designed to ensure that FBI assessments and investigations are subject to responsible review and approval."

New York Times
Cybersecurity Experts Aren't Sure if Email Hacker Is a Person or a Front
Thursday, 28 July 2016
Byline: Charlie Savage, Nicole Perlroth

Washington - Who is Guccifer 2.0, the self-proclaimed Romanian "lone hacker" responsible for copying thousands of emails and other files from the Democratic National Committee -- a real person, or a front created by Russian intelligence officials?
Technology specialists have been debating that question since June 15, when CrowdStrike, a cybersecurity firm hired by the Democratic National Committee, announced that sophisticated hacker groups with Russian links were responsible for breaching the committee's computer servers. Within hours of the announcement, someone using the moniker Guccifer 2.0 started a blog to mock that finding, posting several of the stolen documents and claiming sole credit.

But the publication by WikiLeaks of an archive of the committee's internal emails -- and the uproar they caused on the eve of the Democratic National Convention -- have focused wider attention on who, or what, is operating behind that name. While WikiLeaks has not said how it obtained the emails, Guccifer 2.0 claimed in a blog post last month to have sent them to WikiLeaks.

Cybersecurity specialists have pointed to an array of forensic and technical evidence suggesting that Guccifer 2.0 might not be a Romanian as claimed. That evidence included metadata hidden in the early documents indicating that they were edited on a computer with Russian language settings. American intelligence officials believe that Guccifer 2.0 is a front for the G.R.U., Russia's military intelligence service, according to federal officials briefed on the investigation.

In blog posts, Twitter messages, and electronic chats with journalists, Guccifer 2.0 has insisted such skeptics are wrong.

Against that backdrop, Guccifer 2.0's words are taking on heightened interest. They may be clues to a person's decision to intervene in the American election, or they may be a case study of a 21st- century Russian information campaign -- the work of different intelligence officials, crowded around a keyboard.

"Just because the Wizard of Oz says he's a wizard doesn't actually mean he is," said Peter Singer, a security strategist at the New America Foundation, a public policy institute.

The original "Guccifer" (pronounced GUCCI-fer) is a real person: Marcel Lazar Lehel, a Romanian hacker who used the pseudonym Guccifer to hack various accounts belonging to American celebrities and government officials, including members of the Bush family, former Secretary of State Colin L. Powell, and Sidney Blumenthal, an informal adviser to Hillary Clinton.

Mr. Lehel was arrested in Romania in 2014 for hacking the email accounts of several Romanian officials. In April, he was extradited to the United States to face hacking charges and pleaded guilty in May before

a federal judge in Alexandria, Va. While awaiting sentencing, Mr. Lehel claimed to have hacked Mrs. Clinton's private email server, but federal officials have found no evidence to support his claim.

Mr. Lehel is known for his fixation on what conspiracy theorists call the Illuminati, a shadowy group that they believe controls the world. The first Guccifer 2.0 blog post, and messages Guccifer 2.0 sent along with packages of files that same day to the websites Gawker and The Smoking Gun, also denounced the Illuminati.

Other oddities also arose. Technical specialists, scouring metadata on documents posted to Guccifer 2.0's blog, found some that were last marked by a person with a user name in Cyrillic that appeared to be a nod to Felix E. Dzerzhinsky, best known for establishing the early Soviet secret police forces.

On June 21, Motherboard, an online technology magazine, posted a Twitter chat log of an interview with Guccifer 2.0, in which the person using that account claimed to be Romanian and denied working with the Russian government. Pressed on why Russian language markings showed up in the metadata of the documents he had sent out, Guccifer 2.0 claimed that was just a "watermark."

"I don't like Russians and their foreign policy. I hate being attributed to Russia," Guccifer 2.0 wrote.

During the interview, Motherboard switched from using English to Romanian and to Russian. Guccifer 2.0 claimed not to speak Russian and abruptly cut off the interview.

Motherboard later reported findings of linguistics specialists who said that his Romanian answers did not seem like those of a native speaker, and that the syntax of several of his English lines echoed Russian sentence constructions.

And a linguistic analysis provided to The New York Times by Shlomo Argamon, a chief scientist at Taia's Global, a cybersecurity firm that has questioned cyberattack attribution claims in the past, also concluded that Guccifer 2 is Russian.

Mr. Argamon, who is a professor of computer science and the director of the master of data science program at the Illinois Institute of Technology, found seven oddities in the hacker's English text, five of which pointed clearly to Russian as the speaker's native tongue.

"The linguistic evidence consistently points towards the writer being either a native Russian speaker," Mr. Argamon said. "It is possible that the writer is a Romanian speaker who has studied Russian. However, the writer denied knowing any Russian, and so the most reasonable conclusion is that he is a Russian native speaker rather than a Romanian native speaker."

On June 30, Guccifer 2.0 posted additional documents from the Democratic National Commitee's servers on the WordPress blog. The post again denied Russian links, and spoke admiringly of Julian Assange, the founder of WikiLeaks; Edward J. Snowden, the former intelligence analyst who leaked

archives of surveillance documents; and Chelsea Manning, the Army private who sent a huge trove of military and diplomatic documents to WikiLeaks in 2010.

That post accused Mrs. Clinton of being "bought and sold," in contrast to Mr. Trump, who it said "has earned his money himself. And at least he is sincere in what he says."

But the post still expressed opposition to Mr. Trump's ideas "about closing borders and deportation policy." Of Senator Bernie Sanders of Vermont, the post said, "He never had a chance to win the nomination as the Democratic Party itself stood against him!"

The Hill, a newspaper that covers Congress, reported on July 13 that Guccifer 2.0 had reached out to it and had provided documents about Democratic campaign donors and lobbyists.

It quoted Guccifer 2.0 as saying in an electronic chat, "The press [is] gradually forget[ing] about me, [W]ikileaks is playing for time and [I] have some more docs." The next day, Guccifer 2.0 posted those documents on the blog. That was the last blog posting.

The Guccifer 2.0 Twitter account posted a few more messages. The most recent one, on July 22, expressed excitement that WikiLeaks had posted the archive of nearly 20,000 Democratic committee emails that "I'd given them!!!"

Since then, that account has fallen silent, too. No messages were posted even as the Democratic Party chairwoman, Representative Debbie Wasserman Schultz, resigned and Mrs. Clinton's campaign manager accused the Russian government of providing the leaked emails to WikiLeaks to help Mr. Trump.

The Hindu
India the most targeted country for data breaches
Thursday, 28 July 2016
Byline: Varun Aggarwal

New Delhi - The average cost incurred by Indian enterprises for a data breach has shot up to Rs. 9.73 crore this year from Rs. 8.85 crore last year, making India the most targeted country for data breaches in the world, says a study by IBM and the Ponemon Institute.
"If you go by the average number of records breached per country, the highest is India. In India, 31,225 records were breached in 2015 whereas 29,611 records got breached in the US. There was a 64 per cent increase in security incidents in India in 2015 compared to 2014, with incidents growing both in terms of volume and sophistication," Vaidyanathan R Iyer, Business Unit Executive, IBM Security Solutions, told BusinessLine .

The number of breached records per incident this year in India ranged from 4,500 to 100,100 records. The study found that companies lose up to Rs. 3,704 per compromised record. Breaches in highly

regulated industries were even more costly with financial institutions losing as much as Rs. 5,544 per record.

"There is a growing awareness around the importance of cybersecurity among Indian government organisations as well as enterprises. However, India's high economic growth also makes it a big target for attacks," Iyer said.

Iyer said the growth of cybersecurity insurance policies taken by enterprises in India highlights how they are trying everything to safeguard themselves from the impact of cyber attacks.

"Indian organisations are also not as well-equipped as maybe US companies, making them the most likely to experience a data breach caused by a system glitch or business process failure," Iyer said.

Incident-response teams can expedite and streamline the process of responding to a breach, as they're expert on what companies need to do once they realise they've been compromised. These teams address all aspects of the security operations and response lifecycle, from helping resolve the incident, to satisfying key industry concerns and regulatory mandates. Additionally, incident response technologies can automate this process to further speed up efficiency and response time.

The study also found the longer it takes to detect and contain a data breach, the more costly it becomes to resolve. While breaches that were identified in less than 100 days cost companies an average of Rs. 8.94 crore, for breaches that were found after the 100-day mark the average cost rose significantly, to Rs. 10.56 crore.

The most difficult incident to detect and contain is the malicious or criminal act (97 and 203 days), while data breaches caused by human error take the least time to identify and contain (69 and 139 days), the report said.

The 'Cost of a Data Breach' study annually examines both direct and indirect costs to companies in dealing with a single data breach incident. Through in-depth interviews with nearly 37 companies across the country, the study factors in costs associated with breach response activities, as well as reputational damage and the cost of lost business.

Asharq Al-Awsat
U.S. Issues Guidelines for Responding to Major Cyber Attacks
Thursday, 28 July 2016
Byline: Staff Report

Washington - The White House recently released a new set of instructions on how government agencies should respond to major cyber security attacks. The Tuesday published directory was seen as an attempt

to combat perceptions and criticisms on the Obama administration being inactive when addressing threats from sophisticated hacking foes.
The announcement was made amid suspicion in the U.S. government that Russia-hired hackers may have engineered the leak of emails stolen from the Democratic National Committee in an attempt to influence the Nov. 8 U.S. presidential election.

The directive includes a five-point scale to grade the severity of an incident, provides the first public guidance on the specific roles of federal agencies in coordinating efforts to investigate and respond to cyber security breaches in government and the private sector.

"To put it bluntly, we are in the midst of a revolution of the cyber threat - one that is growing more persistent, more diverse, more frequent and more dangerous every day," White House counter-terrorism adviser Lisa Monaco said at a cyber security conference in New York.

She said that the new presidential policy directive "will help answer a question heard too often from corporations and citizens alike - 'In the wake of an attack, who do I call for help?'"

Monaco named Russia and China as cyber adversaries that have become more assertive and she noted that Iran and North Korea are capable and willing to carry out destructive attacks.

The directive defines a significant cyber incident as one that is likely to result in harm to national security or economic interests, foreign relations, or the public confidence, health safety or civil liberties of the American people, according to a White House fact sheet.

An event would be designated as an emergency, or level 5, if it posed an imminent threat to wide-scale critical infrastructure, the stability of the government, or lives of Americans, according to a severity schema provided by the White House.

No attack against the United States so far would register as a five, and the hack on the Democratic Party organization would likely earn a lower grade, depending on how much evidence emerges on whether or not a foreign government is using the stolen information to try to influence the election, a source familiar with the policy discussions said. The magnitude of a response will be determined by the severity assigned to an attack, Monaco said.

Asked about the DNC hack, Monaco said it would be a thorough investigation "and I'm sure there will be more to say later." The FBI is investigating while cyber security experts and U.S. officials said there was evidence of Russia's involvement. The Kremlin dismissed the allegations, labeling them as absurd.

President Barack Obama has increasingly prioritized cyber security during his second four-year term, which has been marked by a spate of high-profile hacks against government agencies and private companies that exposed tens of millions of individuals' personal data.

Lawmakers and cyber security experts have often criticized the administration for not developing a clear road map for how and whom companies should contact when facing a cyber-attack.

The new directive largely codifies existing practices and norms rather than change policy, said Ari Schwartz, a former top cyber security adviser at the White House who is now with the law firm Venable.

"But there have been times when the language used has caused major confusion," Schwartz said. "We've seen agencies use the same terms to mean different things and that has confused victims."

U.S. Department of Justice, working through the Federal Bureau of Investigation and National Cyber Investigative Joint Task Force, will be the lead agency for investigating criminal intrusions or those that could affect national security, according to the policy.

The U.S. Department of Homeland Security will serve as the lead contact in helping companies respond to breaches of their networks. Intelligence agencies will be in charge of gathering information in order to identify who is behind an attack.

Philippines News Agency
Comelec assures safeguards against data hacking
Thursday, 28 July 2016

Manila - In the midst of the voter registration for the forthcoming barangay and Sangguniang Kabataan (SK) polls, the Commission on Elections assured the public that safeguards are in place against a repeat of the hacking of its database last March.
Comelec Chairman Juan Andres "Andy" Bautista noted that the commission has made sure that data has been secured from those who would try to hack their systems again. "We are more secure this time than before against data hacking," he said.

The poll body chief added that they are coordinating closely with the Department of Science and Technology to make sure that Comelec systems are safe from hackers. "We have undertaken several steps to secure the database after the hacking," Bautista said.

He added that they continue to monitor hacking attempts on their system. "We are constantly monitoring them (hacking attempts) as part of our protocol. We monitor them versus any attempts to penetrate our website," Bautista said.

Hacker group Anonymous Philippines defaced the Comelec website a month before the May 9 polls.

The incident was followed by the release of the personal information of millions of registered voters that were made searchable online. Among the sebsitive information that was leaked were voters' full names, complete addresses and passport numbers.

New York Times
Trump Eggs on Moscow in Hack of Clinton Email
Thursday, 28 July 2016
Byline: Ashley Parker, David E. Sanger

Doral, Fla. - Donald J. Trump said on Wednesday that he hoped Russian intelligence services had successfully hacked Hillary Clinton's email, and encouraged them to publish whatever they may have stolen, essentially urging a foreign adversary to conduct cyberespionage against a former secretary of state.
"Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing," Mr. Trump said during a news conference here in an apparent reference to Mrs. Clinton's deleted emails. "I think you will probably be rewarded mightily by our press."

Mr. Trump's call was another bizarre moment in the mystery of whether Vladimir V. Putin's government has been seeking to influence the United States' presidential race.

His comments came amid questions about the hacking of the Democratic National Committee's computer servers, which American intelligence agencies have told the White House they have "high confidence" was the work of the Russian government.

At the same news conference, Mr. Trump also appeared to leave the door open to accepting Russia's annexation of Crimea two years ago -- which the United States and its European allies consider an illegal seizure of territory. That seizure, and the continued efforts of Russian-aided insurgents to undermine the government of Ukraine, are the reason that the United States and its allies still have economic sanctions in force against Moscow.

When asked whether he would recognize Crimea "as Russian territory" and lift the sanctions, Mr. Trump said: "We'll be looking at that. Yeah, we'll be looking."

Mr. Trump's apparent willingness to avoid condemning Mr. Putin's government is a remarkable departure from United States policy and Republican Party orthodoxy, and has fueled the questions about Russian meddling in the campaign. Mr. Trump has denied that, saying at the news conference that he has never met Mr. Putin, and has no investments in Russia.

"I would treat Vladimir Putin firmly, but there's nothing I can think of that I'd rather do than have Russia friendly as opposed to the way they are right now," he said, "so that we can go and knock out ISIS together."

Mr. Trump later tried to modify his remarks about hacking Mrs. Clinton's emails, contending they represented an effort to get the Russians to turn over their trove to the F.B.I.

With the political conventions coming to an end on Thursday, Mr. Trump is expected to receive his first national security briefings from American intelligence agencies in coming days. It is unclear whether those briefings -- which describe the global challenges facing the United States but not continuing covert operations or especially sensitive intelligence -- will change any of his views.

His comments about Russian hacking came on a day when Obama administration officials were already beginning to develop options for possible retaliation against Russia for the attack on the Democratic National Committee. As is often the case after cyber incidents, the options for responding are limited and can be viewed as seeming too mild or too escalatory.

The administration has not publicly accused the Russian government of the Democratic National Committee hacking, or presented evidence to back up such a case. The leaked documents, first published by a hacker who called himself "Guccifer 2.0" and who is now believed to be a character created by Russian intelligence, portrayed some committee officials as favoring Mrs. Clinton's candidacy while denigrating her opponent, Senator Bernie Sanders. The release of the internal party emails and documents led to the resignation of Debbie Wasserman Schultz as chairwoman of the party.

Mr. Trump contended on Wednesday that the political uproar over whether Russia was meddling in the election was a "total deflection" from the embarrassing content of the emails. Many Republicans, even some who say they do not support Mr. Trump, say they agree.

If Mr. Trump is serious in his call for Russian hacking or exposing Mrs. Clinton's emails, he would be urging a power often hostile to the United States to violate American law by breaking into a private computer network. He would also be contradicting the Republican platform, adopted last week in Cleveland, saying that cyberespionage "will not be tolerated," and promising to "respond in kind and in greater magnitude" to all Chinese and Russian cyberattacks.

In the past, the Obama administration has stopped short of retaliating against Russia -- at least in any public fashion -- for its attacks on the State Department and White House unclassified email systems, or on networks used by the Joint Chiefs of Staff. It never even publicly identified Russian intelligence as the source of those intrusions, though the subject was widely discussed by senior United States officials when they were not speaking for attribution.

In contrast, the United States did bring indictments against Chinese and Iranian hackers for thefts of intellectual property and attacks on American banks, and imposed economic sanctions against North Korea in early 2015, for hacking into Sony Pictures Entertainment's computers.

Almost as soon as Mr. Trump spoke, other Republicans raced in to try to reframe his remarks and argue that Russia should be punished. A spokesman for Speaker Paul D. Ryan termed Russia "a global menace led by a devious thug." The spokesman, Brendan Buck, added: "Putin should stay out of this election."

Even Gov. Mike Pence of Indiana, Mr. Trump's running mate, issued a statement, saying that "if it is Russia and they are interfering in our elections, I can assure you both parties and the United States government will ensure there are serious consequences." Mr. Pence did not attend Wednesday's news conference because he was giving local television interviews, and an aide to Mr. Pence said that his team had written his statement about Russia before Mr. Trump began speaking.

Shortly after that Mr. Trump sent a message on Twitter declaring "If Russia or any other country or person has Hillary Clinton's 33,000 illegally deleted emails, perhaps they should share them with the FBI!"

The fact that the Democratic committee's servers were targeted -- and, apparently, not those of the Republican National Committee -- has brought up inevitable comparisons with the origins of the Watergate scandal, when burglars found little after breaking into Democratic committee offices before the 1972 election. The hackers, more than 40 years later, were more successful: A reconstruction of events suggests the first successful piercing of the Democrats' networks occurred in June 2015, long before the Russians, or anyone else, could have known Mr. Trump would get the nomination.

The Clinton campaign, eager to turn the subject from the chaos caused by the email release to the question of Russian interference, accused Mr. Trump of encouraging Russian espionage.

"This has to be the first time that a major presidential candidate has actively encouraged a foreign power to conduct espionage against his political opponent," said Jake Sullivan, Mrs. Clinton's chief foreign policy adviser, whose emails from when he was a State Department aide were among those that were hacked.

"This has gone from being a matter of curiosity, and a matter of politics, to being a national security issue," he added.

For his part, Mr. Trump cast doubt on the conclusion that Russia was behind the hacking. "I have no idea," he said. He said the "sad thing" is that "with the genius we have in government, we don't even know who took the Democratic National Committee emails."

Mr. Trump then argued that if Russia, or any other foreign government, was behind the hacking, it showed just how little respect other nations had for the current administration.

"President Trump would be so much better for U.S.-Russian relations" than a President Clinton, Mr. Trump said. "I don't think Putin has any respect whatsoever for Clinton."

Former Representative Pete Hoekstra of Michigan, a Republican who had served as chairman of the House Intelligence Committee, said Mr. Trump was right to keep hammering Mrs. Clinton on the subject of her private emails.

Mr. Hoekstra said he was untroubled by Mr. Trump's goading of a foreign power, particularly in light of Mrs. Clinton's use of a private server while she was secretary of state.

"Trump is bringing up a fairly valid point: Hillary Clinton, with her personal email at the State Department, has put the Russians in a very enviable position," Mr. Hoekstra said. "Most likely the Russians already have all that info on Hillary."

But Representative Jason Chaffetz, a Utah Republican who led the House oversight committee that looked into Mrs. Clinton's emails, was more critical. If Mr. Trump's comments were meant literally, he said in an interview, "I think he was absolutely wrong and out of line. I would never have said it that way, and I think it was ill-advised."

If the remark was tongue-in-cheek, he added, it failed at political humor.

Toronto Star
Snowden made Canadian spies review contractor policy
Sunday, 31 July 2016
Byline: Alex Boutilier

Ottawa - When Edward Snowden begin leaking secrets about mass surveillance in the United States, Canada's electronic spy agency quietly wondered if their security screening was sufficient to stop a copycat.
Newly released documents show some of the behind-the-scenes actions taken by the Communications Security Establishment (CSE) three years ago, when contractor Snowden first pulled back the curtain on the West's pervasive mass surveillance capabilities.

Whatever changes were contemplated have been blacked out from the heavily censored document, most watermarked "secret" or "top secret." While the documents note that CSE is generally confident in its security clearance process for contractors, officials added that contractors are only "assessed for engagement for short, defined periods of time."

Snowden fled the U.S. with a massive cache of documents relating to the National Security Agency, CSE's American counterpart and close partner, while he was working as a contractor for the spy agency. While hiding in Hong Kong in 2013, Snowden passed the documents to reporters from the Washington Post and the Guardian newspapers.

On June 6, 2013, the first stories about U.S. mass surveillance hit the front page - - the NSA had a program called PRISM, which gave them direct access to the data mined by massive internet companies including Google and Facebook.

Within a month, CSE officials told then chief John Forster the agency might want to review some of its security practices around external contractors.

"Similar to its allies, CSE relies significantly on contractors for expertise in a broad range of activities," the documents, requested by the Star in 2013 and obtained only this month, read.

"(But) there are some areas of contractor engagement that may benefit from a review of current practices."

Two weeks later, another memo to Forster complained about a "pervasive lack of knowledge and understanding, in the public realm, of CSE's role and mission." The secretive spy agency, who had received less than 40 media calls in 2012, was suddenly thrust into the spotlight.

"As CSE has not been able to provide the level of detail about activities that the media requested, academics, so-called experts and commentators have provided their opinions on the subject," the memo reads.

"While some commentators have been well-versed on the issues, and have outlined accurate accounts of CSE activities, others, including [name censored] have inaccurately represented CSE's activities and authorities."

"CSE has been accused of being too secretive, which has led to misunderstandings of the agency's activities and authorities. This has highlighted the need for outreach to the academic community and to the media."

CSE's communications staff recommended a briefing for academics and journalists, including reporters at the Star, La Presse, the Globe and Mail, the CBC and a number of other outlets both Canadian and international. It does not appear that briefing took place.

CSE did give a briefing earlier this year, when its independent oversight body revealed the agency had inadvertently broken the law by transferring Canadian metadata to international partners. It was touted at the time as the first press conference in CSE's 70 year history.

More of Snowden's documents were reported over the summer in 2013. The U.S. and Britain, two members of the Five Eyes security alliance that includes Canada, spied on foreign diplomats at a G20 summit. The NSA spied on ordinary German citizens as well as high-value targets like Chancellor Angela Merkel. The Americans also kept tabs on foreign media organizations.

As the stories continued to roll out both in North America and abroad, the CSE kept a careful eye on the debate in the United States. An August 14 memo to Forster noted that while a dozen or so important disclosures about U.S. signals intelligence had been revealed, the debate in that country stayed stubbornly on the collection of telephone metadata.

On August 28, Forster briefed the prime minister's national security adviser about Snowden. At the time, documents revealing CSE's powers and actions had not yet been made public -- but the agency had figured out just how much Snowden accessed and downloaded.

"CSE has focused its efforts on reviewing key Canadian (signals intelligence) access and collection capabilities that are deemed most valuable to determine the potential damage should information on these capabilities be released," Forster wrote.

"CSE and its Five Eyes partners are working together to ensure consistent public messaging across all the allies regarding the unauthorized disclosures and their impact."

The Star requested an interview with CSE about their security screening of external contractors, and what changes the agency has put in place after Snowden's disclosures. In a written response, the agency said they could not discuss security issues.

"However, I can tell you that CSE constantly reviews its security posture to ensure that security policies and practices remain effective at protecting CSE's capabilities and information," wrote agency spokesperson Ryan Foreman in an email, noting contractors must undergo an extensive screening process that includes an in- depth interview, polygraph testing, and a psychological review.

Foreman added that Snowden's disclosures have been harmful to CSE's operations -- a line Five Eyes countries have consistently used since Snowden first revealed their activities.

Snowden remains living in exile in Moscow, but has said repeatedly said that he would return to the United States if he could be guaranteed a fair trial. The 33-year old recently joined the U.S.-based Freedom of the Press organization as a director.

New York Times
Russian News Group Walks a Tightrope in Covering the U.S. Election
Sunday, 31 July 2016
Byline: Michael M. Grynbaum & Nicholas Fandos

Philadelphia - The American news media is wildly overplaying Russia's role in a major email leak. The Democratic National Convention was troubled by chaos and dissent. Donald J. Trump's request for President Vladimir V. Putin of Russia to hack Democratic emails was a joke that American pundits simply did not get.
Such is the worldview presented by RT, the state-run, Moscow-based international news organization that, this week, found itself in a strange position: covering an American presidential election where Russia is suddenly playing a major role.

The network, formerly known as Russia Today, has long been scrutinized for being a propaganda outlet of sorts for the Putin government, which oversees its finances. But its American arm, which attracts about eight million weekly viewers, has aspired to more mainstream success, hiring a team of on-the-ground journalists and familiar, if past-their-prime, television stars like Larry King and the former MSNBC anchor Ed Schultz.

That balancing act has been strained by Russia's suspected role in the release of stolen emails from the Democratic National Committee, a leak widely viewed as an attempt to meddle with the American election process. But the small group of RT journalists in Philadelphia said this week that their only instructions were to find fresh angles in a crowded news marketplace.

"People think, as a reporter for state media, that I have to toe this line, and speak to a narrative all the time," Lindsay France, the channel's lead presidential campaign correspondent, said in an interview.

"Have I ever gotten a phone call that says, 'You need to cover a story this way or that way'? No," Ms. France said. She added: "If I had serious dilemmas, I would have left a long time ago."

Still, RT's coverage has tended to emphasize a theme of America in disarray. President Obama's convention speech on Wednesday was notable for being "upstaged by T.P.P. protesters and other noisy audience members," according to the opening paragraph of an article on the channel's website. On Friday, its lead story on Hillary Clinton's climactic address was an item about Bill Clinton being "caught napping" during the remarks.

Then there is Mr. Trump, who shocked the American foreign policy establishment by seemingly inviting Mr. Putin to hack the emails of the Democratic leader. RT's site features a skeptical headline -- "MSM Misses Trump's Joke on Russia & Hillary Emails" -- and notes that American news outlets "freaked out."

"Mainstream media can apparently no longer tell the difference between when Republican presidential nominee Donald Trump is being bombastic and when he's joking," read the article, which ran without a byline, as is the case with other RT articles. (Mr. Trump has said his remarks were sarcastic.)

Contacted for this article, representatives from RT issued a lengthy statement from the network's editor in chief, Margarita Simonyan, who wrote: "There is no special policy for treating any news stories differently when they pertain to Russia."

But, Ms. Simonyan added, "It is alarming to see the American political and media establishments across the political spectrum painting Russia as the ultimate boogeyman, referring to it exclusively as a menace, a thug, or a dictatorship."

"The same talking heads never mention the rampant crackdowns by the absolute monarchies, theocracies and ruthless strongmen allied with the U.S.," Ms. Simonyan added.

RT was founded in 2005 as an arm of a state-owned news conglomerate, RIA Novosti, intended to serve as a counterbalance to coverage by Western media companies. (Current slogan: "Question More.") RT America, based in Washington, began in 2010, and its site pledges to deliver "stories overlooked by the mainstream media to create news with an edge."

This week, those stories have focused on dissatisfied supporters of Senator Bernie Sanders of Vermont, who were infuriated by the leaked Democratic emails. Mrs. Clinton's nomination came amid "sharp divisions and mass disappointment of Sanders's delegates," the network reported.

Video of skirmishes between protesters and the police in Philadelphia were prominently featured, even though such episodes were relatively rare at a convention that was more peaceful than some observers had expected it to be.

Ms. Simonyan, the editor in chief, said that the American news media's focus on Russia's presumed role in the leak was overblown.

"There are 10 times as many articles about Russia's supposed involvement with the DNC emails than there are about what's actually in the emails," Ms. Simonyan wrote. "Hypothetical Russia connections are being used by other Americans to discredit a major party's nominee, and yet Russia's the one sabotaging the process?"

Ms. France, the correspondent, put it this way: "People call us propaganda. We take a look at what we see every day, and we do something different."

In an interview, Mr. King, the former CNN star who now anchors a prime-time interview show on RT, said that he had never received directions on coverage from the network. He said he was surprised that Russia was now such a dominant focus of the American political conversation.

"I'm almost expecting Putin to come to America to make a speech," Mr. King said by telephone from Los Angeles. "Obviously, Putin wants Trump to be the president. I've never heard that before from a Russian president."

His biggest concern, Mr. King said, is that Mr. Trump, whom he has known for decades, has so far declined to appear on his show during this election cycle.

"Donald Trump is the easiest guy to book in the world," said Mr. King, who has said he will probably vote for Mrs. Clinton. "He has not responded lately, and I have no reason for it. I've always been friends with him, we go back 40 years."

"He keeps saying, 'next Tuesday, a week from Tuesday,' " Mr. King said. "I'm a little disappointed."

Find out what you need to know about the 2016 presidential race today, and get politics news updates via Facebook, Twitter and the First Draft newsletter.

Washington Post
Russia's DNC hack: A prelude to intervention in November?
Sunday, 31 July 2016
Byline: David Ignatius

Column: For decades, Russian intelligence agencies have used what they call "active measures" to destabilize their rivals. Now they seem to be turning those tools on the U.S. political system, though in the process they appear to have violated Rule No. 1 of the spy business: Don't get caught.
U.S. officials say they have strong evidence that Russian intelligence agencies hacked the files of the Democratic National Committee over the past year. What's less certain is whether they deliberately leaked some of those files to WikiLeaks, with the aim of disrupting Hillary Clinton's election campaign - though some experts think this "weaponization" of information was likely.

The scope of possible Russian political hacking broadened Friday with reports that computer systems of the Clinton campaign and the Democratic Congressional Campaign Committee had been breached.

"Anything's possible," President Obama told Savannah Guthrie of NBC's "Today" show when asked Wednesday whether Russia might have deliberately tried to influence the U.S. election. "What we do know is that the Russians hack our systems," he said, adding that "on a regular basis they try to influence elections in Europe."

Russian President Vladimir Putin grew up in a KGB culture in which such use of active measures was a standard tool of the Cold War. He seems to have carried this tradecraft into the Kremlin - employing hacking, black propaganda and other covert tools as part of what's politely described these days as "hybrid warfare."

U.S. officials say that Russian intelligence in recent years has secretly funded right-wing political parties in Europe, sponsored covert propaganda channels, hacked the electrical grid of Ukraine and cyber-sabotaged other neighboring states, and created networks of "trolls" to attack enemies online.

Why does Putin use these active measures to destabilize his rivals? Because they work. They're invisible and deniable and, for the most part, the targets don't fight back.

But the DNC hack may have been a bridge too far. It triggered blunt responses in recent days from top national security officials who were gathered here for an annual conference known as the Aspen Security Forum.

When the United States discovers evidence of foreign hacking, it should "be public about it," urged John Carlin, the assistant attorney general for national security. "Take it out of the intelligence channel ... that's the only way to change behavior," he said. James Clapper, the director of national intelligence, said that he wasn't yet ready to identify the perpetrator of the DNC hack but that from an intelligence standpoint, the United States is already "at war" with Russia.

"The Russians have had for years a doctrine of ... active measures," said Elissa Slotkin, acting assistant secretary of defense for international security affairs. She said that the Kremlin's tactics attempt "to sow dissent generally, either on a specific issue or just to cause political chaos ... in order to create an opening for themselves."

What worries U.S. officials most is that given Russia's demonstrated willingness to use covert action against its adversaries, it might secretly intervene just before the November election. That might mean releasing embarrassing Clinton emails, as GOP nominee Donald Trump has urged Moscow to do. It might mean leaking phony news stories, or finding ways to upset financial markets. The American political system is an open and vulnerable target.

Why would Russia target the DNC, in an operation that's eerily similar to the Nixon White House's 1972 burglary at the committee's headquarters at the Watergate? Partly, it was an information-gathering operation, like the reported Chinese intelligence hacks of the campaigns of Barack Obama and John McCain in 2008.

But Moscow may have had a special animus toward Clinton. When she was secretary of state, she endorsed Russian dissenters in the 2011 and 2012 elections. A furious Putin charged back then that she "gave them a signal" and that the dissidents, "with the support of the U.S. State Department, began active work." In other words, Putin thinks Clinton shot first.

The DNC noticed a problem in its computer system in April and hired a forensics firm called CrowdStrike to analyze the evidence. The firm concluded that two Internet addresses linked to Russian intelligence had been inside the DNC systems.

How did the DNC information get to WikiLeaks? A supposed Romanian hacker who calls himself Guccifer 2.0 claimed credit. But some experts believe this is what's known in intelligence parlance as a "false flag" aimed at masking the Russian hand.

And what about Trump? Some have argued that he was the intended beneficiary of Moscow's DNC hack. But it seems more likely that Trump is what Russian intelligence officers sometimes describe as a "useful idiot" - a person who unintentionally fosters Moscow's campaign of instability.

Sunday Telegraph (UK)
Cyber threat is too great to risk it, says former top spy
Sunday, 31 July 2016
Byline: Robert Verkaik

London - Theresa Mayès decision to review the Hinkley Point deal was applauded yesterday by a former head of counterterrorism, who warned against giving control of a nuclear power plant to the Chinese. Chris Phillips, who headed the police's National Counter Terrorism Security Office, told The Sunday Telegraph it was "crazy to give away a piece of critical national infrastructure to the Chinese when the world is in such a state of flux".

He said ceding any control of a nuclear plant would be a mistake. Mr Phillips, who advised the Home Office until 2011, when Mrs May was still Home Secretary, said: "The Chinese have been spying on us for years and have battalions of cyber hackers in China who are trying every day to gain a hold of our critical infrastructure and some of our companies.

"If they had access to a nuclear power station, they could turn the electricity off whenever they wanted. Nuclear power is part of the critical national infrastructure that should be protected at all costs - because the risks are so great."

Nick Timothy, Mrs May's joint chief of staff, has previously raised concerns over Chinese involvement in the deal. In a blog post last year, he said MI5 had concerns about Hinkley Point, stating that China's intelligence services "continue to work against UK interests at home and abroad".

One security expert warned that freezing China out of the deal could actually increase cyber attacks.

Professor Anthony Glees, head of the University of Buckingham's Centre for Security and Intelligence Studies, said China might retaliate if its planned 33.5 per cent stake in the £18 billion plant was turned down on security grounds.

He said: "It will be seen by China as insulting and potentially hostile and may well lead to reprisals.

"They have the capability to carry out cyber attacks on us and this may give them the motive.

"This could be the trigger for them to hack us even more in the sense that they've got nothing to lose. However friendly they are towards us, they are well known for their intrusive intelligence gathering."

Sputnik News Service
FSB Detects Cyberattacks on 20 Russian Organizations, Including Military Targets
Saturday, 30 July 2016

Moscow - Russian Federal Security Service (FSB) exposed planting of malicious software designed for cyber espionage in computer networks of about 20 Russian institutions, including government and military bodies, FSB press service said Saturday.
"Instances of planting of malicious software designed for cyber espionage in computer networks of some 20 organizations located on the territory of Russia have been exposed... Information resources of public authorities, scientific and military institutions, enterprises of the military -- industrial complex and other objects of country's critical infrastructure were contaminated," the statement read.

The press service stressed that the attack was professionally planned, has similar traits with the previously exposed attacks from all over the world.

"The latest sets of software are made for each 'victim' individually, based on the unique characteristics of the targeted PC. The spread of the virus is carried out by the means of targeted attacks on PC by sending an e-mail containing a malicious attachment," the statement continued adding that the software made it possible to do screenshots, turn on web-camera and microphones, collect data from the keyboard use.

FSB in cooperation with the ministries and agencies took a number of measures to identify all the "victims" of the malicious program on the Russian territory, as well as to localize the threats and minimize the consequences caused by its spread.

South China Morning Post
Strategic aim behind Anti-missile revelation
Saturday, 30 July 2016
Byline: Minnie Chan

Beijing - Timing of media reports on successful tests of Chinese system suggests Beijing is responding to South Korea's decision to deploy the US THAAD
Strategic and political goals are likely to be behind China's unusual disclosure this week of advances in one of its antiballistic missile systems, analysts say.

On Sunday and Monday, China National Radio, CCTV and PLA Daily's Tv.81.cn website carried reports touting four consecutive successful tests of a "ground-based midcourse defence" (GMD) system at the Korla Missile Test Complex in Xinjiang (??).

GMD systems plot, target and destroy ballistic missiles in space.

A clip of the first two tests was aired for the first time on the Tv.81.cn website.

CCTV said the four tests indicated that the system was ready for basic deployment in war, making China the second country after the United States to have the -technology.

The release of the footage came about two weeks after Washington and Seoul announced they would deploy the US Terminal High Altitude Area Defence (THAAD) anti-missile system in South Korea to counter threats from North Korea.

The THAAD system is expected to be up and running by the end of next year and Beijing has objected to its deployment in South Korea, saying the system's radar could penetrate Chinese territory.

Asked on Thursday if the GMD footage suggested China was preparing to deploy its own anti-missile system, defence ministry spokesman Yang Yujun answered with an indirect confirmation.

Yang said "prudent development" of anti-missile technology was in the interests of national defence but such a system would not target any specific country and would not affect global strategic stability.

That was the same day that PLA Daily said in an editorial that China would never "swallow insults and submit to humiliation when facing provocation", and referred to China fighting the US-led coalition in

the Korean war in the 1950s. "The Chinese people and Chinese military ... do not intend to become involved in an arms race with any country, but will firmly defend our security interests," it said.

The editorial accused the US of increasing regional tensions and warned South Korea that agreeing to deploy the THAAD system to serve the US "Asia rebalance" strategy was like inviting a wolf into the house.

There has long been speculation that China is on track to install its own answer to THAAD and there are signs that it could be well on the way to doing so.

Military experts said the ballistic missile interceptors shown in the footage were HQ-19 rockets armed with a kinetic kill vehicle, weapons that rely on damaging targets through the force of impact rather than warheads.

Together they are designed to engage ballistic missiles and satellites in lower-earth orbit.

According to the footage, the two tests were conducted on -January 11, 2010, and January 27, 2013. Other state media reports said China started the GMD project in 2007, with the last test carried out in October last year.

Macau-based military observer Antony Wong Dong said the timing of this week's announcement was deliberate.

"Obviously, China is very unhappy since the US and South Korea started negotiating the deployment of THAAD on the Korean peninsula," Wong said.

Song Zhongping, a retired instructor for the People's Liberation Army's former strategic missile force, the Second Artillery Corps, said the reports suggested the technology was reasonably advanced and was being put into service.

But Wong cautioned that the rush to develop and deploy the technology could carry hidden risks. Even the US needed to conduct at least 11 tests for its THAAD system and of those only seven were successful, he said.

"Learning from mistakes and failures is very important for weaponry development. It's not appropriate to save time and money on development of cutting-edge weapons," Wong said.

"The crash of one of China's -J-15 fighter jets in April is one of the best lessons. The aircraft project was pushed too fast and developed based on the unfinished Soviet-designed Su- 33."

CNR reported on Wednesday that a 29-year-old PLA pilot died after he lost control of his J-15 during a simulated deck landing exercise at a unspecified inland base on April 28. It is the first confirmed crash of a J- 15 since the jets went into service in December 2013.

Hong Kong-based military expert Liang Guoliang said recent official disclosures about sophisticated weapons in the last month indicated the two giants' space arms race was gathering pace.

But Song said there was still a gap between the anti-missile technology of China and the US.

"Compared with the US military, the Chinese anti-missile system lacks real battle testing, raising questions about its maturity and reliability," he said.

Additional reporting by Liu Zhen and Catherine Wong

Reuters
Russia has motive, capability and form for U.S. email hack
Saturday, 30 July 2016
Byline: Andrew Osborn

Moscow - The Kremlin says it had zero involvement in the hacking of Democratic Party emails while U.S. officials say the hack originated in Russia. We may never know who is right, but one thing is for sure - Russia had motive, capability and form.
Seen through Kremlin eyes, Moscow would only be doing what it feels the United States has been doing to it for years anyway - interfering in a geopolitical rival's domestic politics in an attempt to destabilize and shape events.

President Vladimir Putin said in February he had seen specific intelligence suggesting Russia's foreign enemies - code for Washington - were preparing to meddle in Russian parliamentary elections later this year.

And in 2011, Putin accused the U.S. State Department and Hillary Clinton, its then head, of stirring up street protests against his rule.

"We need to head off any external attempts to interfere in the elections, in our domestic political life," Putin, who is facing re-election in 2018, told officers from Russia's FSB security service in February.

"You know that certain kinds of (political) technologies exist and have already been used in many countries."

That was shorthand for Ukraine, Libya, Egypt and Syria, which Putin thinks Washington irresponsibly destabilized. People who have studied him for years say he believes the United States is trying to foment the same kind of unrest to oust him.

His credo, set out when talking about Islamic State last year, is to strike first "if a fight is inevitable" and, as Russia has shown in its reaction to what it sees as NATO's aggressive build-up near its borders, to respond in kind.

"Clearly the Kremlin feels it should and can insert itself into domestic politics in other countries in much the same way it believes the United States and Europe insert themselves into Russian politics," Samuel Greene, the director of the Russia Institute at London's King's College, told Reuters.

"In their view it is fair play. They have seen the West involving itself in politics in Ukraine and other former parts of the Soviet space and feel they should be able to pretty much do the same thing."

He said such disruptive behavior was driven by a calculation: to stir up trouble in other countries so they have less bandwidth to focus on Russia.

Mark Galeotti, senior research fellow at the Institute of International Relations Prague, said he believed another motive for the hack - if Russia was behind it - would be to portray U.S. democracy as venal and chaotic and so take the sting out of Western accusations that Russian elections are corrupt.

Kremlin-backed media has tilted its coverage in favor of Trump over Clinton, and Putin has praised the Republican candidate as "very talented". But Greene said he thought what would matter most to Moscow would simply be to destabilize and to ensure that whoever won on Nov. 8 emerged as a weak figure.

Navigating a grinding economic crisis caused by low oil prices, and at odds with the United States over both Syria and Ukraine, Putin is under pressure.

He needs the West to lift the sanctions it imposed on Russia over its 2014 annexation of Crimea from Ukraine, which have cut off access to Western credit markets and technology imports.

Above all, though, he wants to make sure that external forces do not derail his own push for continued dominance in a political landscape where the liberal opposition is almost completely absent from TV screens and parliament.

RED WEB

Nikolai Patrushev, the head of Russia's Security Council, said earlier this year there had been a spike in the number of cyber attacks on Russian government bodies and critical infrastructure by foreign intelligence services.

And Putin, speaking in February, complained about what he said were more than 24 million attacks in the past year.

Andrei Soldatov, an expert on the FSB and co-author of Red Web, a book about the Kremlin's sprawling surveillance machine, told Reuters he thought if Russia had hacked the Democratic Party it would have been to send a signal that it could do the same and wanted U.S. intelligence services to desist.

"This could have been an attempt to deter the United States (from hacking and meddling), to try to shake the U.S. establishment, and to try to weaken Clinton," said Soldatov.

"It's pure politics, it's not about military secrets."

In Moscow, Trump, who has spoken of his desire for better relations with Russia and praised Putin, is seen as far more likely to cut a sanctions deal with Russia, while Clinton is regarded as a hawk on Russia.

"Everyone in Moscow believes that with Clinton in the White House it would be absolutely impossible to get the sanctions lifted," said Soldatov.

Trump has already raised hackles in Ukraine by saying he would be willing to consider lifting sanctions.

CAPABILITY

Experts say the Russian state, via the FSB, has a well developed offensive hacking capability. It has previously been accused of deploying that capability in Estonia, Georgia and Ukraine. Russian military intelligence, GRU, is known to have similar capabilities, Soldatov said.

There are also other non-state hacker groups which experts say sometimes collaborate with the security services, motivated by patriotism or money.

Galeotti said Russia's capacity to mount cyber attacks had increased over the past two years. Previously, Moscow would force amateur hackers into its service, he said, but lately "what we are seeing is much more of a push towards creating professional in-house capacity".

In this case, however, Soldatov said he thought it more likely that amateur hackers would have been responsible for the U.S. hack rather than the FSB or GRU who, if involved at all, would have played only a very minor role.

One reason for reaching that conclusion was how sloppily and hastily prepared the cover-up of the hack looked, he said.

(Additional reporting by Christian Lowe; Editing by Catherine Evans)

Pakistan Dawn
FIA presents proposals to deal with cybercrime
Tuesday, 02 August 2016
Byline: Zulqernain Tahir

Lahore - As the Senate recently passed a law against cybercrime, the Federal Investigation agency (FIA) has proposed establishment of a special tribunal, purchase of (IT-related) equipment and extensive training of officials of all departments of law enforcement agencies to deal with the new challenge. "The FIA has proposed to the interior ministry that there is an urgent need for capacity building of law enforcement agencies and acquiring of modern equipment by the departments concerned to deal with cybercrime offences after enactment of the new cyber law. There is also a need for setting up a special tribunal to exclusively hear the cases related to cybercrime. Otherwise, mere introducing a new cyber law may not fully help achieve the purpose," an FIA official told Dawn on Monday.

The agency has also suggested that investigating officers, judges and prosecutors be taught local and international cyber laws and training of cybercrime investigation officers of FIA's National Response Centre (NRC) be conducted by foreign experts.

"International linkage for information sharing regarding cyber security should be established and signing of international covenants and agreements for international cooperation in combating cybercrime should be made. In addition to this, procurement strategies for secure and resilient hardware and software products should be developed," the FIA said.

The agency pointed out that since the general public and government institutions took cybercrime security casually which often resulted in hacking of accounts, misuse of IPs and breaking into software systems through backdoor and other serious offences, there was a need for launching awareness and education campaigns for cyber security (through media, seminars and workshops).

The NRC was established in 2007 at only five FIA stations -- Lahore, Karachi, Rawalpindi (Islamabad), Peshawar and Quetta -- with 'limited' resources, space, manpower and logistic support.

After the launch of 3G/4G technology in Pakistan, the use of internet has increased tremendously. The FIA official said that subscriber logs were not currently being provided by cellular companies, which meant that if a crime was committed by using 3G/4G subscriber, the IP (internet protocol) address of mobile number was not easily accessible.

The FIA called for developing a mechanism for monitoring internet traffic.

At present all internet service providers (ISPs) in the country are under the Pakistan Telecommunication Authority (PTA).

The FIA said that since Pakistan had not signed any mutual legal assistance treaty (MLAT) with the United States or other European countries, social networking sites often refused to provide detail of the suspects involved in cybercrimes through their websites.

"Technical experts of FIA's cybercrime wing use their own social engineering methods to trace suspects. Different web hosting service providers also often do not provide data regarding ownership of websites, thus making it difficult to lay hand on suspects," another FIA official said, adding that offenders usually used the software over internet or other different websites to make calls anonymously through Skype, Viber, etc.

"These calls do not reflect in the call data record. The mobile companies and other long distance and international licence calling companies should be directed to only allow those incoming calls which are through legitimate channels and also in proper caller line identification format," he said.

Times of Israel
Israeli lawmakers advance bill to streamline cybersecurity
Tuesday, 02 August 2016
Byline: Judah Ari Gross

Jerusalem - The Knesset's Foreign Affairs and Defense Committee approved a bill to bring the country's various cyber defense groups under one umbrella on Monday, the committee announced.
The bill will return to the plenary for a second and third reading later this week, where it will likely pass, before it is signed into law, the chairman of the committee, Likud MK Avi Dichter, told reporters Monday. "I'm not exaggerating if I say that the central threat of the beginning of the 21st century is the cyber threat," he said.

To address that threat, the committee's cyber-defense subcommittee has worked since July 2015 to craft a comprehensive and streamlined proposal to address the country's preparedness toward hacks and other digital attacks.

"During the last year, we spent dozens of hours with each body to hear how they work and how they think our preparedness should be," Dichter said in the Knesset on Monday.

One of the subcommittee's main findings was the need for one responsible body -- the National Cyber Authority -- to oversee both civilian and military networks. For example, the authority would monitor the cyber defenses of the IDF and the Mossad, as well as the Electric Company and the Water Authority.

This National Cyber Authority will be responsible for the nation's networks and overall security against cyberthreats. However, it will not necessarily act as a shield for hacks and attacks of private citizens.

Committee member Omer Barlev, a Labor MK, cited the recent hack of the US Democratic National Committee, in which the political group's emails were accessed -- allegedly by Russia -- and distributed, as an example of a cyberattack the authority would not necessarily protect against.

"It depends on which political party was affected. If it was Labor, then probably not," Barlev said with a laugh. "But really it depends on how classified the information is," he said. "There's a list of specific groups the authority protects, which doesn't include political parties."

While the committee said that something along the lines of the DNC hack would not fall under the purview of the National Cyber Authority, some American analysts have categorized the allegedly Russian operation as a full-scale attack on the United States itself, not on a political party, as it represented an attempt by one country to muddle the affairs of another.

"This is not a Democrat or a Republican issue, this is a national security and a democracy -- with a big D -- issue," Peter W. Singer, a senior fellow at the New America Foundation, told Reuters's War College podcast this week.

To explain the exact nature of the kinds of attacks the authority will try to prevent, Foreign Affairs and Defense Committee member MK Ofer Shelah mentioned the Russian cyberattacks against Georgia, which kicked off a six-day war between the former Soviet republic and Russia in August 2008.

Throughout the short conflict, Russian hackers brought down some of the country's network infrastructure and also attacked and defaced government websites as a form of psychological warfare. "That war started in the cyber realm, not with something physical," Shelah said. "If you wanted to you could see it as a weapon of mass-destruction."

The cyber-defense subcommittee presented its findings in a report released Monday, in both classified and unclassified form, dealing specifically with the "division of responsibilities and authorities" in that area.

Shelah and the other members of the cyber- defense subcommittee met with representatives from the Israel Defense Forces, Shin Bet security service, Mossad, Israel Police and Foreign Ministry.

"There was no single body that had the exclusive ability to deal with the challenge [of cyberattacks] and commit itself to true cooperation between the different groups," the subcommittee said in a statement.

The subcommittee determined that an umbrella organization was necessary due to the fact that it discovered during the course of its investigation "disputes and even clashes between the different bodies."

This National Cyber Authority is meant to prevent such conflicts; however, the decision to have the civilian, governmental authority responsible for both civilian and military networks rankled some members of the subcommittee, including its new chairperson, Likud MK Anat Berko.

"Something that definitely bothers me is that it is a non-defense agency," Berko told reporters. "That means it's breached in terms of security. There will be academics and completely civilian bodies, along with sources and information from the defense agencies. We can't have a leak of intelligence information and work methods."

The National Cyber Authority was created in February 2015 and brought into operation two months later, but did not officially receive any powers or responsibility under Israeli law, an issue that the bill will address.

The legislation will amend an existing law -- the "Regulation of Public Security Bodies" -- to formally allow the prime minister to appoint a head of the National Cyber Authority who will serve as the "authorized officer" for issues concerning cyber defense. Under a temporary order in place until 2018, Baruch Carmeli has been named head of the National Cyber Authority.

This proposed law is only one of a series of actions the government will take to formalize and create the country's digital defenses. However, members of the subcommittee noted the future is still unclear for cyber defense, as the field and the threats presented by it are rapidly evolving and changing. "Things are changing at tremendous speed," Shelah said. "And we will have to change while on the move."

Dichter, who presented the subcommittee's report, took pride in the fact that the issue of cyber defense was being addressed proactively rather than reactively. Unlike "Iron Dome or the different Patriots" -- Israel's missile defense batteries -- "which were created in response to rockets being fired at Israel," Dichter said, the decision to address digital threats preceded the attacks.

Times of Israel
IDF looks to a 'one-network' army to fight future wars
Tuesday, 02 August 2016
Byline: Shoshanna Solomon

Jerusalem - As Israel marks a decade since the Second Lebanon War, the army has used the past 10 years to take stock of lessons learned from the conflict.
One of the key changes has been to make a technological push to increase collaboration between the Israel Defense Forces' various military arms so that the air and ground forces, the navy and intelligence corps can join efforts on the battlefield based on real-time information they receive

"Today, instead of the army adding budgets for more units or planes or ships, the push it so invest in better connecting the existing forces and increase their effectiveness through collaborative activities,"

said Yariv Nir, head of the army's operations department in the signal (C41) corps, in an interview with The Times of Israel.

In 2006, the IDF encountered a significantly tougher enemy in Lebanon's Hezbollah than it had faced in its skirmishes with Palestinians in Gaza and the West Bank, armed with guns and improvised explosives. Over the course of the 34-day war, 121 Israeli soldiers fell to the Shiite group's anti-tank missiles, mines, rockets, and machine gun fire.

Some 44 Israeli civilians were also killed during the course of the conflict from the near-constant barrage of missiles that rained down on northern cities. In Lebanon, nearly 1,200 people died, though the civilian-to-combatant ratio remains highly contested. Israel says that more than half of those killed were combatants, while Hezbollah claims just 250 fighters died in the war.

The conflict began on July 12, 2006, when two Israeli soldiers -- Eldad Regev and Ehud Goldwasser -- were kidnapped by Hezbollah gunmen near Zar'it along the northern border and smuggled back to Lebanon.

Investigations into the unfolding of the events revealed that there had been command failures during the war, with soldiers unprepared for the new kind of warfare and terrain they were facing. They also highlighted an acute lack of communication that existed between the various military forces, Nir said.

One of the more glaring examples of these communication failures occurred on the first day of the war, following the kidnapping of Regev and Goldwasser. In a 2009 tell-all book, Brig. Gen. (res.) Gal Hirsch, who led the Northern Command's 91st Division during the conflict, details how crucial intelligence ahead of the kidnapping did not reach him or his soldiers on the ground until weeks later.

The army is addressing these issues, Nir said, ensuring relevant training is given to all soldiers at all levels and increasing the level of communication between the branches.

For the past three years the Signal (C41) Corps has been implementing a plan called the Network Centric IDF Program (NCIP), which will create a "one-networked army" based on a joint communications platform for all the various arms of the military.

"The idea is to create a network on which all the forces operate together - to allow the pilots, the tank commanders, the ships and the soldiers on the ground to speak on one network and be on the same page at the same time," Nir said.

The joint network already works like this: if commanders on the ground identify terrorists in a house, they can pinpoint the location on a laptop screen, and signal in real time to a nearby plane or ship the location of their target. "The aim is to deepen this kind of networked operations," Nir said.

Still today each base and the general staff receive separate inputs from the air force, intelligence, land forces and navy. Each of these arms have their own communications fiber with their own routers and encryption systems.

"The aim of the 'one-network army' is to have one fiber on which everyone works, one computer for all. Access will be allowed to all those who are eligible," Nir said. "This will enable greater resources efficiency, but also greater operational efficiency. We have started implementing this process in the past year."

The army's decision to move many of its bases to the Negev, with tens of thousands of soldiers relocating to the wide open spaces down south, was a key catalyzer in making a networked army much more of a reality, Nir said.

"We are taking advantage of this move to build new technologies that support this plan. We are setting up a new telecoms infrastructure, developing new virtual and cloud technologies, increasing our data centers. All this will enable us to be a joint force with joined platforms." The ability to share video, voice and data, will be central to the army's technological push, he said.

Operation Protective Edge, fought against Hamas in the Gaza Strip in 2014, was in effect the first networked war in the world and one in which the IDF operated with some of the new joint-network systems in place, Nir said. "That operation very much strengthened the concept of a one-network army, proving that we are going in the right direction."

In an age of greater digitalization and just one network, the threat of cyber-security attacks is high, Nir said. Securing the network will be a significant challenge in the coming years, and the IDF has to make sure that it maintains the security of its data even as it makes the most of the potential of the joint network.

The main challenges ahead, according to Nir, are to learn from past mistakes and make sure the soldiers and forces are trained to meet the tasks they will be facing in the future and to ensure the security and continuity of the network operations, he said.

Fars News Agency
Coordinated Cyber Attacks Target 20 Russian Organizations
Tuesday, 02 August 2016

Tehran - Computer networks of some 20 Russian organizations, including, state, defense and scientific organizations, came under cyber attack, the Russian Security Service (FSB) said.
The high profile organizations' network have been infected with malware used for cyberespionage, Alwaght reported.

"The advanced software was tailored for each target individually based on unique characteristic of the computer under attack," the FSB said in a statement.

According to FSB report, the malware could be used to monitor internet traffic, take screenshots, secretly take recordings with an infected computer's camera or microphone, log keyboard strokes and conduct other forms of surveillance, the FSB said.

"The IT assets of government offices, scientific and military organizations, defense companies and other parts of the nation's crucial infrastructure were infected," the report added.

The security agency said that all the cases are linked and appear to be part of a well-coordinated attack requiring considerable expertise. The coding of the malware and vectors of attack are similar to those used in previous cyber-offensive operations against targets in Russia and other nations, the report stated.

The agency did not specify which party it suspects to be behind the reported cyber espionage or whether it was sponsored by any foreign government.

Kaspersky Lab, a Russian computer security company, said that it is investigating the activities of a "powerful cyber gang" that has targeted Russian organizations.

"We need some time to confirm the data in our possession. After that we'll be ready to share the results of our inquiry," Kaspersky Lab's press-service said.

The report comes shortly after the US media accused Russia of hacking the DNC, claiming that the Kremlin wants to influence the outcome of the November presidential election. When asked about the allegations, Russian Foreign Minister Sergey Lavrov said that he would not comment because he did not want to swear.

Fars News Agency
Iran Unveils Home-Made Drone with Jamming Capability
Tuesday, 02 August 2016

Tehran - Iran on Monday unveiled a new home-made drone which is capable of jamming the enemies' communication systems.
The drone was displayed in an exhibition of the Iranian Ground Force's latest achievements in Tehran. Ground Force Commander Brigadier General Ahmadreza Pourdastan visited the exhibition on Monday.

In addition to the drone, other Unmanned Aerial Vehicles (UAVs) with the capability of taking images and footages and jamming enemy drones' camera and surveillance systems as well as a drone equipped with destructive laser weapons were unveiled in the exhibition.

Also, in May, Iran had unveiled a new UAV which can be used for reconnaissance and combat operations.

The drone named 'Siraf' has a flying range of 100km and was unveiled during Beit ul-Muqaddas 28 wargames in the Central province of Isfahan at the time.

Siraf which is capable of taking images and real-time transfer of them has been built by students at the college of the Ground Force's artillery training center in Isfahan.

Also, in February, the Islamic Revolution Guards Corps (IRGC) showed the newly-designed model of its longest-range drone, Shahed (Eye Witness) 129, during the annual rallies on the occasion of the 37th anniversary of the victory of the Islamic Revolution in Iran.

The new model whose features haven't been revealed yet to the public is different from its predecessors, at least, in appearance. Yet, it could be said that the aircraft's nose has gone under some changes.

The Shahed 129, which was unveiled in September 2012, is capable of carrying out eight combat and reconnaissance missions for 24 hours and has a flying range of 2,000 km.

Khaleej Times
Hackers can access WhatsApp in seconds
Tuesday, 02 August 2016

Dubai - It takes intruders just 30 seconds to gain access into a smartphone's instant messaging services such as WhatsApp, the UAE-based non- profit online safety organisation, Emirates Safer Internet Society (E-SAFE) has warned.
E-SAFE Emirati youth champion, Hussain Adel Al Hashmi, a student of Al Ittihad National Private School, provided a live demo during a Press conference held in Dubai on Sunday on how a user could be tricked by intruders to gain access to their instant messaging apps.

The E-SAFE team launched the Youth Online Safety Campaign with the hashtag, '#SafeUpWhatsApp', informing teens how they can stay safe on social media.

The team said a survey conducted by Kaspersky Lab with B2B International in 2015 showed that despite the UAE's relatively small population, it is the second most attacked country online in the Middle East.

The Dubai Police's Al Ameen Service received nearly 300 calls from blackmail victims between 2013 and 2014. Various cases of trauma and attempted suicides have been reported by victims of online

sextortions and blackmailing. In a noteworthy case from a neighbouring country, a man blackmailed 60 children and published 45 indecent photos of them online when they refused to give in to his blackmail.

In a new dipstick survey undertaken by E-SAFE in the region to determine the level of security practised by WhatsApp users, 42 per cent of respondents said they use the app 'extensively', while over 50 per cent use the app 'moderately'.

The survey also found that 88 per cent of WhatsApp users would allow immediate family members to access their phone unattended, while 22 per cent said they allow friends to go through their phone.

Also, 70 per cent of the participants said they never log out of WhatsApp Web - an option which allows individuals access to their WhatsApp account from a PC or other devices.

Following the discovery of the potential misuse of the app's web feature, E-SAFE has reached out to WhatsApp Inc. to urge it to introduce a safety notification feature that informs users whenever their WhatsApp account is accessed from a web device.

Yonhap News Agency
Emails of Seoul officials hacked by N. Korea: prosecution
Tuesday, 02 August 2016
Byline: Staff reporter

Seoul - A group of presumably North Korean hackers have attempted to break into the emails of some 90 South Korean diplomats, security officials and journalists, and dozens of passwords have been leaked in the process, state prosecutors said Monday.
The latest cyberattacks took place as Seoul is striving to better guard against Pyongyang's online infiltrations following a string of malicious attacks on government and corporate websites, for which the communist country has been blamed.

The Supreme Prosecutors' Office said that between January and June the group attempted to hack into the emails of officials at the ministries of foreign affairs, defense and unification, and also those of the journalists posted at these ministries. The victims also include some researchers specializing in North Korean issues.

During the attempts the passwords of 56 email accounts were compromised, the office said.

The investigators acted on a report earlier this year that some hackers had attempted to launch "spear phishing" attacks to break into some government officials' emails. Spear phishing is a type of fraudulent email attack that targets specific individuals or organizations by appearing to be a legitimate email from another known person or organization and asking unauthorized access to their confidential data.

Investigators are currently trying to ascertain whether any state secrets had been leaked during the hacking attempts.

Prosecutors pinpointed North Korean hackers as the culprits in the latest attacks, as the method used mirrored North Korea's high-profile cyberattack in 2014.

The prosecutors found that the hackers established some 27 phishing sites to carry out the schemes.

In cooperation with the National Security Service and the Korea Internet and Security Agency, prosecutors have shut down the phishing sites.

"It is important (for government officials) to refrain from using private email accounts for official work, and they should frequently change their email passwords," a prosecution official said. "When officials carry out important tasks, it is desirable for them to take some security steps such as temporarily shutting down the internet."

In recent years, the North has repeatedly shown a willingness to use its cybercapabilities to not only pose security challenges to its potential adversaries, but also wring out financial gains -- as evidenced in its May attack on a major South Korean commercial website, observers here said.

The North is alleged to have broken into the server of online shopping mall Interpark, which resulted in the leak of the personal data of an estimated 10.3 million people, including their names, home addresses and email addresses. It then tried to blackmail the mall for profit.

Seoul officials believe that the North's General Bureau of Reconnaissance (GBR), its premier military intelligence agency, has masterminded major online attacks on South Korea. Among the pivotal organs under the GBR is Unit 121, which is tasked with penetrating enemy computer networks to secure confidential documents or spread viruses.

According to defectors and reports, the North selects cybersavvy students from across the country at an early age and sends them to Geumseong Middle School in Pyongyang to give them intensive hacking lessons.

They are then enrolled into Command Automation University, Kim Chaek University of Technology or Moranbong University for further education. Upon graduation, they begin their career as elite cyberwarfare officers.

Xinhua News Agency
Cyber regulation to better protect users' interests
Tuesday, 02 August 2016
Byline: Staff reporter

Beijing - A series of cyber regulations officially took effect Monday, as China aims to better protect online users' interests and better guide the development of China's Internet industry.
According to a regulation on search engines, released by the Cyberspace Administration of China, search providers must ensure objective, fair and authoritative search results.

Search providers must improve censorship and remove any illegal content that could harm national interests and people's lawful rights.

The regulation ordered that search engine providers must change the paid-for listings model and rank search results according to credibility rather than price-tag.

All paid-for listings should be labeled clearly, so that they are distinguishable from normal search results, and the returned content should not mislead users, the regulation said.

The regulation came after an investigation into Baidu, which was criticized for influencing users' choices by presenting misguiding information.

Wei Zexi, a computer science major at Xidian University in northwest China who had cancer, fell victim to Baidu's "pay to play" scheme. He died in April after a controversial treatment he found via a Baidu search failed. An investigation revealed that the search engine giant had sold highlighted advertizing space to questionable medical institutions.

Another online regulation taking effect requires real-name registration for users of mobile phone apps, in an effort to hold users responsible for content they share.

On one hand, if users break the rules, they will be warned, their use of the service may be restricted and, as a last resort, accounts may be closed.

On the other hand, providers of app services must protect the privacy of its users. They will be subject to public supervision and must deal with illegal content in a timely manner.

The fast growing mobile app market has seen a boom in malicious cyber attacks, online malware and security breaches. The regulation clearly defines the role of app developers and service providers, and ordered the protection of users' right to know and purchase option.

These two regulations order all web directories to have a channel to receive complaints and compensate for any damage caused to users.

"Cyber security isn't just about national development, but also concerns the immediate interests of every Internet user. Online service providers should be aware of their social responsibility," said Li Yuxiao, a professor on Internet governance from Beijing University of Post and Telecommunications.

The regulations reflect the growing importance China attaches to public concerns over the Internet, as well as its resolve to improve its governance capability both online and offline, said Li.

The regulations are expected boost netizens' awareness of their own duty and rights online, and supervise the operation and management of Internet companies, to create a healthy environment for the people and the Internet Plus industry, said Li Zhigang, chief of Beijing Academy of Telecommunication Research.

The number of Chinese netizens has soared to 668 million.

Associated Press
Seoul blames North Korean gov't organization for email scams
Tuesday, 02 August 2016
Byline: Hyung-Jin Kim

Seoul - An organization likely run by North Korea's government hacked into the email accounts of dozens of officials, journalists and others in South Korea this year, Seoul officials said Monday, the latest cyberattack that the South blames on its rival.
The organization sent phishing emails to government officials, journalists and professors who specialize in North Korean affairs to try to trick them into giving away their passwords, Seoul's Supreme Prosecutors' Office said in a statement.

The passwords for at least 56 of the email accounts were eventually leaked, according to the statement. Seoul authorities were investigating whether any confidential government information was stolen, but the prosecutors' office said there had been no reports of leakage of sensitive information.

The statement said the contents of the phishing emails, a China-based IP address and a web-hosting service provider were the same ones used in a previous North Korean cyberattack. It didn't identify the suspected organization.

South Korea accuses North Korea of launching a series of cyberattacks in recent years, but the North has dismissed the allegations. Last week, South Korean police said they believe North Korea was behind the recent leakage of personal data for more than 10 million users of an online shopping site.

South Korea said last year that North Korea has a 6,000-member cyber army dedicated to disrupting the South's government and military. The figure was a sharp increase from a 2013 South Korean estimate of 3,000 such specialists.

North Korea's hacking technology has been improving every year, according to Simon Choi at Seoul-based anti- virus company Hauri Inc. He said the North has carried out many more cyberattacks than is publicly known, making it difficult for South Korea to fend off all of them.

Many previous alleged North Korean cyberattacks failed to infiltrate the targeted computer systems at businesses and government agencies. But in several cases, hackers destroyed hard drives, paralyzed banking systems or disrupted access to websites. One attack was so crippling that a South Korean bank was unable to restore its online services for more than two weeks.

The Koreas have been divided by the world's most heavily fortified border since the Korean War ended in 1953 with a cease- fire, not a peace treaty. Earlier this year, North Korea conducted its fourth nuclear test explosion and conducted a prohibited long-range rocket launch, prompting worldwide condemnation and tougher U.N. sanctions.

Le Figaro
Antiterrorisme : Israël s'attaque à Facebook
Tuesday, 02 August 2016
Byline: Marc Henry

Jérusalem - Pour tenter d'empêcher les crimes des « loups solitaires » et l'essor du « terrorisme viral » , un projet de loi prévoit jusqu'à 70 000 euros d'amende par message incitant à la violence sur les réseaux sociaux.
Proche-Orient Israël s'est lancé sur la piste des « loups solitaires » en déclenchant une offensive contre Facebook. Ce réseau social est accusé de refuser de censurer les messages encourageant les Palestiniens à recourir à la violence. « Facebook est devenu un monstre » , proclame Gilad Erdan, le ministre de la Sécurité intérieure, qui a été jusqu'à affirmer qu'une « partie du sang des victimes » d'attentats anti-israéliens « retombe sur la tête de Mark Zuckerberg » , le patron du réseau social. Des propos très durs qui reflètent un certain désarroi face à une « intifada » menée par des Palestiniens auteurs d'attentats au couteau ou à la voiture bélier qui ont la particularité de n'appartenir à aucune organisation susceptible d'être surveillée et infiltrée.

Face à ce nouveau type de violences, l'armée israélienne, le Shin Beth, le service de sécurité intérieure et la police ont constitué ou renforcé leurs unités spéciales chargées de placer les réseaux sociaux sous très haute surveillance. Mais ce dispositif n'a pour le moment qu'un succès limité. En dix mois, une centaine de Palestiniens de Cisjordanie accusés d'avoir posté des messages incitant au terrorisme ont été arrêtés. Résultat : le gouvernement veut passer à la vitesse supérieure contre le « terrorisme viral » .

Un projet de loi a été présenté au Parlement. Des amendes pouvant aller jusqu'à 70 000 euros pour chaque message incitant à la violence seront infligées. « Les motivations de Facebook sont avant tout financières, c'est pourquoi nous devons l'attaquer au portefeuille si les dirigeants de cette entreprise

continuent à ignorer les appels au terrorisme » , a expliqué Revital Swid, du Parti travailliste, coauteur du texte.

Mission impossible

Le projet de loi doit permettre à un tribunal d'ordonner à Facebook, Google, YouTube, Twitter ou d'autres réseaux sociaux et sites d'informations de retirer tout contenu présentant un danger pour « les personnes, la collectivité ou la sécurité de l'État » . « Si les réseaux sociaux s'étaient décidés à agir plus agressivement contre les messages terroristes, nous aurions évité de faire appel à la loi » , assure Ayelet Shaked, la ministre de la Justice.

Sur le papier, cette nouvelle législation doit permettre de retirer beaucoup plus rapidement des messages jugés dangereux. Jusqu'à présent, les responsables des services de sécurité lorsqu'ils repéraient des textes, des photos et autres vidéos appelant à commettre des attentats devaient s'adresser au réseau social qui relayait ces contenus pour demander leur suppression. En cas de refus, un juge pouvait statuer. Mais cette procédure pouvait prendre des jours. Une éternité dans le monde virtuel. Autre difficulté : passer au tamis les messages constitue un énorme défi : plus de 80 % des Palestiniens utilisent des réseaux sociaux pour s'informer et échanger des messages.

La tactique adoptée pour tenter de contrôler ce gigantesque flux d'informations ne fait d'ailleurs pas l'unanimité. « Le projet de loi qui veut contraindre une entreprise privée à se transformer en un énorme système de censure nécessiterait une quantité totalement irréaliste de personnel qualifié pour assurer toute la supervision. Il s'agit d'une mission qu'il est pratiquement impossible de mener à bien » , estime l'Institut israélien pour la démocratie.

Dans les médias, le ton est plutôt au scepticisme. Le quotidien Maariv souligne que la fermeture éventuelle de Facebook ne mettrait pas fin au terrorisme : « Des réseaux sociaux se créent tous les jours et se font concurrence. Ce n'est pas l'État d'Israël qui peut empêcher cette évolution. » Et de conclure : « Telles sont les nouvelles règles du jeu. »

Washington Post
Cyberwar, out of the shadows
Tuesday, 02 August 2016
Byline: Editorial Board

Editorial - Thousands of U.S. businesses and other institutions have been besieged by cyberattacks in recent years. But the penetration of the Democratic National Committee stands out. The theft of internal emails, attributed by some to Russia, and the use of those emails to sow discord in the middle of a presidential campaign, deserve a strong response from the United States. Along with the massive attack on Sony Pictures Entertainment and the colossal theft of sensitive records from the Office of

Personnel Management, the DNC hack is a sign of how dangerous and real this field of conflict has become.

A strong response may not be easy. The problem of attribution is exceedingly complex and not always solvable. Retaliate against whom? And what kind of response is appropriate? Would it be fair play to turn the tables on Russia and leak information about the financial holdings of President Vladimir Putin and his cronies? When specific culprits were identified in other cases, the United States issued criminal indictments against Chinese military and Iranian hackers, although they are unlikely to be prosecuted; in the Sony Pictures case, the administration imposed more sanctions on North Korea. In the OPM loss, quite probably to China, the government remained mum, as it often does about espionage.

The DNC hack is a fresh reminder that the United States needs a more robust and open debate about cyber-conflict than it has had to date. Most of the public discussion has been about defensive measures, such as how to protect networks of the government and the private sector from attack. Offensive cyber-capabilities have been largely hidden. The United States has been loath to admit it has cyberweapons or has used them, such as the secret Stuxnet computer worm used to attack Iran's nuclear program.

There are signs of change. In The Post last month, reporters Ellen Nakashima and Missy Ryan described a new team created by U.S. Cyber Command to carry out offensive cyber-operations against the Islamic State. The group, called Joint Task Force Ares, is composed of about 100 people, based at Fort Meade, Md., home to Cyber Command and the National Security Agency. The fact that this unit, under Army Lt. Gen. Edward Cardon, has been openly identified is a genuine step toward transparency. Aaron Hughes, a senior Pentagon official for cyber-policy, was quoted as saying, "We want to take cyber out of the shadows, where people think we're doing something malicious or spooky, and treat it like we do our operations in other domains." Exactly right: Cyber now ranks with air, land, sea and outer space as a domain of military conflict.

Secrecy in military and intelligence, including offensive cyberattacks, is essential to protect operations. But that should not preclude a broader discussion, to better understand the threats and what to do about them.

In 2012, President Obama signed Presidential Policy Directive 20, which stipulated that offensive cyber-operations would require presidential approval if they could result in loss of life, serious levels of retaliation, damage to property, adverse foreign policy consequences or economic impact. This settled some uncertainty about chain of command, but there are still many other questions that could be usefully debated in public. For example, what are the real effects of cyberweapons? How were cyber-operations used in Iraq and Afghanistan? How does the United States stack up against other military cyber-forces?

On July 26, Mr. Obama approved a new presidential directive that attempts to further define cyberattacks and what constitutes a "significant cyber incident," as well as how to respond. This seems to be a worthwhile exercise but is hardly the last word. We need more discussion about the limitations

and unknowns of cyber-conflict, including how to manage escalation and the risk of retaliation; and when to move beyond the cyber domain.

During the Cold War, the nuclear arms race involved many secrets, but policy and doctrine about the atomic bomb were widely debated. The United States maintained a nuclear weapons employment policy, kept classified, and also issued a declaratory policy, open for all to see. Cyber could use this, too: a simple declaratory policy. Meanwhile, let's have an open debate about how to respond to the DNC hack.

IDG News Service
Cybercrime infrastructure being ramped up in Brazil ahead of Olympics
Tuesday, 02 August 2016
Byline: Lucian Constantin

New York - Over the past few months, cybercriminals have set up thousands of malicious domains and servers in Brazil in anticipation of the 2016 Olympics in Rio.
Threat data collected by Fortinet from over 2 million sensors worldwide shows that between April and June, the number of malicious URLs detected in Brazil grew by 83 percent. That's an unusually large spike compared to the 16 percent growth in malicious URLs for the rest of the world.

According to a Fortinet report due to be released Tuesday, the number of spoofed domains that are typically used in phishing attacks has also increased, particularly those that try to mimic payment systems and government institutions.

The company's sensors detected over 3,800 malicious websites and URLs containing the government designation ".gov.br" that have likely been set up to target government and other officials involved in the Olympics.

Phishing activity increased 76 percent worldwide between April and June, with Brazil, Colombia, Russia and India representing the top four countries where this type of activity was observed. The top 5 phishing domains with the .br extension were used to spoof popular online banking services.

The Fortinet researchers believe that a large number of cybersecurity attacks will occur during the Rio Olympics, which is not unusual for such an event. However, compared to previous Olympic games, more of the attacks are likely to succeed because cyber threats are not treated as a very high priority in Brazil, they said.

According to a World Economic Forum (WEF) survey, businesses in Brazil ranked data fraud and theft as 16th among the risks they're concerned about, while cyberattacks were ranked 23rd. By comparison, U.S. businesses view cyberattacks as the number one risk and for those in the U.K. it's the number two concern.

Taking cyberattacks seriously might explain why 165 million cybersecurity events detected during the 2012 London Olympics resulted in only 97 confirmed security incidents.

"This level of aggregation and protection does not happen without the right priority and investments for cyber attacks," and is unlikely to apply in Brazil, the Fortinet researchers said in their report.

Moscow Times
Clinton Hacking Claims 'Absurd,' Says Kremlin
Monday, 01 August 2016
Byline: Staff report

Moscow - Russian officials have rejected accusations of Russian involvement in the hack of U.S. Democratic Party computers as "absurd" and "insulting."
U.S. presidential nominee Hillary Clinton made the claims in an interview on American television program Fox News Sunday.

"We know that Russian intelligence services hacked into the DNC, and we know that they arranged for a lot of those emails to be released, and we know that Donald Trump has shown a very troubling willingness to back up Putin, to support Putin," Clinton said.

Clinton's statement comes weeks after Democratic Party officials were targeted by a cyber attack which resulted in the leak of thousands of private emails. Her campaign chairman Robby Mook earlier claimed the hack "was done by the Russians for the purpose of helping Donald Trump," an accusation that both Trump and the Kremlin deny.

The Russian government again denied the involvement of Russian agencies in the cyber attack on Monday, calling the accusations "vague" and "absurd."

"Official Russian departments certainly are not engaged, and have never been engaged in, cyberterrorism. It is entirely out of the question," Kremlin spokesman Dmitry Peskov said, as quoted by the RIA Novosti news agency.

Clinton's statement is merely part of her election campaign, Peskov said.

Russian Foreign Ministry also responded to the accusations Monday calling them "insulting and unworthy," the Interfax news agency reported.

Andrei Krutskikh, Special Representative of the Russian President for International Cooperation in Information Security, also said that Washington had not officially complained about the hack.

"These claims are put forward by people who are fighting for the presidency. Officials in the White House avoid commenting or do so only vaguely," he told Interfax.

Wall Street Journal
Social-Media Firms Target Terrorism
Monday, 01 August 2016
Byline: Sam Schechner

New York - Nearly half a million teenagers and young adults who had posted content with terms like "sharia" or "mujahideen" began last fall seeing a series of animated videos pop up on their Facebook news feeds.
In one, cartoon figures with guns appear underneath an Islamic State flag. "Do not be confused by what extremists say, that you must reject the new world. You don't need to pick," the narrator says. "Remember, peace up. Extremist thinking out."

The videos are part of three experiments -- funded by Google parent Alphabet Inc., with help from Facebook Inc. and Twitter Inc. -- that explore how to use the machinery of online advertising to counterbalance the growing wave of extremist propaganda on the internet, both from Islamist radicals and far-right groups.

The goal: See what kinds of messages and targeting could reach potential extremists before they become radicalized -- and then quickly roll the model out to content producers across the internet.

The study, detailed in a report set to be published Monday by London-based think tank Institute for Strategic Dialogue, is a step toward understanding what techniques work, said Yasmin Green, who heads the counter-radicalization efforts at Jigsaw, the Alphabet unit formerly known as Google Ideas.

"At the end of the day, it is a battle of ideas," said Zahed Amanullah, head of the counter-narrative program at Institute for Strategic Dialogue.

A drumbeat of violent attacks by radicalized individuals or small groups has killed hundreds in Europe, Asia and the U.S. over the past two months.

The government response has largely been to demand technology firms move faster in removing extremist content from their services.

But Islamic State is fast to open new accounts and expand its propaganda to new apps, leading to a game of whack-a-mole. "It's simply impossible to remove it all," said Susan Benesch, a faculty associate at Harvard University's Berkman Klein Center. "Even if one platform successfully takes something down, usually that content is available somewhere else."

Institute for Strategic Dialogue began working with Alphabet on how to better target its messages in 2014 in the U.K. In that study, Google showed some sponsored search results and videos to people in selected demographics searching for information about Islamic radicalism. In the new study, organizers expanded that work to different content on Twitter, YouTube and Facebook for users in the U.S., U.K. and Pakistan.

U.S.-based nonprofit Average Mohamed made animated videos that explain Islam and criticize jihadist groups for American teens. Harakat-ut- Taleem, run by an anonymous group in Pakistan, created videos to dissuade people from joining the Taliban.

The third project, called ExitUSA, targeted white supremacists and focused on people who had already become radicalized.

By the end of the experiments, each of which lasted about three weeks, internet users had been exposed to some element of the three campaigns about 1.6 million times. The most concrete impact was that eight people approached ExitUSA producer Life After Hate for help leaving white- supremacist groups.

Wall Street Journal
Putin's Infowar on America
Monday, 01 August 2016
Byline: L. Gordon Crovitz
Section: column

Column - This column recently predicted that Russia would disclose hacked emails just before the presidential election as an "October surprise." The first surprise came early, with last week's release of emails hacked from the Democratic National Committee, whose chairman resigned for rigging the primaries in Hillary Clinton's favor.
Expect more surprises before the election. Vladimir Putin has an unprecedented trove of hacked communications at his fingertips -- and shows canny timing on when to hit "send." Moscow has an ambitious strategy for information war that goes beyond affecting a presidential election. Israeli analyst Dima Adamsky wrote last year that the Russian "information struggle" entails "technological and psychological components designed to manipulate the adversary's picture of reality, misinform it, and eventually interfere with the decision-making process of individuals, organizations, governments, and societies."

Security experts believe Russia hacked all 63,000 of Mrs. Clinton's emails as secretary of state, including the 33,000 emails she destroyed, and that Russia supplemented this information by later hacking the Clinton Foundation and the State Department. That would mean Mr. Putin has a trifecta of sources to identify suspicious links between Mrs. Clinton and multi-million dollar donors to her foundation,

including authoritarian governments and crony capitalists, and favors granted by the Clinton State Department.

According to Mr. Adamsky, Russia's goal is to cause "disillusionment and discontent with the government and disorganization of the state and military command and control and management functions." It's hard to imagine anything more disillusioning to Americans than the release by Russia of incriminating emails Mrs. Clinton had refused to disclose even under U.S. court order.

In a paper entitled "The Anatomy of Russian Information Warfare" written in 2014, Polish analyst Jolanta Darczewska traced Russian information warfare theory to Stalin's spetspropaganda (special propaganda) program in the 1940s. In recent years Mr. Putin, a KGB veteran, extended infowar to include "information manipulation," which includes "using authentic information in a way that gives rise to false implications," disinformation, fabricating information and blackmail.

Russia attacked Estonian government websites and hacked Ukraine's election commission days before a vote. A German investigator last year concluded there was no evidence behind the WikiLeaks claim that the National Security Agency eavesdropped on Chancellor Angela Merkel's mobile phone. It was likely disinformation to drive a wedge between the U.S. and Germany. Russia's information manipulation is intended both to embarrass people and to inhibit honest communications by demonstrating that governments can't protect confidential communications.

Liberals who long treated Edward Snowden and Julian Assange as heroes are now offended that WikiLeaks distributed the Russian hacks of the DNC. Journalist Franklin Foer complained in Slate last week that the "breathtaking transgression of privacy" of Democratic Party officials will have a "chilling effect" undermining the ability "to communicate honestly." That was the exact purpose of the hacks of hundreds of thousands of U.S. diplomatic cables distributed by WikiLeaks in 2011 through the New York Times and London's Guardian.

"It is not our goal to achieve a more transparent society," Mr. Assange, the WikiLeaks founder, told Time in 2010. Instead, the objective is to force U.S. officials to "lock down internally and to balkanize" so they will "cease to be as efficient as they were."

What can be done about infowar? Donald Trump was criticized last week for encouraging Russia to disclose Mrs. Clinton's emails, but making them public would be the best way to deprive Mr. Putin of the advantage he gains by holding them. A U.S. ally that spies on Washington as much as Washington spies on it, such as Israel or France, would do Americans a favor by making public its copy of Mrs. Clinton's emails. Otherwise, Moscow can drip the emails out on its schedule with its spin -- or hold them back as blackmail against Mrs. Clinton should she reach the White House. American voters should know what Mr. Putin knows.

The Obama administration has been passive in response to Russia's infowar -- even reluctant to admit its existence officially. Washington's best deterrence would be to reply in kind. The U.S. could hack and

release Mr. Putin's bank accounts detailing how rich he has become in office. U.S. prosecutors could use hacked information to indict Putin business cronies and deny visas to their associates and relatives.

Despite Russia's audacious hacking, Director of National Intelligence James Clapper last week would only go as far as to concede: "It's fair to say Vladimir Putin feels like he is fighting a low-level, asymmetric war with the U.S." Because of the Obama administration's failure to fight back, Mr. Putin is enjoying many victories.

Christian Science Monitor
The secret linguistics clues researchers used to link DNC hack to Russia
Monday, 01 August 2016
Byline: Paul F. Roberts

Boston - Call it the telltale font.
For security researchers delving into the source of malicious software that infected the Democratic National Committee's computers, linguistic clues in computer fonts, messages buried in malicious applications, and even comments from the alleged culprit helped tie the attack back to Russia.

In fact, linguistics is becoming increasingly important as governments and cybersecurity firms seek to accurately identify lone hackers or the nations that are behind high-profile attacks. And the stakes for this kind of attribution are growing higher as the US has responded to recent breaches with sanctions, political pressure, and in the future could retaliate with military action.

"In the digital world, we look at every aspect of communication," says Mario Vuksan, chief executive officer of the cybersecurity firm ReversingLabs. "From the way a hacking group connects to an asset to the way the binary code is written to text and email messages."

For instance, code could be compiled on machines that are loaded with specific languages. And hackers could tip their hand by using expressions common in certain countries or languages.

When it comes to investigating cybercrimes, techniques range from classical linguistic pursuits, such as word count analysis that examines patterns of language use, to more behavioral analysis that tries to identify unique patterns or behaviors using lexical analysis, says Steve Bongardt, a former agent in the FBI's Behavioral Analysis Unit who know works with the firm Fidelis Cybersecurity.

Mr. Bongardt likens it to investigating a crime scene, with hacking groups or individuals falling back on well-worn modus operandi that govern how an attack is carried out and less regimented "rituals" that are just as suggestive of a particular actor.

But linguistic clues often fall far short of pinning attribution for any single actor, Bongardt and others agreed. Rather, they say, governments and law enforcement agencies investigating crimes need to look

to the preponderance of evidence - most of it not linguistic - as they attempt to understand who was behind an incident.

In the case of the DNC hack, a previously unknown hacker who identified himself as Guccifer 2.0 claimed responsibility for the breach. He said he was Romanian without any connections to the Russian government. But cybersecurity experts and tech journalists poked holes in those claims by closely analyzing his comment and other language and cultural identifiers in metadata.

Initially, however, an early profile of the suspected DNC hackers by the cybersecurity firm CrowdStrike relied on a wealth of technical evidence to support the theory two groups with links to Russian intelligence were responsible.

CrowdStrike's analysis did not rely at all on linguistic clues. Rather, it compiled a list of 12 separate indicators of compromise that were common to the two hacking crew. They ranged from malicious programs to tools for managing malicious software and extracting sensitive data.

But after Guccifer 2.0 emerged to claim responsibility for the DNC breach, researchers soon noted subtle clues in his speech - as well as in documents offered from his website - that cast doubt on his account of the hack. For instance, the tech news site Ars Technica noted those clues ranged from Russian language text buried in the PDF format of leaked opposition research on Donald Trump.

But that kind of information is still not conclusive, says Mr. Vuksan of ReversingLabs, making attribution a challenge when it comes to cyberattacks and breaches,

"Cyber being what it is, it's an area where covert action can be done at different levels in many different ways," he says. "Decoys, intelligence, and counter intelligence can all reside within the same breath."

Still, clues buried in language in blog posts, social media, or malicious code is critical in an age when nation-backed hackers aren't beyond using disinformation campaigns to cover their tracks.

Experts say that Guccifer 2.0's claim of credit for the DNC hack is strikingly similar to claims of responsibility following an attack on the French TV5Monde network in April 2015. After attackers took over the network's websites and displayed images promoting the Islamic State, a group calling themselves the CyberCaliphate said they were behind the breach.

However, on closer examination, the attack was carried about by the same group tied to the DNC hack, says Toni Gidwani, director of threat research operations at the firm ThreatConnect.

The purpose of such ruses isn't to fool everyone, says Mr. Gidwani. Instead, he says, its to be "good enough" to create doubt about the prevailing narrative. "If you look at the broader Russian doctrine of cyberoperations, sowing discord is a measure of success."

The Australian
ADF seeks eye in the fly in the sky
Tuesday, 02 August 2016
Byline: Brendan Nicholson

Canberra - The Australian Army will buy up to 200 spy planes -- small enough to be held between two fingers -- fitted with cameras to let troops see what threat is lying ahead.
The army says the nano drone will provide soldiers in the field with an "over the hill, down the road and around the corner" -reconnaissance capability.

It is likely to be used by a special forces combat team of four or five soldiers or by a platoon of 30.

The Australian Defence Force has opened tenders to supply 200 of the tiny helicopters, which The Australian has been told that with control units, batteries and other supporting equipment are likely to cost several million dollars.

One option is the game-changing Black Hornet nano, which was successfully trialled by Australian troops on operations in Afghanistan and Iraq.

The drones, which can help prevent soldiers walking into ambushes, bring back clear images by day or night in close to real time.

The army wants nano drones quiet and small enough to avoid being spotted by an enemy and their cameras sharp enough to collect clear images from at least 1km away and from up to 2.5km in rough terrain or through the windows of high-rise buildings.

It must be possible for troops to launch them while lying down and taking cover in vegetation or rocky terrain.

"It is vital for the patrol not to break from their position and potentially expose themselves to the enemy to use the system," Defence documents say.

The army wants a drone with an encrypted datalink so that an enemy cannot hijack it in flight.

It should also be able to land on a vantage point such as a building or in a tree and to continue to film.

The documents contain scenarios in which the mini spy aircraft could increase troops' safety and capabilities.

A patrol on foot could hide and send out the drone to gather intelligence so that an enemy might never know it was being watched.

Or a unit which comes under fire or which moves into a potential ambush zone can launch the drone to spy on enemy positions.

"The commander uses the data to formulate the assault plan. The team moves into assault positions to clear the enemy while the NUAS (nano unmanned aerial system) loiters to provide situation awareness during the assault."The operator would be able to carry the equipment easily with his normal load of military gear and his rifle and ammunition and would be able to advance with the rest of the unit.

London Times
Putin wages propaganda war on UK
Saturday, 30 July 2016
Byline: Dominic Kennedy

London - President Putin has launched a secret propaganda assault on Britain from within its own borders, The Times can reveal.
The Kremlin is spreading disinformation through a newly opened British bureau for its Sputnik international news service, and is infiltrating elite universities by placing language and cultural centres on campuses.

Analysts said that the push was part of Russia's military doctrine, which specifies the use of "informational and other non-military measures" in conflicts.

Moscow's intelligence agencies were accused by US cybersecurity experts this week of hacking the computer servers of the Democratic National Committee, which has nominated Hillary Clinton as its candidate in November's presidential election.

The release of 20,000 stolen emails, many of them embarrassing to the party's leaders, was blamed on the Kremlin after retrieved data suggested the documents had passed through its computers. It has led to suspicion that Russia is trying to subvert the US political system and gather support for the Republican nominee, Donald Trump.

The Russians' main British target is Edinburgh, which has been chosen as the UK headquarters of Sputnik. Since opening in the city, the news agency has published reports suggesting that the Labour MP Jo Cox may have been killed because of a plot by supporters of the European Union to sway the referendum result, a conspiracy theory that has run on Russian television. It also peddles the myth that the West agreed never to expand Nato to Russia's borders, a key plank of Moscow propaganda to excuse its 2013 invasion of Ukraine.

Sputnik's bureau is in an office building where tenants have minimum leases of five years. Although it is a fringe broadcaster, its stories are picked up by respectable media and politicians. Its immediate

predecessor, Russia's international news agency RIA Novosti, used Scotland as a testing ground for a black propaganda exercise by claiming that the 2014 referendum vote to stay in the UK had been rigged. The spoof story led to a 100,000-name petition for a recount.

It can also be revealed that the University of Edinburgh accepted £221,000 from the Russkiy Mir (Russian World) Foundation to host Britain's first Moscow-sponsored language and cultural centre. The foundation has also opened centres at Durham University, which accepted £85,000, and St Antony's College, Oxford.

Russkiy Mir and Sputnik were created by decrees issued by Mr Putin. Sputnik, which was set up in 2013, is the international wing of a governmentcontrolled news agency. It is headed by Dmitry Kiselyov, who is notorious for his homophobic pronouncements and has been put on an EU sanctions blacklist for being the central propagandist for the Russian invasion of Ukraine.

Russkiy Mir was launched by the president in 2007 and is run by Vyacheslav Nikonov, a former assistant to the Continued on page 2, col 3 Continued from page 1 head of the KGB, the Soviet Union's spy agency. Vladimir Yakunin, a longstanding member of Mr Putin's inner circle, sits on the board of the foundation.

Professor Nikonov, a dean at Moscow State University who outflanks even the president in anti-western rhetoric, is the grandson of Stalin's deputy Vyacheslav Molotov, whose 1939 pact with the Nazis led to the Soviet annexation of the Baltic states. The agreement that Professor Nikonov signed with the university, which awarded him an honorary doctorate in 2012, gives his foundation the right to be consulted on staff appointments at the learning centre in Scotland.

A Nato source accused Russia of "operationalising information" from within Britain. "The Russian information effort is to muddy the waters, to create uncertainty," he said. "Sputnik is part of an overall effort [to] present a Russian view."

Mr Putin backs the concept of a "Russian world", in which the millions of speakers of the language inside and beyond its borders have a shared "living space". His invasion of neighbouring Ukraine was under the pretext of defending the rights of Russian speakers in Crimea, leading to a conflict that has claimed thousands of lives.

Scotland is an attractive strategic target for Russia, which sees Britain -- a nuclear power and permanent member of the United Nations Security Council -- as a check on its ambitions.

The Scottish National Party's desire for independence from the rest of the United Kingdom is compared favourably in Russian media with Crimea's departure from Ukraine. The Trident submarine missile system, which is opposed by the SNP, is based on the River Clyde at Faslane. President Duda of Poland has warned of marked consequences for Nato if Scotland leaves the UK. Scotland also has a ban on

fracking. Some analysts have suggested that a vote for independence would make the country dependent on natural gas from Russia.

The University of Edinburgh said it was working with the foundation on the Russian centre as "part of our wider commitment to increasing the understanding of different parts of the world". The centre "should be judged by its academic and cultural activity, which demonstrates its progressive vision, academic rigour and an evidencebased critique of the regime in Russia". Sputnik said: "We have no preference towards one political force."

The Tory MP Sir Nicholas Soames said: "If people are stupid enough to be suckered by the Russians, that's their lookout."

Washington Post
Snowden, WikiLeaks clash over DNC emails
Saturday, 30 July 2016
Byline: Andrea Peterson

Washington - Two of the biggest names in government data leaks clashed over how to responsibly release information on Twitter late Thursday.
It started when Edward Snowden tweeted that WikiLeaks's "hostility to even modest curation" was a mistake. WikiLeaks wasn't happy about the criticism - and hit Snowden back by accusing him of pandering to Democratic presidential nominee Hillary Clinton.

The spat spotlights a major split between how WikiLeaks and Snowden have handled the data they helped make public. Snowden worked with The Washington Post and other news outlets to expose National Security Agency surveillance programs. The journalists vetted the documents, many of which have not been made public, and chose to withhold some information that government officials said would compromise national security.

WikiLeaks's approach to data disclosure is more radical: It often posts massive, searchable caches online with few, if any, apparent efforts to remove sensitive personal information.

The group's release of emails from the Democratic National Committee exposed information such as the credit card numbers, Social Security numbers and passport numbers of some donors - putting them at risk of identity theft. Some observers, including University of North Carolina at Chapel Hill professor Zeynep Tufekci, also criticized the organization for promoting links to a leaked database containing Turkish citizens' personal information after a recent coup attempt.

WikiLeaks founder Julian Assange was the subject of a U.S. investigation after WikiLeaks posted a cache of diplomatic cables and military documents provided by the now-imprisoned Chelsea Manning - then

known as Bradley Manning - in 2010. Although Assange was not charged, he has accused Clinton of pushing to indict him while she was secretary of state.

WikiLeaks released the DNC emails just before the Democratic National Convention, where Clinton formally received her party's presidential nomination. The Clinton campaign and some cybersecurity experts have alleged that the Russian government was behind the release, possibly in a bid to hurt her candidacy. (Snowden lives in Russia, where he was granted temporary asylum following his NSA disclosures. A WikiLeaks activist accompanied him from Hong Kong to Moscow, making the current tension all the more surprising.)

On Wednesday, Republican nominee Donald Trump publicly urged Russian hackers to go looking for emails from the private server Clinton used during her tenure at the State Department. Trump later defended his comments as being "sarcastic."

ABC News
Predators Exploiting Personal Info in DNC Hack
Sunday, 31 July 2016
Byline: Staff Writer

Washington - The NSA deferred direct questions about its potential involvement in the DNC hack investigation to the FBI, which is the leading agency in that probe. Representatives for the bureau have not returned ABC News' request for comment. Lisa Monaco, President Obama's homeland security and counterterrorism adviser whose responsibilities include cyber policy, declined to comment.
A former senior U.S. official said it was a "fair bet" the NSA was using its hackers' technical prowess to infiltrate two Russian hacking teams that the cybersecurity firm Crowdstrike alleged broke into the DNC's system and were linked to two separate Russian intelligence agencies, as first reported by The Washington Post. In some past unrelated cases, the former official said, NSA hackers have been able to watch from the inside as malicious actors conduct their operations in real time.

Rajesh De, former general counsel at the NSA, said that if the NSA is targeting the Russian groups, it could be doing it under its normal foreign intelligence authorities, as the Russian government is "clearly ... a valid intelligence target." Or the NSA could be working under the FBI's investigative authority and hacking the suspects' systems as part of technical support for investigators, said De, now head of the cyber security practice at the law firm Mayer Brown.

In the aftermath of an attack, a CIA official said that if there is an "overseas component," the NSA would be involved along with the CIA's own newly formed Directorate of Digital Innovation. The two agencies would work, potentially along with others in government, to sniff out suspects' "digital dust."

"It turns out that the people who carry out these activities use their keyboards for other things too," said Sean Roche, Associate Deputy Director for Digital Innovation at the CIA. Any attribution

investigations, Roche said, would also include offline information -- the product of old fashioned, on-the-street intelligence gathering.

Like Joyce, Roche said he was speaking generally and could not comment on the DNC hack.

While U.S. officials have told news outlets anonymously they concur with Crowdstrike and other private cybersecurity firms who have pointed to Russian culpability, the U.S. government has declined to publicly blame the Russians.

The Russian government has said the hacking allegations are "absurd".

Director of National Intelligence James Clapper told the audience at the Aspen Security Forum Thursday that the U.S. intelligence community was "not quite ready to make a call on attribution," though he said there were "just a few usual suspects out there." The next day CIA Director John Brennan said that attribution is "to be determined" and a lot of people were "jumping to conclusions."

Professional hackers often use proxies, Brennan said, so investigators have to make two or three "hops" before tracing cyber attacks back to a state's intelligence agency, which makes the attribution process more difficult.

Kenneth Geers, a former cyber analyst at the Pentagon who recently published a book about Russian cyber operations, told ABC News earlier this week that he didn't necessarily doubt it was the Russians, but said that even in the best cases when doing cyber investigations, "You can have a preponderance of evidence -- and in nation- state cases, that's likely what you'll have -- but that's all you'll have."

That, he said, opens the possibility, however remote, that a very clever hacker or hacking team could be framing the Russians.

Michael Buratowski, the senior vice president of cybersecurity services at Fidelis Cybersecurity which studied some of the malicious code, said the evidence pointing to the Russians was so convincing, "it would have had to have been a very elaborate scheme" for it really to have been anyone else.

The NSA's Joyce said that in general it's very difficult to properly frame someone for a complex attack, since too many details have to be exactly right, requiring a tremendous amount of expertise and precision.

But Joyce said that before the U.S. government pins blame on anyone for a cyber attack publicly, the evidence has to pass an "extremely high bar."

So when they do come forward, he said, perhaps based on the results of attribution techniques that have not been publicly described, "You should bank on it."

New York Times
D.N.C. Hack Raises a Frightening Question: What's Next?
Saturday, 30 July 2016
Byline: Amanda Taub

Analysis: If Russia was indeed behind last week's leak of stolen data from the Democratic National Committee, we may be seeing one of the most sordid tools of its domestic politics deployed as a hostile weapon in foreign policy.
There is a Russian word for this practice: "kompromat." A portmanteau of the Russian words for "compromising" and "material," it refers to the timeworn tradition of obtaining information and using it to smear or influence public officials. Unscrupulous Russian politicians have been doing it for decades; there are kompromat websites (which, unsurprisingly, are often blocked or harassed).

The way it works is simple. First, Kremlin insiders or other powerful individuals buy, steal or manufacture incriminating information about an opponent, an enemy, or any other person who poses a threat to powerful interests. Then, they publish it, destroying the target's reputation in order to settle public scores or manipulate public events.

If American law enforcement officials and analysts are correct in their assessment that Russia was behind this spring's hack of the Democratic National Committee's computer servers, it seems that kompromat is being translated to the international stage.

The United States has had plenty of experience with hackers, government and otherwise, but the D.N.C. hack is something new. Rather than using the information seized for intelligence purposes, the hackers selected damaging excerpts from the cache of stolen data, and then leaked them at a pivotal moment in the presidential election.

And analysts are worried that such activity could soon become a routine element of geopolitics.

"This is not just about the United States, it is not just about Trump or Clinton, or just about American democracy," said Thomas Rid, a professor of security studies at King's College London. "If they consider this a success, they may conclude that, 'Of course, we can do this elsewhere. We can do this again. We can probably also find things, kompromat, on the next president.' "

The risks of weaponizing information

The history of kompromat in Russia shows how damaging this practice can be to democracy and the rule of law.

A 2008 article in Wired, for instance, detailed how the Kremlin leaked footage of a well-known broadcaster at an orgy to a website, apparently in order to relieve the Russian government of a

prominent news media critic. In another case, leaked surveillance video showed a prosecutor investigating high-level official corruption frolicking in bed with two young prostitutes. (The investigation eventually died.)

The term may be Russian, but kompromat is not limited to the country's borders. Chinese officials and businessmen, for instance, have long been rumored to spy on their personal and professional rivals, searching for information that could be used to discredit them.

For instance, Bo Xilai, a senior party official in Chongqing who was jailed for corruption in 2013, reportedly wiretapped a call by China's president at the time, Hu Jintao, as part of a widespread surveillance operation that gathered information on party leaders and other powerful individuals, to aid in Mr. Bo's political ambitions.

Last week's leak of data stolen from the Democratic National Committee fits that pattern, only now it is playing out in a new arena -- in an attack by one state against the political system of another.

A future of D.N.C.-style hacks and leaks

To be sure, history offers numerous examples of countries, including the United States, meddling in one another's elections. But although the aims may not be new, these technological methods and their potential consequences are.

The D.N.C. leak shows that kompromat need not reveal anything illegal to be damaging: The party's chairwoman, Representative Debbie Wasserman Schultz, had to step down after party officials were shown to have taken sides during the primaries. This sets a precedent in which virtually anyone who uses email or social media could be vulnerable to any state or private group with a grudge and access to hackers.

The Chinese and Russians are used to these tactics to settle political and business rivalries. The D.N.C. hack, in exporting kompromat abroad, has established a precedent that may tempt other hackers foreign and domestic, state-sponsored and private.

Because technology makes hacks easier to start than to counter, the risk is difficult to overcome. And anyone with money or expertise can undertake a hack, particularly against nonstate targets that have weaker security systems, and often with little risk of being caught because the attack can be denied.

"In counterintelligence before, there was a kind of granularity of targeting individuals," said Adam Segal, who studies cybersecurity at the Council on Foreign Relations and is the author of "The Hacked World Order." "And now with digital technology, you can do that with a scope and scale you couldn't have done before."

In the past, he pointed out, someone who wanted to obtain lurid details of an adversary's sex life would have had to set up a "honey trap" operation and then photograph the target in flagrante. "But now if you break into someone's email," Mr. Segal noted, "you can find a message that 'so-and-so is an idiot,' or their porn history" -- private, personal information that could be tremendously embarrassing or discrediting if released publicly.

In that climate, everyone who has something to lose, has enemies, or is a public figure is susceptible to this kind of reputational destruction. The higher a person climbs, the greater the risk becomes -- and the greater temptation to a rival.

Uncertainties on responding to hacking

More attacks may already be on the way. Last year, the federal Office of Personnel Management announced that hackers had breached its computers and stolen vast quantities of data gathered for security clearances and background checks.

Mr. Segal said that the stolen data included information on government employees' sex lives, relationships, finances, contacts with foreign governments and a host of other private details.

The data, which goes back to 1985, was gathered so that American counterintelligence officers could assess employees' vulnerability to blackmail. But that well-intentioned project may have ended up conveniently cataloging their most vulnerable points for the hackers.

Government offices and political organizations are hardly the only targets.

In 2014, North Korea hacked Sony Pictures in retaliation for its release of the film "The Interview," a comedy about a plot to assassinate the North Korean leader Kim Jong-un. The trove of released emails included information on salaries, Amazon receipts for a network executive's personal-grooming products, and plenty of embarrassing and offensive conversations. It damaged reputations and careers.

Analysts said hacking is likely to expand in the realm of foreign policy by giving states a new, low-risk method to tweak one another or to meddle in one another's internal affairs. State-sponsored hacks meant to weaponize information are relatively inexpensive and difficult to defend against, making them a tempting tool.

But it is precisely their appeal that gives these tactics the potential to make the international arena more volatile. It is difficult to determine responsibility, which creates a risk that states will punish the wrong culprit -- or respond too harshly, forcing an unintended cycle of escalation.

Because there are no established norms for what is and is not tolerated in such attacks, or for how a targeted state is expected to respond, even the prospect of this kind of hacking creates dangerous uncertainty.

This practice is beyond the reach or enforcement of most laws, and outside the scope of the established norms that limit states' interference in one another's affairs. And because effective defense is so difficult, it is hard to predict what the limits -- or the consequences -- of that might be.

Washington Post
Russian hackers could target voting machines
Sunday, 31 July 2016
Byline: Bruce Shneier

Comment: Russia was behind the hacks into the Democratic National Committee's computer network that led to the release of thousands of internal emails just before the party's convention began, U.S. intelligence agencies have reportedly concluded.
The FBI is investigating. WikiLeaks promises there is more data to come. The political nature of this cyberattack means that Democrats and Republicans are trying to spin this situation as much as possible. Even so, we have to accept that someone is attacking our nation's computer systems in an apparent attempt to influence a presidential election. This kind of cyberattack targets the very core of our democratic process. And it points to the possibility of an even worse problem in November - that our election systems and our voting machines could be vulnerable to a similar attack.

If the intelligence community has indeed ascertained that Russia is to blame, our government needs to decide what to do in response. This is difficult because the attacks are politically partisan, but it is still essential. If foreign governments learn that they can influence our elections with impunity, it will open the door for future manipulations, both document thefts and dumps like this one that we can see and more subtle manipulations that we can't.

Retaliation is a politically fraught step and could have serious consequences, but this was an attack against our democracy. The United States needs to confront Russian President Vladimir Putin in some way - politically, economically or in cyberspace - and make it clear that it will not tolerate this kind of interference by any government. Regardless of your political leanings this time, there's no guarantee the next country that tries to manipulate our elections will prefer the same candidates that you do.

Even more important, we need to secure our election systems before the fall. If Putin's government has already used a cyberattack to attempt to help Donald Trump win, there's no reason to believe it won't do it again - especially now that Trump is inviting the "help," albeit "sarcastically."

Over the years, more and more states have moved to electronic voting machines and have flirted with Internet voting. These systems are insecure and vulnerable to attack.

But while computer security experts like me have sounded the alarm for many years, states have largely ignored the threat, and the machine manufacturers have thrown up enough obfuscating babble that election officials are largely mollified.

We no longer have time for that. We must ignore the machine manufacturers' spurious claims of security, create tiger teams to test the machines' and systems' resistance to attack, drastically increase their cyberdefenses and take them offline if we can't guarantee their security online.

Longer term, we need to return to election systems that are secure from manipulation. This means voting machines with voter- verified paper audit trails, and no Internet voting. I know the old- fashioned way is slower and less convenient, but the security risks are simply too great.

There are other ways to attack our election system on the Internet besides hacking voting machines or changing vote tallies: deleting voter records, hijacking candidate or party websites, targeting and intimidating campaign workers or donors. There have already been multiple instances of political doxing - publishing personal information and documents about a person or organization - and we could easily see more in this election cycle. We need to take these risks much more seriously than before.

Government interference with foreign elections isn't new, and, in fact, that's something the United States itself has repeatedly done. Using cyberattacks to influence elections is newer but has been done before, too - most notably in Latin America. Hacking of voting machines isn't new, either. But what is new is a foreign government interfering with a U.S. national election on a large scale. Our democracy cannot tolerate it, and we as citizens cannot accept it.

In April 2015, the Obama administration issued an executive order outlining how we as a nation respond to cyberattacks against our critical infrastructure. While our election technology was not explicitly mentioned, our political process is certainly critical. And while the technology is a hodgepodge of separate state-run systems, together their security affects every one of us. After everyone has voted, it is essential that both sides believe the election was fair and the results accurate. Otherwise, it will have no legitimacy.

Election security is now a national security issue; federal officials need to take the lead, and they need to do it quickly.

Bruce Schneier is a lecturer at the Kennedy School of Government at Harvard University and the author of "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World."

New York Times
U.S. Wrestles With How to Fight Back Against Cyberattacks
Sunday, 31 July 2016
Byline: David E. Sanger

Aspen, Colo - It has been an open secret throughout the Obama presidency that world powers have escalated their use of cyberpower. But the recent revelations of hacking into Democratic campaign computer systems in an apparent attempt to manipulate the 2016 election is forcing the White House to confront a new question: whether, and if so how, to retaliate.
So far, the administration has stopped short of publicly accusing the Russian government of President Vladimir V. Putin of engineering the theft of research and emails from the Democratic National Committee and hacking into other campaign computer systems. However, private investigators have identified the suspects, and American intelligence agencies have told the White House that they have "high confidence" that the Russian government was responsible.

But suspecting such meddling is different from proving it with a certainty sufficient for any American president to order a response.

Even if officials gather the proof, they may not be able to make their evidence public without tipping off Russia, or its proxies in cyberspace, about how deeply the National Security Agency has penetrated that country's networks. And designing a response that will send a clear message, without prompting escalation or undermining efforts to work with Russia in places like Syria, where Russia is simultaneously an adversary and a partner, is even harder.

The Russians tried to make it tougher still on Saturday when they declared that they had found evidence of American activity in their government systems.

It was hardly a shocking revelation; anyone who leafed through Edward J. Snowden's revelations saw evidence of daily efforts to break into Russian spy agencies, nuclear installations and leadership compounds.

But in a talk on Friday evening at the Aspen Security Forum, an annual gathering that draws many of the nation's top intelligence and military officials, John Brennan, the director of the Central Intelligence Agency, made clear that while spying on each other's political institutions is fair game, making data public -- in true or altered form -- to influence an election is a new level of malicious activity, far different from ordinary spy vs. spy maneuvers.

"When it is determined who is responsible for this," Mr. Brennan said, choosing his words carefully to avoid any direct implication of Russia, there "will be discussions at the highest levels of government about what the right course of action will be. Obviously interference in the U.S. election process is a very, very serious matter."

The Russia problem is thorny, and persistent. Just four months into his presidency in 2009, President Obama and his top national security advisers received a warning from American intelligence agencies: Of all the nations targeting America's computer networks Russia has the most "robust, longstanding

program that combines a patient, multidisciplinary approach to computer network operations with proven access and tradecraft."

Mr. Obama may have been a bit distracted at the time. While setting up his new administration, he was also learning the dark arts of cyberwar, descending into the Situation Room to oversee a complex American-Israeli offensive operation to disable Iran's nuclear centrifuges. He expressed concern to his aides that the operation would help fuel the escalation of cyberattacks and counterattacks.

The concern was justified. Since then, Iran has attacked Saudi Arabia, Russia has brought down a power grid in Ukraine, the North Koreans have attacked the South. The list gets longer every month.

But deterrence has been spotty. In the D.N.C. case, two senior administration officials said midlevel officials were considering options, ranging from counter cyberattacks on the F.S.B. and the G.R.U., two competing Russian spy agencies at the center of the current hacking, to economic, travel and other sanctions aimed at suspected perpetrators.

But each approach has downsides: A counterattack, for example, one senior official said, "brings us to their level, and their moral code."

At the same time, the cost of doing nothing could be high. As the United States and other nations move to more electronic voting systems, the opportunities for mischief rise exponentially. Imagine, for example, a vote as close as the 2000 presidential election between George W. Bush and Al Gore, but with accusations about impossible-to-trace foreign manipulation of the ballots or the vote count, leaving Americans wondering about the validity of the outcome.

For Mr. Obama, the president who has done the most to raise alarms about the risks of cyberattacks and the most to build up the United States Cyber Command, this is fraught territory.

"I think that the administration needs to be ironclad on the evidence here to convince the American people that this is about policy, not politics," said Jason Healey, a scholar at Columbia University who specializes in cyberconflict between nations. "This has got to be about defending a constitutional process, not a party."

Mr. Obama often says the world of cyberconflict is still "the Wild West." There are no treaties, no international laws, just a patchwork set of emerging "norms" of what constitutes acceptable behavior.

For example, Mr. Obama has pressed President Xi Jinping of China to work with the United States and other nations to develop rules about the theft of intellectual property, and about not interfering with a nation's efforts to bring attacked systems back online. Attacking another nation's power grid in peacetime is considered out of bounds.

But every new case brings a new and imaginative way to weaponize cyberpower. Until November 2014, when North Korea hacked into the computers at Sony Pictures Entertainment in retaliation for a comedy that portrayed a C.I.A. plot to assassinate Kim Jung-un, the country's leader, no one seriously considered a movie studio to be "critical infrastructure."

Yet the attack on Sony -- which melted down 70 percent of its computing power -- was the only case that brought the president to the White House press room to accuse another nation of launching a deliberate cyberattack, and to promise retaliation. Mr. Obama said he was driven to go public by the fact that North Korea was trying to suppress free speech and intimidate Americans with threats if they went to the theater.

It is unclear how the United States may have retaliated against the North in secret, if it even did so. But the public punishment, the announcement of some mild economic sanctions, seemed highly ineffective. They were lost in the sea of other sanctions imposed on the North since the signing of the armistice that halted, but did not end, the Korean War 63 years ago.

Yet the decision to name North Korea -- a country with which the United States does no other real business -- was an outlier.

China was never formally named in the theft of the security clearance files on more than 21 million Americans, revealing fingerprints, personal financial details and the personal data about family, friends and former lovers. To James R. Clapper Jr., the director of national intelligence, that wasn't an "attack," it was just very good espionage. Given the chance, he said last year, "we would have done the same thing."

Similarly, the administration decided not to call out Russia when the same intelligence agencies implicated in the D.N.C. attack were believed to be behind the siphoning of tens of thousands of unclassified emails from the systems of the State Department and the White House. There was also a more targeted cyberespionage operation, which investigators attributed to the same actors, aimed at the Joint Chiefs of Staff. But again, it was considered within the bounds of spy vs. spy.

Speaking at the Aspen forum on Thursday, Mr. Clapper, while stepping around who conducted the hack, argued that in Mr. Putin's mind, the United States has meddled in Russian politics, in Ukraine and Georgia -- all part of former Soviet territory. (Mr. Putin complained that Hillary Clinton, in 2011, helped spark protests over a Russian parliamentary election that the United States considered riddled with voter fraud.)

"Of course they see a U.S. conspiracy behind every bush and ascribe far more impact than we're actually guilty of, but that's their mind-set," Mr. Clapper said. "And so I think their approach is they believe we are trying to influence political developments in Russia, trying to affect change, and so their natural response is to retaliate and do unto us as they think we've done unto them."

He later described Mr. Putin as "paranoid" and said "he is less of a throwback to the Communist era, than to the czars." He added later: "He wants to be seen as the leader of a great power, coequal with the United States."

Motherboard Blog
What's the Future of Chinese Hacking?
Saturday, 30 July 2016
Byline: Adam Segal

Analysis: Adam Segal, the Ira A Lipman Chair for Emerging Technologies and National Security and director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations, is the author of The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. After years of public reporting on the theft of intellectual property, business strategies, and trade secrets, last month the cybersecurity firm FireEye issued a report headlining a steep decline in Chinese cyber espionage against organizations in the US and 25 other countries.

The number of network compromises by 72 suspected China-based groups dropped from 60 in February 2013 to less than 10 by May 2016. While FireEye did not rule out the possibility that improvements in tradecraft were leading to less detection (FBI Director James Comey once compared Chinese hackers to drunk burglars who kick in the door and knock over a vase on their way out with the TV), US Assistant Attorney General John Carlin confirmed the company's findings that attacks were less voluminous but more focused and calculated.

A combination of the threat of US sanctions, a diplomatic accord signed by President Barack Obama and President Xi Jinping, and internal reforms of the People's Liberation Army may have temporarily produced a dramatic decline in cyber espionage, but is it time to shut down the firewall, send the threat intelligence analysts home, and declare victory? Very unlikely.

China hacks because it wants to move its economy from labor intensive manufacturing to high technology innovation.

For Beijing, cyberspace is essential to economic growth, sustaining and strengthening the Chinese Communist Party, and maintaining domestic stability and national security. As a result, China hacks because it wants to move its economy from labor intensive manufacturing to high technology innovation; defeat foreign ideologies and weaken opponents of the regime; and counter the technological advantages of the US military in the Pacific.

These fundamental motivations direct state-backed hackers to a set of high value targets. Because Chinese leaders do not want to be dependent on foreign technology suppliers, and are impatient with the results produced so far by massive investments in education and scientific research, Chinese hackers steal intellectual property from high technology companies as well as business secrets from the

pharmaceutical, financial, energy, legal, and other sectors. "The situation that our country is under others' control in core technologies of key fields has not changed fundamentally, and the country's S&T foundation remains weak," President Xi Jinping told a gathering of the nation's top scientists in May 2016. The companies breached are global, with victims identified in Germany, Australia, Japan, India, and the United Kingdom.

Worried about the spread of ideologies that threaten regime legitimacy, and the ability of domestic opponents to organize and foment dissent, Beijing supports cyber attacks on Tibetan and Uighur activists, NGOS and think tanks, and the diplomatic, military, and political agencies of all the major powers. When the New York Times and Bloomberg published stories about the massive wealth amassed by the families of China's top leaders, they, along with other media outlets, were hacked.

Chinese hackers also conduct intelligence and counterintelligence operations. The theft of 22 million records from servers of the Office of Personnel Management included information perfect for blackmail, and might also allow Chinese counterintelligence agencies to identify spies working undercover at US embassies around the world.

Chinese defense planners are preparing the PLA to fight "informationized local wars": short, technologically-intense regional wars. The potential enemy in these future wars is usually referred to as a "technologically advanced" adversary but is clearly a stand-in for the United States and its allies. As a result, these planners want to both understand and disrupt US weapons platforms. Two PLA groups, Units 61938 and 61486, have reportedly stolen information from over two dozen Defense Department weapons programs, including the Patriot missile system, the US Navy's new littoral combat ship, and the F-35 and F-22 stealth fighter jets.

Cyberspace remains central to all of Beijing's predominant economic and political interests, and cyber attacks are, and will continue to be, a potent tool.

If a conflict breaks out over Taiwan or the South China Sea, the PLA will want to disrupt communication, transportation, intelligence, and reconnaissance systems, so hackers have mapped these networks. In addition, Chinese leaders want to signal to US policymakers that the conflict may not stay regional, and so PLA operators have penetrated into banking, energy, and other critical infrastructure networks, and may have intentionally left evidence of the intrusions as a reminder that the US homeland is not immune to attack.

Given Beijing's long-term strategic concerns about technological innovation, domestic stability, and national security, Chinese hackers may change tactics and organization, but they will remain focused on a similar set of targets.The creation of the Strategic Support Forces, a move intended to centralize space, cyber and information warfare troops, will result in greater coordination among the many different hacking groups and better tradecraft overall.

Continued tension over China's sovereignty claims in the South China Sea mean that the networks of the US military and its regional allies will remain prime targets. As the economy moves up the value chain, and as Chinese technology companies like Xiaomi, Huawei, and AliBaba compete in global markets, cyber economic espionage will be narrower and more tailored to specific technologies. The attacks on domestic opponents and outside ideological threats are will become more sophisticated and increase in pace as the Chinese Communist Party appears increasingly worried about domestic stability, regime legitimacy, and the spread of information within China.

Chinese leaders will also be watching closely how the Obama administration responds to the alleged Russian hacking of the Democratic National Committee. Like Moscow, Beijing also believes that it is in an ideological contest with the West and it has tried to shape the information space, though in a more limited way, for example by trolling Tibetan independence activists on Twitter and using distributed denial of service attacks to knock GitHub offline for hosting anti-censorship technology.

However, the complex interdependence of the Chinese and US economies and a greater slate of shared interests in global affairs make a hack as brazen as an effort to influence the US election highly improbable. Still, cyberspace remains central to all of Beijing's predominant economic and political interests, and cyber attacks are, and will continue to be, a potent tool.

The Hacks We Can't See is Motherboard's theme week dedicated to the future of security and the hacks no one's talking about. Follow along here.

Sunday Times (UK)
Kremlin pours cash into media 'black ops' in UK
Sunday, 31 July 2016
Byline: Tom Harper

London - Russia has ramped up spending on foreign information "black ops" by more than £100m. The Kremlin approved a large increase last year in the budget for Russia Today, its English-language channel, and other services, including Sputnik, a news wire service that has opened new headquarters in Edinburgh and which has been accused of running conspiracy stories.

Total spending by Russia on television, radio and online services overseas was projected to be £151m in 2015, but was raised last year to £255m, according to the latest Kremlin budget.

The increase was attributed to the opening of Russia Today's office in London and other "day-and-night channels broadcasting in German and French".

News of the rise in spending comes just days after Curtis Scaparrotti, the new commander of Nato, warned that Moscow was funding "misinformation" campaigns in order to destabilise Europe. In a

speech delivered to a security conference in the US last week, Scaparrotti said Moscow had become an "adversary ... that we need to take very seriously".

He called on the West to mount its own information "black ops" campaigns in order to "meet them in that battlespace", adding: "We see the activities in cyber-space, we see the influence in Europe in terms of political parties' funding, some misinformation to build facts on the ground that really aren't true."

Scaparrotti said the use of such propaganda was an attempt by Russia to "be successful in its objectives without even approaching a conflict".

He added, however: "I think we can deal with it. It's difficult, particularly in the western world, because we believe in freedom of the press, we believe in being truthful in the press, we believe in the rule of law, so we have difficulty in approaching and countering this, but we have to."

US security sources last week accused Russian intelligence agencies of hacking the computer servers of the Democratic National Committee and releasing thousands of damaging emails just as the party was set to confirm Hillary Clinton as its presidential candidate.

The emails, published by the WikiLeaks website, were alleged to be part of a plot to boost the election chances of Clinton's Republican rival, Donald Trump.

It is the latest twist in an "information war" that security analysts say has escalated since the Russian invasion of Ukraine in 2014.

A report by the Chatham House think tank in March accused Russia Today of being a "corrosive" force in the UK.

Shortly before the invasion of Ukraine, a Russian general, Nikolay Bordyuzha, was asked about the Kremlin's propaganda efforts and was quoted as saying: "In information warfare, the side that tells the truth loses."

Washington Post
U.S . can use submarines to monitor and hack other nations ' communications
Sunday, 31 July 2016
Byline: Andrea Peterson & Brian Fung

Washington - When Donald Trump effectively called for Russia to hack into Hillary Clinton's emails last week, the Republican nominee's remarks touched off a (predictable) media firestorm. Here was a presidential candidate from a major U.S. party encouraging a foreign government to target American interests with cyberspying - an act that could not only expose national security information but also potentially undermine the security infrastructure of the United States.

Cyberwarriors working for Moscow and other regimes are already poking and prodding at our networks, so there's little reason to think Trump's words were all that damaging in themselves. But it's a good opportunity to talk about the state of state-sponsored hacking, and to offer a reminder that the United States is just as active in this space as the next government.

The U.S. approach to this digital battleground is pretty advanced. For example: Did you know that the military uses its submarines as underwater hacking platforms?

In fact, subs represent an important component of the United States' cyber strategy. They act defensively to protect themselves and the country from digital attacks, but - more interesting - they also have a role to play in carrying out cyberattacks, according to two U.S. Navy officials at a recent Washington conference.

"There is a - an offensive capability that we are, that we prize very highly," said Rear Adm. Michael Jabaley, the Navy's program executive officer for submarines. "And this is where I really can't talk about much, but suffice to say we have submarines out there on the frontlines that are very involved, at the highest technical level, doing exactly the kind of things that you would want them to do."

The "silent service" has a long history of using information technology to gain an edge on rivals of the United States. In the 1970s, the U.S. government instructed its submarines to tap undersea communications cables off the Russian coast, recording the messages being relayed back and forth between Soviet forces. (The National Security Agency has continued that tradition, monitoring underwater fiber cables as part of its globe-spanning intelligence-gathering apparatus. In some cases, the government has struck closed-door deals with the cable operators ensuring that U.S. spies can gain secure access to the information traveling over those pipes.)

These days, some U.S. subs come equipped with sophisticated antennae that can be used to intercept and manipulate other people's communications traffic, particularly on weak or unencrypted networks.

"We've gone where our targets have gone" - that is to say, online, Stewart Baker, the NSA's former general counsel, said in an interview. "Only the most security-conscious now are completely cut off from the Internet." Cyberattacks are also much easier to carry out than to defend against, he said.

One of America's premier hacker subs, the USS Annapolis, is hooked into a much wider U.S. spying net that was disclosed as part of the 2013 Edward Snowden leaks, according to Adam Weinstein and William Arkin, writing last year for Gawker's intelligence and national security blog, Phase Zero. A leaked slide showed that in a typical week, the Navy performs hundreds of "computer network exploitations," many of which are likely the result of submarine-based hacking.

"Annapolis and its sisters are the infiltrators of the new new of cyber warfare," wrote Arkin and Weinstein, "getting close to whatever enemy - inside their defensive zones - to jam and emit and spoof and hack. They do this through mast-mounted antennas and collection systems atop the conning tower,

some of them one-of- a-kind devices made for hard to reach or specific targets, all of them black boxes of future war."

But even this doesn't compare to what the Navy wants to be able to do next: turn its submarines into motherships for underwater drones that can maneuver themselves closer to shore and conduct jamming or hacking operations while allowing the sub to work at a distance.

"We want the boat to grow longer arms," said Rear Adm. Charles Richard, director of the Navy's undersea warfare division. "We are at all-ahead flank [speed], both on unmanned aerial and undersea vehicles."

It's unclear how far behind - or ahead - other navies may be when it comes to submarine-based cyber offense. Many of the cybersecurity and military experts we interviewed for this report had hardly heard of the Defense Department's undersea cyber capabilities.

But, Baker said, "espionage is a game where there's a lot of following the leader - so it's perfectly possible it's happening in this field, as well."

What is clear is that the U.S. military operates some of the most sophisticated information networks ever designed, and it's using them to penetrate foreign computer systems as part of an evolving cyber strategy.

We may never know precisely what dirt the Pentagon is digging up with its submarine espionage, or be able to draw a link between it and any political or military events in the real world. But despite the rising prominence of Russian hackers in the news - and Chinese hackers before that - it's worth pointing out that the United States has grown fairly proficient in cyberspace, too.

Toronto Star
Travel Smart: Cyberthieves to take advantage of Rio Olympics
Saturday, 30 July 2016
Byline: Henry Stancu

Analysis: Personal safety should be a key concern for anyone at the Olympics in Rio de Janeiro in August, and so should cybersecurity.
The Games will attract not only athletes and spectators, but hackers eager to sniff Wi-Fi traffic, snatch data and infect devices with malware.

So, taking steps to safeguard your digital information is as crucial these days as protecting your money and belongings.

Losing cash, credit cards, a passport or visa to a pickpocket or purse snatcher can ruin a vacation, but identity theft can be even worse, and it can all begin anywhere you use an insecure Wi-Fi hot spot.

On its "Cyber security while travelling website" (travel.gc.ca) , the Government of Canada warns us to "use free computing resources with the assumption that any information you enter could be seen by an unauthorized third party."

The Rio Olympics will no doubt be third- party central in terms of hackers.

Just as it's smart to travel with as few valuables as possible to cut the risk of losing them or having them stolen, the same goes for the amount and sensitivity of data you take with you.

Many countries monitor information passing through their networks, so travellers must realize any personal or corporate data stored on devices can be compromised.

Mobile devices can be hijacked and infected with malware, used to track the owner's movements via GPS, and to even activate the device's microphone or camera. Hackers can intercept personal communications and use the devices to also infect connected networks.

Not only are things such as tablets, laptops and smartphones prime targets for data theft, but we should assume arenas, hotels, internet cafés and any public Wi-Fi spots are fishing holes for cyberscammers.

In fact, hackers have been known to set up free internet hot spots for the express purpose of attracting prey, by naming their Wi-Fi access points to appear related to a hotel or legitimate business.

"Hotel Lux Wi-Fi" may be legit, but "Secure Hotel Lux Wi-Fi" could be the bait.

The best way to protect your data is to leave your devices at home, and the second best way is to keep any vital information backed up on your home computer or hard drive rather than on the smartphone you travel with.

You can join a VPN (virtual private network) service, which encrypts data between devices and the internet while hiding customers' IP addresses. Some charge a membership fee and some offer free online subscriptions.

Check user ratings and specs on sites such as vpncomparison.org (www.vpncomparison.org) , because some VPN services have been known to be questionable.

Communication Security Establishment Canada (CSEC), the organization that looks after the protection of electronic information at the national level, has the following tips for travellers:

Password protect your device and change the password before setting out on a trip. It's also a good idea to periodically change your password when you get back.

Identify the device as your property and how you can be contacted if it is lost. The information can be engraved on the device or on a sticker attached to it, or highlighted in a screen saver. That way, if an honest person finds it they'll know how to get in touch.

Set your device to erase all the data if invalid passwords have been entered after a number of failed attempts.

Enable your device's location detection and anti-theft features, such as data encryption.

Don't leave your device unattended but if you have to, remove the battery, expanded memory and SIM card and keep them with you.

Find out from your phone/internet service provider, or your company's IT department, whether your device will work at your destination before you head out.

Don't ever charge your device via a USB connection of an unknown or unsecured computer.

An insecure Bluetooth setting leaves a device vulnerable to hacking. Disable the function before a trip.

Sunday Telegraph (UK)
PM demanded vetting of Chinese investors.
Sunday, 31 July 2016
Byline: Tim Ross

London - Theresa May privately demanded strict new national security checks on Chinese companies seeking to take over British industries, a former cabinet colleague has revealed.
Sir Vince Cable, business secretary until last year, suggested the Prime Minister had a "general prejudice" against Chinese investments in Britain and wanted to emulate American rules banning foreign takeovers that could undermine security.

The disclosure came after Mrs May delayed a decision on whether to allow the China-backed Hinkley Point nuclear project to go ahead. Speaking to The Sunday Telegraph, Sir Vince detailed Mrs May's long-held security concerns over China's involvement in the £18 billion nuclear power plant in Somerset and other business links with China.

He said she was "never completely satisfied about Huawei", the Chinese telecommunications giant, which has a major partnership with BT.

"I and others thought they were a good thing but I think she was worried about them," he said.

During private cabinet talks, she was also reluctant to relax visa rules for Chinese businessmen, he said.

However, George Osborne, the then chancellor, overruled her and pursued what she saw as a "gung-ho" approach to wooing Chinese investment, Sir Vince said. "She has expressed in several different contexts severe reservations about China getting too close to the UK," he said.

Sir Vince argued Mrs May's stance was "bound to" lead to a cooling in relations between the UK and China, putting in doubt Chinese plans to invest tens of billions of pounds in Britain.

His comments came after the Government announced on Thursday it would delay the final decision on approving the deal on the Hinkley C power station, which would be Britain's first new nuclear plant for a generation.

Downing Street insists that Mrs May Prime Minister wanted tighter screening but was overruled by Cameron and Osborne, Sir Vince says wants to examine all of the "component parts" of the deal with the French firm EDF before deciding whether to give it the green light.

However, government sources suggest Mrs May has concerns over the security implications of allowing China's state-owned companies to take a 33.5 per cent stake in Hinkley Point and to have the opportunity to design and build a new reactor in Essex.

Sir Vince, who served alongside Mrs May in the cabinet throughout the 2010- 2015 coalition, said the Prime Minister had been unhappy with the positive attitude of David Cameron and George Osborne towards Chinese investments while she was home secretary.

He said: "Fairly early on in the coalition, she wanted to introduce a more stringent test of foreign investment, based on the American model of screening out projects that threaten national security."

Mrs May was "very hot" on this issue, he said, but "was basically overruled by Osborne and my own department".

"Secondly, my recollection was that when approval was sought for Hinkley, she raised objections on grounds of national security issues and China."

Nick Timothy, Mrs May's joint chief of staff, has said MI5 held concerns over China'sbecause Chinese intelligence services are working "against British interests at home and abroad".

He warned in an article before he began working in Downing Street that the Chinese could use their role in the Hinkley nuclear programme to "build weaknesses into computer systems which will allow them to shut down Britain's energy production at will".

Government sources confirmed that the national security issue was one of many questions the Prime Minister wanted to examine before approving the plan for Hinkley.

But it raised questions over whether she could also object to £40billion of other Chinese investments in the UK, which were announced last year. Mr Osborne had been encouraging Chinese companies to invest in the High Speed 2 rail project .

Sir Vince said Mrs May's new approach could put other investments in doubt and create difficulties for the relationship between the two countries .

"It's bound to affect it negatively for two reasons: one that Osborne isn't there and he was the main champion.

I supported him but we are no longer there. Secondly, "She has expressed in several different contexts severe reservations about China getting too close to the UK," he said. "It came up in all kinds of different ways.

Osborne kept pushing for more liberal treatment of visas for Chinese businessmenand she was very reluctant to go along with that.

So I think she has form in adopting a more suspicious approach, more in line with the American position." Last night, Downing Street declined to comment on Sir Vince's disclosures.

The chief executive of EDF yesterday attempted to downplay the signifi- cance of the Hinkley delay, insisting that he understood the Government's desire for more time.

Vincent de Rivaz has written to workers in an attempt to reassure them that the project is still "strong" despite the unexpected delay.

The company's board narrowly voted on Thursday to give the final go-ahead to the long-delayed project but the Government pulled back from signing the contract, saying it would make a decision in the early autumn.

Mr de Rivaz said: "The new Prime Minister has been in post for just 16 days. Her full Cabinet has been in post even fewer.

"We can understand their need to take a little time. We fully respect the Prime Minister's method. The very good news is that we are ready. The board's decision means that when the Government is ready to go ahead, we are ready too."

Mr de Rivaz said he had met Greg Clark, the Business and Energy Secretary, after the minister announced the Government would "consider carefully" all parts of the project before making a decision.

Jason Millett, chief operating officer for major programmes and infrastructure at Mace, a major contractor at Hinkley Point, said the decision to delay it had left people "bewildered".

Osborne kept pushing for liberal treatment of visas for Chinese businessmenand she was reluctant'

The Australian
Australian to head Lockheed Martin research lab
Friday, 05 August 2016
Byline: Brendan Nicholson

Canberra - A top Australian defence scientists will run the new research laboratory to be set up in Melbourne by US aerospace and defence giant Lockheed Martin.
Tony Lindsay, who now heads the national security and intelligence, surveillance and recon-naissance division of the Defence Department's Defence Science and Technology Group, will be the director of the Lockheed Martin Science Technology Engineering Leadership and Research Laboratory -- or STELaR Lab.

Dr Lindsay's 30-year engagement with research includes time as Defence's top science diplomat at the Australian Embassy in Washington.

He is considered a world expert in electronic warfare and intelligence, surveillance and reconnaissance. Dr Lindsay will set up the lab and oversee research and development programs including hypersonics, autonomy, robotics, and command, control, communications, computing, intelligence, surveillance and reconnaissance.

Lockheed Martin picked Melbourne as the location for an advanced research and development facility because it viewed the city as one of the world's most advanced university research centres.

The chief executive of Lockheed Martin Australia and New Zealand, Raydon Gates, said this would be the first such centre Lockheed Martin had established outside the US and that the lab had followed a rigorous internal evaluation process.

Mr Gates said Melbourne was one of the strongest-performing university cities in the world -- third only behind Boston and London. He said the centre based there would be able to attract world-beating scientists and researchers.

Mr Gates said the selection of Dr Lindsay was evidence of the depth of Australia's world-class science and technology leadership. "I am proud we were able to identify such a strong homegrown candidate to establish this leading-edge facility, which is a further endorsement of Australia's global reputation for research," he said.

Dr Lindsay said the company's reputation for research and development was unparalleled and its decision to invest in Australia by establishing the new lab had been enthusiastically welcomed by the local research community.Lockheed Martin chief technology officer Keoki Jackson said Melbourne's growing international reputation for research was a key factor in the choice of the laboratory's location. "Australia is recognised as a world research leader in fields from engineering and computer science to physics, space science and molecular biology," Dr Jackson said.

The Hindustan Times
Kaspersky Lab announces Bug Bounty Program with HackerOne
Friday, 05 August 2016

Undisclosed placeline - Kaspersky Lab announces Bug Bounty Program with HackerOne has announced at the Black Hat USA Conference the launch of the Kaspersky Lab Bug Bounty Program with HackerOne, an industry leading bug bounty platform provider. With this program, Kaspersky Lab will not only further bolster its mitigation strategy for addressing inherent software vulnerabilities, but also continue enhancing its relationship with external security researchers.
Today's cyber threat landscape is becoming increasingly complex, requiring security companies to continuously identify and implement effective tools in order to provide the most robust level of protection. Bug bounty programs are an effective and proven security measure that incentivizes external researchers to safely find and disclose software vulnerabilities to companies. As a result, these organizations are able to fix the reported issues without placing customers at risk.

The first phase of the Kaspersky Lab bug bounty program will officially began on August 2, 2016 and will last for a six-month period. During this initial phase, Kaspersky Lab will offer a total of $50,000 in bounty rewards to security researchers. Bug bounty participants will examine our flagship products for consumers and enterprises, Kaspersky Internet Security and Kaspersky Endpoint Security. After the preliminary phase is complete, the company will evaluate the results to determine what additional products and rewards should be included in the second phase of its bounty program.

"Our bug bounty program will help amplify the current internal and external mitigation measures we use to continuously improve the resiliency of our products," said Nikita Shvetsov, chief technology officer, Kaspersky Lab. "We think it's time for all security companies, large and small, to work more closely with external security researchers by embracing bug bounty programs as an effective and necessary tool to help keep their products secure and their customers protected."

"Vulnerabilities are inevitable and bug bounty programs are proven to supplement traditional security best practices with the help of the incredibly diverse global hacker community," said Alex Rice, CTO and co-founder, HackerOne. "We look forward to partnering with Kaspersky Lab to help them run the most competitive bug bounty program and continue to protect customers.".

Haaretz
ISIS Plans Attack on U.S. Air Bases, Israeli Intel Firm Says (Canada).
Friday, 05 August 2016

Jerusalem - An Israeli cyber intelligence company claims it has hacked ISIS communications and learned about the group's plans to attack U.S. air bases in Kuwait, Bahrain and Saudi Arabia.

Intsights, which is run by former Israel Defense Forces intelligence officers and based in Herzliya, said Wednesday it had hacked the forum on which ISIS operatives publish terror attack plans, Channel 10 reported.

According to Intsights, ISIS uploads potential targets to the forum, hosted through the Telegram encrypted messaging app. Some targets listed there, such as the church in Normandy, France where a priest was murdered on July 26, have been attacked after appearing on the site.

"Telegram is completely encrypted and there's no fear that someone will intercept the messages and understand what you wrote," Intsight co-founder Alon Arvatz told Channel 10.

The Intsight team did not say how it managed to hack into the group.

Arvatz said that a map uploaded to the ISIS' Telegram forum identifies air force bases in the United States, Canada, United Kingdom and other Western European countries, as well as Israeli air force bases.

Times of Israel
BioCatch tracks memory use to catch cybercrooks
Friday, 05 August 2016
Byline: Shoshanna Solomon

Jerusalem - Did you know that everyone has a distinctive way of moving a mouse, tapping a phone or typing on a keyboard? Moreover, when you identify yourself to your bank or an online store by inserting information about yourself, like your home address or date of birth, you are using long- term memory rather than short-term, and this can be seen from the way you interact with your computer or smartphone. In fact, that's what Israeli start-up BioCatch uses to distinguish the bad guys from the good guys.
The company's latest product, which is already deployed in a set of tier- one banks and eCommerce customers, "differentiates between good users and criminal users, for situations where there is no historic data about these first time visitors," said Avi Turgeman, the founder of Tel Aviv based BioCatch, a financial security tech firm.

The company has already been selling software that checks over 500 bio-behavioral, cognitive and physiological parameters to create unique user profiles -- and an individual web presence -- for visitors to banking and eCommerce sites.

BioCatch is able to continuously authenticate users at every stage of an online banking session by analyzing these parameters, including hand tremors, eye-hand coordination, and how a person moves a mouse, combined with behavioral traits such as usage preferences and device interaction patterns. This enables the creation of what BioCatch calls a Cognitive Signature, a sum total of all the factors that go into an interactive session.

BioCatch's technology can record all this information, associating it with the user who is logged in and interacting with the site. In this way, banks or e-commerce sites can be alerted if the person performing the actions isn't who they should be, for example. The company has already been marketing its continuous authentication software and its malware and RAT detection products to banks and other customers globally.

At the end of 2015 there were more than 33 million banking customers globally using the company's behavioral biometric software, the company said. Its customers include some of the largest banks and eCommerce sites in Europe, Latin America and North America.

BioCatch's latest software, called Criminal Behavior, comes at a good time. Cyber crime will cost businesses over $2 trillion by 2019, market analysts Juniper Research has forecast, almost four times the cost of breaches in 2015.

"Today, with so much personal, financial and sensitive data open to potential threats, BioCatch uses unique personal behavioral metrics to continuously ensure that the individuals accessing their accounts are in fact who they say they are, thereby preventing security breaches before they happen and saving companies losses of millions of dollars in fraudulent activities," said Pini Lozowick, Chief Investment Officer at OurCrowd, an investor and member of the board of BioCatch, by email.

Biocatch's Criminal Behavior software is based on behavior patterns that emerged from the data the company has collected from interactions of people with their computers and phones. The data shows that interactions differ when users use short-term vs long-term memory: most people remember their birthdays and addresses without needing to check them first, before they tap them into the computer. Their credit card information, however, is stored in their short-term memories. They generally need to check the number before they click it into their phone or computers while performing a transaction.

So behavior and interaction with a device is different when using short- term vs long-term memory, though Turgeman declined to say how exactly so as not to give out too much information that would help criminal activity. And here is the clinch, because the bad guys, the impostors, only have short- term memory of your details, and the BioCatch software can home in on those behaviors that should be long-term but are actually short-term, alerting the vendors or the banks that the person in question could be an impostor.

"Today when someone is requesting an online loan or opening a new digital bank account, there is no way to know if this first-time visitor is actually who they say they are. It could be a fraudster using a stolen identity," Turgeman said. "But criminals, when impersonating a person they are not familiar with, behave very differently from an innocent user. One example is that they don't hold the details of that person in their long term memory, and that has a dramatic influence on how their interactions look, and allows us to know if the user is a criminal or not."

Other times, cyber criminals who are generally well prepared before an attack reveal that they actually know too much, and fill in the forms too quickly and perfectly.

BioCatch, which has raised a total of about $12 million from investors to date and employs 40 people in Tel Aviv, London, New York and Boston, is targeting banks and eCommerce sites for its latest product.

"The virtual world of the internet and mobile are still protected by security systems devised for the physical world," Turgeman said. "Most of the cyber security solutions try to replicate security concepts from the physical world in the virtual world. But walls and gates in the virtual world are simply made of bits and bytes, and these can be manipulated."

"Today, in the cyber space, fraudsters can enter into secured environments via the 'virtual gates,' almost hand in hand with the authorized users, or just right after them, without anyone noticing," Turgeman said. "Therefore the only way to truly protect the users' identity in the cyber space is through continuous authentication based on user activity, and this is what we do."

Gulf News
Criminals turn focus on Bitcoin
Friday, 05 August 2016
Byline: Naushad K. Cherrayil

Dubai - On Wednesday, Hong Kong-based exchange -- Bitfinex -- halted trading after hackers stole about $65 million of the digital currency Bitcoin.
It's the second major attack on Bitcoin technology, called Blockchain, this year. In July, criminals managed to steal over $50 million from a project called the Decentralised Autonomous Organisation.

Blockchain technology is fast emerging as a key area of financial technology (fintech) innovation. The technology behind Blockchain has created huge interest in everything from digital currencies to commodities trading to insurance. In simple terms, Blockchain is a cloud-based encrypted database used to record and analyse data.

Moe Levin, a member of the UAE- based Global Blockchain Council, said that blockchain is the greatest invention since the internet and has revolutionised and simplified the process of conducting financial interactions between organisations.

He said that Bitcoin and Blockchain are still in a nascent stage in the region, and the UAE is the first country to actively take the next step and encourage use of Blockchain.

As of first quarter this year, Levin said that total venture capital investment in Bitcoin and Blockchain start-ups now exceeds $1.1 billion.

Bitfinex said it was still investigating details and cooperating with law enforcement, but acknowledged 119,756 bitcoin, or about $65 million at current prices, was stolen. Bitcoin slumped 5.5 per cent against the dollar as of 2:30pm on Wednesday in Tokyo, bringing its two-day drop to 13 per cent.

"Yes -- it is a large breach," Fred Ehrsam, co-founder of Coinbase, a cryptocurrency wallet and trading platform, wrote in an email to Bloomberg. "Bitfinex is a large exchange, so it is a significant short term event, although Bitcoin has shown its resiliency to these sorts of events in the past."

Nicolai Solling, chief technology officer at security solutions provider Help AG Middle East, said that he doesn't think Bitcoin hacking is likely to stop in the near future. He said it is relatively a young currency, adding that when e-banking systems were introduced, there were lot of vulnerabilities in the system.

He believes this will take time to fix. Since digital currencies are traded anonymously, he said, this makes it even more difficult to find the hacker.

Many in the tech industry have criticised the anonymity of these transactions but that is the way Blockchain and similar technologies were designed to work, he said.

Ramez Shehadi, Executive Vice-President and Managing Director of Booz Allen Hamilton Mena, said that an increasingly digital economy has called cybersecurity risks into sharper focus. Annual losses to companies worldwide from cyberattacks now exceed $7.7 million on average per organisation, according to the Ponemon Institute.

London Times
Israelis crack secret message app used by Islamic State terrorists
Friday, 05 August 2016
Byline: Multiple reporters

Tel Aviv - An Israeli cyber-intelligence company claims to have penetrated a private messaging forum used by Islamic State to plan and inspire attacks against "extremely specific" western targets, including American military bases in the Middle East.
Intsights, which is run by former intelligence officers from the Israel defence forces, said that it had discovered the list on an encrypted channel on Telegram, a popular messaging app, used by more than 500 members of the jihadist group across the globe.

The list was said to include the locations of numerous US air force bases, with particular attention to those in the Gulf states of Saudi Arabia, Bahrain and Kuwait.

Several of the plots discussed on the channel this year eventually came to fruition, such as the attack on a church in Normandy last week, where two young men slit the throat of a priest.

Telegram has become a communication channel for Isis supporters because it uses end-to-end encryption, making it hard for the authorities to intercept messages easily. For the same reason, it is also used by human rights activists in repressive regimes such as Iran and Saudi Arabia. "Telegram is completely encrypted and there's no fear that someone will intercept the messages and understand what you wrote," Alon Arvatz, the service's co-founder, told Israel's Channel 10.

Intsights did not reveal exactly how it gained access to the channel, whether through hacking or by infiltrating the network by posing as an Isis supporter or potential recruit. Isis defectors and prisoners have said that such access requires at least one level of verification from a trusted Isis member.

Mr Arvatz said they had discovered that the Normandy attack was discussed several months ago, suggesting that the target may have been chosen by Isis long before any individuals were commissioned or inspired to carry it out. French investigators who examined a mobile phone belonging to one of the jihadists, Adel Kermiche, believe that he began communicating with his associate on Telegram only four days before the attack.

The Israeli claims underline the fear of European security forces that services such as Telegram have become vital technology for the Isis arm known as Emni, which has been described by a captured French jihadist as "the secret service for the exterior of the Islamic State".

Investigators are still teasing out to what degree secret encrypted channels are used to inspire, direct or commission specific attacks. Other, more open, channels, many of which have been closed down only to resurface with minor name changes, trade in the kind of propaganda Isis uses to encourage supporters.

One German former Emni operative, now in custody, told The New York Times that services such as Telegram were seen as crucial for future attacks on American soil.

Last night President Obama pledged that both Mosul in Iraq and Raqqa in Syria would be recaptured, but he warned that the group's violent ideology would continue even if they lost their main strongholds

.Egypt's military said that Abu Doaa al-Ansari, the leader of Islamic State's local affiliate has been killed in the Sinai peninsula, along with several key aides and 45 other members of the group. Officials said al-Ansari and his aides were killed in an airstrike that targeted a house located amid olive groves south of el-Arish. Aerial images of the strike released by the military appeared to confirm the account.

NBC News
More Than 1,000 U.S. Spies in Brazil Protecting Rio Olympics
Friday, 05 August 2016
Byline: Robert Windrem, William Arkin

New York - U.S. intelligence has assigned more than 1,000 spies to Olympic security as part of a highly classified effort to protect the Rio 2016 Summer Games and American athletes and staff, NBC News has learned.
Hundreds of analysts, law enforcement and special operations personnel are already on the ground in Rio de Janeiro, according to an exclusive NBC News review of a highly classified report on U.S. intelligence efforts.

In addition, more than a dozen highly trained Navy and Marine Corps commandos from the U.S. Special Operations Command are in Brazil, working with the Brazilian Federal Police and the Brazilian Navy, according to senior military officials.

The U.S. military, as expected, has placed larger military units on call should a rescue or counterterrorism operation be needed, the officials said.

The classified report outlines an operation that encompasses all 17 U.S. intelligence agencies, including those of the armed services, and involves human intelligence, spy satellites, electronic eavesdropping, and cyber and social media monitoring.

Areas of cooperation include vetting 10,000-plus athletes and 35,000-plus security and police personnel and others; monitoring terrorists' social media accounts; and offering U.S. help in securing computer networks, the review shows.

"U.S. intelligence agencies are working closely with Brazilian intelligence officials to support their efforts to identify and disrupt potential threats to the Olympic Games in Rio," said Richard Kolko, a spokesman for National Intelligence Director James Clapper.

The operation is being conducted with the full cooperation of the Brazilian government.

"U.S. intelligence cooperation with Brazil has been excellent since 9/11," a senior intelligence official said, adding, "We consider the Brazilians to be well-prepared and highly professional."

There is no indication of any specific plot against the Games, which officially kick off with Friday's opening ceremonies.

But two weeks ago, Brazilian authorities detained a dozen Rio residents for alleged ties to the Islamic State and arrested a Brazilian of Lebanese descent for alleged links to ISIS. Brazil's justice minister described those arrested as "amateurs" but noted they had discussed attacking the Olympics. U.S. intelligence documents from March also identify Hezbollah activity in Brazil.

Another U.S. intelligence official told NBC News that the U.S. has not seen "any threats" of an ISIS attack, contrasting the Olympics with the EuroCup soccer championship last month in France, "which was overlaid with the ISIS threat profile."

According to the intelligence review, the U.S. put a 24/7 multi- agency "Olympic Watch" in place late last year, involving all agencies of the intelligence and law enforcement communities, including the CIA, the NSA, the Secret Service, the FBI. It also included the National Reconnaissance Office, responsible for spy satellites, and the National Geospatial Intelligence Agency, in charge of imagery interpretation.

The NSA, America's eavesdropping agency, is the lead agency and played the "leading role for the [intelligence community] in the Olympics since the 1984 Los Angeles games," the review said. Officials told NBC News that the NSA has proven most able to provide unique intelligence on the ground and real-time warnings that the host nations can't provide themselves.

The U.S. is one of 51 countries supplying intelligence to the Brazilian counter terrorism effort, but the American effort is second only to the Brazilians' operation. According to senior U.S. intelligence officials, 800 intelligence professionals, mostly analysts operating in the U.S., have been assigned and another 350 are on the ground supporting U.S., Brazilian and International Olympic Committee efforts.

The official noted that the each of the U.S. military services have athletes participating in the Olympics, including shooting, men and women's boxing, and wrestling competitions. "We have actual equities involved," said the official in explaining the breadth and depth of the operation.

Reuters
The world's best cyber army doesn't belong to Russia
Thursday, 04 August 2016
Byline: James Bamford

Comment - National attention is focused on Russian eavesdroppers' possible targeting of U.S. presidential candidates and the Democratic Congressional Campaign Committee. Yet, leaked top-secret National Security Agency documents show that the Obama administration has long been involved in major bugging operations against the election campaigns -- and the presidents -- of even its closest allies.
The United States is, by far, the world's most aggressive nation when it comes to cyberspying and cyberwarfare. The National Security Agency has been eavesdropping on foreign cities, politicians, elections and entire countries since it first turned on its receivers in 1952. Just as other countries, including Russia, attempt to do to the United States. What is new is a country leaking the intercepts back to the public of the target nation through a middleperson.

There is a strange irony in this. Russia, if it is actually involved in the hacking of the computers of the Democratic National Committee, could be attempting to influence a U.S. election by leaking to the American public the falsehoods of its leaders. This is a tactic Washington used against the Soviet Union and other countries during the Cold War.

In the 1950s, for example, President Harry S Truman created the Campaign of Truth to reveal to the Russian people the "Big Lies" of their government. Washington had often discovered these lies through eavesdropping and other espionage.

Today, the United States has morphed from a Cold War, and in some cases a hot war, into a cyberwar, with computer coding replacing bullets and bombs. Yet the American public manages to be "shocked, shocked" that a foreign country would attempt to conduct cyberespionage on the United States.

NSA operations have, for example, recently delved into elections in Mexico, targeting its last presidential campaign. According to a top-secret PowerPoint presentation leaked by former NSA contract employee Edward Snowden, the operation involved a "surge effort against one of Mexico's leading presidential candidates, Enrique Peña Nieto, and nine of his close associates." Peña won that election and is now Mexico's president.

The NSA identified Peña's cellphone and those of his associates using advanced software that can filter out specific phones from the swarm around the candidate. These lines were then targeted. The technology, one NSA analyst noted, "might find a needle in a haystack." The analyst described it as "a repeatable and efficient" process.

The eavesdroppers also succeeded in intercepting 85,489 text messages, a Der Spiegel article noted.

Another NSA operation, begun in May 2010 and codenamed FLATLIQUID, targeted Pena's predecessor, President Felipe Calderon. The NSA, the documents revealed, was able "to gain first-ever access to President Felipe Calderon's public email account."

At the same time, members of a highly secret joint NSA/CIA organization, called the Special Collection Service, are based in the U.S. embassy in Mexico City and other U.S. embassies around the world. It targets local government communications, as well as foreign embassies nearby. For Mexico, additional eavesdropping, and much of the analysis, is conducted by NSA Texas, a large listening post in San Antonio that focuses on the Caribbean, Central America and South America.

Unlike the Defense Department's Pentagon, the headquarters of the cyberspies fills an entire secret city. Located in Fort Meade, Maryland, halfway between Washington and Baltimore, Maryland, NSA's headquarters consists of scores of heavily guarded buildings. The site even boasts its own police force and post office.

And it is about to grow considerably bigger, now that the NSA cyberspies have merged with the cyberwarriors of U.S. Cyber Command, which controls its own Cyber Army, Cyber Navy, Cyber Air Force and Cyber Marine Corps, all armed with state-of-the-art cyberweapons. In charge of it all is a four-star admiral, Michael S. Rogers.

Now under construction inside NSA's secret city, Cyber Command's new $3.2- billion headquarters is to include 14 buildings, 11 parking garages and an enormous cyberbrain -- a 600,000- square-foot, $896.5-million supercomputer facility that will eat up an enormous amount of power, about 60 megawatts. This is enough electricity to power a city of more than 40,000 homes.

In 2014, for a cover story in Wired and a PBS documentary, I spent three days in Moscow with Snowden, whose last NSA job was as a contract cyberwarrior. I was also granted rare access to his archive of documents. "Cyber Command itself has always been branded in a sort of misleading way from its very inception," Snowden told me. "It's an attack agency. ... It's all about computer-network attack and computer-network exploitation at Cyber Command."

The idea is to turn the Internet from a worldwide web of information into a global battlefield for war. "The next major conflict will start in cyberspace," says one of the secret NSA documents. One key phrase within Cyber Command documents is "Information Dominance."

The Cyber Navy, for example, calls itself the Information Dominance Corps. The Cyber Army is providing frontline troops with the option of requesting "cyberfire support" from Cyber Command, in much the same way it requests air and artillery support. And the Cyber Air Force is pledged to "dominate cyberspace" just as "today we dominate air and space."

Among the tools at their disposal is one called Passionatepolka, designed to "remotely brick network cards." "Bricking" a computer means destroying it - turning it into a brick.

One such situation took place in war-torn Syria in 2012, according to Snowden, when the NSA attempted to remotely and secretly install an "exploit," or bug, into the computer system of a major Internet provider. This was expected to provide access to email and other Internet traffic across much of Syria. But something went wrong. Instead, the computers were bricked. It took down the Internet across the country for a period of time.

While Cyber Command executes attacks, the National Security Agency seems more interested in tracking virtually everyone connected to the Internet, according to the documents.

One top- secret operation, code-named TreasureMap, is designed to have a "capability for building a near real-time interactive map of the global Internet. ... Any device, anywhere, all the time." Another operation, codenamed Turbine, involves secretly placing "millions of implants" -- malware -- in computer systems worldwide for either spying or cyberattacks.

Yet, even as the U.S. government continues building robust eavesdropping and attack systems, it looks like there has been far less focus on security at home. One benefit of the cyber-theft of the Democratic National Committee emails might be that it helps open a public dialogue about the dangerous potential of cyberwarfare. This is long overdue. The possible security problems for the U.S. presidential election in November are already being discussed.

Yet there can never be a useful discussion on the topic if the Obama administration continues to point fingers at other countries without admitting that Washington is engaged heavily in cyberspying and cyberwarfare.

In fact, the United States is the only country ever to launch an actual cyberwar -- when the Obama administration used a cyberattack to destroy thousands of centrifuges, used for nuclear enrichment, in Iran. This was an illegal act of war, according to the Defense Department's own definition.

Given the news reports that many more DNC emails are waiting to be leaked as the presidential election draws closer, there will likely be many more reminders of the need for a public dialogue on cybersecurity and cyberwarfare before November.

Note: (James Bamford is the author of The Shadow Factory: The Ultra-Secret NSA From 9/11 to the Eavesdropping on America. He is a columnist for Foreign Policy magazine.)

Washington Post
Policy on drone strikes is declassified
Sunday, 07 August 2016
Byline: Karen DeYoung

Washington - President Obama must approve operational plans to target overseas terrorist suspects with drones or other weapons outside war zones but in some cases does not sign off on specific strikes, according to newly declassified administration guidelines.

In addition to setting out the role of the president, the guidelines emphasize the importance of "verifying" the identity of high-value targets, even as they outline the criteria and legality of striking unidentified others when "necessary to achieve U.S. policy objectives."

The guidelines provide rules for targeting U.S. citizens abroad and include lengthy guidance on what to do with captured terrorist suspects. "In no event," the document says, "will additional detainees be brought to the detention facilities at the Guantanamo Bay Naval Base."

The 18-page top-secret document was declassified and released late Friday, with relatively minor redactions, in response to a federal court order. When Obama signed the guidelines, in May 2013, the administration released a brief "fact sheet" on procedures and criteria for such operations that were drawn from the classified version.

Those rules included "near certainty" that the terrorist target was present and that no civilians would be injured or killed, that the target posed a "continuing and imminent" threat to Americans, that capture was not feasible, and that all relevant domestic and international laws were obeyed.

Since then, the president has made clear that he anticipates the more detailed, newly declassified procedures will govern future administrations. "My hope is, is that by the time I leave office, there is not only an internal structure in place that governs these standards that we've set, but there is also an institutionalized process" to increase transparency and oversight of lethal action outside war zones abroad.

There is no legal requirement that Obama's successors adhere to the same rules. But administration officials, speaking on the condition of anonymity about internal discussions, have said that compilation of the guidelines, and making them public, will restrain other presidents.

"The president has emphasized that the U.S. government should be as transparent as possible with the American people about our counterterrorism operations, the manner in which they are conducted and their results," National Security Council spokesman Ned Price said of the new release.

"Our counterterrorism actions are effective and legal, and their legitimacy is best demonstrated by making public more information about these actions, as well as setting clear standards for other nations to follow," he said.

Despite its pledges of transparency, the administration has waited until Obama's waning months in office to release detailed information on drone and other lethal airstrikes. Last month, it published aggregate numbers on how many civilians have been killed by CIA and military strikes in countries including Yemen, Pakistan, Somalia and Libya.

The numbers - 64 to 116 civilians and 2,372 to 2,581 "combatants" in 473 strikes in countries where the United States is not at war - were challenged by nongovernment groups as discounting many more civilian deaths. The figures do not include actions in the war zones of Afghanistan, Iraq and Syria.

The newly released document was the subject of a lawsuit filed by the American Civil Liberties Union in fall 2013. The administration, on the basis of "presidential communications" privilege, had denied the ACLU's petition for its release under the Freedom of Information Act.

Early this year, after Judge Colleen McMahon, in the Southern District of New York, questioned that privilege, the government said it would publicly release a redacted version.

After extended back and forth with the court over proposed redactions, McMahon last month ordered that the document be turned over to the ACLU no later than Aug. 5. It was posted without announcement Friday evening on the Justice Department website.

"The PPG should have been released three years ago, but its release now will inform an ongoing debate about the lawfulness and wisdom of the government's counterterrorism policies," said ACLU Deputy Legal Director Jameel Jaffer. "PPG," as the government refers to the document internally, stands for Presidential Policy Guidance.

"The release of the PPG and related documents is also a timely reminder of the breadth of the powers that will soon be in the hands of another president," Jaffer said.

The document's dry, bureaucratic language seems in stark contrast to the presumably dire consequences of the actions it outlines, and it leaves a number of questions unanswered. What appears to be a description of information to be included in the profile of an individual target is blacked out.

It provides no details of how high-value targets are chosen or any geographic limitations, and it includes several presidential waivers of its criteria in the event of "fleeting opportunity" to take action.

"Nothing in this PPG shall be construed to prevent the President from exercising his constitutional authority as Commander in Chief and Chief Executive, as well as his statutory authority, to consider a

lawful proposal" that falls outside the guidelines, including a possible strike against "an individual who poses a continuing, imminent threat to another country's persons," it says.

Numerous international law experts have said that the administration's overall terminology and justification for lethal strikes are novel and without precedent.

"The government has essentially invented its own set of standards ... somewhere in between international law covering war zones and outside areas," Jaffer said. "This doesn't provide any more clarity about the substantive standards the government is using."

The document does provide new details on the president's role in deciding when a strike will be taken. "Operating agencies" - the CIA and the Defense Department - are to provide overall plans for detaining and/or targeting named high-value targets and other "lawful" targets. The plans, to be authorized by the president, must "indicate with precision" the counterterrorism objective and duration of time the authority is to remain in force, the international legal basis for taking action and assets that may be deployed.

Decisions by operating agencies to take strikes against high-value targets require no additional presidential approval, unless U.S. citizens are involved, although "operational disagreements" among top national security officials are to be brought to the president for adjudication.

"Verifying a target's identity before taking lethal action ensures greater certainty of outcome" and the ability to "satisfy the policy standard," the guidelines say. Proposals to strike other targets - presumably the "signature strikes" against groups of unidentified terrorist suspects, massed outside or in buildings or vehicles - are to be submitted for approval and require written presidential authorization.

The document devotes several pages to captures and detentions of terrorist suspects - though they are vastly outnumbered by kills - which require proposals for "long-term disposition" for such individuals and include a "screening process" for any differences of opinion among departments.

An Interagency Disposition Planning Group assesses "the availability, including the strengths and weaknesses, of potential disposition options." Captures of terrorist suspects have long been complicated by decisions on what to do with them. Some have been transferred to third-party countries, while others have been held aboard U.S. naval vessels for interrogation before being brought to the United States for prosecution.

The Guardian (London)
NSA denies 'Raiders of the Lost Ark' stockpile of security vulnerabilities
Saturday, 06 August 2016
Byline: Alex Hern

Las Vegas - The agency's stockpile of unpatched, undisclosed vulnerabilities is a big concern to the security community, but research suggests it discloses more than it keeps
America's National Security Agency (NSA) spends upwards of $25m in a year buying previously undisclosed security vulnerabilities - known as zero days, because that's the length of time the target has had to fix them - but the large investment may not result in as much of a collection of hacking capabilities as is widely assumed.

Jason Healey, a senior research scholar at Columbia University and director at the Atlantic Council policy thinktank, argues that the true number of zero days stockpiled by the NSA is likely in the "dozens", and that the agency only adds to that amount by a very small amount each year. "Right now it looks like single digits," he says, adding that he has "high confidence in this assessment."

Healey presented the research at the Defcon hacking conference in Las Vegas to a packed crowd on the opening day of the event. "I don't know if we've got the right answer, but we've tried to run down every line of evidence that we can."

Related: Using Wi-Fi in Airbnb rentals poses security threat, researchers say

The question of quite how many unpatched, undisclosed vulnerabilities the NSA has stockpiled cuts to the heart of a long-running concern the information security community has about the agency's so-called "dual mandate": it is in charge of procuring intelligence about the actions of America's enemies, a goal it often pursues through targeted hacking attacks, which are made easier by having knowledge of useful zero days, but at the same time, it is in charge of protecting the information security of the nation, a role which naturally entails warning vendors about unpatched security vulnerabilities it discovers.

NSA claims its discloses 91% of vulnerabilities to vendors The same tension exists within the wider American government, Healey says. "You see this tension between these agencies, and the government is certainly not of one mind on this ... Until 2010 it doesn't seem like there was a government-wide policy to handle this."

Before beginning his talk, Healey asked the audience how many vulnerabilities they thought the NSA had stockpiled: hundreds, thousands, more than thousands or less than hundreds. The straw poll showed roughly even numbers guessing each possibility, something that underscores how little trust there is among hackers at large that the NSA will do the "right thing" when it has knowledge of critical bugs.

While emphasising that the closed nature of the NSA makes it hard to state anything categorically, Healey argues that all the available evidence supports the case that the agency actually has much less than the hundreds or thousands or vulnerabilities some in the audience thought it might.

One key piece of evidence comes from the NSA itself, which in 2015 claimed that 91% of vulnerabilities it procured were eventually disclosed to the vendors whose products were at risk. Of the other 9%, at least some of those weren't disclosed because they were fixed before they could be, the agency adds.

Similarly, the White House has revealed that in one year since the current disclosure policy was implemented, it reviewed about 100 software vulnerabilities discovered by the NSA to determine if they should be disclose, and "kept only about two". Healey adds that in the autumn of 2014, he was personally told that every single vulnerability which had come up for review had been disclosed.

'We don't have a stockpile of zero days' Aside from anything else, the figures fit with the comparatively low number of zero days found used in the wild in general. According to security researchers Symantec, just 54 were found through the whole of 2015, "so single digits sounds reasonable".

Healey also cites Michael Daniel, a special assistant to the president and the US's cybersecurity coordinator, to support the claim: "The idea that we have these vast stockpiles of vulnerabilities stored up - you know, Raiders of the Lost Ark -style - is just not accurate," Daniel has said.

The figures don't include the actions of other agencies, though. As the war between Apple and the FBI revealed, conventional law enforcement bodies also have an interest in securing unpatched vulnerabilities. When the FBI eventually bought one such zero day to break into the iPhone 5 at the heart of its fight with Apple - for a reported $1m - it managed to avoid government regulations about zero day disclosure by arguing that it only bought the use of a tool, not the zero day itself. "To me," Healey said, "it seems to contravene pretty direct presidential guidance."

Similarly, they don't include the actions of other governments. Around 30 are known to stockpile their own vulnerabilities, but only one - Britain's GCHQ - is anywhere approaching public about their activities. GCHQ announced disclosure of 20 zero days last year.

Healey closed with a plea to governments and to the hacker attendees of the conference: "Normally in warfare if one side disarms themselves all they've done is disarm themselves. This is the one area where you can disarm governments, because once that information goes to a vendor, everyone is disarmed."

Sunday Mirror (UK)
Cyber crime poses 'real threat' to UK economy
Sunday, 07 August 2016
Byline: Geraldine McKelvie

London - Cyber attacks could devastate Britain's infrastructure and economy, the National Crime Agency has warned.
It is urging more businesses to work with law enforcement agencies in a bid to reduce the growing menace.

Its report into the crisis said: "A cyber attack that poses an existential threat to one or more major UK businesses is a realistic possibility.

"The long-term impact of such a cyber attack could include substantial loss of revenue and margin, of valuable data, and of other company assets."

The NCA said it estimated cyber crime already costs the UK economy billions per year - and that is likely to keep rising as businesses struggle to deal with the issue. The report added: "In any calculation we must consider there are millions of individual victims, many thousands of corporate victims and correspondingly substantial losses.

"Moreover, the accelerating pace of technology and criminal cyber capability development currently outpaces the UK's collective response to cyber crime.

"This cyber arms race is likely to be an enduring challenge, and an effective response requires collaborative action from government, law enforcement, industry regulators and, critically, business leaders."

The NCA went on to say that business chiefs should "challenge" their management teams to go beyond normal cyber security standards to ensure "the threat to the UK is reduced".

The organisation also urged businesses to report all forms of cyber crime to the authorities.

It said: "Directors also have an important role in addressing the underreporting of cyber crime. "In particular, we urge businesses to share more intelligence, both with law enforcement and with each other."

The Australian
The bear in the room
Saturday, 06 August 2016
Byline: David Wroe

Canberra - Cyber spying China and Russia are considered the major culprits in attacks on Australia. The Australian Signals Directorate, a grey and dull-looking building in the defence precinct on a hill above Lake Burley Griffin in Canberra, houses the nation's offensive cyber capability.

This power to attack other countries or non-state adversaries digitally - as opposed to merely shielding ourselves against their attacks - was only acknowledged in April when Malcolm Turnbull unveiled his Cyber Security Strategy.

It would be used only in extreme circumstances, such as if an enemy posed a serious cyber or other military threat to Australia. But the nation's government agencies and vital industries are routinely being hit by attempted attacks that sit somewhere below that trigger level.

The dilemma of how to respond to these regular jabs from shadowy hackers was underscored for the United States last week when the Democratic National Committee was hacked and information embarrassing to Hillary Clinton released by WikiLeaks. The hackers were widely thought to have been from Russian intelligence and there is a strong suspicion it was done to help Clinton's rival, Donald Trump, who for geo-strategic reasons the Kremlin would rather see in the White House come January.

King's College London cyber guru Thomas Rid summed up the view of the security community by branding such a brazen effort by Moscow to interfere in the US's internal politics "a game changer". Yet President Barack Obama's response was mild, saying that if Russia was behind the hack, it would not "wildly" alter Washington-Moscow relations and it was just one more item on a "long list" of differences between the countries.

In the fast-changing world of cyber threats, information is being weaponised in unpredictable ways that are difficult for the victim to respond to.

Cyber attacks are cheaper than armies. They get to ignore geography. They can be conducted in a way that makes it hard for the victim country to prove who did it without revealing its own capabilities.

"They can invest smaller amounts of money and people and asymmetrically get more for it," said Alastair MacGibbon, special adviser to the prime minister on cyber security.

"The internet gives great scope to nation-states, trouble-makers and various threat actors to do things from their lounge room that otherwise they would have had to do face to face. It's been a great enabler. It knocks down geography and a whole lot of other things that previously would have got in the way."

Canberra has admitted to two major cyber breaches in recent years, one on federal Parliament's email system and the other on the Bureau of Meteorology, which is plugged into other agencies including Defence. Both are suspected of coming from Chinese government hackers.

Concerns over the security of government information hit the headlines again this week as Australians began filling out the census largely online, with personal details being held on government systems for four years.

Serious cyber attacks are designed for warfare situations - the first shots in a conflict between major powers would be digital, attempting to take out the other side's ability to command and control their forces.

But the same capabilities can be used in scenarios well short of war to coerce, intimidate and influence, just as traditional military hardware can be used in the way it is now in the South China Sea.

Tobias Feakin, a cyber expert with the Australian Strategic Policy Institute and an independent adviser on the government's classified Cyber Security Review, said Russia was already suspected of having used cyber means for "political destabilisation and interference in its near region" in the form of attacks on Ukraine and Estonia that weren't wartime operations.

Feakin is one of those who believes the Democratic National Committee case was a "quite dangerous" watershed moment, assuming it was indeed Russia as reported.

"It is crossing the boundary around non- interference in a state political process ... almost to weaponising that information and making it harmful to another government without having to confront it."

One veteran security insider told The Age such state-on-state attempts at cyber coercion are likely being done "on a much wider scale than you would think and ... certainly than is reported". He said there was "potential for this to go seriously astray", with sabotage, manipulation of information and even blackmail of political leaders all becoming possible.

"We've created a new monster that will allow people to manipulate information for political gain," the insider said.

In a similar vein, MacGibbon noted everyone has information they wouldn't want to be made public.

"I can guarantee you I've got some of that stuff. I'm suspecting you do as well, whether it's about my personal life, or my personal finances. Could people release that for the purposes of embarrassment and causing resignation? Absolutely. Would it be nation-states or just malicious people who do it? Yes, it could be anyone."

A spokesman for the Australian Cyber Security Centre, housed in ASIO's headquarters in Canberra, said the centre was seeing a "variety of intrusion activity based on a growing range of cybersecurity threats".

"Foreign state-sponsored adversaries are targeting the networks of the Australian government (including state and territory), industry and individuals to satisfy requirements for economic, foreign policy, defence and security information, to gain advantage over Australia," he said. He declined to say where the attacks came from, saying that would "jeopardise ongoing investigations, monitoring of incidents and the ability to protect information and networks".

"The more that is disclosed about cyber incidents, the more that the perpetrators will know about our capability and the methods we have for detecting cyber threats."

Everyone in the business knows China and Russia are considered the major culprits in attacks on countries such as Australia. Feakin said Russia was known for the quality of its hacking, China for the quantity. Both use proxies, hackers who are outside the countries' intelligence agencies but do their bidding.

Where Russia is more about political destabilisation, China has a tradition of economic espionage.

There isn't any obvious looming scenario in which another country such as China might try to influence or destabilise Australia politically, Feakin said.

But he said that amid the great strategic change going on in our region and as a major US ally, there would be strong interest "in how powerful players are thinking, what future actions might be taken".

"The political cycle is always of interest for countries that might be non-aligned with us strategically."

The Turnbull government has pledged $230 million over four years under its Cyber Security Strategy for new staff and resources. The Defence White Paper put a heavy focus on cyber with a further $400 million over 10 years, noting there were more than 1200 attacks on government agencies and nationally critical sectors such as defence industry in 2015 - a steady rise on previous years.

MacGibbon said in the 15 years he's been working in cybersecurity, as a federal police officer, a consultant and a government adviser, there's been a "progressive realisation by agencies" in government that they are vulnerable.

"I would not be so churlish as to say to you that we've reached Nirvana in terms of agencies accepting that they need to mitigate those risks really aggressively," he said. "We have a way to go, there's no doubt. But I would tell you that in 2016, we are better placed than we were in 2006."

But he adds that no security will ever be perfect. Foreign cyber operations will get through.

This means countries including Australia need to figure out ways to respond, Feakin said. Hitting back needn't necessarily be done digitally. The US, for instance, has considered economic sanctions against Chinese hackers. Diplomatic responses are also an option.

But eye-for-an-eye responses are unlikely when it's hard to prove who was behind the hack without exposing one's own classified capabilities. China and Russia are "some of the worst offenders" when it comes to using criminal and hacktivist groups as proxies to carry out attacks, Feakin said.

"Without the categorical, 100 per cent proof, it becomes almost impossible to take action."

Turnbull said on revealing the ASD's offensive capability in April that by finally going public on a capability that had long been assumed to have existed he was adding "a level of deterrence".

So why don't we just surreptitiously hit back in kind whenever we are attacked? Turnbull noted that Australia would only use offensive cyber lawfully and consistent with "the international rules-based order".

In other words, we have better standards. Margaret Stone, the Inspector-General of Intelligence and Security - a watchdog on spy agencies - addressed this question to an audience of intelligence officials and experts this week. In short, she said Australia is not Russia. But this raised a looming problem - do we have to lower our standards to keep up? Stone said she didn't think so but acknowledged it was a challenge.

"The task that our intelligence agencies, particularly in the international area, are being asked to do, is becoming increasingly complex and increasingly difficult. But the demand is greater," Stone said. "So does that lead to a push for lower standards? ... I think that that is a real issue."

Endgaget
US reportedly elevates the role of Cyber Command
Sunday, 07 August 2016
Byline: Jon Fingas

Washington - Now that the US treats cyberwarfare as a staple of its combat operations, it's ready to raise the prominence of its internet warriors. Reuters sources say that the Obama administration is planning to elevate Cyber Command, turning it into a "unified command" that's just as crucial as a major regional section like Pacific Command. The proposed shuffle would also detach Cyber Command from the NSA, giving it more input on the use of online weapons and defenses.
There's no guarantee that the reorganization will go through as it exists right now. Neither Cyber Command nor the NSA are commenting, and an unnamed official tells Reuters that the link between Cyber Command and the NSA is "critical to national security." If the report is accurate, though, the reform isn't likely to face significant opposition.

A switch-up like this might be necessary. Military leaders are reportedly annoyed at the sluggish pace of Cyber Command's campaign against ISIS, and have already created a task force that partners with Central Command to improve its performance. A more powerful Cyber Command might get better resources and would have greater independence. As it is, the shift would be an acknowledgment that online warfare is no longer a side project -- it can be crucial to winning a conflict.

Daily Telegraph (Australia)
BBC detector vans to spy on internet users
Saturday, 06 August 2016
Byline: Peter Foster

London - The BBC is to spy on the internet users in their homes by deploying a new generation of Wi-Fi detection vans to identify those illicitly watching its programmes online.
The Daily Telegraph can disclose that from next month, the BBC vans will fan out across the country capturing information from private Wi-Fi networks in homes to "sniff out" those who have not paid the licence fee.

The corporation has been given legal dispensation to use the new technology, which is typically only available to crime-fighting agencies, to enforce the new requirement that people watching BBC programmes via the iPlayer must have a TV licence.

The disclosure will lead to fears about invasion of privacy and follows years of concerns over the heavy-handed approach of the BBC towards those suspected of not paying the licence fee. However, the BBC insists that its inspectors will not be able to spy on other internet browsing habits of viewers.

The existence of the new strategy emerged in a report carried out by the National Audit Office (NAO).

It shows that TV Licensing, the corporation's licence-fee collection arm, has developed techniques to track those watching television on laptops, tablets, and mobile phones.

The disclosure of the controversial new snooping technique will lay to rest the persistent claims that detector vans are no more than an urban myth designed to intimidate the public into paying the licence fee.

Sir Amyas Morse, the comptroller and auditor general of the NAO, writes in the report: "Detection vans can identify viewing on a non-TV device in the same way that they can detect viewing on a television set.

"BBC staff were able to demonstrate this to my staff in controlled conditions sufficient for us to be confident that they could detect viewing on a range of non-TV devices."

Currently, anyone who watches or records live programming - online or on television - needs to buy a £145.50 licence. But from September 1, those who use the iPlayer only for catch-up viewing will also need to pay the fee, after the BBC successfully lobbied the Government to change the law.

Under the Regulation of Investigatory Powers Act, the corporation is entitled to carry out surveillance of suspected licence-fee dodgers.

The BBC confirmed that its newly developed detection techniques had been authorised under the legislation.

While the corporation would not disclose how the new technology works, the report states that the BBC has ruled out combing its own records of computers that have logged into the iPlayer website to hunt down non-paying viewers.

Sir Amyas writes in the document: "The BBC rightly acknowledges that this would be an inappropriate invasion of privacy."

Instead, electrical engineering experts said that the most likely explanation for how the BBC would carry out it surveillance was a technique known as "packet sniffing", which involves watching traffic passing over a wireless internet network without hacking into the connection or breaking its encryption.

Researchers at University College London disclosed that they had used a laptop running freely available software to identify Skype internet phone calls passing over encrypted Wi-Fi, without needing to crack the network password.

Privacy campaigners described the developments as "creepy and worrying".

A spokesman for Privacy International, the human rights watchdog, said: "While TV Licensing have long been able to examine the electromagnetic spectrum to watch for and investigate incorrect usage of their services, the revelation that they are potentially developing technology to monitor home Wi-Fi networks is startlingly invasive."

A spokesman for TV Licensing said: "We've caught people watching on a range of devices, but don't give details of detection as we would not want to reveal information helpful to evaders.

"Our use of detection is regularly inspected by independent regulators."

The Daily Beast
How Russia Dominates Your Twitter Feed to Promote Lies (And, Trump, Too)
Saturday, 06 August 2016
Byline: Andrew Weisburd & Clint Watts
Section: Analysis

Analysis: Fake news stories from Kremlin propagandists regularly become social media trends. Here's how Moscow does it... and what it means for America's election 2016.
"Ladies and Gentlemen, We have a situation in #Turkey #Incirlik" the cry went out on Twitter last Saturday night, as news spread of the Turkish forces surrounding the U.S. airbase in Incirlik.

Thousands of armed police had reportedly surrounded the airbase amid swirling rumors of another coup attempt, according to stories tweeted within two minutes of each other on RT.com and Sputnik, the two biggest Russian state-controlled media organizations publishing in English. The stories were instantly

picked up by a popular online aggregator of breaking news and prompted hours-long storm of activity from a small, vocal circle of users.

In English, the tweets soon grouped into certain patterns of similar (and sometimes identical) content. The first were panicky expressions of concern about nuclear weapons allegedly stored at Incirlik:

#Incirlik There r 25 underground vaults, each holds up to 4 bombs. The estimated total is 50 B61 thermonuclear bombs--1/4 of B61 stockpile.

Turkey is soon going to acquire some nice nuclear weapons unless Obama pulls his finger out & does something

#Incirlik does anybody else find it ODD that there's a lot of dump trucks. Big enough to carry 90 nuclear warheads

What exactly is going on with the nuclear weapons in Turkey? And why the hell are they there, of all places?

The second group compared the situation to Benghazi.

A third group wondered aloud and repeatedly about why the media wasn't covering the alleged activity.

Why is USA MSM failing to report on events in Turkey surrounding Incirlik AFB and Erdogan's accusation that USA orchestrated the coup?

Hey MSM, you've got 10000 Muslims, steps away from a stockpile of thermonuclear weapons.

Nothing on #msm, no #potus, no #dem or #gop speaking out! Nuclear warheads, up to 90 at stake!

The main reason the media didn't show up was that the story was substantially untrue. As a later statement by the Pentagon clarified, a peaceful protest had taken place involving about 1,000 people--not the 7,000 Turkish police reported by Russian news outlets or the 10,000 cited by Twitter users. Officials at the air base had been warned of the protest in advance. The base was not "surrounded", Turkish security focused on securing the visit of U.S. Chairman of the Joint Chiefs Joe Dunford to Incirlik the next day.

The Incirlik disinformation campaign failed but demonstrates the unique way in which Russia can influence foreign audiences. Incirlik stories on RT and Sputnik news were rapidly promulgated by a curious group of English speakers on Twitter.

One of the first English tweets promoting the Incirlik story came from a Twitter user under the name Marcel Sardo--an account previously identified for instigating pro-Russian campaigns. From this initial

tweet, a cascade of Twitter accounts rebroadcast RT and Sputnik Incirlik articles adding commentary and hashtags. Accounts initially broadcasting the #Incirlik story from seemingly different locales and online communities quickly merged in the first 90 minutes after release of the RT and Sputnik news story.

An increasingly common social media pattern over the past two years as Russia has become more aggressive both on the ground and online as tensions ratchet in a renewed Cold War with the West.

The evolving pattern of retweets reveal a close-knit network and circular information flow where key amplifiers re-broadcast the base #Incirlik story adding commentary and fomenting fears. And here's the odd part: many members of this network seem to be Trump fans.

Some of the top hashtags attached to tweets broadcasting #Incirlik #Turkey were #nato, #coup, #benghazi, #trumppence16. Each of these add-on hashtags pointed to recently hot button issues in the U.S. Presidential contest. Bios of these English speaking accounts retweeting the #Incirlik story commonly included the words "god," "country," "family," "conservative," "Christian," "America," "constitution," and "military."

Two or three tweets called for prayers for U.S. service members potentially in harms way, suggesting Americans were again being overrun in another Benghazi type scenario. More than 10 percent of English speakers citing #Incirlik contained the word "Trump" in their user profile information. From the public view, it's difficult to determine which of these English accounts are real Americans supporting the Trump campaign or instead manufactured accounts inciting support for the Trump campaign and fomenting dissent amongst the U.S. electorate.

This melding of Russian-friendly accounts and Trumpkins has been going on for some time.

"I created this list of Russian trolls," writer Adrian Chen told the Longform podcast in December 2015. "And I check on it once in a while, still. And a lot of them have turned into conservative accounts, like fake conservatives. I don't know what's going on, but they're all tweeting about Donald Trump and stuff."

The Incirlik story, despite failing to endure more than a couple hours before losing credibility, provoked a reaction from Turkey and the U.S. Both countries publicly responded to a non-event seeking to maintain public confidence overseas and at home. More importantly, the propaganda effort comes alongside accusations of Russia meddling in the U.S. election on behalf of Trump. Most sources implicate Russia for hacking the Democratic National Committee's emails and subsequently releasing them on the eve of the DNC convention. Donald Trump's pro-Russia, anti-Ukraine, anti-NATO policy positions have been repeatedly questioned over the past two weeks. Trump's top aide lied about the campaign's changes to the RNC platform limiting support to Ukraine to only defensive weapons.

In a sense, this is the return of an old game. From the 1950s through the Soviet Union's collapse, the Soviet Union sought to use "the force of politics rather than the politics of force" to disrupt and defeat

their adversaries from the inside out. As explained by the 1992 U.S. Information Agency report to Congress, "Active measures seek to use slogans, arguments, disinformation and selected true information to influence the attitudes and actions of foreign publics and governments." Soviet propaganda pushed stories regarding the flaws of democracy, collapse of the world economy, environmental catastrophe, and global calamities like nuclear war.

Conduct of Soviet and Russian 'Active Measures' before the internet proved challenging, particularly in the West. Soviet agents and paid communist supporters would need to reside in the countries they sought to influence, create a print or radio media outlet or gain a job working at an established platform and evade the scrutiny of Western counterintelligence. But these days, it's as easy as setting up a Twitter account. Russia influence operations in social media represents a far more effective and efficient return to their 'Active Measures' campaign of the Cold War.

And when combined with the alleged hacks of political actors, the promotion of these Incirlik-style stories through overt Russian media outlets and 'grey' English speaking propagandists could make for a powerful one-two punch to disrupt the American election. The synchronization of hacking and social media information operations not only has the ability to promote a favored candidate, like Trump, but also has the potential to incite unrest amongst American communities.

Since Incirlik, Trump and Russian media have simultaneously pushed a new theme: the illegitimacy of U.S. elections. The Incirlik disinformation campaign, while a failure, raises the question of Russia's ability to use social media 'Active Measures' to destabilize the American public. #Incirlik wasn't the first Russian influence effort on social media and it most certainly won't be the last. To date, there's been no public U.S. response to alleged Russian hacking or social media information operations. How much longer can the U.S. wait?

New York Times
Did She 'Short-Circuit' on the F.B.I. Inquiry? Clinton Seeks to Explain
Saturday, 06 August 2016
Byline: Yamiche Alcindor

Washington - Hillary Clinton on Friday sought to explain her recent mischaracterization of the F.B.I. investigation into her private email server, saying she "may have short-circuited" in her remarks during a television interview on Sunday when she asserted that the F.B.I. director, James B. Comey, had called her statements about her private email servers "truthful."
Mrs. Clinton made the remarks while taking her most extensive questions from journalists in months -- after going more than 200 days without holding a formal news conference.

She has been under fire from Republicans and others since her remarks Sunday on Fox News about her use of a private email server as secretary of state and the resulting F.B.I. investigation. While Mr. Comey

did not recommend charges in the case, he said Mrs. Clinton had been "extremely careless" in her use of a private email server and contradicted statements she made about her handling of her email.

In her remarks here before the National Association of Black Journalists and the National Association of Hispanic Journalists, Mrs. Clinton tried to explain the discrepancy with what Mr. Comey actually said.

"I was pointing out in both of those instances that Director Comey had said that my answers in my F.B.I. interview were truthful," she said. "That's really the bottom line here."

Mrs. Clinton reiterated her explanation that the classified emails the F.B.I. had identified as having passed over her private server were not marked classified at the time.

The explanation did not appease Republicans.

"It's not hard to see why she hasn't held a press conference in 244 days," said the Republican National Committee chairman, Reince Priebus. "Hillary Clinton is once again proving herself incapable of telling the truth."

During her remarks, Mrs. Clinton said she took "seriously" the problems she has had winning voters' trust.

Questioned about why a majority of voters do not trust her, Mrs. Clinton referred to her high approval ratings when she was secretary of state and a senator from New York.

"Were 67 percent of the people in New York wrong? Were 66 percent of the American public wrong?" she asked. "Just maybe, when I'm actually running for a job, there is a real benefit to those on the other side with trying to stir up as much trouble as possible."

And she explained that the economic frustration driving many of Donald J. Trump's supporters should be taken seriously.

When asked about what Mr. Trump's millions of supporters, who are often drawn to language she and others have called racist and sexist, says about the electorate, Mrs. Clinton said that while some people were backing the businessman because of his "bigotry," she acknowledged that many were motivated by economic hardships.

"We have to recognize that of course some of the appeal is xenophobic and racist and misogynistic and offensive," she said. "We have to acknowledge that -- but let's not lose sight of the real pain that many of Americans are feeling because the economy has left them behind."

Mrs. Clinton also criticized Mr. Trump on Friday as someone who would be a dangerous president and stressed that if elected, she would work on issues related to systemic racism and the economy that often hit black and Hispanic communities the hardest.

"He is harkening back to the most shameful chapters of our history and appealing to the ugliest impulses of our society," she said. "We need to stand up as a country and say that Donald Trump doesn't represent who we are and what we believe."

Mrs. Clinton also vowed to push hard to pass a comprehensive immigration overhaul bill with a path toward citizenship for those in the country illegally, and said she would prioritize the issue during her first 100 days in office.

Mrs. Clinton joins a long list of political leaders who have spoken at the groups' conventions, which often focus on increasing diversity in newsrooms. President Obama, former President Bill Clinton, former president George W. Bush, Bob Dole and former Vice President Al Gore have all addressed past conventions. The groups invited Mr. Trump to speak, but he declined, according to the organizers.

Before taking questions, Mrs. Clinton delivered a 15-minute address focused mostly on how her plans to improve the economy would especially benefit blacks and Latinos. "Rosa Parks opened up every seat on the bus," she said. "Now we've got to open up every opportunity."

Hovering over the address was the image of Mrs. Clinton addressing a room full of journalists. Although she occasionally holds informal sessions with the news media on campaign stops, Clinton aides have spent months explaining why she hasn't held an official news conference, as most candidates, particularly Mr. Trump, do regularly.

"We'll have a press conference when we want to have a press conference," Joel Benenson, the campaign's chief strategist and pollster, told ABC News last month.

She even had some words of encouragement for the Fourth Estate: "We need you to keep holding leaders and candidates accountable," Mrs. Clinton told the hundreds of journalists attending the five-day conference here of the National Association of Black Journalists and the National Association of Hispanic Journalists.

Near the end of the event, Mrs. Clinton talked about her African-American girlfriends, whom she rarely mentions in public. Asked what the most meaningful conversation she has had with one of them, she said she was "blessed to have a crew of great friends." These include some of her most senior aides, including Cheryl D. Mills, Maggie Williams and Minyon Moore.

"I can't compress it into one conversation," Mrs. Clinton said. "They've supported me. They've chastised me. They've raised issues with me."

Find out what you need to know about the 2016 presidential race today, and get politics news updates via Facebook, Twitter and the First Draft newsletter.

Wall Street Journal
Password Hacking Forces Big Tech Companies to Act
Monday, 08 August 2016
Byline: Robert McMillan

New York - In the past few months, hackers have taken over the social-media accounts of Facebook Inc. Chief Executive Mark Zuckerberg, Google CEO Sundar Pichai and Twitter Inc.'s CEO, Jack Dorsey. Behind the scenes, security teams at every major technology company -- and many smaller firms, too -- are scrambling to protect others from the same fate.

Some of the executives apparently reused passwords that had been stolen in earlier hacks of LinkedIn, Myspace and other sites; others may have fallen victim to software that uses the old passwords to guess new ones.

Nearly two billion old passwords can be viewed for as little as $2 at a database called LeakedSource, run by anonymous operators.

Investigators estimate that maybe up to 8% of the LinkedIn usernames and passwords will work on other services, giving hackers a way to take over accounts elsewhere. LinkedIn, meanwhile, reset its own users' passwords and fixed a security hole that had allowed data to be stolen in 2012. The company is in the process of being acquired by Microsoft Corp., a $26.2 billion deal that is expected to close by year's end.

Hacking creates a dilemma for operators of other popular consumer web services. They can require all users to change their passwords, and risk losing some users. If they don't force password changes, users' accounts could be hacked.

"If they change passwords for their users, no matter how well they explain it, the perception may be completely off," said Alex Holden, the founder and chief information security officer of Hold Security LLC, which helps companies spot stolen credentials on hacking sites. "If even 0.1% of these users panic and they have to call customer service in one day, it creates a nightmare."

Carbonite Inc., which offers online backup services, chose to reset passwords for each of its 1.5 million users. The company also analyzed the hacked data and required customers whose credentials appeared in the database to confirm their identities in order to access their accounts.

Carbonite moved decisively because of the serious consequences of a compromise, said Norman Guadagno, Carbonite's senior vice president of marketing. "When you have a Carbonite account -- or

any backup service -- and you have the username or password to that account, you have access to everything," he said.

Twitter, Facebook, Yahoo Inc. and others chose a different course. Instead of resetting all passwords, they analyzed the stolen credentials and then urged or forced affected users to reset their passwords.

Over the past years, companies such as Yahoo have put in place data-analysis and customer warning systems that allow them to methodically process these huge volumes of data and protect customers who reuse their passwords against these types of disclosures.

Last week, Yahoo's security team responded to a report that 200 million of the company's user names and passwords were up for sale in hacker forums. A Yahoo spokesman said the company was aware of the claim and "working to determine the facts."

The identity intelligence company InfoArmor Inc. examined the database in question last week and believes that it isn't a brand-new database of Yahoo passwords.

The Daily Beast
Vladimir Putin Plots a New Fleet of Spies in Space
Monday, 08 August 2016
Byline: David Axe

Washington - The Russian military is apparently getting ready to launch a new generation of high-tech spy satellites.
It could help Moscow begin to match the as-yet-unrivaled resolution of America's own eyes in orbit. But the U.S. space force isn't standing still. While Russia races to catch up to the United States in one particular aspect of orbital reconnaissance--that is, imagery detail--the United States is plotting a sort of technological sidestep that could actually extend its lead over its rivals in space-based espionage.

Moscow reportedly plans to launch three of the new Hrazdan satellites--one each in 2019, 2022 and 2024. Essentially orbital telescopes that point down toward Earth, the Hrazdans will replace Russia's two existing Persona spy satellites.

Moscow has come to rely heavily on its military spacecraft to support long-distance deployments. Spy satellites, including the Personas, have played a central role in the Russian intervention in Syria, helping to spot targets for Russian bombers and cruise missiles.

The Hrazdans are built around huge, finely-crafted lenses. Where the Personas' feature 1.5-meter-diameter lenses, the Hrazdans' boast lenses with a diameter greater than two meters, according to Kommersant, a Russian newspaper.

The Personas maintain circular orbits around Earth at an altitude of 700 kilometers. At that altitude, the older sats' lenses afford them a 31-centimeter resolution, Ted Molczan, an independent satellite-tracker and space expert, told The Daily Beast. In other words, when a Persona takes a snapshot of the Earth's surface, each pixel in the image represents an area 31 centimeters by 31 centimeters.

At the same altitude, the Hrazdans would significantly improve on the Personas. Their resolution could go as high as 24 centimeters, according to Molczan.

"This is a significant upgrade for the Russian capabilities," Brian Weeden, a space expert with the Secure World Foundation in Colorado, told The Daily Beast.

But while Russia focuses on improving its spy satellites' resolution, the United States is working hard to make its own spacecraft more responsive--and combining them with for-hire, commercial satellites. That's a major, major shift for the American military and intelligence communities.The U.S. National Reconnaissance Office, which operates America's main spy satellites on behalf of the military and intelligence communities, can get resolutions as high as seven centimeters from its KH-11 Keyhole spy satellites, whose 2.4-meter-diameter lenses formed the basis of NASA's famous Hubble telescope.

But there's a catch. The KH-11s traditionally maintain elliptical orbits that dip as low as 260 kilometers and climb as high as 1,000 kilometers. At the highest altitude, the Keyholes' resolution degrades to 28 centimeters, Molczan said. It's only at the low point that the U.S. sats' can peer down with seven-centimeter resolution.

The elliptical orbits are no accident. They allow the satellites to modulate between viewing huge swathes of Earth at low resolution and much smaller sections of the planet at high resolution. By coordinating the orbits of the KH-11s--there are apparently four of the spy sats in operation--the NRO can maintain simultaneous wide and narrow surveillance.

But the NRO apparently has a new and, it clearly believes, better scheme in mind--one that could vastly improve America's space reconnaissance capability without simply counting on ever-larger lenses on successive generations of spy satellites.

The NRO appears to be shifting its KH-11s in lower, more circular orbits--and is set to continue this deployment pattern as new Keyholes come on line starting in 2018. "There are indications that the next-generation KH-11 may adopt a 260-kilometer-by-500- kilometer orbit, which would maintain the present seven-centimeter best resolution, but significantly improve the overall resolution around the orbit," Molczan explained.

That would leave gaps in wide-area surveillance compared to the traditional orbital pattern. But the NRO has a plan, according to Molczan. "The task of lower-resolution, wide-area coverage would shift to commercial satellites."

Private firms such as DigitalGlobe sell space-based imagery at resolutions as high as 30 centimeters, the current cap under U.S. law. Weeden told The Daily Beast that companies now possess the technology to collect 25-centimeter-resolution imagery, even if they can't legally sell it to private users.

DigitalGlobe's satellites orbit at 770 kilometers, near the KH-11s' old peak. The NRO could substitute imagery from DigitalGlobe or another company for the lowest-resolution Keyhole imagery--25 to 30 centimeters--and free up the KH-11s to do what they do best--take detailed snapshots at very, very high resolution.

At the same time, the NRO is improving its satellite-communications infrastructure. Spy satellites are really just remote-controlled cameras. To make use of their imagery, analysts on the ground must download the photos.

That's only possible when the spacecraft has a line of sight to a ground station and can beam down a digital file. Alternatively, the spy sat can beam its data to a constellation of dedicated, very-high-altitude "satellite data system" relay spacecraft that stays in constant contact with controllers on the ground.

The United States is the world leader in these SDS relay sats--and might be on the verge of pulling even farther ahead of rivals. "The U.S. appears to be investing a lot more in that than the Russians or anyone else," Weeden commented. The NRO generally doesn't disclose the exact nature of its satellite launches, but Weeden and Molczan both said they believe the most recent NRO launch, on July 28, involved a new SDS satellite.

So yes, the Russians are reportedly getting new spy satellites. They're apparently pretty sophisticated. But that doesn't mean the Russia is pulling ahead of the United States in the field of space reconnaissance. "From what I can tell, the U.S. still has a pretty sizable advantage at least qualitatively, if not quantitatively," Weeden said.

New York Times
Can We Still Trust WikiLeaks?
Monday, 08 August 2016
Byline: Alex Gibney

Op-ed - The release of a cache of emails from the Democratic National Committee by WikiLeaks last month has raised a great many questions -- about the role of the D.N.C. in trying to influence the primary and about the alleged interference of Russian intelligence in an American election.
It also raised long-debated questions about WikiLeaks itself, about how an organization dedicated to radical transparency continues to bring secretive worlds to light. And the episode reveals some of the weaknesses of WikiLeaks and its founder, Julian Assange, like their recklessness with personal data and their use of information to settle scores and drive personal agendas.

I've had my own run-ins with Mr. Assange. During the making of my 2013 film, "We Steal Secrets: The Story of WikiLeaks," I spent an agonizing six hours with him, when he was living in an English country house while out on bail. I was struck by how insistently he steered the conversation away from matters of principle to personal slights against him, and his plans for payback. He demanded personal "intel" on others I had interviewed, and dismissed questions about the organization by saying, "I am WikiLeaks" repeatedly. (Later, Mr. Assange and his followers attacked both me and my film.)

Even given that history, I believe that WikiLeaks was fully justified in publishing the D.N.C. emails, which provided proof that members of the D.N.C., in a hotly contested primary, discussed how to undermine the campaign of Bernie Sanders. They are clearly in the public interest.

As for Mr. Assange's animus against Hillary Clinton -- he has written that she "lacks judgment and will push the United States into endless, stupid wars which spread terrorism" -- that is evidence of bias, but no more than that. After all, many news outlets are clearly, and sometimes proudly, biased.

We still don't know who leaked the D.N.C. archive, but given Mr. Assange's past association with Russia, it wouldn't surprise me to learn that it was a Russian agent or an intermediary. Mr. Assange insists this is a mere distraction from the issue of D.N.C. interference, but the answer is also in the public interest. We should all be concerned (although hardly surprised) if it is that easy for the Russians to break into the D.N.C. and possibly United States government networks.

As for the way the leak was published, Mr. Assange and WikiLeaks have more to answer for. Contained in the D.N.C. archive were Social Security numbers and credit card data of private individuals, information that served no public interest. Mr. Assange defended this invasion of privacy by claiming that deleting the information would have harmed the integrity of the archive.

But there is a responsible tradition of redacting potentially harmful private information. In 2010, just before publishing the first Afghan war logs provided to WikiLeaks by Chelsea Manning, Mr. Assange and a group of journalists from The Guardian, The New York Times and Der Spiegel were engaged in a tussle over redacting the names of Afghan informants. The three publications all decided to do so, but Mr. Assange disagreed. As he told Nick Davies of The Guardian, "If an Afghan civilian helps coalition forces, he deserves to die."

Others present at this time insist that he was concerned about their safety but had little technical ability to do the redactions on a tight deadline. The net result: Mr. Assange held back 15,000 documents and published the rest, including the names of about 100 Afghan civilians.

There is no evidence that any of those people were killed. But people could have been hurt. And his refusal to redact allowed the United States government to deflect attention from the evidence of possible war crimes by claiming that Mr. Assange had blood on his hands.

In an underappreciated part of the WikiLeaks saga, computer- savvy volunteers at the organization corrected Mr. Assange's mistake and used an inventive computer program to scrub names and identities from the second leak of documents, the Iraq War Logs. It was an exemplary display of how to publish sensitive materials. Sadly, Mr. Assange reverted to form in subsequent leaks, including the unredacted publication of 251,000 State Department cables and his recent release of the emails from the A.K.P., Turkey's ruling party, which exposed the personal information of more than one million Turkish women.

By comparison, Edward J. Snowden has been much more careful about how leaked documents were published. He recently criticized Mr. Assange, noting that WikiLeaks' "hostility to even modest curation is a mistake."

Mr. Assange has also leaked documents to benefit his private aims. In 2010, he ordered an associate named James Ball to pass 90,000 cables covering Russia, most European countries and Israel to a shady journalist named Israel Shamir, who, according to Mr. Ball, later offered them to pro-Putin Russian media outlets for a $10,000 fee. It also seems likely that Mr. Shamir passed documents to Belarus's brutal president, Aleksandr G. Lukashenko, just before a crackdown on opposition activists (which WikiLeaks has denied). Mr. Shamir is also the father of Johannes Wahlstrom, a Swedish journalist who helped to engineer a vilification campaign against the two women who accused Mr. Assange of sexual assaults and who was to be a key witness had Mr. Assange been tried for rape in Sweden.

For many of those who know him well, Mr. Assange is afflicted by what the police call "noble cause corruption," a belief that noble ends justify reckless or immoral means. In a world awash in new information -- and misinformation -- context, motivation and trust are crucial when weighing the importance of leaks and their accuracy. Mr. Assange still claims that WikiLeaks is a beacon of transparency. We should no longer take him at his word.

Note: Alex Gibney is a filmmaker whose latest documentary, "Zero Days," is about cyberwarfare.

The Guardian (London)
The Chinese firm taking threats to UK national security very seriously
Monday, 08 August 2016
Byline: Juliette Garside

Banbury, Oxfordshire - Welcome to the Cell. All visitors must surrender their phones at the door. No cameras or filming equipment allowed.
In a deceptively humdrum office block on the outskirts of Banbury, Oxfordshire, a team of cybersecurity experts is working to combat the risk of surveillance and hacking attacks from China.

The Cell's technicians have the highest level of security clearance, with their personal and financial histories combed by investigating officers. Their work is overseen by a board that includes directors from GCHQ, the Cabinet Office and the Home Office.

But the Cell's staff are not on the British government payroll. They are employed by Huawei, one of China's largest technology companies. A maker of broadband and mobile network equipment, its kit is installed all over the UK.

In Banbury, the task is to check Huawei hardware and software for faults and bugs that could be exploited for nefarious purposes. Circuit boards are dismantled, and millions of lines of software code are analysed.

The centre was created as a compromise - between the security concerns of intelligence agencies and the private sector's desire for cheap imported technology.

With George Osborne's ejection from the Treasury, China has lost its main cheerleader in government. The new prime minister, Theresa May, is taking a more cautious approach. A decision on allowing the Beijing-backed Hinkley Point power station project to go ahead has been delayed at her request.

In a climate of cooling economic relations, could the Cell provide a model for managing the potential risks of Chinese involvement in critical national infrastructure?

Perhaps. Up and running for five years now, the Huawei Cyber Security Evaluation Centre, to use its official name, is regarded as a success by the board of government officials which oversees its work.

In their second annual report, published this spring, they found the arrangements to ensure the Cell was independent from Huawei were operating "robustly and effectively", and that any potential threats to national security "have been sufficiently mitigated".

But in 2013, the Banbury operation was heavily criticised by parliament's intelligence and security committee, then chaired by the former defence secretary Sir Malcolm Rifkind.

MPs had decided to review its work after a US senate report raised the alarm, urging American firms not to use the company's equipment. Attempts by Huawei to take over US technology companies had been blocked. In Australia, it was barred from bidding for the country's multibillion-pound project to connect every home to a superfast broadband service.

Rifkind's committee concluded that the Cell's staff should not be Huawei employees. His report warned this amounted to Huawei "effectively policing themselves". He recommended Banbury be staffed by GCHQ, and failing that, subject to much greater scrutiny by government officials.

And so, in 2014, security experts from the highest echelons of the civil service were brought together, along with representatives of Vodafone, Huawei and BT, to create the Cell's oversight board. It is currently chaired by Ciaran Martin, director general for cybersecurity at GCHQ.

Concerns persist. Ernst & Young, hired to evaluate whether the Cell is truly independent from Huawei headquarters, concluded that the ability of the company to set the bonus of the Cell's managing director, David Pollington, hired from Microsoft last year, "provides a vector by which performance ... could be influenced".

Ernst & Young argued that "by withholding or awarding the bonus (irrespective of performance), which constitutes a significant element of the reward package, the bonus could be used as a tool to motivate certain behaviours from the MD". The risk was reconsidered, but "accepted as reasonable", according to the 2016 annual report.

A spokesman for the company points out that the Huawei and Hinkley scenarios are not quite comparable. The technology firm sells its equipment to other companies which then own and manage it. At Hinkley, the proposal is to sell a stake to the Chinese state, and in return for the investment, allow it to build Chinese- designed reactors at a new nuclear power station in Bradwell, Essex.

So what kind of risk does Huawei's equipment present? The company makes everything from the routers and switches that steer traffic across the internet, to BT's green street cabinets, to the transmission equipment used in mobile phone masts.

Sending an email from your home computer, making a mobile phone call from a street corner, or using the tablet to order a weekly shop - wherever you are in the UK, the chances are your private communications will be carried over Huawei equipment.

With customers in Europe, the Americas, Africa and of course China, it claims to connect a third of the world's population.

Founded by a former Red Army officer, Ren Zhengfei, the firm has no public list of shareholders, but it claims to be privately owned and independent from the state.

Its biggest UK customers are Vodafone and BT. Until recently the only British-owned mobile network, Vodafone has carved out a niche as the largest supplier to government ministries and major corporations. The phone calls made by the prime minister and her cabinet run over its network.

BT's broadband grid stretches from Whitehall to remote rural areas and is still the largest in the UK, supplying much of the infrastructure used by rivals including TalkTalk and Sky to connect their customers.

The concern is that so-called "back doors", hidden in the Huawei software, could be used to eavesdrop on sensitive government, military and business communications. They could even be used to disrupt or shut down mobile networks in the event of a conflict.

"Bugs can be hidden in sloppy code," says Graeme Batsman, a data security consultant and blogger at datasecurityexpert.co.uk. "China and others are known for spying. But I don't think China is a terrorist state which would make these devices explode one day. The UK and US are probably just as bad anyway."

Indeed, the papers leaked from America's National Security Agency by Edward Snowden revealed that it had hacked into Huawei's headquarters, obtaining technical information and monitoring the communications of its top executives. One of the reported aims was to try and uncover vulnerabilities in the products to use them for US surveillance operations.

The Cell has identified multiple vulnerabilities in Huawei products. The latest annual report warns: "Code quality has shown signs of improvement, but remains below industry good practice." More than 100 concerns had been raised with Huawei's research and development arm in China, the 2015 report stated. Three issues identified that year resulted in interventions having to be made in equipment already deployed in telecoms networks.

On the plus side, using company staff to identify faults means they are more likely to be fixed quickly. And the cooperation has brought cash into the UK. In 2012, Ren met with David Cameron to promise £1.3bn of procurement and investment. The following year, after Rifkind's inquiry, he confirmed the deal when Osborne visited Shenzhen.

For Huawei, the monitoring arrangement not only improves its products, but makes good business sense. Cooperating with the UK advertises its trustworthiness to other foreign governments.

Reassuring the prime minister is another matter. Vince Cable has revealed that while he was in government, May was "never completely satisfied about Huawei". The Cell's recent efforts may have quelled those fears. For now, it is business as usual in Banbury.

The Independent (UK)
Police tackling fourfold rise in drone-related crime
Monday, 08 August 2016
Byline: Peter Yeung

London - Police are having to investigate a fourfold rise in the number of crime reports involving shop-bought drones - including allegations they are being used by paedophiles over children's playgrounds, peeping toms spying through bedroom windows, burglars scoping out people's properties and even cashpoint scammers recording pins.
An investigation by The Independent has found that the number of incidents reported to the police involving drones surged by 352 per cent in a single year as the public became increasingly aware, and suspicious, of the machines.

Reflecting the rapid uptake of the flying robotic devices, which can be fitted with cameras, reports to police surged from 94 in 2014 to 425 in 2015. The projected figure for 2016 is set to be even higher, with 272 reports recorded up until May this year.

The figures were obtained from freedom of information requests, with 21 of the UK's 45 police forces responding.

The numbers also include reports of drones endangering commercial airliners, causing fights between neighbours and being used by criminal gangs to transport drugs, often into prisons.

The majority of the reports, 257, were listed as a concern for public safety and under suspicious circumstances, but five cases involved acts of violence, 13 related to burglary, 14 to dangers posed to transport - largely related to air space - and seven made reference to drones in the vicinity of young children.

One remarkable incident recorded by the Police Service of Northern Ireland in June last year revealed a drone allegedly being used to film a cashpoint in Templepatrick as people entered their security codes.

The witness told police that when the drone was spotted it flew off and crashed into a taxi. The police said a male suspect had been forced to pay compensation to the taxi driver, but officers had been unable to prove the footage was being taken with criminal intent.

Drones, quadcopters and multi-rotor helicopters already equipped with 360-degree 4K video cameras, more than twice the quality of HD, are currently available to buy without any registration or permit.

Speeds range as high as 70mph for mass-produced drones, while potential altitudes up to 10,000 feet make them a threat to aircraft flying in or out of airports.

Many also offer image transmission to a handheld device, such as a mobile phone, and others include night vision.

Sexual offences involving a drone were reported in both London and South Wales, with the Metropolitan Police investigating a case of "voyeurism" and the Welsh force revealing a drone had been used to record footage of a young woman getting undressed in her apartment.

In Leicester, a pedestrian claimed to have seen a drone falling from the sky, while in Sutton Coldfield another fell and damaged the roof of a BMW, as regulation of air space has become increasingly demanding with unprecedented new risks.

Reports of disturbances to flight paths around Birmingham, Stansted and Luton airports were also provided, raising wider concerns for public welfare and potentially the threat of terrorism. In April,

Elstree Aerodrome air traffic control noted that a drone had been seen five miles north-east of Elstree, Hertfordshire, by a pilot whose aircraft was at 6,000 feet.

Greater awareness of privacy concerns has also led to some direct confrontations. In South Wales, one homeowner threatened to shoot a drone out of the sky, and dozens of other reports related to surveillance.

In a similar incident in Bedham, West Sussex, one person fired a shotgun at a neighbour's drone.

In Spennymoor, County Durham, a fight broke out over a drone, with one disgruntled bystander pushing a man and throwing his remote control into a bush.

Elsewhere, a drunken man was found to be "causing distress to livestock" after using a drone to fly close to cows in Plymouth.

There are also fears that drones could be used by paedophiles, with reports of drones flying over children's areas in Kingswinford, Dudley, and schools in Hemel Hempstead and Northumbria.

David Dunn, a professor at Birmingham University who has led research into UAVs, said there needed to be more regulation. He told The Independent: "What you have is a massive proliferation of easy access to the air from machines that have the capacity to cause nuisance, to carry out surveillance, to cause potential injury, and to frighten people and cause collisions with cars and aeroplanes.

"There needs to be regulation, and there need to be systematic attempts to educate the public. At the moment, you can buy one of these things in a supermarket without any safeguards. We are lacking accountability or a deterrent. The police are being forced to use laws that were designed before the invention of drones fit in terms of personal safety and privacy, but actually what we need is a drone bill through the House of Commons to address the technological challenges."

Mr Dunn said the terror threat was a "massive concern" to law enforcement agencies, adding: "These machines have the ability to actually deliver drugs into prisons, to deliver sim cards into prisons."

Corroborating previous reports, the data reveals a significant number of sightings of drones around prisons. At HM Prison Leicester, legal highs and a mobile phone were caught in netting around the perimeter - a measure used across UK prisons to counteract smuggling devices such as drones - and drugs were also found attached to a machine by Sherwood Prison. The Mount Prison in Bovingdon was the centre of a high number of interceptions, alongside institutions in Exeter, Bedford and Greyfriars.

Anyone found using drones to smuggle contraband into a prison can be given a sentence of up to two years.

A spokesman for the Prison Service said it was working to ensure the "right tools" are in place to tackle the problem of drones. He added: "We take a zero-tolerance approach to illicit material in prisons and work closely with the police and CPS to ensure those caught are prosecuted and face extra time behind bars."

Steve Barry, the National Police Chiefs' Council lead for unmanned aerial systems, told The Independent: "Both the police and Civil Aviation Authority (CAA) are aware of the ever-increasing use of drones by members of the public and are keen to ensure that people are aware of the rules that apply to their use. We have issued guidance to all forces on how to respond to drone misuse by the public. Work is ongoing to better understand the threat posed by drones, and to develop an appropriate technical response. We are working with the Home Office on how drones might be used to enhance operational capability in law enforcement, including for support for emergency response or for public order events."

Sara Ogilvie, policy officer at the advocacy group Liberty, said: "As the use of drones by both individuals and the police continues to soar, the need for thorough public debate and robust regulation of this shadowy industry becomes all the more obvious and urgent. As these figures show, the public have serious concerns about drone use, but the safeguards are flimsy and obscure.

"Drones have the potential to serve as incredibly intrusive spying tools, and their capacity for violating people's privacy will only increase as the technology improves. Our authorities need to wake up fast to the stark implications for our privacy and safety."

The figures also reveal a large amount of investment in drones by some UK police forces as a new way of tackling crime and helping with other investigations. Last year alone, Sussex and Surrey Police spent £ 413,000 in a joint initiative, training 38 officers to fly the remote- controlled aerial cameras. They now have five drones - more than any other force in the country. The drones are being used in missing person searches, forensic collision investigations and airport security, as well as patrol teams and neighbourhood response units.

Mr Barry, who is also assistant chief constable of Sussex Police, said in a statement: "Our drone operations will be overt, open and transparent, and we will use all outlets available to ensure the public are informed of our drone use."

Police forces in Devon, Cornwall and Dorset are also testing the use of drones for missing people searches and the photographing of crime scenes.

In September, Nigel Wilson, from Bingham in Nottinghamshire, became the first person in England to be prosecuted by the CPS for illegally flying drones. He admitted nine breaches of filming footage over football grounds and tourist attractions.

Amazon, the world's biggest online retailer, this week agreed a partnership with the Government to start using drones for deliveries by 2017.

The Australian
China bid must pass test on security
Sunday, 07 August 2016
Byline: Brendan Nicholson & Annabel Hepworth

Canberra - Scott Morrison has declared the nation's security will be the top priority as the Turnbull government faces a crucial decision on whether to allow a Chinese -company to buy a 99-year lease on half of the major NSW power distribution network, Ausgrid.
The issue is set to escalate against a background of increasing concerns about Chinese -aggression in the South China Sea and warnings in the Chinese state-owned media that if Australia joined US naval patrols through contested waters "it will be an ideal target for China to warn and strike".

The Foreign Investment -Review Board is considering whether the two Chinese bidders, the state-owned State Grid -Corporation and Cheung Kong Infrastructure Group (CKI), which is registered in Hong Kong and part owned by billionaire Li Ka-shing, should be -allowed to lease the grid.

"National security will be my prime consideration," the Treas-urer said on Sky News's Australian Agenda program yesterday.

The deal would be worth more than $10 billion and the possibility that one or both of the Chinese companies could be knocked out of the race could set the federal Liberal Party up for a battle with the Baird government, which fought last year's NSW election on its promise to use the sale proceeds to fund the biggest infrastructure building program since the Sydney Olympics in 2000.

A NSW government spokesman declined to comment last night.

But The Australian has been told there have been extensive talks of the deal among the NSW government, bidders and bodies such as the Australian Compet-ition & Consumer Commission, the tax office and the FIRB.

Mr Morrison pointed out that he appointed former ASIO chief David Irvine to the FIRB board to help more clearly identify security threats.

Mr Morrison said the Ausgrid decision was "not too far away". The decision will follow the controversial lease of Darwin's port to a Chinese- owned company, the rejection of the sale of the Kidman cattle properties over security concerns and the -government's approval of the Kimberley Ord River cattle -station sale before the election.

Peter Jennings, the executive -director of the Australian -Strategic Policy Institute, warned in The Weekend Australian that the way Australia dealt with -Chinese investment in critical infrastructure needed to be reconsidered in the face of Beijing's assertive posture in the region.

Andrew Hastie, a former SAS officer and now the Liberal MP for the West Australian seat of Canning, endorsed Mr -Jennings's concerns. "This is an important article that Australians should read and discuss," Mr Hastie said.

One Nation leader Pauline Hanson and fellow Queenslander Bob Katter have campaigned aggressively against foreign investment in critical -infrastructure. Nick Xenophon has said any sale to a foreign government-owned company should raise national -interest concerns.

But former Business Council president Tony Shepherd said -foreign capital had always been vital for Australia's prosperity. "Provided the bidder is of good standing then the best deal for NSW should win," he said.

Former Ansett and British Airways chief Rod Eddington -cautioned against anti-Chinese sentiment, saying the nation had "always relied on foreign capital to help us grow our businesses and create our jobs".

TransGrid chairwoman Kerry Schott said Australia needed foreign capital to develop.

While she expected security to be part of the FIRB's -assessment, "it's not as if somebody in China is going to flick a switch and the lights are suddenly going to go off".

Former Shanghai Australian Chamber of Commerce president Peter Arkell said he was baffled that Australia could risk squandering the opportunity for Chinese -investment as the topic "gets kicked around like a footy".

But Mr Morrison, asked how big a part in the -decision would be played by -security factors and concerns about control of strategically important infrastructure, said: "It is the prime consideration. It is the most -important consideration and -always is.

"It is why I put David Irvine on the FIRB. It is why I put David Peever (who headed a major review of the Defence Department) on the FIRB -- to have the -national security experience and input into these decisions and to assist me making these decisions." Privatisation in NSW is expected to pay for $20bn of infrastructure, which includes a second harbour rail crossing and extensions to WestConnex.

While the government reaped more than $10bn from its lease of TransGrid, key projects will -depend on the partial lease of -Ausgrid and also of distributor -Endeavour Energy going ahead.

Gary Sturgess, who advised former Liberal premier Nick Greiner and is at the Australia and New Zealand School of Government, said the Ausgrid lease was different to the sale of cattle properties.

"If people want to pour some of their spare cash into Australian -assets, I mean, frankly that's how this country got built ... the -Europeans pouring money into our country," Mr Sturgess said. "This is not an asset they can run away with." Industry sources said that should State Grid be successful in acquiring Ausgrid it would control electricity and gas connections to more than one million homes and businesses across NSW.

An issue likely to be considered by the government is whether safeguards, conditions or limitations can be imposed on the bidders to ease security concerns.

Another is whether the two companies should be viewed differently. State Grid is clearly owned by China's government. CKI has already invested heavily in Australian infrastructure but its base in Hong Kong is under increasingly intrusive control from Beijing.

State Grid already holds 46 per cent of the South Australian transmission business Electranet and 60 per cent of the Jemena energy distribution business and its 11,000km network, which delivers electricity to more than 319,000 homes and business in northwest Melbourne, and its 25,000km system which delivers gas to more than 1.3 million homes, businesses and industrial customers in NSW.CKI owns SA Power Networks, a primary state electricity distribution business, CitiPower, which supplies electricity to Melbourne's CBD and inner suburbs, Powercor, Victoria's largest electricity distributor, Transmission General Holdings, a Victorian renewable energy power transmission -business, and Australian Gas -Networks, one of Australia's largest natural gas distribution firms.

BBC News
India sets up agency to probe cyberterror
Sunday, 07 August 2016

New Delhi - The increasing use of social media by global terror groups, like ISIS [Islamic State] and the Al Qaeda, for radicalizing young people and a sharp upward trend in cyber-related offences has led to the government launching a major initiative in setting up a highly-specialized cyber agency to watch and probe such cases.
The agency will work under the Union home ministry and would be to cyber crime what the National Investigation Agency (NIA) is to probing terror-related incidents in the country, sources said. The NIA was set up in the aftermath of the 26/11 Mumbai terror attacks.

The new cyber unit will investigate all major cases of cyber crime in close coordination with respective state agencies.

The steady increase in cases of breach of cyber security across the country prompted the much-needed move by the Centre. From 5,693 cyber crime related cases registered in 2013, the spike has been to 9,622 in 2014 and 11,592 in 2015. The situation has only gone from bad to worse with 21,248 cases already reported till May this year. Intelligence officials claim they have been closely monitoring the

trend in cyber security over the last few years and it has been showing a spiraling increase, particularly in the last four years. And this is what has pushed the government to finally go ahead with a specialized agency to probe incidents related to cyber security. "The intelligence agencies too have been stressing on the need for a professional outfit to deal with cyber security. Things have now started moving and a fund of 400 crore [Indian rupees] has been earmarked for the project. The agency will have highly-trained professionals in cyber security," a government official said.

The proposed cyber agency apart from investigating cases will also assist and provide technological support to the state police and other central agencies. The new cyber agency will be the nodal agency for investigating all cyber cases where ISIS is found to be using social media for recruitment.

In fact, the increasing threat from ISIS on the cyber space is one of the main reasons why the government plans to fast-track the setting up of this agency.

"The experience of having a professional outfit like NIA for investigating terror cases has been good and it works as a nodal agency in close coordination with the States also. Now we want to do the same in the case of cyber security as well," the official added.

Associated Press
Official says Australian security key to Chinese investment
Tuesday, 09 August 2016
Byline: Rod McGuirk

Canberra - Australia's treasurer said Monday that national security would be his overriding consideration when he makes a decision on whether to allow a Chinese consortium to lease a major Sydney electricity grid.
Scott Morrison said he was close to making a decision on whether to allow Chinese state-owned State Grid Corp. and Hong Kong-registered Cheung Kong Infrastructure Group to buy a 99-year lease for half of the New South Wales state-owned electricity network Ausgrid for more than 10 billion Australian dollars ($7.6 billion).

"This is not an easy decision," Morrison told Sydney Radio 2GB. "National security out ranks everything."

Chinese foreign investment, particularly from state-owned companies, has become increasingly contentious in Australia as China takes a more aggressive stance in territorial disputes in the South China Sea.

President Barack Obama raised questions with Prime Minister Malcolm Turnbull last year after Australia allowed a Chinese company, Landbridge, to secure a 99-year lease over the strategically important Port of Darwin, which has become a U.S. Marines training hub in northern Australia. Turnbull said Australian defense and security officials determined the AU$506 million deal did not threaten national interests.

Peter Jennings, executive director of the Australian Strategic Policy Institute, a government-established independent think tank, said neither the Darwin Port lease nor the proposed Austgrid deal were in Australia's security interests.

Jennings said a Chinese-controlled Austgrid could become vulnerable to being shut down by cyberattack as hackers linked to Russia had done in the Ukraine in December.

Hackers used a coordinated attack to take down part of western Ukraine's power grid, blacking out more than 225,000 people after hitting regional electric power distribution companies. U.S. officials called it the realization of a nightmare scenario -- hackers able to take down a critical system on which a country depends.

"You have to be concerned in a future world where we might find ourselves in a much more hostile relationship with China: Could they do us damage domestically by hacking into our electricity grid in Sydney?" Jennings told Australian Broadcasting Corp.

Senator Nick Xenophon, the leader of three senators whose support could be crucial to the government to pass legislation through the upper chamber when Parliament resumes this month, said the foreign investment decision-making process lacked transparency.

"I don't believe it is in the national interest for a state- owned enterprise to control one of our biggest power assets in this country," Xenophon told ABC.

Sydney Morning Herald
E-currencies regulated to fight terrorism (Canada)
Tuesday, 09 August 2016
Byline: Jewel Topsfield

Jakarta - Australia is moving to become one of the first countries to regulate e-currencies such as bitcoin under its anti-money laundering and counter-terrorism financing laws.
Bitcoin - the most prominent digital currency to emerge globally - is backed by a computer code rather than a physical substance such as gold or mainstream currency.

The anonymity of payments using digital currencies make them attractive for terrorism financing, according to Australia's financial intelligence agency, AUSTRAC, which is co-hosting a counter-terrorism financing summit with Indonesia in Bali this week.

Justice Minister Michael Keenan will inform the summit of the work Australia is doing to improve its anti-money laundering and counter-terrorism financing legislation after a review recommended the regulation of digital currencies.

"The report ... recommends strengthening an already robust legal framework to respond to new and emerging threats," he said.

"The government is committed to facilitating growth and innovation in this sector and appropriate anti-money laundering and counter-terrorism financing regulation will aid that development."

The AUSTRAC report, Terrorism Financing in Australia 2014, said electronic, online and new payment methods posed an emerging terrorism financing risk, which was likely to increase over the short term as use of these systems grew.

"Terrorist groups engaged in radicalisation, recruitment and communication online [such as through social media] are a particularly high risk of using online payments systems and digital currencies," it said.

"Prepaid travel money cards [a type of stored value card] have also been used to transfer funds offshore for terrorism financing."

AUSTRAC's national manager of strategic intelligence and policy, Brad Brown, said there were examples of the misuse of bitcoin globally.

He pointed to Mt Gox, a defunct bitcoin exchange in Tokyo where bitcoins worth hundreds of millions of dollars went "missing", and Silk Road, a now closed online black market that sold illegal drugs.

"I think it's important to regulate where there is a potential risk of abuse of money laundering and terrorism financing," Mr Brown said.

The statutory review of the Anti-Money Laundering and Counter-Terrorism Financing Act, which Mr Keenan tabled in Parliament on April 29, recommends the act be amended to regulate activities relating to digital currency.

It also recommends the definition of e-currency be broadened to include digital currencies such as bitcoin that are not backed by a physical asset.

"While digital currencies have undoubted legitimate uses, the transfer of convertible digital currencies can occur without passing through the formal financial sector," it says.

"This provides another tool for criminals and terrorist financers to move and store illicit funds beyond the reach of law enforcement and other authorities and purchase illicit goods and services."

In 2014, Canada became the first country to regulate bitcoin and other virtual currencies under its anti-money laundering and counter- terrorism financing laws.

The Australian
Morrison warned blocking China tender will hurt ties and budget
Tuesday, 09 August 2016
Byline: Kylar Loussikian and David Uren
Section: oped

Blocking a Chinese state-owned company's $14 billion bid for control of NSW power distribution network Ausgrid could be a -"colossal blow" for the state budget and would risk diplomatic -issues with Australia's largest trading partner, the government has been warned.
After Scott Morrison sparked speculation about State Grid Corporation of China's bid by declaring national security would be his "prime consideration", former premier Bob Carr said rejection would affect NSW's infrastructure plans, while former Liberal federal leader John Hewson described national security concerns as "spurious".

Deputy director of the Australia China Research Institute, James Laurenceson, said a government decision to block State Grid's further involvement in Australian electricity assets would create diplomatic problems for the China relationship.

In 2012, Australia signed a memorandum of understanding with China for co-operation on opportunities for infrastructure investment. Australia promised in the Australia-China free- trade agreement that it would take a non-discriminatory approach to Chinese investment.

Mr Laurenceson told Chinese newsagency Xinhua yesterday Australia had to get away from its Cold War approach. "The people I've talked to in cyber security say ownership and cyber-hacking are two separate issues. If you want to hack a network, you do not need to pay ($11 billion) for the privilege of taking half ownership of that asset," he said.

The Treasurer is under pressure to reject the Chinese offer, with crossbenchers including Pauline Hanson, Bob Katter and Nick Xenophon objecting on -national interest grounds.

Mr Morrison on Sunday said national security would be his "prime consideration" for assessing the sale, which is being considered by the Foreign Investment Review Board.

After a furore over the leasing of the port of Darwin to a Chinese company, Mr Morrison last year appointed former ASIO chief David Irvine to FIRB's board to advise on national security issues.

Maurice Newman, chairman of the Abbott government's business advisory council, yesterday suggested anti-investment sentiment was becoming "a little xenophobic".

"I understand when it comes to agriculture there may be some food security issues, but it's not clear to me what how this is pertinent to the electricity grid," Mr Newman said.

A Moody's spokesman told The Australian the credit ratings agency was considering the effect on NSW's rating of delaying or deferring of the transaction.

State Grid is competing with Hong Kong-listed Cheung Kong Infrastructure, a public company headed by billionaire Li Ka-shing, for a 99-year lease, giving the winner 50.4 per cent of Ausgrid.

Mr Carr, who now heads the Australia-China Relations Institute at University of Technology, Sydney, said if Ausgrid bids were rebuffed, it would be a "colossal blow to the NSW budget, to infrastructure spend, and to the state's economy".

"The simple fact is there are only Chinese bidders for these -assets, ownership of electricity grids doesn't help anyone spy; no owner is going to blow it up.

"State Grid is the single largest owner of the national grid of The Philippines, and the lights in Manila didn't flicker for a second when the two countries were at odds (over the South China Sea)." Concerns about State Grid -include its leaders' close connection to the Communist Party and People's Liberation Army, and suspicions the company made a higher bid for strategic, rather than commercial, reasons.The Baird government will use the proceeds from the deal, together with $10.26bn from selling TransGrid, to fund $20bn worth of infrastructure projects. FIRB approved State Grid's unsuccessful bid for TransGrid.

The Australian
Data is only of value when it can be accessed
Tuesday, 09 August 2016
Byline: Anthony Wong

Op-ed: Amid all the noise about big data, the internet of things and open government data (OGA), it's tempting to think that if we just run the algorithm, slice the data and dive into the analytics, we'll gain the insights and intelligence we need to change the world.
It's not quite that simple. Data is the new capital and as the current debate over tonight's census clearly illustrates, data increases in value according to its level of specificity, uniqueness, maintainability, reusability and relevance to the audience, along with the integrity of the actual data.

But the value can only be unlocked through access. Sensitivities of the census aside, there are enormous economic benefits to be gained from appropriately increasing access to different government data sets.

This is the main driver for the current Australian Productivity Commission review into data availability and use. The commission has received more than 150 responses from stakeholders across the community and is due to release its draft report in -November this year.

The Australian Computer Society's response outlined a series of recommendations designed to provide a consistent, predictable framework within which government data can be classified, managed and shared in ways that will benefit all Australians.

We should continue to strongly advocate the benefits of data sharing and OGA as major drivers of innovation and productivity. The Australian Government Bureau of Communications Research suggests the potential economic return for Australian from effective use of OGA could be as high as $25 billion per annum.

But in order to create an environment conducive to the development of the trust so essential for effective open government, we need a range of measures aimed at improving collaboration and ensuring privacy protection. The ACS response to the Productivity Commission includes recommendations for: . Mandatory reporting of data breaches.

. The appointment of an open data evangelist, both to oversee strategic and operational progress, and to advocate for the rights of individuals.

. A national education and awareness-raising campaign.

. A review of regulatory and legislative settings to ensure they align with, and actively enable, a world-leading open data regime.

. A framework that defines and supports anonymisation of valuable datasets to facilitate wider sharing while protecting individuals and organisations.

. A nationally accepted definition for personally identifiable data (PID) and recommended methods for de-identifying PID from other data.

. A new accounting standard.

Australia lags behind the UK and the US when it comes to releasing public data for business. By embracing the potential of open government we could maximise the inherent opportunities for all Australians.

Anthony Wong is president of the ACS and chief executive of AGW Consulting, a multidisciplinary ICT, intellectual property legal and consulting practice.

The Australian Financial Review
Security fears deter investors, say academics
Tuesday, 09 August 2016
Byline: Lisa Murray

Shanghai - The Australian government is putting Chinese investors offside by stressing national security concerns in the Ausgrid sale before any final regulatory decision has been made, according to two senior Chinese government-linked academics.
Han Feng, from the state-run China Academy of Social Sciences, said it was inappropriate for Australian politicians to be making comments ahead of a decision from the Foreign Investment Review Board, which is assessing bids from China's State Grid and the Hong Kong- listed Cheung Kong Infrastructure.

"This will have a negative impact on the long-term investment relationship and it's not good for the China-Australia relationship," said Mr Feng, a former deputy director and researcher at CASS's National Institute of International Strategy.

"When the [Australian] government stresses national security concerns, it needs to explain to China what the rules are."

Australian Treasurer Scott Morrison earlier stressed security was the "primary consideration" in assessing the bids for a 50.4 per cent stake in Ausgrid, the country's biggest electricity distribution grid. He signalled the federal government would be prepared to go against NSW Premier Mike Baird to block the sale.

Wang Zhenyu, from the China Institute of International Studies, a think tank attached to the Foreign Ministry, said Mr Morrison's emphasis on national security was an "investment barrier" for Chinese companies.

"In my view, Australian politicians make these comments based on domestic politics rather than economic considerations," he said.

"This would create negative sentiment among Chinese investors looking at Australia because it suggests their investment is not welcome. This shows the Australian government's inclination not to support Chinese investment."

Security analysts have raised concerns about the bid from State Grid given it is a state-owned enterprise and has strong links with the Communist Party and the military at a time when Beijing is adopting an increasingly assertive foreign policy stance.

While CKI is listed in Hong Kong and controlled by billionaire Li Ka-Shing, analysts have also pointed out Beijing's growing influence over the city government and its big corporations could be a potential risk.

"These national security concerns are targeted at China and I would describe them as an investment barrier," said Mr Wang. "This is discrimination against investment from China."

Peter Jennings, executive director of the Australian Strategic Policy Institute, recently said the federal government needed to take into account the ability of so-called "malign actors" to shut down critical infrastructure by means of offensive cyber-attacks.

However, James Laurenceson from the Australia-China Relations Institute (ACRI) at the University of Technology Sydney, said that State Grid, which is attracting the most concern, already owned electricity distribution assets in Victoria and South Australia and had been assessed by FIRB.

He also points out the only bidders for Ausgrid are Chinese and if the sale was blocked it would be a big economic loss for NSW.

ABC (Australia)
Jacqui Lambie to push for Foreign Investment Review Board overhaul
Tuesday, 09 August 2016

Byline: Brett Worthington

Tasmanian senator Jacqui Lambie is vowing to push for an overhaul of the Foreign Investment Review Board (FIRB).
The re-elected politician says she will grill officials when they front Senate Estimates later this year over FIRB's history of approving foreign farm and asset purchases had been against the national interest.

"I just don't think they're getting the job done," she told RN Drive.

"Whether it's the Chinese or anybody else buying from outside and when it comes to assets like our power and our water and what's going on with cyber security and all the rest.

"I've had a gutful like many other people have of selling our assets and leasing our assets out there. We've had enough."

Debate about the role of the FIRB has raged this week as it considers the Chinese state-owned business State Grid's bid for a 50 per cent stake in Australia's largest electricity network.

The FIRB is required to review all foreign investments in farmland, irrespective of size, once a buyer has a portfolio worth $15 million.

It also assesses all agribusiness sales above $55 million.

There is also an automatic trigger for the FIRB to review to invest in Australian farmland.

Senator Lambie last year failed in her bid to amend investment laws to require , regardless of the sale's value.

"You can only sell the farm gate once," she said this week.

But Professor James Laurenceson, from the Australia-China Relations Institute, rejected the need for an overhaul of FIRB.

the appointment of former ASIO boss David Irvine to review board late last year had it well placed to assess foreign purchases.

"Look I think it is helpful to have someone like David Irvine casting their mind over these deals and look each deal is going to be different.

"I don't think it necessarily serves the national interest to have a fixed-in-stone approach."

The Australian Financial Review
China 'spies' put power sale at risk (Canada)
Tuesday, 09 August 2016
Byline: Aaron Patrick and Primrose Riordan

Canberra - Chinese spies have been caught by the intelligence services conducting "brazen" espionage in Australia over the past year, hardening concerns within the federal government about allowing a Chinese company to buy a $10 billion power company from NSW.
Senior government officials were "deeply concerned by the consequences" of a Chinese state- owned company, State Grid Corp, being issued a 99-year lease to operate Ausgrid, which provides all of Sydney's electricity, according to a security source. There were at least 60 cyber attacks on energy networks last financial year, according to official figures.

Cabinet's national security subcommittee has already been briefed on their concerns and Treasurer Scott Morrison seems not to be afraid of vetoing the deal, which would fund a large part of the NSW Coalition government's new infrastructure projects.

"That's the job. There are no easy decisions. This is not an easy decision and there are implications of the decision either way. Foreign investment is a very sensitive issue out there in the public and it has to be managed carefully," Mr Morrison said.

The decision over Chinese investment in Australia's power grid is shaping up as the first major foreign policy test of the re-elected Turnbull government, which wants to promote foreign investment to drive the economy.

Along with State Grid Corp, Cheung Kong Infrastructure, the largest publicly-listed infrastructure company in Hong Kong, is also waiting for government clearance to purchase a 99-year lease for 50.4 per cent of Ausgrid.

State Grid Corp already owns electricity networks in South Australia and Victoria and was cleared by the Foreign Investment Review Board to bid last year for Transgrid, a NSW electricity distributor that was sold to Canadian interests.

Sources said the change in ministers last year meant the bureaucracy had to work hard to explain to the government's new leaders the threat posed by Chinese espionage, and the discovery of several Chinese agents "red handed" had highlighted the security challenges.

Security experts said Chinese security services were active in Australia and making Ausgrid the responsibility of a company controlled by the Chinese central government was too great a risk.

"The public has to understand that there are some countries taking substantial intelligence operations against this country," said Ross Babbage, a former senior Defence Department official and the managing director of consulting firm Strategy International.

"This is not a figment of someone's imagination. It takes a big leap of faith to say there is no security risk [from selling Ausgrid]."

Former Ausgrid chief George Maltabarow said critics of State Grid Corp's bid were "xenophobic" and security threats could be resolved by the buyer.

"I don't really believe that the security concerns are really justified and some of it seems to be just plain xenophobia to me, populist xenophobia that you do get from some politicians," Mr Maltabarow said.

"The idea that somehow the governance of the company is going to be result in security being compromised I think is just pathetic. Quite frankly, if the Chinese wanted to hack into the Ausgrid systems, they don't need to own it."

Former prime minister Tony Abbott added his voice to the debate on Monday, saying he was not opposed to foreign investment, but there should be a way of selling the grid that does not cede control of the asset.

Ausgrid, which has been state owned for 112 years, supplies electricity to Sydney, the NSW Central Coast and the Hunter Valley. It has more than 200 large electricity substations, 30,000 small distribution substations, 500,000 power poles and almost 50,000 kilometres of electricity cables.

Deakin University Research Fellow Shihanur Rahman, who researches grid cyber security, said it was entirely possible for a grid to become a target if it was sold to a foreign government. "For the data that is stored in a secure database, what we called secure, the existing security is not sufficient," he said.

Knocking out one of the bidders could reduce the amount the NSW government gets.

The Pioneer
The spy who hacked a thousand Indian sites
Tuesday, 09 August 2016

New Delhi- Pro- Pakistan hacker Afzal Faizal who breached the firewalls of more than a thousand Indian websites in the last two years has come under the scanner of Indian security agencies, five days after he claimed to have got access to the e- payment system of a nationalized bank.
Intel officials said earlier, Faizal restricted his hacking efforts to defacing random websites and teasing Indian techies, but has now stepped up to target websites of the Indian government and critical institution such as banks.

Cyber security experts went into tizzy when on August 2, Faizal claimed to have got access to E-payment gateway of nationalized bank. Officials, however, claim that no financial loss or data leak took place. After the defacement, he also challenged Indian hackers to secure the Indian cyber space as he may target more such critical websites in the future. Similarly, in June this year, he had hacked the websites of the Indian embassy in up to seven countries and defaced them with pro-Pakistan messages as a warning to India.

The hacked websites had an image of a person in a red and black hooded jacket, with a message: "Intruder Here. You got hacked". This included websites of Indian embassies in Dushanbe (Tajikistan), Bucharest (Romania), Athens (Greece), Ankara (Turkey), Mexico City, Sao Paolo and Pretoria. The hackers also left a message on the front page of the website that read, "Hey Indian Government, Don't Mess with Us." "Faizal and other members of Pro-Pakistan hacking community have carried out some serious attacks recently. They have hacked several government websites in north-eastern and southern states. They have also made a breakthrough in web security system of banks and educational institutions. They are mocking Indian web security at a time when country is pushing for digital India," a senior officer of central security agency told Mail Today.

He explained that all such attempts are being seriously monitored and as most of these hackers are based out of India. He added that they are being tracked and monitored online. Experts believe that Faizal was also tracked in Dubai recently and may be routing his attacks from South-Asian countries, including Indonesia.

Earlier, Pakistani hackers used to carry mass defacement but now they are more focused on targeting government websites. Even state police websites are being defaced by Pakistani hackers where they post anti- India comments with an image of the Pakistan flag. However, Indian hackers have taken on the mantle for retaliation and claim a similar large scale attacked will be launched against Pakistan. "He has cre- Vaishnodevi, Amarnath pilgrims stranded due to landslides ated nuisance in Indian cyber world and we will destroy their web space," said a hacker, requesting anonymity. "We had tracked Faizal and even got his accounts blocked in past but now we are working on getting access to their critical establishment and will expose their security by hacking their bank accounts and websites on August 15 and celebrate our Independence Day," the hacker told Mail Today.

Cyber security experts say that attacks coming from Pakistan are alarming, but believe that it is the handiwork of youngtechies. "These are nationalistic hacker groups and they flaunt each successful hack. But, the damage they could create should not be ignored. Each attack on government websites or banks should be treated seriously, which unfortunately is not being done at the moment. Indian hackers have informed about several vulnerabilities in Indian banks, which have not been patched yet," Kislay Chaudhary, a cyber security analyst and CEO of Indian Cyber Army said. Another cyber crime expert, Deep Shankar believes that recent hack attempts are just warm up before Independence Day. "India and Pakistan's Independence Days, which fall on August 15 and August 14 respectively, has seen mass defacement the past few years.

Times of Israel
Major security flaw in 900m Android phones, tablets, says Check Point
Tuesday, 09 August 2016
Byline: Dan Schwartz

Jerusalem - Nearly a billion Android phones and tablets are vulnerable to malware that could allow hackers "complete control of devices and access to sensitive personal and enterprise data on them," according to Israeli cybersecurity firm Check Point.
The hacks are possible due to a series of four vulnerabilities -- dubbed QuadRooter -- affecting Android devices built on Qualcomm chipsets, which are found in nearly two-thirds of mobile devices. "If any one of the four vulnerabilities is exploited, an attacker can trigger privilege escalations and gain root access to a device," said the Check Point research team that discovered the problem.

Unlike most malware, which can be rooted out or at least detected by antivirus software, there's little users can do except wait for Qualcomm to issue patches to fix the problem, according to Check Point. The vulnerabilities are in the chipset's software drivers - the basic operating system-level programs that provide usability to the chipsets - which control communication between the chipset components.

As such, the vulnerability is on the hardware level, built into the device itself - and accessible only through software packages that update those drivers. "Pre-installed on devices at the point of manufacturing, these vulnerable drivers can only be fixed by installing a patch from the distributor or carrier. Distributors and carriers can only issue patches after receiving fixed driver packs from Qualcomm," according to Check Point.

With 900 million devices affected, there is no "safe" phone or brand; the list of devices affected includes some of the most popular models by Samsung, HTC, Motorola, LG and more. Among the many models affected are the LG G4, G5, and V10; Samsung Galaxy S7 and S7 Edge; Sony Xperia Z Ultra; Google Nexus 5X, 6 and 6P; and OnePlus One, 2 and 3.

Android devices, of course, are the industry foil to Apple's ioS devices, with the Android operating system the default OS for manufacturers of devices that are not iPhones. Many iPhones and iPads contain Qualcomm chipsets as well, but because the operating system handles communications and software differently, Apple devices are not vulnerable to the hacks.

Android pitches a big tech tent, inviting manufacturers large and small to build their devices around the operating system, which allows programmers a great deal of freedom in app design (unlike Apple, which places many security and function strictures on programmers).

But according to Check Point, Android's openness, generally considered its strength, is actually its greatest weakness. "A myriad of device models, operating system versions, and unique software modifications makes handling Android vulnerabilities a challenge," according to the Check Point team.

"The earlier these vulnerabilities are born in the supply chain, the more difficult they are to fix. The fragmented world of Android leaves many users exposed to risk, even with out-of-the-box devices."

According to Google, which develops the Android operating system, three of the four vulnerabilities have been patched; a patch to prevent hackers from exploiting the fourth will not be available until September. Until then, said Check Point, users need to tread very carefully - installing only well- known apps, "carefully reading permission requests when installing apps, being wary of apps that ask for unusual or unnecessary permissions or that use large amounts of data or battery life, using known, trusted Wi-Fi networks" -- and hope for the best.

Khaleej Times
Student-run cyber security event in Abu Dhabi hacks a global issue
Tuesday, 09 August 2016
Byline: Silvia Radan

Dubai - The world's largest student-run cyber security event - Cyber Security Awareness Week (CSAW) - will take place at the New York University Abu Dhabi (NYUAD), and the Indian Institute of Technology (IIT), Kanpur, this year in November. Finalists from the Middle East, India, North Africa and the US will compete at the event in November 2016. The event was founded 13 years ago by the New York University Tandon School of Engineering.
This year, the schools are also accepting registrations for the elimination rounds in August and September. Last year, nearly 20,000 students competed in CSAW, from high schools through doctoral programmes, against global contestants, all working from their own computers.

The competitions challenge their knowledge of virtually every aspect of IT security, from hardware and software penetration testing and protection, to digital forensics and government policy.

This year, the best students from the MENA region, India, and the US will earn travel awards to participate in the final rounds, to be held on November 10-12, 2016, at IIT Kanpur, NYUAD, and NYU Tandon.

At the regional CSAW campuses, students network with top professionals who serve as judges, hear experts address emerging issues, meet recruiters eager to fill what is expected to be a shortfall of 1.5 million cyber security professionals by 2020, and face tough competition from other schools.

The CSAW games were founded by Professor Nasir Memon, now chair of the NYU Tandon Department of Computer Science and Engineering, and his students. Memon heads NYUAD's cyber security programme, as well as NYU Tandon's.

Students continue to design the contests under the mentorship of IT security professionals and faculty. "Data security is a critical global issue. Attackers know no national boundaries and neither should those who protect our personal privacy and institutions," said Memon.

"In the past, CSAW brought high school teams to New York. This year, thanks to the leadership of students and faculty, it will expand its reach to high school and university students across the MENA region."

Each regional finalist competition will vary slightly in content. Winners of the final rounds can walk away with cash prizes, scholarships and more. This year, CSAW will have eight different competition categories. Among them is 'Capture the Flag', a hacking competition, 'High School Forensics', a case of fictional murder mystery and 'Embedded Security Challenge', where a Blue Team from NYU Tandon designs a target system and everyone else - Red Teams - will hack it to mimic real-world attacks.

"With hobby hackers, foreign state actors, terrorist organisations and other adversaries abounding, cyber security is not just a computer science topic, but a national security issue. IIT Kanpur is delighted to join hands with the NYU Tandon School of Engineering to bring cyber security awareness competitions to India," said Manindra Agrawal, professor at IIT Kanpur's Department of Computer Science and Engineering.

For more info and registration, visit csaw.engineering.nyu.edu (follow @CSAW_NYUTandon) Preliminary rounds for the Embedded Security Challenge will be held in August; the other preliminary challenges will be in September.

Khaleej Times
Are 900m Qualcomm-powered Android devices at risk?
Tuesday, 09 August 2016
Byline: Alvin R. Cabral

Dubai - Qualcomm's processors are powering over 900 million Android devices globally, which would be a haven for hackers should a vulnerability can be exposed and exploited. Apparently, that could be the case, according to a not-so-inspiring report.
Cyber-security firm Check Point says that it has uncovered a set of four vulnerabilities affecting almost a billion Android devices that use Qualcomm chipsets.

The company called the issue "QuadRooter", which, according to them, is "a set of four vulnerabilities that gives attackers complete control of your Android smartphone or tablet".

"These vulnerabilities are found on out-of-the-box devices and can only be fixed by installing patches when they become available," the report added.

The company listed the following devices as among those that can potentially be compromised: BlackBerry Priv; Blackphone 1 and 2; Google Nexus 5X, Nexus 6 and Nexus 6P; HTC One, M9 and 10; LG G4, G5 and V10; the new Motorola Moto X; OnePlus One, 2 and 3; Samsung Galaxy S7 and S7 Edge; and Sony Xperia Z Ultra.

While there has been no proof so far that these vulnerabilities have been used for illegal means, it could happen "in the next three or four months", Check Point head of mobility product management Michael Shaulov said in a BBC report.

In the UAE, the devices listed are available either from retailers, online or both.

However, latest figures from the Telecommunications Regulatory Authority (TRA) show that there might not be much of a concern here in the UAE.

The TRA report, released on August 7, revealed that in the first quarter of 2016, 68.9 per cent of handsets registered on the UAE's networks were smartphones, with the iPhone 6 and iPhone 5 - which use ARM chipsets - being the most used at 4.48 per cent and 2.39 per cent, respectively.

The Samsung J100H/J1, which uses Spreadtrum, and the iPhone 6s were third (1.81 per cent) and fourth (1.69 per cent), respectively. The Nokia 108 feature phone was overall the second most-used phone at 2.92 per cent.

The report added that Samsung is the most widely-used brand in the UAE in the January-to-March period, boasting a 33 per cent share of all registered handsets. Nokia was second at 28 per cent, followed by Apple (14 per cent) and BlackBerry (two per cent).

However, no specific device breakdown was provided. As at Press time, the TRA was unreachable for comment.

Khaleej Times also sought statements from device manufacturers listed in the Check Point report.

BlackBerry says that its engineers in its headquarters in Canada are looking into the matter, while LG Gulf says it has not received any statement from its corporate offices in Seoul.

HTC, Samsung and Sony Mobile did not respond to requests either, while Qualcomm has yet to release a statement on the report.

Shaulov is just hopeful that those who would find the bugs first are the type who would squash them. "It's always a race as to who finds the bug first - whether it's the good guys or the bad."

Asharq Al-Awsat
Russia Admits Drone Entered Israeli Airspace
Tuesday, 09 August 2016
Byline: Nazir Majli

Tel Aviv - Three weeks after the Russian drone entered the Golan Heights airspace, Moscow admitted to the incident saying that it belonged to the Russian forces stationed in Syria.
A high-ranking Israeli source, who spoke on condition of anonymity, said the drone had crossed into the Israeli airspace as a result of human error.

The incident was considered the gravest between the Russian and the Israeli armies since Russian President Vladimir Putin declared the deployment of the Russian military in Syria in September 2015.

On July 17, a Russian aircraft crossed four kilometers into the airspace under Israeli occupation. Israel fired two Patriot missiles and an air to air missile at the unidentified drone, but the missiles failed to intercept the drone returned to its origin.

Following the incident, a series of discussions were launched between officials at the Russian and Israeli armies as part of their coordination mechanism.

Investigations by the Israeli army revealed that the aircraft was a Russian drone, yet the infiltration was not clear whether it was an error or intentional to gather information or test the Israeli response.

The Israeli official said that Russians had clarified that the crossing over was an error.

He added that this was also discussed during a phone call between the Israeli Prime Minister Benjamin Netanyahu and the Russian president on July 23.

The Russian statement issued back then didn't discuss the incident and stated that the phone call was about the coordination against terrorism between both countries. The two also discussed regional matters.

During his meeting with political correspondents last week, Netanyahu refused to comment whether the drone was Russian, but didn't deny the information either. He told the press that there is constant communication between Israel and Russia regarding Syria. He added that coordination is important between the two armies.

The Guardian (London)
The state of cyber security: we're all screwed
Tuesday, 09 August 2016
Byline: Dan Tynan

Las Vegas - When cybersecurity professionals converged in Las Vegas last week to expose vulnerabilities and swap hacking techniques at Black Hat and Defcon, a consistent theme emerged: the internet is broken, and if we don't do something soon, we risk permanent damage to our economy.
"Half of all Americans are backing away from the net due to fears regarding security and privacy," longtime tech security guru Dan Kaminsky said in his Black Hat keynote speech, citing a July 2015 study by the National Telecommunications and Information Administration. "We need to go ahead and get the internet fixed or risk losing this engine of beauty."

There's no lack of things to be worried about: organized cybercriminal gangs; government surveillance; not to mention hack attacks from nation states.

That may be good news for the cybersecurity industry, which is expected to grow more than 10% annually and surpass $200bn worldwide by 2021, according to research firm Markets and Markets.

But it's bad news for the rest of us. As we conduct more of our lives online, we're being asked to become increasingly savvy about computer security. Many are simply uninterested or not up to the task.

Add up all these factors, and the question becomes not why many consumers are losing confidence in the internet, but whether they should have any confidence at all.

Consumers: the new ATM for cyber crooks The online crooks' weapon of choice: crypto-ransomware, which encrypts all the data files on a user's machine, making them inaccessible. The malware, which accounts for nearly 60% of all infections, according to research firm Malwarebytes, then displays a screen demanding hundreds of dollars. If victims don't pay up in time, the files are destroyed.

"Over the last few years attackers realized that instead of going through these elaborate hacks - phishing for passwords, breaking into accounts, stealing information, and then selling the data on the internet's black market for pennies per record - they could simply target individuals and businesses and treat them like an ATM," says Brian Beyer, CEO and founder of enterprise security firm Red Canary.

According to Symantec, the average ransom paid doubled from just under $300 in 2015 to $679 this year. Last year, the criminals behind the CryptoWall3 malware cost victims more than $325m, according to estimates from the Cyber Threat Alliance ; 2016's haul is expected to be significantly higher.

A ransomware attack is relatively easy to overcome if you have a current and complete copy of your data; you can simply restore the untainted files to your machine, says Beyer. (Before you do, though, be sure to install security software that will remove the ransomware, or you may find yourself being jacked all over again, he warns.)

The problem? About 3 in 10 people never back up their data, while others do it sporadically. And even for those who do backup religiously - or use software such as iCloud or CrashPlan that automatically copies files to machines in the cloud - restoring data can be a hassle.

Which is why for many victims it just seems easier to pay up, says Beyer. And that's what the criminals are counting on.

The cyber enemy is us It's a truism that the biggest threat to security isn't increasingly sophisticated cyber criminals, data-hungry corporations or even espionage-happy nation states; it's the people who get duped into clicking random links or opening rogue files.

To paraphrase Pogo : we have met the cyber enemy, and he is us.

In a Black Hat demonstration, Zinaida Benenson, a researcher at University of Erlangen-Nuremberg in Germany, measured how many people would click on a potentially malicious link inside an email, then compared the results to how many did the same with a message they received on Facebook. (Spear phishing, or targeting a specific person via a message containing bogus links, is a common way for attackers to steal information.)

The results: one in five test subjects clicked a link from a stranger in an email; more than twice as many did it on the social network. Lured by curiosity, even tech-savvy users in the study could not resist clicking.

In another study, Elie Bursztein, head of Google's anti-abuse research team, tracked whether people would pick up a USB thumb drive they found lying on the ground and stick it into their computers (which, he noted, was used as a major plot point in season one of USA Network's Mr Robot). His research team left 300 USB drives at various locations at the University of Illinois Urbana-Champagne campus. Unwitting test subjects picked up 98% of them; nearly half plugged the drives in and opened the files contained on them.

Ask security companies what consumers should do to stay safe, and you'll get the same advice they've been handing out for years - use better passwords, keep software up to date, back up your data, etc. Dan Kaminsky's advice is more stark: keep a close watch on your financials and immediately report anything that looks suspicious.

"If you have a bank account that will not send you a text message when there's a transaction, move your money," he says. "Because now it's not about preventing the fraud, it's about seeing it as soon as it happens."

In other words, assume you're going to be hacked, and try to catch it before it does too much damage.

Could the situation change? If everyone really followed all the advice out there, we wouldn't be in this mess. But they don't. Many consumers will never do any of these things, and scant few will do all of them all the time.

Jake Braun, CEO of strategic security consultancy Cambridge Global Advisors, says moves by companies such as Apple, Google, and Facebook to encrypt data and communications are a huge step in the right direction. When your data is encrypted, the bad guys can't get to it. (And, sometimes, neither can the good guys. That's why the US government is putting huge pressure on these companies to relax their encryption standards to allow access by law enforcement - known colloquially as " the crypto wars ".)

Braun is optimistic that as younger generations take over, they'll demand more secure versions of products from vendors. Still, he says, the scope of the problem is so large that more government intervention is needed.

"I think consumers should be putting more pressure on their elected officials to fund criminal investigation programs that more aggressively track down cyber criminals domestically and abroad," Braun says. "For example, the Homeland Security investigations unit investigates many types of cybercrime (most notably child pornography and online human trafficking that often targets unwitting children) but is embarrassingly underfunded."

In his keynote, Kaminsky called for a federal agency devoted to security issues, similar to the National Institutes of Health, that can "create engineering solutions to the real-world security problems that we have".

"It can't just be two guys," he said. "I need a pile of nerds to be able to work for on this 10 years. We can support health and energy and roads and cars, but somehow we can't support the thing that is driving our economy right now? That's crazy."

Reuters
New spyware detected targeting firms in Russia, China: Symantec
Monday, 08 August 2016
Byline: Staff report

Frankfurt - A previously unknown hacking group variously dubbed "Strider" or "ProjectSauron" has carried out cyber-espionage attacks against select targets in Russia, China, Iran, Sweden, Belgium and Rwanda, security researchers said on Monday.
The group, which has been active since at least 2011 and could have links to a national intelligence agency, uses Remsec, an advanced piece of hidden malware, Symantec researchers said in a blog post.

Remsec spyware lives within an organization's network rather than being installed on individual computers, giving attackers complete control over infected machines, researchers said. It enables keystroke logging and the theft of files and other data.

Its code also contains references to Sauron, the all-seeing title character in The Lord of the Rings, Symantec said. Strider is the nickname of the fantasy trilogy's widely traveled main character Aragorn.

Separately, Moscow-based Kaspersky Lab has labeled the same group using the Remsec spyware as "ProjectSauron".

The newly discovered group's targets include four organizations and individuals located in Russia, an airline in China, an organization in Sweden and an embassy in Belgium, Symantec said.

Kaspersky said it had found 30 organizations hit so far in Russia, Iran and Rwanda, and possibly additional victims in Italian-speaking countries. Remsec targets included government agencies, scientific research centers, military entities, telecoms providers and financial institutions, Kaspersky said.

"Based on the espionage capabilities of its malware and the nature of its known targets, it is possible that the group is a nation state-level attacker," Symantec said, but it did not speculate about which government might be behind the software.

Despite headlines that suggest an endless stream of new types of cyber-spying attacks, Orla Fox, Symantec's director of security response said the discovery of a new class of spyware like Remsec is a relatively rare event, with the industry uncovering no more than one or two such campaigns per year.

Remsec shares certain unusual coding similarities with another older piece of nation state-grade malware known as Flamer, or Flame, according to Symantec.

Kaspersky agreed that the same group it calls ProjectSauron appears to have adopted the tools and techniques of other better-known spyware, including Flame, but said it does not believe that ProjectSauron and Flame are directly connected.

Flamer malware has been linked to Stuxnet, a military-grade computer virus alleged by security experts to have been used by the United States and Israel to attack Iran's nuclear program late in the last decade

Reuters
Facebook Denies Withholding User Data in German Criminal Investigations
Monday, 08 August 2016
Byline: Staff report

Berlin - Facebook rejected on Monday claims made by Germany's state authorities that it was reluctant to co-operate with them on criminal investigations, saying many of the requests it received for user data were incorrectly formulated.
Several regional interior ministers have complained that the social media group is hesitant to respond to requests for data and have called on the Federal Justice Ministry to introduce new laws.

But Facebook said it had provided "round the clock assistance" to the authorities in Bavaria following a spate of violent attacks in Munich, Wuerzburg and Ansbach last month.

A spokeswoman for the Justice Ministry said it was examining whether there was a need to change the law or whether there was a problem with its implementation.

A recent spate of attacks in Germany has highlighted the importance security agencies give to working with social networks to uncover possible links to militant groups.

Police said the Ansbach bomber had six Facebook accounts including one held under a false identity. Traces of an online messaging conversation found on his phone also suggest he was influenced by an unknown person up until the time of the attack, Bavaria's interior minister said.

Germany's spy chief called on Monday for a more intensive exchange of information between social networks and security agencies in the fight against terrorism.

"Social networks are an important communication method for jihadists. Therefore closer co-operation between the security agencies and the operators of social networks is necessary," Hans-Georg Maassen, the head of the BfV domestic intelligence agency, told the Rheinische Post newspaper.

Facebook produced data for 42% of requests in Germany relating to criminal cases in the second half of 2015, compared with 54% in France and 82% in Britain. It said it rejected requests that were overly broad or vague.

The company said it worked with law enforcement officials to help them use their systems, but said there were still a large number of officers that didn't know how to make a successful request.

"Along with our points of contact in Law Enforcement we work tirelessly to raise awareness of the correct procedures," a Facebook spokeswoman said.

A spokesman for the Interior Ministry said co-operation between Facebook and the BKA federal police agency and the BfV was good.

"Conversations are constructive and co- operation is also fruitful as far as we can see," he said, adding they were not in a position to judge how well Facebook worked with the state authorities.

The Express (UK)
Lawyer with links to Russian secret service says Edward Snowden is 'alive and well'
Monday, 08 August 2016
Byline: Will Stewart

London - A lawyer with close links to the Russian secret services took the extraordinary step of announcing that US whistleblower Edward Snowden is "alive and well".
Rumours spread following a mysterious 64- character tweet appeared on Snowden's Twitter account and was then deleted, triggering speculation that he had been kidnapped or even killed.

The former National Security Agency (NSA) contractor, wanted in the US for spilling state secrets, currently has asylum in Russia granted by Vladimir Putin.

Lawyer Anatoly Kucherena said: "I can authoritatively say that he is alive and well, he is living in Russia and is busy with his favourite work."

The lawyer, close to the secret services, did not explain how suspicious messages appeared on Snowden's Twitter account, or what they meant.

Nor has Snowden been seen in public.

But Kucherena said: "Again, we are seeing certain speculations about Edward Snowden.

"Of course, there probably are people interested in speculating on this matter who have been doing this for the last several years."

He claimed without further explanation that "the appearance of certain codes in his Twitter does not mean that he is in danger of some sort.

"This is an attribute of his work and there is nothing bad about it."

One message sent out on Snowden's account read: "It's time."

The second carried 64 characters of code. Both were then deleted.

In 2013, computer geek Snowden started revealing classified documents pertaining to mass surveillance practices carried out by US authorities around the globe.

The same year, Russia granted the whistleblower temporary asylum for one year.

In August 2014, Snowden received a three-year residence permit to live in Russia.

In the United States, he faces up to 30 years in prison on charges of espionage and theft of government property.

Kucherena has represented Snowden since 2013.

Glenn Greenwald, a journalist who helped Snowden to leak details of the secret US data, said the whistleblower was fine.

Reuters
European intelligence database seen aiding fight against suspected militants
Monday, 08 August 2016
Byline: Staff report

Amsterdam - A European counter-terrorism intelligence database designed to generate greater intelligence sharing among allies to avert deadly Islamist attacks has gone online after overcoming traditional reluctance by spy agencies to sharing information.
European officials were spurred into setting up the project by the Paris attacks last November by Islamist militants which exposed intelligence gaps. A total of 130 people were killed in those attacks.

Hosted by the Dutch intelligence service in the Hague, the database went live on July 1, the German Interior Ministry and the German domestic intelligence agency (BfV) said.

"The intelligence database will make it much easier and quicker to share information about possible threats," said one intelligence official.

The database enables European intelligence agencies to share real-time information about suspected Islamist militants collected by members of the Counter-Terrorism Group (CTG), which groups all 28 European Union countries, Switzerland and Norway.

Its creation marks a step forward in the fight against Islamic State, which is focused increasingly on orchestrating large-scale and "lone wolf" attacks as it suffers setbacks and loses territory in Iraq and Syria.

"We need a close exchange of information that is rapid and comprehensive, based on the relevant legal and privacy regulations," said one official at the German interior ministry.

A refinement of earlier databases, the new system is designed to make it easier to cross-reference material provided by different countries' security services, a Dutch security services official told Reuters.

"If we see one of our targets traveling to Amsterdam, we haven't been checking until now if his brother or nephew is also traveling," the official said, giving an illustration of the way the new database worked.

European police agencies have long shared information about potential criminals through Europol and Interpol, but spy agencies are generally reluctant to share intelligence data, except on a specific case-by-case or bilateral basis.

Lack of cooperation was a focal point after the Paris attacks. Several of those involved in the attacks had been on the radar of authorities in other countries.

Abdelhamid Abaaoud, suspected mastermind behind the Paris attacks, for instance, had mocked European frontier controls and boasted how easy it was for him to move between Syria to his Belgian homeland and the rest of Europe.

In another case, the former French spy Claude Moniquet has been quoted as saying that France did not pass on information about Mehdi Nemmouche, a French-Algerian dual national, who shot four people at the Jewish Museum in Brussels in 2014.

After Abdesalam's arrest, U.S. officials privately disparaged European intelligence-gathering and said they were working closely with European authorities to ensure they had the training needed to prevent another Paris-style attack.

The Netherlands, which held the rotating EU presidency at the time, played a key role in setting up the database. Dutch officials urged global counter-terrorism officials to agree to greater sharing of banking details and key data about potential militants after missed signals in Paris.

In the past, they said, countries often failed to share lists of suspects whose assets had been frozen, making it possible for someone blacklisted in one country to drive across the border and use their bank cards in a neighboring country.

ABC News
Concerns About Election Day Cyberattacks Mount in the Wake of DNC Hack
Tuesday, 09 August 2016
Byline: Geneva Sands

New York - Officials and security experts have raised concerns about potential Election Day cyber vulnerabilities amid reports that hackers -- believed to be from Russsia -- breached the Democratic National Committee's (DNC) computers last month.
On Monday, the Ranking Member of the Senate Homeland Security Committee called on the federal government to examine its efforts to protect election systems and voting machines in the United States against similar attacks.

"Election security is critical, and a cyberattack by foreign actors on our election systems could compromise the integrity of our voting process," wrote Sen. Tom Carper, D-Del., in a letter to the Department of Homeland Security (DHS).

The DNC intrusion raised concerns about the ability of foreign actors to interfere in the American political process, including through cyberattacks targeting electronic voting machines or the information technology of state and local election officials, wrote Carper.

The senator said that while the risk of voter fraud and a successful cyberattack is remote, the federal government can play a role in addressing the potential for these types of attacks.

The letter follows DHS Sec. Jeh Johnson's announcement last week at that the department should consider designating the election system "critical infrastructure," like the power grid, which would have "several implications."

The official designation would make it easier to unlock the department's resources to help local and state jurisdictions, according to a Senate aide.

In response to the DNC hack, CIA Director John Brennan said, "if there has been some manipulation of the election process here, this is going to be something that this government and our country is going to have to look at," during the annual Aspen Security Forum at the end of July.

He said the nation will have to look at "what the vulnerabilities are to the system out there," and some places may decide to go with paper ballots. But he said the country should focus on strengthening the cyber security of the relevant systems.

"[The DNC hack] points out a number of imperatives for the Congress, and chief among them are ensuring the integrity of the election itself," said Rep. Adam Schiff (D-Calif.) at the same conference.

There are currently more than 9,000 different voting jurisdictions and security varies widely among them.

Forty-three states are using electronic voting machines that are at least 10 years old, "perilously close" to the end of most systems' expected lifespan, according to a report by the Brennan Center for Justice.

In many cases vendors no longer serving the machines and as a result election officials are "basically jerry- rigging" these systems, said Larry Norden a deputy director at the Brennan Center.

"If you have a system that has a lot of reliability flaws, those are security concerns as well," he said.

People imagine votes are going to get switched, but there's also the threat of denial-of-service attacks, which could result in long lines or voting disruptions, said Norden.

However, Norden points out that a lot of progress has been made over the past ten years, moving from electronic-only ballots to ballots with a paper trail.

This November 80 percent of Americans will vote on with paper ballot or machine with paper trail. A paperback-up is an important deterrent to make sure bad actors don't hack the machines or infrastructure, said Norden.

Reuters
Australia sets up specialist cyber unit to trace terrorism payments
Tuesday, 09 August 2016
Byline: Staff reporter

Sydney - Australia has set up a cyber-intelligence unit to identify terrorism financing, money laundering and financial fraud online, the government said on Tuesday, because of "unprecedented" threats to national security.
The measure expands on a major platform of conservative Prime Minister Malcolm Turnbull, who narrowly won re-election last month after promising to improve Australia's cybersecurity and transform the economy into a tech-savvy business hub.

Justice Minister Michael Keenan said the new unit, set up under money-tracking agency the Australian Transaction Reports and Analysis Centre (AUSTRAC), would investigate online payment platforms and financial cybercrime to crack down on money-laundering and criminal networks.

"We know that the use of fraudulent identities continues to be a key enabler of serious and organised crime and terrorism," Keenan said in a statement.

The statement said the new AUSTRAC unit would work with the Australian and New Zealand government-funded identity support service, ID Care, to target job recruitment scams that crime syndicates used to recruit innocent people to traffic money between jurisdictions.

The new unit would also work with the Australian Cybercrime Online Reporting Network to identify patterns and trends that could indicate large-scale financial scams or their methodology, Keenan said.

Reuters previously reported that a decision by Australia's major banks to stop offering overseas remittance services had driven the money transfer business underground, making it harder for the authorities to track.

In February, unknown hackers tried to steal nearly $1 billion from the Bangladesh central bank's account at the Federal Reserve Bank of New York, and succeeded in transferring $81 million to four accounts at RCBC in Manila.

Wall Street Journal
Security Screeners Cut Corners at Rio Games
Tuesday, 09 August 2016
Byline: Multiple reporters

Rio de Janeiro - Security screeners posted outside some Olympics venues have taken to waving spectators through checkpoints without X-raying their bags in order to help reduce long lines, the latest breakdown in a process that has raised fears about lax security at the Rio Games.
Olympics security officials have at times been halting the use of X-ray scanners and instead inspecting bags by hand to help shorten wait times, an organizing committee spokesman said Monday.

He said security personnel were also performing "random" checks, an acknowledgment that at times not all bags are being screened in an effort to speed the lines.

At several Olympics locales over the weekend, including the beach-volleyball stadium in Copacabana and the equestrian venue in Deodoro sports complex on the city's north side, screeners opted for visual inspections of bags in lieu of machine screening of backpacks and purses. In some cases, screeners didn't review bags at all, although ticket holders were required to walk through metal detectors.

Mario Andrada, a spokesman for the Rio 2016 Organizing Committee, said the occasional lack of X-ray screening was deliberate, describing it as a move meant to reduce congestion. Security lines to enter some Olympic venues have been so long that some fans have given up, leaving swaths of empty seats at many events.

"Sometimes we go to manual screening when we see the lines forming...but it's never like, open the doors, open the gates," Mr. Andrada said. "We do manual screening and we do random screening and we have very experienced people." Mr. Andrada said such moves don't compromise security.

But Benjamin Yelin, a senior law and policy analyst at the University of Maryland Center for Health and Homeland Security, said shelving X-ray screening at a megaevent is a "radical" move that should only be attempted by veteran screeners capable of quickly assessing which people pose the highest risks.

"It's a significant step to sacrifice X-ray screening," Mr. Yelin said. "You can be incredibly skilled and still not be able to do the level of security that's achieved when every single person is subject to an X-ray."

As the Games officially opened Friday, Brazil's government was still scrambling to patch together a team of weapons screeners to pat down spectators and search for weapons and other contraband outside

Olympics venues. The government was forced to call up retired police officers with little experience operating X-ray machines to replace a similarly inexperienced private contractor that had failed to hire enough staff after Brazil waited until July 1 to award the contract.

On the eve of the opening ceremonies, the retired police officers were still being trained in the use of metal detectors and other equipment, according to Brazil's Ministry of Justice, which is in charge of venue security.

A spokesman for the Ministry of Justice didn't immediately respond to a request for comment about the latest screening issues.

Brazil has been on high alert following recent terror attacks in Europe, Turkey and the U.S. The federal government has deployed about 85,000 police and soldiers during the Games. Brazilian officials have repeatedly assured visitors and competitors that they will be safe while in Rio, and that security measures for the Games are adequate. Heavily-armed soldiers and police are stationed throughout the city.

In July, Brazilian authorities arrested at least a dozen suspected Islamic State sympathizers, who police said had been planning attacks during the Olympic Games.

But the screening lapses, plus a spate of recent muggings in Rio, have cast doubt on the effectiveness of Brazil's massive show of force.

Over the weekend Portugal's Minister of Education was robbed at knife point near the rowing venue, and a Chinese athlete was robbed of his luggage last month by a thief pretending to be drunk.

Brett Costello, a photographer for News Corp Australia, lost around $40,000 of camera equipment Thursday after a team of thieves snatched his bag at a coffee shop in Ipanema. One of the alleged thieves was captured two days later when Mr. Costello spotted him walking inside the Olympic Park.

The suspect, who was wearing Mr. Costello's Olympic-issued photographer's vest, had apparently slipped through security without the official press credentials required of all journalists seeking to enter the facility.

News Corp owns The Wall Street Journal.

Journalists have observed a number of security lapses at Olympic venues. At the media center near Rio's main Olympic Park on Sunday, a Journal reporter was waiting for his bag to be checked at the entrance when security workers walked away, leaving the journalist free to enter the facility with no challenge or inspection. Two others wandered out of the perimeter of the Olympic Park on Saturday and got back in through an unguarded gap in a security fence.

Mr. Andrada, however, cast the security- screening operation as a success because it has significantly reduced wait times outside the venues.

"Yesterday the main goal was, let's get rid of the lines without compromising security," Mr. Andrada said Monday of the previous day's events. "We did that."

The Daily Beast
Spies-for-Hire Now at War in Syria
Tuesday, 09 August 2016
Byline: Kate Brannan

Washington - Every day at 5 p.m., the Pentagon releases a list of that day's contracts worth more than $7 million. On July 27, buried in the daily email was an eye-catching detail: military contractors would be working inside Syria alongside the roughly 300 U.S. troops already deployed there.
This appears to be the first time the Pentagon has publicly acknowledged that private contractors are also playing a role in the fight against the so-called Islamic State inside Syria, and it's one more signal that the U.S. military is deepening its involvement in the fate of the country.

The contract announcement said Six3 Intelligence Solutions -- a private intelligence company recently acquired by CACI International -- won a $10 million no-bid Army contract to provide "intelligence analysis services." According to the Pentagon, the work will be completed over the next year in Germany, Italy and, most notably, Syria.

Beyond this, details are scant. For example, it is difficult to say, given how little information is available, how many contractors might have to go into the country under this contract. It could be just a few (presumably well-paid) intelligence analysts augmenting a military unit or it could be many more.

The Pentagon and CACI would not elaborate on the kind of work Six3 would be doing either, other than "intelligence analysis services," which encompasses a broad spectrum of activities.

But Sean McFate--a professor at Georgetown University's School of Foreign Service, the author of Shadow War, and a former gun-for-hire himself--told The Daily Beast: "This is no ordinary contractor... Six3 Intelligence Solutions is a private intelligence company, and the fact that we outsource a good portion of our intelligence analysis creates a strategic dependency on the private sector to perform vital wartime operations."

Six3, which gets the bulk of its work from the intelligence agencies, specializes in biometrics and identity intelligence-- figuring out who people really are--as well as cyber and reconnaissance. Its former CEO has said that 95 percent of the company's staff has the highest level of security clearance.

An archived version of Six3's website says this about the company's biometrics division: "Our expertise ranges from finger, palm, face, and iris examinations to exploitation and forensic analysis."

Fewer of its contracts are with the military, but it has previously provided intelligence services in Afghanistan and Europe, as well as supporting the "Counter-Insurgency Targeting Program," and related intelligence and operational support for the Army National Ground Intelligence Center and U.S. forces in Afghanistan, according to a search of the Defense Department's contracts archive.

Recognizing this is an ever- expanding field, CACI acquired Six3 Intelligence Solutions, which had only been around for four years, for $820 million in 2013, describing it as "the biggest deal" in CACI's "51-year history."

At the time of the purchase, CACI CEO Ken Asbury said he thought Six3 would open up an additional $15 billion in contract opportunities. CACI has been providing the U.S. military contractor support for years, including interrogators assigned and working at Abu Ghraib prison at the time of the abuse scandal.

"Contractors do a lot more than drive trucks and cook meals; they do intelligence, pull triggers and support Special Operations forces," McFate said.

So far, there has been no mention of private contractors going inside Syria with U.S. troops, but military contracting and special operations experts said it is safe to assume that Six3 isn't the first.

"I've long said, the military looks at professional services contractors like the old American Express commercial, i.e., they dare not leave home without them," said David Isenberg, author of Shadow Force: Private Security contractors in Iraq.

The intelligence community is particularly reliant on contractors today, he added.

But due to the highly sensitive and dangerous nature of the mission in Syria, little information is unclassified. In Iraq -- where there are just over 4,000 U.S. troops on the ground -- the Pentagon is more transparent. Since last summer, the number of contractors working for the Defense Department had just about doubled from 1,300 to 2,500.

The number has ticked up as the number of U.S. troops on the ground steadily increases and bases grow to house them. Private companies are providing everything from meals to perimeter security at Iraq's Besmaya Compound and Camp Taji, both sites where U.S. troops are training Iraqi soldiers to fight ISIS. In 2015, only 98 people were on the ground in Iraq providing base support. Today, that number is 390, and includes American contractors, third country nationals and local Iraqis, according to a July report from U.S. Central Command.

These are just the Pentagon's numbers. The U.S. government -- including the U.S. Embassy in Baghdad -- employ far more contractors. The Central Command report says there are approximately 7,100

contractors supporting U.S. government operations in Iraq. They're washing laundry, cooking meals and providing security, to name a few of the jobs the U.S. government outsources.

"Contractors encourage 'mission creep' because they allow the Administration to put more people on the ground than they report to the American people," McFate said.

Last week's clue that contractor support is growing in Syria suggests something similar might be happening in that country.

The Pentagon first announced in November that 50 U.S. commandos were deploying to northern Syria to advise forces battling the Islamic State there. Before that, the CIA was believed to be operating in the country, arming rebel groups as part of a separate clandestine program. Needless to say, if contractors were supporting the CIA mission, those details were classified.

In April, the U.S. military presence in Syria expanded when President Barack Obama announced that an additional 250 special operations forces would deploy to help local fighters as they battled ISIS. With more troops on the ground, local infrastructure is quietly being built or improved to support them and the local fighters they are there to advise. For example, the length of an airstrip in Hasakah, a town in northern Syria controlled by Kurdish forces, is being doubled to receive larger planes, CNN reported in February.

While the battle against ISIS continues, Iraq and Syria will continue to offer opportunities to defense contractors, but the big money will come when reconstruction begins. The U.S. spent $60 billion in Iraq on reconstruction efforts and so far, over $110 billion in Afghanistan.

Last week, Defense Secretary Ashton Carter signaled that after ISIS is pushed out of towns and cities across Iraq and Syria, there will be an opportunity for private contractors.

"There will be towns to rebuild, services to reestablish and communities to restore," Carter told troops July 27 in Fort Bragg, N.C.

"That's not a principally American job. We will play a role in it, but remember the more than $2 billion in pledges that we got last week will mostly be executed through civilian agencies and frequently they'll use contractors to do that," he said later that day, speaking to reporters. It's "going to be a big job."

1. Times of Israel

Hard drive noises could betray sensitive data

Tuesday, 16 August 2016
Byline: Dan Schwartz
Section: general

Jerusalem - First it was video screens sending out electromagnetic waves that could be picked up by a cellphone; then it was Radio Shack-type equipment hidden inside something the size of a pita bread that could be used to "read" the electromagnetic pulses emanating from a standard laptop's keyboard. Now, Ben Gurion University researchers have discovered a new take on air-gapped network **hacks** - malware that reads sensitive data and sends it out to a waiting device.

It's another example of how malefactors could pull off a **hack** on some of the most secure networks and individual computers in the world - networks and computers that are not connected to the **internet**. **Hackers** generally practice their craft on connected systems, using long-distance network and wifi connections to reach into troves of sensitive data. Ostensibly, though, systems that are not connected to the **internet** are not within reach of **hackers**.

Not quite. New research led by the Ben Gurion University team, led by security researcher Mordechai Guri, shows that even unconnected systems are vulnerable. All a **hacker** has to do is implant the right kind of malware into a system (usually accomplished by connecting a USB drive or other peripheral to a computer) and get a cellphone within range of the computer. This peripheral manipulates the computer's hard drive to broadcast data to a waiting cellphone or other device, which then stores it and can later upload it to **hackers**.

This is known as an air-gap attack. In the past, researchers at Ben Gurion and Tel Aviv universities have discovered several other applications of this kind of attack - like PITA, the Portable Instrument for Trace Acquisition attack, which uses electromagnetic wave detection equipment (available at any computer hardware store) that could "read" the electromagnetic pulses emanating from a standard laptop's keyboard, including the keystrokes used to de-encrypt secure documents.

The new attack, called DiskFiltration, does something similar using the acoustic signals emitted from the movement of a computer's hard disk drive (HDD). Malware on the computer seeks out data like text files, logins and passwords, databases, and other useful information. Once the preferred data is discovered, the malware manipulates the hard driver's actuator (a device that controls the hard drive head arm, which reads data off the disk) to create specific sound patterns - the clicks and whirrs of the movement of the drive.

Those patterns are recorded by a device like a smartphone, smartwatch, or other **Internet** of Things (IoT) device that could either transmit the sound patterns to a remote computer (via the cellphone network connection of the device) or keep it intact, awaiting the retrieval of the device by a **hacker** or their agent.

It sounds implausible, if not impossible, but air-gap attacks are nothing new. According to many experts, the Stuxnet attack on Iran's nuclear system - in which a virus infected the servers controlling the Iranian nuclear program's centrifuges, "choking" them until they ground to a halt - was an air-gapped one, as the computers were not connected to the **internet**.

One way to beat air-gap attacks, according to the researchers, is to switch to solid-state drives (SSDs), which have no moving parts and therefore emit no noise. However, according to the researchers, "despite the increased rate of adoption of SSDs, HDDs are still the most sold storage devices, mainly due to their low cost. In 2015, 416 million HDD units were sold worldwide, compared to 154 million SSD units. Currently, HDDs still dominate the storage wars, and most PCs, servers, legacy systems, and laptops are installed with HDD drives," so there are still many vulnerable systems out there.

Other than that, say the researchers, the best bet is to keep devices away from secure computers. "Procedural countermeasures involve a physical separation of emanating equipment from potential receivers," says the team. "Smartphone and other types of recording devices should not be permitted in close proximity of the computer."

Back to top

2. The Pioneer

34 cyber labs operationalised

Tuesday, 16 August 2016
Section: general
Mumbai - In a major initiative to combat growing cyber crimes, the Maharashtra on Monday launched a comprehensive Crime and Criminal Tracking Network System (CCTNS) through the operationalisation of 34 cyber laboratories across the state.

Announcing the commencement of the operations of 34 cyber cells in the, Maharashtra chief minister Devendra Fadnavis said on the occasion of the 70th Independence Day: "The 34 cyber laboratories are out a total 51 such labs that we intend to set up in the state by December this year. The labs will come in handy for the Maharashtra police in tackling complex crimes in the cyber era we are in".

Fadnavis said that under the CCTNS, a dedicated cyber police force would be developed and "We will train 1,000 policemen under CCTNS to handle cyber crimes across the state," he said.

The CM said that the cyber labs would analyse mobile forensic and call detail records. He said that the Maharashtra police would develop a mobile application by October this year to provide services to the people under CCTNS.

Speaking at an inauguration ceremony of the Cyber Lab project held at the World Trade Centre here, Fadnavis said: " With the increased use of internet, criminals are using advanced techniques to commit newer types of online crimes. I am confident, the Cyber Labs will track down the criminals involved in online crimes...Advanced technology will be deployed for the safety and security of all the citizens and their properties through the Cyber Police Force".

The CCNTS will facilitate linking of all police stations across the state with one another for sharing information about crimes in their respective jurisdictions "in real time", a scenario that that would make a 'Digital Police Force' a reality in Maharashtra.

Linked by secure high-speed fibre optic cable network, the data from the cyber labs will be at the disposal of the police to address security concerns of private organizations and banks among others, the chief minister said.

Back to top

3. Arab News

Latest technology put in place for emergencies

Tuesday, 16 August 2016
Byline: Staff Report
Section: general
Riyadh - The Unified Operations Center, 911, will help the security staff to coordinate and respond to emergencies within a few minutes, thanks to the latest technology used for the system.

Maj. Gen. Abdulrahman Al- Saleh, commander of the National Operation's Center in the Ministry of Interior, said latest cameras have been installed at holy sites to serve Umrah and Haj pilgrims.

"The unified operations project represents a quantum leap in security work. The center has been launched in Makkah, Taif and Jeddah to contribute to speedy coordination between security bodies and other supporting services," he told local media.

The project was launched by Crown Prince Mohammed bin Naif during the Haj season last year through a number of phases. It started with road security patrols, and was then introduced to other security sectors, such as Civil Defense, traffic and security patrols.

Al-Saleh pointed out the secretariat of security planning and development in the Ministry of Interior is responsible for the project, while the National Operations Center is delegated the task of its operation.

The project was launched from Makkah and then Taif, while it was launched in Jeddah on Saturday. The project will be operational after 10 days in certain parts of the Makkah Province, and work will be finalized on Aug. 20, to bring the whole of Makkah Province under the emergency number 911.

The government has put in a lot of efforts in the preparation of this project, which is housed in the government complex, which was constructed by the Ministry of Finance in the Al-Awali area in Makkah, said Al-Saleh.

The operations room in Makkah manages security operations in all parts of the Kingdom, and there are other projects that will be implemented in phases in other cities. He revealed that the number 911 was carefully chosen because it is different from previous emergency numbers, in addition to it being popular globally.

Advanced systems have been used in the project to guarantee speedy response and supervision of workers' performance, which is a very important requirement for the success and smooth running of the operations.

Al-Saleh said the unified center has a number of supporting bodies, such as the Ministry of Health, Red Crescent, water company, electricity and the Ministry of Transport. He confirmed that these bodies offer support to security bodies only during emergencies.

The center includes a directorate for Haj and Umrah, called crisis management. There are advanced cameras at the holy sites.

911 is the emergency number in Makkah Province and anyone who calls this number from inside the Kingdom will be answered from the operations center in Makkah.

A number of officers have been enrolled for a training course in King Fahad Security College and will be employed in the center as soon as they graduate.

Al-Saleh confirmed that some people were sent to China and Germany to study the system and technology used in the center. "We don't underestimate the efforts of previous operations' rooms. Their experience over the years is appreciable," added Al-Saleh.

4. Fars News Agency

Security Experts: Remotes Are Hackable on Many Vehicles

Tuesday, 16 August 2016
Section: general
Tehran - A group of computer security experts say they figured out how to hack the keyless entry systems used on millions of cars, meaning that thieves could in theory break and steal items without leaving a broken window.

The experts say that remote entry systems on millions of cars made by Volkswagen since 1995 can be cloned to permit unauthorized access to the car's interior. The same experts say another system used by other brands including Ford, General Motor's Opel and Chevrolet and Renault can also be defeated.

In a paper to be delivered Friday at the Usenix security conference in Austin, Texas, the authors say a thief could use commonly available equipment to intercept entry codes as they are transmitted by radio frequency, and then use that information to clone another remote so the car could be opened.

Volkswagen said its latest models such as the Golf, Tiguan, Touran and Passat were not affected. It said it was having a "constructive exchange" with the experts aimed at improving security technology.

"The bar for theft prevention is constantly being raised, but ultimately there is no comprehensive guarantee for security," the company said in a statement.

The paper leaves out key details on how to perform the hack but says the codes can be intercepted with commercially available equipment.

"It is unclear whether such attacks... are currently carried out in the wild by criminals," the report says. "However, there have been various media reports about unexplained theft from locked vehicles in the last years."

The report did not establish the exact number of cars that use the vulnerable systems.

General Motors said that it "does not consider this item to be a significant risk to customers due to the technical sophistication of the demonstration and the very limited circumstances under which the demonstration can be carried out."

The company added that "the issue in question does not impact the operation of the vehicle or the safety of its occupants."

The report authors said that insurance companies might have to accept that car theft scenarios that would otherwise be considered insurance fraud have a higher probability of being genuine. The only surefire countermeasure, they said, would be to stop using the remote and fall back on the mechanical lock using the conventional metal key.

The authors are Flavio Garcia, David Oswald, and Pierre Pavlides from the University of Birmingham School of Computer Science and Timo Kasper from German security firm Kasper & Oswald GmbH.

5. Wall Street Journal

The Specter of an Accidental China - U . S . War

Tuesday, 16 August 2016
Byline: Andrew Browne
Section: general
Shanghai - The last time America and China went to war--in Korea in 1950--they fought each other to a standstill.

Later that decade, as the Cold War ramped up, they came close to blows again; the Eisenhower administration repeatedly threatened "Red China" with nuclear devastation as tensions bubbled over Taiwan.

Today, given the astronomical stakes at play, many assume that armed conflict between the two giants is out of the question. They are each other's largest trading partner. Military confrontation wouldn't only threaten these huge flows but also student exchanges, scientific collaboration, joint technical projects and the myriad other ways in which the fates and fortunes of the world's two largest economies and their peoples are inextricably linked.

Yet, as China flexes its muscles in the South China Sea and East China Sea, the risks of an inadvertent clash on the water or in the air are growing by the day.

A new RAND Corp study says that a Sino-U. S. war as a result of such a crisis "cannot be considered implausible."

Violence could ignite quickly, the report warns. That is because each side has deployed precision-guided munitions, as well as cyber and space technologies, able to inflict devastating damage on the other's military assets, including Chinese land- based missile batteries and American aircraft carriers. Thus they have a strong incentive to launch massive strikes first as part of a "use it or lose it" calculation.

Once out of control, fighting could be prolonged, although it is unlikely to go nuclear, according to the RAND study sponsored by the U.S. Army. Both nations possess the military, industrial and demographic resources to absorb heavy losses and slog on. As in Korea, there would likely be no clear victor.

Washington and Beijing "need to contemplate the possibility of a severe, lengthy, uncontrollable and devastating, yet indecisive, conflict," the RAND paper asserts.

This is the troubling context in which to view China's defiant response to last month's ruling by a panel of jurists in The Hague, who struck down Beijing's claims to almost the entire South China Sea and rebuked it for dredging artificial islands topped by military-capable runways that have intimidated other claimants, including Vietnam and the Philippines.

Instead of backing off, China has doubled down on its assertive strategy, flying a bomber over the Scarborough Shoal, which it has effectively seized from the Philippines, announcing war games with Russia and sending militia fleets swarming into waters contested with Japan.

The Center for Strategic and International Studies, a Washington think tank, has published satellite photos showing aircraft hangers springing up on the fake islands, reinforced apparently to withstand air attack.

So far there are no signs that the People's Liberation Army has stationed military aircraft on the mid-sea platforms.

Then again, some Western experts think China may be biding its time so as not to spoil a Group-of-20 summit of leading economies it is hosting for the first time next month. Watch out for even more aggressive moves between then and the U.S. presidential election in November, they say.

Washington's response to The Hague ruling has been conspicuously restrained. U.S. officials seem to hope that avoiding provocative words and actions, such as sending warships steaming close by the island fortresses in "freedom of navigation" missions, will make it easier for Beijing to find a graceful way to comply with the ruling over time.

For the U.S., striking the right balance between displays of conciliation and resolve is critical. As the RAND report argues, war is much more likely to arise as a result of China misjudging America's willingness to defend its East Asian allies, and pushing them too far, than from a premeditated attack.

Indeed, Chinese leaders -- arch-realists on foreign policy -- may even feel emboldened now. Their man-made islands are a fait accompli; the tribunal has no power to enforce its judgment.

Southeast Asia has been silent. So has a struggling Europe, as ever, most concerned with ginning up Chinese investment.

"Nobody is pushing back," says Jennifer Lind, an East Asia specialist at Dartmouth College. She thinks the Chinese strategy has been successful. "They control more territory; they have more influence than ever before," she says.

Worryingly, the RAND report notes an increasing confidence among Chinese military strategists that they could conduct a short, sharp and victorious war.

Among the report's recommendations: America should make clear it doesn't favor pre-emptive strikes against China and must "expand communications with China in times of peace, crisis, and war."

On that latter objective, history isn't encouraging. In 2001, when a Chinese fighter ran into an America spy plane, its pilot killing himself and forcing the crippled U.S. plane to make an emergency landing on Hainan Island, then U.S. President George W. Bush tried to reach his Chinese counterpart, Jiang Zemin, on a hotline. Mr. Jiang wouldn't take the call.

Back to Top

6. Wall Street Journal

China Makes Quantum Leap Forward

Tuesday, 16 August 2016
Byline: Josh Chin
Section: general
Beijing - A rocket that shot skyward from the Gobi Desert early Tuesday is expected to propel China to the forefront of one of science's most challenging fields.

It also is set to launch Beijing far ahead of its global rivals in the drive to acquire a highly coveted asset in the age of **cyberespionage**: **hack**-proof communications.

State media said China sent the world's first quantum-communications satellite into orbit from a launch center in Inner Mongolia about 1:40 a.m. Tuesday. Five years in the making, the project is being closely watched in global scientific and security circles.

The quantum program is the latest part of China's multibillion- dollar strategy over the past two decades to draw even with or surpass the West in hard-sciences research.

"There's been a race to produce a quantum satellite, and it is very likely that China is going to win that race," said Nicolas Gisin, a professor and quantum physicist at the University of Geneva. "It shows again China's ability to commit to large and ambitious projects and to realize them."

Scientists in the U.S., Europe, Japan and elsewhere are rushing to exploit the strange and potentially powerful properties of subatomic particles, but few with as much state support as

those in China, researchers say. Quantum technology is a top strategic focus in the country's five-year economic development plan, released in March.

Beijing hasn't disclosed how much money it has allocated to quantum research or to building the 1,400-pound satellite. But funding for basic research, which includes quantum physics, was $101 billion in 2015, up from $1.9 billion in 2005.

U.S. federal funding for quantum research is about $200 million a year, according to a congressional report in July by a group of science, defense, intelligence and other officials. It said development of quantum science would "enhance U.S. national security," but said fluctuations in funding had set back progress.

Beijing, meanwhile, has tried to lure Chinese-born, foreign-educated experts in quantum physics back to China, including Pan Jianwei, the physicist who is leading the project.

"We've taken all the good technology from labs around the world, absorbed it and brought it back," Mr. Pan told Chinese state TV in an interview that aired on Monday.

With state support, Mr. Pan was able to leapfrog his former Ph.D. adviser, University of Vienna physicist Anton Zeilinger, who said he has tried since 2001 to persuade the European Space Agency to launch a similar satellite.

"It's a difficult process, which takes a lot of time," said Mr. Zeilinger, who is now working on his former student's satellite.

Neither Mr. Pan nor the Chinese Academy of Sciences, which is directing the project, responded to requests to comment. The European Space Agency and the U.S.'s National Science Foundation, which provides federal funding for basic American science research, also didn't respond to requests to comment.

China's investment in the field is likely being driven in part by fear of U.S. cyber capabilities, said John Costello, a fellow at Washington, D.C.-based New America specializing in China and cybersecurity, pointing to 2013 disclosures that the U.S. had penetrated deeply into Chinese networks. He also noted that U.S. institutions are researching how to build powerful quantum computers theoretically capable of shattering the math-based encryption now used world-wide for secure communication.

Quantum encryption is secure because information encoded in a quantum particle is destroyed as soon as it is measured. Gregoir Ribordy, co-founder of Geneva-based quantum cryptography firm ID Quantique, likened it to sending a message written on a soap bubble. "If someone tries to intercept it when it's being transmitted, by touching it, they make it burst," he said.

Quantum physicists have recently advanced the use of photons to communicate securely over short distances on earth. The satellite, if successful, would vastly expand the range of unhackable communication. Mr. Pan has said he and his team will try to beam a quantum cryptographic key through space from Beijing to Vienna.

7. Voice of America

Homeland Security Offering States Voting Cybersecurity Help

Tuesday, 16 August 2016
Byline: Staff report
Section: general
Washington - The U.S. Department of Homeland Security offered Monday to help state elections officials with the challenge of securing voting systems from the threat of cyber attacks.

Homeland Secretary Jeh Johnson hosted a meeting by telephone with officials from around the country as well as representatives from the Justice Department and the National Institute for Standards and Technology.

Most voters in the U.S. encounter some kind of machine during the voting process, whether they vote directly on a touchscreen device or put their paper ballot into a scanner. But which system is used is up to officials overseeing the 9,000 separate voting jurisdictions across the country, not the federal government.

Johnson encouraged states to implement recommendations that include making sure electronic voting machines are not connected to the internet while voting is taking place.

He also announced a new campaign to bring together government and private sector experts to promote voting security and heighten awareness of the potential risks to the infrastructure involved in the process.

Back to top

8. Motherboard (Vice)

Hackers Say They Hacked NSA-Linked Group, Want 1 Million Bitcoins to Share More

Monday, 15 August 2016
Byline: Lorenzo Franceschi-Bicchierai
Section: general
New York - A mysterious hacker or hackers going by the name "The Shadow Brokers" claims to have hacked a group linked to the NSA and dumped a bunch of its hacking tools. In a bizarre twist, the hackers are also asking for 1 million bitcoin (around $568 million) in an auction to release more files.

"Attention government sponsors of cyber warfare and those who profit from it!!!!" the hackers wrote in a manifesto posted on Pastebin, on GitHub, and on a dedicated Tumblr. "How much you pay for enemies cyber weapons? [...] We find cyber weapons made by creators of stuxnet, duqu, flame."

The hackers referred to their victims as the Equation Group, a codename for a government hacking group widely believed to be the NSA.

The security firm Kaspersky Lab unmasked Equation Group in 2015, billing it as the most advanced hacking group Kaspersky researchers had ever seen. While Kaspersky Lab stopped short of saying it's the NSA, its researchers laid out extensive evidence pointing to the American spy agency, including a long series of codenames used by the Equation Group and found in top secret NSA documents released by Edward Snowden. The Equation Group, according to Kaspersky Lab, targeted the same victims as the group behind Stuxnet, which is widely believed to have been a joint US-Israeli operation targeting Iran's nuclear program, and also used two of the same zero-day exploits.

The Shadow Brokers claimed to have hacked the Equation Group and stolen some of its hacking tools. They publicized the dump on Saturday, tweeting a link to the manifesto to a series of media companies.

The dumped files mostly contain installation scripts, configurations for command and control servers, and exploits targeted to specific routers and firewalls. The names of some of the tools correspond with names used in Snowden documents, such as "BANANAGLEE" or "EPICBANANA."

It's unclear if the data is legitimate, but some security experts agree that it likely is.

"If this is a hoax, the perpetrators put a huge amount of effort in," the security researcher known as The Grugq told Motherboard. "The proof files look pretty legit, and they are exactly the sorts of exploits you would expect a group that targets communications infrastructure to deploy and use."

Claudio Guarnieri, an independent security researcher who's investigated other hacking operations by the Western intelligence agencies, told me that the files might be from a hacked NSA server used in an operation. He also cautioned that this is a preliminary analysis and that more analysis is needed.

The most recent file is dated June 2013, though the hackers could have tampered with the dates. Dmitri Alperovitch, the co-founder of security firm CrowdStrike, theorized that "the leakers were probably sitting on this information for years, waiting for the most opportune time to release."

Matt Tait, another security researcher and former British intelligence officer, tweeted that the data could come from "an old counter-hack."

A Kaspersky Lab researcher declined to comment. Another Kaspersky Lab researcher noted on Twitter that there is "nothing" in the dumped files that links them to the Equation Group, but some of their names are from the ANT Catalog, an NSA hacking toolset published by Der Spiegel in late 2013. It's worth noting that while the files dumped by The Shadow Brokers might not have a direct connection with the Equation Group, they could come from a different operation that those seen by Kaspersky Lab.

The Shadow Broker claimed to have gotten the files by following Equation Group "traffic," hacking the group and finding its "cyber weapons." (The hackers did not respond to a request for comment, and neither did the NSA.)

At the time of writing, the Bitcoin wallet where the hackers accept auction offers has yet to receive any funds.

The motives behind this strange dump are unclear, but if legitimate, this could be one of the most shocking hacks ever.

1. Jerusalem Post

India to tap Israeli radar tech to thwart terrorism in volatile Kashmir area

Thursday, 18 August 2016
Byline: Staff Report
Section: general
Jerusalem - India is reportedly preparing to install Israeli radar technology in the jungles of the volatile Kashmir Valley region as part of operations to prevent terrorists from infiltrating from Pakistan.

Representatives from India's Border Security Force are due to visit Israel later in August as part of the acquisition of the detection system, a senior security officials told India Today TV this week. During the trip, the Indian forces are set to receive training on the system's operations.

The so-called foliage penetrating radar is allegedly equipped with high- sensitivity sensors that can track human and vehicular movement in areas of dense foliage.

According to India Today, the Indian government will established a 24/7 control room to monitor the signals received from the Israeli technology installed throughout the Kashmir Valley and the Line of Control (LoC) between India and Pakistan.

India is working to erect an air-tight defense mechanism along the borders with nuclear-armed Pakistan modeled after Israeli security apparatus, the officials said.

Indian National Security Adisor Ajit Doval approved the deal to purchase the radar system from Israel, the officials added.

India and neighboring Pakistan have been embroiled in a territorial dispute over the Jammu and Kashmir region since the partition of India in 1947.

Islamic insurgents, many identifying with jihadi elements, have carried out attacks in the region in efforts to claim the contested land for Pakistan.

Back to top

2. The Pioneer

Cyber Meeting

Thursday, 18 August 2016
Byline: Special Correspondent
Section: general
Thiruvananthapuram - Lt. Gen. Sheik Saif bin Zayed Al Nahyan, Deputy Prime Minister and Minister for Interior, UAE, will be the guest of honour at a two-day international cyber security and policing conference scheduled to be held at Hotel Raviz in Kollam on October 19.

Governor P. Sathasivam will inaugurate the function. Chief Minister Pinarayi Vijayan will address the valedictory session on October 20.

Julie Gommes, renowned cyber security expert from Devoteam, France, will speak on Crypotgraphy and Jihadism, while renowned cyber evangelist Ben Herzberg will speak on the latest cyber attacks.

Other noted speakers included Gulshan Rai, Cyber Security Chief, Prime Minister's Office, Government of India, and Aruna Sundararajan, Secretary, Ministry of Electronics & Information Technology.

Bessie Pang, Executive director of Polycb (Society for Policing of Cyber Space), will speak on private-public participation in cyber security. Polycb is supporting the conference.

The event will run in two parallel streams from 10 a.m. onwards. Track one will be non-technical and track 2 will be a purely technical. Apart from foreign delegates, students, IT experts, police cyber cells, and police officers from around the country will attend the conference.

The conference will focus on Innovations in cyber security, Prevention - detection of cyber crimes against women, Digitization for better service delivery, Digitalization as a force Multiplier, Cyber safe government, tackling latest cyber crimes and ethical hacking.

The conference, is aimed at providing a platform to discuss and share new information and latest trends in cyber crimes, across the world.

The conference will be a platform to share latest information on high tech cyber crime methods. It will focus on data theft, piracy, hacking, identity theft, violation of intellectual property rights, etc.

3. Bangladesh Daily Star

From crackers to rocket launchers

Thursday, 18 August 2016
Byline: Zayadul Ahsan
Section: general
Dhaka - They are no longer into small arms and crude crackers only. Local terrorists over the years have mastered the skills of making deadly weapons like rocket launchers, mines, car bombs, and cycle bombs.

They even took initiative to make drones. Besides, various types of sophisticated weapons like AK-47 assault rifle and MK-11 sniper were recovered from them in the last three to four years.

In close liaison with cross-border terror outfits, they not only went abroad to train in making arms and explosives, but also brought in foreign experts for training programmes within the country.

Piecing together information gleaned from captured militants, findings of investigators and news of the recoveries, we get a picture where militants appear to have developed much earlier the capacity to launch attacks like the July 1 Gulshan café strike.

Though law enforcers had considerable success in recovering arms and ammunition, the policymakers failed to foresee the looming crises. They didn't notice the ominous signs in the reports of the recoveries, security experts observed.

As the possibility of further attacks like Gulshan and Sholakia cannot be ruled out, the experts call for constant vigilance, especially to prevent building of new terror networks and stockpiling of weapons by militants.

"The recovery of arms and explosives proves that our law enforcers are vigilant. But what if an extremist group manages to gather military strength beyond the knowledge of law enforcers?" said security expert Brigadier (retd) Shahed Anam.

"There is always a risk like that. So the government must focus on capacity building of law enforcement agencies."

DMP's counterterrorism unit chief Monirul Islam believes that no radical group is likely to emerge with considerable military strength again because of continuous raids, seizures and arrests. "But to eliminate the threat permanently," he said, "we need to do a lot of capacity building." One can recall that experts were brought in from Pakistan to train militants on making car bombs.

Two Pakistani nationals -- Mehmud and Osman -- came to Bangladesh sometime in 2012 posing as businessmen. When it came to the knowledge of the detectives, the two were interrogated several times but no information could be gleaned from them.

So they were produced before a court and sent to jail for suspicious activities under section 54 of the Code of Criminal Procedure. They came out on bail about a year later. Then their mentor Fakhrul Hasan came to Dhaka from Pakistan.

The Detective Branch of police arrested the three from the gate of Shilpakala Academy in the capital on January 19, 2014. A manual on bomb-making was found with them. Their laptops contained information about training on military weapons. In police interrogation, they confessed they were members of Tehrik-e-Taliban of Pakistan.

After primary interrogation, Monirul Islam, also additional commissioner of Dhaka Metropolitan Police (DMP), told the media that the Pakistani militants were capable of making 12 types of explosives, including car bombs and grenades.

A group in Bangladesh has brought them to train militants. The official said attempts were on to detect the group and arrest them. It is not known whether the group has been tracked down or efforts to do that are still on.

In February this year, DB police recovered a good number of car bombs from Mohammadpur in the capital. The information was not given to the media thinking that it might spread panic.

It is possible that the trainers from Pakistan before being arrested trained others on making car bombs or some new trainers replaced them.

DB police on December 16, 2014 arrested two members of Ansarullah Bangla Team (ABT) at Jatrabari in the capital with a "drone" or "quadcopter".

Drone-making project, equipment for making drones and various types of electronic devices were recovered from them.

ABT had been manufacturing drone using advanced technology for launching attack on important installations and persons. It is notable that one of the arrestees, Golam Maula Mohan, had studied computer science at a private university in Dhaka.

Officials at that time told the media that since the important installations are well guarded, the militants planned to strike those from air using drones. After research for about six months, the two arrestees were at the last stage of making a drone capable of carrying a 30Kg bomb. They made the drone for carrying out attack from the top of a 25- 30-storey building.

The incident of recovering a bicycle bomb from Karnaphuli Garden City area in the capital's Shantinagar on March 8 last year was beyond the imagination of the detectives.

Explosives were put inside the rods of the bicycle. It was meant to explode with a big bang the moment it comes in contact with fire. At that time Rab said that if it exploded, the bicycle bomb could cause a disaster within 30 yards.

The militants attacked the Hossaini Dalan premises in Old Dhaka on the night of October 23 last year with three grenades made with chemicals. Two persons, including an adolescent, were killed in the incident. That was the first attack in the country using a bomb or grenade made with chemicals.

In a 15-hour raid on December 24 last year, detectives recovered 16 hand-made grenades, two hand bombs, some suicide vests, pipe bombs and equipment for making more than 200 grenades.

The suicide vests were of special type -- it had "double switch" system. If one switch somehow fails to trigger the explosion, a backup switch is there. Explosives, arms, bullets and money could be kept in the vest at the same time.

After the recovery of a huge amount of arms, ammunition and new type of suicide vests, Monirul Islam of the DMP said it was a high-profile raid.

On December 27 last year, police recovered an MK-11 sniper rifle along with 250 bullets from a JMB den. This semiautomatic weapon is highly accurate and durable. Its firing rate is 750 rounds per minute and the range 1,500 yards.

A military uniform and rank badge were also found with the modern rifle, made in the United States. The explosives recovered were enough to blow up four buildings, said the then chief of Chittagong Metropolitan Police.

On February 20, detectives recovered some car bombs, handmade mines and some new kinds of grenades from two apartments in the capital's Mohammadpur and Dakkhin Khan. Each of the

grenades weighed between 3-4kg. At least eight hand grenades that looked like tennis balls were also recovered.

Police at the time said the grenades, bombs and explosives found there could blow up multi-storey buildings. The grenades looking like tennis balls were the new invention of the militants.

On April 4, high-power explosives were found in Bogra. Made on the model of Arges grenades, those explosives were capable of causing massive destruction. It was possible to make about 300 powerful explosives with bomb-making materials recovered then.

On May 23, 2010, JMB chief Saidur Rahman, caught by police, admitted that the JMB militants had suicide vests and rocket launchers. They even successfully tested several rocket launchers in areas near the Sundarbans in Barguna and in remote areas of Jamalpur district. Police recovered 10 suicide vests from a Siddhirganj den on May 24 on information given by the JMB chief.

A bomb found there was of a special type. After its pin is removed like a grenade, the outer shell opens on one side. A metallic object gets connected with a battery and electricity begins to flow, causing explosion.

Inside the bomb, there is a pencil battery, a circuit and white explosive powder. The powder is pentaerythritol tetranitrate (PETN). A car can be destroyed with just 100 grams of it. When the bomb goes off, tiny pieces of its shell hit the target like splinters.

In January, eight AK-22 rifles were recovered from the members of Shaheed Hamza Brigade of Islami Chhatra Shibir in Chittagong. AK-22 rifles were used in the Holey artisan attack.

Besides, the law enforcement agencies on different occasions informed journalists about recovery of arms and ammunition. There were AK-47 and submachine guns.

In the last 12 years, law enforcers seized over a thousand grenades, more than one hundred firearms and 4-5 tonnes of explosives from militants.

Talking to officials dealing with militancy it is learnt that law enforcers hardly have time to look back to the past as they are mostly busy cracking down on Neo JMB or other radical groups.

Experts believe that to understand the strategy of new radicals, there is no alternative to studying and investigating the militant activities in the past.

They say law enforcers should not forget that many key persons behind those remained out of touch and many mysteries remained unsolved.

4. Washington Post

NSA's use of software flaws to hack foreign targets posed risks to cybersecurity

Thursday, 18 August 2016

Byline: Ellen Nakashima, Andrea Peterson
Section: general

Washington - To penetrate the computers of foreign targets, the National Security Agency relies on software flaws that have gone undetected in the pipes of the Internet. For years, security experts have pressed the agency to disclose these bugs so they can be fixed, but the agency hackers have often been reluctant.

Now with the mysterious release of a cache of NSA hacking tools over the weekend, the agency has lost an offensive advantage, experts say, and potentially placed at risk the security of countless large companies and government agencies worldwide.

Several of the tools exploited flaws in commercial firewalls that remain unpatched, and they are out on the Internet for all to see. Anyone from a basement hacker to a sophisticated foreign spy agency has access to them now, and until the flaws are fixed, many computer systems may be in jeopardy.

The revelation of the NSA cache, which dates to 2013 and has not been confirmed by the agency, also highlights the administration's little-known process for figuring out which software errors to disclose and which to keep secret.

The hacker tools' release "demonstrates the key risk of the U.S. government stockpiling computer vulnerabilities for its own use: Someone else might get a hold of them and use them against us," said Kevin Bankston, director of New America's Open Technology Institute.

"This is exactly why it should be U.S. government policy to disclose to software vendors the vulnerabilities it buys or discovers as soon as possible, so we can all better protect our own cybersecurity."

The weekend's release prompted immediate speculation about who might be behind it. A group calling itself Shadow Brokers claimed responsibility. Some experts and former employees suspect, although without hard evidence, that Russia is involved. Other former employees say it is more likely a disgruntled insider seeking to make a profit.

Whoever it is, "it's very concerning that potentially someone working for another government is essentially holding hostage companies that are sitting behind these [firewalls], making them very vulnerable," said Oren Falkowitz, chief executive of Area 1 Security and a former NSA analyst.

The firewalls sold by Cisco, Juniper and Fortinet are highly popular and work on large-scale enterprise systems. "These are very, very powerful and successful" products, Falkowitz said. "They aren't devices bought by two people."

Already, the firms are racing to reverse-engineer the code, identify any flaws and devise patches. Cisco confirmed Wednesday that one of the flaws was a "zero-day" -- previously unknown to the public - - and that it is working on a fix. The flaw was in a tool or exploit code-named Extrabacon.

Juniper spokeswoman Leslie Moore said the company is reviewing the released file. "If a product vulnerability is identified, we will address the matter and communicate to our customers," she said.

Fortinet spokeswoman Sandra Wheatley Smerdon said that the firm is "actively working with customers" who are running the FortiGate firewall version 4.X and that it "strongly" recommends that they update their systems "with the highest priority."

The government has a process for determining when to share software flaws. Agencies such as the NSA and the FBI are supposed to submit any flaws they discover to a multiagency group of experts, who then weigh whether the advantage of keeping the vulnerabilities secret outweighs the public's cybersecurity.

White House cybersecurity coordinator Michael Daniel has said that "in the majority of cases," disclosure of the bug is in the national interest. The multiagency process didn't really begin until spring 2014. The NSA had had its own internal process for years before that.

Either way, in this case, disclosure never happened.

"This is what happens when you have security agencies hoarding exploits insecurely -- poorer security for all," said Kevin Beaumont, a cybersecurity researcher who verified that some of the leaked tools rely on still unpatched vulnerabilities.

Former NSA personnel who worked with the tool cache that was released say that when they worked at the agency, there was an aversion to disclosure.

"While I was there, I can't think of a single example of a zero-day [flaw]" used by the agency "where we subsequently said, 'Okay, we're done with it and let's turn it over to the defensive side so they can get it patched,' " said the former employee, who worked at the agency's Tailored Access Organization for years. During that time, he said, he saw "hundreds" of such flaws.

He added: "If it's something in active use, my experience was they fight like all get-out to prevent it from being disclosed."

Said a second former employee, who also spoke on the condition of anonymity to describe sensitive government operations: "It's hard to live in a world where you have capabilities and you're disclosing your capabilities to your defensive team."

This former operator said that sometimes a vulnerability is patched, but that "if you weaponize it in a different fashion" with a special technique, "maybe that's one way to increase the longevity of a tool."

In that way, a flaw could still be good for several years.

"Two or three years is not really a long time for a bug to go undiscovered," said Joseph Lorenzo Hall, the chief technologist at the Center for Democracy & Technology.

For example, a major vulnerability called Heartbleed made its way into the code of widely used encryption software in 2011, but didn't come to light until 2014, he noted. Last year, Microsoft fixed a critical zero-day bug that had been lurking in Windows for at least a decade.

"There are so many vulnerabilities in software that we can't possibly find them all," Hall said. "It's really kind of scary, especially when you're talking about technology like firewalls, which are supposed to help keep systems safe."

Experts studying the release say the material probably was stolen in October 2013, the date of the last file creation. If that's true, then someone or another spy agency has had time to hack companies using the vulnerable firewalls or watch NSA's own cyber spying.

Past NSA employees, including former contractor Edward Snowden, say it is unlikely that the material was hacked from the agency's servers. It is more likely, some say, that the tools were uploaded and inadvertently left by a TAO hacker on a server used to stage hacks on targets. These servers are sometimes called redirectors or staging servers, and they mask the hacker's true location.

The NSA has always had audit controls on its systems. But particularly in the wake of leaks of classified material by Snowden that began appearing in the media in June 2013, the agency has strengthened its control mechanisms.

5. Associated Press

UN experts: Extremists foiling governments with encryption

Thursday, 18 August 2016
Byline: Staff report
Section: general
The United Nations - Increasing numbers of foreign fighters for the Islamic State group and al-Qaida are returning home, potentially to carry out attacks, and are using the "dark web" or encrypted messaging that the most sophisticated intelligence agencies can't penetrate, U.N. experts said in a report circulated Wednesday.

The experts monitoring sanctions against the extremist groups said governments highlighted the challenge to national security from the communication methods being used by these "foreign terrorist fighters" and people being radicalized at home who need to be monitored and investigated.

They said the rise in the use of the "dark web" -- a collection of thousands of websites which use tools to maintain anonymity -- and especially encrypted messaging "has closed off the ability of even the most sophisticated agencies to penetrate huge quantities of messages."

The result, the experts said, is that governments are "potentially losing much of their previous technological advantage over terror groups."

Recruiters for the Islamic State group, once they engage potential fighters, also swiftly move them to "closed forums" and guide them toward encrypted messaging systems, the experts said.

The expert panel's report to the Security Council said the threat from al-Qaida, the Islamic State, and their associates "is serious and diversifying," despite military setbacks for Islamic State fighters in Iraq, Syria Afghanistan and Libya.

The Islamic State "demonstrated its ability to conduct complex, multi-stage attacks outside the conflict zone" while at the same time the role of its affiliates in the wider region was elevated, the panel said.

The near-simultaneous attacks conducted by Islamic State operatives in Paris in November 2015 and Brussels in March generated an overwhelming flow of information to command centers which governments described as a deliberate tactic by the extremist group "to make it more difficult to mount coordinated and targeted responses to the most dangerous continuing threats," the experts said.

Al-Qaida and its affiliates also maintained their position in various regions "and also demonstrated an ability to successfully plan and execute significant attacks," the panel said.

The experts said governments estimate that the Islamic State has up to 30,000 fighters in Syria and Iraq.

Significant numbers of IS fighters have been killed as a result of military attacks and the rate of fighters leaving the extremist group has increased, but the panel said governments report that this trend is partially offset by the continued flow of new fighters into Syria and Iraq and by forced recruitment among tribes and the use of child soldiers since 2014.

The panel said the Islamic State group's financial situation has deteriorated since last July, with oil production declining by between 30 and 50 percent as a result of air strike targeting oil infrastructure.

"Consequently oil revenue has fallen by tens of millions of dollars per month," it said.

The group's financial woes have also led to salary cuts for fighters, the panel said, but the Islamic State continues to earn significant revenue from taxation and extortion, the panel said.

According to governments, IS may earn as much as $30 million a month from these methods which include business taxes, fees for electricity and water, rent for seized real estate and customs duties and passage fees.

In a sign of desperation, the panel said that in February IS started to tax the most impoverished civilians in areas under its control who had previously been exempt.

Back to top

6. Wall Street Journal

Hacked Attack Code Looks Genuine

Thursday, 18 August 2016
Byline: Robert McMillan

Section: general

New York - Evidence is mounting that a mysterious hacking group claiming to have stolen data from a spying operation linked to the National Security Agency is telling the truth.

Security vendor Kaspersky Labs ZAO, which first identified the NSA-linked operation last year, said files released in the latest hack use an unusual mathematical approach it had seen in that operation's code. Kaspersky dubbed the operation the Equation Group, and said it appeared to be supporting U.S. interests in cyberspace.

The new files were released last weekend by a hacking group calling itself the Shadow Brokers, which claims to have a bigger cache of files it is offering to sell. They appear to be attack code that targets security software on routers that direct computer traffic around the internet.

"This code similarity makes us believe with a high degree of confidence that the tools from the Shadow Brokers leak are related to the malware from the Equation Group," Kaspersky said in a blog post.

Two former NSA employees said the code published by the Shadow Brokers looked authentic.

Security analysts, meanwhile, said several attacks that appear in the files can in fact alter how internet routers handle certain traffic.

None of the code appears to be of the high-value type that could command the millions of dollars that the Shadow Brokers are seeking, said Pedram Amini, chief technology officer of computer-security firm InQuest LLC. He estimated the most significant attacks, targeting products built by Cisco Systems Inc., would fetch "tens of thousands of dollars" in the attack-code market.

On Wednesday, Cisco confirmed that the Shadow Broker code took advantage of a bug in its software that wasn't publicly known, along with a second bug that it had patched in 2011. Fortinet Inc., another router maker identified in the attack code, confirmed that the Shadow Broker code could be used to attack versions of its products that were built in 2012 and earlier.

A third router maker, Juniper Networks Inc. didn't reply to requests for comment.

The developments add to a murky affair. The previously unknown Shadow Brokers released an encrypted version of files that it said contain hacking tools, pledging to disclose the password that would unlock them free to the world if they raised 1 million bitcoins, or close to $600 million, in an online auction.

Nicholas Weaver, a researcher with the International Computer Science Institute who also has examined the files, said they appear to be legitimate NSA attack code that was copied in mid-2013. Some of the files dated months after former NSA contractor Edward Snowden disclosed classified data that he had removed from the NSA.

Mr. Weaver doesn't know who is behind the attacks. Like other U.S. security experts, he said he believes that entities related to the Russian government are likely suspects, amid allegations that Russian hackers had compromised servers belonging to the Democratic National Committee and other organizations.

Susan Hennessey, a Brookings Institution fellow and former lawyer for the NSA, said a nation-state might be involved in the Shadow Brokers breach and might be signaling the U.S. to be careful about accusing foreign countries of cyberattacks. "It also has the significance of potentially warning the United States that attribution is also available against them," she said.

Kaspersky, which didn't explicitly link the Equation Group to the NSA, declined to comment beyond its blog post. The NSA didn't respond to requests for comment on the hacking group's claims, nor did the Shadow Brokers respond to messages.

The Kaspersky analysis sheds some light on the situation, but leaves many unanswered questions, including the identity of the Shadow Brokers and what information the group actually has.

Former NSA employees interviewed by The Wall Street Journal said it is extremely unlikely the attackers were able to access the full catalog of NSA attack code. Some experts, including Mr. Snowden, have said the Shadow Brokers may have accessed a "staging server" that was used for a time by the Equation Group and wasn't properly scrubbed of information.

"NSA malware staging servers getting hacked by a rival is not new," Mr. Snowden said via Twitter on Tuesday. "A rival publicly demonstrating they have done so is."

Return

7. L'Humanité

Cyberespionnage Un oeil pour les espionner tous

Thursday, 18 August 2016
Byline: Pierric Marissal
Section: general
Moscou - Sauron, l'outil de cyberespionnage le plus ingénieux jamais conçu, est actif depuis juin 2011. Son existence vient d'être mise au jour.

Le 30 juillet dernier, le FSB, le service de renseignements de Moscou, a reconnu que pas moins de vingt systèmes informatiques gouvernementaux, militaires et scientifiques russes ont été infiltrés par un cyberespion. Ce programme dont les spécificités ont été publiées mardi dernier est nommé comme le méchant du Seigneur des anneaux, représenté par un menaçant oeil cerclé de flammes : Sauron. Parfaitement camouflé, cet espion a pu se fondre pendant des années - les premières infections découvertes datent de l'été 2011 - au coeur des réseaux les plus stratégiques. Sauron a espionné aussi en Iran et au Rwanda, au sein d'une ambassade à Bruxelles. Touchées aussi, des entreprises de télécommunication et une compagnie aérienne chinoise. « Et on n'a découvert que le sommet de l'iceberg », reconnaissent dans leur rapport les chercheurs de la société de sécurité informatique russe Kaspersky.

Lorsque le cyberespion s'est niché, il se développe et crée son propre écosystème camouflé

« On était vraiment très excités », raconte à l'Humanité Orla Cox, qui dirige le département de recherche en sécurité de Symantec, entreprise qui a débusqué le programme chez l'un de ses clients stratégiques, en octobre dernier. « Ces découvertes-là, on en fait à peine une fois par an. » Une fois repéré, on traite un tel programme informatique comme on le ferait d'un virus

inconnu, dans un laboratoire ultrasécurisé. « On regarde comment le programme se développe dans un environnement fermé, comment il réagit, se protège, et on analyse les lignes de code une à une, explique la chercheuse. On a essayé ensuite de détecter sa signature, le schéma qui fait que Sauron est unique. De manière à le reconnaître sur d'autres machines. » Ces spécialistes de la sécurité informatique disposent d'outils extrêmement précieux : leurs programmes sont installés sur des millions d'ordinateurs dans le monde et composent un maillage dense qui permet de cartographier les réseaux informatiques. Et c'est en scrutant des anomalies comportementales que les analystes dénichent des virus aussi fourbes que Sauron.

On n'a aucune idée de la façon dont ce cyberespion rentre et s'installe dans ces systèmes si protégés. En revanche, lorsqu'il s'est niché, il se développe et crée son propre écosystème camouflé, quasiment indétectable. Il va en premier lieu se développer dans le système d'attribution des mots de passe. Ainsi, sa première tâche est d'envoyer à ses commanditaires tous les codes et les clés de cryptage des systèmes infectés. Pour ne pas être découvert, il se cache très astucieusement. Il se déguise par exemple en requête de nom de domaine (DNS). Lorsqu'on rentre une adresse dans un navigateur, celui-ci envoie au site un message poli : « Bonjour, qui êtes-vous ? Moi je suis le navigateur de X », et si les deux parties se reconnaissent, le navigateur affiche le site. Ces requêtes sont considérées comme sûres et ne sont pas surveillées par les services de sécurité. Sauron a réussi à cacher dans ces messages apparemment anodins les mots de passe et clés de cryptage volés. Les sites en question sont, en apparence, d'innocentes pages Web de fleuristes, de vente de vélos, une cave à vin allemande... Mais les mots de passe arrivent directement chez les commanditaires, qui peuvent désormais prendre la main sur le logiciel Sauron installé dans la machine infectée. Il devient alors la boîte à outils parfaite pour cyberespion. Il peut enregistrer tout ce que les victimes tapent sur leur clavier, faire des captures d'écran, activer les micros et la webcam de l'ordinateur, dérober des pans entiers du disque dur ou tous les messages envoyés et reçus... Des options de sabotage sont peut-être incluses, comme la destruction de fichiers, la modification de certains programmes ou dossiers, la falsification de résultats... Mais les analystes en sécurité interrogés n'ont repéré aucune preuve d'une telle pratique. Selon eux, Sauron ne fait qu'espionner et il est le plus discret possible, ce pourquoi les meilleurs experts ont mis presque cinq ans à repérer sa présence...

Sauron voyage aussi sur des clés USB, où il est quasiment indétectable, même lorsqu'il transporte de grosses quantités de données volées. Lorsqu'il doit envoyer à ses commanditaires, via Internet, tous les documents dérobés, Sauron est capable de simuler une mise à jour générale de Windows ou de tous les antivirus du système informatique pour camoufler le transfert des documents. Symantec et Kaspersky se sont ainsi aperçus que des données ont été volées, cachées derrière l'activité factice de leurs propres logiciels de sécurité.

Sauron a de solides liens de parenté avec de précédents programmes espions comme Flame

Pour les chercheurs, pas de doutes possibles : au moins un État est derrière ce programme. Selon Orla Cox, il faut au moins cinquante ingénieurs et hackers chevronnés pour le faire fonctionner. Cela représente des moyens colossaux. Et comme aucune pratique mafieuse n'a été dénichée, les chercheurs excluent sans hésitation l'implication d'une entreprise criminelle. De plus, Sauron a de solides liens de parenté avec de précédents programmes espions comme Flame, un peu moins sophistiqué, qui a infecté des structures stratégique au Moyen-Orient, particulièrement en Palestine, en Iran ou au Liban. Pour Orla Cox, il y a de fortes probabilités pour que les auteurs soient les mêmes. Mais Symantec se refuse à avancer une quelconque hypothèse sur le ou les pays derrière ce cyberespionnage. En cherchant des indices,

Kaspersky a par exemple repéré des mots en italien à l'intérieur du code, de même que plusieurs notes en alphabet non latin. Mais dans leur rapport, les chercheurs russes restent prudents : « Tout indice trouvé dans un programme aussi sophistiqué est certainement un écran de fumée. »

Back to TOC

8. Le Monde

La Chine prend de l'avance dans le cryptage des communications

Thursday, 18 August 2016
Byline: Harold Thibault avec David Larousserie
Section: general
Pékin - L'envoi réussi d'un satellite " quantique " permettra à Pékin de tester une technologie destinée à un usage commercial et militaire

La Chine a pris une longueur d'avance dans la maîtrise des technologies de cryptage en lançant, mardi 16 août, un satellite de communication quantique. Pékin se démarque ainsi en mettant à l'essai, au niveau spatial, une technique de transmission de clés d'encodage réputée inviolable, fondée sur les lois de la physique quantique. Le projet est suivi de près par les physiciens mais aussi par les militaires.

Une fusée Longue Marche 2-D tirée mardi à 1 h 40 de la base de Jiuquan, dans le désert de Gobi, a placé en orbite un satellite d'expérimentation quantique à échelle spatiale (Quess, selon l'acronyme anglais). Egalement surnommé Mozi, du nom du philosophe et scientifique chinois du Ve siècle avant J.-C., il permettra, sur une mission de deux ans, de tester l'envoi de clés hypersécurisées.

" De tels moyens en disent long sur les ambitions de la Chine. Elle n'hésite pas à investir des sommes colossales dans ces recherches ", commente Hoi Kwong Lo, chercheur en cryptographie quantique à l'université de Toronto (Canada). La recherche quantique est l'une des priorités du treizième plan quinquennal, feuille de route présentée en mars et qui guidera l'économie chinoise jusqu'à la fin 2020.

Clés de chiffrement De son côté, le Conseil national américain des sciences et technologies note dans un rapport rendu public le 26 juillet que si les Etats-Unis dépensent actuellement 200 millions de dollars (177 millions d'euros) par an dans ce domaine de recherche, leur rythme de progression dans le -domaine de l'information quantique a souffert de " l'instabilité " des financements.

Le protocole du satellite chinois utilise des propriétés quantiques des photons qui peuvent être corrélés de telle manière que modifier l'un modifie immédiatement son jumeau, trahissant donc une intervention non désirée.

Si les signaux transitant entre le satellite et la Terre sont interceptés par un espion, la source s'en rendra compte immédiatement et n'utilisera pas les informations envoyées. Des clés de chiffrement de messages pourront ainsi être transmises sans risque, assurant la sécurité des communications. Derrière ce projet se trouve un scientifique chinois, Pan Jianwei. A la fin des années 1990, M. Pan a effectué sa thèse à l'université de Vienne, sous la direction d'un

chercheur en physique quantique, Anton Zeilinger. Ce dernier raconte avoir demandé un peu plus tard à l'Union européenne (UE) d'appuyer un programme de développement d'un satellite quantique sans jamais avoir obtenu les financements.

De leur côté, les Chinois ont perçu les applications stratégiques d'une telle technologie, y voyant un intérêt national. M. Pan, devenu vice-président de l'Université chinoise des sciences et technologies, a pris, en 2011, la tête de ce nouveau programme.

" Beaucoup de gens pensent que les communications quantiques joueront un rôle, notamment, dans le futur d'Internet. C'est à double usage, on pourra aussi bien crypter une communication militaire que commerciale, ce ne sera qu'une question d'applications ", résume par téléphone le professeur Zeilinger, qui assiste Pan Jianwei sur le projet chinois et était présent lors du lancement de la fusée.

" Usage à l'échelle planétaire "En mai, M. Pan se référait aux fuites de dossiers de l'Agence nationale de sécurité (NSA) américaine pour justifier le développement par la Chine de nouvelles technologies de cryptage. " Le cas Edward Snowden nous a appris que, dans les réseaux de transmission, l'information est exposée au risque d'être surveillée et attaquée par des hackers ", déclarait-il à la presse officielle. La Chine testera d'abord des communications sécurisées entre Pékin et Urumqi, grande ville de l'ouest du pays distante de 2 400 kilomètres, puis entre la capitale chinoise et celle de l'Autriche.

La technologie de cryptage quantique est déjà utilisée au sol, par exemple à l'essai entre des banques reliées par fibre optique, mais sur des distances très limitées. " On sait depuis plusieurs années faire du cryptage quantique dans une même ville, mais pas entre des régions éloignées. L'emploi du satellite permet d'envisager un usage à l'échelle planétaire ", résume Alexander Ling, professeur au Centre de technologies quantiques de l'université de Singapour.

Le président chinois, Xi Jinping, avait regretté en mai la " faiblesse " de son pays, " toujours sous le contrôle d'autres pour ce qui est des technologies fondamentales dans les secteurs clés " . Il avait détaillé les objectifs fixés par l'Etat : s'imposer comme " l'un des pays les plus innovants en 2020 " puis comme une puissance technologique incontournable en 2049, pour le centième anniversaire de la fondation de la République populaire.

9. The Australian

National Security must come firm in any China deal

Thursday, 18 August 2016
Byline: Greg Sheridan
Section: column
The Turnbull government made exactly the right decision in rejecting proposed Chinese bids for majority ownership of the NSW poles and wires company Ausgrid, and it did so in substantially the right way. There is no reputational damage to Australia in this at all.

Most, not all, of the criticism of both the decision and the process has been wildly overblown and demonstrates a lack of understanding of the national security issues involved or the reality of Chinese foreign investments and strategic policy. There are three positions open to a

government. Either the Chinese can invest in any Australian infrastructure, in which case our national security would be hopelessly compromised. Or they can invest in no Australian infrastructure. This would be a very controversial and discriminatory policy, hard to justify and cost some otherwise welcome investment.

Or there is reality, that difficult and sensitive cases must be exhaustively evaluated case by case.

The Ausgrid rejection by Scott Morrison was on national security grounds. This was the unanimous recommendation of every relevant national security agency and the unanimous view of every member of the Foreign Investment Review Board. Calls for greater transparency are utterly ridiculous. Name the nation that publishes the most sensitive vulnerabilities and secrets of its critical national infrastructure.

After the disastrous Port of Darwin sale to a Chinese company, the Turnbull government, in consultation with the states, and with their full agreement, amended the relevant regulations so all state and territory sales of critical infrastructure to foreign entities will be reviewed by FIRB.

It is absolutely right that the government, not some notionally apolitical bureaucracy, makes the final decision. It is the government that has the political authority, and the constitutional and democratic requirement, to safeguard Australian national security.

But each piece of infrastructure is different -- indeed, each is unique -- and each bid is different. Australia welcomes foreign investment, including Chinese investment. The overwhelming majority of Chinese investment applications have been approved by FIRB. By any Asian standard, Australia has a remarkably liberal and welcoming approach to foreign investment.

That does not mean we have given up our sovereignty and, unique among the nations of the world, cannot exercise it over any particular proposed foreign investment. So the question of, say, a Chinese company buying Australian farmland is more a political than a security question. But it is perfectly legitimate for a government to take a political view of that.

At the other end of the scale is Chinese investment in our telecommunications network. That would be unlikely to be approved. Power companies lie somewhere in the middle. When a proposed sale is reviewed, the government asks the security agencies a lot of technical questions. What harm, if it wanted to do harm, could the Chinese investment facilitate? How important and sensitive is the infrastructure involved? Are there thresholds of potential influence, or information, that a controlling investment would yield as opposed to a passive investment?

All of these questions can be answered in each specific case only in response to a specific bid. They cannot be meaningfully addressed in a policy paper, a grand vision statement or even a treaty unless Australia decides to strip itself of the normal powers of sovereignty, which may please the Chinese but is a perverse action for us to take.

There are a few points of context to bear in mind. It is no longer a crucial distinction, if it ever was, between a Chinese state-owned company and simply a Chinese company based in China. The former Labor government banned Huawei from involvement in the National Broadband Network even though Huawei is not government owned. The intelligence and analytical

agencies of every significant Western and Asian nation all conclude that, in the end, when push comes to shove, a Chinese company will do as its government tells it to.

For the first time in our history, we have a big foreign investor who is not an ally or a broadly strategically aligned power. National security agencies have to look at credible worst-case scenarios. Rejecting a proposed investment does not mean the government has decided the proposed investor is a bad actor. Rather, it is just saying the overall risk is unacceptable.

The second point of context is that you cannot possibly ignore Beijing's appalling behaviour over the past half decade and more, and this is not solely, or even in a sense mainly, about the South China Sea. Although they won't say this publicly, the security agencies are aware that the biggest source of hostile cyber intrusions against Australia is China. The Americans have made this case at length in public and in detail. The Chinese are also the most active foreign espionage power in Australia. Good China policy requires balance. We welcome China's economic development and take every opportunity for co- operation. But we don't abdicate our responsibility for our own national security.

The Australian National University's Peter Drysdale has co- authored a pretty useless paper with a lot of silly recommendations that would cede a lot of Australian power to China in the guise of promoting greater co-operation. Drysdale, and his long-term friend and collaborator Ross Garnaut (not involved in this paper), have made big contributions to Australian policy over the years, but they have been very poor guides on China policy for many years now.

In 2009 the Chinese state-owned Chinalco bid for a huge stake in Rio Tinto fell over as it became clear the Australian government was very reluctant about it. Drysdale wrote in The Australian Financial Review that "our policymakers looked like a bunch of stumblebums ... opposition leaders (Malcolm Turnbull, Peter Costello, Joe Hockey) performed like a bunch of clowns" and so on. He went on to rhapsodise that among the official Chinese, "There is generosity (to Australia) to a fault, about what failings we might have ... Above all, there is a genuine warmness towards Australia." Shortly after this column the Chinese arrested Stern Hu, a senior Australian Rio Tinto executive in China whose life of alleged corruption had apparently gone unnoticed until the Chinalco bid fell over. More recently Chinese state-owned media have been threatening to shoot our planes out of the sky in the South China Sea. I'd hate to see what Drysdale would regard as coolness towards Australia. In any event we would be ill advised to take his advice or that of a document that advances Chinese strategic interests while being disguised as an economic study.Australian leaders since Bob Hawke have handled China policy exceptionally well. This may become harder in the future, but there is no case at all for sacrificing our national security interests.

10. Wall Street Journal

Privatization Of Internet Governance Begins Oct. 1

Wednesday, 17 August 2016
Byline: John D. McKinnon
Section: general

Washington - The Obama administration said Tuesday it will formally shift authority for much of the internet's governance to a nonprofit multi- stakeholder entity on Oct. 1, a move likely to spark a backlash from some in Congress.

The administration regards the move as necessary to maintain international support for the internet and prevent a fracturing of its governance. They say transferring authority for the internet's domain-name system from the U.S. government to the Internet Corporation for Assigned Names and Numbers will have no practical effect on the internet's functioning or its users.

But the move is likely to stir concerns among conservative Republicans, who say it could endanger national security. As recently as Friday, Sens. Ted Cruz (R., Texas) and Mike Lee (R., Utah) and Rep. Sean Duffy (R., Wis.) sent a letter to the administration, complaining again of its "planned internet giveaway." Lawmakers have adopted budget restrictions in recent years to try to stave off the move. But restrictions expire Sept. 30, giving lawmakers little time to act if they want to block the executive action.

The administration in March 2014 announced its intent to wind down the U.S.'s stewardship role when it comes to the domain-name system and relinquish control to Icann, which manages technical functions that help computers locate servers and websites.

Back to TOC

11. New York Times

'Shadow Brokers' Leak Raises Alarming Question: Was the N.S.A. Hacked?

Wednesday, 17 August 2016
Byline: David E. Sanger
Section: general
Washington - The release on websites this week of what appears to be top-secret computer code that the National Security Agency has used to break into the networks of foreign governments and other espionage targets has caused deep concern inside American intelligence agencies, raising the question of whether America's own elite operatives have been hacked and their methods revealed.

Most outside experts who examined the posts, by a group calling itself the Shadow Brokers, said they contained what appeared to be genuine samples of the code -- though somewhat outdated -- used in the production of the N.S.A.'s custom-built malware.

Most of the code was designed to break through network firewalls and get inside the computer systems of competitors like Russia, China and Iran. That, in turn, allows the N.S.A. to place "implants" in the system, which can lurk unseen for years and be used to monitor network traffic or enable a debilitating computer attack.

According to these experts, the coding resembled a series of "products" developed inside the N.S.A.'s highly classified Tailored Access Operations unit, some of which were described in general terms in documents stolen three years ago by Edward J. Snowden, the former N.S.A. contractor now living in Russia.

But the code does not appear to have come from Mr. Snowden's archive, which was mostly composed of PowerPoint files and other documents that described N.S.A. programs. The documents released by Mr. Snowden and his associates contained no actual source code used to break into the networks of foreign powers.

Whoever obtained the source code apparently broke into either the top-secret, highly compartmentalized computer servers of the N.S.A. or other servers around the world that the agency would have used to store the files. The code that was published on Monday dates to mid-2013, when, after Mr. Snowden's disclosures, the agency shuttered many of its existing servers and moved code to new ones as a security measure.

By midday Tuesday Mr. Snowden himself, in a Twitter message from his exile in Moscow, declared that "circumstantial evidence and conventional wisdom indicates Russian responsibility" for publication, which he interpreted as a warning shot to the American government in case it was thinking of imposing sanctions against Russia in the cybertheft of documents from the Democratic National Committee.

"Why did they do it?" Mr. Snowden asked. "No one knows, but I suspect this is more diplomacy than intelligence, related to the escalation around the DNC hack."

Around the same time, WikiLeaks declared that it had a full set of the files -- it did not say how it had obtained them -- and would release them all in the future. The "Shadow Brokers" had said they would auction them off to the highest bidder.

"I think it's Snowden-era stuff, repackaged for resale now," said James A. Lewis, a computer expert at the Center for Strategic and International Studies, a Washington think tank. "This is probably some Russian mind game, down to the bogus accent" of some of the messages sent to media organizations by the Shadow Brokers group, delivered in broken English that seemed right out of a bad spy movie.

The N.S.A. would say nothing on Tuesday about whether the coding released was real or where it came from. Its public affairs office did not respond to inquiries.

"It certainly feels all real," said Bruce Schneier, a leading authority on state-sponsored breaches. "The question is why would someone steal it in 2013 and release it this week? That's what is making people think this is likely the work of Russian intelligence."

There are other theories, including one that some unknown group was trying to impersonate hackers working for Russian or other intelligence agencies. Impersonation is relatively easy on the internet, and it could take considerable time to determine who is behind the release of the code.

The Shadow Brokers first emerged online on Saturday, creating accounts on sites like Twitter and Tumblr and announcing plans for an auction. The group said that "we give you some Equation Group files free" and that it would auction the best ones. The Equation Group is a code name that Kaspersky Labs, a Russian cybersecurity firm, has given to the N.S.A.

While still widely considered the most talented group of state- sponsored hackers in the world, the N.S.A. is still recovering from Mr. Snowden's disclosures; it has spent hundreds of millions of dollars reconfiguring and locking down its systems.

Mr. Snowden revealed plans, code names and some operations, including against targets like China. The Shadow Brokers disclosures are much more detailed, the actual code and instructions for breaking into foreign systems as of three summers ago.

"From an operational standpoint, this is not a catastrophic leak," Nicholas Weaver, a researcher at the International Computer Science Institute in Berkeley, Calif., wrote on the Lawfare blog on Tuesday.

But he added that "the big picture is a far scarier one." In the weeks after Mr. Snowden fled Hawaii, landing in Hong Kong before ultimately going to Russia, it appears that someone obtained that source code. That, he suggested, would be an even bigger security breach for the N.S.A. than Mr. Snowden's departure with his trove of files.

However, the fact that the code is dated from 2013 suggests that the hackers' access was cut off around then, perhaps because the agency imposed new security measures.

The attack on the Democratic National Committee has raised questions about whether the Russian government is trying to influence the American election. If so, it is unclear how -- or whether -- President Obama will respond. A response could be public or private, and it could involve sanctions, diplomatic warnings or even a counterattack.

"The real problem for us is that the Russians seem to have taken the gloves off in the cyberdomain," said Mr. Lewis, of the Center for Strategic and International Studies, "and we don't know how to respond."

Back to top

12. Washington Post

Powerful NSA hacking tools have been revealed online

Wednesday, 17 August 2016
Byline: Ellen Nakashima
Section: general
Washington - Some of the most powerful espionage tools created by the National Security Agency's elite group of hackers have been revealed in recent days, a development that could pose severe consequences for the spy agency's operations and the security of government and corporate computers.

A cache of hacking tools with code names such as Epicbanana, Buzzdirection and Egregiousblunder appeared mysteriously online over the weekend, setting the security world abuzz with speculation over whether the material was legitimate.

The file appeared to be real, according to former NSA personnel who worked in the agency's hacking division, known as Tailored Access Operations (TAO).

"Without a doubt, they're the keys to the kingdom," said one former TAO employee, who spoke on the condition of anonymity to discuss sensitive internal operations. "The stuff you're talking

about would undermine the security of a lot of major government and corporate networks both here and abroad."

Said a second former TAO hacker who saw the file: "From what I saw, there was no doubt in my mind that it was legitimate."

The file contained 300 megabytes of information, including several "exploits," or tools for taking control of firewalls in order to control a network, and a number of implants that might, for instance, exfiltrate or modify information.

The exploits are not run-of-the-mill tools to target everyday individuals. They are expensive software used to take over firewalls, such as Cisco and Fortinet, that are used "in the largest and most critical commercial, educational and government agencies around the world," said Blake Darche, another former TAO operator and now head of security research at Area 1 Security.

The software apparently dates back to 2013 and appears to have been taken then, experts said, citing file creation dates, among other things.

"What's clear is that these are highly sophisticated and authentic hacking tools," said Oren Falkowitz, chief executive of Area 1 Security and another former TAO employee.

Several of the exploits were pieces of computer code that took advantage of "zero-day" or previously unknown flaws or vulnerabilities in firewalls, which appear to be unfixed to this day, said one of the former hackers.

The disclosure of the file means that at least one other party -- possibly another country's spy agency -- has had access to the same hacking tools used by the NSA and could deploy them against organizations that are using vulnerable routers and firewalls. It might also see what the NSA is targeting and spying on. And now that the tools are public, as long as the flaws remain unpatched, other hackers can take advantage of them, too.

The NSA did not respond to requests for comment.

"Faking this information would be monumentally difficult, there is just such a sheer volume of meaningful stuff," Nicholas Weaver, a computer security researcher at the University of California at Berkeley, said in an interview. "Much of this code should never leave the NSA."

The tools were posted by a group calling itself the Shadow Brokers using file-sharing sites such as BitTorrent and DropBox.

As is typical in such cases, the true identity of whoever put the tools online remains hidden. Attached to the cache was an "auction" note that purported to be selling a second set of tools to the highest bidder: "!!! Attention government sponsors of cyber warfare and those who profit from it !!!! How much you pay for enemies cyber weapons?"

The group also said that if the auction raised 1 million bitcoins -- equivalent to roughly $500 million -- it would release the second file to the world.

The auction "is a joke," Weaver said. "It's designed to distract. It's total nonsense." He said that "bitcoin is so traceable that a Doctor Evil scheme of laundering $1 million, let alone $500 million, is frankly lunacy."

One of the former TAO operators said he suspected that whoever found the tools doesn't have everything. "The stuff they have there is super-duper interesting, but it is by far not the most interesting stuff in the tool set," he said. "If you had the rest of it, you'd be leading off with that, because you'd be commanding a much higher rate."

TAO, a secretive unit that helped craft the digital weapon known as Stuxnet, has grown in the past decade or so from several hundred to more than 2,000 personnel at the NSA's Fort Meade, Md., headquarters. The group dates to the early 1990s. Its moniker, Tailored Access Organization, suggests a precision of technique that some officials have likened to brain surgery. Its name also reflects how coding whizzes create exquisite tools from scratch, in the same way a fine tailor takes a bolt of wool and fashions a bespoke suit -- only the computer geeks more often work in jeans and T-shirts and "have epic Nerf gun fights," as one former hacker said.

Some former agency employees suspect that the leak was the result of a mistake by an NSA operator, rather than a successful hack by a foreign government of the agency's infrastructure.

When NSA personnel hack foreign computers, they don't move directly from their own covert systems to the targets', fearing that the attack would be too easy to trace. They use a form of proxy server called a "redirector" that masks the hackers' origin. They use one or more such servers to make it difficult to trace a hack.

"NSA is often lurking undetected for years on the .?.?. [proxy hops] of state hackers," former agency contractor Edward Snowden tweeted Tuesday. "This is how we follow their operations."

At the same time, other spy services, like Russia's, are doing the same thing to the United States.

It is not unprecedented for a TAO operator to accidentally upload a large file of tools to a redirector, one of the former employees said. "What's unprecedented is to not realize you made a mistake," he said. "You would recognize, 'Oops, I uploaded that set' and delete it."

Critics of the NSA have suspected that the agency, when it discovers a software vulnerability, frequently does not disclose it, thereby putting at risk the cybersecurity of anyone using that product. The file disclosure shows why it's important to tell software-makers when flaws are detected, rather than keeping them secret, one of the former agency employees said, because now the information is public, available for anyone to employ to hack widely used Internet infrastructure.

Snowden, Weaver and some of the former NSA hackers say they suspect Russian involvement in the release of the cache, though no one has offered hard evidence. They say the timing -- in the wake of high-profile disclosures of Russian government hacking of the Democratic National Committee and the Democratic Congressional Campaign Committee -- is notable.

The Russians are also suspected of involvement in the release of hacked DNC emails and of the private email addresses and personal cellphone numbers of Democratic lawmakers that

were taken from DCCC computers. Those moves have caused great consternation among party officials and dread that more is to come.

Tweeted Snowden: "Circumstantial evidence and conventional wisdom indicates Russian responsibility." He said that the disclosure "is likely a warning that someone can prove U.S. responsibility for any attacks that originated from this" redirector or malware server by linking it to the NSA.

"This could have significant foreign policy consequences," he said in another tweet. "Particularly if any of those operations targeted U.S. allies" or their elections.

"Accordingly," he tweeted, "this may be an effort to influence the calculus of decision-makers wondering how sharply to respond to the DNC hacks."

In other words, he tweeted, it looks like "somebody sending a message" that retaliating against Russia for its hacks of the political organizations "could get messy fast."

13. National Post

Fighting crime in the digital age

Wednesday, 17 August 2016
Byline: Adam Belsher
Section: oped
Op-ed - This week, top police officials from coast to coast have descended on our nation's capital for the 111th annual Canadian Association of Chiefs of Police conference. The topic that will shape their discussion, Public Safety in a Digital Age: Real Victims - Real Crime, is timely, given that we're at an important societal juncture.

So much of our daily lives now take place online: our wealth passes through jurisdictions in the form of ones and zeros; the most intimate details of our lives, whether they are held by government or industry, rest on servers located somewhere around the globe; and our critical infrastructure, whether it is managed by the public or private sector, is operated digitally.

Given the recent media coverage of data breaches and many people's personal experiences with fraudulent phishing schemes, it's understandable that we, as consumers and citizens, want to erect the highest walls possible around our valuable digital assets. This is a natural human reaction, but it isn't a realistic societal response, given the magnitude of our online world. Consider some facts. Ninety per cent of the data that has ever been created has been produced in the past two years. Every minute, 300 hours of video are uploaded to YouTube. Current prototypes of driverless cars generate a gigabyte of data a second. This year alone, 1.4 billion smartphones will be shipped. In the next five years, it is estimated that there will be 50 billion connected devices worldwide. And these are conservative estimates, given the exponential innovation we've seen in the field of information technology in recent years.

Securing ourselves and our digital assets on our own is not feasible. We cannot create a zero-risk digital environment. The statistics underscore this. In Stats-Can's last national analysis on

crime, it reported that the overall crime rate is down to its lowest point since 1998. However, three areas of crime have increased significantly: fraud, child exploitation and terrorism.

What ties these together is the fact that they are crimes that are enabled by our digital connectivity and how hard it is for police agencies to deter and investigate these felonies, because technology allows the perpetrators to conduct their crimes with relative anonymity. But that has not deterred police forces throughout the country from trying to tackle these issues - especially in the case of child sexual exploitation, which is one of the most heinous crimes imaginable.

Last year, a number of federal, provincial and municipal agencies worked together to apprehend 41 Canadian suspects involved in a child pornography ring. In that case, there were allegedly 7,500 unique IP addresses in 100 countries used to create and trade the content. There was 1.2 petabytes of digital evidence. For context, that's the equivalent of 22 million four-drawer filing cabinets filled with documents, or 13 years of high-definition video. Most importantly, there were 19 children, whose ages ranged from nine to 15, who were being exploited.

Due to the intensive resource requirements needed to overcome the technological and legal complexities they encounter while investigating and prosecuting such cases, police agencies get to pursue only one such multi-jurisdictional child exploitation case every year. This means that many perpetrators remain free to continue exploiting children.

If we as a society are to curb these heinous crimes, and other emerging areas of crimes enabled by the Internet, building digital walls, such as end-to-end encryption, will not suffice. We must rally around our police organizations and their leaders, so they can modernize, in order to effectively fight crime in the 21st century.

This is not only about providing more resources to our police agencies. It will also require our political leaders to work with chiefs of police to change the laws surrounding evidence, jurisdictional responsibility and information sharing. Many of these laws were written before evidence resided in a virtual cloud and criminals could cross borders at the speed of light.

Information technology companies also have an important role to play. Their social licence to operate will depend, in part, on the principles by which they support police agencies' efforts to maintain a just and secure society in the digital age.

This does not mean they should give the police unfettered access to Canadians' data. It means they should establish the principles under which they will work constructively with law enforcement and under what circumstances they won't.

The digital age has shifted how we do business and socially connect here in Canada and around the world. This has largely been to the benefit of mankind. However, these technological advancements have empowered unscrupulous, technologically savvy criminals. It's time we get behind our law-enforcement agencies and give them the ability to tackle these real crimes and help real victims.

Adam Belsher is CEO of Magnet Forensics, a software company headquartered in Waterloo, Ont., that supports more than 3,000 police, national security and other agencies with investigative authorities in 93 countries by developing evidencemanagement tools.

14. ABC News

Hackers Claim to Hit NSA-Linked Super-Cyberespionage Group

Tuesday, 16 August 2016
Byline: Lee Ferran
Section: general

New York - A group of mysterious hackers recently claimed to have broken into the systems of another hacking group with suspected links to the National Security Agency, and the attackers are now attempting to auction off the cyber superweapons they said they found.

Cybersecurity experts were abuzz Monday after a group calling itself the Shadow Brokers claimed in stilted English in messages online to have hacked the Equation Group. The Equation Group was revealed last February to be an extremely high-level veteran hacking squad with "solid links" to the creators of the cyber superweapon Stuxnet, which was reportedly used in a joint NSA-Israeli intelligence operation that targeted an Iranian nuclear facility.

"How much you pay for enemies cyber weapons?" says one of the messages purportedly from the Shadow Brokers. "You see pictures. We give you some Equation Group files free, you see. This is good proof, no? You enjoy!!!"

The hackers said that they are auctioning off the best cybertools -- "better than Stuxnet" -- to the highest bidder and that if the auction raises a total of more than 1 million bitcoins -- worth more than $560 million -- they will dump more Equation Group files online to the public.

Cybersecurity experts were initially split on whether the hack was legitimate, but after initial analysis of some teaser code released by the Shadow Brokers, some have come to the conclusion that at least those tools appear to be real.

"The level that a nation-state would have to go through to fake this stuff would be like nothing we've seen before and highly unlikely," said one cybersecurity expert, who requested he not be identified because of the sensitivity of the subject.

The U.S.-based cybersecurity firm Symantec wrote today in a blog post, "It will take some time to assess all of the released files. However, early indications are that at least some of the tools released are functioning exploits."

The question remains if the tools yet to be seen are real and if they were stolen from an American intelligence agency -- presumably the NSA or its partner hacking organization U.S. Cyber Command -- a contractor, an allied intelligence agency or someone else, though some file names match the names of NSA operations revealed by former NSA contractor Edward Snowden. Four cybersecurity experts, including a U.S. official, told ABC News that from time to time the NSA outsources the development of cyberespionage tools to private contractors.

Snowden weighed in on the purported hack today on Twitter, saying that apparently an NSA "malware staging server" -- essentially a holding pen for cyberweapons -- had been breached. He suggested that someone, possibly Russian hacking teams, had been sitting on the server for a long time, collecting intelligence and stealing code.

"NSA's hackers (TAO) are told not to leave their hack tools ("binaries") on the the server after an op. But people get lazy," Snowden wrote. TAO refers to the NSA's elite offensive hacking squad, Tailored Access Operations.

Like some others who analyzed the teaser code, Snowden noted that the date references appear to end in 2013, the same year he walked out of the NSA with a huge cache of data on NSA operations so he could expose what he believed were illegal or unconstitutional surveillance programs. He said that's no coincidence; the NSA would have "migrated offensive operations to new servers as a precaution" and unknowingly cut off the mysterious hackers' access.

"You're welcome, @NSAGov. Lots of love," Snowden tweeted.

The Shadow Brokers claimed in their posting that the group "followed" Equation Group traffic, found its "source range" and then hacked it, finding "many many Equation Group cyber weapons."

The NSA did not respond to ABC News' requests for comment for this report. Dick Clarke -- a former White House counterterrorism adviser, a cybersecurity expert and an ABC News consultant -- said, "You can bet the NSA is trying to figure out whether or not this is legitimate."

According to the Russian-based Kaspersky Lab's profile, the Equation Group may have been born as far back as the mid-1990s and was found to have "solid links" indicating it was connected to the hacking team that created the Stuxnet worm that attacked and physically damaged the Iranian nuclear facility before Stuxnet's discovery in 2010. The New York Times reported that the NSA was deeply involved in the creation and deployment of Stuxnet, an unprecedented cyberweapon.

Kaspersky did not directly connect Equation Group with any government organization, but it noted that attacks from the Equation Group have focused on Iran, Russia, Pakistan, Afghanistan and others including China. The same targets would presumably be at the top of a list of U.S. intelligence priorities.

"[The Equation Group] is unique almost in every aspect of their activities: They use tools that are very complicated and expensive to develop, in order to infect victims, retrieve data and hide activity in an outstandingly professional way, and utilize classic spying techniques to deliver malicious payloads to the victims," said a Kaspersky online post in February 2015.

Representatives for the White House National Security Council declined to comment on specific cases and declined to elaborate on what actions, if any, the U.S. government would take to inform private companies about potential vulnerabilities in their systems that may be revealed to any number of malicious actors, should the hack and the auction prove real. In 2014 the White House laid out its criteria for when the U.S. government will alert private companies about vulnerabilities in their systems and when it will keep quiet about those vulnerabilities in order for U.S. intelligence to exploit them.

The Shadow Brokers' auction for the cyberweapons got off to a slow start and, as of this report, has received 13 bids, topping out at just under $1,000.

15. The National (UAE)

Haj security alert for organisers

Wednesday, 17 August 2016
Byline: Haneen Dajani
Section: general

Abu Dhabi - Haj pilgrims should be made aware of safety precautions to avoid becoming victims of crime or stampedes, authorities have warned. This year almost 5,000 people from the UAE have been issued permits to attend the pilgrimage in Saudi Arabia.

At a meeting for Haj mission organisers on Tuesday, officials from the General Authority of Islamic Affairs & Endowments (Awqaf) reminded attendees that it was their duty to ensure the safety of pilgrims under their command. "It is inevitable that we should be on security alert more than usual," said Dr Mohammed Al Kaabi, general director of Awqaf.

He said the heads of missions should pass on security advice to pilgrims. "The UAE is targeted by [some] pilgrims and other concerned parties, so by all means you should sense security issues and educate pilgrims on these issues," he said. "Don't let them act randomly, you should coordinate with them."

He instructed the organisers to monitor the entrances to their pilgrims' camps, not allowing anyone without a UAE Haj permit to enter. Pilgrims should also be told that they are not allowed to let strangers or non-UAE-based pilgrims inside their tents. "This is also to avoid congestion inside the tents," said Mr Al Kaabi.

There will be electronic scanners on entry to the camps, which will display the pilgrims' details, tent and bed number.

The Emirates Identity Authority has provided Awqaf with 200 electronic ID readers for this year's Haj. He said that pilgrims should be made aware of the location of the UAE's official mission headquarters in Mecca, Mina, Muzdalifa and Arafat - the locations of the Haj.

At last year's Haj, hundreds of pilgrims were killed in a stampede in Mina in which crowds were crushed into a bottleneck. Mr Al Kaabi said the UAE mission heads were able to handle the situation "with great expertise" as they congregated all the pilgrims in a place away from the crush, thus preventing any injuries.

He stressed that mission heads should keep all their clients' passports with them in a safe place, so they do not get lost or stolen if left with the pilgrims. "Instruct them to keep copies of their ID cards and passports with them for emergencies."

Captain Mohammed Al Naqbi, a border official from the Ministry of Interior, said pilgrims should try to avoid crowded areas for security reasons. "Their permit must always be with them, because it is a must to enter Mina (and other Haj locations), to avoid delaying procedures."

The UAE's 4,982 pilgrims have been allocated special airport entry checkpoints in Saudi Arabia to avoid getting stuck in long queues, he said. "We already prepared our borders and added more staff members and counters for pilgrims."

He reminded the audience that Saudi Arabia, like many other countries, will not allow anyone with less than six months passport validity to enter. "So everyone should double check their passports beforehand," he said.

Omran Khamis, general manager of the Al Ghoroob Haj agency, said every year they faced problems when trying to leave Arafat to go to Muzdalifa. "Last year we were standing in the queue, but the police let pilgrims who were staying on the streets pass first," he said. "So you could send an official letter to the police informing them that we should be given priority, because they follow orders."

Another problem was women's accommodation in Mina and Arafat. The Awqaf said this problem would be solved this year, because each mission manager will be in charge of big camp for all his pilgrims with enough sofa beds and facilities in advance. "So each owner will have the keys and run his tent by himself."

16. La Presse canadienne

Cybersécurité au Canada L'accès légal aux mots de passe réclamé par la police

Wednesday, 17 August 2016
Byline: Jim Bronskill
Section: general
Ottawa - Les chefs de police canadiens réclament une loi pour contraindre les gens à révéler leurs mots de passe aux forces de l'ordre s'ils ont obtenu l'approbation d'un juge.

L'Association canadienne des chefs de police (ACCP) a adopté une résolution incitant le gouvernement à prendre des mesures législatives pour faciliter l'obtention de preuves électroniques. L'ACCP estime que les criminels ont de plus en plus recours au chiffrement pour dissimuler leurs activités illicites en ligne.

Le commissaire adjoint de la Gendarmerie royale du Canada (GRC), Joe Oliver, a déclaré qu'aucune loi canadienne ne contraignait actuellement le détenteur d'un mot de passe à le révéler aux policiers dans le cadre d'une enquête.

Lors d'une conférence de presse mardi, M. Oliver a soutenu que les criminels, qu'ils soient membres de la mafia ou pédophiles, bénéficient d'un anonymat quasi absolu grâce à des outils en ligne qui camouflent leur identité de même que leurs communications.

«Les victimes dans l'espace numérique sont réelles, a rappelé M. Oliver. Les lois du Canada et sa capacité à maintenir l'ordre doivent suivre le rythme de l'évolution technologique.»

Début des consultations

Cette résolution de l'ACCP survient alors que le gouvernement fédéral entame ses consultations en matière de cybersécurité, notamment par rapport à l'équilibre entre les besoins des policiers et les libertés fondamentales. Ces consultations se poursuivront jusqu'au 15 octobre.

Au cours des dernières années, les demandes de policiers quant à l'accès aux communications en ligne ont attisé les tensions entre les autorités et les défenseurs des libertés civiles préoccupés par le droit à la vie privée.

L'enjeu a ressurgi, l'an dernier, lorsque le bureau fédéral d'enquête des États-Unis (FBI) est allé devant la cour pour obtenir le mot de passe du cellulaire d'un présumé terroriste, dans la foulée de la tuerie de San Bernardino, en Californie.

Le commissaire adjoint Joe Oliver affirme que les policiers du pays cherchent à obtenir plus aisément des informations de base sur les abonnés de services de télécommunications, dont leur nom et leur adresse, pour démarrer les enquêtes.

Autorisation d'un juge nécessaire

En juin 2014, la Cour suprême du Canada a statué que l'autorisation d'un juge est nécessaire à l'obtention de données personnelles auprès d'un fournisseur Internet.

Le plus haut tribunal au pays a rejeté l'idée que la loi fédérale sur la vie privée permettait aux entreprises de révéler, de leur propre chef, des informations relatives à l'identité de leurs clients.

Les policiers soutiennent que les entreprises de télécommunications ainsi que d'autres fournisseurs de services, telles les banques ou les agences de location, exigent dorénavant un mandat de perquisition pour pratiquement toutes les demandes d'informations de base sur une personne.

Illustration(s) :

PHOTO LA PRESSE CANADIENNE, HO-GROBO

Les criminels, qu'ils soient membres de la mafia ou pédophiles, bénéficient d'un anonymat quasi absolu grâce à des outils en ligne qui camouflent leur identité de même que leurs communications, soutient le commissaire adjoint de la Gendarmerie royale du Canada, Joe Oliver.

Back to top

17. Le Figaro

La Chine s'offre un satellite « quantique »

Wednesday, 17 August 2016
Byline: Cyrille Vanlerberghe
Section: general
Pékin - Une fusée Longue Marche a mis en orbite un satellite expérimental qui va tester la transmission de clés de chiffrement par laser, une technologie dite « de cryptographie quantique » , théoriquement inviolable.

Espace La Chine a une nouvelle fois fait la preuve de son immense ambition, à la fois scientifique et technique, en envoyant en orbite le premier satellite de cryptographie quantique.

Cet engin, appelé Mozi (ou Micius dans sa transcription latinisée), en hommage à un philosophe et artisan chinois du Ve siècle avant J.-C., peut théoriquement permettre un système inviolable de communications cryptées.

Cette mission, qui a décollé mardi matin à bord d'une fusée Longue Marche depuis le centre spatial de Jiuquan, dans le désert de Gobi, est pour l'instant purement scientifique, mais nul doute qu'elle intéresse fortement les militaires chinois, en recherche de solutions pour contrer les efforts massifs d'espionnage numérique des Américains.

« Le satellite ne transmet pas lui- même le message codé que l'on veut sécuriser, mais il permet d'échanger entre l'expéditeur et le destinataire une clé de chiffrement qui va rendre la communication inviolable. Le message codé est transmis de manière classique par **Internet** » , explique le Pr Anton Zeilinger, de l'université de Vienne, l'un des meilleurs experts au monde dans cette **technologie** de cryptographie quantique, et collaborateur du programme chinois. Le responsable scientifique du satellite, Pan Jianwei, physicien à l'université des sciences et **technologies** de Chine, est un des anciens étudiants d'Anton Zeilinger à Vienne.

La clé de chiffrement, un outil très courant en cryptographie, transmise par le satellite est une suite de 0 et de 1 qui permet au départ de transformer un message clair en une forme indécryptable, puis de le déchiffrer à l'arrivée.

L'étonnante particularité du satellite Mozi tient dans la manière dont la clé de chiffrement est partagée entre l'expéditeur et le destinataire, en exploitant des propriétés très étranges de la mécanique quantique, et plus particulièrement des photons, les particules élémentaires de la lumière. À bord du satellite se trouve un dispositif optique qui peut créer ce qu'on appelle des paires de photons en état d'intrication quantique.

Pré carré de l'Europe et des États-Unis

Un état très particulier créé pour la première fois au début des années 1980 par le Français Alain Aspect à l'Institut d'optique à Orsay. Les deux particules créées sont dans un état corrélé, et toute modification des propriétés quantiques de l'une d'entre elles se répercute immédiatement sur l'autre, même si elles sont éloignées de centaines de kilomètres l'une de l'autre. En écrivant la clé de chiffrement avec de tels photons, qui sont envoyés du satellite vers la Terre, où ils sont reçus par des télescopes, on peut ainsi s'assurer qu'aucune personne extérieure n'a pu intercepter le code. Car, en mécanique quantique, la simple opération de « lire » l'état d'une particule modifie son état, ce qui dans ce cas modifierait aussi celui de l'autre photon corrélé (resté dans le satellite) et permettrait de détecter une tentative d'espionnage. Grégoire Ribordy, cofondateur de l'entreprise suisse de cryptographie ID Qantique, prend l'analogie d'un message écrit sur une bulle de savon : « Si quelqu'un essaie de l'intercepter pendant la transmission, en touchant la bulle, il va la faire éclater. »

En utilisant ce principe de chiffrement de l'information, le satellite chinois va servir à échanger une clé quantique entre deux interlocuteurs distants de plusieurs milliers de kilomètres, au début entre Pékin et Urumqi, la capitale de la région du Xinjiang, puis entre Pékin et Vienne, avec l'équipe du professeur Zeilinger. Mais comme le satellite se trouve sur une orbite basse, à 600 km d'altitude, il ne peut survoler les deux destinations au même moment, et la transmission de la clé de chiffrement se fera en deux temps. « Le satellite échangera d'abord une clé quantique avec Pékin, puis quelques heures plus tard une autre avec Vienne, et par une

opération mathématique simple, il sera possible de reconstruire une clé commune utilisable entre Pékin et Vienne » , décrit par téléphone depuis la Chine le physicien autrichien.

Si l'expérience chinoise réussit, ce qui dépendra principalement de la finesse du pointage du satellite vers les stations au sol, cela ouvrira la voie à un échange global de clés quantiques de chiffrement. « Aujourd'hui, les applications de cryptographie quantique existantes sont basées sur une transmission par fibre optique, ce qui limite leur portée à 100 ou 150 kilomètres à cause de l'absorption de la lumière, précise Grégoire Ribordy. Notre solution est essentiellement utilisée pour sécuriser des communications sur des réseaux optiques, par exemple entre deux centres de calcul, par des clients ayant des besoins de sécurité à long terme, comme des gouvernements, des banques ou des entreprises du secteur de la santé. »

Mais l'idée que la Chine puisse prendre le leadership mondial dans un domaine aussi sensible que la cryptographie quantique, domaine qui a longtemps été le pré carré de l'Europe et des États-Unis, pourrait avoir des conséquences importantes en termes de sécurité au niveau mondial. Car le système chinois qui gérerait l'échange des clés de chiffrement « pourrait obtenir une copie des clés, et donc intercepter toutes les communications de ses éventuels clients » , prévient Grégoire Ribordy.

Aujourd'hui, les applications de cryptographie quantique existantes sont basées sur une transmission par fibre optique

Grégoire Ribordy

18. Global Times

China faces serious threat of Internet vulnerabilities

Wednesday, 17 August 2016
Section: general
China is facing a serious threat of Internet vulnerabilities to hacking, as statistics show that over 200,000 vulnerabilities were found from 2009 to 2016, a cyber security expert said at a conference on Tuesday.

According to China's National Vulnerability Database (CNVD), domestic Internet security monitoring platforms reported 25,314 vulnerabilities in 2015. Meanwhile, a report published by a security center affiliated to IT company Qihu 360 showed that 43.9 percent of 2.3 million monitored websites were found to have vulnerabilities, and 12.3 percent had high-risk vulnerabilites as of November 2015.

Yan Hanbing, a senior official with the National Computer Network Emergency Response Technical Team Coordination Center (CNCERT), said Tuesday that an increasing number of cyber vulnerabilities have been found by general software or revealed by individuals, partly due to the activity of domestic Internet security monitoring platforms in recent years.

Yan made the remarks at the 2016 China Internet Security Conference, which was jointly held by Qihu 360 and the Cyber Security Association of China on Tuesday in Beijing.

"The increase in number does not mean that our cyberspace is not safe. Instead, it shows that China is paying more attention to cyber security and will put more investment in the field," said Yan.

Xie Yongjiang, an associate professor at Beijing University of Posts and Telecommunications, said that Internet vulnerabilities are a double-edged sword, as they can bring harm to consumers or become strategic resources for companies or countries.

But several recent cases have stoked public concern about possible information leaks caused by Internet vulnerabilities.

In April 2015, Qihu 360's Internet security monitoring platform butian.360.cn found that tens of millions of Chinese residents registered in the country's social security system face a risk of personal information leaks due to system loopholes.

Yan pointed out that despite the exposure of Internet vulnerabilities, large numbers of them fail to be repaired quickly. For example, 40 percent of government websites failed to repair high-risk vulnerabilities that had been exposed for one month.

Cyber security expert Qin An previously told the Global Times that loopholes are common in the Internet era, but they should serve as a reminder to local governments to fix them as quickly as possible.

19. Associated Press

China's launch of quantum satellite major step in space race

Wednesday, 17 August 2016
Section: general
China's launch of the first quantum satellite Tuesday will push forward efforts to develop the ability to send communications that can't be penetrated by hackers, experts said.

The satellite launched into space from the Jiuquan launch base in northwestern China's Gobi desert will allow Chinese researchers to transmit test messages between Beijing and northwestern China as well as other locations around the world.

If the tests are successful, China will take a major step toward building a worldwide network that can send messages that can't be wiretapped or cracked through conventional methods.

"It moves the challenge for an eavesdropper to a different domain," said Alexander Ling, principal investigator at the Centre for Quantum Technologies in Singapore. "Lots of people around the world think having secure communications at a quantum level is important. The Europeans, the Americans had the lead, but now the Chinese are showing the way forward."

Quantum communications use subatomic particles to securely communicate between two points. A hacker trying to crack the message changes its form in a way that would alert the sender and cause the message to be altered or deleted.

Researchers around the world have successfully sent quantum messages by land. But a true satellite-based network would make it possible to send quickly encrypted messages in an instant around the world and open the door to other possible uses of the technology.

Cybersecurity has been a major focus in recent years for China, which has pushed regulations aimed at limiting technology imported from the U.S. in the wake of Edward Snowden's revelations of widespread surveillance by the U.S. through the use of American hardware.

China has in turn been repeatedly accused by the U.S. of hacking into computer systems to steal commercial secrets and information that could harm American national security. China has rejected claims that it runs a state-sponsored hacking program and says that it is among the leading victims of cybercrime.

Quantum messaging could become a major defense against hackers and have applications ranging from military and government communications to online shopping.

The biggest challenge, Ling said, is being able to orient the satellite with pinpoint accuracy to a location on Earth where it can send and receive data without being affected by any disturbances in Earth's atmosphere. The results of China's tests will be closely watched by other research teams, he said.

"It's very difficult to point the satellite accurately," Ling said. "You're trying to send a beam of light from a satellite that's 500 kilometers (310 miles) above you."

Hoi Fung Chau, a professor and quantum communications researcher at Hong Kong University, said that it was too soon to say if the tests will succeed, but added he expected quantum messages by satellite to become the global standard eventually.

"The theory is already there, the technology is almost there," he said. "It's just a matter of time."

The launch is a major triumph for China, which has spent years researching quantum technology and developing the satellite and other uses for it. China has previously announced the construction of a quantum link between Beijing and Shanghai that would be used by government agencies and banks.

Pan Jianwei, chief scientist on the satellite project, was quoted by the official Xinhua News Agency as saying the launch proved China was no longer a follower in information technology, but "one of the leaders guiding future IT achievements."

1. The International News

Seriousness towards cyber crime laws in Pakistan

Friday, 19 August 2016
Byline: Dr Nadia Khadam
Section: general

Islamabad - After the advent of 3G and 4G technology in Pakistan, cyberspace seemed to be more sensitive area. Cybercrime's rate in Pakistan is also considerably increasing day by day. To control any such like situations law is the only tool. Even if the issue got attention somewhere in preceding years that also proved to be an attempt to misuse the law either in favour or against someone. This remained a dilemma in Pakistan that whenever this issue was focused, it was with some hidden motives and not to redress the grievances of the aggrieved.

Initially due to lack of any proper specific legislation on this subject, offences relating to cybercrime are dealt under Electronic Transaction Ordinance 2002 (ETO 2002). ETO 2002 was promulgated after accepting the challenging situation created by the increased use of internet vis-a-vis electronic commerce. Section 36 of ETO 2002 penalises the violation of privacy with imprisonment up to seven years whereas Section 37 of same penalises the damage to information system with imprisonment up to seven years.

On perusal of preamble of Electronic Transaction Ordinance 2002, it is clear that this law was not enacted with an intention to penalise the offences relating to cybercrimes. That is the reason limitations of this law are very much visible. Due to the increase in use of computer, new ways of crime were emerged but none of them was included in this Ordinance, hence made this legislation less effective. The effect of this legislation is that most offenders easily escape from the law and judges are unable to frame charge against them.

After observing the deficiencies in Electronic Transaction Ordinance 2002 with respect to cybercrime a detailed law was introduced in the form of Ordinance i.e. Prevention of Electronic Crimes Ordinance 2007 (PECO 2007). PECO 2007 was likely to improve problems relating to misuse of technology. Since, this Ordinance, to a certain extent, gives provisions regarding cyber or electronic crimes and devices to curb the menace through effective legislation. But unfortunately, this ordinance remained unable to attain the status of an Act, hence, repealed in 2009. Since then, offences relating to cybercrime are dealt under ETO 2002.

After passing of six years, fortunately, cybercrime laws came under limelight again in 2014 when three bills were introduced before Parliament -- two were tabled before Senate and one before National Assembly. One was Cyber Security Council Bill, 2014 was introduced before Senate by Senator Mushahid Hussain Syed. This bill proposed the formation of National Cyber Security Council empowering the Council to make policies, guidelines and governance model, conduct research, advise different branches of government, to make laws and to analyse the situation in international perspective and more.

The other bill was Protection of Cybercrimes Bill 2014, introduced by Senator Karim Ahmad Khawaja with a purpose to prevent unauthorised acts with respect to electronic crimes and for related offences as well as procedure for their investigation, trial, prosecution, punishment and international collaboration in this regard.

Third bill namely Prevention of Electronic Crimes Bill 2014 was introduced by Ms. Anusha Rehman, Minister of State for Information Technology. It is presented before National Assembly. This law is under heated discussion currently. This bill was introduced in 2014 and approved few days back by the Parliament and it is waiting for the assent of the president. The Prevention of Electronic Crimes Bill gained more attention due to vast coverage of crimes in it. It is penalising the unauthorised access, copying, transmission, interference with information system and critical infrastructure information system or data.

Moreover, if any of the above mentioned acts done with intention to create fear in society shall be punished with imprisonment of fourteen years. Electronic forgery and fraud is penalised which will definitely help to curb emerging related crimes in Pakistan. Identity information should not be obtained or used by anyone without authorisation, if so it would be criminalised. Offences against dignity like displaying and transmitting of false information with intention to harm the reputation or privacy of natural person is a declared offence now but there is an important exception, and that is, if anything aired by the broadcast media or distribution service licensed under Pemra Ordinance 2002.

No one would now think to blackmail or harm the reputation of other by displaying immoral pictures otherwise person would face criminal liability. No individual will do cyber stalking by threatening or creating fear for any kind of contact. Glorification of an offence or convict of a crime relating to terrorism is also penalised. Selling of unauthorised SIM cards will declared as an offence. This is comprehensive law which was dire need of the time.

This area was remained neglected by the Parliament but this time concerned authorities taken this issue with much seriousness and commitment, which resulted in the passing of this bill after exhaustive debates. This law is passed and certain issues can be removed and improved through amendments. This is the beauty of law that it can be changed anytime through amendments as per requirement of time.

The way this bill was presented, perused, shared and discussed with the stakeholders and public at large is significant. Moreover, the way the criticism over the bill was welcomed is also appreciable and improvements were made in the light of the suggestions. After passing of any Act people have two options whether to do criticism for the sake of criticism or to do criticism with suggestion to make laws better and more practicable.

Ministry of Information Technology is to be commended for making it possible and all the stake holders are also to be acknowledged for giving their feedback and for helping to improve this upcoming legislation for Pakistan which is need of the hour.

Even after the passage of this Bill from the Parliament a lot of criticism is on record. The critics to this law were of the view that this law might pose serious obstacles in freedom of information and some provisions of the law needs clarification since according to them there is a danger of misuse of certain provisions. But, prudently observing those obstacles, if any, could be taken care of by suitable amendments. Those should be welcomed by the Parliament to amend and improve the law. If the same is not done this time then again Pakistan will be in a position of lawlessness in terms of cybercrimes.

2. The Pioneer

Central varsity's website hacked

Friday, 19 August 2016
Section: general
Bhopal - The official website of Dr Hari Singh Gour Central University in Sagar was allegedly hacked from across the border. The Pakistani hackers put up their national flag on the homepage and posted messages mocking India's cyber security.

As the news about Pakistani hackers breaking into the varsity's website went viral on Thursday, the university administration acted swiftly and closed the site for a while.

As soon as the administration got information about hacking of the institute's website, it was closed. Later, when it was re-started, it was again hacked by them following which it was made offline by the authorities concerned, University's Media Officer Diwakar Rajput said.

The hackers mocking Indian cyber security wrote messages on the website beginning with a dialogue of an Indian film, "...Kamaal karte ho Pandeyji...Well it's hacked by Pakistani hackers and a slap on the faces of Indian cyber security."

Describing themselves as the cyber world's Al-Qaeda, the hackers further wrote, "Bharat sarkar hume cyber apradhi manti hai...Haa hum cyber space ke Al-Qaeda hai (Indian Government treats us as cyber criminals...Yes we are the Al-Qaeda of cyber space)."

Meanwhile, varsity authorities are planning to restore the website by this evening. "The website will be re- started by this evening. Entire data is safe. A formal complaint has been registered in this regard with the Civil Lines Police Station and a report has been sent to the Union Human Resources Development Ministry on the issue," Rajput said.

However, a senior police officer posted in Cyber Cell told that it is a routine affair. Whenever there is vulnerability in the website, the hackers attack the website, not matter where it belongs.

Back to top

3. Gulf News

Al Qaida suicide bomber kills four Yemen troops

Friday, 19 August 2016
Byline: Staff Report
Section: general
Aden - An Al Qaida suicide bomber killed four Yemeni soldiers in an attack on Thursday in the southern Abyan province, where government forces have launched an anti-terror offensive, a military official said.

The attacker rammed his car into two military vehicles parked on a road linking the towns of Loder and Moudia in Abyan province, the source said. "Four soldiers were killed and others were wounded," the official said.

Military sources said the bombing was a retaliation attack by Al Qaida after government troops recaptured parts of Abyan, including provincial capital Zinjibar.

Government forces, backed by air power from a Saudi-led coalition, launched the offensive to retake Abyan on Sunday, after they failed to recapture the vast province earlier this year.

Al Qaida and Daesh terrorists have exploited a power vacuum in Yemen to expand their presence in the country's south and southeast.

Yemeni authorities had trained hundreds of soldiers in the nearby province of Aden over the past two months to retake Abyan.

The Arab coalition, which intervened against Iran-backed rebels in March last, began supporting the government's war on terrorists this year.

The United States has also pressed a drone war against them. Washington considers the Yemen-based Al Qaida in the Arabian Peninsula, or AQAP, to be the extremist network's deadliest franchise.

Back to top

4. Gulf News

Mobilising the datacentre with modular solutions

Friday, 19 August 2016
Byline: Jyoti Lalchandani
Section: general
Dubai - The term 'datacentre' has been part of the technologist's lexicon since the 1960s. Back then, organisations housed large mainframe computers in huge rooms and referred to them as datacentres. However, it wasn't until the late 90s that datacentres actually started living up to their name by functioning as central hubs for storing, managing, and circulating enterprise data.

Today, the datacentre is critical to enterprise operations, as it is the place where the organisation's most critical processes are run and managed from. The transformation of the datacentre over the last 50 years has helped organisations embrace the advantages of consolidation, convergence, and cloud implementations. Indeed, the datacentres of today are an essential cloud-enabling technology, forming the platform for private cloud implementations.

Over the last five years or so, various breakthroughs in the datacentre market helped organisations to efficiently manage their data and processes while also keeping a lid on their capital expenditure. Consolidation has been a key motivator in spurring innovations within the datacentre space, and one such innovation has been the introduction of the modular datacentre solution.

Modular datacentres (MDCs) are modular facility products that are portable in nature and procured with the purpose of mobilising datacentre resources. Container datacentres (CDCs) are a subset of modular datacentres, where the IT and facilities assets are all bundled in a

single unit the size of a standard shipping container. While MDCs are usually built indoors, CDCs can typically be found outdoors.

Although these New-Age solutions are still in the early stages of adoption here in the Middle East, they are being embraced by datacentre providers and end-user organisations alike. This is because both MDCs and CDCs offer a string of benefits that traditional datacentres simply cannot match.

The construction of traditional datacentres is a lengthy and complex affair, with traditional datacentres often taking years to design, build, and put into operation. By contrast, MDCs and CDCs can be built in a matter of months.

The main reason for this is that certain parts of these solutions are prefabricated, meaning they are built in a factory and shipped to their desired location ready for use. This saves considerable time for the end user and enables a much quicker return on investment.

The initial capital costs for building a traditional datacentre are also very high when compared to MDCs. The main reason for this is that MDCs are extremely scalable, so additional datacentre capacity can be deployed as and when needed. This eliminates unnecessary costs around unused capacity, which is a common complaint with traditional datacentres. Furthermore, construction costs for MDCs and CDCs are much lower than for traditional datacentres.

Traditional datacentres are also not particularly secure when it comes to storing and exchanging mission-critical information. As such, many organisations prefer to use modular solutions when setting up their datacentres, which is another clear advantage that MDCs and CDCs have over traditional brick-and-mortar data centers.

Crucially, these new modular solutions can be deployed in any place and at any time. Indeed, both MDCs and CDCs have proved extremely popular in remote locations and places that experience extreme weather conditions, and they are now increasingly seeing traction among enterprises that are looking to expand their existing datacentres. CDCs are also regularly used for temporary deployments, such as in a disaster-affected area or during the construction phase of a new project.

MDCs come with different options and a variety of capacity levels. The most popular MDCs in the Middle East region come with a power density of 5KW/rack and feature in-row cooling systems. The in-row cooling is a particularly popular feature here due to the high temperatures that characterise the region's climate.

The government sector is the region's biggest user of MDCs and CDCs, with the solutions often deployed in remote locations or as border control stations. Other verticals deploying these solutions include the oil and gas sector for offshore projects, the health care sector for use inside hospital pharmacies, and the BFSI sector for managing huge amounts of data, particularly in insurance organisations.

They are also finding use in the telecommunications sector as operators look to expand their current datacentres in order to cope with the huge amounts of data that is being generated on a daily basis.

While many organisations see modular datacentres as the future, the traditional datacentre market continues to grow in the region. This is simply because one size cannot possibly fit all, and a lot of organisations still prefer the build-to-suit concept. So the emergence of these New-Age modular solutions does not necessarily sound the death knell for the traditional datacentre.

Instead, they are offering a viable alternative to those organisations that are seeking a more economical and efficient way to manage their IT infrastructure.

Modular datacentre solutions make up anywhere between 10--20 per cent of the total datacentre market in the Middle East, depending on the country in question. Datacentre providers are constantly trying to build awareness around these solutions and the benefits they offer.

So, while traditional datacentres aren't going anywhere in the near future, you can be sure that the region's MDC and CDC markets are set to grow at a very fast pace over the next five years.

5. Business Insider (UK)

Here's why the NSA won't release a 'smoking gun' implicating Russia in these major hacks

Friday, 19 August 2016
Byline: Paul Szoldra
Section: general
London - Was Russia behind the massive hack of the Democratic National Committee, or the latest breach of what appears to be the NSA's elite hacking unit?

That's quite possible, but the US National Security Agency is probably not going confirm that -- even as former employees proclaim that it can do so, and top US officials say that there is "little doubt" Moscow is involved.

Former NSA contractor Edward Snowden said on Twitter that "evidence that could publicly attribute responsibility for the DNC hack certainly exists at NSA" with a tool known as XKeyscore, which he previously described as a "one stop shop" for information it collects.

If that's true, then it's likely that that same tool could find the culprits behind the latest attack.

But Dr. Peter Singer, a strategist at the think tank New America and coauthor of "Ghost Fleet," argues that releasing a "smoking gun" clearly pointing the finger at Russia -- or some other nation -- for a cyberattack bears a much larger risk of blowing future operations.

If the NSA has covert computers just sitting back and watching as Russian hackers hit a target, then it probably doesn't want to give those up by trying to prove it.

"You give away capabilities and maybe even access if you reveal that," Singer told Business Insider, adding that it's a case of "I can't show you my homework because it means I'll give up this intelligence goldmine."

That's not to say that Russia is not involved in the hack of the DNC or the NSA. Cybersecurity firm CrowdStrike found two different Russia-linked hacker groups inside the DNC servers, while providing a technical analysis of its findings. And some former agency employees believe that Moscow is behind the mysterious "Shadow Brokers" claiming to have hacked the NSA.

But a detailed dump of evidence like President John Kennedy did in 1962, proving that nuclear missiles were inside Cuba, is probably not coming.

"President Kennedy famously gave his press briefing where he actually showed U-2 spy plane photos, and this gave away great secrets of the United States, but it also proved to the world that there were, in fact, missiles in Cuba," Cris Thomas, a strategist at Tenable Network Security and former hacker at the legendary L0pht collective, told Business Insider in May of the Sony hack, which officials publicly blamed on North Korea.

The US should "say 'this is why we think this country did this thing ... here's our evidence, here's our IP addresses, here's our packet captures,' just so that it's not a he-said/she- said type of thing."

Many in the computer-security community are often skeptical of attribution claims, since attacks can originate from previously hacked machines and hop over a variety of servers, and exposed code and hacker toolkits can end up pointing the finger at someone else entirely.

In short, attribution is difficult, if not impossible.

The problem is twofold: Gathering definitive evidence is extremely hard, and even that data, if obtained, is not easy to understand by average people outside the world of computer-security research.

"What is persuasive when so few people understand the topic?" Singer asked. "The most persuasive stuff might be the most technical."

Even a former NSA hacker who took part in cyberattacks on behalf of the US agrees.

"I can tell you that if I got onto a machine today and I found a Russian backdoor and I started using it, it's just software. You wouldn't know that I was using it," the source, who spoke on condition of anonymity to discuss sensitive matters, told Business Insider. "It's just really hard to know who's using, who created it. I find these analyses that 'the code had a reference to this part of the Bible, so it must be Israel,' it's just really kind of silly."

6. Ottawa Citizen

Parliament Hill and Rideau Hall overflown 14 times so far in 2016

Friday, 19 August 2016
Byline: Andrew Duffy
Section: general

Ottawa - The restricted airspace over Parliament Hill and Rideau Hall has already been violated 14 times this year in a series of incidents that highlight the difficulty of securing the capital's most sensitive facilities.

Among the offenders was a lowflying helicopter that violated both protected airspaces on the same day in late March. Contacted by air traffic controllers, the pilot said that his GPS was broken and he was having trouble finding the Casino du Lac Leamy.

The incident was reported both to the Royal Canadian Mounted Police and the North American Aerospace Defense Command (NORAD), according to a Transport Canada database that tracks federal airspace violations.

In the first seven months of this year, five aircraft violated the airspace over Parliament Hill and nine penetrated the protected space over Rideau Hall, the grounds on which Prime Minister Justin Trudeau and his family are living while 24 Sussex Drive is repaired.

Most of the offending aircraft were privately owned small planes or helicopters.

One, a Piper aircraft, was owned by the Airborne Sensing Corporation of Toronto, a company that does aerial photography. It descended to 1,500 feet above Parliament Hill on April 23.

During 2015, there was a total of 15 incursions into Ottawa's protected airspace, and 13 the year before that, according to a Postmedia analysis of the federal government's Civil Aviation Daily Occurrence Reporting System (CADORS) database.

In 2011, there were only three airspace violations in Ottawa, but those numbers skyrocketed in 2012 when the restricted area over the two sites more than doubled in size.

After conducting a risk evaluation, the RCMP sought and received approval from Transport Canada to increase the designated altitude for the restricted areas to 3,000 feet from 1,500. The radius of the protected areas also increased.

Air traffic controllers at Ottawa International Airport monitor the restricted airspace over Parliament Hill and Rideau Hall, while Transport Canada officials enforce the no-fly regulations. Fines - usually $750 to $1,000 - are regularly imposed against offending pilots.

The RCMP's National Division is responsible for the protection of key federal properties in the city, including Parliament Hill, Rideau Hall, the Supreme Court and the

prime minister's residences.

A National Division spokesperson declined to comment on the challenge posed by airspace incursions, as did Sen. Vern White, the former Ottawa police chief who co-chairs an advisory committee on Hill security.

The RCMP's security posture on Parliament Hill, including its approach to airspace defence, was reviewed after Michael Zehaf-Bibeau, 32, an armed jihadist, stormed into Centre Block in October 2014.

He was shot dead by security forces within four minutes of entering Parliament's front doors. In March 2015, the OPP released its review and also made recommendations about airspace defence, but that part of the report was not made public.

The challenge posed by airspace defence is considerable, particularly when today's drones are so small that they can evade radar.

Early last year, for instance, a small drone, a DJI Phantom, crashed into the South Lawn of the White House after a government employee lost control of it. Under U.S. federal law, it is illegal to fly a drone in Washington, which has a large flight-restricted zone.

Also last year, in April, a small aircraft known as "gyroplane" flew into Washington's restricted airspace and landed on the West Lawn of the Capitol building. The Florida mailman who staged the stunt as a protest was later sentenced to four months in jail.

In September 1994, a light plane crashed on the White House lawn during the night, killing the pilot. Twenty years earlier, in 1974, a U.S. soldier commandeered a military helicopter and flew it to the White House - the same year that another man, Samuel Byck, tried to hijack a commercial aircraft in a failed attempt to assassinate thenpresident Richard Nixon.

Return to TOC

7. itWorldCanada.com

Canada's police chiefs: "We need laws that force cybercriminals to reveal their passwords"

Friday, 19 August 2016
Byline: Ryan Patrick
Section: general
Ottawa - The news that Canada's police chiefs are advocating for federal laws that would compel individuals to provide electronic passwords with a judge's consent isn't sitting well with some members of Canada's IT community.

Earlier this week at its annual conference in Ottawa, the Canadian Association of Chiefs of Police (CACP) passed a resolution that formally requests legal measures to lawfully unlock digital evidence, citing the rise of cybercriminals who are using encryption tools to hide illicit activities as the impetus.

During a news conference on Tuesday, RCMP Assistant Commissioner Joe Oliver noted that at present under Canadian law, police cannot compel individuals to comply with a request to provide a password during an investigation. Law enforcement needs to keep pace with modern criminals who are effectively "going dark" by operating in cyberspace with tools that mask their identities, said Oliver.

"The victims in the digital space are real," said Oliver, adding that Canada's law and policing capabilities aren't keeping pace with the evolution of technology.

But according to Jacob Ginsberg, senior director for Toronto-based email encryption software firm Echoworx, such as move would be an "unconscionable" one.

"While we don't blame CACP for wanting tools to make their jobs easier, a law of this kind would criminalize privacy, and it would be unconscionable for a democratic society to draft a law whereby denying a request from police to go through your things, digital or otherwise, would be illegal," he said in an email.

The association represents in excess of 90 per cent of the police community in Canada which include federal (RCMP), First Nations, provincial, regional and municipal, transportation and military police leaders. The CACP theme for its 111th conference was "public safety in a digital age" and police chiefs such as Ottawa Police Chief Charles Bordeleau noted in a statement the event was intended as an "opportunity to share, learn and work together on a way forward that helps us fuse traditional policing with modern day cyber activity."

"Police services across the world are facing new challenges and threats related to technological developments and the criminal innovation that has ensued," Bordeleau said.

In 2014, the rights of online users were upheld in a Supreme Court of Canada ruling that Internet service providers cannot deliver user names and addresses to law enforcement without a warrant. At the time, The Supreme Court didn't agree with the concept of users having "no reasonable expectation of privacy" for the data obtained by police.

According to police, service-oriented enterprises such as financial firms and telecommunication companies currently require court approval for nearly all types of requests from authorities for basic identifying information.

The CACP also cited a recent Osterman Research report that revealed that 44 of 125 Canadian companies interviewed suffered a ransomware attack in the past 12 months -- of which 33 of the victims paid a ransom that was between $1,000 and $50,000 in order to regain stolen data.

But the issue of handing over passwords --even with a court order -- will be controversial, predicts Ray Boisvert, CEO of I-Sec Integrated Strategies and former deputy director of intelligence at the Canadian Security Intelligence Service (CSIS).

In an interview with IT World Canada, he said he understands the view of those worried about privacy. However, he also understands the position of police, who have legitimate obligations to investigate crime.

In the non-digital world, he noted, search warrants already allow police to seize and go through paper documents looking for specific information spelled out in the warrant. Sometimes, he added, the warrant can be quite broad.

"On the face of it, this seems like it's clearly unconstitutional," David Christopher of Internet advocacy group OpenMedia told CBC News, adding the CACP request represents a "wildly disproportionate" response considering the individual privacy risks involved.

Added Echoworx's Ginberg: "Policy makers and courts across the globe are still adjusting to crime in the digital age, but having the power to access a person's whole digital life, especially

during the course of an investigation where it's not established that wrongdoing has taken place, should not make you a criminal."

Back to top

8. Reuters

Japan eyes fighter drone, seeks record defence budget amid China assertiveness

Friday, 19 August 2016
Section: general
Japan aims to develop a prototype drone fighter jet in two decades with private sector help in a technology strategy that focuses on weapons communications and lasers, according to a document seen by Reuters.

The plan will be announced this month when the Defence Ministry also unveils its request for a record budget of 5.16 trillion yen ($51 billion) for fiscal 2017, as tension rises in the East China Sea and North Korea steps up its missile threat, government officials with direct knowledge of the matter said.

The military technology plan calls for first developing an unmanned surveillance aircraft in the next decade and then an unmanned fighter jet 10 years later, the document showed.

The rise of 2.3 percent over this year's budget of 5.05 trillion yen marks the fifth successive annual increase sought by the ministry, which is keen to stiffen Japan's defences as North Korea upgrades its ballistic missile technology.

However, one security analyst said the spending was insufficient. "The security environment surrounding Japan is severe, due to neighbouring North Korea and China," said Takashi Kawakami, a security expert at Japan's Takushoku University.

"I personally think it's not enough."

Japan will this month formally unveil budget requests for its defence and other ministries for the year ending March 2018.

The defence ministry's request covers the 100 billion yen cost to upgrade Japan's PAC-3 missile defence system, said one government source, who declined to be identified, as he was not authorised to speak to the media.

Such an upgrade would roughly double the missile system's range to more than 30 km (19 miles), other sources have said.

The budget proposal also includes the cost of production of the Block IIA version of the Standard Missile-3 system being jointly developed with the United States to shoot down missiles at higher altitudes, the source added.

The ministry will also allocate budget funds to acquire an upgraded version of the F-35 stealth fighter, made by U.S. company Lockheed Martin Corp, the source said.

The budget request also includes the cost of strengthening the coast guard in the southern islands of Miyakojima and Amami Oshima to allay worries over China's more assertive activities in the East China Sea, said the source.

Tension mounted this month after a growing number of Chinese coast guard and other vessels sailed near disputed islets in the East China Sea.

Japan, China and South Korea are in talks to hold a meeting of their foreign ministers next week.

9. Global Times

Watchdog asks websites to strictly manage online content

Friday, 19 August 2016
Section: general
China's Internet watchdog has vowed to strengthen supervision over new Internet products and functions, including live webcasts and bullet screens.

At a forum in Beijing on Wednesday, the Cyber Administration of China (CAC) proposed eight measures for websites to better manage online information, including better scrutiny of online news products, applications, functions, such as live webcasts and bullet screens, The Beijing News reported Wednesday.

Bullet screens refer to comments that users make while watching videos. The comments shoot across the screen, a barrage of one-line quips like shots fired from a gun.

News websites would be required to develop a list of responsibilities for their chief editors, who should take charge of news content as well as the process that goes with it, according to an announcement on the CAC's official website.

Websites should also build 24/7 duty systems, provide comment management and report replies. In its inspection of eight major commercial websites, the State Internet Information Office found several problems, including information security bugs.

Deputy chief Ren Xianliang said administrative departments and Internet companies should work together to find new methods.

The Beijing Cyberspace Administration shut down some portions of several commercial news portals run by major Internet giants for publishing original articles related to social and political issues in July.

Les chefs des grands services de renseignements

Friday, 19 August 2016
Byline: Vincent Nouzille
Section: general

Paris - Ils ont fait carrière dans l'armée, la diplomatie, la police ou... les services secrets, et disposent de la toute confiance des chefs d'Etat qu'ils servent. Mais qui sont vraiment les patrons des grandes centrales du renseignement contemporain?

? Bernard Bajolet (DGSE), l'homme de confiance de Hollande

À 67 ans passés, Bernard Bajolet ne devrait normalement plus occuper le siège de patron de la Direction générale de la sécurité extérieure (DGSE) et profiter d'une retraite méritée dans son château d'Ouge, en Haute-Saône. Mais cet énarque diplomate a déjà été prolongé deux fois à son poste par François Hollande, qui veut le garder jusqu'en mai 2017. Car le président de la République a toute confiance en ce Lorrain au tempérament rugueux, qu'il a connu lorsqu'il effectuait son stage à l'ambassade de France à Alger en 1978. Les deux hommes se tutoient et se parlent presque tous les jours.

Bernard Bajolet n'a pas été nommé par hasard au printemps 2013 à la tête de la DGSE. Il connaît tous les arcanes de la diplomatie, des couloirs du Quai d'Orsay au palais Farnèse à Rome. Ce polyglotte arabophone a surtout occupé des postes exposés dans des pays difficiles: en Jordanie, en Bosnie-Herzégovine, en Irak où il a rouvert l'ambassade de France en 2004, en Algérie, en Afghanistan de 2011 à 2013. Habitué à vivre dans des bunkers blindés, l'ambassadeur a négocié, avec la DGSE, de nombreuses libérations d'otages, comme celles des journalistes Georges Malbrunot et Christian Chesnot en Irak en 2004. Repéré par Nicolas Sarkozy, il a aussi étrenné le poste de coordonnateur national du renseignement créé à l'Elysée en 2008.

A la tête de la DGSE, qui emploie près de 5000 personnes dont un quart de femmes*, il gère ses dossiers en toute autonomie, n'hésitant pas à assumer des opérations clandestines musclées, que ce soit en Libye ou en Syrie. Il est aussi à l'aise avec les experts du monde arabe qu'avec ses pairs étrangers, qu'il rencontre régulièrement. Il lui arrive aussi de voyager incognito lors de missions secrètes, dont il ne rend compte qu'à son ami François Hollande.

*À lire sur le sujet, l'enquête de Dalila Kerchouche: Espionnes (Flammarion, 360 p., 21 , à paraître le 21 septembre).

? Patrick Calvar (DGSI), l'expert de l'Intérieur

Lorsque Patrick Calvar explique, le 24 mai, devant les membres de la commission parlementaire sur les attentats de 2015, que les risques terroristes n'ont jamais été aussi élevés et que Daech va continuer de monter en puissance, tout le monde l'écoute. Car ce policier de 60 ans, qui pilote la Direction générale de la sécurité intérieure (DGSI) depuis quatre ans, est un expert reconnu du monde arabo-musulman. Ce commissaire de police d'origine bretonne se consacre aux affaires de terrorisme depuis son arrivée en 1984 à la Direction de la surveillance du territoire (ancêtre de la DGSI), maison dont il a gravi les échelons jusqu'au poste de directeur adjoint en 2007-2008. Il a aussi fait quelques incursions aux Renseignements

généraux, à l'ambassade de France à Londres et, surtout, de 2009 à 2012, à la Direction du renseignement de la DGSE, le service concurrent avec qui il a gardé de bonnes relations. Réputé pour son caractère discret et sa connaissance des dossiers, Patrick Calvar a enduré les attentats de 2015 comme autant d'échecs. Mais il garde la confiance du ministre de l'Intérieur, Bernard Cazeneuve, qui se repose sur ce bagarreur.

? Alex Younger (MI6), le diplomate au service de Sa Majesté

Un diplomate de haut vol, Alex Younger, 53 ans, dirige depuis fin 2014 le très fameux MI6, le service de renseignement extérieur britannique, connu également sous le nom de Secret Intelligence Service. La réputation du MI6 a été ternie par les informations biaisées sur les armes de destruction massive en Irak en 2002- 2003, base de l'engagement dans la guerre de Tony Blair aux côtés des Américains. Pour redorer son blason, l'ambassadeur John Sawers, en poste de 2009 à 2014, s'est évertué à fournir des renseignements plus étayés au gouvernement, que ce soit sur la Libye ou la Syrie. Son successeur Alex Younger - appelez-le «C» - est un habitué des postes difficiles: il a supervisé la sécurité des JO de Londres en 2012 et il a été ambassadeur au Moyen-Orient et en Afghanistan. Son profil s'apparente à celui du patron français de la DGSE, Bernard Bajolet, qu'il connaît bien.

? Robert Hannigan (GCHQ), le gardien des grandes oreilles britanniques

Diplomate, Robert Hannigan, 51 ans, est né dans le comté du Gloucestershire, non loin du siège du Government Communications Headquarters (GCHQ), qu'il pilote depuis avril 2014. Cette agence technique, qui emploie 6000 agents, est célèbre pour avoir déchiffré le code de cryptage des communications allemandes Enigma durant la guerre. Le GCHQ est le partenaire privilégié de la NSA depuis 1947, selon les termes d'un traité baptisé UKUSA, resté secret durant des décennies. Mis en cause par les révélations d'Edward Snowden en 2013, le GCHQ, alors dirigé par le très influent sir Iain Lobban, a défendu ses programmes de surveillance au nom de la lutte antiterroriste. Pour calmer le jeu, sir Iain Lobban a été prié de quitter ses fonctions après treize ans de règne. Son remplaçant n'est pas un amateur: ancien directeur au Foreign Office en charge de la défense et du renseignement, Robert Hannigan conseilla Tony Blair sur le processus de paix en Irlande du Nord, puis Gordon Brown sur les questions de sécurité nationale de 2007 à 2010. Un homme de confiance pour un poste stratégique.

? Michael Rogers (NSA), technologiquement vôtre

Réputé pour sa connaissance du renseignement et de la cyberguerre, l'amiral Michael Rogers, 56 ans, a succédé, en avril 2014, au tout-puissant général Keith Alexander, en poste depuis 2005. La National Security Agency (NSA), née en 1952, s'occupe pour les Américains de la collecte de renseignements électroniques dans le monde entier et de la cyberguerre, avec un budget annuel estimé à 10 milliards de dollars et plus de 20.000 employés. La NSA s'est retrouvée sous les feux des projecteurs avec la révélation, en 2013, par son ancien consultant Edward Snowden, de ses programmes de surveillance très intrusifs. Malgré le scandale, l'Administration Obama n'a guère limité les pouvoirs de la NSA, dont les commandes ont été confiées au moins controversé Michael Rogers.

? John Brennan (CIA), le cow-boy de Langley

Agé de 61 ans, John Brennan dirige depuis mars 2013 la Central Intelligence Agency (CIA), la plus connue des agences de renseignements américaines, dont le siège est installé à Langley,

en Virginie. Mais c'est un vieux routier de la maison, puisqu'il y a fait carrière durant vingt-cinq ans, avec notamment des postes en Arabie saoudite, à la division Proche-Orient, au contre-terrorisme et au sein de la direction. Passé dans le privé en 2005, il est devenu le conseiller du président Obama pour les affaires de sécurité intérieure et pour la lutte antiterroriste en 2008. Favorable aux techniques de torture pratiquées par la CIA sous le mandat de Bush, Brennan a soutenu les attaques de drones et les assassinats ciblés décidés par Obama.

? Alexandre Bortnikov (FSB), l'exécuteur de Poutine

Il ne fait jamais parler de lui. Pourtant, le général Alexandre Bortnikov est l'un des rouages essentiels du système de pouvoir de Vladimir Poutine. A la tête du service fédéral de sécurité (FSB) de la Fédération de Russie, ce militaire chevronné de 64 ans, entré au KGB en 1975, est en poste à la Loubianka, siège du FSB, depuis 2008. Héritier du KGB, le très redouté service de renseignement extérieur soviétique dissous en 1991, le FSB a repris la main progressivement, notamment en intervenant en Tchétchénie, en Géorgie, mais aussi en Syrie et en Ukraine. Soumis à une interdiction de visa par les Occidentaux, Alexandre Bortnikov a quand même pu se rendre à Washington début 2015 pour discuter de terrorisme avec le patron de la CIA. Aux côtés d'Alexandre Bortnikov, Vladimir Poutine, qui a dirigé le FSB de 1998 à 1999, s'est inquiété, en février dernier, des 4000 Russes partis faire le djihad en Syrie qui risquent de provoquer des attentats à leur retour. «Il faut les identifier et les neutraliser», a expliqué le président russe. Message reçu au FSB, qui n'hésite jamais, si besoin, à recourir aux exécutions.

? Yossi Cohen (MOSSAD), l'homme des secrets de Netanyahou

Surnommé «le modèle» à cause de son physique de playboy, Yossi Cohen, 54 ans, a été nommé en décembre 2015 à la tête du Mossad, le service de sécurité extérieure d'Israël. Proche du Premier ministre Benyamin Netanyahou, dont il fut le conseiller à la sécurité nationale, Yossi Cohen est issu de la droite religieuse. Vétéran du Mossad, il y a travaillé durant trente ans jusqu'à diriger l'ensemble de ses opérations à la tête du département Tzomet. A son actif: le sabotage partiel du programme nucléaire iranien, par des moyens allant de l'élimination de scientifiques à la destructions de matériels en passant par l'intrusion de virus informatiques ralentissant son développement. Nul doute que, malgré l'accord international sur le nucléaire iranien signé mi-2015, le pays des mollahs restera une de ses priorités, outre la surveillance de la Syrie voisine et des soubresauts de Daech.

? Bruno Kahl (BND), le verrouilleur de Merkel

Le **scandale** a fini par emporter Gerhard Schindler, le très secret patron du service fédéral de renseignement extérieur allemand, le Bundesnachrichtendienst (BND). Accusé d'avoir travaillé sans vergogne pour les Américains de la NSA, y compris en espionnant des Allemands, Gerhard Schindler a été démis de ses fonctions au printemps dernier. Pour le remplacer, la chancelière Angela Merkel a choisi un fidèle de son parti, Bruno Kahl. Agé de 54 ans, juriste de formation, il dirigeait le secteur public et les privatisations au ministère des Finances, tenu par son ami Wolfgang Schäuble. A lui de remettre de l'ordre au BND, en lien direct avec la chancelière, dans une maison de 6500 employés jugée opaque et incontrôlable.

Note(s) :

Mise à jour : 2016-08-19 08:51 UTC +02:00

Vanity Fair
How the Clinton campaign is foiling the Kremlin
Saturday, 27 August 2016
Byline: Nick Bilton

On May 17, as dusk was setting over Brooklyn, around a dozen employees from Hillary Clinton's campaign, and a consultant who worked with the Democratic National Committee, walked through the cavernous halls of the campaign's office headquarters, which tower over Cadman Plaza's expansive fields and the elegant federal buildings surrounding them. Through the halls, they wandered past endless posters adorned with blue "H"s bisected by red arrows and posters that proclaimed, "I'm with her." Eventually, they settled upon an empty conference room. As the Democratic staffers took their seats, they were joined by Marc Elias, the general counsel for Clinton's 2016 presidential campaign, and given a grave warning: from that point forward, they should avoid using one single word in their e-mails. That word, according to someone with intimate knowledge of the meeting, was one with which they were increasingly familiar: "Trump."

This meeting took place one month before the news would break that the D.N.C. had been hacked, allegedly by Russians, and two months before its controversial chairwoman, Debbie Wasserman Schultz, would resign after thousands of embarrassing e- mails were published on Wikileaks, including some suggesting her favoritism of the Clinton campaign over Bernie Sanders's operation.

According to reports, the D.N.C. was notified as far back as April that the organization's servers had been compromised. Consultants from the private security firm CrowdStrike were brought in at the time, but it wasn't until June that the hackers were kicked out of the server. In the intervening weeks, staffers were told, according to a person who works with the committee, that if anyone was going to communicate about Donald Trump over e-mail or text message, especially if those missives were even remotely contentious or disparaging, it was imperative that they do so using an application called Signal. In July, the trove of e-mails was posted to the Wikileaks Web site. (One of the most damning e-mails found in the D.N.C. archives, which focused on Sanders's religious beliefs, was sent on May 5, several days after the intrusion was allegedly discovered, and two weeks before staffers were told to use Signal.)

Signal, staffers in the meeting were told, was "Snowden-approved." A week after the meeting at the campaign headquarters, according to two people who have worked with the D.N.C. and the Clinton campaign, an e-mail was sent out instructing staffers where to download the app and how to use it. Shortly thereafter, the news broke that the D.N.C had been hacked. (Elias did not respond to e-mails and voicemails. A spokesman for the D.N.C. declined to comment, as did a spokesman for Hillary Clinton's campaign.)

The fear of what could lurk in people's e- mails has--particularly in the wake of the Sony hack and several hundred massive data breaches last year--left many Americans oscillating between a state of anxiety and one of resignation. People who use Web-based e-mail accounts have correspondences going back a decade or more, and text-message trails that reach back just as far. (Gmail was founded 12

years ago; Hotmail goes back 20 years.) Regarding the stuff in most people's digital archives, you essentially have two choices: either delete everything (and hope it is also deleted from the server) or leave it all, cross your fingers, and hope for the best.

"THERE ARE TWO KINDS OF COMPANIES OUT THERE. THOSE THAT HAVE BEEN HACKED, AND THOSE THAT DON'T KNOW THEY HAVE BEEN HACKED YET."

Moving forward, however, companies and organizations are urging people to use products like Signal, which is an encrypted message and voice app for smartphones, or other applications that feature self-destructing messages, such as Wickr, which vanquishes messages after they have been read. Some people take their correspondence to further extremes. I know journalists who now use burner phones to talk to sources (these are the smartphone of choice for drug dealers, cheating spouses, or those engaged in other nefarious things, as you've inevitably noticed on any number of HBO or Netflix series), and then get rid of the phone when they are done working on a story.

When Sony Pictures was hacked by a group that called themselves Guardians of Peace, in 2014, the public release of memos and correspondence led to a lot of embarrassment among executives, and eventually contributed to the resignation of co-chair Amy Pascal. At the time, I called around to people in Hollywood asking if the breaches had changed their behavior. Were they more sensitive, perhaps, about how they referred to mega-stars in e- mails, or even public figures, like the president? I was told that it wasn't that people were saying less disparaging things, but rather that they were now simply doing so in person or over the phone. "I've seen much, much worse," a well-known screenwriter told me at the time, and then noted, "Heck, I've sent much, much worse."

Gossiping about Hollywood industry professionals is one thing, but operating a campaign amid perhaps the most controversial election in history is another altogether. The Clinton campaign is right that the Signal app is Snowden-approved. Edward Snowden, who famously requires that people place their cell phones in a freezer before he agrees to meet with them in person (the freezer, or fridge, acts as a faraday cage and blocks any N.S.A.-like snooping of people's whereabouts), has touted the security of Signal numerous times, saying on Twitter, "I use Signal every day."

Other security experts I know speak just as highly of the service because it uses end-to-end encryption to secure all communications to other people on the app, which means that only the two people sending and receiving the message can see it. In other words, it's not hanging out on a server for Russian hackers to peruse. Even phone calls on Signal are allegedly safe. "We cannot hear your conversations, and no one else can either," the app says. "No exceptions." (If you really want to nerd-out, you can look online at the tech Signal uses. According to Wikipedia, "instant messages are encrypted with the Signal Protocol which combines the Double Ratchet Algorithm, prekeys, and a 3-DH handshake. It also uses Curve25519, AES-256, and HMAC-SHA256 as primitives"--whatever any of that stuff means.)

Signal also has a very clever solution to ensure that you know if the person you're speaking to is really them. For example, let's just say that I'm calling my editor, Jon, on Signal. His phone would ring, and

once he accepted the call, we would both be shown the same two words, like "spyglass pacific" or "nightbird undaunted." If both of us do not see the same matching words, then it means our phone call has been compromised.

Signal was founded by Moxie Marlinspike, who formerly oversaw security at Twitter, and is a member of the Anarchist Yacht Clubb (two Bs). If you mention his name in Silicon Valley, the response you'll inevitably hear (as I have many times) is that "Moxie is legit, and doesn't fuck around." Hence, why his app is the preferred choice for a clearly shaken and scared national political committee and an ex-N.S.A. operative exiled to Russia. But that doesn't mean that everyone is adhering to the rules laid out for them months ago. While the D.N.C. hack sent tremors down the spines of virtually everyone in Washington, it didn't take long for people to take the easy route, once again e-mailing sensitive information that could easily hamper the campaign if it ever became public. Or, as one Washington insider told me: "No one really learned."

There's a saying in the cyber-security world that goes something like this: "There are two kinds of companies out there. Those that have been hacked, and those that don't know they have been hacked yet." As we all parlay more and more of our communication to digital platforms that are as easy to use as they are to hack, it seems that mantra will soon start to apply to people, too. In the not-too-distant future, we might all start to worry about what could be lurking in not only our e- mails, but also every correspondence we've ever exchanged on a digital device--virtually ever.

Wall Street Journal
Bank Hackers Target Smartphones
Saturday, 27 August 2016
Byline: Robin Sidel

Washington - Hackers are using the growing popularity of mobile banking apps on smartphones to launch new types of attacks on big banks and their customers.
While it is difficult to quantify how much money has been stolen as a result of malicious software, or malware, on mobile phones, the trend is alarming the Federal Bureau of Investigation and U.S. banking regulators. The move by cyber thieves to target mobile banking apps has occurred amid a glut of stolen credit-card data for sale on underground websites.

Cyber thieves are using the malware to steal banking credentials from unsuspecting consumers when they log onto their bank accounts via their mobile phones, according to law enforcement officials and cybersecurity specialists.

Attacks have occurred on the two most common mobile operating systems -- Apple Inc.'s iOS and Alphabet Inc.'s Android. Phones typically come with built-in security protections, but the devices can still be vulnerable. On Thursday, Apple urged some iPhone users to update their software due to a security flaw that could allow a hacker to remotely take control of the operating system.

The problem for banks, which have stepped up spending on cybersecurity in recent years after several high-profile breaches, is that consumers often aren't as vigilant about security on their phones as they are on their desktop computers.

"As a bank, you can have all the protections you want, but unless there is protection on the device, you can't protect against this kind of attack," says Ross Hogan, global head of the fraud prevention division at Kaspersky Lab, a cybersecurity firm.

Also troubling is that the attacks can be hard to track down because thieves can access an account through any normal channel after they steal credentials through a phone.

The FBI is seeing new types of malware specifically aimed at banking applications for the purpose of stealing account credentials, says Richard Jacobs, an assistant special agent in charge who handles cybercrimes. He has been warning the financial-services industry about the trend, which is typically aimed at large banks.

The Federal Financial Institutions Examination Council, which brings together five banking regulatory bodies, in April updated its guidance for banks to include potential threats facing mobile financial services, including mobile-phone malware.

The malware often gets onto a phone when a user clicks on a text message from an unknown source or taps an advertisement on a website. Once installed, it lies dormant until the user opens a banking app.

The malware then creates a customized overlay on the authentic banking app. This allows criminals to follow a user's movements on the phone and eventually grab credentials to the account.

In some cases, the malware adds fields that request the customer's date of birth or Social Security number, says the FBI's Mr. Jacobs. Some of the more advanced forms of malware can even track verification codes that the bank may send to the customer in text messages as a secondary authentication, cybersecurity officials said.

Once the malware captures a phone user's banking credentials, it can send them remotely to the criminal, who can use them or sell them.

Bank executives say they are trying to thwart the malware by frequently updating and revising their banking applications.

They also say that the banks' security systems can often trigger alerts for unusual behavior, such as a large withdrawal or if the account is accessed from a previously-unknown device or an unfamiliar location. In such cases, the bank may require additional authentication from the user.

Malware that has gained popularity around the world among criminals have names like Acecard and GM Bot. Some of the bank- specific malware sells for as much as $15,000, according to people who are tracking the trend.

Ian Holmes, banking fraud solutions manager for analytics firm SAS, estimates that the Acecard malware has customized overlays to imitate 50 financial-services apps. The malware "is gaining credibility in the criminal underworld," said Mr. Holmes.

The growing threat represents a new entry point for criminals who typically steal bank credentials by other means, such as installing skimmers on automatic teller machines or by using scams targeting desktop computer users.

It is a setback for banks that are pushing customers toward digital channels as a way to reduce costs and improve efficiency. Banks typically reimburse customers for money stolen from their accounts, particularly if they notify the institution quickly after the theft occurs.

Kaspersky, the security firm, said in a recent report that banks may be underestimating the risk associated with the malware. "While the industry has so far been relatively unscathed by a major mobile banking security attack, the sophistication and levels of malicious activity on mobile solutions have begun to rise, which we believe increases the security risks of mobile banking," it said.

The rising popularity of mobile-banking malware also creates yet another security headache for consumers who are increasingly turning to their mobile phones for everyday tasks from banking to shopping.

The crimes can be difficult to track because customers might not notice thefts have occurred until well after they used their phones to log onto their accounts. Plus, customers are unlikely to consider a mobile phone as an entry point for hackers if the phone hasn't left their possession.

A recent study conducted by SAS and Javelin Strategy & Research found that fewer than one-third of smartphone owners use mobile antivirus or anti-malware software on their phones. Additionally, some mobile-phone owners unknowingly make their devices vulnerable to attacks when they tamper with operating systems in order to run unauthorized apps.

Guardian (London)
The police chief battling cybercriminals from Russia and Ukraine
Saturday, 27 August 2016
Byline: Patrick Collinson

London - Half of online fraud comes from abroad, says Ian Dyson, commissioner of the City of London police, who has enlisted the help of Google and Microsoft to fight it.

Last Christmas Ian Dyson got a call from his bank. Was he really in a Travelodge, ordering takeaway pizzas? No, was his answer, he was at home with his family. Like millions of others, Dyson had fallen victim to card fraudsters stealing from his account. But Dyson is not like everyone else - he is the commissioner of the City of London police, with the job of protecting not just London but the whole country from fraud. And the depressing reality is, like so many other frauds, the criminals got away with it.

Dyson is disarmingly honest about the explosion in online fraud and cybercrime, and what realistically the police can do about it. "Every month Action Fraud [the national fraud reporting service] receives 40,000 reports, half a million a year, and we know from the ONS stats that's only a small percentage of what is going on. There were 3.8 million frauds and two million cyber offences. You cannot enforce your way out of this. It's physically impossible."

It's partly because the perpetrators are abroad, with around half of all cybercrimes reported to Action Fraud originating overseas, says Dyson, citing Indian call centres and Russian and Ukrainian websites. The City of London police have a specialist officer permanently stationed in Wall Street, and worked with the Spanish police to swoop on 110 conmen operating a "boiler room" fraud targeting elderly investors.

But Russia? Do the London police receive any help from their counterparts in Moscow? "No, not at all. Ukraine is limited too. You'll be aware of the limitations of some foreign jurisdictions."

Another limitation is budgets. "Policing has taken a 20% hit in its budget so I've got to do what I can with what I've got," he says, while noting that virtually everyone else in the public sector has faced similar cuts.

"You have to be realistic with the volumes [of crimes] you've got, [and] about the global nature of the crime issue. I cannot possibly sit here and say I am going to investigate every crime. You can't. But policing has never investigated every crime."

The 40,000 reports to Action Fraud every month are whittled down to ones where the police think there are "actionable leads". Some go up to the National Crime Agency or the Serious Fraud Office, some are pushed out to the other 43 police forces across the UK, while the City of London police tackle the rest.

"There are 700 cases the City of London police are investigating at the moment. That's me rather than ones disseminated to other forces. In the top 10 there is about half a billion pounds worth of fraud being investigated."

What he dubs "CEO fraud" is the latest online crime wave City of London police are facing. It's when a junior person in the finance department of a big company receives an email from the chief executive officer of the firm, asking him or her to move money from one account to another. The email is fake; somehow the fraudsters have hijacked the boss's email account, or created one that is near identical.

There are 700 cases the City of London police are investigating at the moment

"One major company lost three lots of £250,000 this way," says Dyson, noting that the culture in some big businesses is such that junior staff are too nervous about confronting their bosses when they receive an email which appears to be from them.

Dyson notes that the other worrying online crime wave is "mandate fraud". You receive an email from your builder, who's doing your extension, politely telling you he has changed his bank account details, and could the next £20,000 payment for the extension go into this account? Again, the email has been hijacked, and the householder hands over their life savings - never to be seen again, as banks do not take responsibility. Guardian Money has highlighted numerous sad tales of how people have been conned this way.

Have online fraudsters caught the police napping? Did we put bobbies on the beat when we should have been investing in fighting online fraud? In a frank admission, Dyson says: "To be honest, who'd hold up a bank these days? Who would rob a bank now when you can make it all online in seconds?" His office is just yards from the Bank of England, yet about the only robberies he sees are of betting shops, one of the last major cash-handling businesses around.

He acknowledges that the public think that when they report an online crime, nothing seems to happen. "There is a public perception that PC Plod is losing the war against these highly sophisticated cybercriminals. It's a perception I'm trying to address.

"Last year 180,000 websites, phonelines and bank accounts involved in fraud were closed down following police intelligence. So disruption is a big thing... Your report, combined with hundreds of others could lead us to close down that website and prevent people from becoming victims of fraud. While you might not get your money back, it will go at least some way to stopping others [from being a victim]."

Disruption is a word Dyson uses a lot. He reckons the best approach for his force is to gain intelligence from the public and other government agencies, and use that to intervene before more victims are conned. It's why he's investing heavily in a new IBM project for Action Fraud that should turn it into the world's most sophisticated anti-fraud intelligence system in the world. The quicker the police can see the signs, the more rapidly they are able to respond, he says.

But the public have to do more: "The public have to shift their mindset around crime. The public have to understand we cannot enforce our way out of this, [given] the volume of crime, the fact that it is global and happening so fast, and that money can be moved so quickly. It has to be about prevention and protection."

Don't use "password" as your password, he says. If that email arrives asking you to pay the money into another account, ring the builder, he adds. There are many, many more simple measures the public can take, he insists. In September, the government will begin a public information campaign, which Dyson says will evoke the message of the 1970s "clunk-click, every trip" campaign to get the public to use seatbelts in cars. We need the same thinking when it comes to transacting online, he says.

But shouldn't the banks be doing more? Can the public really protect themselves from genius hackers determined to break into their accounts?

Dyson is reluctant to criticise the big banks, though he says insurance companies have a much better record than high-street banks at cooperating in fighting fraud. The insurers have paid for 35 police officers in the City of London force alone to battle fake insurance claims and have had a string of prosecution successes.

He would like the banks to be rather more intelligent when an elderly customer walks into a branch and demands to withdraw nearly all their savings when they have never taken out more than £100 before in one go. It's usually because they are being conned.

Banks may often fail to report a fraud, in part because of the odd way in which crime is recorded. When Dyson's own card details were stolen, he was fully compensated by the bank. That means, according to Home Office rules, that the bank was the victim of the crime, not Dyson. "It's something we are talking to the Home Office about," he says.

Critics say that police fraud-busters are just not technically competent and resourced to catch cybercriminals. Dyson bridles: "I'd like to disabuse anyone of the view that they are all smart computer geeks, the archetypal spotted teenager hacking into US military computers. They are not. You have some people who are business people who before the internet would have been conning people out of investments. They are doing the same now but are doing it online. Then you have the people with a slightly smarter mate who have found a quick way to make money."

The boiler room criminals in Spain are the type who were breaking into cars before the advent of the internet, he says. But in 33 years of policing, he says criminals are changing. They used to specialise in a line of business - armed robberies, drug dealing, etc. Now, Dyson says, everybody tries a bit of everything.

Meanwhile, the police have their own geeks. Dyson says the City of London force have staff seconded to them from Google and Microsoft whose internet expertise is a match for any cybercriminal in Russia: "My guys will understand the forensic footprint of these crimes in the same way detectives are aware of forensic opportunities at the scene of a burglary."

He is proud of his force's work to fend off pension fraud, which was widely expected to balloon in the wake of the new pension freedoms, but has so far been suppressed by the police working with the

pension providers. The force was also instrumental in stopping BT from keeping lines open after a phone is put down, a frequent tactic used by fraudsters to convince people who called back that they were speaking to their bank.

More money would help, Dyson says. For every pound invested in fighting fraud "we are preventing about £60 worth of fraud". Meanwhile he's behind a pilot project in which private law firms will be hired by police to help seize the proceeds of crime and repay victims earlier.

"We're an innovative police force," he says. "The investment in the last 10 years was in neighbourhood policing and the visibility of police officers. We are shifting, in fairness, policing is shifting to deal with online."

Unfortunately, as he looks out of his offices over the towers of London, while fighting fraud fills much of his time, there is another more serious threat. "My number one priority at the moment is counter-terrorism. We are quite a target-rich environment."

How to protect yourself

There were more than 5.8m incidents of cybercrime in the past year, enough to nearly double the headline crime rate in England and Wales, writes Patrick Collinson.

The Office for National Statistics said last month that one in 10 adults have been victims of cybercrime and online fraud over the previous year in the first official estimate of the scale of scams, virus attacks, thefts of bank details and other offences. An initial ONS estimate in October last year put the annual figure at 3.8m, or 40% of all crimes.

Costing an estimated £193bn a year, cybercrime is nearly as big as all other crime, such as home burglary, car thefts and violence against the person. The ONS added that the chance of being a victim is the same regardless of social class or whether you live in a deprived or affluent, urban or rural area.

Meanwhile, the figures for crime excluding online offences dropped in the year, falling by 6%. The long-term trends in traditional crimes such as burglary, car thefts and criminal damage showed that the fall in crime since its 1995 peak had slowed down since 2005. The survey found there had been no change in the overall level of violent crime compared with the previous year.

So what are the easy steps to protect yourself from online crime that Commissioner Ian Dyson recommends?

. Never disclose security details, such as your pin or full banking password

Banks and other trusted organisations will never ask you for these in an email, on the phone, by text or in writing. Before you share anything with anyone, pause to consider what you're being asked for and

question why they need it. Unless you're 100% sure who you're talking to, don't disclose any personal or financial details.

. Don't assume an email or phone call is authentic

Just because someone knows your basic details (name and address, even your mother's maiden name), it doesn't mean they are genuine. Fraudsters may try to trick you and gain your confidence by telling you that you've been a victim of fraud. Fraudsters can also make any telephone number appear on your handset, so even if you recognise the number or it seems authentic, do not assume they are genuine.

. Don't be pressured into a decision

Under no circumstances would a bank or organisation force you to make a financial transaction on the spot; they would never ask you to transfer money into another account for fraud reasons.

. Listen to your instincts

If something feels wrong, it is usually right to question it. Fraudsters may lull you into a false sense of security when you are out and about or rely on your defences being down when you're in the comfort of your own home. They may appear trustworthy, but they may not be who they claim to be.

. Stay in control

Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel embarrassed when faced with complex conversations, but it's OK to stop the discussion if you do not feel in control of it.

The Guardian (London)
Burglars aren't the problem, we need to catch Russian cybercriminals
Saturday, 27 August 2016
Byline: Patrick Collinson

London - Just how defeatist are our police over online crime? The top fraud crime fighter in the country, City of London Police commissioner Ian Dyson, won't agree with that, but he certainly talks down the possibility of arrests and convictions. There's a bluntness to his assessment that won't, perhaps, go down too well with the Foreign Office. Crooks in Russia and Ukraine are behind much of it, he says, and law enforcement there won't cooperate with the British.
It's a common saying that you can't put a policeman on every street corner, and we certainly can't put one on Kreschatik Street or Old Arbat. But arguably our problem is that we tried to put too many bobbies on the beat, with the vogue for neighbourhood policing skewing resources to threats, such as home burglary and car theft, that have actually been in steep decline.

One sound that always greets me when I return to London from abroad is police sirens. New York and Paris are no match for the hyper-visibility and siren volumes of police here, but given the decline in traditional crime (even the terrorism death tolls are lower than in the 1980s) then it's time to assess whether we need to switch priorities.

The volume of cybercrime now matches the number of traditional crimes, and its estimated £193bn cost is far in excess of the value of physical goods nicked from homes, cars and workplaces. Yet we devote relatively few resources to fighting it. The City of London police force's budget is around £120m a year, yet it is the country's lead force on fraud - and also has the not-insignificant duty to protect the likes of St Paul's, the Tower of London and other high-value targets from terrorism. The commissioner reckons that each £1 spent on fighting fraud prevents around £60 in online theft; even if the reality is that it's only half that, then it's still one hell of a return.

More money could go into prevention and disruption, where Dyson thinks the returns are best. My guess is that the public would prefer to see many more arrests and convictions. If crooks think the worst that could happen is their website being prematurely shut down, then it's hardly much of a deterrent.

Dyson was determinedly uncritical of the banks when I interviewed him. Yet the banks can't escape the fact that they are the getaway car when it comes to online crime. Without online banking, the money simply can't be stolen or lured out of your account and into the scammer's account.

The banks save a colossal sum from shutting their branch networks (eventually they will nearly all go) and making us do the work the bank tellers used to do. We firmly believe that one reform - forcing sort codes and account numbers to be matched with individual names - will go some way to halting a number of frauds. But Dyson doesn't share our belief that this will change much.

A second reform requires consent as much from the public as from the banks. The "faster payments" system - transferring money instantly - opened up a gold mine for fraudsters. We all like the speed and convenience, but it means there is no time for second thoughts. So often here on Money we hear stories from fraud victims who say they were not quite sure what was going on, and it was a day (or even hours) later when they tried try to block the transaction. But too late, the money had been looted. There is a strong argument for three-day clearance on transfers to new payees, say for sums above £250. And would it be that onerous if all transfers above £1,000 took a day or so to clear?

CBC.CA
Hacker targets remote northern Alberta communities
Sunday, 28 August 2016
Byline: Zoe Todd

Edmonton - A northern Alberta municipality is in emergency mode after a suspected computer hack.

The Municipal District of the Opportunity No. 17 is concerned all its files were accessed, including personal and financial information, according to a public notice released by the municipality.

Administrative staff say they first became aware of "suspicious activity" in July. Last Friday, the activity escalated.

"We just unplugged everything and cut ourselves off from the outside world," said Deborah Juch, the municipality's manager of legislative services.

About 3,400 people live in its seven hamlets, about 400 km north of Edmonton. Many residents log personal information with the municipality, such as social insurance numbers, credit card numbers and payroll bank deposit card numbers.

Juch cited money as the most likely motive for hackers.

"We're working in emergency mode," she said. "The northern municipalities have a large amount of tax dollars coming and going through their accounts."

The district's sole information technology veteran worked a 22-hour shift to protect the municipality's servers and network. But someone continued to undo his efforts, Juch said.

"We were not going to be able to stop whatever was trying to get in the door," she said. "We ordered an unplug."

The municipality has reported the problem to the RCMP, and has now flown in what Juch described as a team of "high-power IT people" to work on the server.

She said the network should be restored within two weeks, at which point the municipality will know how much information has been accessed.

New Strait Times
Military forms cyber defence unit
Monday, 29 August 2016
Byline: Nur Aqidah Azizi

Kuala Pilah - A cyber defence unit has been set up to prevent the leak of the country's confidential and sensitive data.
Defence Minister Datuk Seri Hishammuddin Hussein said the unit was formed last year under the Royal Intelligence Corps in the armed forces.

"This unit is different from the cyber security unit under the Home Ministry. It serves to defend and protect the country from cyberattacks. It also protects confidential data and information on assets from being leaked to irresponsible parties."

Hishammudddin, who is also Umno vice-president, said the formation of the unit was crucial, especially following the alleged leak of secret documents from French shipbuilding company DCNS recently.

"We should learn from this. This is a wake-up call for all countries to tighten and improve security defence. "The world is changing rapidly and it will be hard to avoid such situations if we are not prepared.

"Since last year, we have worked closely with other countries to prevent any leak of the country's confidential information," he said after officiating the Kuala Pilah Umno division delegates' meeting at Dato Bahaman Hall here yesterday.

On the Scorpene-class submarines, Hishammuddin said the vessels Malaysia owned were not affected by the documents that were allegedly leaked from DCNS.

"The leak of classified information only involved the Indian Navy's six new Scorpene-class submarines.

"Navy chief Admiral Tan Sri Ahmad Kamarulzaman Ahmad Badaruddin has made it clear that our submarines were built with different specifications than those of other countries.

"We are confident that this issue won't affect the operations and capabilities of Malaysia's submarines."

He said the Defence Ministry had launched an investigation into the alleged leak of information related to the Scorpene-class submarines. "We will investigate this matter thoroughly."

A report in The Australian on the leak of secret documents from DCNS was published recently.

Some 22,400 pages of documents detailing the capabilities of the Scorpene- class submarines the company designed for the Indian Navy were allegedly leaked.

The discovery of the alleged leak raised fears about the future security of top-secret data of the Indian Navy's future fleet.

A variant of the same French-designed submarine is used by the Navy of various countries, including Malaysia.

Tehran Times

Iran detects malware in petrochemical plants, rejects link to recent fires

Monday, 29 August 2016

Tehran - Head of Iran's civilian defense said on Saturday that the country has detected and removed malicious software from its petrochemical units, rejecting links to recent fires in some of the country's petrochemical facilities, Mehr reported.
"Necessary defensive measures were taken" after the malware was detected and removed, according to brigadier general Gholam-Reza Jalali.

Over the past two months, a number of Iran's petrochemical units, including Imam Khomeini as the biggest one, stopped operating wholly or partially due to fires. The issue is still being probed by Iranian officials and expert teams. Initial informal speculations linked the fires to cyber-attacks.

Last week, Iran's National Cyberspace Council announced that it was investigating whether the recent fires triggered in petrochemical plants were caused by a cyber attack. Following the investigations, Jalali said while the malicious software affected two petrochemical complexes, it did not play a role in the recent fires because it was inactive at the time.

According to the official, the malware packages petrochemical units had purchased from abroad were to blame. "Investigations indicated that the industrial software packages, bought from foreign countries, were already corrupted," he added. Iran has been increasingly afflicted with the threat of cyber attacks by foreign countries.

Learning from the cyber attack by the U.S. and Israel on its nuclear facilities in 2009, what came to be known as Stuxnet virus, the country has been upgrading its cyber security capabilities in recent years, developing homegrown firewalls for its sensitive facilities, including nuclear, military, and economy sites.

Haaretz
Sophisticated Tracker Program' That Wormed Into Apple
Monday, 29 August 2016
Byline: Yisrael Fischer and Ruti Levy

Jerusalem - On August 10, Ahmed Mansoor, a human rights activist in the United Arab Emirates, received a text message that invited him to click on a link that would reveal new information about torture in jails in his country.
Mansoor, who has been a repeated target of the regime, grew suspicious and turned over the message to researchers from Citizen Lab.

Mansoor's gut feeling was right. The link would not have led him to information on torture but rather would have taken advantage of three flaws that Apple was not aware of to surreptitiously hack his iPhone, turning it into the perfect spying device.

The researchers discovered that the malware enabled recording conversations, accessing photos, text messages and geographic location, and control of the phone such as remotely operating the camera or loudspeaker. The program was connected to 200 different servers, some of them leading to a Herzliya-based company called NSO Group and to software it developed called Pegasus.

Lookout, a company involved in discovering how NSO's malware operates, was impressedy. "It's the most sophisticated tracking software we have encountered, that completely takes over the device with just one click of a link," one person at the company said.

Lookout said another advantage was the company's ability to maintain secrecy: Pegasus hacks the device without its owner being able to detect its existence, and can only be detected by a lab.

For the past six years, almost all global technology companies have offered hefty cash prizes to hackers who could detect bugs in their systems and warn them - save for Apple. Its iOS platform is considered particularly secure and many people handling sensitive data choose Apple products for this reason. Apple's announcement over the weekend about an urgent software update due to security problems showed that the company finally realized that no one is safe in the new spying age.

Omri Lavie, Shalev Hulio and Niv Carmi founded NSO in 2009, naming it from the initials of their first names. Carmi left shortly thereafter over disagreements with his partners. Meanwhile, a group of investors, headed by Eddy Shalev, a founding partner of Genesis Partners, took a 30% the company for just $1.8 million. When Francisco Partners, a California private equity firm, bought NSO in 2014 they bought it for $130 million. Reuters reported last year that the fund was looking to sell NSO for $1 billion.

NSO, based in Herzliya Pituah, employs 200 people, more than twice as many as two years ago. NSO's annual revenue is estimated at $100 million.

"We insisted that all intellectual property remains in Israel, that the development center remains in Herzliya and not move to Silicon Valley or anywhere else outside Israel," Hulio, the CEO, wrote on Facebook after the acquisition.

NSO's asserts that the technology is meant to help fight crime and terror. "The company develops products to help governments fight crime and terror. The company only sells to authorized government bodies, subject to all security export laws," the company said in a statement.

It also stressed that it sells the technology but doesn't operate the systems for its customers. "The contracts signed with clients require strictly legal use of the technology, only for investigating and preventing crime and terror."

But its Pegasus product may have been put to unauthorized uses. Israeli media reported in 2012 that Pegasus was sold to the Mexican government for $15.5 million to help it fight the country's drug cartel.

But The New York Times said last week that the software was also used to spy on Rafael Cabrera, a Mexican journalist who uncovered conflicts of interests among the country's ruling family.

In other cases, according to the report, NSO's tools were adapted for use against targets in Yemen, Turkey, Mozambique, Kenya and the United Arab Emirates.

The Israeli government regards its tracking software as no less than a weapon, whose exports are supervised by the Defense Ministry. The ministry lets NSO sell the software only to countries with good relations with Israel and not to businesses.

Israel is a star of the global interception and tracking industry. According to Bloomberg, there are some 230 companies, prominent among them being Israeli Verint, European Nokia-Siemens, French QOSMOS and Amesys, American Blue Coat and SS8, Italian Hacking Team and British Gamma.

Other prominent Israeli companies are Alut, Cellebrite and Elta, as well as Israeli-American Narus, which Lockheed Martin acquired. Israeli company Nice Systems last year exited the defense market, which generated limited profitability for it and unflattering headlines about problematic regimes using its products.

Lavie and Hulio, 35, have been starting up companies since their high school days in Haifa.

Hulio served six years in the army, half in intelligence and later as a search-and-rescue commander. In reserve duty, he has joined all of Israel's overseas rescue missions in recent years, including in Nepal, Haiti and Turkey.

Lavie served in artillery before studying business administration at the University of Haifa, while Hulio started studying law at Herzliya's Interdisciplinary Center. But they both dropped out in favor of entrepreneurship.

They founded their first startup, MediAnd, which helps viewers locate and buy items appearing on the screen, in 2007. It closed after three years, ending in a court case with the third founder, Yael Lerner Levy.

They founded their second startup, CommuniTake, a year later to help cellular operators remotely identify problems and support. The two left it following disputes with their cofounders and then founded NSO.

In 2013 they teamed up with Avi Rosen, the former vice president for development at Cyota, Education Minister Naftali Bennett's security information company that was sold to RSA for $145 million in 2005. The three founded Kaymera Technologies, which develops cellular security solutions, in other words security from spyware like NSO's.

"Anybody who sees the capability of NSO systems immediately thinks of ways to protect themselves against similar capabilities," Rosen, Kaymera's CEO, told Bloomberg in 2014.

Kaymera has developed secure smartphones for governments and private customers worldwide, with annual sales estimated at $15 million. The company has raised $13 million, $10 million of that in February. Its investors include Hong Kong-based GOEC Go Capital Ventures and Israeli angels Yariv Gilat and Eddy Shalev, who has accompanied the entrepreneurs the entire way.

Kaymera is located in Herzliya Pituah, in the same building as NSO. However, the company asserts Hulio and Lavie are not involved in Kaymera's daily operations.

Fars News Agency
AEOI Launches 2nd Cybersecurity Network Center at Arak N. Facilities
Monday, 29 August 2016

Tehran - Iran has launched a second cybersecurity network center at the country's nuclear facilities near the Central city of Arak, a senior advisor to the head of the Atomic Energy Organization of Iran (AEOI) said on Sunday.
Asqar Zare'an made the remarks in the Central city of Isfahan, addressing a ceremony to pre-launch a semi-industrial unit to produce the raw materials for the production of stable isotopes.

"We are happy that today we could pre-launch the semi-industrial unit to produce the raw materials for stable isotopes at Isfahan's UCF center," he said.

"Before this, the know-how and capability to produce stable isotopes were monopolized by a few countries, including the US, Russia and Germany," Zare'an added.

Iranian Foreign Ministry's Director General for Political Affairs and International Security Hamid Baeedinejad underlined in June the country's plans to further expand its nuclear industry despite powers' attempts to prevent it.

Iran's nuclear industry will never be shut down nor will it be subjected to restrictions, but it will make further progress day after day, Baeedinejad said.

He added that despite attempts by the world powers, led by the US, Iran's nuclear industry will continue to prosper.

While they sought to shut down Arak heavy water plant, now the US and Russia are main customers of Iran's heavy water, Baeedinejad said.

Fars News Agency
Iran Unveils National Data Network's Phase 1
Monday, 29 August 2016

Tehran - Iran unveiled the first phase of its National Data Network project on Sunday. Iranian First Vice President Eshaq Jahangiri and Minister of Communications and Information Technology Mahmoud Vaezi attended the unveiling ceremony.
The main purpose of the network is to help Iranian users to use the capacities of the network systems for communication purposes anytime and anywhere, while enhancing security of Iranian operaters' data.

Earlier this year, Head of Iran's Information Technology Organization Nasrollah Jahangard had said that national network means having a network across Iran which could provide services under Iran's security, management and control. "The network cannot be attacked at all," Jahangard said.

Last week, Iranian Minister of Communications and Information Technology Mahmoud Vaezi underlined that several international mobile operators have voiced their willingness to invest in Iran's telecommunication projects.

"Iran Connect 2016' conference would be an economic and technical forum in which the major operators will get acquainted with Iran's ICT capabilities," Vaezi said.

He said that international mobile operators have already welcomed taking part in the upcoming Iran-Connect Conference in Tehran.

Iran's Telecommunication Infrastructure Company (TIC) will host the conference on in Tehran on September 6-7.

Vaezi reiterated that the government is interested in cooperation between domestic and foreign private companies.

The Daily Beast
FBI vs. State Department Over Hillary Clinton's Secrets
Monday, 29 August 2016
Byline: Shane Harris

Washington - The FBI and the State Department are at odds over whether Hillary Clinton's personal lawyers had the proper government-issued security clearances that they needed to keep copies of her emails in a Washington, DC, law office last year.
Some of those emails contained classified information, which the lawyers and State Department officials knew at the time.

The issue has become a flashpoint in the broader controversy over Clinton's private email server. Republican lawmakers are pressing the FBI on whether it investigated the State Department's decision to give security clearances to Clinton's attorneys and let them store copies of the emails on a thumb drive. And statements from FBI and State Department officials show that there's no clear agreement on whether Clinton's attorneys were appropriately cleared to handle the material.

In July, FBI Director James Comey testified before the House Oversight and Government Reform that Clinton's attorneys didn't have the security clearances they needed. The FBI elaborated in a statement this week to The Daily Beast, saying "most of the attorneys representing former Secretary of State Clinton in this matter did not have the appropriate security clearances to review special access program material," which is highly secret information that is restricted only to a few people based on their need to know.

Seven email chains, which included messages sent and received by Clinton, contained such material, the FBI found.

The bureau didn't specify which lawyers didn't have the right clearances, but Clinton has been represented by at least two lawyers in matters related to her email, including her longtime personal attorney, David Kendall, of Williams & Connolly, and his colleague, Katherine Turner.

Kendall, who has previously said he and Turner hold a top secret clearance from the State Department, didn't respond to a request for comment.

But the State Department says Clinton was represented by appropriately cleared lawyers. A department spokesperson defended the decision in 2015 to let the attorneys keep the thumb drive in a government-issue safe, which department security officers provided after visiting Williams & Connolly's offices. At the time, Clinton's lawyers said they needed a full record of the emails in order to respond to questions from the House committee investigating the Benghazi, Libya, terrorist attacks, which happened on Clinton's watch.

"It's routine for individuals outside government to have temporary security clearances to work on a range of issues," State Department spokesperson Elizabeth Trudeau told The Daily Beast. "This includes legal representatives who may need it to better represent their clients appropriately. The Department does not confirm individuals' security clearance status, however, as we have confirmed in the past, former Secretary Clinton has counsel with clearance."

While Clinton's lawyers won't face any criminal prosecution over the issue, legal and security experts say giving them access to classified emails in their own offices was an unorthodox decision that appeared to give preferential treatment to the former secretary of state. Keeping classified information stored outside a government facility increases the possibility that it could be seen or stolen by people who aren't authorized to have it.

Rep. Jason Chaffetz, the chairman of the powerful House Oversight Committee, held Clinton personally responsible for the matter.

"Hillary Clinton gave her private attorneys, without proper security clearance, access to classified information. This once again illustrates Secretary Clinton's cavalier and sloppy behavior in handling highly sensitive information," Chaffetz told The Daily Beast. Earlier this week, Chaffetz asked Comey in writing whether law enforcement officials had "investigated the possibility that Secretary Clinton's classified emails were improperly stored or accessed" either by her "personal representatives" or her attorneys.

The issue is complicated by the fact that not all classified government information is treated the same. There are three ascending levels of classification: confidential, secret, and top secret. Clinton's emails contained information in all three categories.

But her lawyers learned about classified information in the emails at different times. First, they were informed in May 2015 by the State Department that at least one email contained "secret" information. At the time, State decided to install the safe at Williams & Connolly's offices.

Then, in June 2015, the State Department told the lawyers that 25 emails contained "confidential" information. That's a lower level than secret, and department security officers had determined that the safe and the law office were appropriate for handling information up to the secret level.

But in July, the inspectors general for the State Department and the intelligence community said they'd found four emails that contained information derived from intelligence agencies. That signaled that the emails could contain information from the most highly-classified category, and the law offices weren't set up to handle those sensitive secrets.

"We knew nothing about the clearances for counsel or for the law firm," Charles McCullough, the inspector general for the intelligence agencies, told Congress last month. "I was facing a situation where I had classified information, it appeared to me, outside the care, custody, and control of the U.S. government."

After the inspectors general discovered the classified information, intelligence agencies and the State Department would spend the next several months arguing over precisely how many of Clinton's emails contained which category of secrets. And internal emails obtained by The Daily Beast under the Freedom of Information Act show that in late July and early August of 2015, State Department lawyers were trying to determine whether attorneys representing Clinton had the clearances they needed.

The question was pressing enough that a State Department legal adviser sent several emails marked "URGENT" to the security officers who had been in charge of vetting Clinton's attorneys' offices and setting up the safe.

"Do any of the attorneys have TS [top secret] clearances," the adviser, Sarah Prosser, wrote, apparently not knowing the answer. The replies from her colleagues are heavily redacted, but the exchanges make clear that State's attorneys tried to sort out the issue at a critical time.

On the same day Prosser sent the message, the FBI took possession of the thumb drive from Clinton's lawyers. They would no longer be allowed to keep the emails in their office.

In its statement to The Daily Beast, the FBI seemed to absolve Clinton's attorneys of any responsibility for knowing what was in the emails. "The FBI does not believe the lawyers knew, or should have known at the time, that there was classified information in her emails," the statement read.

But clearly the lawyers did know that the emails contained confidential and secret information, because they were told so by State Department officials. Asked to clarify which levels of classification the lawyers did or didn't know about, an FBI spokesperson declined further comment.

But in the end, it was the responsibility of the State Department to ensure that the lawyers were properly vetted and their firm was prepared to handle classified information. And, the department says, its staff did just that.

The decision to give the attorneys a safe was approved by the State Department's Diplomatic Security Bureau, "taking into account all relevant factors including security clearances and access controls," Trudeau said. State also provided "instructions for how to secure the material (up to the Secret level of classification)," the second-highest of the three basic classification levels the government uses.

"Through a physical security expert, we confirmed that they were taking those measures," Trudeau continued. "The Department also informed counsel that additional steps would be required if the Department determined the material contained more highly classified information."

That ultimately proved unnecessary because the FBI came in August and took the thumb drive. At the time, investigators also seized Clinton's private server. In going through those records, investigators determined that Clinton's lawyers hadn't actually read all her emails when they tried to sort out which ones were work-related--the ones that ended up on the thumb drive--and which ones were personal. The lawyers deleted those.

Last week, the FBI revealed that investigators have found another 15,000 emails that Clinton's attorneys never turned over. It's not clear how many of those involved official communications, and the FBI has said there's no evidence the lawyers intentionally withheld the messages. But the revelation has only added to Republican suspicions that Clinton--and her attorneys--haven't told the full story about her email.

USA Today
Spyware firm linked to hack of iPhone has strong ties to U.S.
Monday, 29 August 2016
Byline: Elizabeth Weise

Washington - The spyware firm tied to an iPhone hack that prompted an emergency patch this week by Apple keeps a very low profile. But the NSO Group has strong ties here as well as in Israel, where it's staffed by specialists from Israel's military cyber division.
One of its recent owners, U.S. private equity firm Francisco Partners, operates from an office complex in San Francisco's leafy Presidio district that's also home to Lucasfilm and Industrial Light & Magic.

In Herzelia, an area of near Tel Aviv with a thriving tech culture, NSO was founded by Shalev Hulio and Omri Lavie in 2009, according to Hulio and Lavie's LinkedIn pages. Several of its employees previously worked for United 8200, the Israeli Army's cyber division, which produces spying software.

The tech company's background, pieced together from industry reports, reflects the growing boom in cybersecurity firms that operate in a nebulous area: creating software and processes that break into encrypted devices for government entities.

Company 'gotten caught'

NSO is described as "a leader in the field of cyber warfare," according to an apparent company brochure posted online by Privacy International.

The company uses "a powerful and unique monitoring tool, called Pegasus, which allows remote and stealth monitoring and full data extraction from remote target devices via untraceable commands," the brochure says.

While these hacks can be legal, they raise severe privacy worries from consumer groups. They also highlight concerns that increasingly rigorous encryption from Apple and other consumer tech companies is vulnerable to attacks funded by deep-pocked entities.

"What most people don't understand about espionage these days is just how dramatically sophisticated the technologies to conduct this kind of intelligence gathering have become," said Michael McFaul, director of the Freeman Spogli Institute for International Studies at Stanford University and the former U.S. ambassador to Russia.

Cybersecurity firms that can thwart encryption shot into the spotlight earlier this year when the FBI hired an unnamed private contractor to help it hack into the contents of the iPhone used by one of the San Bernardino shooters. The successful hack allowed the U.S. government to shelve a contentious fight with Apple, which did not want to provide a software override to its mobile operating system.

The NSO Group is rare "because it's one company that's gotten caught," said Eva Galperin, a global policy analyst with the Electronic Frontier Foundation, a digital rights group in San Francisco. "There's still a lot of light to be shed on this world," she said.

Its involvement, according to researchers who published findings on the spyware and notified Apple, was traced to the software's coding.

Suspicious text sent

Ahmed Mansoor, a prominent human rights activist in the United Arab Emirates, told University of Toronto's Citizen Lab he was sent a suspicious SMS link. Working with mobile security firm Lookout, Citizen Lab said the link carried a powerful, rare form of spyware that could have cost as much as $1 million. If Mansoor had clicked on it, it would have given the sender the ability to control his phone's camera and microphone, track his movements and rifle through all his apps, files and contacts, they said.

NSO Group spokesman Zamir Dahbash would not confirm or deny involvement in the Mansoor spyware. He said: "NSO's mission is to help make the world a safer place, by providing authorized governments with technology that helps them combat terror and crime."

Apple said it immediately fixed the vulnerability upon learning of it. On Thursday it advised customers to download the latest version of its iOS, version 9.3.5, for security protection.

Citizen Lab's John Scott-Railton said a likely suspect for the attempted attack was the United Arab Emirates, where Mansoor is seen as a dissident. He has been unable to leave the country since 2011 after his passport was taken. A representative for the UAE did not return a request for comment.

NSO Group has an extremely low profile. The company does not have a Web page. On its LinkedIn page, it is described as working "in the field of Internet security software solutions and security research." No contact information is listed.

NSO is U.S. owned

In 2014, Francisco Partners bought a majority stake. The private equity company, founded by West Coast investment banking pioneer Sanford Robertson and run by former Texas Pacific Group investor Dipanjan Deb, did not respond to requests for comment. Among its 75 portfolio companies, it does not list NSO as an investment.

According to a Reuters report last year, NSO Group had annual earnings of around $75 million.

If the software was produced, sold and used outside of the U.S., there would be no U.S. jurisdiction over it, said Robert Cattanach, a partner at Dorsey & Whiney who specializes in cyber security law. If it had

been used inside of the U.S., the Computer Fraud and Abuse Act would apply, but that doesn't appear to have happened here, he said.

Some say the availability of software is at least partly due to technology firms' reluctance to provide a back door to law enforcement.

"We are going to continue to see law enforcement agencies buying 'hacking tools,'" said Chris Hoofnagle, a professor of cyber crime law at the University of California- Berkeley.

Wall Street Journal
U.S. Revamps Line of Attack in Social-Media Fight Against Islamic State
Monday, 29 August 2016
Byline: Nicole Hong

New York - Recent initiatives by technology companies to push back against Islamic State's social-media messaging highlight a sobering fact: The U.S. government's battle on that front has mostly sputtered. In a number of terrorist attacks over the past year, the attackers were found to have been inspired by Islamic State propaganda and videos, which are often described as Hollywood-level productions. Despite numerous military victories against Islamic State, U.S. officials acknowledge they have struggled to counteract the terrorist group's online campaign.

"We were able to disrupt networks, arrest terrorist cells, kill terror operatives," said Ali Soufan, a former Federal Bureau of Investigation counterterrorism agent who now runs a security consulting firm, the Soufan Group. But "we haven't been doing a great job in countering the ideology."

Since early 2014, approximately 100 individuals have been arrested in the U.S. on charges related to providing support to Islamic State. In 69% of the cases, officials found the individuals had watched or read the group's electronic dispatches, according to a report released last month by Fordham University's Center on National Security.

The government's countermessaging efforts so far have been scattershot and, some close to the government think, largely ineffective. Officials say the government's new strategy is to empower third parties to create their own messages, a contrast from earlier efforts that were criticized for having too much direct government involvement.

One of the government's earliest messaging campaigns against Islamic State began in 2013 with a Twitter account run by the State Department called "Think Again Turn Away," which aimed to dissuade people interested in joining the terrorist group. But the account would often tweet directly at pro-Islamic State accounts, sparking back-and-forths on Twitter that drew more attention to the voices of individual jihadists, critics said.

People looking to view the account's tweets are now redirected to the account for the Global Engagement Center, a new State Department initiative created this year to combat Islamic State messaging. Unlike the previous effort, the center aims to reduce the government's direct engagement online, especially in English, which officials saw as ineffective.

There are some encouraging signs. Since June 2014, there has been a 45% drop in pro-Islamic State tweets, said U.S. officials, citing data analytics technology that tracks Islamic State's presence on social media. It's unclear, however, whether the drop in tweets has resulted in fewer foreign fighters wanting to join the terrorist group. Islamic State supporters are also becoming more active on encrypted messaging apps, experts say, which raises the question of whether counternarratives on platforms like Twitter or Facebook are reaching the proper audience.

Government-backed messaging has always been fraught with challenges. In 1948, Congress passed the Smith-Mundt Act, which said government information about the U.S. could only be distributed overseas. Those restrictions were later loosened but are still seen as somewhat outdated in the internet age. Nevertheless, the legal rules have forced the State Department to be careful not to present its messaging efforts as domestic propaganda, experts say.

The most significant hurdle lies not with the messages themselves, but with the messenger, according to current and former government officials. Experts widely acknowledge that directives from the U.S. government are unlikely to resonate with young people interested in joining Islamic State.

That presents the dilemma of how the government can support countermessaging efforts by tech companies and Muslim community leaders without undermining them.

A bipartisan congressional task force and the Homeland Security Advisory Council, which advises the Homeland Security secretary, have both recommended stronger countermessaging efforts by the government.

The task force's report, released last September, noted that a State Department video featuring an Islamic State defector received only 500 views after two months, while Islamic State execution videos received tens of thousands of views within hours of going online. The task force recommended the government "urgently" develop ways to contest the propaganda and work with partners such as social-media companies and universities.

The Department of Homeland Security announced last month that it would set aside $10 million of its budget to launch the first federal grant program devoted exclusively to "countering violent extremism," which includes countermessaging initiatives. School districts, local governments and nonprofits around the U.S. have been invited to apply.

Both the government and private sector are trying to use data analytics to target the messaging at the most vulnerable audiences.

Earlier this month, the Institute for Strategic Dialogue, a London think tank, published a report studying what kinds of counternarratives are most effective online. The experiments were funded by Google parent Alphabet Inc., Facebook Inc. and Twitter Inc. One conclusion from the study: The messages should be narrowly targeted to a particular audience.

Over the past year, the government has helped tech companies like Facebook create competitions for college students around the world to come up with their own campaigns against extremism. The efforts recognize that young people will respond best to messages created by other young people. This spring there were 54 universities in the competitions, up from 45 schools last fall.

In April, the House passed a bill that would require Homeland Security to use testimonials of former extremists and defectors to combat terrorism, a strategy that is widely employed in Europe. State Department officials also have encouraged media companies and filmmakers to host workshops where Muslim activists can learn to film their own content.

Whether the messages are dimming the appeal of Islamic State is hard to know. It's virtually impossible to quantify the number of people who were convinced not to join a terrorist group. For that reason, some experts say the government should be wary of devoting too many resources to this area and focus on military efforts with more tangible results.

"You're never going to get rid of bad ideas," said Will McCants, a former senior adviser at the State Department who now is a senior fellow at the Brookings Institution. "If we want to diminish them in the eyes of the public, let's have it, but let's also recognize that it is a marginal effort."

ABC (Australia)
Government computer networks breached in cyber attacks as experts warn of espionage threat
Monday, 29 August 2016
Byline: Linton Besser & Jake Sturmer

Canberra - Sensitive Australian Government and corporate computer networks, including those holding highly confidential plans for a privately financed geostationary communications satellite, have been penetrated by sophisticated cyber attacks, Four Corners reveals.
Sensitive Australian Government and corporate computer networks -- including those holding highly confidential plans for a privately financed geostationary communications satellite -- have been penetrated by sophisticated cyber attacks, a Four Corners investigation has established.

Austrade and the Defence Department's elite research division, now named the Defence Science Technology Group, both suffered significant cyber infiltrations in the past five years by hackers based in China.

Intelligence sources say they suspect the attackers in these cases were sponsored by Beijing.

Four Corners has also confirmed Newsat Ltd, an Australian satellite company whose assets were sold off last year after the company went into administration, was so comprehensively infiltrated three years ago that its entire network had to be rebuilt in secret.

But these incidents, revealed for the first time, are only a fraction of the cyber attacks being waged against Australian governments and companies.

The Prime Minister's cyber security adviser, Alastair MacGibbon, told the program the Australian Government was "attacked on a daily basis".

"We don't talk about all the breaches that occur," he said.

Former Central Intelligence Agency boss Michael Hayden, who also served for six years as the head of the US electronic spying division, the National Security Agency (NSA), said both Australia and the US had to harden up their defences and "protect their data" from foreign cyber attacks.

"It is what adult nation states do to one another," he said.

"What my dad told me when I came home beat up from a fight once when I was about 10 years old: 'Quit crying, act like a man and defend yourself'."

A spokesman for the Chinese Embassy in Canberra denied China had conducted any cyber espionage against Australian interests, calling such allegations "totally groundless" and "false cliches".

"Like other countries, China suffers from serious cyber attacks and is one of the major victims of hacking attacks in the world," he said.

Defence assets may have been target in BoM hack

Four Corners has also been given fresh details about the high-profile , which was officially confirmed by Mr Turnbull earlier this year.

Government and industry sources said the true targets for the cyber attack may have been defence assets linked to the BoM and its vast data-collection capabilities.

One was the Australian Geospatial-Intelligence Organisation, an intelligence agency within the Department of Defence which provides highly detailed mapping information for military and espionage purposes.

The other was the Jindalee Operational Radar Network (JORN), a high-tech over-the-horizon radar run by the Royal Australian Air Force.

JORN provides 24-hour military surveillance of the northern and western approaches to Australia but also assists in civilian weather forecasting.

Four Corners was told the cyber attack failed to reach into these networks, and that it was "sandboxed", or contained within the BoM.

Intelligence sources confirmed the attack was attributed to China, which was again denied by Beijing.

Mr MacGibbon said he did not know what the intention was of the people who compromised the system.

"I would say to you that people who compromise systems will usually try to find a way to move laterally through it. If that means through a third party that's what they'll try to do," he said.

The Australian Signals Directorate (ASD) has conducted detailed investigations into the cyber intrusion, but its boss, Dr Paul Taloni, declined to comment.

A former high-ranking intelligence officer told Four Corners the Defence Department itself had significant, unresolved, cyber-security issues and had "to look at itself".

He confirmed that in about 2011 the Defence Science Technology Organisation had been successfully hacked by China-sponsored hackers, but declined to provide any further details citing national security concerns.

A spokesman for the Defence Science Technology Group said: "Defence policy is to not comment on matters of national security."

Sensitive information 'stolen for profit'

Mr Hayden said, however, China's efforts against Australia had been primarily focused on "the theft of information, and really by and large the theft of information for commercial profit", activities which he said go beyond acceptable state-on-state espionage.

The Newsat attack by China- based hackers may be a case in point.

"Given we were up against China, state-sponsored, a lot of money behind them and a lot of resources and we were only a very small IT team, it certainly wasn't a fair fight for us," Newsat's former IT manager Daryl Peter said.

While the company carried communications for resources and fossil fuel companies, as well as the US military's campaign in Afghanistan, Mr Peter said the real target for the cyber infiltration was its plans for a Lockheed Martin-designed satellite dubbed Jabiru-1.

"A company like Lockheed Martin, they have restrictions on the countries where they can build their satellites," he said.

"So a country like China being able to get a hold of confidential design plans would be very beneficial for them because it's not something they would see or be able to have access to."

Mr Peter was first told about the hack of the company in 2013 at a top-level meeting with ASD. The issue had come to a head because of Newsat's advanced plans to employ a restricted encryption tool for use with the new satellite designed by the US Government's NSA.

ASD refused to release the tool to Newsat until it tackled the sophisticated cyber intrusion, with intelligence officials telling the company its networks were "the most corrupted" they had seen.

"They actually said to us that we were the worst," Mr Peter said.

"What came out of that meeting was we had a serious breach on our network and it wasn't just for a small period of time, they'd been inside our network for a long period, so maybe about two years. And the way it was described to us was they are so deep inside our network it's like we had someone sitting over our shoulder for anything we did."

To rid the network of the infestation, Mr Peter had to build a parallel network in secret so as to not tip off the hackers that had been identified.

That work took almost a year and cost the better part of $1 million.

Mr MacGibbon said the revelations were no surprise.

"I can't say which particular nation state would get involved in getting into a telecommunications system but I can understand why a nation state would," he said.

"If you wanted to listen to someone's communications that's probably a good place to start."

Austrade regularly challenged by security issues

Australia's trade and investment commission, Austrade, has had persistent problems with cyber security, Four Corners has learned.

The discovery of a major infestation in the Austrade network was made during work that began in 2013 within the department to develop a new data centre and a redesigned IT infrastructure.

In March 2014, the agency's cyber security regime underwent an ASD-designed security assessment required because Austrade not only carries sensitive communications but works closely with the Department of Foreign Affairs and Trade.

An intelligence community figure said the tests resulted in a "series of red flags". He said the infiltration was "covering the network".

Austrade brought in UXC Saltbush, a cyber security contractor, to investigate its networks and put mitigation works in place to prevent future breaches

A former high-ranking intelligence official said the Austrade breach followed a previous problem in 2011, which was a textbook example of a "successful [and] deeper penetration".

Jim Dickins, an Austrade spokesman, said the organisation "faces ongoing and fluid challenges to its information technology security".

"Austrade has worked with the Australian Signals Directorate on occasion to contain and eradicate threats but is unable to comment on specific instances. Mitigation strategies developed on those occasions are applied on an ongoing basis."

The intelligence community figure said the problems had still not been entirely addressed because of the high cost of a comprehensive network-wide security upgrade, but Mr Dickins denied there were any "significant" persistent issues.

"Austrade is not currently dealing with any significant threats or breaches of its network," he said.

A third intelligence source told Four Corners that "Austrade is inherently vulnerable" because of its international footprint and reliance on locally-employed staff.

"People are getting breached all the time," he said.

Watch Cyber War on Four Corners tonight at 8.30pm on ABC TV and on iView.

Globe and Mail
RC hack nearly brought agency 'back to the buggy'
Saturday, 03 September 2016
Byline: Colin Freeze

Ottawa - Upon discovering that it had been hacked by China, the Canadian government's scientific-research body did digital damage control on an enormous scale. Firing up its vintage fax machines, it jettisoned scores of computer servers, bought its staff hundreds of new laptops and drew up a list of about 20,000 corporate partners in Canada whose secrets risked being collateral damage.
Records newly released to The Globe and Mail reveal these and other details about the extensive fallout from this nightmare at the National Research Council.

The hack of the NRC was highlighted in July, 2014, when the then-Conservative government blamed China, making it the first and only cyberespionage campaign that Canada has ever pinned on a specific state adversary.

While hacks of government departments occur relatively routinely, the NRC could be considered a more valuable target than most. For decades, it has been routing tax dollars to fund cutting-edge research in agriculture, engineering and computer science. Placing bets on Canadian companies helps the NRC work to ensure future prosperity, and its staff gets a glimpse of emerging technologies and proprietary business plans.

That's why the Canadian government was alarmed when federal officials announced two years ago that they had "detected and confirmed a cyberintrusion" within the NRC by "a highly sophisticated Chinese state- sponsored actor."

But while prime minister Stephen Harper's government took the unprecedented step of allowing officials to make the controversy public, it remains unknown how or when Chinese hackers first infiltrated the NRC's computer systems, or what drew them to it in the first place.

The records released to The Globe under the Access to Information Act show only the aftermath. Job No. 1 at the agency was to warn the "clients" - corporations, academics, entrepreneurs - via phone calls and mailed letters that they were at risk. "The NRC has been the target of a cyberintrusion. As a result the information held in our systems from your organization may have been compromised," one form letter reads.

One version of this letter in the NRC files was accompanied by a spreadsheet of more than 20,000 Canadian firms, most of them apparently engaged in governmentsponsored research.

"As a precautionary measure, NRC informed all clients and research partners involved in business relationships and research activities of the cyberintrusion," spokesman Guillaume Berube said in reply to questions about this list.

Several of the companies that were contacted by The Globe said they felt that the fallout was minimal because they were careful, even before the hack, about sharing trade secrets with the agency.

Their biggest gripe with the NRC was that correspondence and payments became frustratingly slow in 2014. "It wasn't back to the buggy, but it was pretty close," said one entrepreneur, who asked not to be named.

This was because staff at the scientific agency had been told not to use computers to communicate. E-mail "must not be used to transmit secure, sensitive or confidential information," one memo reads. "The preferred way of transferring confidential information ... is paper (fax, mail, courier)," another says.

Clients were to be told that "if you must share sensitive information with the NRC, the best practice is to do it via physical media" - meaning on paper or via USB sticks.

As the hack was announced publicly, one enterprising NRC employee wrote that he found a stash of safe digital devices. "I've dug up a box of brand new McAfee USB keys that we bought a few years ago," he told colleagues in an e-mail. Calling them "state of the art" for their encryption capability, he said they could serve as a "stopgap, at least until NRC gets in more for everyone."

Even the act of plugging a smartphone into an NRC computer was deemed risky. "Instead of using your computer to charge your phone, charge it through a wall outlet," one memo says.

The agency started to pull the plug on almost all its existing computer architecture as it created the data equivalent of an airlock. The hope was to move electronic files from the NRC's legacy "black" environment to a blank slate of new machines dubbed the "green" environment.

The in-between step was the "grey zone," a locked-down "scrubbing" station with no external network connectivity and which banned unfamiliar digital devices and outsiders.

"The process of scrubbing data to be taken out of the Grey Zone can take a long time. We have seen up to 40 minutes to scrub 1 GB [gigabyte] of data," one employee complained.

The NRC's initial hope was to have fully rebuilt systems within a year. Most are in now place, but The Canadian Press recently reported that some parts will not be ready until July, 2018.

Early this summer, the NRC announced that it had embarked on a partnership with its scientific counterparts in a foreign country.

And that country is China. This new joint venture with Guangdong Province aims to better fund collaborative Canadian and Chinese research projects.

The NRC was asked by The Globe why it would want to do business with a country that allegedly stole from it just two years ago.

Mr. Berube said simply that "global collaboration is a competitive necessity to generate new business opportunities." The NRC spokesman added in his e- mailed reply that "the government of Canada is committed to deepening our trade relationships with established and emerging markets, including China."

The Hill Times
Canadians lack understanding of CSE and why it needs to snoop
Monday, 05 September 2016
Byline: Phil Gurski
Section: oped

OTTAWA--If there is one spy agency in Canada that is poorly understood and about which much of little veracity has been published it has to be CSE, or the Communications Security Establishment.
CSE has a number of roles, but the one that gets the most public attention is signals intelligence, or SIGINT. This method of intelligence collection entails capturing telecommunications in a variety of forms by a variety of techniques, few of which are known. This is indeed a good thing: the spy agency that openly shares how it gathers intelligence will not be in the spy business very long. This may sound sacrilege to some, but some things need to remain secret.

CSE is not a law-enforcement agency and does not go to court to acquire warrants to collect information, unlike CSIS and the RCMP. It is limited to the collection of intelligence outside Canada and it cannot include Canadians (or Americans, British, Australians, and New Zealanders for that matter--Canada's so-called "five eyes"partners) in its dragnet.

And yet, some information pertaining to Canadians has apparently been picked up, and the scale of that collection appears to be on the upswing, according to a recent National Post article. Should Canadians be worried?

It is hard to say, but I will go with no. Before I explain why I think that there are limited circumstances under which CSE should be able to collect information on Canadians. it would be remiss not to note that I worked for that organization for almost 20 years. I knew how it operated very well in the pre-9/11 period, but would not purport to be an expert on how it operates now. Nevertheless, I am certain that the same rigour and observance of Canadian law, as well as internal policies, are being followed today much as they were when I was there.

We do not know precisely what kinds of information were collected, but there is a particular circumstance under which Canadian communications should and must be intercepted by CSE, and I think that Canadians would agree with me.

Much discussion has been held in recent years over how and whether CSE should assist other Canadian security agencies--i.e., CSIS and the RCMP--in their lawful investigations. CSE's partners do take action to monitor threats like terrorism and they have a suite of tools with which to do so. They do a very good job but on rare occasions could use the help of an agency like CSE.

Consider the following scenario. Either CSIS (under its Section 21 powers) or the RCMP (Part VI) have successfully obtained a warrant to capture the communications of a person under investigation. These warrants are granted by Federal Court judges once these agencies provide compelling arguments as to why they need these intrusive powers (not a rubber-stamp process by any stretch) and apply them to communications within Canada. But what if the subject of investigation high tails it to Somalia or Syria or Afghanistan? Not only do Canadian warrants not apply in those countries, but it would be next to impossible to get local law enforcement or intelligence agencies there to cooperate with us. That is where CSE could assist.

I have absolutely no issue with CSE helping either the RCMP or CSIS collect an individual's communications while outside the country when they already have such powers within Canada. Having access to this information can assist ongoing investigations and could make a difference in stopping a terrorist act or not. We have seen instances, here and abroad, where terrorists have travelled to some hotspot, received training, and returned to their homeland to kill and maim people. Having that extra information should not be seen as injurious to privacy concerns or outside CSE's remit.

As I have said many, many times, we need an adult conversation in this country on what is reasonable to expect from our intelligence agencies and what they need to keep us safe. We have to stop relying on information from pseudo experts and engage in meaningful dialogue. CSE has a lot of resources and tools at its disposal and it should not be handcuffed in its efforts to help keep us safe.

Phil Gurski is president and CEO Borealis Threat and Risk Consulting.

The Hindu
Scorpene data breach echoes on G20 sidelines
Tuesday, 06 September 2016
Byline: Atul Aneja

Hangzhou - The breach of sensitive data regarding the French Scorpene submarines being built in India has echoed in Hangzhou, with Prime Minister Narendra Modi taking up the issue during the "pull aside" with French President Francois Hollande on the sidelines of the G20 summit on Monday.
Foreign Ministry spokesperson Vikas Swarup, during his briefing on Monday afternoon confirmed that the Scorpene issue was raised during the Prime Minister's brief meeting with the French President. However, he was non-committal when asked separately by The Hindu on whether the sensitive information seepage, reported by the Australian newspaper, also came up during Sunday's talks

between Prime Minister Modi and his Australian counterpart, Malcolm Turnbull. "I can neither confirm nor deny it," he said. Official sources, however, had earlier told The Hindu that "it was inconceivable" that the Scorpene issue did not feature during the Prime Minister's talks with Mr. Turnbull.

The Mazagon Docks Limited (MDL) is building six Scorpene submarines with technology transfer from DCNS of France. "The stunning leak, which runs to 22,400 pages and has been seen by The Australian, details the entire secret combat capability of the six Scorpene-class submarines that French shipbuilder DCNS has designed for the Indian Navy," The Australian had reported last month.

On Monday, the Financial Review reported from Hangzhou that Mr. Turnbull has received assurances from Mr. Hollande regarding the submarines that Australia is set to acquire from DCNS of France in the aftermath of the data leakage of the Scorpene.

The daily said that Mr. Turnbull revealed on Monday that he had already raised the matter with Mr. Hollande on the sidelines of the G20 leaders' summit. It was formally raised when the pair had a bilateral meeting later in the day.

"We've had a brief discussion about it already and we will be addressing it in more detail," Mr. Turnbull said before formal talks.

"Maintaining absolute maximum security, total security on information of this kind is critical. The leaks of the material relating to Scorpene submarine are very, very regrettable."

Mr. Turnbull said that while the Scorpene submarine was different to the 12 Barracuda subs DCNS would be building for Australia, he needed an assurance that the security breach would not happen again.

"There's a thorough investigation going on the French side to see how that happened -- of course it's a different submarine to the one that we are going to build in collaboration with the French -- but it is absolutely critical to continue to maintain the highest level of security," he said.

When asked by The Hindu to comment on the grave security implications of the leak on Monday, the sources said that "a court injunction in Australia has already been obtained" that would prevent further seepage of information regarding the Scorpene submarines. The Australian has said that it would not be publishing additional confidential data on the Indian Scorpene Class submarines after the New South Wales Supreme Court imposed a temporary ban on further publication of the documents.

Reuters had earlier reported that Indian officials have pointed to a "non-disclosure of information" clause that was written into the 2005 contract at French insistence. Quoting a defence ministry official, it said that New Delhi could only invoke that clause if it was established that the data was leaked and not stolen.

Arab News
Shortage of IT specialists exposes govt networks to spy threats
Tuesday, 06 September 2016
Byline: Sharif M. Taha

Riyadh - An information technology expert said a shortage of specialized cadres in information security has exposed government and service sector networks to spy and infiltration attacks.
Last week, the Electronic Security Center (ESC), an affiliate of the Interior Ministry, detected foreign attacks targeting the electronic networks of a number of government agencies and other vital sectors in the Kingdom.

Dr. Hani Al- Zaid, an expert in information security, told local media that the issue is linked to challenges facing the Saudization of technical jobs, notably those related to information security.

Based on his experience in the government sector, he said there were two challenges facing the Saudization of technical jobs: Shortage of specialized cadres in information security, and difficulty in the recruitment of qualified cadres due to limited privileges of such jobs.

To address the problem, he suggested the assignment of information security jobs in the government sector to government companies specialized in information security. This will help in rotating qualified cadres into such specialized jobs, safeguarding the secrecy of information circulated in the public sector, he said.

According to the ESC report last week, the foreign electronic attacks came on a number of governmental and service sector networks.

The governmental sector received 39 percent of the total electronic attacks, followed by the media sector (23 percent), the telecom and IT sector (15 percent), whereas the electricity and water sector was the least attacked at 8 percent, the ESC said.

Al-Zaid estimated the Kingdom's losses arising from the electronic attacks at SR2.8 billion. He stressed that the electronic attacks sustained by some government agencies necessitates the building of a national plan to qualify national cadres in information security.

Lebanon Daily Star
STL: Telecoms expert details final calls before bombing
Tuesday, 06 September 2016
Byline: Ned Whalley

Beirut - A telecoms expert described to the Special Tribunal for Lebanon how a covert network of cellphones exhibited striking call patterns in the leadup to the assassination of ex-Prime Minister Rafik Hariri, culminating in a flurry of activity in the hour before his death. John Edwards Philips testified that the activity of a group of eight "red phones" can be strongly associated with the crime. "They worked in a pattern together. They were coordinated and cohesive," he said.
Philips is the prosecution's primary expert on cell-siting and the analysis of call data records. Overlaying coverage maps with satellite photos, he demonstrated the remarkable activity of the red phones in the final minutes before a massive car bomb killed the former prime minister outside Beirut's St. Georges Hotel.

Prosecutors say they have identified a number of covert networks used in the conspiracy, giving each a color. The red phones were allegedly used in the actual execution of the bombing. The phones made 28 calls in the hour before the attack, six in the final three minutes. One in particular made a rapid succession of calls to the others just before the blast. Philips' map showed each as they made way their way south, away from the soon-to-be blast site. The handsets were never used again.

Philips said the phones demonstrated "high-forensic visibility," due to their heavy usage in physical and temporal proximity to the incident. He called their discovery "inevitable" and suggested that any analysis of cellphone usage would have revealed them. Furthermore, he suggested the operators of the red phones knew this. What was intended to be secret was the association with other covert networks and, ultimately, the identities of users.

Philips documented the "hierarchical call flow" exhibited by the activity of these other groups, where a call from one phone appeared to precipitate atypical activity among the entire network.

"Whenever certain activities occur, the command element is inextricably involved," Philips said.
Prosecutors contend this evidence illustrates the phone of defendant Salim Ayyash being used to send other members of the operation on trips to Tripoli, Baalbeck and Anjar.

The excursions to Tripoli were allegedly undertaken to purchase the Mitsubishi van used in the attack and to travel to Baalbeck and Anjar to obtain the necessary explosives. Anjar held particular significance at the time as the Lebanese headquarters of Syrian intelligence.

Associated Press
Kuwait warns citizens on carrying extremist materials to US
Sunday, 04 September 2016

Kuwait City - The Gulf nation of Kuwait has warned citizens travelling to the U.S. to check their phones and laptops to ensure they do not contain any material that could be linked to extremist groups.
The official Kuwait News Agency reported Saturday that the Kuwaiti Embassy to Washington also urged citizens to ``co-operate fully'' with American airport officials seeking access to their devices.

It warns that immigration officials could interrogate Kuwaitis and cancel entry visas if extremist photos, videos or other materials are found.

The warning comes after Kuwaiti media reported that three Kuwaitis were refused entry to the U.S. earlier this year.

Kuwait is a U.S. ally that hosts American troops taking part in operations against the Islamic State militant group.

Pajhwok Afghan News
Attempt at smuggling drone parts to Pakistan foiled
Sunday, 04 September 2016
Byline: Javed Hamim Kakar

Kabul - An attempt to smuggle military equipment, including drone parts, to Pakistan was frustrated by security forces in eastern Nangarhar province on Sunday, a source revealed.
One official wishing to go unnamed told Pajhwok Afghan News that Special Forces were dispatched from Kabul to eastern Nangarhar province in the morning.

The Special Forces conducted a joint raid jointly with Nangarhar Border Police in Momand Dara district and recovered the military gear from a house.

New York Times
F.B.I. Email Inquiry Reveals Some of Secretary's Habits
Saturday, 03 September 2016
Byline: Michael S. Schmidt

Washington - Documents released by the F.B.I. on Friday revealed new details about the Justice Department's yearlong investigation into Hillary Clinton's use of a private email server and whether she and her aides mishandled classified information. Among the documents was an 11-page summary of an interview F.B.I. agents conducted with Mrs. Clinton on July 2. Two days later, the F.B.I. director, James B. Comey, said the bureau had recommended to the Justice Department that neither Mrs. Clinton nor her aides should be charged with a crime. Here are six highlights from those documents:
New details about the deletion of Mrs. Clinton's emails

According to the F.B.I., in December 2014 a top aide to Mrs. Clinton told the company that housed her server to delete an archive of emails from her account. The company, Platte River Networks, apparently never followed those instructions. On March 2, 2015, The New York Times reported that Mrs. Clinton had exclusively used a personal email account when she was secretary of state. Two days later, the

congressional committee investigating the 2012 attacks in Benghazi, Libya, and Mrs. Clinton's response to them, told the technology firms associated with the email account that they had to retain "all relevant documents" related to its inquiry.

Three weeks later, a Platte River employee realized he had not deleted the emails as instructed. The employee said he then used a special program called BleachBit to delete the files. The F.B.I. said Mrs. Clinton was unaware of the deletions.

The F.B.I. said it was later able to find some of the emails, but did not say how many emails were deleted, or whether they were included in the 60,000 emails that Mrs. Clinton said she sent and received while secretary of state from 2009 to 2013.

But Mrs. Clinton's lawyer, David Kendall, said in a letter to Congress on March 27, 2015, that after Mrs. Clinton gave roughly 30,000 work-related emails to the State Department, Mrs. Clinton "chose not to keep" her personal emails while she was secretary of state, which she has said numbered roughly 30,000. Mr. Kendall said he confirmed with Mrs. Clinton's support staff that no emails from the time she was in office "reside on the server or on any backup systems associated with the server."

Mrs. Clinton relied on her staff to know what was classified

In Mrs. Clinton's interview with the F.B.I., she said she did not recall receiving any emails "she thought should not be on an unclassified system." She said she had relied on State Department officials to use their judgment when emailing her sensitive information, adding that she "could not recall anyone raising concerns with her regarding the sensitivity of the information she received at her email address."

Colin Powell had told Mrs. Clinton to 'be very careful'

In a summary of the investigation, the F.B.I. said Mrs. Clinton had emailed Colin L. Powell, a former secretary of state, a day after she was sworn into office about Mr. Powell's use of a personal email account when he was the country's top diplomat. Mr. Powell warned Mrs. Clinton that if she used her BlackBerry for official business, those emails could become "official record[s] and subject to the law."

Mr. Powell, apparently implying that he was cautious in his use of his personal email account, added: "Be very careful. I got around it all by not saying much and not using systems that captured the data." According to a summary of her interview, Mrs. Clinton said she did not know exactly what Mr. Powell meant and that his message "did not factor into her decision to use a personal email account."

Some of Mrs. Clinton's closest aides were unaware of the server

Mrs. Clinton said in her interview it was "common knowledge" that she had a private email address because it was "displayed to anyone with whom she exchanged emails." But the F.B.I. said in a summary of its findings that "some State Department employees interviewed by the F.B.I. explained that emails

by Clinton only contained the letter 'H' in the sender field and did not display her email address." The F.B.I. said that some of Mrs. Clinton's closest aides were aware she used a private email address but did not know she had set up a private server. The aides said they were "unaware of the existence of the private server until after Clinton's tenure at State or when it became public knowledge."

Mrs. Clinton had taken her BlackBerry into prohibited areas

According to the summary of the investigation, Mrs. Clinton brought her BlackBerry into a secure area on the seventh floor of the State Department, where such electronics are prohibited. The F.B.I. interviewed three former State Department diplomatic security agents who said that Mrs. Clinton kept her BlackBerry in her desk drawer in the secure area, a so-called Sensitive Compartmented Information Facility, or SCIF. But Huma Abedin, a top aide to Mrs. Clinton, told the F.B.I. that Mrs. Clinton left the secure area to check her BlackBerry, often going to the State Department's eighth-floor balcony to do so.

Mrs. Clinton had used a lot of electronic devices to send emails

The F.B.I. said that it had identified 13 mobile devices that Mrs. Clinton potentially used to send emails. Mrs. Clinton's aides were in charge of buying replacement BlackBerry devices when she was in office. Ms. Abedin told the F.B.I. that "it was not uncommon for Clinton to use a new BlackBerry for a few days and then immediately switch it out for an older version with which she was more familiar." Ms. Abedin and another aide told the F.B.I. that "the whereabouts of Clinton's devices would frequently become unknown once she transitioned to a new device." An aide to Bill Clinton, Justin Cooper, who helped set up the server, told the F.B.I. that he recalled "two instances where he destroyed Clinton's old mobile devices by breaking them in half or hitting them with a hammer."

New York Times
Microsoft's Legal Challenge to Government Secrecy Wins Dozens of Supporters
Saturday, 03 September 2016
Byline: Nick Wingfield

Seattle - Dozens of allies threw their weight behind Microsoft on Friday in a case that challenges law enforcement's use of secrecy orders to cloak its pursuit of digital communications in investigations. Amazon, Google, Snapchat, Salesforce and several others filed a brief on Friday in support of Microsoft in its case against the United States Justice Department, while Apple, Mozilla and others made their own filing. Civil liberties groups and media organizations like Fox News, National Public Radio and The Washington Post submitted their own briefs.

Microsoft was also backed by a collection of law professors and a group of former United States attorneys who worked in the Western district of Washington, where Microsoft filed its federal lawsuit in April.

Microsoft's effort to rally support is part of a growing resistance by technology companies to government attempts to snoop on the electronic communications of their customers.

Revelations by Edward J. Snowden, the former United States government contractor, about the extent of electronic surveillance by spy agencies have rattled technology companies, which worry that trust in their products is being undermined.

In a statement, Brad Smith, Microsoft's president and chief legal officer, said the company was grateful for the support from what it expected to total 80 signatories on multiple briefs by the end of the day. He noted the diversity of backgrounds of the signatories, saying, "it's not every day that Fox News and the A.C.L.U. are on the same side of an issue."

"We believe the constitutional rights at stake in this case are of fundamental importance, and people should know when the government accesses their emails unless secrecy is truly needed," Mr. Smith added.

Peter Carr, a spokesman for the Justice Department, declined to comment.

The lawsuit argued that the government's use of a provision of the Electronic Communications Privacy Act of 1986 -- which prevents Microsoft from notifying customers when their communications have been turned over to law enforcement, sometimes indefinitely -- is unconstitutional.

Microsoft said the secrecy orders violated the Fourth Amendment, which grants people and businesses the right to know if the government seizes or searches their property, along with the company's First Amendment right to communicate with its customers.

Technology companies are concerned that secrecy orders are especially troubling in the era of cloud computing. "In contrast to a search of a home or a seizure of physical property, there may be no way for a user to detect that the provider has disclosed information stored in the account to the government," the brief filed by Amazon, Google and others said.

In March, nearly every major technology company, including Microsoft, Amazon and Google, filed briefs backing Apple in a legal showdown with the federal government, which had demanded Apple's technical assistance in bypassing security software on an iPhone used by a gunman in the shootings in San Bernardino, Calif., last year.

The F.B.I. eventually broke into the phone with the help of an outside party, not Apple.

The Microsoft lawsuit is different in that it does not center on any individual case, but instead is aimed at the legal process the government uses to keep its information requests secret.

The company said such secrecy orders are becoming more frequent. In its lawsuit, Microsoft said of the more than 5,600 federal demands for customer data it received between September 2014 and March 2016, nearly half were accompanied by secrecy orders that prevented Microsoft from telling affected customers that it had turned over their information to the government.

Microsoft executives have said they appreciate the necessity of secrecy orders in some cases. But they have criticized as too low the bar that prosecutors must meet to obtain a secrecy order from courts.

Microsoft is also concerned about the absence of time limits on when it can disclose to customers that the government has obtained their communications. For physical searches of files and the like, most secrecy orders delay notification for a limited period of time, often one to three months.

For the government data requests with secrecy orders that Microsoft received in the period it examined between 2014 and 2016, more than 68 percent contained no fixed end date.

"Law enforcement officials have no practical need to keep their searches secret indefinitely, except in the rarest of circumstances, which must be supported by particularized need," read the brief filed Friday by former United States attorneys supporting Microsoft.

Le Figaro
Le piratage de l'Elysée en 2012 venait bien des Etats-unis (Canada)
Saturday, 03 September 2016

Paris -Les Etats-Unis sont bien à l'origine d'une attaque informatique contre l'Elysée au printemps 2012, a déclaré un ancien responsable des services secrets français. Dans une conférence donnée en juin dev... Les Etats-Unis sont bien à l'origine d'une attaque informatique contre l'Elysée au printemps 2012, a déclaré un ancien responsable des services secrets français. Dans une conférence donnée en juin devant les élèves de l'école d'ingénieurs CentraleSupélec, dont LeMonde.fr diffuse un enregistrement samedi, Bernard Barbier reconnaît également la responsabilité de la France derrière une autre attaque informatique détectée par les services canadiens en 2009. Cet ancien chef de la direction technique de la Direction générale de la sécurité extérieure (DGSE) raconte qu'il a reçu un appel à l'aide du responsable de la sécurité informatique de l'Elysée en mai 2012, entre les deux tours de la présidentielle, à la suite d'un piratage d'ordinateurs de collaborateurs du chef de l'Etat, alors Nicolas Sarkozy.

"On a vu qu'il y avait un 'malware' (logiciel malveillant) qui avait une signature identique à celui que nous avions identifié lors d'une attaque contre la Communauté européenne en 2010. Il n'y avait que les Américains et les Russes qui avaient pu faire cette première opération", a- t-il dit. "En 2012, nous avions davantage de moyens et de puissance techniques pour travailler sur les métadonnées. J'en suis venu à la conclusion que cela ne pouvait être que les Etats-Unis", ajoute-t-il en précisant que le logiciel en question avait été infiltré lors de connexions sur Facebook.

Bernard Barbier indique qu'il a reçu par la suite l'ordre de François Hollande se rendre aux Etats-Unis pour protester contre cette opération auprès de l'Agence nationale de sécurité (NSA) américaine.

"Ce fut le 12 avril 2013 et ce fut vraiment un grand moment de ma carrière professionnelle (...) A la fin de la réunion, Keith Alexander (NDLR: directeur de la NSA de 2005 à 2014), n'était pas content. Alors que nous étions dans le bus, il me dit qu'il est déçu car il pensait que jamais on ne les détecterait. Et il ajoute : 'Vous êtes quand même bons.'"L'ancien responsable de la DGSE reconnaît que les services français ont commencé à faire du piratage informatique dès 1992 et qu'ils sont responsables d'une vaste opération lancée en 2009, comme le soupçonnait le Canada dans une note dévoilée en 2013 par le lanceur d'alerte américain Edward Snowden. Les cibles étaient alors des institutions iraniennes liées au programme nucléaire de la République islamique mais aussi plusieurs pays, dont le Canada, et des objectifs en France. "Les Canadiens ont fait du 'reverse' sur un malware qu'ils avaient détecté. Ils ont retrouvé le programmeur qui avait surnommé son malware 'Babar' et avait signé 'Titi'. Ils en ont conclu qu'il était français. Et effectivement, c'était un Français", dit-il.

Fars News Agency
Putin calls DNC hack public service, denies Russia's involvement
Saturday, 03 September 2016

Moscow - Russian President Vladimir Putin said Thursday that the hack of the Democratic National Committee's emails was a public service, but denied that Moscow played any part in the cyberattack. Security experts have suggested that Russian-backed cyber militias were behind the cyberattacks on top Democratic Party groups and the possible breach of Clinton Foundation computers. But Putin wondered why it mattered who was behind the hacks.

"Listen, does it even matter who hacked this data?" he said in an interview with Bloomberg News. "The important thing is the content that was given to the public."

U.S. officials have pointed to the Russian government as the possible culprit of the attacks on DNC servers earlier this year that led to WikiLeaks published 20,000 DNC documents prior to the Democratic National Convention. The leaks showed that party officials leaned favorably toward Hillary Clinton over Bernie Sanders and led to Debbie Wasserman Schultz stepping down as the chairwoman of the Democratic National Committee.

"There's no need to distract the public's attention from the essence of the problem by raising some minor issues connected with the search for who did it," Putin said of the breach. "But I want to tell you again, I don't know anything about it, and on a state level Russia has never done this."

Based on available data and what's known of the time line on the recent attacks, the first was on the Democratic National Committee.

2016 Election Headquarters

The latest headlines on the 2016 elections from the biggest name in politics.

See Latest Coverage ?

Then hackers "island hopped" to other computer networks after staffers at the Democratic Congressional Campaign Committee and perhaps elsewhere opened phishing emails from which their user IDs, passwords and other credentials were stolen.

The FBI is investigating the breaches at the DNC, made public in late July, and the DCCC, announced in August. It is not clear whether that work has expanded with the apparent targeting of the Clinton Foundation.

Putin has repeatedly denied involvement, but Russian intelligence is thought to routinely use cyber gangs to do its bidding and to create plausible deniability.

"Within the former Soviet bloc, Russian- speaking hackers pay homage as cyber-militia members to the regime in Russia," CEO of the next-generation tech group Strategic Ventures Tony Kellerman told Fox News in August. "They act as proxies ... when called upon to leverage their sophisticated tool sets and attack against victims in the U.S."

Putin is thought to have a vendetta against Clinton after a failed attempt to re-establish positive relations in 2009. Putin also blamed her for stoking protests in 2011. Clinton had compared Russia's annexation of Crimea in 2014 to Adolph Hitler's advancements in Europe during World War II, Bloomberg News reported.

A person familiar with the hack attack told Bloomberg News that the FBI is highly confident that the Moscow government was behind the security breach of the DNC and other Democratic groups.

The Clinton campaign accused Putin of trying to influence that U.S. election.

"Unsurprisingly, Putin has joined Trump in cheering foreign interference in the U.S. election that is clearly designed to inflict political damage on Hillary Clinton and Democrats," Clinton spokesman Jesse Lehrich said in an email to Bloomberg. "This is a national security issue and every American deserves answers about potential collusion between Trump campaign associates and the Kremlin."

Though Putin is not taking blame, an internal probe of the DNC hack found that two groups connected to Russian federal security and the Defense Ministry were responsible for the hack.-

New York Times
Phone Spying Is Made Easy. Choose a Plan.
Saturday, 03 September 2016
Byline: Nicole Perlroth

San Francisco - Want to invisibly spy on 10 iPhone owners without their knowledge? Gather their every keystroke, sound, message and location? That will cost you $650,000, plus a $500,000 setup fee with an Israeli outfit called the NSO Group. You can spy on more people if you would like -- just check out the company's price list.
The NSO Group is one of a number of companies that sell surveillance tools that can capture all the activity on a smartphone, like a user's location and personal contacts. These tools can even turn the phone into a secret recording device.

Since its founding six years ago, the NSO Group has kept a low profile. But last month, security researchers caught its spyware trying to gain access to the iPhone of a human rights activist in the United Arab Emirates. They also discovered a second target, a Mexican journalist who wrote about corruption in the Mexican government.

Now, internal NSO Group emails, contracts and commercial proposals obtained by The New York Times offer insight into how companies in this secretive digital surveillance industry operate. The emails and documents were provided by two people who have had dealings with the NSO Group but would not be named for fear of reprisals.

The company is one of dozens of digital spying outfits that track everything a target does on a smartphone. They aggressively market their services to governments and law enforcement agencies around the world. The industry argues that this spying is necessary to track terrorists, kidnappers and drug lords. The NSO Group's corporate mission statement is "Make the world a safe place."

Ten people familiar with the company's sales, who refused to be identified, said that the NSO Group has a strict internal vetting process to determine who it will sell to. An ethics committee made up of employees and external counsel vets potential customers based on human rights rankings set by the World Bank and other global bodies. And to date, these people all said, NSO has yet to be denied an export license.

But critics note that the company's spyware has also been used to track journalists and human rights activists.

"There's no check on this," said Bill Marczak, a senior fellow at the Citizen Lab at the University of Toronto's Munk School of Global Affairs. "Once NSO's systems are sold, governments can essentially use them however they want. NSO can say they're trying to make the world a safer place, but they are also making the world a more surveilled place."

The NSO Group's capabilities are in higher demand now that companies like Apple, Facebook and Google are using stronger encryption to protect data in their systems, in the process making it harder for government agencies to track suspects.

The NSO Group's spyware finds ways around encryption by baiting targets to click unwittingly on texts containing malicious links or by exploiting previously undiscovered software flaws. It was taking advantage of three such flaws in Apple software -- since fixed -- when it was discovered by researchers last month.

The cyberarms industry typified by the NSO Group operates in a legal gray area, and it is often left to the companies to decide how far they are willing to dig into a target's personal life and what governments they will do business with. Israel has strict export controls for digital weaponry, but the country has never barred the sale of NSO Group technology.

Since it is privately held, not much is known about the NSO Group's finances, but its business is clearly growing. Two years ago, the NSO Group sold a controlling stake in its business to Francisco Partners, a private equity firm based in San Francisco, for $120 million. Nearly a year later, Francisco Partners was exploring a sale of the company for 10 times that amount, according to two people approached by the firm but forbidden to speak about the discussions.

The company's internal documents detail pitches to countries throughout Europe and multimillion-dollar contracts with Mexico, which paid the NSO Group more than $15 million for three projects over three years, according to internal NSO Group emails dated in 2013.

"Our intelligence systems are subject to Mexico's relevant legislation and have legal authorization," Ricardo Alday, a spokesman for the Mexican embassy in Washington, said in an emailed statement. "They are not used against journalists or activists. All contracts with the federal government are done in accordance with the law."

Zamir Dahbash, an NSO Group spokesman, said that the sale of its spyware was restricted to authorized governments and that it was used solely for criminal and terrorist investigations. He declined to comment on whether the company would cease selling to the U.A.E. and Mexico after last week's disclosures.

For the last six years, the NSO Group's main product, a tracking system called Pegasus, has been used by a growing number of government agencies to target a range of smartphones -- including iPhones, Androids, and BlackBerry and Symbian systems -- without leaving a trace.

Among the Pegasus system's capabilities, NSO Group contracts assert, are the abilities to extract text messages, contact lists, calendar records, emails, instant messages and GPS locations. One capability that the NSO Group calls "room tap" can gather sounds in and around the room, using the phone's own microphone.

Pegasus can use the camera to take snapshots or screen grabs. It can deny the phone access to certain websites and applications, and it can grab search histories or anything viewed with the phone's web browser. And all of the data can be sent back to the agency's server in real time.

In its commercial proposals, the NSO Group asserts that its tracking software and hardware can install itself in any number of ways, including "over the air stealth installation," tailored text messages and emails, through public Wi-Fi hot spots rigged to secretly install NSO Group software, or the old-fashioned way, by spies in person.

Much like a traditional software company, the NSO Group prices its surveillance tools by the number of targets, starting with a flat $500,000 installation fee. To spy on 10 iPhone users, NSO charges government agencies $650,000; $650,000 for 10 Android users; $500,000 for five BlackBerry users; or $300,000 for five Symbian users -- on top of the setup fee, according to one commercial proposal.

You can pay for more targets. One hundred additional targets will cost $800,000, 50 extra targets cost $500,000, 20 extra will cost $250,000 and 10 extra costs $150,000, according to an NSO Group commercial proposal. There is an annual system maintenance fee of 17 percent of the total price every year thereafter.

What that gets you, NSO Group documents say, is "unlimited access to a target's mobile devices." In short, the company says: You can "remotely and covertly collect information about your target's relationships, location, phone calls, plans and activities -- whenever and wherever they are."

And, its proposal adds, "It leaves no traces whatsoever."

Le Monde
Les confessions d'un maître de l'espionnage français (Canada)
Saturday, 03 September 2016

Bernard Barbier, l'ancien chef de la direction technique de la DGSE, a levé le voile sur plusieurs secrets d'Etat lors d'une conférence dans son ancienne école d'ingénieurs.
C'est une intrusion inespérée dans un monde interdit aux regards extérieurs, celui du renseignement et des guerres secrètes. Face aux élèves de l'école d'ingénieurs CentraleSupélec, dont il est issu, Bernard Barbier, l'un des personnages les plus importants de l'espionnage français des dix dernières années, a levé le voile sur des mystères qu'on pensait insolubles. Au cours de cette causerie, il a ainsi fait oeuvre de transparence sur certaines des principales affaires d'espionnage récentes ayant touché la France. Il a brisé des tabous, notamment en relatant l'attaque chinoise sur Areva et en confirmant la responsabilité de la France derrière une attaque informatique mondiale détectée par les services canadiens.

Espionnage et cybersécurité, Bernard Barbier reçu par Symposium CentraleSupélec

M.Barbier, qui fut de 2006 à 2014 l'homologue du directeur de l'Agence nationale de sécurité (NSA) américaine, en tant que chef de la direction technique de la Direction générale de la sécurité extérieure (DGSE), a commencé sa carrière au Commissariat à l'énergie atomique (CEA). Au sein de la DGSE, il obtient, en2008, une enveloppe de 500millions d'euros et 800 nouveaux postes pour l'une des plus formidables révolutions du renseignement français: créer un système de collecte massive de données replaçant la France dans la course à l'espionnage moderne.

De façon surprenante, le contenu de son intervention, faite en juin sur le campus de l'école à Châtenay-Malabry (Hauts-de-Seine) et dont nous avons pu consulter l'enregistrement filmé, n'a eu aucun écho public. En revanche, le milieu du renseignement et sa principale figure, Bernard Bajolet, le chef de la DGSE, ont eu tout l'été pour s'offusquer de ces déclarations qui montrent, sans doute, que les vrais secrets ne sont peut-être pas là où l'on croit. Extraits choisis.

La vérité sur l'attaque informatique contre l'Elysée en2012

A ce jour, il ne s'agissait que de soupçons. Les Américains auraient pu jouer un rôle dans le piratage, découvert entre les deux tours de l'élection présidentielle, en mai2012, des ordinateurs des collaborateurs du chef de l'Etat français, alors Nicolas Sarkozy. Une note interne de la NSA, dévoilée par Le Monde à l'automne 2013 et préparant la visite, le 12avril 2013, de deux hauts responsables français, dont M. Barbier, venus demander des comptes aux Américains, orientait plutôt les soupçons vers les services secrets israéliens...

«Le responsable de la sécurité informatique de l'Elysée était un ancien de ma direction à la DGSE, relate M. Barbier. Il nous a demandé de l'aide. On a vu qu'il y avait un "malware" [logiciel malveillant] qui avait une signature identique à celui que nous avions identifié lors d'une attaque contre la Communauté européenne en2010. Il n'y avait que les Américains et les Russes qui avaient pu faire cette première opération. En2012, nous avions davantage de moyens et de puissance techniques pour travailler sur les métadonnées. J'en suis venu à la conclusion que cela ne pouvait être que les Etats- Unis.

Ce malware avait aussi attaqué d'autres pays avec une méthode révolutionnaire qu'a révélée, en2013, Edward Snowden: la " quantum attack " . Quelqu'un de l'Elysée allait sur Facebook, mais au lieu d'aller directement sur le serveur du réseau social, cette consultation était interceptée par une machine de la NSA qui répondait à la place de Facebook (...), lui permettant d'entrer dans votre ordinateur. Ce malware trouvait la faille et permettait de prendre le contrôle de votre ordinateur.

J'ai reçu l'ordre du successeur de M. Sarkozy d'aller aux Etats-Unis les engueuler. Ce fut le 12avril 2013 et ce fut vraiment un grand moment de ma carrière professionnelle. On était sûrs que c'était eux. A la fin de la réunion, Keith Alexander [directeur de la NSA de 2005 à 2014] , n'était pas content. Alors que nous étions dans le bus, il me dit qu'il est déçu car il pensait que jamais on ne les détecterait. Et il ajoute: "Vous êtes quand même bons." Les grands alliés, on ne les espionnait pas. Le fait que les Américains cassent cette règle, ça a été un choc.

Quand Le Monde s'apprêtait à publier le document interne de la NSA préparant notre visite du 12avril 2013, j'ai demandé à mon correspondant de la NSA à Paris de m'en donner une copie. Il me répond qu'il ne peut pas, car le niveau de secret de la note est tel que seul le président Obama peut le déclassifier. J'ai réagi en disant que dix millions de Français allaient lire cette note alors que je n'y ai pas accès. Je l'ai finalement eue un jour avant sa publication.»

Babar ou la fin d'un secret d'Etat

En2013, Le Monde publie une note dévoilée par Edward Snowden révélant que les services secrets canadiens suspectent leurs homologues français d'être derrière une vaste opération de piratage informatique lancée en2009. Si l'attaque vise une demi-douzaine d'institutions iraniennes liées au programme nucléaire de ce pays, elle cible également le Canada, l'Espagne, la Grèce, la Norvège, la Côte d'Ivoire, l'Algérie et même certains objectifs en France. Sur ses auteurs, les Canadiens restaient flous: «Nous estimons, avec un degré modéré de certitude, qu'il s'agit d'une opération sur des réseaux informatiques soutenue par un Etat et mise en oeuvre par une agence française de renseignement.» Du côté français, silence absolu. Paris admet s'être doté de capacités défensives, mais dément toute activité offensive, un tabou. Jusqu'au récit de M. Barbier.

«Les Canadiens ont fait du " reverse " [remonter la trace informatique] sur un malware qu'ils avaient détecté. Ils ont retrouvé le programmeur [le codeur] qui avait surnommé son malware "Babar" et avait signé "Titi". Ils en ont conclu qu'il était français. Et effectivement, c'était un Français (...). On a franchi un seuil énorme entre 1990 et 1995 quand on a acheté un supercalculateur américain Cray. On s'est aperçu qu'avec une très grande puissance de calcul, on pouvait casser les mots de passe.

On a commencé à faire du hacking en1992. J'ai monté les premières équipes de hacking étatique, les premiers soldats de la cyber-armée française. Les meilleurs n'ont pas de formation universitaire. Ce n'est pas un problème de connaissance, c'est un problème de cerveau. C'est quelqu'un qui, à partir de 15-16 ans, a commencé à bidouiller. Il va trouver des choses et donc des failles. Aujourd'hui, ce n'est pas 100 personnes qu'il faudrait recruter, il en faut 200 à 300.»

La fusion de la DGSE et de son homologue allemand, le BND

M. Barbier ne s'est pas contenté de relater des opérations. Il a également évoqué la frilosité du pouvoir politique face à ses propositions visant à répondre plus efficacement aux nouvelles menaces, et notamment son projet audacieux esquissant un embryon de renseignement européen.

«Il est impossible de construire un seul service de renseignement européen avec vingt-huit pays qui n'ont pas les mêmes moyens ni la même culture. Les meilleurs, par rapport à leur nombre d'habitants, ce sont les Suédois. Les Italiens sont mauvais. Les Espagnols sont un peu mieux, mais n'ont pas de moyens. Et les Britanniques, avec 6500 agents au sein du GCHQ [le renseignement électronique

britannique] , sont forts, mais sont-ils européens? Et la France est la première force de renseignement technique en Europe continentale.

Restent les Allemands, qui sont de solides partenaires. J'ai beaucoup travaillé avec eux, à la fois en transmettant notre savoir-faire mais aussi en leur apportant des moyens techniques. Les ingénieurs allemands et français travaillent très bien ensemble. En revanche, l'ingénieur britannique avec l'ingénieur français, c'est compliqué.

Pour être plus efficaces, j'ai dit aux politiques en France qu'il fallait fusionner le BND [le Service fédéral allemand de renseignement] et la DGSE. C'est la seule solution. Cela ferait un service de 15000 personnes. La NSA compte 60000 personnes, et la direction technique de la DGSE, seule, c'est 3000 agents. Mais les politiques français n'ont jamais donné suite.»

Une révolution dans le secret de la DGSE

Au cours de son exposé, Bernard Barbier a illustré le rôle primordial joué désormais par la direction technique dans la lutte contre les milieux djihadistes et l'espionnage moderne.

«Pour avoir du renseignement humain sur les réseaux djihadistes, c'est quasiment impossible. Leurs membres [de ces réseaux] ne travaillent qu'avec des gens qu'ils connaissent. Dans la direction, on était déjà bien conscient en2012 que des Français voulaient revenir faire le djihad en France. A plusieurs reprises, en2013, mes équipes m'avaient déjà fait écouter des interceptions de Français de Syrie parlant à leur famille ou à des proches, en évoquant clairement leur projet de venir en France (...) .

J'ai réussi à convaincre le service "action" de travailler avec ma direction technique lors d'une première opération conjointe en juillet2010 sur une équipe qui voulait faire sauter l'ambassade de France à Nouakchott, en Mauritanie. On a montré aux militaires que, grâce aux satellites, on pouvait faire une maquette 3D de leur lieu d'intervention [le campement djihadiste] au milieu de dunes, et donc leur permettre de choisir virtuellement leur chemin. Ils les ont éliminés à leur réveil.

Cette collaboration a été une vraie révolution au sein de la DGSE. Pour moi, en tant qu'ingénieur, c'était fondamental. Pour les commandos, faire venir des gens d'autres services avec eux, c'était une révolution. Car leur règle absolue, c'est: "Je fais tout moi-même." En guise de remerciement pour le succès de l'opération, le chef du service action m'a offert une des kalachnikovs prises aux djihadistes.»

Edward Snowden, «un traître qui nous a plutôt aidés»

Enfin, interrogé sur le lanceur d'alerte le plus connu de l'histoire du renseignement, M.Barbier a apporté une nuance inattendue au discours officiel tenu habituellement sur Edward Snowden, soulignant les services rendus à la France.

«Pour moi, Snowden est un traître à son pays, mais il n'a rien à voir avec Julian Assange [fondateur de WikiLeaks] . Les Américains ont fait de Snowden, contractuel extérieur de la NSA, un administrateur système. Alors que ceux qui font ce métier à la DGSE sont des fonctionnaires qui ont entre quinze et vingt ans d'ancienneté. La probabilité d'avoir un Snowden en France est très faible. Snowden a montré que l'espionnage entre alliés existait et que le matériel était piraté par les Américains comme celui vendu par l'entreprise Cisco, ce qui pose un problème d'indépendance pour la technologie. A ce titre, Snowden nous a plutôt aidés.»

New York Times
F.B.I. Files on Email Inquiry Show Grilling on Clinton's Judgment
Saturday, 03 September 2016
Byline: Eric Lichtblau

Washington - F.B.I. officials questioned Hillary Clinton extensively about her judgment in using her private email system to discuss classified drone strikes and in allowing aides to destroy large numbers of emails, before ultimately deciding she should not face criminal charges, according to investigative documents released Friday.
The documents provided a number of new details about Mrs. Clinton's private server, including what appeared to be a frantic effort by a computer specialist to delete an archive of her emails even after a congressional committee had requested they be preserved.

In a 3Â½-hour interview with the Justice Department's top counterintelligence officials on July 2, Mrs. Clinton defended her handling of the private email system by repeatedly saying she had deferred to the judgment of her aides, an F.B.I. summary of the interview showed.

Mrs. Clinton's use of the private server has shadowed her presidential campaign for a year and a half. And the newly disclosed records, while largely reinforcing what had already been known about the F.B.I. investigation, provided Republicans more ammunition to attack the Democratic nominee's judgment and honesty as she heads into the final, post-Labor Day phase of the campaign.

Among the other key findings in the F.B.I. documents:

â- Mrs. Clinton regarded emails containing classified discussions about planned drone strikes as "routine."

â- She said she was either unaware of or misunderstood some classification procedures.

â- Colin L. Powell, a former secretary of state, had advised her to "be very careful" in how she used email.

The F.B.I. documents show that an unnamed computer specialist deleted the archive of Mrs. Clinton's emails weeks after the existence of the private server became public in March 2015.

Days after The New York Times first reported that Mrs. Clinton had used a private email system exclusively as secretary of state, the House committee investigating the 2012 attacks in Benghazi, Libya, asked that her emails be preserved and subpoenaed those that were related to the attacks.

About three weeks later, however, the unnamed specialist "had an 'oh shit' moment" and realized that he had not destroyed an archive of emails that was supposed to have been deleted a year earlier, according to the F.B.I. report.

The specialist then used a program known as BleachBit to delete an unknown number of emails, according to the report. Mrs. Clinton told investigators that she was unaware that the aide had deleted the emails.

Dozens of times during her interview, Mrs. Clinton said she did not remember details about the server or guidance she had received on how to handle classified information.

In its summary of the investigation, the F.B.I. said that Mrs. Clinton had emailed Colin Powell, a former secretary of state, a day after she was sworn in to office about Mr. Powell's use of a personal email account when he was the country's top diplomat. Mr. Powell warned Mrs. Clinton that if she used her BlackBerry for official business, those emails could become "official record[s] and subject to the law."

Mr. Powell, apparently implying that he was cautious in his use of a personal email account, added: "Be very careful. I got around it all by not saying much and not using systems that captured the data." According to the summary of her interview, Mrs. Clinton said that she did not know exactly what Mr. Powell was saying in that email and that his message "did not factor into her decision to use a personal email account."

F.B.I. officials appear to have questioned Mrs. Clinton most aggressively about her judgment in using her private, unsecured system to get emails about how or where the Obama administration was planning to launch drone strikes against terrorism suspects, the documents indicated.

The F.B.I. showed her one email after another containing information about possible drone strikes that was considered classified. But Mrs. Clinton appeared almost blasÃ© in explaining her use of her private system to gather information on drone strikes.

After being shown one email that was redacted from the public release of her emails, Mrs. Clinton "stated deliberation over a future drone strike did not give her cause for concern regarding classification," according to the F.B.I. summary of the interview.

"Clinton understood this type of conversation as part of the routine deliberation process," the summary said. "Moreover, she recalled many conversations about future strikes that never occurred."

Mrs. Clinton's lawyer, David Kendall, declined to comment. In a statement, her campaign said it was pleased that the F.B.I. had made the documents public.

"While her use of a single email account was clearly a mistake and she has taken responsibility for it, these materials make clear why the Justice Department believed there was no basis to move forward with this case," the campaign said.

But Representative Jason Chaffetz, Republican of Utah and the chairman of the House Oversight and Government Reform Committee, said that the deletion of the emails violated an order his committee issued to Mrs. Clinton in 2012 and a subpoena issued by the Benghazi committee in 2015.

He said he planned to seek answers from Mrs. Clinton about the deletions. "These were not Hillary Clinton's emails -- they were government records, and this was potentially one of the largest security breaches at the State Department because they had all these years of security records that just went out the door," Mr. Chaffetz said. "It's a very black-and-white order. There's no wiggle room."

Reince Priebus, the chairman of the Republican National Committee, called the F.B.I. documents "a devastating indictment of her judgment, honesty and basic competency."

The F.B.I. released only small portions of its thick files on the Clinton investigation, and Senator Charles E. Grassley, the Iowa Republican who leads the Senate Judiciary Committee, accused the F.B.I. of withholding key documents -- including many unclassified ones -- from public view.

The selective release, he said, produced "an incomplete and possibly misleading picture of the facts without the other unclassified information that is still locked away from the public and even most congressional staff."

Mrs. Clinton told F.B.I. investigators that she had used a personal email server "out of convenience" and did not remember anyone raising legal concerns about the practice.

She also said that she "did not recall receiving any emails she thought should not be on an unclassified system," the F.B.I. documents say. "She relied on State officials to use their judgment when emailing her and could not recall anyone raising concerns with her regarding the sensitivity of the information she received at her email address," they say.

The document summarizing Mrs. Clinton's interview, known in the F.B.I. as a 302 report, runs only a dozen pages. The memorandum on the investigation is lengthier, and goes into greater detail about aspects of the case. The materials were presumably provided to James B. Comey, the F.B.I. director, who later decided to not recommend charges in the case.

A senior law enforcement official said the interview at F.B.I. headquarters had been intended "to fill the gaps" of what the F.B.I. did not know about why Mrs. Clinton used a private email server. Both documents were partly redacted, which slowed their release as the bureau sought to protect some information while satisfying the public's right to know.

The documents offer the most detailed account of Mrs. Clinton's role from the bureau's yearlong investigation into whether she or her aides broke the law by using a private system -- clintonemail.com -- to send tens of thousands of emails about government business, including classified matters.

Find out what you need to know about the 2016 presidential race today, and get politics news updates via Facebook, Twitter and the First Draft newsletter.

Sputnik News Service
German Intelligence Service Accused of 'Systematically' Violating Constitution
Saturday, 03 September 2016

Moscow - President of the German Federal Intelligence Agency (BND) Gerhard Schindler stands at the former monitoring base of the National Security Agency (NSA) in Bad Aibling, south of Munich, June 6, 2014.
The confidential report, dated March 2016, was brought to attention by public broadcasters NDR and WDR on Thursday evening. The 60-page study was carried out by Federal Data Protection Commissioner Andrea Voßhoff, who is responsible for ensuring that government agencies do not violate German citizens' rights when using their personal data.

"The BND systematically lifted and used personal data without a legal basis to do so," wrote the commissioner.

Voßhoff named a total of 12 violations of the law in seven spheres of activity, including obstruction of her own work.

"The BND massively and illegally blocked my ability to oversee it -- a comprehensive and efficient oversight on my part was therefore not possible. These are serious breaches of the law."

According to the report, the commissioner was blocked from checking so-called selectors -- the lists of the key concepts, which identify information such as phone numbers and email addresses used by the BND for targeted surveillance.

Voßhoff also called for shutting down large parts of the BND's data base in Bad Aibling, Bavaria. "According to law these databases must be immediately deleted. They must not be used anymore," the document said.

Opposition politicians said that the report confirmed what they had long been saying -- that the BND acts outside the law.

"The report cannot be misunderstood, either in its unusual level of clarity or in the extent of its criticism," said Konstantin von Notz, Green Party Member of Parliament and head of the parliamentary committee on the NSA.

Activities of the Germany's Federal Intelligence Service attracted the attention of the German public and the Bundestag after the scandalous revelations of Edward Snowden. BND management was accused of helping the American NSA, when it was spying on a global scale. It was revealed that the NSA tapped a number of European governments and organizations, including German ones.

The Australian Financial Review
PM's stance on China worries experts
Saturday, 03 September 2016
Byline: Aaron Patrick

Canberra - The government's top intelligence experts are concerned Prime Minster Malcolm Turnbull isn't taking their warnings about the security threat posed by China seriously enough and the former banker is relying on advice from outside experts.
Despite vetoing a Chinese bid for Sydney's electricity network this month, Mr Turnbull and some other cabinet ministers are reluctant to act on or receive warnings that China is engaging in spying on an "industrial scale" and that business secrets are among its top targets, three sources with senior contacts in the security services said.

"It is far more ambitious and better resourced than ever before," said Paul Monk, an intelligence and foreign affairs expert who headed China analysis for the Defence Intelligence Agency. "It's notorious with politicians that they find intelligence to be a new thing when they go into politics. It's things they would prefer not to know or suggest actions that can be embarrassing."

Mr Turnbull, who flies this weekend to Hangzhou, near Shanghai, for a Group of 20 leaders summit, has a history of pro-Chinese comments but has taken a tougher approach in public since he became prime minister.

A senior government source denied Mr Turnbull wasn't listening to advice from the intelligence and security services and said people outside the government would not know what was happening in his office.

Security experts say China has a well-resourced effort that uses cyber-espionage and human agents to steal Australian commercial secrets and obtain sensitive government information.

"There is an unspoken rule that we spy on each other," said Alan Dupont, a former military officer and defence analyst. "But to target in a massive way the business community of your trading partners and friends, in a way China has done, is unprecedented."

Mr Turnbull has frustrated the intelligence services by seeking outside advice and through an apparent scepticism towards some of his official briefings, the sources said.

The former Goldman Sachs partner has wide contacts in international business circles, did business in China before he moved into politics, and has a reputation for confidence in his own opinions. His intelligence advisers are uncertain about where he is seeking outside advice from, one source said.

The government official said Mr Turnbull's appointment two months ago of Frances Adamson as the secretary of the Department of Foreign Affairs and Trade, which works with the Australian Security Intelligence Service, which collects information overseas, showed the important he placed on advice about China from government experts. Ms Adamson was previously ambassador to China and Mr Turnbull's international relations adviser.

The Australian Security Intelligence Organisation declined to comment.

Intelligence leaders are conscious Mr Turnbull predicted five years ago that China would not use the expansion of its navy to become more militarily assertive and opposed the Labor government's strategy of preparing for a naval war in the South China Sea, where China is now turning islets into bases.

Now in office, Mr Turnbull has become less enthusiastic about China in public. He has criticised Chinese aggression in the South China Sea while emphasising China's importance to the Australian economy.

Some foreign policy experts, including former foreign minister Bob Carr, and business leaders are pushing Mr Turnbull to take a more friendly approach to China. They are opposed by the intelligence establishment, which appears staunchly anti-Chinese and pro-American.

Mr Turnbull has taken a low profile on foreign affairs since he became prime minister. But in 2011 he advocated that Australia prepare for the end of US military dominance in east Asia and said it was futile to try to contain China, a position more dovish than his four Liberal and Labor predecessors, John Howard, Kevin Rudd, Julia Gillard and Tony Abbott. "Suggestions that China's recent launch of one aircraft carrier and plans to build another are signs of a new belligerence are wide of the mark," Mr Turnbull said in a speech to the London School of Economics. "Prejudice is not a substitute for coolly rational analysis." Mr Turnbull, when communications minister, pushed for Chinese telecommunications equipment manufacturer Huawei to be allowed to help build the national broadband network. He was overruled by cabinet on national security grounds. As prime minister, he hasn't sought to open the contracts.

"There is still a lot of cynicism among senior officials about him," a government contractor with close links to the intelligence services said, referring to Mr Turnbull.

"Their view is they know about what the problems are but they are hesitant about pushing it too hard because the indications are that a couple of key ministers are not going to give them a good reception or think they know better.

"He is probably the first time since [Gough] Whitlam where we have had a prime minister where we don't know where he stands on national security grounds."

Australian Associated Press
Queensland police access social justice advocate's personal file 1,400 times
Saturday, 03 September 2016
Byline: Kym Agius

London - A Queensland Council for Civil Liberties social advocate has had her personal file accessed by Queensland police 1,400 times since 2008, in what she says is an abuse of privacy.
A social justice advocate has had her personal file accessed by Queensland police 1,400 times since 2008, which she says is an abuse of privacy.

The database, where her file was accessed, is a secure online tool capturing administrative and intelligence information, which police access during the course of their work, such as when checking a speeding motorist.

Queensland Council for Civil Liberties advocate Renee Eaves, who does not have a criminal record, submitted a Right to Information (RTI) request in to see how many times her Queensland Police Records and Information Management Exchange (QPRIME) file had been accessed.

She was startled to see it had been checked 1,400 from 2008 to May.

Ms Eaves said officers are supposed to give a reason each time they access a personal file, but she was not given any insight into the 1,400 cases.

When she submitted a second RTI application to see how many times her personal file was accessed between May and last month, Ms Eaves said it was knocked back on the grounds that there was an investigation underway into her first complaint.

She initially became suspicious when officers would ask her date of birth when advocating on behalf of police brutality victims, or officers who had issues with upper management.

"I was right in that there was a gross abuse of this system," Ms Eaves told 612 ABC Brisbane.

"It is being used against innocent members of the public who deserve and are entitled to privacy.

"It should only be for the eyes of only people who are authorised and have a reason to access that information."

Ms Eaves said police are now denying RTI requests by other members of the public.

"This goes to the very heart of transparency with the Queensland Police Service," Ms Eaves said.

"Once they realised that this questionable behaviour was going on, they started to shut down and close ranks and reject applications.

"Maybe this is just the tip of the iceberg?"

Police Commissioner needs to explain: QLS

Queensland Law Society president Bill Potts said he was concerned Ms Eaves' file was being accessed when she was not the subject of a police investigation.

"It is extraordinarily important they don't misuse, or at least have perception of misuse, of such details as well," he told ABC 612 Brisbane.

"Rather than have extended secrecy and hiding behind walls of bureaucratic paper, perhaps the Police Commissioner can have a look at it and give some reasons or an explanation as to why this is happened.

"And if it has happened, and there is no proper basis for it, then the people who are doing this really seriously should be looked at.

Queensland Police have been contacted for comment.

New York Times
Does the Messaging Service Telegram Take Privacy Too Far?
Tuesday, 06 September 2016
Byline: Celestine Bohlen

Paris - The encryption of digital information is considered the best protection against hackers, snoops or potential enemies looking to poke around into private exchanges of all sorts.
That is why technology experts and privacy advocates in Europe went on high alert last month when the French Ministry of the Interior suggested that it might limit encryption as part of the fight against terrorist threats.

That fear abated somewhat on Aug. 23 when the French interior minister, Bernard Cazeneuve, at a joint news conference with his German counterpart, Thomas de Maizière, stepped back from a more sweeping proposal. Instead, he pressed for a coordinated international effort to get messaging services to comply with judicial warrants for information.

Mr. Cazeneuve named one such service: Telegram, a three-year-old messaging application, that is a favorite of the Islamic State, also known as ISIS or ISIL, which has claimed responsibility for a series of terrorist attacks in Europe in recent years.

According to news reports, killers in two attacks in France this summer -- one against two police officers and the other in a church in Normandy, during which they slit the throat of a Catholic priest -- were exchanging messages on Telegram, even boasting of their plans. In August, Telegram was again used in two abortive cases, one involving a 16-year-old girl.

Telegram's vaunted privacy safeguards, involving multiple servers in different countries, are designed to prevent access to information about its users, even by the service itself.

At the news conference, Mr. Cazeneuve admitted as much but claimed that French investigators, armed with a court order, had been unable to even contact "an interlocutor" at Telegram.

In response to a query on his Telegram account, Pavel Durov, co-founder of the service, batted back the widely reported French claims.

"We haven't received any such request and have no idea what the French officials are after," he wrote. "In any case, Telegram Secret Chats and information on them are not logged on our servers."

Last November, after attacks in Paris that left 130 people dead, Telegram scrubbed 78 Islamic State-related public channels hosted on its servers, but Mr. Durov insisted that privacy would remain paramount on the rest of the service.

Mr. Durov's background explains his die-hard libertarian attitude on privacy. He left his native Russia in 2014 after refusing to give intelligence information about Ukrainian protesters.

However, most privacy advocates agree that messaging services should cooperate with court-issued warrants, even if they are unable to provide investigators with complete information about their users.

"There is an issue with Telegram," said Mounir Mahjoubi, president of the National Digital Council, an independent advisory group established by former President Nicolas Sarkozy that focuses on privacy issues. "They had done everything to make it a technological nightmare to find where their server is."

At a time of heightened public anxiety over terrorism, technology companies and privacy advocates are wary about politicians looking to mandate "back door" access to encrypted data.

This, they say, would not only violate privacy rights but put the wider public at an even greater risk, leaving users even more vulnerable to terrorists and other criminals.

Mr. Mahjoubi, for one, supports alternative approaches, such as an international network that could call on judges in individual countries to swiftly react to requests from antiterrorism investigators.

These ideas also are also backed by the Computer and Communications Industry Association, a lobbying organization that counts Amazon, Google and Microsoft among its members.

"Cyberspace blurs the notion of national jurisdictions, and companies are caught in the middle," said Christian Borggreen, the organization's Europe director. "The tech industry encourages like-minded nations to develop international frameworks for quicker response to law enforcement requests while respecting users' right and the rule of law."

That kind of targeted approach -- aimed at criminals, not at privacy -- would be more effective than a blank check for law enforcement to break open encoded messages, Mr. Mahjoubi said.

"I am deeply and heartily against any effort to limit encryption," he said, "and I will fight my whole life against that possibility."

Fars News Agency
Supreme Leader Calls for Reinvigoration of Iran Cyberspace Activities to Confront Enemies' Threats
Tuesday, 06 September 2016

Tehran - Supreme Leader of Islamic Revolution Ayatollah Seyed Ali Khamenei underlined the vital importance of cyberspace's potentials and capacities in the promotion of the country in various fields and also in defusing enemies' threats.
"The enemy is seeking to pervert devoted and righteous youths from the essence of religion; today this is being done across the cyber world," Ayatollah Khamenei said on Tuesday on the occasion of the commencement of education at seminaries across Iran.

He noted that confronting this scheme was the first and foremost responsibility of the clergymen, and said, "Seminaries and religious scholars should equip themselves with the capability to confront the massive enemy army."

The Supreme Leader said that the cyber world was a simultaneous source of blessing and cursing.

Ayatollah Khamenei reiterated that Iran's Supreme Council of Cyberspace was created toward lending concentration to such a goal.

On March 7, 2015, Ayatollah Khamenei assigned the administration of former president Mahmoud Ahmadinejad with the task of establishing the Supreme Council of Cyberspace in an effort to safeguard national and cultural values as well as ensuring the safety of the Internet in Iran.

The Council is now headed by President Hassan Rouhani and is comprised of high-ranking officials.

In September 2015, Ayatollah Khamenei underlined the vital importance of cyberspace's potentials and capacities in the promotion of the country in various economic, cultural, and political fields.

"Using capability and talents of the country's youth and through making right policies and adopting well-calculated and coordinated measures and without losing time, let's move towards ridding the cyberspace of passivity and having active, influential presence and production of reliable and attractive Islamic content," said the Supreme Leader in a meeting with Head of Supreme Council of Cyberspace (President Rouhani) and members of the Council.

Referring to the wide-scale impact of cyberspace, as an extraordinary soft power on various fields, such as culture, politics, lifestyle, faith, religious ideology and morals, Ayatollah Khamenei underlined appropriate and careful designs to guarantee intellectual and ethical security of the society in the field.

The requisite for active and influential presence in the cyberspace is concentration on the decision making, seriousness in execution without wasting time, coordination among organs and avoiding parallelism and confrontation, concluded the Supreme Leader.

He also underlined that planning and support of government, especially the Science and Technology Department of the Presidential Office, for expansion of the Information Technology (IT) is highly necessary.

In July 2014, Ayatollah Khamenei appreciated Iranian scientists for their rapid progress and achievements, and underlined the necessity for the non-stop continuation of this trend.

The great significance of keeping up the rapid pace of the country's scientific movement is due to the fact that it is a main factor in shaping up both Iran's future fate and that of the Islamic world, Ayatollah Khamenei said in a meeting with hundreds of Iranian university professors and elites in Tehran at the time.

24 Heures (Suisse)
Qui a passé à tabac le patron de Swiss Space Systems?
Monday, 05 September 2016

Byline: Journaliste maison

Payerne, Suisse - Le Vaudois qui veut révolutionner le lancement de satellites s'est fait sauvagement agresser
Qui a passé à tabac le patron de Swiss Space Systems? « La pression était forte depuis longtemps: intimidations, lignes sur écoute, espionnage. C'est de la folie, du vrai James Bond. » Au bout du fil, cet investisseur du projet Swiss Space Systems (S3) est consterné. Pascal Jaussi, 40 ans, patron de la société basée à Payerne, qui ambitionne de lancer des satellites depuis des navettes spatiales, est au CHUV sous bonne garde et dans un état sévère. Le jeune entrepreneur souffre de graves brûlures sur 25% du corps, il a été victime d'une strangulation et de divers coups. Une agression mystérieuse intervenue la semaine dernière dans un bois de la Broye fribourgeoise, où deux individus armés ont forcé Jaussi à se rendre avant de bouter le feu à sa voiture. Une enquête est ouverte pour lésions corporelles graves, incendie intentionnel et contrainte.Depuis plusieurs mois, le fondateur de S3 confiait à ses proches et à la police se sentir menacé. Le secteur spatial conjugue des enjeux financiers et stratégiques importants, et l'arrivée d'un acteur indépendant est génératrice de tensions. L'an dernier, les locaux de S3 avaient été saccagés, des inconnus arrosant les ordinateurs de la société à la lance à incendie.Ce printemps, S3 avait acquis un Airbus A340 pour effectuer des vols « zéro gravité » dès cet hiver. Qui a passé à tabac le patron de Swiss Space Systems?Le Vaudois qui veut révolutionner le lancement de satellites s'est fait sauvagement agresserVaud et régions, page 15Les détailsde l'agression sauvage dont a été victime Pascal JaussiLe projetde Swiss Space Systems, une révolution spatiale

Le Monde
DGSE L'espion qui parlait trop
Monday, 05 September 2016
Byline: Journaliste maison

Paris - Lors d'une anodine réunion d'anciens élèves d'une grande école d'ingénieurs, Bernard Barbier, personnage central de la DGSE durant dix ans, a livré en public, dans une intervention filmée, quelques secrets d'Etat, notamment sur la guerre cybernétique.
Comment les Etats-Unis ont espionné l'Elysée, par le biais des logiciels malveillants glissés sur Facebook par la NSA. Comment la France a monté ses équipes de " hacking " et créé son propre logiciel malveillant, baptisé " Babar ". Comment Bernard Barbier a proposé une fusion entre la DGSE et son homologue allemand, qui a été rejetée pour des raisons politiques. Comment les révélations d'Edward Snowden ont aidé la France à se protéger de l'espionnage " ami " des Américains. Ces révélations intempestives ont agacé en haut lieu. Le Monde a pu en prendre connaissance.

ABC News
Obama Met With Putin, Said Hackers Shouldn't Create a Cyber 'Wild Wild West'
Monday, 05 September 2016

Byline: Jordyn Phelps

New York - President Obama addressed his tense, 90-minute-long meeting with Russian President Vladimir Putin on the sidelines of the G20 in a press conference on Monday. The two leaders apparently held fast to their positions on hot button issues like cyber-security and brokering a cease- fire in Syria. Russian hackers having been implicated in some current cyber threats and security issues was a key topic. Though Obama didn't identify specific instances, he said "we have had problems with cyber intrusions from Russia in the past" and that the goal is to not to duplicate a "cycle of escalation" that has occurred in arms races of the past.

"What we cannot do is have a situation where this becomes the wild, wild West, where countries that have significant cyber capacity start engaging in unhealthy competition or conflict through these means," the president said. He added that nations have enough to worry about in the realm of cyber attacks from non-state actors without nation-states engaging in hacking against one another.

Obama also said the two countries "haven't yet closed the gaps" that remain to reach a meaningful ceasefire deal for Syria but said that they had a productive conversation.

The president said he has instructed Secretary of State John Kerry to continue working with Russian Foreign Minister Lavrov to broker a deal in the coming days.

Describing the current situation in Syria as one where the Assad regime is again "bombing with impunity," Obama emphasized the need to reach a compromise quickly and provide needed humanitarian relief for civilians caught in the crossfire of the raging civil war. He also said the two countries should focus on common enemies like ISIS and Al Nusra.

Washington Post
Intelligence community investigating covert Russian influence operations in the United States
Monday, 05 September 2016
Byline: Multiple reporters

Washington - U.S. intelligence and law enforcement agencies are probing what they see as a broad covert Russian operation in the United States to sow public distrust in the upcoming presidential election and in U.S. political institutions, intelligence and congressional officials said.
The aim is to understand the scope and intent of the Russian campaign, which incorporates cyber-tools to hack systems used in the political process, enhancing Russia's ability to spread disinformation.

The effort to better understand Russia's covert influence operations is being spearheaded by James R. Clapper Jr., the director of national intelligence. "This is something of concern for the DNI," said Charles Allen, a former longtime CIA officer who has been briefed on some of these issues. "It is being addressed."

A Russian influence operation in the United States "is something we're looking very closely at," said one senior intelligence official who, as others interviewed, spoke on the condition of anonymity to discuss a sensitive matter. Officials are also examining potential disruptions to the election process, and the FBI has alerted state and local officials to potential cyberthreats.

The official cautioned that the intelligence community is not saying it has "definitive proof" of such tampering, or any Russian plans to do so. "But even the hint of something impacting the security of our election system would be of significant concern," the official said. "It's the key to our democracy, that people have confidence in the election system."

The Kremlin's intent may not be to sway the election in one direction or another, officials said, but to cause chaos and provide propaganda fodder to attack U.S. democracy-building policies around the world, particularly in the countries of the former Soviet Union.

U.S. intelligence officials described the covert influence campaign here as "ambitious" and said it is also designed to counter U.S. leadership and influence in international affairs.

One congressional official, who has been briefed recently on the matter, said "Russian 'active measures' or covert influence or ma-nipu-la-tion efforts, whether it's in Eastern Europe or in the United States" are worrisome.

It "seems to be a global campaign," the aide said. As a result, the issue has "moved up as a priority" for the intelligence agencies, which include the FBI and Department of Homeland Security as well as the CIA and the National Security Agency.

Some congressional leaders briefed recently by the intelligence agencies on Russian influence operations in Europe, and how they may serve as a template for activities here, have been disturbed by what they heard.

After Senate Minority Leader Harry M. Reid (D-Nev.) ended a secure, 30-minute phone briefing by a top intelligence official recently, he was "deeply shaken," according to an aide who was with Reid when he left the secure room at the FBI's Las Vegas headquarters.

The Russian government hack of the Democratic National Committee, disclosed by the DNC in June but not yet officially ascribed by the U.S. government to Russia, and the subsequent release of 20,000 hacked DNC emails by WikiLeaks, shocked officials. Cyber-analysts traced its digital markings to known Russian government hacking groups.

"We've seen an unprecedented intrusion and an attempt to influence or disrupt our political process," said Rep. Adam B. Schiff (Calif.), the ranking Democrat of the House Intelligence Committee, speaking about the DNC hack and the WikiLeaks release on the eve of the Democratic convention. The

disclosures, which included a number of embarrassing internal emails, forced the resignation of DNC Chairwoman Debbie Wasserman Schultz.

Members of both parties are urging the president to take the Russians to task publicly.

Sen. Ben Sasse (R-Neb.) in a statement urged President Obama to publicly name Russia as responsible for the DNC hack and apparent meddling in the electoral process. "Free and legitimate elections are non-negotiable. It's clear that Russia thinks the reward outweighs any consequences," he wrote. "That calculation must be changed. .?.?. This is going to take a cross-domain response -- diplomatic, political and economic -- that turns the screws on [Russian President Vladimir] Putin and his cronies."

Administration officials said they are still weighing their response.

Russia has denied that it carried out any cyber-intrusions in the United States. Putin called the accusations against Russia by U.S. officials and politicians an attempt to "distract the public's attention."

"It doesn't really matter who hacked this data from Mrs. Clinton's campaign headquarters," Putin said, referring to Democratic presidential nominee Hillary Clinton, in an interview with Bloomberg News. "The important thing is the content was given to the public."

The Department of Homeland Security has offered local and state election officials help to prevent or deal with Election Day cyber-disruptions, including vulnerability scans, regular actionable information and alerts, and access to other tools for improving cybersecurity at the local level. It will also have a cyber-team ready at the National Cybersecurity and Communications Integration Center to alert jurisdictions if attacks are detected.

Last month, the FBI issued an unprecedented warning to state election officials urging them to be on the lookout for intrusions into their election systems and to take steps to upgrade security measures across the voting process, including voter registration, voter roles and election- related websites. The confidential "flash" alert said investigators had detected attempts to penetrate election systems in several states.

Arizona, Illinois and both the Democratic and Republican parties, as well as the DNC, have been the victims of either attempted or successful cyberattacks that FBI agents with expertise in Russian government hacking are investigating.

Federal law enforcement and local election officials say the decentralized nature of the voting process, which is run by states and counties, makes it impossible to ensure a high level of security in each district.

"I have a lot of concern" about this year's election, said Ion Sancho, the longtime supervisor of elections in Leon County, Fla. "America doesn't have its act together," said Sancho, who has authorized red team attacks on his voting system to identify its vulnerabilities. "We need a plan."

Sancho and others are particularly concerned about electronic balloting from overseas that travels on vulnerable networks before landing in the United States and efforts to use cyberattacks to disrupt vote tabulations being transmitted to state-level offices. Encryption, secured paper backups and secured backup computers are critical, he said.

Tom Hicks, chairman of the U.S. Election Assistance Commission, an agency set up by Congress after the 2000 Florida recount to maintain election integrity, said he is confident that states have sufficient safeguards in place to ward off intrusions. He noted that electronic balloting from overseas is conducted by email, not through online voting machines. The overseas voter "waives their right of privacy" by emailing the ballot, which is tabulated by election officials. The email may still be hacked, but it is not a systemic risk, he said.

Recently, Homeland Security Secretary Jeh Johnson said he favors designating the various voting systems used in the country's 9,000 polling places as "critical infrastructure" -- in other words as vital to the nation's safe functioning as nuclear power plants and electrical power grids.

Such a designation could mean increased DHS funding to localities to help ensure that voter registration, ballots and ballot tabulation remains free from interference. But it won't happen before the November elections, federal and local officials said.

Russia has been in the vanguard of a growing global movement to use propaganda on the Internet to influence people and political events, especially since the political revolt in Ukraine, the subsequent annexation of Crimea by Russia, and the imposition of sanctions on Russia by the United States and the European Union.

The Baltic states, Georgia and Ukraine have been subject to Russian cyberattacks and other hidden influence operations meant to disrupt those countries, officials said.

"Our studies show that it is very likely that [the influence] operations are centrally run," said Janis Sarts, director of the NATO Strategic Communications Center of Excellence, a Riga, Latvia-based research organization.

He also said there is "a coordinated effort involving [groups using] Twitter and Facebook and networks of bots to amplify their message. The main themes seem to be orchestrated rather high up in the hierarchy of the Russian state, and then there are individual endeavors by people to exploit specific themes."

Sarts said the Russian propaganda effort has been "successful in exploiting the vulnerabilities within societies." In Western Europe, for instance, such Russian information operations have focused on the politically divisive refugee crisis.

On the eve of a crucial post-revolution presidential vote in Ukraine in 2014, a digital assault nearly crippled the country's Central Election Commission's website. Pro-Moscow hackers calling themselves the CyberBerkut claimed responsibility, saying they were not state-affiliated, but the authorities in Kiev blamed Moscow. The Russians used a "denial of service" technique, flooding the commission's Web server with a high volume of requests, which was meant to slow down or disable the network.

The Register (UK)
Parliament's back for Snoopers' Charter. Former head of GCHQ talks to El Reg
Monday, 05 September 2016
Byline: Alexander J. Martin

London - Parliament has returned from recess (only for a fortnight before conference season begins) and the House of Lord's committee stage examination of the Investigatory Powers Bill will resume this afternoon.
The upper chamber had been waiting for the publication of a review of the bill's bulk powers, which had been led by the independent reviewer of terrorism legislation, David Anderson QC.

Anderson's report was published while the politicians were on their holidays, and although it found that there was no proven case GCHQ needs to engage in bulk hacking missions, it was otherwise overwhelmingly supportive of the bulk powers provided for in the Snoopers' Charter.

Anderson made what he called a "single, major, recommendation" -- the creation of a Technical Advisory Panel to monitor how developments in technology affect the investigatory powers.

An amendment to the bill [PDF] proposed by Lord Rosser would create such a panel to advise both the Secretary of State and the Investigatory Powers Commissioner on "the impact of changing technology on the exercise of the investigatory power; and the availability and development of techniques to use investigatory powers while minimising interference with privacy."

Those bulk hacking missions were addressed last week at a panel convened by the Chartered Institute of IT. Academics, National Crime Agency representatives, and Sir David Omand -- the former director of GCHQ and visiting professor at KCL -- discussed the difficulties that traditional law enforcement techniques encountered when attempting to tackle cybercrime.

Corresponding with The Register, Sir David explained how in his experience such bulk hacking powers were necessary for law enforcement purposes on the internet, rather than just being necessary for national security reasons.

Omand wrote: "Over 20 years ago Parliament in the 1994 Intelligence Services Act wisely recognised the added value that GCHQ and MI6 could bring to the fight against international crime, and made the prevention and detection of serious crime a statutory function for the agencies."

"The recent serious rise in global cybercrime by organised criminal groups based in jurisdictions that do not cooperate with law enforcement has only reinforced the importance of having the specialist techniques and international liaisons of the secret agencies available to support the investigations of law enforcement, for example in helping to dismantle child abuse networks," he explained. "And where it is not possible to bring the perpetrators before a Court, the Agencies may be able to help law enforcement reduce the potential harm to the public by disruption of the criminal operations."

Disrupting cybercriminals through hacking involves sinkholing malware strains, or borking all of the nasties' command-and- control nodes so they can't communicate any more. Such targeted hacking operations are not only available to the spooks, but to police forces too.

As terror law reviewer Anderson explained in the 200-plus page report: "There is no requirement for a link to the interests of national security: it is enough that the warrant be necessary for the purpose of preventing or detecting serious crime, or (in some cases) preventing or mitigating death, injury or damage to a person's physical or mental health."

Sir David, meanwhile, in his correspondence with The Register, considers that old- fashioned Snowden-revelation surveillance couldn't be understated in the fight against cybercrime:

Less publicised has been the part that bulk access to digital communications now plays in detecting cyber attacks. By scanning the technical detail of Internet communications GCHQ has been able to pick up the electronic signatures characteristic of cyber exploits, including new attacks, and share the warnings with industry partners.

95% of the cyber attacks on the UK detected by the intelligence community in the last 6 months came from the collection and analysis of bulk data. Right now GCHQ is monitoring cyber threats from high-end adversaries against 450 companies across the aerospace, defence, energy, water, finance, transport and telecoms sectors.

According to Omand, GCHQ dealt with more than 200 "cyber national security incidents" each month last summer, doubling its work-load on the previous year. This involved assisting Blighty's law enforcement agencies tackle a number of "high-profile operations against pernicious cybercrime malware threats, like Dridex, Shylock and GameOver Zeus."

So if 2013 and 2014 saw the revelation of the capability of the digital revolution to supply intelligence on those who mean us harm, and if 2015 and 2016 sadly saw the recognition of the legitimacy of the demand for such intelligence to counter terrorists and cyber criminals, then this also has to be the year in which Parliament passes the Investigative Powers Bill, with all its added safeguards and judicial oversight, to allow this vital activity to continue.

These issues, Lord Rosser's amendment, and other arguments will be considered when the House of Lords convenes to debate these matters this afternoon

Press TV

Iran's Leader urges confronting enemy schemes in cyberspace

Wednesday, 07 September 2016

Section: general

Tehran - The Leader of the Islamic Revolution Ayatollah Seyyed Ali Khamenei has called attention to attempts by Iran's enemies to undermine Islamic values by making inroads across the cyberspace, urging the clergy to confront such attempts.
Ayatollah Khamenei made the remarks on Tuesday on the occasion of the commencement of education at seminaries countrywide. The Leader said the enemy is seeking to pervert devoted and righteous youths from the essence of religion.

"Today, this is being done across the cyber world," Ayatollah Khamenei said, noting that confronting this scheme was the first and foremost responsibility incumbent upon the clergy. "Seminaries and religious sages should equip themselves with the capability to confront the massive enemy army."

The cyber world, the Leader asserted, was a simultaneous source of blessing and cursing, noting that its potentials had to be rightly availed of toward the large-scale promotion of Islamic concepts.

"Iran's Supreme Council of Cyberspace was created toward lending concentration" to such a goal, the Leader said.

On March 7, 2015, Ayatollah Khamenei assigned the administration of former president Mahmoud Ahmadinejad with the task of establishing the Supreme Council of Cyberspace in an effort to safeguard national and cultural values as well as ensuring the safety of the Internet in Iran.

The Council is now headed by President Hassan Rouhani and is comprised of high-ranking officials.

Jerusalem Post

Israeli start-up 'imitates the way computer hackers think'

Wednesday, 07 September 2016

Byline: Staff Report

Section: general

Jerusalem - An Israeli start up firm that imitates the way hackers think in order to offer its customers cyber security has raised $3.5 million in financing, Globes reported on Sunday. Including the current round of financing, the company has raised a total of $6.2 million since its founding.
The company described its CTO Matan Azugi as one of the world's leading ethical hackers, according to Globes. Using Azugi's skills and knowledge, the company provides cyber security by using an algorithm which imitates the way a hacker thinks. Cronus is chaired by former head of the Israeli Air Force, Eitan Ben Eliyahu.

The company's current round of financing, according to Globes, has come from US fund, Janvest Capital Partners, a European investor and a Hong Kong investor. The new funding is expected to allow the Haifa-based company to extend its activities to the US. It is currently active in Germany, Hong Kong and the UK. The company also provides cyber security services to local firms, including the First National Bank of Israel.

Asharq Al-Awsat

U.S. Fears E-Piracy Could Manipulate Electoral Results

Wednesday, 07 September 2016

Byline: Heba El Koudsy

Section: general

Washington - U.S. intelligence and law enforcement agencies are investigating several attempts to break through the systems and electronic voting records for the U.S. coming presidential elections, which will be held on November 7.
The agencies are concerned that these cyber attempts might affect the results of the elections between Republican candidate Donald Trump and Democratic candidate Hillary Clinton.

They see these attacks as a broad covert Russian operation in the United States to sow public distrust in the upcoming presidential election and in U.S. political institutions.

The effort to better understand Russia's covert influence operations is being coordinated by James R. Clapper Jr., the director of national intelligence.

"This is something of concern for the DNI," said Charles Allen, a former longtime CIA officer who has been briefed on some of these issues. "It is being addressed."

According to a report by the "Washington Post," the FBI, CIA, National Security Agency (NSA) and Department of Homeland Security are all involved in the probe of what officials say is an "ambitious" Russian cyber-operation to influence both national and local politics in the United States.

A top intelligence official told the newspaper that the agencies do not yet purport to have "definitive proof" of Russian interference.

"But even the hint of something impacting the security of our election system would be of significant concern," the official said.

FBI, last week, warned by issuing a statement confirming it has proofs that foreign hackers were able to hack database in Arizona and Illinois states.

The Russian government hack of the Democratic National Committee, disclosed by the DNC in June but not yet officially ascribed by the U.S. government to Russia, and the subsequent release of 20,000 hacked DNC emails by WikiLeaks, shocked officials. Cyber-analysts traced its digital markings to known Russian government hacking groups.

"We've seen an unprecedented intrusion and an attempt to influence or disrupt our political process," said Rep. Adam B. Schiff, Calif., the ranking Democrat of the House Intelligence Committee, speaking about the DNC hack and the WikiLeaks release on the eve of the Democratic convention.

The disclosures, which included a number of embarrassing internal emails, forced the resignation of DNC Chairwoman Debbie Wasserman Schultz.

Russia denied that it carried out any cyber- intrusions in the United States. Putin called the accusations against Russia by U.S. officials and politicians an attempt to "distract the public's attention."

Australian Associated Press

Govt sets defence innovation priorities

Wednesday, 07 September 2016

Byline: Staff reporter

Section: general

Canberra - The government has spelled out priorities for improving defence capabilities through clever ideas, with boosting intelligence, surveillance, electronic warfare and cyber heading the list.
Defence Industry Minister Christopher Pyne says the new $640 million Defence Innovation Hub to be launched later this year will drive growth in defence industry innovation.

The government has set six areas for research and innovation, with three given top priority for 2016-17.

"In the intelligence, surveillance, reconnaissance, electronic warfare, space and cyber capability stream we will focus on improving intelligence collection, analysis and dissemination," he said in the keynote address to the Land Forces conference dinner in Adelaide.

Mr Pyne said that would include biometric data and cyber innovation to support intelligence capability development.

Next priority is capabilities to better enable defence operations, including command and control systems, satellite communication and simulation.

Third priority will be capabilities to enhance land combat and amphibious warfare, including remotely operated armed reconnaissance aircraft.

"Of course, the beauty of innovation is that we do not yet know what great ideas or fields will yield us the most success," he said.

Mr Pyne said he wanted to ensure that when the government spent taxpayer money, it was spent on what serving men and women need.

That's the best possible equipment with funding invested in Australia where possible.

"We are determined to use the defence dollar to drive a high technology, advanced manufacturing future," he said.

Mr Pyne said the relationship with industry must change.

"We must involve industry earlier in our capacity development processes to understand just what they can contribute," he said.

Mr Pyne said Defence, industry and state and territory governments all had to work together to maximise return on investment and guarantee the best capability available and support for the Australian Defence Force

Adelaide Advertiser

Rare gift as undercover G20 spooks go under the covers (Canada)

Wednesday, 07 September 2016

Byline: Tory Shepherd

Section: general

Vientiane - Gifts, "honeypots" and cyber hacking are among the weapons used by the Chinese to hunt top-secret information at the G20 summit.
Delegates at the global economic forum were warned not to accept presents such as USB sticks that could gather data, and to resist overly friendly people who might be out to scam secrets.

Australians were warned about "honeypots" - women or men who might try to seduce them in order to steal information or plant a listening device. Another strategy is to give a gift with a bug inside.

Prime Minister Malcolm Turnbull and the Australian delegation travelled to Hangzhou in China for the summit - and for those without encrypted communications networks, the main internet option was the easily hacked official G20 network.

Among the more old-fashioned espionage efforts were "tourists" who looked remarkably un-touristy as they focused long lenses on jour-nalists along Hangzhou's fam-ous riverfront.

As Mr Turnbull addressed the crowd at the B20 business leaders' meeting, a man in uniform sidled up behind journalists to read what they were writing. News Corp Australia was warned not to write anything about spies while in China because of the possibility of being detained or not being allowed a visa in the future.

Peter Jennings, the Australian Strategic Policy Institute's executive director, said honeypots were "part and parcel of espionage", adding: "(Sex) has often been used as a way of trying not only to get people in but then to create a suitable basis (for blackmail)."Russian ships sailed close to the coast during the Brisbane G20 and in 2013 Russia reportedly spied on other countries at the G20 by giving out "Trojan Horse" USB sticks, while Canada was accused of allowing spying at the 2010 G20.

New York Times

After Edward Snowden Fled U.S ., Asylum Seekers in Hong Kong Took Him In

Wednesday, 07 September 2016

Byline: Patrick Boehler

Section: general

Hong Kong - When the 42-year-old Filipino woman opened the door of her tiny Hong Kong apartment three years ago, two lawyers stood outside with a man she had never seen before. They explained that he needed a place to hide, and they introduced him as Edward Snowden.
"The first time I see him, I don't know who he is," the woman, Vanessa Mae Bondalian Rodel, recalled in an interview. "I don't have any idea."

Ms. Rodel is one of at least four residents of Hong Kong who took in Mr. Snowden, the former National Security Agency contractor, when he fled the United States in June 2013. Only now have they decided to speak about the experience, revealing a new chapter in the odyssey that riveted the world after Mr. Snowden disclosed that the N.S.A. had been monitoring the calls, emails and web activity of millions of Americans and others.

At the time, governments and news outlets were scrambling to find the source of the leaks, which were published in The Guardian and The Washington Post. In an interview recorded in a hotel room, Mr. Snowden identified himself and revealed he was in Hong Kong. Then he went into hiding. About two weeks later he turned up in Moscow.

It was never clear where Mr. Snowden was holed up during those critical days after leaving his room at the five-star Mira Hotel, when the United States was demanding his return. As it turns out, he was staying with Ms. Rodel and others like her -- men and women seeking political asylum in Hong Kong who live in cramped, substandard apartment blocks in some of the city's poorest districts.

They were all clients of one of Mr. Snowden's Hong Kong lawyers, Robert Tibbo, who arranged for him to stay with them.

Ms. Rodel said Mr. Snowden slept in her bedroom while she and her 1-year-old daughter moved into their apartment's only other room. Not knowing what he would eat, she bought him an Egg McMuffin and an iced tea from McDonald's.

"My first impression of his face was that he was scared, very worried," she recalled.

Ms. Rodel said her unexpected guest "was using his computer all day, all night." She said that she did not have internet service but that Mr. Tibbo provided him with mobile access.

On Mr. Snowden's second day there, he asked Ms. Rodel whether she could buy him a copy of The South China Morning Post, the city's main English-language newspaper, she said. When she picked up the paper, she saw his picture on the front page.

"Oh my God, unbelievable," she recalled saying to herself. "The most wanted man in the world is in my house."

Jonathan Man, another of Mr. Snowden's lawyers in Hong Kong, said that he had initially considered hiding him in a warehouse but that he and Mr. Tibbo quickly dismissed the idea. Instead, after taking him to the United Nations office that handles refugee claims in Hong Kong and filing an application, they brought him to the apartment of a client seeking asylum.

"It was clear that if Mr. Snowden was placed with a refugee family, this was the last place the government and the majority of Hong Kong society would expect him to be," Mr. Tibbo said. "Nobody would look for him there. Even if they caught a glimpse of him, it was highly unlikely that they would recognize him."

There are about 11,000 registered asylum seekers living in Hong Kong, mostly from South and Southeast Asia. They generally cannot work legally and survive on monthly stipends that rarely cover living costs.

Mr. Tibbo said he turned to these clients for help in part because he expected them to understand Mr. Snowden's plight. "These were people who went through the same process when they were fleeing other countries," he said. "They had to rely on other people for refuge, safety, comfort and support."

He noted that Mr. Snowden was not wanted by the Hong Kong police at the time and that he had advised his clients to cooperate with the police if they showed up. He said his clients had decided come forward in the hope that the publicity would put pressure on the Hong Kong authorities to expedite their applications for refugee status and resettlement.

Ms. Rodel, for example, has been waiting nearly six years for a final decision on her application, which she declined to describe.

After a few days with Ms. Rodel and her daughter, Mr. Snowden spent a night with Ajith Pushpakumara, 44, who said he fled to Hong Kong after being chained to a wall and tortured for deserting the army in his native Sri Lanka.

Mr. Pushpakumara said he had listened to online radio broadcasts about Mr. Snowden and was surprised to suddenly find him in the dingy apartment that he shared with several men. He realized Mr. Snowden was in the same situation he was, hiding in a small room. "I was worried about him," he said.

Supun Thilina Kellapatha, his wife and their toddler also sheltered Mr. Snowden, putting him up for about three days in their 250-square-foot apartment.

Mr. Kellapatha, 32, who said he sought protection in Hong Kong after being tortured in Sri Lanka, described their guest as a tired man who was unfailingly polite.

"He said, 'You are a good man,' " when he arrived at the apartment, Mr. Kellapatha recalled. "But I feel he is better than me, because he respected me."

Mr. Kellapatha and his wife, Nadeeka Dilrukshi Nonis, said they were not worried about hosting Mr. Snowden. "I don't think I take the risk," he said. "He is the one who take the big risk."

When Mr. Snowden left, he left the couple $200 under a pillow, which they said they used to buy necessities for their daughter. "Sometimes I tell Supun, maybe he forgot us," Ms. Nonis said. "I want to tell him, 'Edward, how are you? We will never forget you.' "

National Post

Meet the Canadian who hid Snowden

Wednesday, 07 September 2016

Byline: Theresa Tedesco

Section: general

Hong Kong - It's mid-afternoon and Robert Tibbo has sweat through his second shirt of the day in the sweltering subtropical humidity of the Hong Kong summer.
Sitting in a small, non-descript conference room on the ninth floor of the High Court building in Central Hong Kong, the Canadian- born barrister is one of the busiest human rights lawyers in the Chinese city-state, and the strain of coming to the constant aid of more than 70 refugee clients who depend on him for more than just their asylum cases is showing.

In recent days, Tibbo has dealt with eviction notices, improper charges on utility bills and general complaints about not having enough money to buy groceries, which he temporarily rectifies by reaching into his own pocket.

"Good lawyers are hard to find, but one with a big heart is even more rare," said Jonathan Man, a solicitor at Hong-based Ho, Tse Wai & Partners who has worked on numerous cases with Tibbo.

"He is somebody who has devoted his life to protecting refugees and people seeking asylum and he takes that very seriously," added Laura Poitras, a U.S. journalist and Oscar-winning documentary director who has worked with Tibbo.

Despite the accolades, the 52-year-old Montreal native is actually a relative newcomer to the high-minded world of human rights law. Tibbo's bread and butter after he obtained his law licence in Hong Kong in 2005 was corporate and constitutional law.

That changed in 2012 amid mass arrests in the local asylum community. Tibbo established a legal clinic to help hundreds of destitute refugee claimants who had mostly been tortured or sexually abused in their home countries, notably Sri Lanka, Indonesia, the Philippines and West Africa. "My phone never stopped ringing as people who were incarcerated started seeking me out rather than seeking out legal aid," he said.

A year later, Tibbo landed the most famous client on the planet. For two frantic weeks in June 2013, he helped Edward Snowden, the former U.S. Central Intelligence Agency (CIA) contractor who leaked an unprecedented cache of classified documents to the media, escape Hong Kong and the clutches of U.S. law enforcement.

"It was insanity," he said. "It all happened really quickly and I realized that my life was going to change because of my professional association with Ed."

Snowden, now 33, lives in self-imposed exile in Moscow. Tibbo, meanwhile, operates in a post-Snowden bubble. For one, he appears to be in a state of perpetual paranoia, a consequence of what Poitras, who recently returned to live in New York after years of being on the U.S. government's watchlist, called the "backlash" of surveillance directed at the Canadian lawyer by Hong Kong and U.S. officials.

Most days, Tibbo can be seen walking purposefully through the crowded streets of Hong Kong lugging a leather case strapped onto his shoulder packed with plastic zip-lock bags containing an array of burner cellphones, an IBM laptop computer -- whose battery he is constantly removing -- and a spare shirt.

Visitors to his office must deposit their cellphones in a small refrigerator until they leave -- a trick he learned from Snowden.

During a wide-ranging interview, he speaks fondly of his famous client, and still jealously guards certain aspects of their relationship, most notably how he was retained to represent the most-sought-after dissident in the world.

Even Snowden won't answer the question, deferring to Tibbo in an encrypted text message to the National Post. "Let him speak to this one. I've got to say that he's earned it. There aren't a lot of lawyers who could successfully protect their client in the midst of something like that."

Jonathan Man said his Canadian partner took on a lot of responsibility during the frantic days when sheltered the U.S. fugitive. "He had a lot more pressure on him than I did. Most of the plan was Robert, but we executed it together," he said.

"He's what we call a boy scout," said Ben Wizner, Snowden's principal legal adviser and director with the American Civil Liberties Union. "He's an extremely scrupulous and ethical lawyer."

Wizner acknowledged that Tibbo became involved in Snowden's case at a time "of much greater danger than when I got involved and when the outcome not only seemed uncertain, but could have ended badly." For that, he said, "I have enormous respect for Robert and the role that he played."

Masterminding one of the world's greatest political escapes seems an unlikely outcome for Tibbo, a McGill University chemical engineering graduate who spends his annual summers cycling at his property in Nova Scotia. After earning his degree in 1988, he headed to Australia and then in the early 1990s to China, where he learned Mandarin.

For the next decade, Tibbo travelled to Thailand and Hong Kong, studied law at the University of Auckland in New Zealand and graduated in 2001. He settled in Hong Kong, obtained a law licence, married and founded Eastern Chambers the following year.

His cramped one-room office in the Wan chai district is far from the polished chrome and glass towers of the major firms. Bookcases filled with black binders line the back wall, piles of papers are strewn on the floor, mismatched chairs are spread throughout the room, and a large table is pushed up against the wall over which diplomas hang haphazardly. Two small air conditioner units attached to the windows wheeze cool air to break the stifling heat and humidity and a small refrigerator contains bottles of water and cellphones.

As incongruous as it appears, the ramshackle office was the nerve centre for Snowden's getaway and Tibbo was pivotal to the execution of the plan.

"He [Tibbo] played the role that only he could play at that time. That's all it is. I doubt Robert would feel other than lucky than to have been involved in the case," said Snowden's U.S. lawyer Wizner. Currently, there are at least another seven lawyers in other jurisdictions on retainers waiting to play the same role for the U.S. fugitive.

Tibbo has certainly parlayed his association with Snowden to burnish his human rights credentials in Hong Kong. He said he is overwhelmed with refugee client requests, for which he is paid about HK$750 an hour (approximately C$135). Still, his cases haven't won him accolades within the conservative local legal fraternity. "He touched Snowden and that's his biggest claim to fame," said a Hong Kong barrister who is friendly with Tibbo but asked not to be named.

Now, with the world premiere of famed director Oliver Stone's movie on Snowdon imminent, Tibbo's more immediate concern is the potential backlash against the refugees who sheltered Snowden in Hong Kong. "He's very concerned about the people who helped Ed underground knowing they are very vulnerable," Poitras said.

But for Tibbo, fretting over his clients is an integral part of the services he provides -- and the one the asylum seekers count on the most.

National Post

Edward Snowden lauds 'courageous' asylum seekers who sheltered him: 'They had a hundred chances to betray me' (Canada)

Wednesday, 07 September 2016

Byline: Theresa Tedesco

Section: general

Interview - Edward Snowden, the world's most wanted dissident, looks back on his escape from Hong Kong. The National Post's Theresa Tedesco communicated with him via encrypted text messages through his Canadian lawyer, Robert Tibbo. The interview has been edited and condensed.
Q: How are you? How is life in Russia?

A: I'm doing surprisingly well, given some rather sinister figures are still feeling a bit vengeful about having been thrust into the spotlight. Public opinion regarding my decision to reveal mass surveillance to journalists has been moving favourably around the world, including perhaps unexpectedly the U.S. where even the former attorney general who once charged me as a criminal now says that while he can't condone it, he believes what I did was a "public service." Most of my time nowadays is focused on my work at the Freedom of the Press Foundation I sleep in Russia, but thanks to technology, I move all over the world.

Q: Do you have any regrets? Would you have done anything differently?

A: One of the things we've seen in the wake of these revelations is that the abuse of intelligence by authorities acts like a kind of cancer of government. The longer they go undetected, the harder they become to remove. Because the public at large wasn't permitted to know of them, and therefore couldn't object, we reached a point where critical masses of government staff became implicated in these abuses domestically and via foreign liaisons. At that point, if you actually try to enforce the law

and bring investigation and charges, you've got half of the institution fighting you, even if they know it's immoral, because they worry they might be the next one to be held to account. Had I known what was going on sooner, if I had come forward earlier, maybe we'd be in a better place. But there's always next time.

Q: Why did you choose Russia?

A: That's not quite right. I never intended to end up in Russia, much less chose it. When my government learned I had departed Hong Kong en route to Latin America, they cancelled my passport, trapping me in a Russian airport. Unable to travel and unable to leave, I filed applications for asylum in 21 countries, places like France and Germany, Austria and Finland. But those countries neither accepted my respective requests nor permitted safe travel onwards. Later we would learn that this was due to pressure from the White House, possibly in violation of international law forbidding interference with asylum claims. Eventually after spending a month trapped in limbo, I was allowed to leave the airport.

Q: Did you have concrete evidence that you might be killed?

A: Nobody on my team thought it would be the likeliest outcome, but it would have been irresponsible not to consider the possibility. Perhaps I come from a different perspective after working at the CIA for years, but do you really think it's be the first time they've killed someone for having the wrong politics?

Q: How were you able to trust total strangers in that situation? Were you in shock?

A: No matter how much you prepared yourself, taking a decision like that is frightening for sure. But it's also liberating. Think about it: when you walk into a fight you're almost certain you're going to lose, you realize incredible risks work in your favour, not to the adversary's. Suddenly, instead of fixating on your overwhelming odds of failure, you start evaluating tiny chances for success. For me, it was trusting strangers who knew what it meant to be hunted.

Q: What was it like?

A: They had a hundred chances to betray me while I was amongst them, and no one could have blamed them, given their precarious situations. But they never did. Despite not even having enough space for themselves, they never complained. Instead they smiled. The children would watch me crack neighbourhood wireless access points with a special antenna so I could communicate with journalists without drawing the police to where I was. I still remember the feeling in my stomach as I'd hear sirens screaming toward the building. I'd pray like hell that they were for something else as I raced to disable any equipment that might be transmitting, getting ready to move. Fortunately, it was always something else.

Q: How did you react when Robert Tibbo suggested the plan?

A: I was in a mission-focused state of mind by that point, so there wasn't a lot of agonizing. I wasn't bothered by the idea of rough living, but I was worried about accidentally dragging people down with me. Robert promised me they'd have my back despite the risks, and he was right. Supun, Nadeeka, Vanessa and Ajith are among the most courageous people I've ever had the privilege to know. Imagine the world's most wanted dissident is brought to your door. Would you open it? They didn't even hesitate, and I'll always be grateful for that. If not for their compassion, my story could have ended differently. They taught me no matter who you are, no matter what you have, sometimes a little courage can change the course of history.

National Post

How Snowden escaped (Canada)

Wednesday, 07 September 2016

Byline: Theresa Tedesco

Section: general

Hong Kong - The tall, lanky American dressed in all black looked familiar. But Ajith, a 44-year-old Sri Lankan refugee seeking asylum in Hong Kong figured the nervous-looking man with the red-rimmed eyes fidgeting in the darkness outside the United Nations building in the Tsim Sha Tsui district of Kowloon was a U.S. army dodger.
Summoned by his immigration lawyer in the late evening of June 10, 2013, Ajith (last names of the refugees in this story have been withheld), a former soldier in the Sri Lankan military, was told the unidentified man was "famous" and needed "protection." Little else was revealed except that he would be responsible for covertly moving the American around at a moment's notice.

"I was very happy to help him," Ajith recalled during a recent interview with the National Post in his small windowless room in Kennedy Town, on the western tip of Hong Kong Island. "This famous person was a refugee too, same as me."

Earlier that day, that "famous" 29-year-old walked out of the five- star luxury Hotel Mira in Kowloon and sparked an intensive global manhunt not seen since the search for al-Qaeda's Osama Bin Laden after the Sept. 11, 2001, bombings.

Edward Snowden, a former U.S. intelligence contractor, became the most wanted fugitive in the world after leaking a cache of classified documents to the media detailing extensive cyber spying networks by the U.S. government on its own citizens and governments around the world.

To escape the long arm of American justice, the man responsible for the largest national security breach in U.S. history retained a Canadian lawyer in Hong Kong who hatched a plan that included a visit to the UN sub- office where the North Carolina native applied for refugee status to avoid extradition to the U.S.

Fearing the media would surround and follow Snowden -- making it easier for the Hong Kong authorities to arrest the one-time Central Intelligence Agency analyst on behalf of the U.S. -- his lawyers made him virtually disappear for two weeks from June 10 to June 23, 2013, before he emerged on an Aeroflot airplane bound for Moscow, where he remains stranded today in self-imposed exile.

"That morning, I had minutes to figure out how to get him to the UN, away from the media, and out of harm's way with the weight of the U.S. government bearing down on him. I did what I had to do, and could do, to help him," Robert Tibbo, the whistleblower's lead lawyer in Hong Kong told the Post in a wide-ranging interview, the first detailing the chaotic days of Snowden's escape three years ago. "They wanted the data and they wanted to shut him down. Our greatest fear was that Ed would be found."

The covert scheme to dodge U.S. attempts to arrest Snowden could have been ripped from the pages of a spy thriller.

The fugitive was disguised in a dark hat and glasses and transported by car at night by two lawyers to safe houses on the crowded and impoverished fringes of Hong Kong. Snowden hunkered down in small, cluttered, dingy rooms where as many as four people shared less than 150 square feet. Batteries were removed from cellphones when they gathered, burner phones were used to place calls, SIM cards were exchanged and sophisticated computer encryption was used to communicate when face-to-face meetings were not possible. Snowden rarely ventured out, and only at night where he could easily be lost among the many other asylum seekers.

"Nobody would dream that a man of such high profile would be placed among the most reviled people in Hong Kong," recalled Tibbo, a Canadian-born and educated barrister who has practiced law for 15 years. "We put him in a place where no one would look."

Perhaps more importantly, added Jonathan Man, another Snowden lawyer who worked alongside Tibbo: "We knew (the asylum seekers) because we had helped them on their (immigration cases). And we knew they would not betray us."

Until now, details of how Snowden avoided detection, and where and who sheltered him have been closely guarded secrets known only by the famed whistleblower and his Hong Kong-based lawyers. Since then, he has become a controversial figure: a traitor to U.S. lawmakers and many in the intelligence community, but a pop-culture icon to legions of anti-establishment followers. Inevitably, Hollywood has entered the fray with a biopic of his life, directed by Oliver Stone and produced with Snowden's cooperation; the film is scheduled for a world premiere on September 9 at the Toronto Film Festival.

"Imagine the world's most wanted dissident brought to your door. Would you open it? They didn't even hesitate, and I'll always be grateful for that," Snowden said in an exclusive encrypted text to the Post.

The lives of the refugee families who concealed Snowden without question -- and without much choice -- may be forever changed now that their roles in helping him elude law enforcement will become public in the upcoming movie.

"I think these are very brave, selfless people who did something extraordinary at a very difficult time and at enormous personal risk," said Laura Poitras, a journalist and Oscar-winning documentary maker who filmed Snowden inside his Hong Kong hotel room for eight days.

Late on the evening of June 10, 2013, a cellphone rang in one of the dozens of decrepit, filthy apartment complexes that line the streets in the Lai Chi Kok area of Kowloon. Supun, a 32-year-old native of Colombo, Sri Lanka, who has languished in Hong Kong's refugee system since 2005, took a call in a cramped 150-square-foot apartment he shared with his partner Nadeeka and one-year-old daughter Suwasistiki. The voice on the other end of the phone was his immigration lawyer Robert Tibbo, asking to meet outside on the crowded sidewalk. "I was scared to ask questions," Supun said. "I told Nadeeka, 'I don't know why he's coming.' I thought it had to with my [asylum] case."

Reflexively, he brought his baby daughter outside with him. There, he was met by Tibbo, Jonathan Man and Edward Snowden. Asked if he recognized the American, Supun lied and said yes. "I was very scared," he said, and thought Snowden was in the military because of his short haircut.

Supun recalled the three men whispering amongst themselves and overheard them talking about someone being followed. "They told me he was staying with me. Feed him and don't talk to nobody about him," he said. Confused, he nonetheless obliged.

Supun wasn't told that Snowden had earlier that day escaped his hotel room where he had been holed up with journalists Laura Poitras and Glenn Greenwald for eight days leaking classified documents he'd stolen from the National Security Agency's Threat Operations Centre in Hawaii where he worked as an outside contractor for Booz Allen Hamilton Inc. The media's explosive reporting captivated the world and infuriated and embarrassed the U.S. government.

The intensely shy Snowden finally unmasked himself as the source of the classified disclosures on the Guardian's website on June 9. "He was scared for his life. He was fully aware that his life was at risk," Tibbo said. "Ed was clear in his mind about making the disclosures, but Ed's a human being. No matter that he understood intellectually what he did, it was only after he made the disclosures that thousands of tons of realizations weighed heavily on his emotional and physical state. He had the weight of the world on his shoulders and he had to move very quickly."

A high-stakes plan to keep Snowden safe was set in motion that began when he was escorted from the hotel to the UN building where Tibbo was waiting. Because Snowden's visa was still valid, he couldn't be

sure that the Hong Kong government would protect him. However, the UN would with a refugee claim and filing one bought time and tied the hands of Hong Kong authorities -- which answer to China's central government in Beijing -- from extraditing him at the U.S.'s request. As an asylum seeker, though, Snowden would also have been subject to harsh refugee rules and faced the possibility of being incarcerated while his application was processed, which could have taken decades.

At the same time, any thoughts that Snowden could remain in Hong Kong to fight extradition through local courts were quickly banished when it became clear that his freedom -- and his access to computers -- would have been curtailed.

"I wasn't familiar with Hong Kong's asylum policies," Snowden said in his text to the Post. "My plan was just to return this information to the public, not to take care of myself, which I considered impossible. This can be seen in my lack of an after-action plan."

Still, in the flurry of activity on that first day, and in the absence of a clear plan, filing with the UN was a necessary first step. From there, Snowden's lawyers knew they had to embed him somewhere safe until they hammered out an exit strategy, which is why they arrived at Supun's door in a grimy building with cracked walls and chipped green tiles on the stairs.

Children's clothes blow in the dirty air hanging over barbed wire. The squalor is visible; open garbage rots in stairwells and in open pits that were once courtyards. The stench, aided by the unbearable heat and humidity, is overpowering.

These housing estates, where Vietnamese, Indonesian, Filipino, African and Sri Lankan refugees live with inadequate resources from the government through International Social Services (ISS), are not just places where dreams come to die; it's where hope is decimated.

According to government statistics, Hong Kong has only accepted 52 refugees out of tens of thousands since 1992, an acceptance rate of about 0.05 per cent. Currently, there are 12,000 asylum seekers registered with the government, but there are several thousand more unregistered.

"The Hong Kong government hates poor people -- there are 1.5 million of its own and the refugees, who are at the bottom of the pile," said Cosmo Beatson, founder and executive director of Vision First, an independent NGO that advocates for refugees in the city-state founded in 2009.

Inside Supun's cramped two-and-a-half-room living space, a threadbare cotton sheet covers a small filthy window where an air conditioner wheezes incessantly. Supun, 32, Nadeeka, 33, and their now-four- year-old daughter and newborn son Dinath sleep on a mattress that barely fits in a room no bigger a large janitor's closet. A stuffed Minnie Mouse toy rests against a pillow and piles of bags containing their meagre belongings are jammed into a corner.

In the adjacent room where we sit on three plastic red stools are a small refrigerator, tattered green upholstered chair and ancient Dell desktop computer. A nearby bathroom doubles as the kitchen, with pots and pans stacked on top and underneath the sink and toilet.

This is the kind of place where Snowden hid from the world during the first days he went underground. "You're a good man to take care of me," Supun said Snowden told him. When they asked what the stranger liked to eat, he replied, burgers and spaghetti. Armed with the money Tibbo gave him, Supun went to buy food while Nadeeka prepared the only bed in the house for their unexpected guest.

The next day, Supun was dispatched to buy the South China Morning Post, an English-language newspaper he admitted he never reads. It wasn't until he brought the paper home that he and Nadeeka saw the giant front-page photo of the pale young man in their bed. "We were very, very surprised that this famous person was in our house," Nadeeka said. "We can't believe he's here in our house."

The tiny living space soon became overcrowded, especially since during his stay, Snowden "stayed in the room all the time," Nadeeka said. She had to force him to come out to shower so that she could clean the room. Nadeeka, who fled Sri Lanka in 2007 after years of systemic rape and subsequent hospitalization according to her refugee claim, also worried about Snowden, "because I knew he was living a dangerous life."

Once Snowden confirmed his identity, he ordered his host to unplug the old Dell computer because he was worried about it being traced. He also asked Supun to purchase specialized software at a local computer shop that would have allowed Snowden to communicate through sophisticated encryption. Everything was paid in cash so there would be no trace.

"He was in shock for the first three days," Tibbo recalled of his famous client. "He was a zombie, like he'd just walked out of a car crash."

Snowden saw it differently. "I was in a mission-focused state of mind at that point," he said. "I wasn't bothered by the idea of rough living, but I was worried about accidentally dragging people down with me."

Snowden's stay with Supun and Nadeeka was without incident. He ate mostly McDonald's food and loved sweets, especially cake. His legal team limited their presence at the tiny apartment, but dispatched interns to deliver cakes and sweets embedded with USBs as a way to communicate with him.

After almost a week, police suddenly began patrolling Supun's neighbourhood for no apparent reason. During Snowden's stay there, the U.S. government filed sealed criminal charges against Snowden on June 14, and requested Hong Kong authorities detain him the following day under an extradition treaty between the two countries, as a prelude to a formal application. Meanwhile, Snowden's passport and visa to visit Hong Kong remained valid as long as the seal remained in place, but his legal team feared the authorities were closing in.

"I still remember the feeling in my stomach as I'd hear sirens screaming toward the building, I'd pray like hell that they were for something else as I raced to disable any equipment that might be transmitting, getting ready to move," Snowden said.

Once darkness fell, the fugitive hugged Nadeeka, shook hands with Supun and gave them US$200 for their hospitality before he was clandestinely shuttled off to another secret location.

"In the early days, I understood it was a serious case that must be handled with care, but as the days wore on, I came to understand how dangerous the matter was becoming," Tibbo's associate Man said.

Sham Shui Po is among the poorest of Hong Kong's 18 districts. As the birthplace of the city-state's first public housing project, it was once the location of a POW camp for British, Canadian and Indian soldiers during the Second World War. In the 1970s and 1980s, the area was used to house Vietnamese refugees. Today, it is home mainly to the poorest new immigrants, especially from mainland China, and many of the refugees seeking asylum.

Snowden was taken to a cramped one-bedroom apartment in Sham Shui Po where Vanessa, a Filipino asylum claimant, lived with her mother and one- year-old daughter Keana. Again, it was late in the evening when Tibbo, Man and a stranger showed up at the 46-year-old's door. "I had no idea who [Snowden] was," she said. "My lawyer Robert Tibbo told me this man needed help. So I let them come into my house. They talked and I gave them privacy. Then he [Tibbo] told me he wanted him to stay with me. They didn't explain anything; just that he needed help, safety and do not talk to anyone."

Sitting in a tiny two-room apartment near North Point on Hong Kong Island where she moved last year, Vanessa described Snowden that night as "very, very upset" and visibly shaken. Once Tibbo and Man left her home, she changed the linens on her only bed and went to buy Snowden Chicken McNuggets and iced tea from a nearby McDonald's. He thanked her and went to sleep.

The next morning, Snowden woke up early and dispatched Vanessa to buy the local English-language newspaper. "I was shocked," she said, to learn his identity. She demanded to see his passport, and Snowden obliged. Still, despite being shaken and upset, she wasn't overly concerned. "Mr. Tibbo would not put me in trouble. I just listened to him and didn't talk to anyone," she said during an interview with her lawyer present.

Vanessa arrived in Hong Kong in 2002 as a domestic care worker. The contract ended after three years, but she stayed and worked in the country illegally for about five years until she was arrested. She filed for a refugee claim in 2010 and has been Tibbo's client since 2012.

Most of the time, Vanessa said her secret house guest was quiet and preoccupied on his computer. "He was worried a lot about his next step," she said. "He talked about his past life. He was really scared most of the time."

Snowden took cover at Vanessa's home for about four days and once again gave US$200 to his host on his way out the door.

Snowden's next stop was a tiny windowless, one-room apartment belonging to Ajith, the man who had been helping to move him around the city. The two men didn't talk much mostly because of the language barrier -- the Sri Lankan speaks little English. "My feeling was he had big tensions, he was very scared, he was nervous," recalled the lithe man with tattooed arms. Having landed in Hong Kong from a small town just outside Colombo in 2003 (too poor to bring his wife and one-year-old daughter with him) Ajith recalled that his guest was so jumpy "he would not let me open the door."

Snowden stayed with Ajith only one night. On June 21 -- his 30th birthday -- the whistleblower was formally charged with three felonies under the 1917 U.S. Espionage Act. A criminal complaint was filed in the Eastern District of Virginia, and the U.S. formally requested his arrest by the Hong Kong government. With that, the clock began ticking on when the U.S. would revoke his passport.

It was no longer safe to keep Snowden -- who faced the prospect of a trial in Virginia, and up to 30 years in a maximum-security prison if convicted -- with any refugees because they would be harbouring a fugitive from the law, making them even more vulnerable to Hong Kong government authorities.

Snowden was clearly concerned about how he would be treated if he was taken into custody by U.S. law enforcement. At the time, the military trial of Chelsea Elizabeth Manning, a 24-year-old former intelligence analyst in Iraq who passed along more than 700,000 classified documents to the Wikileaks website in 2010, was underway.

Before Snowden, Manning's case ranked as the largest breach of classified materials in U.S. history. Manning was convicted of 20 counts by court martial after she pleaded guilty to 10 of the 22 charges under the U.S. Espionage Act.

During her incarceration, A UN envoy accused the U.S. of cruel, inhuman and degrading treatment for keeping the former solider in solitary confinement at the Quantico military base in Virginia for almost a year. Manning was sentenced to 35 years in a maximum-security military prison at Fort Leavenworth, Kan., in August 2013.

After 12 days of hiding underground in Hong Kong's refugee community, Snowden was shuttled to the home of one of his lawyers. Terrified of a drone attack, according to Tibbo, they still celebrated the fugitive's milestone birthday with pizza, his favourite meal. With the U.S. justice system in hot pursuit, Snowden's lawyers had advised him of his rights as a refugee claimant, including, his various options to cross borders, possible routes and modes of transportation.

It was clear that fighting for asylum in Hong Kong was fraught with too much uncertainty. "It was Ed's decision to leave," Tibbo said. But Snowden also knew he needed assistance elsewhere. He instructed

his lawyers to reach out to Julian Assange and the Wikileaks network whose global group is committed to disclosing government secrets.

Sarah Harrison, a British Wikileaks staffer and close confidante of Assange, flew to Hong Kong from Australia and consulted with Snowden's lawyers. She purchased more than a dozen airline tickets to different destinations, including Iceland, Cuba and India, to confuse U.S., Chinese and Hong Kong officials monitoring the airport, despite having received "neutral to a green-light" from the city-state's government allowing Snowden to leave unhindered. Meanwhile, Assange, who was in self-exile at the Ecuadorean embassy in London, worked his connections with South American governments to obtain diplomatic protection for the young American.

On June 23, Tibbo drove Snowden and Harrison to Hong Kong International Airport. During that journey, Snowden, who had just met his travelling companion from Wikileaks for the first time, seemed unusually nervous. The pair posed as a young couple headed on a vacation. Leaving little to chance, Man simultaneously bought a ticket to Shanghai to get access to the boarding gates in the event Snowden encountered problems before boarding the plane. Tibbo waited at the Immigration department at the airport. Unlike the early days, this escape was meticulously planned.

"We tried our best to avoid surveillance," Man recalled. "Looking back, we must have been crazy. We understood the danger, but we didn't think much about it. Luckily, it turned out successfully."

Once the Aeroflot flight to Moscow had exited Chinese airspace, the Hong Kong government announced Snowden had left the country. The U.S. government was livid. Predictably, Snowden's departure kicked off a global pursuit and his passport was finally revoked.

However, when Snowden landed in Moscow, he was grounded in the transit zone of the airport because his cancelled passport meant he was prohibited from boarding any further commercial flights.

"I never intended to end up in Russia, much less choose it," he said. "When my government learned I had departed Hong Kong en route to Latin America, they cancelled my passport trapping me in a Russian airport. Unable to travel and unable to leave, I filed applications for asylum in 21 countries around the world, places like France, and Germany, Austria and Finland. But those countries neither accepted my respective requests nor permitted safe travel onwards."

In the end, Snowden and Harrison were marooned at the Sheremetyevo airport for a month before the Russian government granted him temporary asylum, which was recently extended for another three years.

Snowden, now 33, remains America's most wanted fugitive, although he has maintained that he would be prepared to return to the U.S. if he were guaranteed a fair trial. His lawyers are working on a plea deal and, more hopefully, are preparing to petition for a presidential pardon this fall. In the meantime,

Snowden has multiple emissaries in different jurisdictions around the world in the event he is able to move from Moscow.

Most of Snowden's time is focused on his work at the Freedom of the Press Foundation as he has forged a new life in Moscow with his long-time girlfriend Lindsay Mills. "I sleep in Russia, but thanks to technology, I (live) all over the world," he said.

Inevitably, Oliver Stone's movie will reignite the debate over whether the high-school dropout turned CIA computer whiz was a reckless traitor to his country or a disillusioned idealist with sincere motives.

For the vulnerable people back in Hong Kong who helped him escape to safety, the danger is potentially more palpable. According to Tibbo, Snowden sent them each US$1,000 when he realized he may have unwittingly put them at risk by revealing their role for the Hollywood movie.

"They had a hundred chances to betray me while I was amongst them, and no one could have blamed them, given their precarious situations. But they never did," Snowden said. "If not for their compassion, my story could have ended differently. They taught me no matter who you are, no matter what you have, sometimes a little courage can change the course of history."

Politico

DHS secretary Johnson vows 'no stone unturned' on election security

Tuesday, 06 September 2016

Byline: Nick Gass

Section: general

Washington - Faced with the potential threat of an election compromised by foreign hackers, Homeland Security Secretary Jeh Johnson on Tuesday sought to reassure Americans, pledging to "leave no stone unturned" when it comes to ensuring the integrity of the process.
"Well first, we have a lot of confidence in the integrity of the election process itself," Johnson told MSNBC's "Andrea Mitchell Reports." "There are some 9,000 state and local jurisdictions that are involved in the election process, including national elections, we've looked at a fair amount of it. We've looked at what states and cities do."

Johnson went on to say that "we have a lot of confidence in the process itself, we're in the mode now of wanting to leave no stone unturned, and so, what DHS, my department, has been going over the last several weeks is contacting state election officials to say, we want to leave no stone unturned."

The FBI said last month that foreign hackers were able to penetrate state election systems in Arizona and Illinois, and both the Democratic and Republican parties, have been compromised by cyberattacks seen as emanating from Russia.

"There are services we can offer by way of vulnerability to detection, incident response, we're in a general environment where there's an increasing level of sophistication by cyber attackers," he continued. "Across the spectrum, whether it's nation-state actors, plain criminals, hacktivists, and so we want to inform state election officials of what we see on a national level as best practices, and we're doing that right now."

Pressed on whether the department could protect the election from interference given past intrusions of top security agencies from China, Russia and others, Johnson responded that the "election process itself is not one that is tied to the Internet, the grid."

"It's a matter of vote counting and delivering vote tallies to a central repository, which occurs multiple different ways in multiple different layers," Johnson said, to which Mitchell responded that it is "electronic in many instances."

Johnson replied, "But it's not generally linked to the Internet."

"In terms of federal.gov, we're moving in the right direction," Johnson continued. "DHS is now installing across lots of federal agencies, including [the Office of Personnel Management] now, the ability to not just monitor and detect cyber intrusions, but to block them as well. We're in a much better place than we were as recently as a year ago, pursuant to a pretty aggressive timetable that I've set for the federal.gov system."

Bloomberg Politics

Putin Says DNC Hack Was a Public Service, Russia Didn't Do It

Friday, 02 September 2016

Byline: Multiple reporters

Section: general

Vladivostok - Vladimir Putin said the hacking of thousands of Democratic National Committee emails and documents was a service to the public, but denied U.S. accusations that Russia's government had anything to do with it.
"Listen, does it even matter who hacked this data?" Putin said in an interview at the Pacific port city of Vladivostok on Thursday. "The important thing is the content that was given to the public."

U.S. officials blame hackers guided by the Russian government for the attacks on DNC servers earlier this year that resulted in WikiLeaks publishing about 20,000 private emails just before Hillary Clinton's nominating convention in July. The documents showed attempts by party officials to undermine her chief Democratic rival, Bernie Sanders, and led to the resignation of the head of the DNC, Representative Debbie Wasserman Schultz of Florida.

Putin, in power since 2000 and facing re-election in 18 months, has had an acrimonious relationship with Clinton since her failed attempt to "reset" relations as secretary of state in 2009. Putin in 2011 blamed her personally for stoking the biggest protests of his rule by sending an activation "signal" to "some actors" inside Russia. Clinton has compared his annexation of Crimea in 2014 to actions taken by Adolf Hitler before World War II.

"There's no need to distract the public's attention from the essence of the problem by raising some minor issues connected with the search for who did it," Putin said of the DNC breach. "But I want to tell you again, I don't know anything about it, and on a state level Russia has never done this."

The Federal Bureau of Investigation has high confidence that the government in Moscow was behind the theft at the DNC and other Democratic Party organizations seeking to propel Clinton to victory over Republican Donald Trump in November, a person familiar with the findings has said. Trump has praised Putin as a great leader and the billionaire's former campaign chairman spent years working for the Kremlin ally who was ousted from Ukraine's presidency in 2014.

Clinton's campaign struck back at Putin on Friday for characterizing the cyber intrusions at Democratic Party groups as a public service and accused him of endorsing the disruption of the U.S. vote.

"Unsurprisingly, Putin has joined Trump in cheering foreign interference in the U.S. election that is clearly designed to inflict political damage on Hillary Clinton and Democrats," Clinton spokesman Jesse Lehrich said in an email. "This is a national security issue and every American deserves answers about potential collusion between Trump campaign associates and the Kremlin."

In a two-hour conversation near Russia's eastern fringe, Putin touched on subjects ranging from the war in Syria to oil prices and trade with China. It came just two days before Putin, Barack Obama and other world leaders gather at a Group of 20 meeting in Hangzhou.

Video: Putin Says Compromise Possible With Japan in Islands Dispute

An internal DNC probe by CrowdStrike Inc., a cybersecurity company, traced the DNC break-in to two groups it says are linked to Russian intelligence services. One, Cozy Bear, it says is affiliated with the Federal Security Service, the main successor to the KGB, while the other, Fancy Bear, it says is tied to the Main Intelligence Directorate, a branch of the Defense Ministry.

James Lewis, a cybersecurity expert at the Center for Strategic and International Studies in Washington, said Russia's "track record" of state hacking goes back at least a decade, so Putin's denials aren't credible.

"Nice try, but no goal," Lewis said.

The digital net cast by the hackers has widened almost weekly -- security experts say it now includes congressional staffers, NATO generals, Washington think tanks and the Democratic Congressional Campaign Committee -- adding another unpredictable element to a highly unusual election. The subsequent leaks have included the mobile number of House Minority Leader Nancy Pelosi, who said she was barraged with "obscene" calls within hours.

Putin also took a dig at the U.S. campaign and what he saw as an obvious party bias in favor of Clinton, saying he "couldn't imagine" that the information leaked from the DNC would be newsworthy for "American society -- specifically that the campaign headquarters worked in the interest of one of the candidates, in this case Mrs. Clinton, rather than equally for all of the Democratic party candidates. "

Alexander Gostev, the chief expert at Kaspersky Lab, a Moscow-based software security firm, said of all the Russian-speaking hacking groups targeting governments, Fancy Bear "is the most notable."

Malware linked to Fancy Bear was widely detected in Ukrainian government computers during the elections that were held after the country's Kremlin-backed leader, Viktor Yanukovych, was deposed, Gostev said, adding that "six or seven" groups may be tied to the Russian government.

At the same time, Russia has come under attack by viruses linked to U.S. and U.K. intelligence services, Gostev said, adding that hacking efforts from China against Russian defense and nuclear agencies have intensified in the past year.

Snowden Warning

Edward Snowden, the former National Security Agency contractor who exposed U.S. surveillance secrets, said on Twitter last month that Russia, where he lives in exile, may have been behind the hack of NSA- linked malware that was made public. The reason, Snowden said, may have been to "influence the calculus of decision-makers wondering how sharply to respond to the DNC hacks."

Putin said that even if Russia did want to try to influence the U.S. election through leaked secrets, it doesn't have the nuanced understanding of American politics required to succeed.

"To do that you need to have a finger on the pulse and get the specifics of the domestic political life of the U.S.," the Russian president said. "I'm not sure that even our Foreign Ministry experts are sensitive enough."

Putin, 63, said the state of hacking is so sophisticated that it's impossible to know the identities or locations of the people ultimately behind them.

"You know how many hackers there are today?" Putin said. "They act so delicately and precisely that they can leave their mark -- or even the mark of others -- at the necessary time and place, camouflaging their activities as that of other hackers from other territories or countries. It's an extremely difficult thing to check, if it's even possible to check. At any rate, we definitely don't do this at a state level."

Moscow Times

Russian Security Services Say 'Spy Pen' Found in Pokemon Go Player's Home

Tuesday, 06 September 2016

Byline: Staff report

Section: general

Moscow - Russian security services say they found a "spy-pen" in the home of video blogger Ruslan Sokolovsky, who was recently detained for filming himself playing Pokemon Go in a Yekaterinburg cathedral. Police have charged Sokolovsky with committing an extremist act and offending religious sensitivities. If convicted, he could face several years in prison.
Russia's Investigative Committee said the pen could be used to receive illegal information from abroad. Other potentially incriminating items in the suspect's apartment include a video camera, a tripod, and a professional microphone.

Police are also investigating magazines published by the video blogger, which they say contain illustrations which incite religious hatred. Earlier this year, Sokolovsky launched a self-titled magazine for atheists. He wrote that: "we have been inspired by Charlie Hebdo and have decided that there are too few such publications in Russia that take an absolutely amoral approach to ridiculing the contemporary national reality."

The Russian Orthodox Church initially called for Sokolovksy's release. Its Yekaterinburg representatives said the church "does not lust for blood." But the church has since changed its stance on the matter. Its local spokesman, Veniamin Raynikov, told the press that the church "will not put pressure on the court so that we appear to be the good guys. We support re-education."

The blogger's mother hopes the church will forgive her 21 year-old son. In an interview with the pro-Kremlin Life News channel, she said: "he should not have done it. We want to talk to bishop Kirill so that the whole thing will end in peace and friendship." She also said she recently lost her older son and that the family buried him in a church ceremony. "I went through such sadness - and now this. I want to talk to the church, perhaps they could release him at least out of pity for me."

Amnesty International has released a statement urging Russian authorities to release the blogger, calling his detention an "absurd attack on freedom of expression."

"The farcical nature of the case against the Russian blogger, detained for playing Pokemon Go in a church, demonstrates what happens when the authorities do not value freedom of expression. Even if someone deems Sokolovsky's behavior disrespectful, authorities should not imprison people purely for offending religious beliefs," said John Dalhuisen, director of Amnesty International's Europe and Central Asia office.

The Local (Germany)

German government attacked by hackers 20 times a day

Tuesday, 06 September 2016

Byline: Staff report

Section: general

Berlin - Cyber attacks on the German government and businesses are becoming ever more sophisticated and effective, security experts warn.
Each day there are more than 20 highly specialized attacks on the government's computer networks, the president of the Federal Office for Information Security (BSI), Arne Schönbohm, told Bild on Tuesday.

"Today cyber attacks are much more precise than before and aimed at single targets, like the German parliament. That unfortunately means they're also more successful," Schönbohm said.

The BSI is at the front line of protecting government networks, and so far "no hacker has yet cracked this".

Last year though, a magazine reported that German-owned Patriot missiles in Turkey were briefly taken over by hackers.

Schönbohm said that the frequency of attacks on both private and public entities has become great.

"Volkswagen says the number of attacks on their IT network is 6,000 per day."

A study last year found that one in five major German firms had been attacked by hackers.

DPA recently found that some German states, in the fight against cyber crime and terrorist activity, have significantly expanded their investigative authorities to include new specialized departments, prosecutors and IT experts.

Security experts fear that terrorists or other groups could, for example, target through cyber attacks certain vital resources for communities, like water or energy supplies.

The German government also warned of cyber attacks in its first civil defence plan since the end of the Cold War. The strategy called for citizens to stockpile food for ten days and water for five in case of cyber or other attacks against resources.

In April, a computer virus found at a Bavarian power plant raised alarm, though plant operators insisted that it did not pose a threat. Authorities later discovered that the virus came from a USB stick rather than over the internet.

Associated Press

Missed opportunities to stop OPM cyber breach spelled out

Wednesday, 07 September 2016

Byline: Staff report

Section: general

Washington - It was time to purge the hacker from the U.S. government's computers. After secretly monitoring the hacker's online movements for months, officials worried he was getting too close to critical information and devised a plan, dubbed "the Big Bang," to expel him.
Trouble was, with all their attention focused in that case, they missed the other hacker entirely.

A new congressional report provides previously undisclosed details and a behind-the-scenes chronology of one of the worst-ever cyberattacks on the United States, laying out missed opportunities before the break-in at the Office of Personnel Management exposed security clearances, background checks and fingerprint records. That attack - widely blamed on China's government - compromised personal information of more than 21 million current, former and prospective federal employees, led to the resignation of the OPM director and drew outrage over changing explanations about the hack's seriousness.

The report by the House Committee on Oversight and Government Reform faulted the personnel agency for failing to secure sensitive data despite warnings for years that it was vulnerable to hackers. It concluded that the hacking revealed last year could have been prevented if OPM had put in place basic, required security controls and recognized from an earlier break-in that it was actually dealing with a sophisticated, persistent enemy.

"We have literally tens of millions of Americans whose data was stolen by a nefarious overseas actor, but it was entirely preventable," Rep. Jason Chaffetz, a Utah Republican and committee chairman, said in an interview.

"With some basic hygiene, some good tools, an awareness and some talent, they really could have prevented this," he added.

OPM Acting Director Beth Cobert said in a statement the agency disagrees with much of the report and it "does not fully reflect where this agency stands today." She said the OPM hack "provided a catalyst for accelerated change within our organization," including hiring new cybersecurity experts and strengthening its security.

The government discovered the first OPM hacking in March 2014 when a specialized Homeland Security Department team noticed suspicious streams of data leaving its network between 10 p.m. and 10 a.m. - the online equivalent of moving trucks hauling away filing cabinets containing confidential papers in the middle of the night. The government's so-called Einstein intrusion warning system detected the theft.

"DHS called us and let us know, hey, we think this is bad," Jeff Wagner, OPM's director of information security operations, told officials investigating the hack, according to the hack.

For two months, the personnel office worked with the FBI, National Security Agency and others to monitor the hacker to better understand his movements. Officials developed a plan to expel the hacker over a three-day weekend in May 2014, dubbed "the Big Bang." The effort included resetting

administrative accounts, building new accounts for users who had been compromised and taking offline compromised systems.

"The risk of kicking them out too early had come and gone," Wagner said, "and now the risk was becoming having them in too long, and we didn't want to keep them around any longer than we had to."

The problem was far from solved.

Unknown to the experts focused on expelling the hacker, a second intruder posing as an employee of a federal contractor had infiltrated the system weeks before "the Big Bang." That hacker used a contractor's credentials to log into the system, install malicious software and create a backdoor to the network, according to the report.

Over the next several months, roaming unchecked through the system, the hacker stole sensitive security clearance background investigation files, personnel files and, ultimately, fingerprint data.

That breach was not detected until April 2015, when an OPM contract employee traced the flow of stolen material back to an Internet address that had been registered to Steve Rogers, the alter ego of Captain America, indicating a spoof account. By then, sensitive information on millions of American workers had already been compromised.

The report also faulted the personnel office for failing to quickly deploy security tools from an outside firm to detect malicious code and other threats. Once deployed, the tool from Cylance Inc. of Irvine, California, "lit up like a Christmas tree," indicating it found malware throughout the federal computers, an engineer is quoted as saying in the report.

"Could they have done better? Absolutely," said Cylance founder and chief executive Stuart McClure. "But once they had been definitively convinced there was a breach, they took it very seriously."

It said OPM officials misled the public about the scope of the breach and also by saying the two breaches were unrelated when, instead, "they appear to be connected and possibly coordinated," according to the congressional report.

"The two attackers shared the same target, conducted their attacks in a similarly sophisticated manner, and struck with similar timing," the report said.

Though the U.S. suspects the hack was an act of Chinese espionage, the House inquiry did not go into great detail about who was responsible. It mentions that the data breaches discovered in April 2015 were likely perpetrated by the group "Deep Panda," which has been linked to the Chinese military.

Times of Israel

Israeli government okayed sale of spyware that exploits iPhones

Wednesday, 07 September 2016

Byline: Staff Report

Section: general

Jerusalem - NSO Group, an Israeli technology company that created spyware that was found being used to compromise a prominent United Arab Emirates activist's iPhone, had sold the software to an Arab company with the express permission of the Israeli Defense Ministry.
The discovery of the sophisticated spyware, called Pegasus, capable of infiltrating and remotely taking control of iPhones without leaving a trace, forced Apple to push out a security update last week. The software came to light after researchers said the Emirati rights activist, Ahmed Mansoor, was targeted by a simple text message that asked him to tap on a link for information on detainees tortured in the UAE. Suspicious, he forwarded it to internet watchdog group Citizen Lab.

The software can track calls and contacts, collect passwords, read text messages and emails, record calls and trace the whereabouts of the user. Mike Murray, a researcher with Lookout, a San Francisco-based smartphone security company, called it "one of the most sophisticated pieces of cyberespionage software we've ever seen."

The exploit took advantage of previously undisclosed weaknesses in Apple's mobile operating system, iOS 9.3.5, according to reports published late last month by Lookout and Citizen Lab.

According to a report Wednesday in the Yedioth Ahronoth daily, the Defense Ministry's Defense Export Controls Agency (DECA), which must approve the export of sensitive security products, gave NSO Group permission to sell the software to an Arab company.

The report said the decision was met with a great deal of criticism within the agency. A senior Defense Ministry staffer called the export license "a scandal."

A Foreign Ministry official -- none of the report's sources were named due to the sensitivity of the case -- noted that the Israeli company is not accused of taking part in the attempted hacking, but said "the very fact that the company is being linked in the press to a cyberattack on a human rights activist damages the country's good name."

According to the report, the original license allowed NSO to sell a version of Pegasus that would take over the iPhone without requiring its user to even tap the link that would download the spyware.

Merely receiving the text message would allow the takeover. DECA then changed the license to only permit the sale of the version that requires a tap on the link.

The sale itself was facilitated by former senior officials in Israel's defense establishment. The Arab company, its home country and the officials involved on either side were not named in the Yedioth report.

In a statement last month that stopped short of acknowledging the spyware was its own, the NSO Group said its mission was to provide "authorized governments with technology that helps them combat terror and crime."

"The agreements signed with the company's customers require that the company's products only be used in a lawful manner," the statement read. "Specifically, the products may only be used for the prevention and investigation of crimes."

The company said that it "does not operate the software for its clients, it just develops it," according to Channel 2.

Israeli companies have been criticized in the past for selling software to monitor internet and phone communication to regimes with poor human rights records, including in Uzbekistan and Kazakhstan, as well as Colombia, Trinidad and Tobago, Uganda, Panama and Mexico, according to the NGO Privacy International.

In a statement to Yedioth, the Defense Ministry said it "operates an orderly oversight mechanism, under law," of sensitive defense exports, "that works in close cooperation with the Foreign Ministry."

Agence France-Presse
L'avocat général de la Cour de Justice de l'UE retoque l'accord PNR avec le Canada
Thursday, 08 September 2016
Byline: Journaliste maison

Paris - L'avocat général de la Cour de justice de l'UE a estimé que l'accord sur le transfert des données des dossiers passagers (PNR) prévu entre l'UE et le Canada ne pouvait être "conclu sous sa forme actuelle".
Selon l'avocat général, Paolo Mengozzi, l'accord "ne peut être conclu sous sa forme actuelle", est-il rapporté dans un communiqué, car contraire aux droits fondamentaux de l'Union.

L'accord envisagé doit être soumis "à un contrôle strict au regard du droit au respect de la vie privée et familiale et du droit à la protection des données à caractère personnel", considère le magistrat.

Ce dernier s'appuie sur deux arrêts de la CJUE sur ces sujets, dont celui concernant le dossier Max Schrems, requérant autrichien à l'origine de l'invalidation du "Safe Harbour", le précédent accord de transfert de données personnelles entre l'UE et les Etats-Unis. Ce dernier a été récemment remplacé par un nouveau cadre juridique baptisé "Privacy Shield" ("Bouclier de protection des données").

"Il est en effet nécessaire que (...) la Cour s'assure que les mesures projetées, fussent- elles sous la forme d'accords internationaux envisagés, reflètent une pondération équilibrée entre le souci légitime de préserver la sécurité publique et celui, non moins fondamental, à ce que toute personne puisse jouir d'un niveau élevé de protection de sa vie privée et de ses propres données", souligne le communiqué de la CJUE.

Le projet d'accord PNR entre l'UE et le Canada a été signé en 2014, avec pour but de lutter contre le terrorisme et les formes graves de criminalité internationale.

Dans ses conclusions, qui ne lient pas la Cour de justice pour sa décision finale attendue ultérieurement, M. Mengozzi liste de nombreuses conditions à remplir pour que l'accord soit compatible.

Mais surtout, il énumère plusieurs dispositions qu'il juge contraires à la Charte des droits fondamentaux, notamment la possibilité d'élargir le traitement des données PNR "au-delà de ce qui est strictement nécessaire".

L'avocat général dénonce aussi l'autorisation donnée au Canada de conserver des données PNR pour cinq ans en cas de besoin de vérification ou enquête "sans que ne soit requis un lien quelconque avec la finalité de sécurité publique poursuivie dans l'accord".

L'arrêt de la CJUE sera très suivi alors que l'Union vient de se doter de son propre registre européen des données de passagers aériens, après cinq ans d'âpres débats. Les Etats membres ont deux ans pour transposer la directive.

Australian Associated Press
Turnbull breaks down walls to China
Thursday, 08 September 2016
Byline: Paul Osborne

Canberra - There are risks and opportunities when it comes to Australia working more closely with China.
But, as Malcolm Turnbull's visit to Hangzhou for the G20 summit showed, the opportunities outweigh the risks.

The risks are both obvious and subtle.

More regular contact with Chinese authorities and business since the 1970s has led to greater interest, and engagement, in the Australian domestic political process.

But allowing any foreign interests to throw their weight around the political process - through donations and gifts to MPs and political parties - is fraught with danger.

There is a clear public benefit for such donations, whether direct or channelled through entities such as educational bodies, to be banned.

More sophisticated technology in China is also posing its problems.

As more business executives, tourists and politicians take their mobile phones, iPads and computers into China, the threat of cyber nasties creeping into Australian corporate and government computer systems grows.

Australians travelling to China for work are routinely warned about not accepting free USB sticks, or using public wi-fi or plugging into local networks which can pass on subtle computer bugs.

Politically, Turnbull's embrace of greater Chinese investment poses problems as he seeks to deal with the likes of One Nation and the Nick Xenophon Team, which advocate protectionism and tougher thresholds for checks if not outright bans.

The release of data this week about China's level of investment in agriculture - less than 1 per cent - should go some way to addressing this.

Then there is the human rights question. Isn't Australia obliged to expect more progress on freedom of speech and religion and getting China to abide by international law when it comes to the South China Sea before it goes further down the trade track?

But it was the prime minister's visit to the headquarters of the global e-commerce giant Alibaba in the G20 host city that showed the depth of opportunity for Australian businesses in China and the thirst for a more open approach from within China.

On Tuesday, Turnbull signed a deal between Austrade and Alibaba to work more closely on selling more Australian goods online on the popular Tmall.com and Tmall Global websites, focusing on fresh produce such as dairy and seafood.

Alibaba online markets have more than 434 million users and take 12.7 billion orders each year.

There are already more than 1300 Australian brands on the two online platforms, 80 per cent of which had never before reached the Chinese market, and demand is growing exponentially.

An Alibaba hub office is planned for Melbourne by the end of the year to support local operations in Australia and New Zealand and encourage small, medium and large businesses to use it as a stepping stone into exports.

Interestingly, Alibaba founder Jack Ma told Turnbull and journalists, during a visit to the Hangzhou headquarters for the agreement signing, it was a trip to a friend in the NSW city of Newcastle in 1985 that opened his mind to the world.

Importantly for free trade advocates such as Turnbull and Barack Obama, Ma said putting up the walls of protectionism "is the road back to poverty" for his country.

Chinese President Xi Jinping was also making the right noises at the G20 summit about tearing down global trade and investment barriers.

In a bilateral meeting with Turnbull, the president remarked he hoped Australia continued to provide foreign investors a "fair, transparent and predictable policy environment".

It wasn't that long ago Treasurer Scott Morrison knocked back the sale of the NSW electricity distributor Ausgrid to two Chinese buyers, on national security grounds.

The prime minister is adamant China understands Australia's sovereign right to determine what investment is allowed.

Helpfully for Australia, Xi is on the same page when it comes to Turnbull's interest in innovation being the driver of the next economic revolution.

The final G20 communique's call for innovation to remain on the summit's agenda into the 2017 Hamburg event is reflective of his and Xi's thinking.

Also going in Australia's favour during the summit was Turnbull's injection of political reality into the talks, especially over the future of the steel industry.

A global forum was agreed which would monitor Chinese steel production as capacity was reduced by as much as 150 million tonnes by 2020.

While the Europeans went in heavy-handed about China needing to quickly cut back on its production of steel, the prime minister warned his fellow leaders at one session that any adjustments would have "political consequences", put millions of jobs at risk and bring with it "social problems and injustices".

It is this empathy and realism that will stand Australia in good stead when it comes to closer ties with China.

Le Soleil
Cyberattaque contre la CS des Appalaches
Thursday, 08 September 2016
Byline: Ian Bussières

Québec - Des pirates paralysent le système informatique depuis la fin de semaine
Des pirates informatiques paralysent depuis la fin de semaine le système informatique de la Commission scolaire des Appalaches (CSA), dans la région de Thetford Mines. Au total, 75 % des données de l'établissement auraient été perdues et l'escouade des crimes majeurs de la Sûreté du Québec tente de régler le problème et d'identifier les responsables de cette cyberattaque.

Les directions des différentes écoles de la CSA ont rencontré leurs employés mercredi après-midi pour leur annoncer qu'ils devraient fort probablement se débrouiller sans le réseau informatique de la commission scolaire au moins jusqu'à la fin de la semaine.

C'est lors de ces rencontres, selon des employés qui y ont assisté, qu'on a annoncé que le système avait été fermé à la suite d'une attaque menée durant la fin de semaine par des pirates informatiques et que les trois quarts des données étaient perdues. Depuis mardi, il était entre autres devenu impossible pour les travailleurs d'entrer normalement dans le système en utilisant leur code.

Enseignants peu affectés

«Concernant les renseignements personnels, on semble nous dire qu'ils n'auraient pas été touchés par l'attaque», a déclaré au Soleil un employé de la CSA qui préfère taire son identité. «On ne sait pas si le système de paie et de perception des taxes scolaires a été touché, mais il semblerait que les horaires et les listes d'élèves soient hors de danger puisqu'ils sont hébergés ailleurs», poursuit notre source.

Les employés de bureau de la commission scolaire et des différentes écoles auraient donc beaucoup de difficulté à faire leur travail. Quant aux professeurs, ceux qui utilisaient les nouveaux tableaux intelligents pourront continuer de le faire, mais sans être branchés au réseau de l'école. Ce serait la classe iPad de la polyvalente de Black Lake qui serait la plus touchée à la suite de l'attaque.

«Les enseignants ne sont pas les plus affectés. La commission scolaire a branché un ordinateur à un photocopieur pour les enseignants qui auraient besoin de documents sur le réseau de l'école», poursuit notre source.

Silence radio

Le directeur général de la CSA, Camil Turmel, a refusé de répondre aux questions des médias mercredi, son adjointe indiquant que le dossier avait été transféré à la Sûreté du Québec.

Le coordonnateur du secteur des technologies de l'information et des communications de la CSA, Manuel Granger, affirmait toutefois dans un message enregistré que c'est pour «limiter les dommages» que la totalité du système informatique de la commission scolaire avait été arrêté et qu'une cellule de crise avait été mise en place.

Du côté de la Sûreté du Québec, on n'était guère plus loquace. Le sergent Claude Denis a indiqué mercredi que des spécialistes en informatique analysaient présentement la situation pour tenter de régler le problème et que le service d'enquête des crimes majeurs avait été saisi du dossier.

Le Soleil
Possible demande de rançon... en bitcoins!
Thursday, 08 September 2016
Byline: Ian Bussières

Québec - Les pirates informatiques qui ont mené une cyberattaque contre la commission scolaire des Appalaches (CSA) auraient demandé une rançon en bitcoins, une monnaie cryptographique, pour fournir la clé qui permettrait de décrypter le système informatique paralysé depuis la fin de semaine. L'information, qui n'a pas été confirmée aux employés par la direction de la commission scolaire, circulait cependant beaucoup mercredi chez certains employés plus au fait du dossier.

«La direction n'a ni confirmé ni infirmé qu'une rançon en bitcoins avait été réclamée par les pirates», a affirmé au Soleil un employé de la CSA à la suite de la rencontre avec la direction de son école. La Sûreté du Québec a refusé elle aussi de confirmer ou d'infirmer ce scénario.

Si tel est le cas, il ne s'agirait pas d'une première puisque les attaques informatiques dont le but est de réclamer une rançon, aussi appelées ransomwares, se multiplieraient à travers le monde.

Dans une attaque ransomware, un pirate inconnu bloque ou crypte un ordinateur ou un réseau jusqu'à ce qu'une rançon soit payée et, lorsque l'argent a été versé, une clé ou une méthode de décryptage est fournie.

De plus en plus fréquentes

En juin, l'Université de Calgary avait payé une rançon de 20 000 $ afin de récupérer le contrôle de son système après une attaque du genre. Une boutique de vin de Calgary, des cabinets d'avocats de Colombie-Britannique, une famille de Winnipeg et une petite station de radio d'Ostego, au Michigan, figurent parmi les victimes récentes de ce type d'extorsion.

Selon les données de la filiale McAfee du géant de l'informatique Intel, ces attaques auraient plus que doublé au cours de la dernière année, permettant aux pirates de récolter entre 10 et 50 millions $ par mois. La plus importante demande de rançon enregistrée jusqu'à maintenant serait de 800 000 $, mais les pirates qui ciblent des individus plutôt que des entreprises demandent généralement une rançon de quelques centaines de dollars.

Islamic Republic News Agency
Iran to take cyber attacks against its nuclear facilities to domestic, int'l courts
Thursday, 08 September 2016

Tehran - Deputy for the Iranian Prosecutor General Abdolsamad Khorramabadi said Iran is to take the case of cyber attacks to its nuclear centers to relevant domestic and international courts.
He said that based on the article 290 of the Iranian law of criminal procedure, the Prosecutor General's Office has asked the Atomic Energy Organization of Iran (AEOI) to work in harmony with the Iranian Foreign Ministry to follow up the case of cyber attacks through domestic and foreign legal channels.

Based on the guidelines given by the Supreme Leader of the Islamic Revolution as to following up the cases of cyber attacks to the Iranian nuclear facilities and networks, he noted, Iran is going to file cases against the individuals and companies which were behind production and using of the Stuxnet viruses.

He noted that all world countries have filed any attacks to computer systems via compiling viruses or ban software as a criminal act so international courts are ready to take such complaints into consideration.

Sputnik (Russia)
German Intelligence Plans 12% Budget Increase for Communications Monitoring
Thursday, 08 September 2016
Byline: Staff report

Moscow - Germany's Federal Intelligence Service (BND) plans a 12 percent increase in spending on communications monitoring, including the deciphering of encrypted communications, in 2017, Der Spiegel reports.
The 2017 BND budget for the purpose is projected to be 808 million euros (about $909 million), the news magazine said on Wednesday citing secret budget documents.

The twelve percent increase over the current year comes amid BND plans to boost its response to the widespread use of messenger services such as WhatsApp, Der Spiegel explained. The services encrypt the messages of its users making it difficult for intelligence services to capture the content. BND is planning to overcome this difficulty, which is necessary amid the rise of cybersecurity and terrorism threats.

The Intercept
Google Program to Deradicalize Jihadis Will Be Used for Right- Wing American Extremists Next Thursday, 08 September 2016
Byline: Naomi LaChance

Washington - A Google-incubated program that has been targeting potential ISIS members with deradicalizing content will soon be used to target violent right-wing extremists in North America, a designer of the program said at an event at the Brookings Institution on Wednesday.
Using research and targeted advertising, the initiative by London-based startup Moonshot CVE and Google's Jigsaw technology incubator targets potentially violent Jihadis and directs them to a YouTube channel with videos that refute ISIS propaganda.

In the pilot program countering ISIS, the so-called Redirect Method collected the metadata of 320,000 individuals over the course of eight weeks, using 1,700 keywords, and served them advertisements that led them to the videos. Collectively, the targets watched more than half a million minutes of videos.

The event at Brookings was primarily about the existing program aimed to undermine ISIS recruiting. "I think this is an extremely promising method," said Richard Stengel, U.S. Undersecretary of State for public diplomacy and public affairs.

Ross Frenett, co-founder of Moonshot, said his company and Jigsaw are now working with funding from private groups, including the Gen Next Foundation, to target other violent extremists, including on the hard right.

"We are very conscious as our own organization and I know Jigsaw are that this [violent extremism] is not solely the problem of one particular group," Frenett said.

"Our efforts during phase two, when we're going to focus on the violent far right in America, will be very much focused on the small element of those that are violent. The interesting thing about how they behave is they're a little bit more brazen online these days than ISIS fan boys," Frenett said.

He noted that this new target demographic is more visible online.

"In the U.K. if someone in their Facebook profile picture has a swastika and is pointing a gun at the camera, that person is committing a crime," Frenett said. "In the U.S., there is absolutely nothing wrong with that. So we found that when we're looking for individuals that are genuinely at risk of carrying out violence, that they're relatively open online."

Adnan Kifayat, head of global security ventures at Gen Next Foundation, said he is optimistic about applying the ISIS approach to North America. "Our interest is in countering extremism... particularly in the homeland," he told the Intercept.

Gen Next Foundation, based in Newport Beach, Calif., was founded by a group of young executives, authors, entrepreneurs and others to fight terrorism.

In the ISIS pilot program, the YouTube channel pulls preexisting videos that, according to Yasmin Green, the head of research and development for Jigsaw, "refute ISIS's messaging."

One video is from a woman who secretly filmed her life in ISIS-controlled Raqqa. Another shows young people in Mosul, their faces obscured by keffiyehs for their protection, talking about life under the Islamic State.

"The branding philosophy for the entire pilot project was not to appear judgmental or be moralistic, but really to pique interest of individuals who have questions, questions that are being raised and answered by the Islamic State," Green said.

The next phase will also hone in on changes in users' behavior.

"The idea that you can't measure consumption patterns online is frankly absurd," Frenett said.

London Daily Telegraph
Rudd warns of struggle to stop online extremists
Thursday, 08 September 2016
Byline: Christopher Hope

London - Security experts are struggling to stop the spread of extremist messages on the internet despite taking down 1,000 videos a week, the Home Secretary has admitted.

Amber Rudd said she was in talks with social media websites about setting up a new industry standard board to agree the rules that set out when sites should be taken down.

The new Home Secretary was grilled by MPs on the Commons home affairs committee about what more could be done to force US sites like Twitter, Facebook and YouTube to take action. Ms Rudd said that major internet companies could take more responsibility "because the speed these damaging videos get put up and then we manage to take down - at the moment we are taking down 1,000 a week of these sites - is too slow compared to the speed at which they are communicated".

Ms Rudd was particularly asked what more could be done to require them "frequently and regularly" to take down websites "but also to report content to the police".

She said: "I do think more can be done and we are in discussions with industry to see what more they are prepared to do. We would like to see a form of industry standard board that they could put together in order to have an agreement of oversight and to take action much more quickly on sites which will do such damage to people in terms of making them communicate terrorist information."

Baroness Shields, a former Facebook executive and a Home Office minister, was also in talks with internet service providers internationally.

The committee warned in its report that social media websites were becoming the "vehicle of choice" for spreading terrorist propaganda but websites are policing them with just a "few hundred" employees.

The committee accused US technology giants including Google, Facebook and Twitter of "passing the buck" and said that they have become a "recruiting platform for terrorism".

Its report said: "These companies are hiding behind their supranational legal status to pass the parcel of responsibility and refusing to act responsibly in case they damage their brands."

'I do think more can be done and we are in discussions with the industry to see what they are prepared to do'

CNN.com
FBI director defends Clinton email probe, document releases
Wednesday, 07 September 2016
Byline: Evan Perez

Washington - FBI Director James Comey is defending the bureau's Friday afternoon release of documents from the Hillary Clinton email investigation, saying "we don't play games" and that the documents were put out when ready.

In a memo to employees Wednesday, Comey said the decision to not recommend charges against the now-Democratic nominee wasn't a close call.

"At the end of the day, the case itself was not a cliff-hanger; despite all the chest-beating by people no longer in government, there really wasn't a prosecutable case," he said in the memo.

In recent weeks, Comey has met with groups of former FBI agents as part of his routine visits to field offices around the country. In at least one recent such meeting,

according to people familiar with the meeting, former agents were sharply critical of the FBI's handling of the Clinton probe and particularly the decision to not recommend charges against Clinton. Comey gave the meeting participants a similar answer about the case not being a cliff-hanger.

Comey said he briefly considered holding the documents until after the Labor Day holiday, knowing that the Friday afternoon release would likely prompt criticism. He also said more document releases are coming.

"I almost ordered the material held until Tuesday because I knew we would take all kinds of grief for releasing it before a holiday weekend, but my judgment was that we had promised transparency and it would be game-playing to withhold it from the public just to avoid folks saying stuff about us," Comey said.

"We don't play games. So we released it Friday. We are continuing to process more material and will release batches of documents as they are ready, no matter the day of the week," Comey said.

He concluded the memo by writing, "Those suggesting that we are 'political' or part of some 'fix' either don't know us, or they are full of baloney (and maybe some of both)."

On Tuesday, Republican House Speaker Paul Ryan criticized the FBI's handling of the matter, accusing the bureau of playing politics with the release.

"It's like the most buried time you could ever put out a story. I'm surprised. I can't believe that they would do what is such a patently political move. It makes them look like political operators versus law enforcement officers," Ryan said in a radio interview with WRJN's Glenn Klein.

Le Soir (Belgique)
« Epier Facebook ne suffit pas : il faut investir dans l'humain »
Thursday, 08 September 2016
Byline: Pierre Vassart

Bruxelles - Sécurité Yvan Mayeur s'agace du mutisme de Jan Jambon

Le ministre de l'Intérieur se réjouissait mardi de l'expérience pilote de recrutement local de policiers à Anvers. La Ville de Bruxelles voudrait faire de même, mais le ministre de l'Intérieur ne répond pas.

Scrogneugneu ! Le bourgmestre de la Ville de Bruxelles Yvan Mayeur (PS) a retrouvé toute sa verve à son retour de vacances. Et lorsqu'il a lu mardi que, sollicité par l'agence Belga, le cabinet du ministre de l'Intérieur Jan Jambon (N-VA) avait indiqué que ce dernier était « disposé à étendre à d'autres zones de police l'expérience en cours depuis l'automne 2015 à Anvers qui vise à permettre de recruter localement des agents afin d'accroître la diversité au sein des corps de police » , citant Gand en exemple, il a respiré un grand coup. Ah bon ?, réagit-il en substance. Et pourquoi la Ville de Bruxelles, elle, ne peut-elle pas procéder à ces recrutements locaux de policiers ?

C'est que, rappelle Yvan Mayeur, il avait déjà écrit au ministre en octobre dernier afin que la Ville puisse également procéder à ce type de recrutement pour la zone de Bruxelles Ixelles. Mais son courrier était demeuré sans réponse. « Le fédéral ne nous aide pas ! Alors qu'avec toutes les tâches qui lui incombent, la police locale souffre d'un vrai problème d'effectifs , rappelle-t-il. Et que la Ville souhaite un effectif policier qui corresponde davantage à sa réalité démographique et sociologique. » Une volonté mise en oeuvre par ailleurs : « Dans tous ses services, administration, hôpitaux, CPAS, etc., la Ville s'est largement ouverte à son caractère diversifié. Mais pour la police, impossible d'avancer ! » , regrette-t-il.

Il est vrai que l'expérience d'Anvers, dont le bourgmestre Bart De Wever (N-VA) se plaît à répéter qu'elle est un succès, est présentée comme un projet pilote, et que son évaluation sur deux ans est toujours en cours. Mais là où tique Yvan Mayeur, c'est lorsqu'il lit les propos du porte-parole du ministre de l'Intérieur, qui déclarait à Belga : « « Nous avons initialement voulu une expérience de deux ans à Anvers, mais les résultats sont si encourageants que nous sommes enclins à regarder si nous pouvons entamer un tel projet à Gand ou dans d'autres villes » La capitale, ses multiples obligations en matière de sécurité (manifestations, sommets internationaux, événements, etc.) ne constitue manifestement toujours pas une priorité pour l'Intérieur, aux yeux du bourgmestre.

Et lorsqu'on objecte que le « plan Canal » du ministre de l'Intérieur, dont la phase 2, qui concerne la Ville de Bruxelles, a démarré début septembre et prévoit un renfort de 25 policiers fédéraux dans la zone de police de Bruxelles Ixelles, Yvan Mayeur avale de travers. « Ils sont affectés dans notre zone mais repartent aussitôt. Rien ne les oblige à rester, par exemple pour une période de cinq ans. Ils demandent tout de suite à être réaffectés. » Ce que confirmait d'ailleurs mardi dans nos pages la bourgmestre de Molenbeek Françoise Schepmans (MR), dont la commune a bénéficié de la première phase du « plan Canal », avec un renfort de cinquante policiers fédéraux : 48 policiers avaient été transférés sur sa zone au premier semestre, il n'en reste plus que 30 aujourd'hui. Autre exemple, cité par La Libre Belgique : pour la zone de police Midi (Anderlecht, Forest et Saint-Gilles), 15 des 18 policiers fédéraux en renfort affectés à cette zone l'ont été sans leur consentement. Leur départ rapide ne constituerait donc pas une surprise.

Ce n'est pas première fois que le bourgmestre de la Ville tire le signal d'alarme. On se souvient que début juillet, il avait (encore) écrit au ministre de l'Intérieur pour réclamer des renforts. « Nos policiers

sont fatigués » , s'était-il désolé (Le Soir du 16 juillet). A l'époque, le cabinet de Jan Jambon avait répliqué que Bruxelles bénéficiait bien de renforts de la police fédérale pour les grandes manifestations (c'était à la veille de la Fête nationale). Aujourd'hui, Yvan Mayeur remet le couvert : « C'est très bien d'investir dans la technologie pour renforcer la sécurité, dans la surveillance des réseaux sociaux et tout ça. Mais épier Facebook ne suffit pas : il faut investir dans l'humain, maintenir le contrôle humain. Les terroristes ne communiquent pas via Facebook d'ailleurs, mais via Telegram Messenger. Un réseau crypté. »

La solution serait-elle pour la Ville de se tourner vers des sociétés de gardiennage privées, comme on en a vu dans le parc de Bruxelles à l'occasion de la Fête de la bande dessinée ou, comme on en verra encore ce week-end autour de l'événement « Eat Brussels, drink Bordeaux » ? Des affichettes ont effet été placardées aux entrées du parc, reproduisant une ordonnance de la Ville de Bruxelles qui autorise les vigiles privés à fouiller les sacs des visiteurs.

« Rien à voir , répond Yvan Mayeur. Ce dispositif est autorisé et réglementé depuis plusieurs années. Mais il est vrai que le climat actuel contraint les organisateurs d'événements privés à assurer la sécurité de leur manifestation. »

24 Heures (Suisse)
Une indiscrétion aussi crasse qu'inutile
Thursday, 08 September 2016
Byline: Yoann Péclard

Opinion - On peut en apprendre beaucoup sur vous en consultant votre ordinateur: votre santé, vos informations bancaires, qui sont vos amis, ce que vous leur dites, où vous avez mangé ou voyagé, ce que vous aimez, ce que vous achetez, vos opinions Bien plus que si l'on fouillait votre maison de fond en comble.
Or, en Suisse, nos foyers sont bien protégés face aux possibles dérives de l'Etat. La police ne vient pas vous fouiller sans raison valable et sans que la justice soit derrière la procédure. A la question « Acceptez-vous que des inconnus entrent chez vous pour vous fouiller, sans vous le demander, sans se justifier et à n'importe quel moment? » je ne connais personne qui répondrait par l'affirmative.

Pourtant, en votant oui à la LRens, c'est ce que vous ferez, non pas pour votre maison, mais pour votre ordinateur. Grâce aux nouveaux moyens de contrôle accordés au Service de renseignement de la Confédération (SRC) et à l'affaiblissement du contrôle judiciaire, vous serez à nu. Exactement comme si un agent entrait dans votre salle de bains au moment de votre douche. Ce sera la même violation de votre intimité, sauf qu'elle sera invisible.

Et pour quelle utilité? Les immenses masses de données collectées en France ou aux Etats-Unis n'ont jamais permis de stopper les criminels. Pire encore, des agents de la justice française critiquent

vertement cette politique d'espionnage, elle ralentirait le véritable travail d'enquête. Alors pourquoi importer ce modèle ici?

Et si, en tant qu'honnêtes citoyens, nous n'avons rien à cacher, nous n'avons justement pas à accepter la suspicion générale et la violation de nos vies sans que nous le sachions et sans recours possible.

Il serait stupide de créer une nouvelle usine à gaz fédérale

La nouvelle LRens est censée améliorer la lutte étatique contre le terrorisme et l'espionnage en légalisant les possibilités d'interceptions téléphoniques et la surveillance d'Internet. Cela en cas d' « indices fondés » (et non de preuves) et sans mandat délivré par un juge. Elle s'inscrit dans l'action de surveillance d'Internet par la NSA américaine et par sa consoeur anglaise, le Government Communications Headquarters. Les deux pratiquent en deux étapes, à savoir que le suspect, ses correspondants et ceux qui prennent contact avec les correspondants sont surveillés à leur insu et parfois pendant longtemps. Ils ne sont avertis qu'éventuellement et a posteriori.

La question qui se pose en Suisse consiste à se demander s'il est absolument nécessaire de pondre 182 articles de loi pour considérer une douzaine de cas par année, comme l'annonce le Conseil fédéral.

S'agirait-il de complaire aux Américains qui nous espionnent éhontément?

Selon Edward Snowden, les agents du renseignement suisse ne font pas du tout peur aux espions américains.

Nous aurions grand tort de surévaluer la menace terroriste en Suisse, ainsi que l'efficacité du renseignement électronique. La collecte du renseignement est une chose, son analyse et son traitement en sont d'autres. Ce dont le pays a surtout besoin, c'est d'analystes en nombre suffisant, compétents et bien formés. Et parmi eux des arabisants pointus.

Enfin, s'agissant des contrôles prévus par la loi, les écoutes sauvages menées en Allemagne de 2002 à 2016 par le Bundesnachrichtendienst pour le compte des Américains devraient nous rendre circonspects. Il serait stupide de créer une nouvelle usine à gaz fédérale.

Fox News
DHS chief has 'a lot of confidence' in security of US electoral infrastructure
Thursday, 08 September 2016
Byline: Matthew Dean

Washington - Homeland Security Secretary Jeh Johnson said Wednesday he has "a lot of confidence" in the security of America's electoral infrastructure despite concerns about intrusions by cybercriminals.

Johnson's declaration, in response to a question from Fox News, follows recent hack attacks on two different state election websites that are believed to have been the work of Russian actors, according to sources.

Those actions, which were disclosed in an August FBI bulletin distributed to law enforcement agencies and obtained by Fox News, urged states to contact their respective Boards of Elections to determine if they had experienced any similar activity.

While he would not comment directly on the cyber activity, citing an ongoing FBI investigation into the matter, Johnson said he could assure the American public that DHS is up to the challenge of safeguarding state election systems. He added that election officials should consult the department on cybersecurity matters.

"The Department of Homeland Security is in a position to shore up electoral infrastructure," the DHS chief said. "We are in a position to help - to offer best practices, information sharing, vulnerability assessments, incident response."

The recently disclosed hacks, which successfully compromised the election system of one state and targeted an election website in another state, have added fuel to already loud concerns over the potential for foreign nationals to influence the 2016 presidential race.

Russian government-linked hackers are also believed to have carried out cyber breaches of the Democratic National Committee and the Democratic Congressional Campaign Committee, seizing troves of information over the course of those attacks.

U.S. officials have yet to publicly name Russia as the perpetrator in either of those incidents and Russian President Vladimir Putin has denied any involvement.

Sources told Fox News that FBI investigators are working to determine the exact scope of the intrusions, which cybersecurity analysts fear could run deeper than already disclosed, given the hackers' ability to "island hop" to other networks once an initial compromise is made.

For some IT security experts, any Russian connection would not be surprising, given the Kremlin's recent reported history of using cyber activity as a clandestine tool for meddling in foreign affairs.

"You're seeing more and more manifestations of information warfare via cyber means to destabilize U.S. public opinion and undermine the trust and confidence in American institutions like, for example, the electoral system," Strategic Cyber Ventures CEO Tom Kellermann told Fox News in a recent interview.

As Fox News has previously reported, cybersecurity analysts have implicated Russia-linked cybermilitias with web-based attacks against a number of foreign entities over the past several years. Specific to the United States, multiple sources familiar with the research behind these incidents said that the Kremlin

has targeted the Department of State, the Pentagon, the White House, and numerous private sector entities, including several media outlets.

While not directly naming Russia as the perpetrator in the DNC, DCCC, or state election system attacks, the United States' top intelligence official did acknowledge the Kremlin's persistent cyber activity.

In agreeing with a recent public admission by President Obama, Director of National Intelligence James Clapper acknowledged "the Russians hack our systems all the time, not just government but also corporate and personal systems."

Speaking Wednesday at the Intelligence and National Security Summit in Washington, D.C., the DNI added a blunt prediction for the nation's path forward when it comes to dealing with the cyber threat.

"Cyber will continue to be a huge problem for the next presidential administration, as it has been a challenge for this one," Clapper said.

Bloomberg View
Snowden Is Turning Into a Liability for Putin
Friday, 09 September 2016
Byline: Leonid Bershidsky

Column - Edward Snowden is increasingly unhappy with the situation in Russia, where he has lived for more than three years. President Vladimir Putin once welcomed the National Security Agency contractor for his propaganda value, but he may be wondering if it's all been worth it.
Snowden arrived in Moscow in June 2013. That was almost a year before the Crimea annexation, and Russia could still try to sell itself to radical leftists who admired Snowden as the lesser evil, compared with the Big Brother U.S. Putin talked a lot about Snowden showing obvious delight for thumbing his nose at the U.S., which had tried to intercept the whistle- blower. He described Snowden as a "weird guy," an idealist, who was safe in Russia even though he had no secrets to pass on.

After Crimea, though, such statements started to appear hollow. "Russia is not the kind of country that hands over fighters for human rights," Putin said at the St. Petersburg Economic Forum in May 2014. That the Russian president could talk about human rights after faking a secession referendum in Crimea would have been funny if it weren't so manipulative.

Snowden appeared to play along. In 2014, he took part in Putin's carefully stage-managed and scripted annual call-in show, asking the Russian leader whether Russia intercepted, stored and analyzed its citizens' electronic communications. Putin said Russia used advanced technology to fight terrorism. "But we do not allow ourselves to use it on a mass scale, in an uncontrolled way," he added. "I hope, I very much hope, that we never will."

Snowden defended what appeared to be a softball question in a column for The Guardian, saying that he had "sworn no allegiance" to Russia and that he would fight total surveillance everywhere. The Guardian article helped him maintain credibility among Western radicals.

On several other occasions, Snowden criticized Russia for its treatment of homosexuality and for attacks on internet freedoms, but the Kremlin was unconcerned. "These are rather arguable statements, but he has his point of view," Putin's press secretary, Dmitri Peskov, said last year. "Yes, he lives in Russia, but it doesn't mean anything is being imposed on him."

In recent months, though, Snowden has stepped up his harsh criticism of Russian ways: It became clear to him that Putin had lied during that call-in show.

The NSA leaker took to Twitter in July, when the Russian Parliament was passing the so-called "Yarovaya package" -- a fiercely repressive set of laws aimed at establishing total control over Russians' online communications. Internet providers and mobile operators are expected to record and store all conversations and message exchanges for six months, and their metadata for three years. Internet

companies are obliged to help the Russian secret police decrypt any encrypted communication. Snowden's condemnation was vehement.

The Yarovaya package is harsher than any electronic surveillance legislation in the U.S., because the Russian measures openly tell citizens that their communications will be monitored pretty much at the discretion of the intelligence services. It embodies all the abuses that Snowden has opposed.

Three years is enough time to understand Russian politics a little better, and Snowden appears to be interested in more than his professional area. On Wednesday, he tweeted about the recent news that Russia's last remaining big independent pollster, the Levada Center, has been designated a "foreign agent," along with some of Russia's strongest human rights organizations, for accepting foreign research grants.

Levada received the designation after publishing a poll that showed Putin's United Russia losing support ahead of the Sept. 18 parliamentary elections. Snowden now openly criticizes the Kremlin on matters of political importance, such as its "anti-terrorism" policy and its own special brand of electoral democracy. The whistle-blower tweets in English, but Russian media, including pro-Kremlin ones, invariably pick up his posts.

I would be surprised if the Kremlin weren't irritated. It does its best to squeeze local critics out of the country or discredit them, yet it's stuck harboring a foreigner whose initial gratitude may have worn out and who is less willing to give Putin the benefit of the doubt.

Snowden has tweeted that he fears retaliation for his criticism, but he won't desist. There aren't too many ways for the Kremlin to retaliate, though, without handing a moral victory to the U.S. It certainly won't extradite Snowden: In March, when Donald Trump called for the return of the whistle- blower, Peskov said the Russian government's position hadn't changed. It would be no surprise, however, if arrangements were quietly made to move Snowden to another asylum country. With his zealotry, he is a liability to Putin, and he may never really have been an asset.

The Media Line
Iran Introduces Halal Internet
Friday, 09 September 2016
Byline: Katie Beiter

Jerusalem - In an effort to "de-Westernize" and maintain control over internet users and the spread of information, the Iranian government has revealed a state-sponsored internet known formally as the National Information Network. This new service, nicknamed the "halal" (lawful) internet, is another ploy by the Iranian state to limit the spread of information into and around Iran.
"The network is basically a government effort to create a nationally controlled internet," Sanam Vakil, an associate fellow at Chatham House, an international affairs think tank, in London, told The Media Line.

"Iran is a state that has heavy internet censorship so a national internet would be a way to provide increased government control."

This state-sponsored internet acts more as an intranet, which is essentially a private network controlled by an organization, which, in this case, is the Iranian government. In this type of system, all users are identifiable and the state controls what users can and cannot see. These types of systems are common in workplaces and other large organizations to control what employees can and cannot access at the workplace.

"It is a more managed, internal internet," Gabi Siboni, head of cyber security at the Institute for National Security Studies at Tel Aviv University, told The Media Line.

The Islamic Republic of Iran, which is a theocracy, has been vehemently anti-Western since the Iranian Revolution of 1979, which overthrew the dictatorial monarchy and instead introduced all- powerful religious figures, known the ayatollahs. Since then, the country has opposed all things Western, blaming the West and American infiltration for being oppressed prior to the 1979 coup.

The state has maintained a tight grip on the press and the spreading of information in and around Iran, which is ranked 169 out of 180 for lack of press freedom by the Press Freedom Index compiled by Reporters Without Borders, an NGO dedicated to defending media freedom. In a country where journalists are arrested and sometimes beheaded, publishing anything anti-government or anti-Islam on websites or social platforms is often grounds for arrest.

"There is no open freedom of information or freedom of the press in Iran," Vakil said. "This new service is an effort to have more institutionalized control over the internet and, particularly, the freedom of information."

Both the government and the clergy fear Western infiltration, especially through the world-wide Internet. Thus, creating an intranet can keep Western topics, from pornography to fashion, out of Iran.

"It's a nice culmination, or next step, in a long series of attempts to control what Iranians can see," Ze'ev Maghen, a Middle Eastern history professor at Bar-Ilan University near Tel Aviv told The Media Line. "It's like an amplified 'Google safe' search."

While the Iranian government does not want to ban the internet, they want to purify it. The government has even created an agency known as the Cyberspace Supreme Council to police internet usage in the country, Vakil added.

This network service is not the only one still available to Iranians, however. In an effort to attract users, the government has offered a series of incentives, like low prices and quick installation, to using this state-sponsored internet, which claims to be 60 times faster than any current internet in Iran.

"This is a persuasive tool to increase internet usage and deceive people that the internet connection is faster," Vakil said.

Most Iranians have figured out ways to circumvent the closely monitored web. Many people use proxies, which are essentially intermediate servers that hide an internet user's IP address creating anonymity and allowing users to access sites that are currently unavailable in their countries.

"If I'm looking at something in Google and I don't want people to know what I am looking for, I go through a VPN (a virtual private network) and the request comes from a different IP address and it is presumably more secure," Siboni said.

This new internet service was unveiled after some 100 internet users were arrested in Iran and two press agencies as well as two online news outlets were blocked, according to Reporters Without Borders.

Journal de Montréal
Une cyberattaque dans 25 écoles sème la grogne
Friday, 09 September 2016
Byline: Eliane Thibault

Thetford Mines - Un programme axé sur l'enseignement avec des tablettes électroniques a dû revenir aux bons vieux cahiers d'exercices en raison d'une cyberattaque.
Les 25 écoles de la Commission scolaire des Appalaches, dans la région de Chaudière-Appalaches, ont dû revoir leurs méthodes d'enseignement depuis mardi matin. Le système informatique de la Commission a été victime d'une cyberattaque qui a paralysé toutes les activités de l'organisation qui nécessitent du matériel informatique.

Les données de la Commission scolaire auraient été cryptées et une demande de rançon en bitcoins aurait été exigée pour qu'elles soient rendues lisibles de nouveau.

«Les tableaux blancs interactifs ne fonctionnent plus dans notre classe, raconte Mariloup, une élève de 8 ans. Notre professeur a dû utiliser l'ancien tableau blanc avec les crayons-feutres qui s'effacent.»

DE LA tABLEttE Au tABLEAu

La fillette trouve ennuyeux d'avoir perdu une période de classe en technologie parce que les ordinateurs ne fonctionnent pas. Quant aux enseignants, c'est surtout le système de paie qui les inquiète. Plusieurs d'entre eux ont contacté leur syndicat à ce sujet.

«Être enseignant, c'est apprendre à se revirer sur un 10 cents. Quand ils ont vu que le matériel informatique ne fonctionnait pas, les enseignants ont tout simplement recommencé à utiliser le tableau et les craies», raconte le président du Syndicat de l'enseignement de l'Amiante, Francis Jacob.

Une plainte a été déposée auprès de la Sûreté du Québec qui a dépêché une équipe spécialisée. Afin de ne pas nuire à l'enquête, la Commission scolaire a refusé toutes les demandes d'entrevue. Impossible de savoir si elle a ou non l'intention de payer la rançon.

Marc-André Léger, spécialiste de la sécurité informatique, n'est pas étonné que des attaques de ce type aient lieu. Toutefois, il affirme qu'habituellement, ce sont de grandes corporations privées qui sont ciblées.

«D'après moi, c'est une coïncidence avec de l'hameçonnage. Quelqu'un a envoyé 1 million de courriels et [il est] probable qu'une personne de la Commission scolaire a cliqué sur quelque chose. Les malfaiteurs ont réussi à entrer dans le réseau et ont pu se dire qu'il y avait de l'argent à faire ici», explique celui qui est aussi chargé de cours à l'Université de Sherbrooke.

BBC News
Errors in communications data use led to wrongful arrests, report finds
Thursday, 08 September 2016

London - Errors in the use of communications data led to the arrests of 13 innocent people, a watchdog has said.
The wrongful arrests were among 23 serious mistakes made in acquiring 761,702 items of communications data, the Interception of Communications Commissioner report found.

Other incidents included delayed welfare checks on vulnerable people.

Communications data includes when and where electronic communications are made, but not their content.

'Devastating impact'

The report found mistakes were made either by law enforcement agencies or communications service providers, with the majority of errors believed to relate to child abuse inquiries.

In these instances often the evidence used was an internet address which was wrongly linked to an individual.

There were six instances in which people unconnected to the investigations were visited by police and seven cases that resulted in delayed welfare checks on vulnerable individuals.

Of the 23 serious mistakes, 14 were human errors and the other nine "technical system errors".

Commissioner Sir Stanley Burnton's annual report said: "Any police action taken erroneously in such cases, such as the search of an individual's house that is unconnected to the investigation or a delayed welfare check on an individual whose life is believed to be at risk, can have a devastating impact on the individuals concerned."

Overall, 1,199 communications data errors were reported to the watchdog in 2015 - an increase of 20% on the previous year.

Of these, 86.6% were attributable to public authorities, 12.6% to communications service providers and 0.8% to other parties.

Nearly 94% of the requests were by police and law enforcement and just under 6% by the intelligence agencies.

The watchdog also inspected prisons and identified some instances where not all of the calls made by inmates subject to monitoring were being listened to, or that the calls were not being listened to quickly enough.

The report said: "This is of concern because a significant piece of intelligence could be missed completely or not reacted to promptly, leading to a serious incident occurring which may have otherwise been prevented."

Meanwhile, a separate report, also released on Thursday, revealed that security services made nearly double the number of mistakes using intelligence powers in 2015 than in the previous year.

Almost all of the 83 errors in 2015 led to an intrusion into privacy "to some degree", the Intelligence Services Commissioner found.

MI5 was also criticised for its form-filling procedures and for inserting unauthorised devices into MI5 systems, such as charging mobile phones, on six occasions.

In a written statement to the Commons, Prime Minister Theresa May said both reports "recognise the diligence and rigour of those who use investigatory powers".

She said: "These are important powers that are used, when necessary, to keep our country safe.

"Both reports contain details of the recommendations that the commissioners have made to continue to improve the way that these powers are used.

"The public authorities who have received these recommendations will be giving careful consideration to them and how to further improve their processes."

Wall Street Journal
U.S. Voting System So 'Clunky' It Is Insulated From Hacking, FBI Director Says
Friday, 09 September 2016
Byline: Devlin Barrett

Washington - The head of the Federal Bureau of Investigation sought to calm fears that Russians or others could electronically sabotage the nation's election in November, saying the 50-state voting system is so dispersed and "clunky" it would be difficult for hackers to affect the outcome.
Appearing at a panel with other senior U.S. intelligence officials Thursday, FBI Director James Comey was asked about the concerns that hackers acting on behalf of the Russian government might try to manipulate the presidential election.

Such concerns have grown in recent weeks, after the FBI issued an alert to state officials about the possibility of hackers penetrating state election computer systems. In Arizona, a hacker obtained one of two credentials needed to access the state's voter-registration system.

The FBI is also investigating a number of computer data thefts from Democratic Party organizations, in which the leading suspects are Russian intelligence operatives, according to officials close to the case.

Mr. Comey wouldn't discuss those investigations, but he tried to reassure participants at the Intelligence and National Security Summit that there is a big difference between accessing voter-registration records and hacking into actual vote-counting systems.

"The beauty of the American voting system is that it is dispersed among the 50 states, and it is clunky as heck," said Mr. Comey. "A lot of people have found that challenging over the years, but the beauty of that is it's not exactly a swift part of the internet of things, and so it is hard for an actor to reach our voting process."

Even federal elections are conducted by state election agencies, meaning there is no centralized computer system or technology tabulating votes. Much of the vote-counting is still done by people, not machines, Mr. Comey noted, which "makes it more resilient and farther away from an actor who might be willing to crawl down a fiber optic cable."

Even if hackers could reach into a state voting system, they may find "it actually isn't a fiber optic cable, it's a woman named Sally, a guy named Joe [who] pull out the punch cards, and that's hard to reach," Mr. Comey said. "There's a lot of pain in that, but there's a lot of beauty."

A day earlier, Defense Secretary Ash Carter warned Russia that the U.S. would not ignore "efforts to interfere with our democratic processes," though he didn't mention hacking specifically.

Russian President Vladimir Putin has denied the Kremlin was involved in the hacks, but he suggested the subsequent leaks of the Democrats' internal discussions was a positive development.

BuzzFeed News
Washington Really Doesn't Want To Deal With A Cyber War With Russia
Friday, 09 September 2016
Byline: Ali Watkins, Sheera Frankel

Washington - The Obama administration is wary of publicly accusing Russia of meddling in the US election despite increasing pressure from within Washington, for fear of fanning public concerns over the security of the election and igniting a cycle of tit-for-tat cyber attacks, several US government officials told BuzzFeed News.
"Do you really want to call it out, and recognize it? With everything you do, you should be reinforcing the public's confidence in the election system," said one US intelligence official, who is frequently briefed on Russia issues. Calling Russia out, he said, could also validate widespread worries over the security of the November election. "Do you really want that shitstorm? I don't think you do."

The White House has not assigned blame for the hack of the Democratic National Committee emails, which cybersecurity experts say were most likely stolen by Kremlin-backed hackers. The emails were eventually published by Wikileaks on the eve of the Democrats' convention. Wikileaks' founder, Julian Assange, has refused to reveal the source for the emails despite growing concerns over his ties to Russia. The private cybersecurity experts who provided the strongest evidence that Russian actors were behind the hack linked them to a group that was previously accused of hacking into the State Department and White House. Suspicions of Russian meddling were further fueled when the FBI warned last week of two suspected-Russian linked hacks into state election systems.

Pressed at the G20 summit in China on Monday, President Barack Obama again declined to publicly point a finger at Russia, citing fears of a Cold War-style cyber arms race.

"Frankly, we got more capacity than anybody both offensively and defensively. But our goal is not to suddenly, in the cyber arena, duplicate a cycle of escalation that we saw when it comes to other arms races in the past," Obama said when asked to address the allegations that Russia was meddling in US politics.

Defense Secretary Ash Carter, speaking in the UK on Wednesday, warned Russia against "efforts to interfere with our democratic process," going a step further than the White House but stopping short of directly blaming them for recent hacks.

Asked whether it was concerned about potentially naming Moscow, National Security Council spokesman Mark Stroh declined to comment, and referred inquiries on the matter to the FBI.

The Bureau, which is investigating the DNC hack, has yet to publicly identify Russia as the culprit. "I'm going to continue the streak of not talking about that," Comey said Thursday, when asked at an intelligence conference to address Russia's alleged attempts to manipulate the election.

Washington has long been worried about Russian hacking, and the intelligence community has begun delegating more and more of its resources to countering and probing Russian threats.

But, until the DNC hack, the concern has been over the type of intelligence Russia was accessing and how it would use it to thwart US ambitions on the world stage. Russian hackers were suspected in 2015 of breaching both the State Department and White House servers, gaining access to sensitive, though unclassified, information.

Nothing from that hack has ever been made public. So why were the DNC emails leaked? Some cybersecurity experts say the US and Russia are already engaged in a type of cyber Cold War, in which each side is continually testing the other to see how far they can go.

"There are no rules to this, but both sides are moving pieces around their chess boards and trying to figure how close they can get to a check-mate without acknowledging that they are actually playing the game," said one cybersecurity expert, who consults with US officials regularly though his position at a private company keeps him from speaking publicly about his work.

Another US intelligence official said it appeared as though actors in Russia weren't even trying to hide their efforts anymore. The official said his organization had buckled down on official travel to Moscow, urging employees to follow protocol and leave their phones and laptops at home. Asked what that meant for working conditions, the official said "We just have to trust that the facilities we use in the embassy are secure."

If Russia is proven to be behind the DNC hack, it would mark a serious escalation, with Russia using intelligence it had accessed through cyberespionnage to try and influence elections in the US.

But the question of concrete attribution is becoming more difficult each year, as techniques to mask location and inject false flags into code become more and more sophisticated.

"If the US were to stand up and say 'Russia hacked the White House, Russia hacked the DNC,' they would need to give solid evidence -- and nothing in cyber is solid, and they would have to be willing to face the repercussions of what came next," the expert said. "Something that has been fought quietly until now would get loud and it would get ugly."

Speaking at the 2016 Intelligence and National Security Summit this week, the deputy head of U.S. Cyber Command, Air Force Lt. Gen. Kevin McLaughlin, said that when it came to drawing red lines on cyberattacks, "Ambiguity, not locking yourself in, is the way that our government prefers to do this."

But the concern is there. In the coming weeks, lawmakers will vote on whether to reinstate a Cold-War era task force dedicated solely to keeping tabs on covert Russian efforts in the US. That panel, proposed in the Senate Intelligence Authorization Bill, would be appointed by the White House and meet monthly. While the panel will be tasked with everything from unmasking Russian spies to foiling assassinations, its primary purpose, another intelligence official said, was to expose Russian propaganda efforts.

Underscoring the White House's timidity on the issue, the National Security Council declined multiple inquiries on whether the White House would support the executive branch panel being proposed by Congress. It also declined to say if the White House was receiving regular briefings on the variety of intelligence community probes into Russian meddling, including a broad effort being led by the Director of National Intelligence's office.

Asked to address Russia's suspected involvement in the hacks, National Security Council spokesman Stroh pointed to several recent public statements from officials, including a comment from White House spokesman Josh Earnest last week.

"The US government has not formally declared any specific entity or country as responsible for these reported intrusions," Earnest said in a press conference.

What Russia's goal is in attacking the US election process remains unclear, the first intelligence official said. There remains widespread suspicion that the Kremlin is working actively to elect Donald Trump -- Democratic nominee Hillary Clinton has said as much.

But that suggests Moscow truly thinks Trump would be easier to work with, a notion that the official thought were "overblown." Instead, it may be a part of a broader Russian effort to cut at the heart of Western democracy.

"It may not be so much intentional as instinctive on their part. They do it because they can," he said. "Any rationale you can try to apply to this is irrational."

Deutsche Welle
Germany to pour cash into mass surveillance
Thursday, 08 September 2016

Berlin - Germany's spies will be working with significantly increased resources next year, if a budget report leaked to three media outlets is approved. The federal domestic intelligence agency, the Verfassungsschutz (BfV) is bidding for an 18-percent budget boost in 2017, up to 307 million euros ($345

million), while the foreign intelligence agency BND will get a 12-percent rise to 808 million euros, according to a report released Thursday by the "Süddeutsche Zeitung" along with public broadcasters NDR and WDR.
A special parliamentary committee must now approve the increase - which, like all secret service budgets, are classified - but opposition parties have already voiced their concern.

The BND says it needs much of the extra money - some 73 million euros over the next few years - to set up "Panos," a new project specifically aimed at decrypting such messaging systems by finding weaknesses in the apps. The leaked plan also says the intelligence agencies need extra money to buy expertise from "external companies and service providers."

This is a dangerous game to play, according to opposition parties, as it likely means using taxpayer's money to shop in the so-called "Darknet" - where anonymous purchasing is made easy and often used for criminal purposes.

"It's a spiral that has no end," said Frank Herrmann, privacy spokesman for the Pirate Party in North-Rhine Westphalia. "No one can guarantee that these security gaps won't be sold on to other bidders. It's a black market. Security gaps are sold on the darknet by hackers, and we already know that government agencies have bought from them, too."

Herrmann says that instead of exposing flaws in services so that they can be corrected, the intel agencies will be getting extra money to make sure that such gaps remain open - which will have consequences for businesses as well as private citizens, since foreign competitors could also exploit those gaps. "Gaps aren't just used to find criminals - gaps are dangerous to everyone," he told DW. "It will create extra insecurity for everyone and feed the black market."

Competing with the NSA?

In the leaked plan, the BfV said it needs extra money because its own resources are currently inadequate to fulfill its mission. This echoed a complaint made by German intel agency chiefs to the German parliament's inquiry into the NSA affair, when they justified providing intelligence to the US National Security Agency by saying they needed access to data from the NSA's mass surveillance programs like XKeyscore - one of the NSA projects revealed by whistleblower Edward Snowden in 2013.

But Herrmann doubts whether the BND can ever really be independent of the NSA, since its budget is less than a tenth of the estimated $10.8 billion the NSA has to work with.

"Given that most of the manufacturers of software are American companies, and that American law gives the NSA all kinds of powers to force those companies to cooperate, the NSA has the power to spy on communications worldwide," said Herrmann. "It doesn't make it better to copy that with our own money here."

Opposition anger

Other budget plans revealed by the leak include 1.6 million euros, and 15 new jobs, to link Germany's Central Register of Foreign Nationals (AZR) - a database containing the details of 20 million non-Germans - with the databases of the BfV, and 55 new jobs to help network databases kept by Germany's federal and state agencies on far-right, far-left and Islamist extremists.

The BfV also wants an extra 4.5 million euros to strengthen its "cyber-defense" capabilities - the budget where it might need to go shopping from shadowy external contractors. Should the plans be approved, the "Süddeutsche Zeitung" said the BfV would end up employing some 2,900 people, plus 800 freelance contractors, in 2017 - a tripling of its personnel since 2000.

Other opposition parties were also appalled at the agencies' alleged plans, not least because the parliamentary inquiry into the NSA scandal had uncovered, they argued, illegal practices by the BND. "With its behavior the government is not only showing that it still does not have the will to draw the necessary legal consequences from Edward Snowden's revelations, it is also showing that the protection of the basic rights of citizens is in very bad hands," the Green party's Internet policy spokesman Konstantin von Notz told DW in an email.

Left party spokesman Jan Korte was equally scathing. "The grand coalition is clearly continuing to march on towards a surveillance state," he said in a statement. "The dwindling trust of people in the state also has something to do with the expansion of surveillance. For who would trust a state that doesn't stick to the law? On top of that, it's clear that this doesn't create more security, but more insecurity."

The majority of the increased funds are expected to be plowed into mass surveillance - particularly decrypting what the report calls "non- standardized telecommunications" - meaning widely-used messaging services, such as WhatsApp.

Such online services appear to be a particular concern to the BND. "Encryption means that of the more than 70 available communication services ... only less than ten can be gathered and the content read," the budget plan read.

Politico
DHS secretary: Ballot counts are largely safe from cyberattack
Thursday, 08 September 2016
Byline: Jennifer Scholtes

Washington - Homeland Security Secretary Jeh Johnson said Thursday it would be very difficult for hackers to alter Election Day ballot counts.

"It is so decentralized and so vast," the secretary said during a forum hosted by The Atlantic. "You've got state governments, local governments, county governments involved in the election process. It would be very difficult to alter the count."

Johnson said federal officials are generally concerned, however, about the potential for state actors, hacktivists or cyber criminals to manipulate or interfere with online state election systems. It was recently revealed that hackers had infiltrated voter registration databases in Illinois and Arizona.

To help protect against those threats, the Department of Homeland Security has been offering to assist election officials with cyber hygiene evaluations, incident response and information sharing.

But the secretary said those offers are being misconstrued. Several state officials have expressed concerns about a federal overreach into local election control.

"There's a lot of chatter on the Internet about what [DHS help] could mean," Johnson said. "It does not mean a federal takeover of state election systems or state elections, or even national elections."

"We don't have the authority to do that," he added. "What we do in homeland security, in cybersecurity, is offer assistance when people ask for it. So I've been trying to educate state election officials about what we are in a position to offer them, to help them manage their election systems."

The Local (Austria)
Turkish hacker group says it was behind airport cyber attack
Thursday, 08 September 2016

Vienna - Austrian police are investigating whether a Turkish nationalist group was behind a failed cyber attack on Vienna airport last week.
Hackers attempted to penetrate the airport's computer systems but were prevented from doing so.

In a tweet, the hacker group "Aslan Neferler Tim" or "Lion Soldiers Team" says it launched the attack in response to the "racism" of airport authorities.

It was referring to the refusal of Austrian officials to issue a group of Turkish nationals emergency visas that would have allowed them to leave the airport and stay the night in a hotel after their flight was grounded for technical reasons

The hackers describe themselves as responding to attacks against "Islam and the (Turkish) nation."

Diplomatic relations between Austria and Turkey have taken a downward turn after the failed coup attempt in Turkey, with Austrian Foreign Minister Sebastian Kurz warning he will stop any move that brings Turkey closer to joining the European Union.

Reuters
White House names retired Air Force general as first cyber security chief
Friday, 09 September 2016

Washington - The White House on Thursday named a retired U.S. Air Force brigadier general as the government's first federal cyber security chief, a position announced eight months ago that is intended to improve defenses against hackers.
Gregory Touhill's job will be to protect government networks and critical infrastructure from cyber threats as federal chief information security officer, according to a statement.

The administration of President Barack Obama has made bolstering federal cyber security a top priority in his last year in office. The issue has gained more attention because of high-profile breaches in recent years of government and private sector computers.

U.S. intelligence officials suspect Russia was responsible for breaches of Democratic political organizations and state election systems to exert influence on the Nov. 8 presidential election. Russia has dismissed the allegations as absurd.

Obama announced the new position in February alongside a budget proposal to Congress asking for $19 billion for cyber security across the U.S. government. The job is a political appointment, meaning Obama's successor can choose to replace Touhill after being sworn in next January.

Touhill is currently a deputy assistant secretary for cyber security and communications at the Department of Homeland Security.

He will begin his new role later this month, a source familiar with the matter said. Touhill's responsibilities will include creating and implementing policy for best security practices across federal agencies and conducting periodic audits to test for weaknesses, according to the announcement.

Grant Schneider, who is the director of cyber security policy at the White House's National Security Council, will be acting deputy to Touhill, according to the announcement.

Washington Post
Men who allegedly hacked top government officials arrested
Thursday, 08 September 2016
Byline: Rachel Weiner, Ellen Nakashima

Washington - U.S. authorities have arrested two North Carolina men accused of hacking into the private email accounts of high-ranking U.S. intelligence officials.

Andrew Otto Boggs, a.k.a. "INCURSIO," 22, of North Wilkesboro, N.C., and Justin Gray Liverman, a.k.a. "D3F4ULT," 24, of Morehead City, N.C., were both arrested Thursday morning and will be extradited next week to the Eastern District of Virginia, where federal prosecutors have spent months building a case against a group that calls itself Crackas With Attitude.

Along with Boggs and Liverman, authorities say the group included three teenage boys. One, a 17-year-old Briton, was arrested in February.

The hacking collective has claimed to have gained access to the private email accounts of CIA -Director John O. Brennan and Director of National Intelligence James R. Clapper Jr. The group regularly bragged about its escapades to reporters, explaining its methods and providing evidence of its activities.

According to U.S. officials, the group also hacked into the accounts of former FBI deputy director Mark Giuliano; Amy Hess, the FBI executive assistant director for science and technology; Gregory Mecher, who is married to White House communications director Jen Psaki; and Harold Rosenbaum, chief executive of the CIA contractor Centra Technology.

In an affidavit, FBI agent B.J. Kang wrote that "Cracka," the British teen, took the lead in hacking the accounts, while Boggs and Liverman encouraged him and used the exposed information to harass the targets.

According to both Kang and interviews the hackers have given to reporters, the group relied not on computer skills but "social engineering" to gain access to social media, phone and email accounts.

Kang wrote that "Cracka" gained access to Brennan's account by posing as a Verizon technician and tricking the company's tech-support unit into revealing the CIA director's account number, password and other details. He then used that information to lock Brennan out of his AOL account. Later, he released the form Brennan filled out to obtain his top-secret security clearance, a 47-page document full of personal details, according to the affidavit.

"Cracka" then gained access to Giuliano's Comcast account information and began forwarding the official's cellphone calls to a number associated with the Free Palestine Movement, according to the affidavit and interviews with the alleged hacker.

Liverman allegedly texted threats to Giuliano, calling him a "f---ing boomer," and paid for a campaign of harassing phone calls to Giuliano's cellphone.

When "Cracka" got access through Giuliano's accounts to a database of sensitive law enforcement information, Liverman allegedly requested information on Miami police. Authorities say a file containing information on 80 Miami-area officers was found on his computer. Those names and numbers were released online.

Boggs also allegedly used the information to post online the prison booking report for Chicago hacker Jeremy Hammond. The work emails and phone numbers for thousands of law enforcement personnel across the country were also posted online.

According to the affidavit, "Cracka" appears to have gotten into the law enforcement database simply by calling an FBI help desk and asking for Giuliano's password to be reset. The group is accused of using the same tactics to access an internal website for staffers at the Civil Division of the Department of Justice and post employee information online. In that instance, a member of the group allegedly used the credentials of a Justice Department contractor.

Both the FBI and Justice Department information was found on Liverman's computer, according to authorities.

Liverman pruportedly asked "Cracka" to target Mecher because Psaki had spoken critically of National Security Agency whistleblower Edward Snowden. Again, "Cracka" allegedly obtained access to Mecher's account simply by pretending to be both him and a Verizon employee in calls to Verizon. Liverman allegedly called Mecher, taunted him on Twitter by pretending to be Snowden, and attempted to gain access to Mecher's account himself.

Hess was targeted because Liverman believed she likely knew government secrets, according to Kang. "Cracka" allegedly obtained access to her Comcast account and began altering her settings, changing her passwords and playing movies on her television. He and Liverman allegedly released her call logs online.

Rosenbaum's company became a target because of its government work, according to Kang's affidavit. "Cracka" allegedly hacked into Rosenbaum's and his wife's Facebook accounts, canceling their dinner reservations and posting anti-Israel and pro-Palestinian messages. They also defaced his LinkedIn page, according to authorities.

"Cracka" and Liverman were also behind a fake bomb threat called in to the Palm Beach police in January, according to Kang.

Last year, before his arrest, "Cracka" told the New York Post he was motivated by "opposition to U.S. foreign policy and support to Palestine."

One member told CNN he smoked pot "all day every day" and was "probably" high when gaining access to high-level accounts.

Wall Street Journal
FBI Arrests Two in String of Breaches at CIA, Justice Department
Thursday, 08 September 2016
Byline: Devlin Barrett

Washington - Two North Carolina men were arrested Thursday on charges that they were part of the hacking group "Crackas With Attitude" that pulled off a series of embarrassing data breaches against the head of the CIA, a senior FBI official, and the Justice Department's case management system. Andrew Otto Boggs, 22, and Justin Gray Liverman, 24, were charged with being part of a conspiracy to access the personal accounts of senior government officials in late 2015 and early 2016.

Although court documents didn't name the victims, they include CIA Director John Brennan and then-Deputy FBI Director Mark Giuliano, according to officials close to the case. The hackers also managed to repeatedly access the Justice Department's computer system over a week earlier this year, according to authorities.

The hacking group also targeted officials from the White House, Department of Homeland Security, and the Office of the Director of National Intelligence, as well as their families, according to authorities.

The two men were charged in a criminal complaint filed in federal court in northern Virginia with conspiring to commit offenses against the U.S. If found guilty they could face up to five years in prison. The two men couldn't immediately be reached for comment, and court records didn't identify lawyers for them.

Three teenagers in the U.K. are also under investigation in the hacking conspiracy, officials said. One of those teens was arrested in February.

The suspects often gained access to the accounts by calling the help lines at internet-service companies and impersonating employees at those companies or the victims they were targeting.

In doing so, they were often able to reset the passwords to their targets' private email accounts, giving them access to those accounts. Computer-security experts refer to such techniques as social engineering, rather than hacking, because they typically depend on one person tricking another into providing key information that allows the suspect to access private accounts.

The "Crackas With Attitude" then used their access to taunt the officials, particularly Messrs. Brennan and Giuliano, with harassing phone calls and public ridicule posted online.

In January, one of the teenage hacker suspects in England was able to sneak into the Justice Department's computer system after calling the department's technical help desk and pretending to be a contract employee, according to an FBI affidavit filed in the case.

The group was able to access the Justice Department's civil division case information management system, the court papers say. They then began posting tens of thousands of names, phone numbers, and email addresses of FBI and Department of Homeland Security employees, officials said.

The Australian Financial Review
Cyber security 'more than just for IT guy'
Wednesday, 14 September 2016
Byline: James Eyers

Canberra -Directors should improve their knowledge about cyber security, assess technology vulnerabilities more regularly than other business risks, and develop more comprehensive plans for responding to attacks according to ASIC commissioner Cathie Armour.
With cyber crime estimated to cost the Australian economy more than $1 billion a year - a figure that will rise as more commerce moves into the digital world and hacker sophistication grows - the corporate regulator is encouraging directors to assess cyber security as part of the broader risk management framework, and not view it as one merely for the IT department.

"We do think there is one universally incorrect answer [for directors], and that is 'I am not sure about our cyber resilience, ask the IT guy'," Ms Armour told the inaugural Sinet61 summit in Sydney on Tuesday.

"We think with the pace of change, directors should be actively thinking about whether cyber security should be assessed more regularly than other risks. I would encourage board members to think about lifting their capability in this area ... and find ways they can get more confident in the space."

The Sinet conference was brought to Australia by the Security Innovation Network and presented by CSIRO and its subsidiary, Data 61. Security experts from some of the major banks will address the summit on Wednesday morning.

The Australian Institute of Company Directors has been working with Data61 since April to improve the digital and cyber literacy of boards and directors across Australia.

"There has been a keen interest from directors in learning about cyber resilience," said AICD chief executive John Brogden, who chaired the panel session at the event. "The digital age has provided businesses with a whole new world of opportunity, but it has also bought with it significant risk. Managing cyber risk is crucial for all organisations, and boards are taking that responsibility seriously."

While financial services cyber attacks around the world have largely focused on retail banking accounts, it is expected that criminals will increasingly focus on critical market infrastructure in order to disrupt economies. ASIC recently stress-tested the cyber resilience framework of both the Australian Securities Exchange and Chi-X. The Nasdaq was the target of a serious cyber attack in 2011.

Amanda Harkness, group general counsel of ASX, said cyber "has been identified as a big operational risk which means there is regular reporting" to the board about threats. The exchange's planning has included conducting simulated attacks to track staff response times. "At ASX, is it not just a matter for the IT guys - for ASX it is very much a brand and reputational issue," she told the summit.

But one issue ASX, like other companies, is struggling with is identifying quality staff. This is "one of the major challenges that we have," she said.

Ms Armour said boards might need to amend hiring practices. It would depend on the nature of each company, but "perhaps strategic technology skills are an important skill when a board is thinking about recruiting," she said.

The special adviser to the Prime Minster on cyber security, Alastair MacGibbon, told Sinet61 that the recent denial of service attacks on the Australian Bureau of Statistics on census night were relatively small but would have a big impact on the government's reputation, so held important lessons for the business community.

"Their impact in terms of trust and confidence of the ability of government to deliver services will last for a significant period and that is what we need to prepare for," he said.

Key points

Directors advised to improve their knowledge about cyber threats.

Criminals expected to target critical infrastructure in order to disrupt economies.

The Register (UK)
So, Gov.UK infosec in 2015. 'Chaotic'. Cost £300m. NINE THOUSAND data breaches...
Wednesday, 14 September 2016
Byline: Alexander J. Martin

London - The Cabinet Office is failing to coordinate the UK's government departments' efforts to protect their information according to a damning report by the National Audit Office.
The NAO found that the Cabinet Office failed in its duty and ambition to coordinate and lead government departments' efforts in protecting such information.

The Cabinet Office has "tried to take a more strategic role in offering support and guidance to central government departments," the NAO report found. "However, senior- level governance remains complex and unclear and, until recently, a wide array of central teams have been involved in information assurance and protecting information, sometimes offering overlapping and contradictory advice."

Reporting personal data breaches is chaotic, with different mechanisms making departmental comparisons meaningless. In addition, the Cabinet Office does not have access to robust expenditure and benefits data from departments, in part because they do not always collect or share such data. The

Cabinet Office has recently collected some data on security costs, though it believes that actual costs are "several times" the reported figure of £300 million.

As a result, NAO stated that GCHQ dealt with 200 "cyber national security incidents" per month in 2015, double the number of attacks it had addressed in 2014, though the result of these attacks has not been reported.

The report certainly suggests that departments need to get their own houses in order before they start opening up access to even more of citizens' data, as per the porn-blocking Digital Economy Bill, with 8,995 data breaches in the 17 largest government departments in 2014- 15.

Government departments are being challenged by the increasing need to share data with other public bodies, with delivery partners, service users, and citizens. According to the NAO, recent years' "cuts to departmental budgets and staff numbers, and increasing demands form citizens for online public services, have changed the way government collects, stores and manages information".

At the same time "the threat of electronic data loss from cyber crime, espionage and accidental disclosure has risen considerably. Alongside this new challenge, reporting to the Information Commissioner's Office (ICO) by public bodies shows that the loss of paper records remains significant."

Efforts have complicated by the lack of coordination by the 12 separate teams and organisations which play a role in governmental infosec, including: GDS; GCHQ; CESG, CERT-UK; and the UK National Authority for Counter Eavesdropping (UKNACE).

That this work hasn't been coordinated "has meant that a large number of bodies continue to have overlapping mandates and activities" according to the NAO, which noted how last November the then-Chancellor of the Exchequer noted this acronym- heavy problem and the need to "address the alphabet soup of agencies involved in protecting Britain in cyberspace."

As part of that address, Osborne announced the launch of a new National Cyber Security Centre (NCSC) which will act as a hub for sharing best practices in security between public and private sectors, and will tackle cyber incident response.

Speaking to The Register earlier this month, the former head of GCHQ Sir David Omand said: "Next month, the new National Cyber Security Centre starts its work, under the Director of GCHQ, drawing on the technical expertise of GCHQ staff in operating in cyberspace, a further major development in harnessing the skills of the intelligence community in protecting the public."

NAO's head, Amyas Morse, said: "Protecting information while re-designing public services and introducing the technology necessary to support them is an increasingly complex challenge. To achieve this, the Cabinet Office, departments and the wider public sector need a new approach, in which the

centre of government provides clear principles and guidance and departments increase their capacity to make informed decisions about the risks involved."

Washington Free Beacon
DNI Declines Required Damage Assessment of Clinton's Leaked Email Secrets
Wednesday, 14 September 2016
Byline: Bill Gertz

Washington - The U.S. intelligence community declined to conduct a required assessment of the damage to national security caused by former secretary of state Hillary Clinton sending and receiving secrets on a private email server.
"ODNI is not leading an [intelligence community]-wide damage assessment and is not aware of any individual IC element conducting such formal assessments," Joel D. Melstad, a spokesman for the of the Office of the Director of National Intelligence, said.

The most sensitive classified information leaked and possibly obtained by foreign intelligence services included ultra-secret information on U.S. drone strikes, according to American intelligence officials.

James Clapper, the director of national intelligence, agreed with security officials who argued against the need to carry out the damage assessment. Intelligence officials argued in internal discussions that since many details of the drone missile program targeting terrorists were disclosed in earlier leaks unrelated to Clinton's use of a personal email server, gauging the damage done by her conduct would be difficult, and possibly unnecessary.

Melstad, the DNI spokesman, declined further comment when asked the reasons behind Clapper's decision not to launch the damage assessment.

Other officials said Clapper's decision appeared based on political considerations and was an effort to avoid embroiling American intelligence agencies in charges they were attempting to influence the outcome of Clinton's bid for the White House.

The intelligence about drone strikes was compromised by its transmission on Clinton's private server. The information is classified above the Top-Secret level and limited to distribution to a few officials in what is called a Special Access Program--an intelligence compartment used to prevent the disclosure of the government's most secret information.

Drone strike intelligence is classified as a part of Special Access Programs in order to prevent revealing the sources and methods used for targeting terrorists with missiles fired by unmanned aerial vehicles, a signature tool of President Obama's counterterrorism policy.

Clinton, the Democratic presidential nominee, lied repeatedly about her handling of the unsecure email server, initially saying no classified information was sent in the private emails, and then asserting no information that was marked classified was sent and received during use of the server between 2009 and 2013.

Both claims were disputed by an FBI investigation that concluded in July. FBI Director James Comey said among the 30,000 emails obtained from the server, "very sensitive, highly classified information" was found, including seven email chains containing Special Access Program secrets.

"These chains involved Secretary Clinton both sending emails about those matters and receiving emails from others about the same matters," Comey said. "There is evidence to support a conclusion that any reasonable person in Secretary Clinton's position, or in the position of those government employees with whom she was corresponding about these matters, should have known that an unclassified system was no place for that conversation."

The Intelligence Community inspector general had requested the investigation focusing on the transmission of classified intelligence on emails sent and received by Clinton and her aides.

A June 2014 counterintelligence directive requires the Intelligence Community to conduct damage assessments in the aftermath of unauthorized disclosures or other failures, such as espionage cases.

The directive, ICD-732, states that "damage assessments shall be conducted when there is an actual or suspected unauthorized disclosure or compromise of classified national intelligence that may cause damage to U.S. national security."

A member of Congress and three intelligence experts disagree with the DNI's decision not to conduct the assessment, which they assert is needed to prevent further national security damage.

Rep. Mike Pompeo (R., Kan.), a member of the House Permanent Select Committee on Intelligence, wants the DNI to do a formal damage assessment.

"FBI Director Comey has made clear that there was highly classified and sensitive information on Secretary Clinton's personal server," Pompeo said. "It is imperative that an investigation be conducted to determine what harm to American national security may have occurred and, just as importantly, to prevent the massive mishandling of sensitive materials from ever happening again."

Pompeo said the refusal to do the damage assessment, despite the FBI's determination that a serious leak of national security data took place, "is inappropriate and a grave failure."

Angelo Codevilla, a former intelligence officer and former Senate Intelligence Committee staff member, said the FBI director's vague and evasive comments regarding Clinton's handling of classified information confirm that she compromised a significant number of secrets.

"Common sense, the intelligence community's standard practice, as well as a 2014 directive, require assessing the damage done by any such compromise," Codevilla said.

Politics in support of Clinton also appeared to be behind the decision. "The DNI's refusal to conduct such an assessment, even more than the FBI director's obfuscation, shows that U.S. intelligence agencies have been reduced to mere political arms of the Democratic Party," Codevilla added.

Michelle Van Cleave, former national counterintelligence executive, a senior counterspy policymaker, also called for the assessment.

"Whenever there is a significant compromise of national security information, as the FBI's report confirms happened here, it is essential to conduct an assessment of the damage in order to protect plans, programs, or lives that may be at risk," she said.

"The FBI has done a first cut at identifying classified information that was transmitted to or from the secretary of state in the 'open'--which means even any second-rate intelligence service could scoop it up," she added. "So you have to assume the Russians, the Chinese, the Iranians, and a host of others, have their hands on it all."

Van Cleave said that under a DNI directive a damage assessment team is responsible for looking at the information that was compromised and analyzing the potential harm to national security, "so we aren't going along blindly thinking all is well when it isn't."

An FBI report on the server investigation stated that foreign hostile hackers penetrated computer systems of people who communicated with Clinton through the private email.

"The FBI did find that hostile foreign actors gained access to the personal email accounts of individuals with whom Clinton was in regular contact, and, in doing so, obtained emails sent to or received by Clinton on her personal account," the report noted.

The report did not identify whether the emails obtained by the foreign hackers included classified information.

Comey said in July that "sophisticated adversaries"--code for states such as Russia and China--likely gained access to Clinton's private emails.

Kenneth E. deGraffenreid, a former deputy national counterintelligence executive, said intelligence bureaucrats have opposed damage assessments for years.

"Intelligence agencies hate conducting damage assessments that could show people that somebody did something wrong, or improper, or did it poorly," deGraffenreid said. "They never want that known. It's a bureaucracy that does one thing: protects itself."

In the past, intelligence agencies ducked conducting damage assessments by claiming the assessments could not be conducted without interfering with law enforcement investigations or prosecutions.

Both the FBI and Justice Department, however, have said the investigation of the Clinton email server was completed and prosecution declined.

DeGraffenreid said Congress should take action to force the intelligence community to launch the damage inquiry.

A special intelligence unit with access to secrets but which is independent of any political pressure from intelligence leaders should be created, he said.

"These assessments can't simply be done by the people in the agencies involved," deGraffenreid said. "That would be like allowing inmates to do an assessment of their crimes."

Congressional sources said the House and Senate intelligence oversight committee are reluctant to require the damage assessment since it would codify in writing the false claim that no damage was caused to the drone program by the compromise of secrets by Clinton and her aides.

The Obama administration has suffered a string of highly damaging security failures, including the theft of some 250,000 secret documents stolen by Bradley Manning, a soldier in the U.S. Army, and given to Wikileaks.

That compromise was followed by the theft of some 1.7 million highly classified documents on electronic intelligence gathering from the National Security Agency by renegade contractor Edward Snowden, currently wanted on espionage charges and living in Moscow.

A Clinton campaign spokesman did not respond to an email requesting comment.

Arab News
All-seeing 'eye' watches over Makkah pilgrims
Wednesday, 14 September 2016

Mina - Under a bank of monitors broadcasting live footage from more than 5,000 cameras, Saudi officers have kept their eyes on every route and gathering spot at this year's Haj pilgrimage.

As custodians of the most sacred sites in Islam, the authorities have been at pains to assure the world that every possible measure has been taken to prevent a repeat of last year's deadly stampede during Haj.

An "eye" which never closes forms the heart of the command and control center located in Mina, near Makkah, said Col. Saad Al-Dosari, its planning chief.

Another officer, Captain Tareq Al-Azam, told AFP that his dozens-strong team has been on duty around the clock monitoring this year's 1.8 million pilgrims who have converged on the desert kingdom from across the globe.

More than 5,000 cameras have been installed in the entire Makkah sector covering a radius of around 10 kilometers (six miles) around its Grand Mosque, the single holiest place in Islam.

From his vantage point, the captain can direct the cameras and is able to zoom in to investigate any suspicious-looking or potentially dangerous activity.

The job of the security team was "to survey the screens to detect any problem or any blockage" in the constant stream of pilgrims navigating the holy sites, explained Dosari. If any anomaly is detected, "they inform the operations center to prevent any problem before it can even happen."

Dozens of soldiers are posted at the center, located a few meters (yards) away, with headphones on and microphones at the ready to pass on information to the tens of thousands of members of the security forces on the ground.

They also redirect any complaints from the pilgrims on a special number provided by Saudi authorities, who have said this year's Haj which started last Saturday and ends on Thursday has been free of any major incident.

Times of Israel
Israel's new spy satellite 'not functioning' as expected
Wednesday, 14 September 2016
Byline: Judah Ari Gross

Jerusalem - The Ofek-11 reconnaissance satellite launched by Israel on Tuesday evening may be malfunctioning, officials involved in the project said a few hours after launch, though they said they have been able to make contact with the craft.
The Israel Aerospace Industries satellite was successfully put into orbit using a Shavit rocket, a locally produced space launch vehicle, the head of the Defense Ministry's Space Department, Amnon Harari, told reporters. However, in the hours after the launch, it was "not clear that everything was in order," he said.

Due to the rotation of the Earth, the teams on the ground are only able to make contact with the satellite "once every few hours," something that makes the work of the engineering teams "sevenfold more difficult," said Doron Ofer, CEO of the Israel Aerospace Industries' Space Division.

"We have downloaded some figures, and we are now checking them. It's not functioning exactly the way we expected, and we don't know what it's status is," Ofer said. "We are now working to stabilize it, but it will take some time because of the small amount of communication we have with it when it comes in our area," he said.

The satellite was shot into space from the Palmachim Air Base, just outside the Tel Aviv suburb of Rishon Lezion, at 5:40 p.m., Harari said.

The Ofek-11 is an upgrade from the Ofek-10 satellite launched in April 2014. However, Ofer would not discuss what exact improvements were made to the design of the satellite to make it superior to its predecessor.

The Ofek-11 was to join approximately 10 other satellites, including the Ofek- 10, Ofek-9, Ofek-7 and Ofek-5, that feed intelligence to Israel's security forces.

The launch came less than two weeks after the civilian Amos-6 communications satellite was destroyed when the SpaceX rocket carrying it exploded on the launchpad in Cape Canaveral, Florida during a pre-launch test.

Facebook had planned to use the satellite, which was built by Israeli company Spacecom, to beam high-speed internet to sub-Saharan Africa.

The National (UAE)
UAE companies 'wide open' to cyber attacks due to lack of staff training
Wednesday, 14 September 2016
Byline: Jennifer Bell

Abu Dhabi - Companies are failing to provide their employees with basic cyber security awareness training, leaving their systems "wide open" to attacks.
Experts say that the vast majority of local organisations underestimate the "human factor" that allows online criminals to infiltrate companies' internal networks, and many budget-cutting businesses do not see the value in investing in adequate training.

"If any organisation lacks the initiative to provide cyber security awareness as a part of their cyber security platform, they might as well remove the doors and windows to their offices and invite the

criminals in," said Amir Kolahzadeh, managing director of Itsec, one of the Middle East's cyber security leaders.

"Cyber security awareness provides the basic knowledge of identifying the barrage of attacks on email boxes, networks and telephone systems."

Mr Kolahzadeh said it was of "utmost importance" that every single employee completed a basic cyber security awareness seminar and be able to identify ransomware, which encrypts data on infected machines and demands a ransom to restore it.

He said because the UAE was an "extremely safe environment", it made people too trustworthy online. "This naturally causes people's guards to be down, versus if we lived in New York or London," he said.

"A cyber criminal can easily use a phone to call an employee and pretend to be a Microsoft engineer that has been assigned to upgrade the PCs for this company to the latest Windows and all the individual needs to do is allow a remote session for the three-minute install and, boom - suddenly the criminal has full access to the employee's PC, files and the company's networks."

Research by Symantec and Deloitte found that more than two thirds of organisations in the Middle East were still incapable of protecting themselves from sophisticated cyber attacks.

Mr Kolahzadeh said there was a lack of will in organisations to invest in security measures. "I would say 99 per cent of all IT directors are not looking to protect the organisation, they are simply looking for the cheapest compliance form they can pass on," he said. "This is a major -security threat for the region."

Mike Weston, vice president of Cisco Systems Middle East, said that no matter how many sophisticated security technologies were deployed within an organisation, a security solution was only as secure as its weakest link.

"UAE workplace security research conducted by Cisco and GBM showed employee behaviour is a genuine weak link in cybersecurity and becoming an increasing source of risk - more through complacency and ignorance than malice - because companies have so insulated employees from the scale of daily threats that people expect the company's security settings to take care of everything for them," he said. "Training employees to understand that they too are liable on an individual level is of critical importance.

"When data breaches are the result of an external attack, it is often the inexperience of employees that is exploited, whether it be by clicking on an email link they shouldn't open or downloading an unapproved app."

David Michaux, of online security company Whispering Bell, also said companies often underestimated the role their employees - from boardroom members to frontline workers - could play in preventing cyber crimes.

"Security awareness needs to be pushed down from the top and enforced," he said. "This means it needs to be written into the HR policies and enforced by IT."

Stephen Brennan, senior vice president of cyber network -defence at UAE cyber security company DarkMatter, said employers needed to have a rolling education programme for staff.

"You look back at the old day and it was 'loose lips sink ships' - the only thing we are really talking about now is transferring this mindset to the digital domain. "[It needs] a constant programme of not just educating people but also positive reinforcement."

The National (UAE)
Shortage of security professionals hindering UAE's cyber crime fight
Wednesday, 14 September 2016
Byline: Jennifer Bell

Abu Dhabi - The UAE must invest in training its own security professionals as a priority in the war against cyber crime, as the global pool of skilled workers is shrinking, experts say.
The Arab Gulf States Institute in Washington said cyber attacks in the region cost US$1 billion (Dh3.67bn) a year - an amount predicted to grow.

The institute said the Middle East was fertile ground for cyber crime, with its wide use of technology and high-value targets.

Mike Weston, vice president of Cisco Middle East, said that although there were more than a million cyber security positions available worldwide, the shortage of professionals to fill them was likely to grow rapidly.

The Cisco Annual Security Report 2016 said the deficit of cyber security workers would rise to 1.5 million by 2019.

"More and more organisations are looking to digitisation to compete in an increasingly global economy, while inadvertently increasing exposure to cyber attacks," Mr Weston said.

"Organisations need to invest in the people, processes and technology that will enable them to become more resilient in the face of new attacks."

David Michaux, of online security company Whispering Bell, said talent was a "big factor" in the UAE's vulnerability.

"We seem to have a lot of thinkers who advise companies on how to change strategies and reorganise their security," Mr Michaux said. "We need more people to do hands-on fixing."

As the UAE forges ahead with its knowledge economy, smart cities and other ambitious strategies, the potential for attacks will grow, he said.

Amir Kolahzadeh, managing director of Itsec, a leading cyber security company in the Middle East, said 85 per cent of UAE residents were online. "The UAE is a major target because of its glamour and vision," he said.

The Local (Austria)
Turkish hacker group targets Austrian National Bank
Wednesday, 14 September 2016

Vienna - A Turkish hacker group has allegedly tried hacking into the National Bank of Austria after reportedly being behind an attempted cyber attack at Vienna airport two weeks ago.
The hackers' collective, which goes under the name of Aslan Neferler, said the cyber attacks on Austrian institutions are revenge for Austria's "anti-Turkish political stance".

They claimed responsibility for two DoS-attacks on Friday night, when most of the bank's IT-technicians were not working. By sending five million emails per minute the attackers tried to clog the bank's server.

Christian Gutlederer, the spokesman for Austria's National Bank, said: "Our website was temporarily unavailable. The hackers did not have any access to any of our sensitive data."

The Turkish nationalists announced their "success" on various social networks, writing that they had "blocked access to the Austrian National Bank for a while". They promised that the attacks would continue.

The hacking attempts come after diplomatic relations between Austria and Turkey sharply deteriorated. After the failed coup attempt in Turkey, Austrian Foreign Minister Sebastian Kurz warned he will stop any move that brings Turkey closer to joining the European Union.

Turkey has recalled its ambassador to Austria and accused the country of being supportive of terrorism and a centre of Islamophobia.

The National (UAE)
A token nod at online security
Wednesday, 14 September 2016
Byline: Jonathan Gornall

Abu Dhabi - They crept up on us almost unnoticed. Small, annoying, plastic pieces of mysterious technology easily lost at the back of a drawer or the bottom of a handbag that have become ubiquitous, tediously essential bits of kit for anyone who banks online, whether at home or on the move. They are also sometimes necessary to gain access to a secure, corporate VPN or virtual private network.
Among banks, for reasons best known to the industry, their precise nature varies according to location. In the Middle East, for instance, including the UAE, they are a simple "token", a branded device that looks a little like a calculator and asks only for a PIN before issuing an apparently random number that allows access to online accounts.

Elsewhere in the world, including the US and Europe, they are card-readers - a slightly more sophisticated version of the token, into which bank cards must be inserted to generate a one-off number.

Either way, they do nothing to improve the consumer experience. At best they are a tiresome wrinkle in what has otherwise become the extremely smooth process of online banking. Lose them, and there's no way you can set up new payments or carry out a range of other online banking acts.

Presented as "an extra layer of protection against online fraud", the device is in fact nothing less than a tacit admission that the digital revolution is fatally flawed. Its very existence is evidence that, for all our digital ingenuity, we have yet to figure out a way of telling if people are who they say they are online.

Surely our usernames and passwords offer sufficient reassurance to the banks? Not any more, say the banks. We need the extra security, they say (although not in so many words), because large numbers of us are stupid and gullible and give away our login details to anyone who asks for them, and the banks are fed up picking up the bill for our collective naivete.

Card readers and tokens first surfaced in the early days of online banking, during the early 2000s, and spread like wildfire among banks. Today, they are everywhere, including in the Middle East - HSBC introduced its first token device in the UAE in June 2012.

The main reason for their introduction, says Ali Imanat, e-crime fraud lead for the UK-based industry organisation Financial Fraud Action, was "to move away from using static passwords for home banking customers, because those details can be easily phished or captured using malware".

It isn't obvious to the average customer - or fraudster, come to that - how "dynamic", or "two-factor authentication", as it is known in the trade, works. When you use the device, it generates an apparently random code that then has to be entered into the bank's website before the user can proceed.

Despite appearances, it's not magic. Although a "dumb" device, unconnected to the internet or your computer and hence immune to e-attack, the little piece of plastic is loaded with a basic algorithm, or pre-loaded set of instructions, designed to generate a different code each time you use it. The bank's system recognises the code spat out by the token, because it is running the same algorithm and, by counting your online transactions or according to the date and time, knows exactly which number to expect next.

So far, so good. In the early 2000s, Mr Imanat says, "this was seen as the most effective way forward in terms of improving security for customers". The banks "recognised it was an additional hardware device and not ideal for all customers, but they believed it would have a substantial impact on improving security, which it has".

Up to a point. The FFA has, but does not release, fraud figures for individual banks, but insists that "when you look at individual bank losses, there is a clear correlation between the introduction of two-factor authentication in about 2004-2005, and a reduction in the fraud figures".

It was, Mr Imanat says, clear which banks had introduced the new precaution and which had not - and it was to the latter that the fraudsters turned their attention.

Overall, however, fraud has pretty much held its ground. There was a spike in the key depression year of 2008 - financial hardship makes people more desperate, and so vulnerable to cruel scams - but in 2014 fraud was costing UK banks £479 million, £40m more than in 2004.

The problem, Mr Imanat says, is that "the fraudsters have worked out methods to circumvent the use of the devices and the security they provide".

Which isn't to say that the portable technology has been hacked. Well, it has been hacked, but as far as anyone can tell only in a university laboratory.

In 2009, a team from Cambridge University's computer laboratory took a peek under the hood. They emerged with a warning that while "the basic principle behind [the system] - a trusted user interface and secure cryptographic microprocessor - is sound, the system has been optimised literally to death".

They clarified the point by quoting the late Roger Needham, a Cambridge computer scientist and security protocols expert. Optimisation, Mr Needham once said, was "the process of taking something that works and replacing it with something that almost works, but is cheaper".

And, technology aside, there were other issues, particularly with card readers. These, Dr Steven Murdoch and his two Cambridge colleagues pointed out in a paper presented to the 2009 Financial Cryptography and Data Security conference in Barbados, could easily be stolen by muggers, along with cards. Whereas previously "muggers marched a victim to an ATM to ensure he gave them the right PIN,

now criminals have a portable device that will tell them if their victim is lying", without the risk that they will be caught on CCTV while loitering by a cash machine.

It would, they concluded, have been "easy enough for the banks to design [the system] without revealing the result of the PIN verification, but they failed to foresee the risk. In our view, this was negligent [and] placed customers in harm's way".

Both card reader and token also offer thieves a low-tech way of figuring out a PIN for themselves. Used often enough, the print on the rubber keys can wear down, decreasing the odds of guessing a four-number PIN in three attempts from 1 in 3,333 to 1 in 8. If the customer has several cards with the same PIN, basic maths dictates that "the attacker has even better odds".

All well and good, Mr Imanat says. The banking sector "is aware of the findings of that paper but it's not something that the industry is massively concerned about".

Yes, in a lab in Cambridge you probably can break in and do all sorts of funny things, but out in the real world "we haven't seen it happen". For the average fraudster, cracking tokens and card readers is simply too much like hard work and, because it would have to be done for each one, "simply isn't a scaleable solution".

As for the charge that the industry was relying on an "optimised" (read: "compromised") device, "banks have to balance gains in security with convenience. We could provide a solution that is 99.9 per cent secure, but we know no consumer will ever use it because it's going to be too cumbersome and inconvenient".

What is "sometimes overlooked in these academic papers", he says, is that "banks have to balance making it easy for customers to go online versus how many padlocks and chains are people prepared to open before they can get to their money".

Besides, he says, the real reason that bank fraud figures continue to climb has nothing to do with technology.

Yes, fraudsters phishing for personal details "continues to be an issue for the industry". Amazingly, it seems there are still people out there falling in large numbers for poorly worded email appeals to click on links, supposedly sent by banks or other organisations. (One pathetic example currently doing the rounds, purportedly emanating from iTunes: "Dear Client, As a part of our security plan, Please Finished your billing informations. This actionis very locked and private. Competed now."

It's enough to make one miss those charming email appeals for help from all those dispossessed African princes.

But such phishing, Mr Imanat says, is "not as significant as it used to be - the introduction of two-factor authentication means capturing static passwords is pretty much useless to the criminal now".

Indeed, phishing as a problem is now dwarfed by the issue of malware, increasingly used by fraudsters as users grow more aware, and planted on home computers or smartphones by innocent-looking attachments or links in emails. ("Click here for latest Britney Spears video", or "Hi, have you seen these HR salaries for 2016??")

Such implanted software lies doggo on your hard drive, springing to life and hoovering up information or even taking over your computer and doing unspeakable things whenever you visit selected target sites, such as banks.

But nothing, Mr Imanat says, compares with the rise of what he calls "social engineering, this is the biggest area of concern for us, more so even than malware".

And what this means is that in our high-tech digital age, it is the old-fashioned conman who has the banking system on the run: "Essentially it's a fraudster using a very clever script to dupe the customer into making payments or giving away their credentials over the phone."

It's the same old problem that has plagued financial transactions ever since currency was invented: a fool and his money are easily parted. "When it comes to social engineering I've seen some very IT-savvy, security-minded individuals duped," Mr Imanat says.

Malware sounds scary, he says, "And it is. But it is a technical problem and so there is a technical solution. Unfortunately it is very difficult to come up with a technical fix for customers' naivete. We have education and awareness campaigns, but at the end of the day you can't put a piece of code into people."

But you can put it on their smartphone. If you haven't already lost your token or card reader, or choked it with biscuit crumbs at the bottom of your bag, don't get too attached to it. Having argued for the invulnerability of the devices because they are not linked to any other device connected to the internet, in the escalating arms race that is online security, banks are now poised to get rid of them.

"Security technology develops," Mr Imanat says. "The banks realised that not every customer wants to have to carry around one of these cumbersome devices."

The solution? "They are starting to move away from hardware devices to use software versions instead, apps that generate the same code, but as a bit of software, so the customers don't have to carry a separate device and can do it all from their mobile device." Brilliant. What could possibly go wrong?

New York Times

Vengeful Russian Hackers Leak Medical Files of Top U.S. Athletes
Wednesday, 14 September 2016
Byline: Rebecca R. Ruiz

New York - Russian hackers -- possibly the same group that compromised the Democratic National Committee's computer servers -- have made top American athletes their latest target.
Joining an intercontinental dispute over sports doping, the hackers penetrated the World Anti-Doping Agency's athlete database and publicly revealed private medical information about three of the United States' most famous athletes: Serena Williams, Venus Williams and Simone Biles.

The hackers published documents this week showing that Ms. Biles, who won four gold medals in gymnastics at the Rio Olympics last month, and the Williams sisters received medical exemptions to use banned drugs.

The antidoping agency confirmed the authenticity of the documents in a statement Tuesday, attributing the hack to Fancy Bear, a Russian cyberespionage group that forensics specialists have tied to breaches against government agencies, nonprofit organizations and corporations. That group is believed to be associated with G.R.U., the Russian military intelligence agency suspected of involvement in the recent theft of emails and documents from the D.N.C.

"These criminal acts are greatly compromising the effort by the global antidoping community to re-establish trust in Russia," WADA's director general, Olivier Niggli, said Tuesday, referring to revelations of elaborate government-ordered doping by Russia that prompted more than 100 of the country's athletes to be barred from the Rio Games.

The hackers wrote on their website that the United States had "played well but not fair" in Rio de Janeiro, and the medical documents were hailed in Russia on Tuesday as evidence of both widespread doping among American athletes and the double standards of global antidoping regulators.

Dmitry Peskov, spokesman for President Vladimir V. Putin, said that the Kremlin was not involved in the hacks. "It's simply ruled out," Mr. Peskov said.

Russia has gone to to great lengths to maintain plausible deniability in matters of espionage. The Kremlin often delegates high- profile political attacks to third parties, such as in the case of a 2007 attack on Estonia, according to one classified American intelligence estimate.

On their website, the hackers claimed to be both members of Anonymous, the global hacking collective, and Fancy Bear, which typically works in extreme stealth and takes great measures to cover its tracks. Those two groups have not been aligned before.

Revenge, apparently, motivated the WADA hacks. In May, The New York Times reported the account of Russia's longtime antidoping lab chief, who said the country had run a doping program and staged an

elaborate cheating scheme at the 2014 Sochi Olympics. A subsequent report commissioned by WADA confirmed that account.

The United States Anti-Doping Agency said that the American athletes in question had sought the requisite approvals to take typically prohibited substances, and that none of the positive drug tests constituted a violation.

The drugs mentioned in the documents are commonly prescribed medications that treat ailments including pain and allergies. The Times is not identifying the drugs for privacy reasons.

Ms. Biles acknowledged on Tuesday that she was prescribed medication for attention-deficit hyperactivity disorder. "Having ADHD, and taking medicine for it is nothing to be ashamed of, nothing that I'm afraid to let people know," she wrote on Twitter.

Athletes with particular medical conditions may apply for special permission to take banned substances, requiring a doctor's diagnosis and the approval of sports authorities. The WADA list of prohibited drugs -- including a range of substances, from cannabis to attention-deficit disorder drugs to anabolic steroids -- is updated each year.

In 2016, meldonium -- a heart medication that improves blood flow -- was added to that list, resulting in infractions for several Russian athletes, including the tennis star Maria Sharapova. (Ms. Sharapova, who said she was unaware the drug had been banned, was barred from competition for two years. She appealed that decision at an arbitration hearing in New York this month, and awaits a verdict in October.)

The records published by the hackers showed that at the Rio Games, Ms. Biles tested positive for a prohibited substance used to treat A.D.H.D. that she had received permission to take.

U.S.A. Gymnastics officials said Ms. Biles's drug use had been approved. "Simone has filed the proper paperwork," said Steve Penny, the organization's president. "Simone and everyone at U.S.A. Gymnastics believe in the importance of a level playing field for all athletes."

The International Tennis Federation confirmed on Tuesday that it, too, had approved exceptions for Serena and Venus Williams to take banned substances in recent years.

"In each of the situations, the athlete has done everything right in adhering to the global rules for obtaining permission to use a needed medication," said Travis T. Tygart, Usada's president. "It's unthinkable that in the Olympic movement, hackers would illegally obtain confidential medical information in an attempt to smear athletes to make it look as if they have done something wrong."

WADA said its management system was infiltrated through the so- called "spearphishing" of email accounts, in which attackers send tailored emails to authorized users to convince them to click on

malicious links or attachments that give attackers a toehold onto their machines. The agency said the attackers used that unauthorized access to gain entry through an International Olympic Committee account that was set up for the Rio Games.

Law enforcement authorities determined that the attacks originated in Russia, WADA said.

This week's hack came in the wake of revelations about the hacking of the WADA account of the Russian whistle-blower Yuliya Stepanova, a middle-distance runner who fled the country and is now living in an undisclosed location in the United States. That account contained her whereabouts.

Ms. Stepanova said last month that she feared for her safety, and that she and her husband -- a former employee of Russia's antidoping agency who has also spoken publicly about the country's systematic doping -- had moved to a new address as a result.

The hackers said Tuesday that they planned to release the medical records of additional athletes from around the world in coming days.

"This is just the tip of the iceberg," a statement posted to the Fancy Bears site said. "Today's sport is truly contaminated while the world is unaware of the large number of American doping athletes."

New York Times
A Hacker Releases Democratic Documents
Wednesday, 14 September 2016
Byline: Alan Rappeport

New York - A hacker who American intelligence officials believe has ties to the Russian government made public on Tuesday a second batch of documents suspected of having been stolen from the Democratic National Committee's computer system, leaving the organization rushing to contain damage or embarrassment less than two months before the presidential election.
The internal documents, which party officials were verifying for authenticity, were distributed at a cybersecurity conference in London.

The release was apparently the work of Guccifer 2.0, a self-identified Romanian hacker who claimed responsibility for publishing a trove of the committee's documents before the Democratic convention in July.

Donna Brazile, the interim chairwoman of the Democratic National Committee, blamed Russian espionage for the hack and said that foreign agents were trying to help Donald J. Trump, the Republican presidential nominee, be elected.

"The D.N.C. is the victim of a crime: an illegal cyberattack by Russian state- sponsored agents who seek to harm the Democratic Party and progressive groups in an effort to influence the presidential election," Ms. Brazile said in a statement. "There's one person who stands to benefit from these criminal acts, and that's Donald Trump."

The first batch of documents showed that party officials had favored Hillary Clinton over Senator Bernie Sanders of Vermont in the Democratic primary campaign, and their disclosure appeared to have been timed to sow discord before a unifying moment.

Ms. Brazile said that the committee had expected more documents to be released and that its legal team was working to determine whether they were real or forged.

The documents released Tuesday were not immediately as damaging as the first trove, and they proved difficult to access. WikiLeaks, the anti- secrecy platform, posted multiple messages on Twitter explaining how to download the documents after users struggled to do so. Initial reports suggested that they were old records related to the committee's donor outreach program.

Their release is likely to put more focus on Russia's efforts to meddle in the presidential election. American intelligence agencies and private investigators concluded in July that the hack was the work of the Russian government.

President Vladimir V. Putin of Russia denied involvement in the security breach in an interview with Bloomberg News this month, but he did describe it as a public service.

Mr. Trump has dismissed suggestions of Russian involvement, but he drew scorn this summer when he invited Russian hackers to track down missing emails from the private server Mrs. Clinton used as secretary of state.

While Mr. Trump laughed off his remark, the Democratic National Committee said Tuesday that the hacking was not a coincidence.

"Not only has Trump embraced Putin, he publicly encouraged further Russian espionage to help his campaign," Ms. Brazile said, calling Mr. Trump's statements "dangerous, divisive and unprecedented."

Nextgov.com
Lawmakers Probe Intelligence Officials on How the US Will Respond to a Cyberattack
Wednesday, 14 September 2016
Byline: Mohana Ravindranath

Washington - The federal government, including the Defense Department, needs a clearer plan about how to respond to attacks on civilian systems, members of the Senate Armed Services Committee argued Tuesday.
Sen. John McCain, R.-Ariz., suggested drafting a policy about "what the United States' actions would be in the case of a threat, in the case of an actual attack," he said during a hearing on encryption and cybersecurity.

"If you don't act, I guarantee you Congress will act," he said, addressing witnesses Adm. Mike Rogers, director of the National Security Agency, and Marcell Lettre, undersecretary of defense for intelligence.

The hearing illustrated disagreements between members of Congress, senior cyber officials and private technology companies about the best way to cooperate on preventing not only future cyberattacks, but physical attacks planned using encrypted communication such as WhatsApp.

In response to McCain's suggestion, Lettre argued during the hearing that "new legal and regulatory approaches are not as potentially productive as robust" conversations between the public and private sectors.

Lettre said the public and private sectors are often able to cooperate "if on the government side, we're able to communicate the problems we're trying to solve, and ask for industry's best expertise and wisdom about solutions."

Sen. Jeanne Shaheen, D-N.H., noted that so far there have been "limits" to that strategy, as Twitter has still been reluctant to share access to its so called firehose of data.

"Right now, we've had mixed reviews of the opportunity to work collaboratively with the private sector," she said.

Senators seemed stumped by Twitter's refusal to share access to its analytics service Dataminr with intelligence agencies.

"Shame on them," McCain said, asking witnesses what could be done other than "exposing [Twitter] for what they are."

The United States "must balance our national security needs and the rights of our citizens," McCain said, though he added the U.S. must recognize that authoritarian governments may search for keys to suppressing dissents and monitor their own citizens.

"Yet, ignoring the issue, as the White House has done, is not an option," he said.

Asked what new technology could change domestic cyber response, Rogers explained his team is especially interested in artificial intelligence and machine learning.

"How do we do cyber at scale, at speed," he said, noting that focusing purely on hiring more cyber talent instead of investing in more advanced technology "will be both incredibly resource intensive and it will be very slow."

Rogers said he was especially worried hackers might become less interested in extracting U.S. data for their own purposes, and more on manipulating information so it can't be trusted. For instance, if military commanders can't trust the tactical maps they have, they can't effectively make decisions, he explained.

"What happens when nonstate actors decide that the internet is not just a forum to coordinate ... but instead offers the opportunity to act as a weapons system?" he asked.

Reuters
Pardon for former NSA contractor Snowden seen unlikely
Wednesday, 14 September 2016

Washington - The U.S. government will not budge on its demand that former National Security Agency contractor Edward Snowden return to face prosecution for stealing thousands of classified intelligence documents, despite new calls for President Barack Obama to pardon him, U.S. officials said on Tuesday. The officials said they expect Snowden's supporters to use the Thursday release of "Snowden" - directed by veteran filmmaker Oliver Stone - to mount a public campaign demanding a pardon before Obama leaves office in January.

Snowden, who lives in Moscow, is scheduled to appear via video link on Wednesday at a New York press conference, where advocates from human rights groups will call for a pardon.

They argue that Snowden performed a public service by exposing excessive and intrusive electronic spying by the intelligence agency and its English-speaking allies, including Britain's Government Communications Headquarters (GCHQ).

In an interview published by The Guardian on Tuesday, Snowden said the U.S. Congress, the courts and the president all "changed their policies" as a result of his disclosures, and that "there has never been any public evidence that any individual came to harm as a result."

White House spokesman Josh Earnest said on Monday that Snowden is charged with "serious crimes, and it's the policy of the administration that Mr. Snowden should return to the United States and face those charges."

Two other U.S. officials said there are no discussions inside the Justice Department about granting him a pardon.

Some officials have acknowledged that Snowden raised legitimate questions about the extent and effectiveness of some electronic eavesdropping, particularly the NSA's sweeping collection of "metadata" on domestic telephone calls by Americans, a practice that was curtailed after his revelations.

Other officials, however, say the material Snowden gave the media included sensitive details about the locations and operations of U.S. and allied global spying operations, some of which were compromised.

London Daily Telegraph
GCHQ blocks 58,000 scam emails from government addresses every day
Tuesday, 13 September 2016
Byline: Cara McGoogan

London - The UK's intelligence agency GCHQ has stepped up the fight against online scammers and created a tool that blocks malicious emails that appear to be sent from government addresses, but are in fact run by cyber criminals.
The blocking system can identify when "gov.uk" emails are being sent from IP addresses not associated with an official government computer and block them.

GCHQ has been testing the system on emails from the fake "taxrefund@gov.uk" address, which was sending 58,000 messages a day.

"Whoever was sending 58,000 malicious emails per day from taxrefund@gov.uk isn't doing it anymore," said Ciaran Martin, the chief executive of the National Cyber Security Centre, which is launching in October.

Emails that appear to come from official accounts can be used to harvest personal information, bank details and tax records. The tax system, which the government plans to make completely digital by 2020, is lucrative for cyber criminals using unsophisticated methods.

In 2014 almost 50 per cent of HMRC consumers reported being targeted in a phishing scam. And in 2015 there were 17,000 fraudulent or incorrect repayment claims to HM Revenue and Customs, potentially worth up to £100 million, some of which could have been filed using information retrieved through phishing emails.

GCHQ's tool could help prevent such phishing attacks in the future, which have also plagued Apple customers, WhatsApp users and people worried about Brexit.

The security breakthrough was announced at Martin's first public appearance as head of the National Cyber Security Centre, Britain's first dedicated cyber unit that will open in October.

The newly established centre is a branch of GCHQ that will work from a separate office in London, allowing it to use the spook agency's intelligence while also working with the private sector.

"The NSCS is designed to bring together various sources of expertise into a single organisation," said Martin. This includes experts from MI5 and GCHQ, as well as partnerships with law enforcement and private companies.

"It's about tackling the most capable threats and protecting our most important national systems. But also our strategy represents a significant shift in thinking towards looking - at a national level - at how we use technology to improve cyber security at all levels."

As a result, the department will be equally focused on the security of the government's, private companies' and individuals' computer systems.

The Guardian (London)
Edward Snowden makes 'moral' case for presidential pardon
Tuesday, 13 September 2016
Byline: Ewen MacAskill

London - Edward Snowden has set out the case for Barack Obama granting him a pardon before the US president leaves office in January, arguing that the disclosure of the scale of surveillance by US and British intelligence agencies was not only morally right but had left citizens better off.
The US whistleblower's comments, made in an interview with the Guardian, came as supporters, including his US lawyer, stepped up a campaign for a presidential pardon. Snowden is wanted in the US, where he is accused of violating the Espionage Act and faces at least 30 years in jail.

Speaking on Monday via a video link from Moscow, where he is in exile, Snowden said any evaluation of the consequences of his leak of tens of thousands of National Security Agency and GCHQ documents in 2013 would show clearly that people had benefited.

"Yes, there are laws on the books that say one thing, but that is perhaps why the pardon power exists - for the exceptions, for the things that may seem unlawful in letters on a page but when we look at them morally, when we look at them ethically, when we look at the results, it seems these were necessary things, these were vital things," he said.

"I think when people look at the calculations of benefit, it is clear that in the wake of 2013 the laws of our nation changed. The [US] Congress, the courts and the president all changed their policies as a result of these disclosures. At the same time there has never been any public evidence that any individual came to harm as a result."

Although US presidents have granted some surprising pardons when leaving office, the chances of Obama doing so seem remote, even though before he entered the White House he was a constitutional lawyer who often made the case for privacy and had warned about the dangers of mass surveillance.

Obama's former attorney general Eric Holder, however, gave an unexpected boost to the campaign for a pardon in May when he said Snowden had performed a public service.

The campaign could receive a further lift from Oliver Stone's film, Snowden, scheduled for release in the US on Friday. Over the weekend the director said he hoped the film would help shift opinion behind the whistleblower, and added his voice to the plea for a pardon.

Ahead of general release, the film will be shown in 700 cinemas across the US on Wednesday, with plans for Stone and Snowden to join in a discussion afterwards via a video link.

In his wide-ranging interview, Snowden insisted the net public benefit of the NSA leak was clear. "If not for these disclosures, if not for these revelations, we would be worse off," he said.

In Hong Kong in June 2013, when he had passed his documents to journalists, Snowden displayed an almost unnatural calm, as if resigned to his fate. On Monday he said that at that time he expected a "dark end" in which he was either killed or jailed in the US.

More than three years on, he appears cheerful and relaxed. He has avoided the fate of fellow whistleblower Chelsea Manning, who is in solitary confinement in the US. Snowden is free to communicate with supporters and chats online late into the night.

His 2.3 million followers on Twitter give him a huge platform to express his views. He works on tools to try to help journalists. He is not restricted to Moscow and has travelled around Russia, and his family in the US have been to visit him.

But Snowden still wants to return to the US and seems confident, in spite of all the evidence to the contrary, that it will happen. "In the fullness of time, I think I will end up back home," he said.

"Once the officials, who felt like they had to protect the programmes, their positions, their careers, have left government and we start looking at things from a more historical perspective, it will be pretty clear that this war on whistleblowers does not serve the interests of the United States; rather it harms them."

Snowden attracts lots of conspiracy theories. Early on, he was accused of being a spy for China and then a Russian spy. In August a cryptic tweet followed by an unusual absence prompted speculation that he was dead. He said he had simply gone on holiday.

There had also been rumours that his partner, Lindsay Mills, had left him, which would have been embarrassing as their romance occupies a large part of the Stone film. Snowden said "she is with me and we are very happy".

His revelations resulted in a global debate and modest legislative changes. More significant, perhaps, is that surveillance and the impact of technological change has seeped into popular culture, in films such as the latest Jason Bourne and television series, such as the Good Wife.

Snowden also welcomed "a renaissance of scepticism" on the part of at least some journalists when confronted by anonymous briefings by officials not backed by evidence.

He warned three years ago of the danger that one day there might be a president who abused the system. The warning failed to gain much traction, given that Obama's presidency seemed relatively benign. But it resonates more today, in the wake of Donald Trump's response to the Russian hacking of the Democratic party: that he wished he had the power to hack into Hillary Clinton's emails.

If Obama, as seems likely, declines to pardon Snowden, his chances under either Clinton or Trump would seem to be even slimmer. He described the 2016 presidential race as unprecedented "in terms of the sort of authoritarian policies that are being put forward".

"Unfortunately, many candidates in the political mainstream today, even pundits and commentators who aren't running for office, believe we have to be able to do anything, no matter what, as long as there is some benefit to be had in doing so. But that is the logic of a police state."

He is even less impressed by the British prime minister, referring to Theresa May as a "a sort of Darth Vader in the United Kingdom", whose surveillance bill is "an egregious violation of human rights, that goes far further than any law proposed in the western world".

Snowden was initially berated by opponents for failing to criticise the Russian president, Vladimir Putin, but he has become increasingly vocal. It is a potentially risky move, given his application for an extension of asylum is up for renewal next year, so why do it?

"Well, it would not be the first time I have taken a risk for something I believe in," he said. "This is a complex situation. Russia is not my area of focus. It is not my area of expertise. I don't speak Russian in a fluent manner that I could really participate in and influence policy. But when something happens that I believe is clearly a violation of the right thing, I believe we should stand up and say something about it.

"My priority always has to be my own country rather than Russia. I would like to help reform the human rights situation in Russia but I will never be well placed to do so relative to actual Russian activists themselves."

Might he end up as part of a US-Russian prisoner exchange, with Putin possibly more amenable to the idea if Trump was in power? "There has always been the possibility that any government could say, 'Well, it does not really matter whether it is a violation of human rights, it does not really matter whether it is a violation of law, it will be beneficial to use this individual as a bargaining chip'. This is not exclusive to me. This happens to activists around the world every day."

He said he saw the Stone film as a mechanism for getting people to talk about surveillance, though he felt uncomfortable with other people telling his story.

Snowden has toyed with writing his memoirs but has not made much progress. There are at least three books about him on the way; an extensively researched one by the Washington Post's Bart Gellman and two others thought to be hostile.

Asked if he was the source for the Panama Papers - the comments by the source sound like Snowden - he laughed. He praised the biggest data leak in history, adding that he would normally be happy to cloak other whistleblowers by neither denying nor confirming he was a source. But he would make an exception in the case of the Panama Papers. "I would not claim any credit for that."

For someone who has spent his life trying to keep out of the public eye, he has now appeared in a Hollywood movie and an Oscar-winning documentary, and several plays, including Privacy, which just ended a run in New York and in which he has a part alongside Daniel Radcliffe.

"It was an alarming experience for me. I am not an actor. I have been told I am not very good at it. But you know if I can, I can try and maybe it will help, I will give it my best shot."

For Snowden, his campaign for a pardon, even if forlorn, offers a chance to highlight his plight, and he expressed thanks to all those who were backing it. He also said he hoped that after the fuss of the movie he could finally fade into the background. "I really hope it is over," he said. "That would be the greatest gift anyone could give me."

Reuters
Spy agencies concerned about possible U.S. election hacks: NSA chief
Tuesday, 13 September 2016

Washington - American intelligence agencies are concerned about reports that foreign governments may be attempting to undermine the Nov. 8 U.S. elections through cyber attacks, Admiral Mike Rogers, the director of the National Security Agency, said on Tuesday.
"We continue to be actively concerned," Rogers told a Senate hearing, responding to a question from Senator John McCain, chairman of the Senate Armed Services Committee.

Marcel Lettre, Under Secretary of Defense for Intelligence, testified that the government is taking any such activities "quite seriously" and said an "aggressive investigation" is under way.

McCain noted that one of the two states in which media reports said there was evidence of attempted Russian hacking was his home state, Arizona.

Some analysts have said Arizona, which recently has been reliably Republican in presidential elections, could be tilting more toward the Democratic nominee, Hillary Clinton, this year. McCain, a Republican, himself is in a tougher than usual re-election fight.

Rogers said he could not provide specifics about spy agencies' current assessment of the alleged hacking in a public setting. But he added, "I will say this, that it continues to be an issue of great focus ... for the foreign intelligence community, attempting to generate insights into what foreign nations are doing in this area."

Under further questioning, Rogers declined to characterize the activity as by a foreign nation-state.

Lettre said the government would adopt a policy for dealing with any such activity once it had the results of the investigation.

"The FBI and the Department of Homeland Security has an aggressive investigation underway," Lettre said.

U.S. security officials have said that, starting last year, hackers infiltrated computers of the Democratic National Committee, Clinton's presidential campaign and her party's congressional fundraising committee.

U.S. officials said they have concluded that Russia or its proxies were responsible, leading to calls by some Democrats and cyber security officials for the Obama administration to blame Russia publicly.

Kremlin officials have dismissed the allegations as absurd, but there is anxiety in Washington over the possibility that a foreign power might be using hacked information to meddle in the November elections.

Financial Times
Spymasters plan to build 'Great British Firewall'
Tuesday, 13 September 2016
Byline: Sam Jones

London - Ambitious new plans are being drawn up by GCHQ to create a "Great British Firewall" to block malicious websites countrywide and combat a doubling of serious cyber attacks threatening national security over the past year.
Though still in its infancy, the scheme is intended to be a flagship project for the new National Cyber Security Centre -- a public- facing arm of GCHQ which will open next month to better co-ordinate the UK's digital defence efforts.

The NCSC plan envisions private-sector internet service providers, such as BT, Sky or Virgin Media, voluntarily complying with its proposals, circumventing any need for legislation. Consumers will be able to opt out of the censorship should they wish in order to allay concerns over civil liberties.

Malicious websites which automatically infect visitors' computers with malware -- often disguised as legitimate domains -- are one of the most common methods of cyber attack.

They are widely used by states such as China, Iran or Russia in efforts to penetrate sensitive government networks, steal commercial information or compromise national infrastructure. They are also a common means for cyber criminals to target individuals.

Ciaran Martin, GCHQ's director-general for cyber security, and the incoming head of the NCSC, told a US audience of security experts and government officials at a conference in Washington on Tuesday that steps were now being taken to combat such websites.

"It's possible to filter unwanted content or spam. It's possible to filter offensive content. It's technically possible to block malicious content," he said. "So, the question is: why aren't we, the cyber security community, using this more widely? Well, we -- in the UK -- now are,"

"We're exploring a flagship project on scaling up DNS [domain name system] filtering: what better way of providing automated defences at scale than by the major private providers effectively blocking their customers from coming into contact with known malware and bad addresses?" Mr Martin said.

Because of its strategic interests and digital development, the UK is one of the most vulnerable economies in the world to cyber attack, Mr Martin added, making the need for more robust government action to protect businesses and civilians urgent.

"Behind the necessarily closed doors of our cyber defence operations centre, last year we detected twice as many national security level cyber incidents -- 200 per month -- than the year before," he said.

Efforts by GCHQ and the government to try to boost the UK economy's cyber defences have so far had a patchy effect. Even large companies, such as the Telecoms provider TalkTalk, have fallen victim to attacks in recent months.

Plans for a national DNS filtering regime are nevertheless likely to raise concerns among civil liberties campaigners: the same technical principles lie behind China's "Great Firewall" which allows the government effectively to control what its citizens have access to online and what not.

It is not yet clear who will decide which websites are blocked and by what criteria.

GCHQ hopes to demonstrate the security benefits of the proposals to ISPs by example: it is already testing a number of automated features across government networks and domains to clampdown on spoofing and attempts by hackers to mimic government services.

It is now far harder for hackers to mask malicious emails with fake "@gov.uk" suffixes. Only emails claiming to be from gov.uk addresses that contain specific keys known to the email domain owner -- the government -- can now be sent to UK internet users.

"Whoever was sending 58,000 malicious emails per day from taxrefund@gov.uk isn't doing it any more," noted Mr Martin.

GCHQ has also rolled out automated detection and response systems which identify large- scale "commodity" attacks where hundreds of spam emails are sent out indiscriminately. Internet companies receive automatic takedown requests from the systems as soon as spam campaigns which masquerade as government services are identified. The average lifespan of such attacks has dropped from 49 hours to 5 hours as a result, Mr Martin said.

"Faced with a problem of this importance and scale, we believe it is worth trying something new, unleashing innovation in the hope and expectation we can achieve a very significant breakthrough in the coming years."

Washington Post
Obama to be urged to split cyberwar command from NSA
Tuesday, 13 September 2016
Byline: Ellen Nakashima

Washington - The Pentagon and intelligence community are expected to recommend soon to President Obama that he break up the joint leadership of the National Security Agency and U.S. Cyber Command to create two distinct forces for electronic espionage and cyberwarfare.
The potential move is driven by a sense that the two missions are fundamentally different, that the nation's cyberspies and military hackers should not be competing to use the same networks and that the job of leading both organizations is too big for one person.

Obama was on the verge of ending the "dual-hat" leadership in late 2013, but was persuaded to hold off when senior officials, including then-NSA Director Keith B. Alexander, argued against it on the grounds

that the two organizations needed one leader to ensure that NSA did not withhold resources from CyberCom.

Three years later, Defense Secretary Ashton B. Carter and Director of National Intelligence James R. Clapper are pressing for the split, with Carter seeking to build Cyber Command into a full- fledged fighting force that has its own network accesses to conduct attacks. Clapper, officials said, supports the idea in part to reduce tension over which force gets to use the networks -- the spooks or the warfighters.

And with the White House apparently eager to get it done before Obama's term ends, some officials said that the decision appears all but certain.

Carter and Clapper also favor having a civilian in charge of the NSA, as at CIA. That would be a break from tradition. Since its inception in 1952, the NSA has been led by a military officer.

The proposed decision reflects a growing debate over how to organize military cyberoperations as they mature and diverge from the intelligence realm that birthed them.

Adm. Michael S. Rogers, currently the head of the NSA and CyberCom, last week told an audience at the Intelligence & National Security Summit that "I believe in the long run the right thing is to keep these two [organizations] aligned, but to separate them."

But on Tuesday, Rogers clarified his remarks to suggest now was not the time.

At a hearing of the Senate Armed Services Committee, the chairman, Sen. John McCain (R-Ariz), noted Rogers earlier this year supported retaining the "dual-hat" relationship. "Is it still your professional advice" that such an arrangement is in CyberCom's best interests? McCain asked. "Yes," Rogers replied.

McCain also issued a warning to the administration. If it separated the two organizations, McCain said he would oppose any nominee put forward to head the NSA if that person is not also picked to lead Cyber Command.

Cyber Command, established in 2009 inside NSA headquarters at Fort Meade, Md., has long depended on the spy agency's capabilities. NSA and Cyber Command personnel sit side-by-side and use the same networks that were built by the agency.

But following revelations of NSA surveillance programs by former contractor Edward Snowden, a presidential commission recommended that NSA and Cyber Command be separated, arguing that the intelligence-gathering and combat functions have distinct targets and purposes. The spies want to steal information without getting caught. The fighters want to disrupt systems and don't mind if the enemy knows who did it.

Carter has brought Cyber Command into the fight against the Islamic State and wants it to act openly, like other military commands, rather than as the annex of a highly secretive spy agency. He also wants Cyber Command to control the resources it needs.

"Whether or not it's true, the perception with Secretary Carter and [top aides] has become that the intelligence agency has been winning out at the expense of [cyber] war efforts," said one senior military official, who like other officials interviewed for this article spoke on condition of anonymity because he was not authorized to discuss the issue publicly.

The Office of the Director of National Intelligence and the Pentagon declined comment.

"We are constantly reviewing if we have the appropriate organizational structures in place to counter evolving threats, in cyberspace or elsewhere," one senior administration official said. "While we have no changes to this structure to announce, the relationship between NSA and Cyber Command is critical to safeguarding our nation's security."

Some former officials believe that Cyber Command can never be fully independent of the NSA and that it makes no sense to cleave one from the other.

"When you have two organizations whose missions overlap or touch, unless you have some way to control both of them, then they will instantly go to war with each other," one former senior intelligence official said.

"Cyber Command's mission, their primary focus, is to degrade or destroy," the former official said. "NSA's is exploit [to gather intelligence] only. So without having one person as the leader for both, the bureaucratic walls will go up and you'll find NSA not cooperating with Cyber Command to give them the information they'll need to be successful."

On Capitol Hill, the Senate Intelligence Committee has put language in its 2017 intelligence authorization bill that bars the NSA director from serving at the same time as the Cyber Command head. The Senate Armed Services Committee, however, is reluctant to see a split until the defense secretary and chairman of the Joint Chiefs of Staff certify to Congress that such an arrangement will not "pose risks" to the military effectiveness of Cyber Command.

There is a uniform agreement, however, that if joint leadership is ended the two organizations must still work closely with one another. They would need to ensure that operations don't interfere with each other's and that the NSA must continue to supply CyberCom with intelligence.

Military officials said that Cyber Command could develop its own network nodes or "accesses" to carry out missions independent of the NSA, although some are skeptical that it can be done without spending substantial sums to duplicate NSA's infrastructure.

"The country can't afford it," the former intelligence official said. "NSA's a trillion-dollar investment."

Others disagreed. "It's not like you have to rebuild all of NSA in order for Cyber Command to be independent," a second administration official said.

If the separation goes forward, a key challenge will be funding for Cyber Command to develop the capabilities it needs. The command is still building up its force structure, aiming for 6,200 personnel by October 2018.

Motherboard (Vice)
Hacker Guccifer 2.0 Gives Rambling Speech at Cybersecurity Conference
Tuesday, 13 September 2016
Byline: Lorenzo Franceschi-Bicchierai

New York - The hacker who claimed to be behind the breach on the Democratic National Committee, who goes by the name Guccifer 2.0, was slated to talk via livestream at a London cybersecurity conference on Tuesday.
But, perhaps unsurprisingly, Guccifer 2.0, whom experts believe is just a front for Russian government hackers, was a no show. Instead, someone else read out loud a rambling statement purportedly sent by the hacker.

In the long statement, Guccifer 2.0 talks about who's really to blame for data breaches (spoiler alert: definitely not hackers like him), accuses Twitter of censoring his "twits," and blames government contractors as the real culprits because they make buggy software.

"As a result they pose a threat to the critical infrastructure elements and the national security as a whole. Total computerization along with inadequate software development may cause a lot of troubles," Guccifer 2.0 said, according to a transcript obtained by Motherboard. "That's why it's better to use paper sometimes. We should start now to prevent electronic apocalypse and rise of the machines in the future. Or else it would be too late."

Guccifer 2.0 also released around 600 megabytes of data, allegedly stolen from NGP VAN, a company that provides services to the DNC. The hacker claimed in an interview with Motherboard earlier this summer that he broke into the DNC by finding a flaw in NGP VAN. NGP VAN did not respond to a request for comment, but there's no evidence that a flaw in the company's software was the way in for the hacker. ThreatConnect, a security firm that's followed the DNC breach since the beginning, said that Guccifer 2.0's claims regarding NGP VAN don't make any sense.

It's unclear why Guccifer 2.0 didn't connect via livestream as it was advertised. The conference organizers did not respond to a request for comment. Guccifer 2.0 also did not respond to a Twitter message.

Here's the full transcript of Guccifer 2.0's rambling message, read out loud during the conference.

Hello everyone This is Guccifer 2.0.

I'm sure you know me because my name is in the conference program list. As I see it, this is the place to discuss cyber security and cyber threats. And may be to propose some solutions. Let's figure out who poses the real threat to begin with.

Cyber security firms are quick to blame hackers for their activity. Yeah, they cause a lot of troubles for business and politics. But, who poses a real cyber threat? what do you think? Is it Guccifer? Or Snowden? Or Assange? Or Lazar? No. It seems obvious. It's plain as day you would say. But still my answer is no. Large IT companies pose a real cyber threat nowadays.

You may perfectly know some of them or may not. But their responsibility for the future of our world is growing from day to day. And I will explain to you why.

So. What's wrong with large IT companies? First. On their way to a global progress and big money they are collecting users' personal data, which is the same as spying on people, because many of us don't even realise they track us online and collect our info. Companies store these data making it vulnerable for leaks.

Second. They create conditions that make people store their info in cloud services. It seems convenient but it's extremely vulnerable because it's thousand times easier to steal the data from the cloud than from a personal cell phone for instance.

The next reason, and the crucial one, is software vulnerability. Tech companies hurry to finish the work and earn money. So they break development cycle very often omitting the stage of testing. As a result, clients have raw products installed on their systems and networks with a great number of bugs and holes.

Fourth. It's well known that all large companies look forward to receiving governmental contracts. They develop governmental websites, communication systems, electronic voting systems, and so on and have their products installed to critical infrastructure objects on the national level. They are aggressively lobbying their interests. You can see it at the diagram that they spent millions of dollars for lobbying. That doesn't mean they will produce better software. That means they will get even more money in return.

Fifth. This is censorship. For example Twitter censors unwelcome users. I can judge it by myself here. You can see how Guccifer 2 hashtag unnaturally abruptly stops trending. It seems impossible that all Twitter users just stop twitting about Guccifer 2 leaks, in a moment. That's why people started Guccifer

3, 4, 5 hashtags to avoid censorship. People also told me their twits [sic] were not shown in the Twitter live wall unlike to their account's wall.

So, the cyber aggressiveness is progressing nowadays. The number of cyber attacks is steadily growing. What's the reason? What's wrong with the cyber defense? Well. they take wrong measures. They search for cyber criminals, sentence them. But two more hackers appear instead of one convicted.

The real problem is inside. This is just the same as in offline world. This is not enough to prosecute criminals. It requires preventive measures, to fight criminality by elimination of the possibility of crime.

So, what's the right question we should ask about cyber crime? Who hacked a system? Wrong. The right question is: who made it possible that a system was hacked? In this regard, what question should you ask me? How I hacked the DNC??? Now you know this is a wrong question. Who made it possible, that I hacked into the DNC. This is the question.

And I suppose, you already know the answer. This is NGP VAN Company that operates the DNC network. And this is its CEO Stu Trevelyan who is really responsible for the breach. Their software is full of holes. And you knew about it even before I came on stage. You may remember Josh Uretsky, the national data director for Sander's presidential campaign. He was fired in December, 2015 after improperly accessing proprietary data in the DNC system.

As it was agreed, he was intentionally searching for voter information belonging to other campaigns. However, he is not to blame. The real reason voter information became available for non- authorized users was NGP VAN's raw software which had holes and errors in the code.

And this is the same reason I managed to get access to the DNC network. Vulnerabilities in the NGP VAN software installed on its server which they have plenty of. Shit! Yeah? This scheme shows how NGP VAN is incorporated in the DNC infrastructure.

It's for detailed examination, if you are interested. And here are a couple of NGP VAN's documents from their network. If you r [sic] interested in their internal documents. You can have them via the link on the screen. The password is usual. It's also on the screen. You may also ask the conference producers for them later.

So, as you see there's no need to breach into separate users accounts or separate systems. You just need to hack their tech company. This is the feature. Big IT companies lead us to a disaster. In their pursuit for money they release raw software, so their clients are highly vulnerable. It became usual to blame everything on hackers while IT companies just pretend they are working hard to patch bugs and to plug holes. And they even ask for more and more money to correct their own mistakes. As a result they pose a threat to the critical infrastructure elements and the national security as a whole. Total computerization along with inadequate software development may cause a lot of troubles. That's why it's better to use paper sometimes.

We should start now to prevent electronic apocalypse and rise of the machines in the future. Or else it would be too late. As the financial corporations are ruling the world now so the IT companies will rule it in the near future. What should we do? You would tell me I could report a bug to the company as it's commonly done. What do you think they would answer me? Thanks? Or this is not crucial? Or maybe they would even give me some money. Yeah But what could it change? Nothing. Yeah. Really. Nothing at all.

We need to shake the situation, to make our voices sound. Yeah, I know if they find me I'm doomed to live like Assange, Snowden, Manning or Lazar. In exile or in prison. But it's worth it for they are the heroes, heroes of new era.

Thanks for ur attention. See you online!

Geek Wire
Edward Snowden's former boss speaks out: 'I would have hired him again' -- but not now
Wednesday, 14 September 2016
Byline: Alan Boyle

Seattle - The cybersecurity expert who hired Edward Snowden for his last job is laying out his lessons learned - but admits it would have been hard to stop the man who spilled some of the National Security Agency's most closely held secrets.
"Knowing what I knew at the time, I would have hired him again," Steven Bay, a former cyberintelligence analyst for Booz Allen Hamilton, said today in Seattle at the IEEE Computer Society's "Rock Stars of Cybersecurity" conference.

"Knowing what I know now, obviously, I wouldn't," he added.

Bay said today's talk marked the first time he discussed his side of the Snowden story in a public forum.

After the story broke, Bay lost his NSA access and had to switch to a different position at Booz Allen Hamilton, which was Snowden's employer for those crucial few months in the spring of 2013. Bay said he couldn't talk openly about the case until he left Booz Allen this June. Now he's the chief information security officer for NuVasive, a medical devices company in San Diego.

'Nerded out' at job interview

Snowden's timeline is well-known by now: After years of working at the CIA, and as a Dell contractor for the NSA, he applied for another NSA contract job in Hawaii with Booz Allen. Bay said he and his office's technical director interviewed Snowden at a Wendy's restaurant near the agency's facilities in Kunia.

"He was a highly technical person," Bay recalled. "He was very passionate about internet anonymization, as he's come out and talked about. He claimed to have run two Tor nodes out of his home ... and he also claimed to have known a zero day vulnerability within Tor."

Snowden knew his stuff so thoroughly that Bay said the technical director took over the interview and "basically nerded out for an hour."

Snowden got the job, and started working as an intelligence analyst at the NSA's facility in Hawaii at the beginning of April in 2013.

Bay said two red flags came up in the weeks that followed. First, Snowden began asking about a highly classified mass-surveillance program that's now known to the public as PRISM. Bay had access to the PRISM data, but Snowden didn't.

Bay didn't give Snowden access to PRISM, but he did provide him with some data that in retrospect he shouldn't have. "I shared a little bit too much information," Bay acknowledged today. He said that's what caused him to lose NSA access after the Snowden story broke.

A case of epilepsy?

The second red flag popped up when Snowden started coming in late to work, only a few weeks after starting the job. When Bay asked about it, Snowden told him he was suffering from epilepsy.

In response, Bay played the role of a supportive manager. Then, in mid-May, Snowden told him the epilepsy was getting worse and that he'd have to go in for tests on the following Monday and Tuesday. If the results weren't good, he might have to be out even longer.

Bay said he suggested that Snowden apply for short-term disability, but Snowden told him he didn't want to bother with the paperwork. "Which made no sense to me ... but to each his own. If he wanted to take leave without pay, take leave without pay," Bay said.

In reality, Snowden wasn't suffering from epilepsy. Unbeknownst to Bay, Snowden took off for Hong Kong on that Monday, May 20, carrying gigabytes' worth of NSA data with him.

Bay said he received an email from Snowden the next day, telling him the test results were bad and that he'd have to take more time off work. In a reply email, Bay reminded Snowden to check in with human resources about filing for disability.

"Wednesday night, the next night, he emails me back, and says, 'OK, sounds good, I'll get in touch with HR.' And that was the last I ever heard from him," Bay said.

Bay tried to check in with Snowden several times afterward, to no avail. At the end of the month, Bay called his boss in Georgia, asking what to do about Snowden's time sheet. In response, the supervisor alerted NSA's security team to Snowden's medical leave and his missing status.

"Thank goodness he did this," Bay said. "It really protected us at Booz Allen, and myself as well."

'I was worried that he was dead'

That was on a Friday. The following Monday, NSA officials told Bay they were on the case. All that week, he and NSA agents went searching for Snowden.

"In my mind, I was worried that he was dead," Bay said. "I was worried that he had an epileptic seizure of some sort, or a blackout while driving on the island, and he drove off a cliff and killed himself. That's what I was concerned about. The thought that Ed could be doing any of this didn't even cross my mind."

Bay said The Guardian published its first story based on NSA leaks on the Thursday of that week in June. "It was the talk of the agency," he said. A couple of days later, one of his best friends at work wondered out loud whether Snowden might be involved.

"I thought, 'No way! There's not a chance that Ed would do that.' And I made the comment that that would be my worst nightmare," Bay said.

The next day - Sunday, June 9 - Bay turned off his phone for a church meeting. When he turned it back on, he faced a torrent of texts. The first text was from his friend, reading: "Sorry, man, it looks like your worst nightmare came true."

'Are people going to die over this?'

That's how Bay found out Snowden was the leaker. Three years afterward, Bay still gets emotional when he remembers the moment.

"I found an empty room at the church, and I broke down," Bay said. "Every negative thought one could have, I had. There were thoughts of 'I'm going to lose my job, I'm going to be blamed, I'm going to get fired, I'm going to go to jail, I'm going to be the scapegoat.' And I started thinking about what this is going to do to NSA, what about all of our undercover agents, what if that sort of information gets out? Are people going to die over this?"

Bay spent most of the rest of the day in meetings with executives at Booz Allen and agents from the FBI. "Surprisingly, the FBI was totally cool," he recalled. "I was expecting to be in a dark room with a hot light on me. ... It was nice to hear, despite all these negative emotions that I felt earlier in the day, that nobody blamed us."

The days after that were devoted to damage control. Eventually, it came out that Snowden had been planning his moves for several years. The fact that he was skilled in information technology and gained access to classified information made him the ultimate "insider threat," Bay said.

"I was visiting with the director of NSA Hawaii, and he made the comment that, well, Booz Allen got caught holding the hot potato when the attack went out. That's pretty accurate," he said.

"It turns out, as [Snowden] admitted a few weeks later, he targeted our contract directly," Bay said. "Somehow he figured out that our contract, and what we did on that contract, were the types of gates he needed to get access to."

American hero or Russian agent?

Today, Snowden is seen as a hero by millions of people opposed to government intrusions and invasions of privacy. An Oliver Stone movie opening this week, titled "Snowden," casts the whistleblower in a sympathetic light. But as you can imagine, Bay is not a fan.

The fact that Snowden has been given asylum by the Russian government, under the leadership of President Vladimir Putin, leads Bay to say that Snowden is probably colluding with that country's security services.

"I do believe that Ed has given up the goods to Putin," Bay said.

Snowden strongly denies making any such deal with Russian intelligence, or handing over any secrets to the Russians. "Everything I had is in the hands of journalists," Snowden told the BBC last year.

La Tribune (France)
La France a été la cible d'une vingtaine de cyberattaques majeures en 2015
Wednesday, 14 September 2016
Byline: Michel Chabriol

Paris - Le directeur général de l'ANSSI Guillaume Poupard a indiqué que la vingtaine d'attaques informatiques majeures lancées en 2015 contre la France a principalement concerné des entreprises. Soit clairement de l'espionnage économique.
Cela fait évidemment froid dans le dos même si, in fine, ce n'est guère surprenant. "Il faut savoir que la France a connu, en 2015, une vingtaine d'attaques majeures informatiques", a révélé le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), Guillaume Poupard, dans le cadre du premier rapport d'activité de l'Agence publié mardi depuis sa création en 2009. Interrogé sur les révélations du "Monde" sur un piratage américain de l'Elysée en 2012, il a répondu lundi lors d'un point presse portant sur le bilan de l'activité de l'ANSSI en 2015, qu'il ne confirmait pas ces informations.

Dans un contexte croissant d'attaques informatiques, le secrétaire général de la défense et la sécurité nationale (SGDSN), Louis Gautier, auquel l'ANSSI est rattachée, a pour sa part assuré lundi que "les mois qui viennent vont être marqués par la continuité des nos actions". Notamment dans le domaine de la prévention. "On n'est pas sur un effet de mode", a d'ailleurs expliqué le patron de l'ANSSI, qui a rappelé que dans ce domaine la France n'avait "pas d'amis mais des alliés".

Espionnage économique

Guillaume Poupard a souligné "un état des lieux particulièrement inquiétant" en matière d'attaques informatiques "plus fortes et mieux organisées". Mais il est resté très discret sur les attaques de grande ampleur lancées contre la France - sabotage ou prise de contrôle du système d'information à des fins d'espionnage -, à l'exception de celle subie en avril 2015 par TV5 Monde.

Cette cyberattaque spectaculaire et médiatique est l'oeuvre de Daech, qui aurait été aidé par des mercenaires informatiques, a soupçonné Guillaume Poupard. Elle a ainsi offert à l'Agence, gardienne de la sécurité des systèmes informatiques de l'Etat et des opérateurs d'importance vitale (OIV), une vitrine de son savoir-faire. "Le cas de TV5 Monde a permis de mettre en avant la menace réelle", a-t-il souligné.

Sinon, pour les autres attaques, c'est le black-out complet ou presque "pour des raisons de sécurité", a expliqué Guillaume Poupard. Le patron de l'ANSSI a simplement indiqué que ces attaques, difficilement attribuables, avaient principalement concerné des entreprises en 2015. Donc très clairement de l'espionnage économique notamment lors d'appel d'offres internationaux. "Reconstruire les réseaux informatiques attaqués est extrêmement compliqué et long à réaliser, a en outre fait remarquer Guillaume Poupard. Cela peut durer entre six mois et deux ans".

4.000 signalements reçus

En 2015, l'activité de l'ANSSI en réponse à des incidents signalés a connu une croissance importante. Ainsi, 4.000 signalements ont été reçus, soit 50 % de plus qu'en 2014. "Cette augmentation est notamment due au développement, par des prestataires privés, de services de détection des attaques au profit des entreprises", souligne l'ANSSI dans son rapport. Un grand nombre de ces signalements (61% concernent des défigurations de sites internet) se sont avérés être des incidents de sécurité et ont été traité par le le centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI.

Ce travail d'enquête a permis à l'Agence de constater l'émergence de nouvelles attaques, dont les "rançongiciels", des logiciels malveillants chiffrant les données d'un ordinateur, qui sont alors prises en otage le temps de payer une rançon. L'an dernier, plusieurs opérations de recherche de codes malveillants ont permis d'en identifier 2.300. L'ANSSI, qui est également chargée de superviser les systèmes d'information de l'Etat et des OIV, a publié 568 avis des correctifs de sécurité, et surtout quinze alertes sur des vulnérabilités critiques. L'Agence a notamment conseillé des OIV, tels ERDF, Areva ou Engie (ex-GDF Suez).

Montée en puissance de l'ANSSI

Ces dernières années avec la lutte contre les attaques informatiques devenue une priorité, l'ANSSI a connu une importante croissance de ses effectifs, passant de 120 agents en 2009 à près de 460 à la fin de l'année 2015. "On approche aujourd'hui les 500 salariés", a souligné Guillaume Poupard. L'an dernier, 108 salariés ont ainsi rejoint l'agence, qui toutefois subit un turn-over important de ces effectifs. "L'effectif cible est de 600 personnes à l'horizon de 2018", a rappelé Louis Gautier.

« Avec la montée de la dimension numérique dans tous les aspects de l'économie et de la société, la place et les missions de l'ANSSI sont nécessairement vouées à s'accroître, souligne Guillaume Poupard. L'agence va donc continuer à renforcer ses moyens, son expertise et ses relations avec les différents acteurs". »

En 2015, l'ANSSI a dépensé pour ses projets 36,9 millions en crédit de paiement. Elle a notamment travaillé à l'acquisition et à la maintenance d'équipements informatiques et de réseaux locaux pour son propre usage. Elle a également oeuvré à la conception, à la réalisation, au déploiement, à la maintenance et à la gestion de dispositifs de communication électroniques sécurisés. Enfin, 2015, l'ANSSI a ouvert un chantier sur les objets connectés, sources d'innovation mais aussi de nouvelles menaces.

La Presse+
Darkrace Un système immunitaire contre les cybermenaces
Friday, 16 September 2016
Byline: Karim Benessaieh

Ottawa - Chaque jour au Canada, 1600 attaques de rançongiciels auraient lieu. Mots de passe et dossiers confidentiels volés font régulièrement l'actualité, stimulant la recherche de nouvelles approches pour assurer la sécurité des réseaux. L'une d'elles, conçue à l'Université de Cambridge et imitant le système immunitaire humain à partir des mathématiques probabilistes, semble prometteuse. Elle est proposée depuis 2013 par l'entreprise britannique Darktrace, qui a ouvert en avril dernier son bureau canadien, dirigé par l'ex-agent des services secrets David Masson. Entrevue.
Q D'abord, pourriez-vous vous présenter ?

R J'ai été membre du service de renseignement britannique, le MI5, pendant plus de 20 ans, puis j'ai travaillé au sein du Service canadien du renseignement de sécurité (SCRS) pendant quatre ans. Je m'occupais de cybersécurité et de sécurité nationale en général. Je me suis ensuite joint à la compagnie Darktrace en janvier de cette année, après une invitation à établir un bureau ici, au Canada.

Q Expliquez-nous l'approche de type « système immunitaire » au coeur de la technologie proposée par Darktrace.

R J'aimerais utiliser une métaphore. On a pris le modèle du système immunitaire humain. La première protection, c'est ma peau. Pour un réseau, c'est le pare-feu. Mais ce n'est pas assez, j'ai besoin d'un système immunitaire à l'intérieur qui a une compréhension innée de mon corps. Au moment où quelque chose traverse la peau, mon système immunitaire sait immédiatement que ce virus ou cette bactérie ne fait pas partie de moi.

Q Comment votre « système immunitaire pour entreprises » reconnaît-il les anomalies ?

R Il n'a pas besoin d'une formation, n'a pas besoin de recevoir des indications, il est sans cesse à l'écoute. Il comprend le comportement normal des utilisateurs et peut repérer ce qui ne fait pas partie du fonctionnement habituel du réseau. Il apprend par lui-même, sans intervention humaine. C'est nécessaire parce que les réseaux ne sont pas statiques, ils se développent sans cesse, ont des visiteurs, de nouveaux membres. Un humain ne pourrait pas gérer toute cette information. Un ordinateur, lui, le peut.

Q Le concept est séduisant. Mais est-ce que ça fonctionne ? Est-ce plus efficace que les antivirus et les protections informatiques classiques ?

R On a toujours besoin des pare-feu et des antivirus. Notre technologie est supplémentaire. Ça marche, absolument : on a trouvé des menaces que les autres méthodes n'avaient pas détectées. La technologie actuelle est basée sur les signatures et les règles. Une signature signifie que quelque chose de mauvais

est déjà passé. C'est de la vieille nouvelle, en quelque sorte. Ça ne vous protégera pas contre les menaces qui n'ont pas encore frappé.

Q Les fameuses vulnérabilités « Zero day », pour lesquelles il n'existe pas encore de protection...

R Oui, les « Zero day », ou une menace qui a déjà traversé le pare-feu, qui existe à l'intérieur du réseau. Un employé qui a cliqué sur un lien sans savoir ce qu'il a fait et a téléchargé un virus, ou un employé qui a décidé de faire des dommages à l'organisation...

Q Êtes-vous la seule entreprise à utiliser cette approche du système immunitaire ?

R Il y en a d'autres, mais nous sommes la seule qui utilise l'apprentissage automatique non supervisé, avec une approche mathématique appelée « estimation récursive bayésienne » [qui évalue les probabilités d'un événement].

Q Quelles sont les cybermenaces les plus dangereuses en 2016 ? Quel est l'état des lieux ?

R Il y en a deux types. Les rançongiciels sont un grand problème partout dans le monde, ils peuvent frapper partout, les statistiques indiquent que le phénomène va aller en s'aggravant. Parce que c'est facile à effectuer pour les pirates : ils entrent, brisent tout et prennent l'argent.

Q Et le deuxième type ?

R L'autre danger, ce sont les menaces intérieures. Un employé qui décide de faire des dommages, qui fait des erreurs... Toutes les entreprises peuvent être touchées. Si 99 % des employés ne représentent aucune menace, le 1 % qui reste peut causer beaucoup de problèmes.

National Post
Dutch police to get Canadian BlackBerry data
Friday, 16 September 2016
Byline: Joseph Brean

Ottawa - After a police raid on a Toronto technology company, Canada has agreed to share a massive stash of encrypted BlackBerry Ltd. messages with Dutch police investigating an underworld conspiracy involving robberies, drug trafficking, attempted murder and assassinations.
But rather than simply hand over the messages, from 20,000 different users, an Ontario judge this week

imposed restrictions designed to prevent a "fishing expedition" by police in the Netherlands or any other country. The ruling ensures the data will remain under Canadian control, and not be shared further without a court's approval.

The fear is that unfettered disclosure would expose innocent people to the unjustified attention of police, just because they used an encrypted Black-Berry.

"Canada remains the home of this data," Judge Ian Nordheimer wrote.

The case arose from a Dutch probe of an organized crime ring, in which police seized assault rifles, machine guns, grenades, vehicles, tracking devices, and large sums of money. Unusually, they also kept discovering BlackBerrys that had been modified to send only encrypted messages, outside the normal cellphone network.

The BlackBerrys had been modified so they could not be used for phone calls or Internet access or to take pictures. Their microphones had been disabled or removed.

That service was offered by a Dutch company, Ennetcom, which sold the modified BlackBerrys for about 1,500 euros ($2,220), and had the power to remotely "wipe" them clean of data. Ennetcom bills itself as a pioneering data protection company that will "defend against all forms of cybercrime."

Dutch authorities, however, allege Ennetcom was actively facilitating organized crime by offering an almost uncrackable encryption service for gangsters, using the famously secure BlackBerry.

Further Dutch investigation revealed the devices were all using a particular IP address, a routing code for Internet traffic, which they traced to Bitflow Technologies Inc., an Internet hosting company with offices at One Yonge Street on the Toronto waterfront.

Riaz Timol, a lawyer for Bitflow, said the company's part in the case is entirely innocent. "They don't know what's on the servers. They rent space to people," he said.

The search warrant executed at Bitflow was coordinated with raids in the Netherlands on April 19. The head of Ennetcom, Danny Manupassa, 36, was held for two weeks by police

on money laundering and weapons charges. He was released with conditions that included not leaving the country.

He later wrote a letter that came before Judge Nordheimer in which he "denies any conscious involvement with anyone who used the services of his company for criminal purposes." Manupassa was also "critical of Dutch authorities for not requesting assistance and/or information from him, prior to taking the steps that they did."

The 20,000 users are said to include the Dutch criminal suspects and their associates, but also likely include many innocent users of Ennetcom's service.

Most are believed to be Dutch.

Washington Post
U.S. gives 'no free pass' to Russia, other nations on cyberespionage, Justice official warns
Friday, 16 September 2016
Byline: Ellen Nakashima

Washington - A senior Justice Department official this week issued a thinly-veiled warning to Russia that significant acts of cyberespionage will not be ignored.
That would include the Democratic National Committee hack, which would be considered an act of political cyberespionage of the sort the United States traditionally has not publicly attributed to a culpable foreign spy agency.

That set of intrusions, disclosed by the DNC in June, has been linked to the Russian government by FBI investigators, though the U.S. government has not publicly acknowledged that.

Nonetheless, said Assistant Attorney General for National Security John Carlin, if Russia or any other country thinks "there's going to be a free pass, that we can't figure out what they're doing in cyber-enabled espionage, I think the message should be clear: You're wrong. You can and will be held accountable." Carlin was speaking at a conference Wednesday at the Center for Strategic and International Studies held on the 10th anniversary of the Justice Department's National Security Division.

He added that although all nations have spy operations, that does not mean the U.S. government will not take action against cyber spies who are detected. "If you get caught spying," he said, "there are consequences."

A White House official echoed Carlin when asked if the administration would take action against Russia for the DNC hack. "Look, we know Russia is a bad actor in cyberspace, just as China has been, just as Iran has been," said Lisa O. Monaco, President Obama's adviser on counterterrorism and homeland security, who also spoke at CSIS. "Nobody should think that there is a free pass when you're conducting malicious cyber activity."

But she said she did not want to say what response the government might take until the FBI completes its investigation into the DNC hack and related incidents, including a mass disclosure by the anti-secrecy site WikiLeaks of stolen DNC emails.

Other officials at the conference made clear that a U.S. response might be under the radar. "We have a variety of tools that we as a government use to try and deter behavior on the Internet outside of norms," FBI Director James B. Comey said. "That can involve a variety of things, only some of which would be visible to the public. Just because you can't see something doesn't mean your government's not doing something to change behavior."

The administration is struggling with whether to publicly blame Russia for the DNC hack. There are political and diplomatic concerns -- and a reluctance to do something that might escalate the situation.

"There's a question of whether public attribution will further the administration's goals and national security interests," said one administration official, who spoke on condition of anonymity because of the matter's sensitivity. "That's always a part of the equation."

BBC News
Edward Snowden hits out at critical report into his activities
Friday, 16 September 2016

London - Edward Snowden has dismissed a report by the House of Representatives intelligence committee that heavily criticised his activities.
It rejected his view of himself as a whistleblower, and said he was a disgruntled employee whose actions did nothing more than help US enemies.

The report comes a day after two rights groups launched a campaign for President Obama to pardon Mr Snowden.

The White House has rejected the possibility of a presidential pardon.

The release of the report, two years in the making, also coincides with that of the film "Snowden", directed by Oliver Stone.

In a series of tweets, Mr Snowden dismissed the report's findings, writing: "Their report is so artlessly distorted that it would be amusing if it weren't such a serious act of bad faith."

Mr Snowden, the former National Security Agency (NSA) contractor, has been living in Russia since 2013, when he gained notoriety for releasing thousands of classified documents that revealed mass phone and internet surveillance put in place after the 9/11 attacks.

Releasing a summary of its 36-page investigation into the case, the House committee said Mr Snowden had fallen out with his colleagues and lied about his background while at the NSA.

It says that most of the material he leaked related to military secrets that had nothing to do with Americans' privacy but were to "protect American troops overseas and... provide vital defenses against terrorists and nation- states".

Amnesty International and the American Civil Liberties Union launched their 'Pardon Snowden' campaign on Wednesday, urging President Obama to do so before he leaves office in January 2017.

Amnesty said no-one should be prosecuted for exposing human rights violations, which, it claimed, is what "indiscriminate mass surveillance of communications" amounts to.

The ACLU acts as Snowden's legal adviser, and called him "a great American who deserves clemency for his patriotic acts".

Dhaka Tribune
CID fears failing to catch hackers
Friday, 16 September 2016
Byline: Kamrul Hasan

Dhaka - At six months into the investigation of the Bangladesh Bank cyber heist, investigators say they are continuing to focus on the beneficiaries of the crime.
They also admitted that they may not be able to trace the hackers at this point as the criminals had had enough head start to erase all traces from the mechanism.

"They can remove their traces but they cannot make the crimes clueless. We have got the names of the people who received the stolen money and keeping them under surveillance with assistance from concerned local police forces," said Criminal Investigation Department (CID) spokesperson Mirza Abdullahel Baqui.

CID took charge of the case on March 16, 41 days after the heist took place. On February 4, hackers stole more than $101 million from Bangladesh Bank's account with the Federal Reserve Bank of New York and wired it to a number of bank accounts in the Philippines and Sri Lanka.

According to the case statement, a total of 101 million dollars were illegally transferred from Bangladesh Bank fund against 35 payment instructions. Of the money, $20 million went to Sri Lanka while $81 million to the Philippines.

The central bank has received the $20 million transferred to Sri Lanka, minus transfer fees of about $70,000. All procedures for getting $18m has been completed in the Philippines, said BB sources.

Two CID teams visited the Philippines and Sri Lanka in April and another team sat on a conference with the concerned countries in Manila later.

CID said they might not get hold of the hackers as the cyber evidence had already been removed when the case was filed. They said the crime should have been given top priority and law enforcement engaged immediately.

Every second was valuable in tracking cyber crime, but the denial of the concerned authorities helped criminals erase their traces, said an investigator seeking anonymity.

Asked if they could trace the hackers or their location, Baqui said they had contacted every advanced agency in the world who had also failed to unearth the truth. Besides, CID is yet to determine the number of suspects.

Confirming that no Bangladeshi, especially any BB officials were involved in the heist, the CID spokesperson said the number of suspects was still uncertain as they were yet to interrogate the foreigners whose names came up in the investigations.

"We cannot name anyone as we do not know who to prosecute due to lack of evidence. We need evidence that we have asked the concern countries to provide."

The CID has not even confirmed any date to interrogate the persons suspected in the Philippines and Sri Lanka, he added.

He said they had asked the concerned officials to provide them some necessary documents several times after they took charge of the investigation. But no country has provided documents yet. However, he said, they were hoping that the documents would be sent soon.

"We were hoping that we would get the documents during the Asia Pacific Group meeting at Dhaka during August but our hopes faded as the meeting was moved to USA. Although the counter countries were to come to our country for attending APG, but an additional meeting was scheduled with them at the same venue," the SS added.

The CID was now planning to arrange another meeting. But could not confirm the date. According to another officials involved in the investigation said polices from around 12 countries were assisting them as the criminals were from those countries were staying there during the time.

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) says it has taken steps to strengthen their security measures.

After the BB heist it sent mails to its users to follow instructions strictly. Reuters reported on May 24 that SWIFT will hold a financial services conference in Brussels where it will launch a five-point plan. On August 30, SWIFT emailed to the user members of the country asking them to update their software.

Abul Kalam Azad, the joint secretary of SWIFT User Group of Bangladesh, confirmed to the Dhaka Tribune of receiving the mail and said they had already taken all necessary measures. He said SWIFT and BB had issued instructions to create improved passwords.

He also said that with the improvement of SWIFT security measures now the system could identify changes in modus operandi, for example accessing the system at odd times from a user account before hacking would alert the users.

Gulf News
Cyber security is the key to happiness
Friday, 16 September 2016
Byline: Faisal Al Bannai

Dubai - As information technology and the internet become integral parts of our daily lives, being secure and confident are one of the essential ingredients of individual happiness.
The advance of technology has been at root a quest to improve a lot of humanity. Investment in intelligent nations and cities is essentially the pursuit of one goal; enabling access to information and tasks to be performed more quickly and efficiently in order to make people's lives easier, and by inference happier.

In the decades ahead, we are likely to see this trend expand even further, as information technology is embedded into every aspect of our daily lives, enabling us to shorten once time-consuming tasks, and be better informed about every aspect of our life from our health to our working schedule.

However, this unprecedented interconnectedness comes with risks. In the world before networked technology, simple threats could be isolated and contained. Intelligent cities, however, thrive because of their very interlinked nature; the dark side of this interconnectedness is a vulnerability. Interconnectedness leaves smart cities and the citizens who live in them vulnerable to cascading threats.

When chaos theory was being popularised at the end of the last century, the "Butterfly Effect" was often cited. The idea that a butterfly flapping its wings in Brazil might, through the complex interaction of weather systems, generate a hurricane on the other side of the world.

Smart cities, and indeed modern civilisations, equally face vulnerability as a consequence of the growing level of interconnectivity and interdependence. Monitoring and control systems may be able to understand traffic flow patterns and adjust energy distribution as required, but the same systems, if hijacked by a malicious hacker, can be used to generate chaos.

Disabling of traffic lights or the shutdown of a power station can generate a wide range of secondary effects, which can often spread far beyond the immediate impact of the initial incident.

A city can still be successful without a beach, or a metro network, or an international airport, but it is impossible for it to be successful without robust digital networks, which can be relied upon to work reliably.

The price to be paid for cyber security breaches is no longer being counted in just monetary terms or dented reputations, but in lives lost and families devastated. In many respects, cyber security is the single most critical issue facing the world today.

Technology has evolved to a point that the 'happiness' we have been able to achieve over the decades through automation and intelligence may effectively be undone if our technological environment is not protected from corruption and abuse.

Nor are threats confined to the city level. We all store, deliberately or through our browsing and consumption habits, vast amounts of personal information online. Should this environment be breached and exploited, it leaves many of US Open to everything from criminal manipulation to theft and potentially reputational damage.

As we are aware of many aspects of our life; remaining happy is harder than pursuing happiness in the first place. If we are to guarantee future happiness, we need to think about security holistically, embedding it routinely into our hardware, networks, and habits. Cyber security isn't just an addition to our everyday lives; it's a vital part of securing our current and future happiness; which is what organisations such as ours are attempting to do -- protecting the future by securing its technologies.

Los Angeles Times
Hack the vote? Not easily
Friday, 16 September 2016
Byline: Del Quentin Wilber, Brian Bennett

Washington - The recent Russian hack into the Democratic National Committee's computers and subsequent FBI warning that two states' elections databases had been victims of cyberattacks are raising fears that a foreign power might penetrate U.S. systems and try to alter the outcome of November's vote. Though possible, such an unprecedented foreign election day hacking would be hard to pull off, experts say. Here are some answers to common questions:
How realistic is the threat that hackers could break into U.S. election systems and alter vote tallies?

Not very, thanks mostly to the fact that even presidential elections are highly decentralized and often still rely on old-fashioned systems rather than cutting-edge technology.

First, there are more than 8,000 separate local jurisdictions where voters cast ballots for president, and each one is largely free to use whatever methods, technology and vendors they deem appropriate, based on varying local or state rules and guidelines. There are few federal mandates on how to conduct elections, and the mechanics of voting have been left to the states. For would-be hackers, that means there's no easy, one-stop target.

Secondly, about 75% of all votes this cycle will be cast on paper, said Pamela Smith, president of Verified Voting, which tracks election systems nationwide. And many results are still conveyed by telephone, fax or hand delivery.

Even in cases where results are tallied or transferred electronically, if someone were to try to surreptitiously alter official results, there are built-in redundancies -- such as following up an email with a phone call, fax or hand delivery. And with paper, a hand recount is always possible whenever in doubt.

Very few voting machines are directly connected to the Internet, where they might be targeted by hackers based in foreign countries, said Denise Merrill, secretary of state of Connecticut and president of the National Assn. of Secretaries of State.

For hackers to infiltrate voting machines not connected to the Internet, they would need to individually install a bug or virus, presumably by hand, and then hope that one machine spreads the virus to another, or to a computer that tabulates the results. It's possible, and experts note that most voting machines are usually left unguarded on election eve in schools, town halls and other polling places. But it's not likely, particularly on a scale that would make a difference.

"I think it is highly improbable that anything that has been suggested could happen," Merrill said. "There are thousands upon thousands of polling places, each operated independently, by nonpartisan people. It is all broken into such small units, it is just hard to imagine someone hacking into them and being able to make much of a difference in the outcome."

James B. Comey, the FBI director, reiterated that view during a security forum in Washington on Thursday, saying that the U.S. election system's antiquated nature is beneficial from a security standpoint.

"The voting system is dispersed among 50 states. It's clunky as heck," Comey said.

Didn't many jurisdictions move to computerized voting after the disputed 2000 election?

After Bush vs. Gore there was a push to modernize and computerize. In 2002, Congress established a $4-billion fund to help states upgrade their voting machines and systems. Many raced to buy and install touch-screen digital devices in the hopes they would eliminate controversy surrounding paper ballots -- remember Florida's "hanging chads"?

But as states soon discovered, digital machines can break down and are more vulnerable to hackers, software bugs and calibration errors than ones based on paper ballots. Many of the early digital machines did not keep paper backups or receipts of votes cast, making it difficult to audit results.

Over the last decade or so, states have been junking purely digital machines in favor of those that spit out paper receipts or keep a paper record of a vote.

Now most cybersecurity experts are pushing states to embrace optical scanning systems, in which voters fill out bubbles or boxes on paper, and then ballots are scanned by machines. (Remember those Scantron tests from high school?) This method has two major benefits -- paper ballots can be checked against the computerized results, and the machines tabulate votes much faster than poll workers counting by hand.

Where are hackers most likely to strike?

Battleground states. If a hacker wanted to tip the election for GOP nominee Donald Trump, he or she would not try to flip California, a strongly Democratic-leaning state, into Trump's column because such a result would immediately raise suspicions.

If hackers penetrated the machines or voting systems in swing states such as Ohio or Pennsylvania -- which deploy digital machines, for example -- to affect just a sliver of the votes, they might change the outcome in a close election.

"In a battleground state, a small nudge may have a big impact," said Dan Wallach, a Rice University computer science professor. He urged battleground states to step up measures to guard against attacks and to upgrade to optical scanners.

Couldn't someone hack into a state's election results website and alter numbers as they were being reported?

They could, and it might result in some initial confusion, but it would almost certainly be detected once local jurisdictions compared their results with the state's tally and noticed discrepancies. "That kind of hack would be caught very quickly," said Merle S. King, executive director of the Center for Election Systems at Kennesaw State University in Georgia.

But it illustrates a bigger problem of credibility. In an election in which Trump has already warned that results might be "rigged," even an unsuccessful attempt to alter tallies could open the door to conspiracy theories and fuel questions about the election's legitimacy for years to come.

Aren't some votes cast online?

A small percentage of votes cast by U.S. citizens and military service members stationed and living overseas are transmitted over the Internet and thereby more susceptible to hacking. However, Merrill said those ballots are first filled out by the voter and then emailed or sent electronically to elections officials who print and then count the ballots.

While there was once a push to permit widespread online voting, election and security officials have resisted, warning it would make hacking and manipulation far easier. In light of recent hacks, the prospects for Internet voting have greatly dimmed.

Sounds like there is nothing to worry about.

Not quite. A bigger concern is that hackers might infiltrate voter registration databases, which are frequently connected to the Internet. They could theoretically delete names, hoping to create delays or confusion on election day.

In recent months, hackers believed to be from Russia penetrated voter registration systems in Illinois and Arizona. They made off with personal data on about 200,000 people from the Illinois, forcing officials to close the registration system for 10 days, Yahoo News reported. The hacks spurred the FBI to issue a flash bulletin warning about the dangers of hacking.

"Those systems have some vulnerability because they are more connected to the Internet than voting systems," King said. "Hacking those systems and disrupting something would certainly satisfy the goal of undermining confidence in the election, but it would not alter the course of the election."

Election officials noted that even if a voter's name does not appear on the rolls, federal law requires they be offered a provisional ballot and allowed to vote. Once the voter's eligibility is confirmed, those votes must be counted. However, if a hacker managed to purge a swath of voters from the rolls, the resulting lines and chaos may discourage others from casting ballots.

"It doesn't require much imagination to ponder what could happen," Wallach said. "If you selectively disenfranchised voters that you didn't like, you could cause havoc. Yes, provisional voting allows voters to say, 'Your data is wrong. I need to vote.' But they are filling out affidavits. The system is meant to handle dozens and hundreds of voters -- not millions."

What's being done to protect against cyberattacks?

In addition to the FBI alert, Homeland Security Secretary Jeh Johnson in an Aug. 15 phone call reminded state officials that the Department of Commerce's National Institute of Standards and Technology and the U.S. Election Assistance Commission have made recommendations for securing election equipment, such as disconnecting electronic voting machines from the Internet while voting is taking place.

Election officials were also told they can call on cybersecurity experts from the Homeland Security Department's National Cybersecurity and Communications Integration Center to check voting systems for vulnerabilities.

Johnson said he was so concerned about the possibility of a hack he was examining whether to declare certain parts of the election system to be "critical infrastructure," which would free up funding and

resources to help secure ballots, according to a description of the meeting released by the Homeland Security Department.

Washington Post
Answer Russia's cyberattack
Friday, 16 September 2016

Editorial - Less than two months ago, President Obama approved a presidential policy directive spelling out how the federal government would respond to "significant cyber incidents." In the shadowy world of cyberconflict, this is often a difficult problem: how to identify the source of an attack and respond appropriately. Mr. Obama set benchmarks. He defined a significant incident as one that is likely to result in "demonstrable harm" to the national security, economy or foreign relations of the United States, or "to the public confidence, civil liberties, or public health and safety of the American people."
In recent weeks, according to private security experts and government sources, hackers associated with Russia's government have carried out high- profile intrusions intended to weaken that public confidence and disrupt the U.S. election campaign. Mr. Obama should do something about it.

The most spectacular act was the hack of the Democratic National Committee on the eve of the party's convention, in which 20,000 embarrassing internal emails were stolen and then made public through WikiLeaks. The leaked emails showed that DNC staffers leaned against Bernie Sanders; party Chairwoman Debbie Wasserman Schultz was forced to quit, and the campaign of Hillary Clinton was damaged, probably as Russia intended. This was followed by an upload this week of internal DNC data such as private phone numbers and email addresses. And in an assault that seems aimed at besmirching Ms. Clinton and sowing discord, hackers obtained and released emails from former secretary of state Colin Powell that maligned her and Republican nominee Donald Trump.

This adds up to a full-blown attempt by Russia to interfere with the U.S. election cycle and weaken public confidence. It probably won't work - we don't think Americans are so easily cowed. But it calls for a forceful response. The administration has been hesitating, in part because of fragile negotiations with Moscow over the war in Syria. The FBI probe is not complete, and some senior officials have told The Post's Ellen Nakashima they want to wait for the results.

Mr. Obama ought to put his foot down, and soon. The cyberattacks are of a piece with a larger attempt by Russian President Vladimir Putin to subvert Western democracies and the ideals of a liberal, rule-based international order. Mr. Putin's broader campaign has included incitement of war in Ukraine, seizure of Crimea, support for right-wing groups and candidates in Europe, and using a tide of war refugees from Syria to create instability.

In responding, Mr. Obama must take advantage of the strength of an open society and call out the perpetrators, telling the American people what is happening. Mr. Obama does not need to release sensitive intelligence to effectively make the point. Second, Mr. Obama should order the preparation of

economic sanctions against Russian individuals under an executive order he signed that permits sanctions against people linked to malicious cyber-acts. He must put Russia on notice that such disruptive "active measures," as the KGB once called them, will not be tolerated. If Mr. Putin thinks he can get away with generating fog and doubt, the best answer is to drag him and his dirty tricks into the sunshine.

Asharq Al-Awsat
Open Cloud Computing, Key to Smart Cities
Friday, 16 September 2016
Byline: Khaldoun Ghassan Said

Jeddah - In the past years, the world has been witnessing a huge transformation with regards to adopting innovative and creative technology solutions. By developing strategies, governments are working on enhancing citizens' lives, moving to smart cities and investing in communication and information technology and digital transformation towards applying cloud services.
Users need to be wirelessly connected to a high-speed internet that makes the process of sending data to internet, processing it via cloud and browsing results on the user's device look like an instant process.

Movement of communities to smart services requires a development of technical infrastructure that covers all services such as healthcare, education, transport, energy and financial sector. For this purpose, advanced programs should be developed to serve the mass quantity of data processed via cloud.

With the development of Application Programming Interface, any person can benefit from the enormous computing capabilities provided by network servers.

Wireless networks will connect everything together and cloud networks will be the source of techniques in the near future. Cloud services must focus on development of individuals' experiences more than enterprises; the infrastructure should be open for all developers to ensure its spread.

During the Huawei Connect Conference 2016, holding the name "Shape the Cloud", Huawei's Rotating CEO Ken Hu expected the coming ten years to witness the launch of the cloud computing second generation. Hu sees that by 2025, enterprises technology solutions will be all based on the cloud computing technology as well as more than 85% of business applications.

Huawei also formed a coalition that includes the world biggest technology companies for the purpose of insuring an integration between technology and cloud computing. The coalition includes Accenture, Linux Foundation, Intel, TianZi Biodiversity & Development Center, Siemens, General Electric, Honeywell, Hexagon and Infosys.

Near future applications will probably transform devices into a gate to pass data to the cloud via using programming interfaces that are made available for everyone. This indicates that data processing will not occur in the user's device but on specialized devices of high performance.

Yet, the bulk role of smart cities is to protect people through identifying criminals "cloudily". This happens when analyzing the data coming from cameras set up in important and critical locations, given that the systems are able to analyze the way suspicious people behave.

This technique can also brief one-hour videos in one minute to be examined by the specialized security forces.

Sputnik Deutschland
Real Secret Agents on New 'Call a Spy' Hotline Answer Your Burning Questions
Friday, 16 September 2016
Byline: Staff report

Berlin - If you ever wanted to chat to a spy, now's your chance - a group of German artists have set up the "Call a Spy" hotline.
Ariel Fischer from the art group "Peng!" told Sputnik Deutschland that they can set up the hotline anywhere with a stable internet connection.

It looks like an ordinary telephone, but is connected to the "Call a Spy" server.

The server contains a database of spy's numbers, and randomly selects one to connect the caller with. Calls are routed through a private network that masks the original source of the call.

Fischer said that despite the secrecy of intelligence work, the majority of the numbers were freely available on the internet, and come from a range of different countries.

"You can find most of the numbers on the internet, some of them are from professional organizations, and some of them became known as the result of intelligence leaks. You just have to search," Fischer explained.

"We have a lot of them, including for the Canadian Security Intelligence Service, NSA, CIA, FBI, BND (Germany's federal intelligence service), and the BfV (Germany's domestic intelligence service). There are also Italian and French intelligence services. We are also constantly searching for people who might be able to find new numbers so that we can bring 'Call a Spy' to different countries," Fischer said.

The group was motivated by a desire to show that "these agents are also people, and not characters in a Hollywood film who sit in dark rooms and control everything."

"At the end of the day, these people are given tasks by our government, they are supposed to protect us and not spy on us."

"The conversations vary from short prank calls to very serious talks about moral questions, work or the intelligence agent's personal view on a particular issue. These people usually consider themselves to be great patriots who carry out their work with conviction. Of course, they have something to say and the media today criticizes them a lot. We also have something to say but there is always the problem of how to ask the question and build a bridge so that that person will talk to you. It's not easy, but it's realistic," the artist explained.

Peng! has developed three different ways of calling a spy. The first is a phone booth, the second is a call center which provides people with training about how to best communicate with the spies, and the third is a live show in which contestants compete to see who can communicate best with their spy.

Fischer said that the reaction of the spies is particularly interesting, given their training. "Of course, these people aren't used to being called on these numbers. However, they have had special training and it is quite exciting to observe how they react, how suspicious they are, what questions they ask, how they automatically start digging for information and how they professionally avoid answering questions."

While some spies reacted positively to calls, some intelligence agencies were less enthusiastic, and Fischer suspects some agents have decided to take further action.

"There have been some different (counter) measures. It happened that our connection with the UK just stopped working. We have had some different technical problems associated with testing the connection. We can't be sure, but there were also some suspicious activities. We are always trying to find more technical solutions, but today it is working," he said.

New York Times
House Intelligence Committee Urges Obama Not to Grant Snowden Pardon
Friday, 16 September 2016
Byline: Charlie Savage

Washington - Lawmakers on the House Intelligence Committee unanimously signed a letter to President Obama on Thursday asking him not to pardon Edward J. Snowden, the former intelligence contractor who leaked troves of information about National Security Agency surveillance and data collection in 2013.
"We urge you not to pardon Edward Snowden, who perpetrated the largest and most damaging public disclosure of classified information in our nation's history," the bipartisan letter said. "If Mr. Snowden returns from Russia, where he fled in 2013, the U.S. government must hold him accountable for his actions."

The committee also said it had completed a 36-page report summarizing the results of its multiyear investigation into the leaks and their effect. The report was classified, but the panel released a three-page executive summary that portrayed Mr. Snowden as a "serial exaggerator and fabricator" who is "not a whistle- blower."

"Snowden caused tremendous damage to national security, and the vast majority of the documents he stole have nothing to do with programs impacting individual privacy interests -- they instead pertain to military, defense and intelligence programs of great interest to America's adversaries," the report said.

The release of the letter and the report coincides with the opening this week of the movie "Snowden," in which the director Oliver Stone portrays Mr. Snowden as a hero, and a new campaign by human rights groups urging Mr. Obama to pardon him before leaving office.

A pardon by the president appears to be unlikely. In late July, the administration responded to an earlier petition campaign by rejecting the idea and saying that Mr. Snowden should return to the United States to face trial.

But in effect, the intelligence committee and Mr. Snowden's supporters are using the idea of a presidential pardon to frame a public- relations duel over whether history should view him as a whistle-blower or a traitor.

Ben Wizner, an American Civil Liberties Union lawyer representing Mr. Snowden, criticized the House report. He noted that it states as a fact -- without supporting documentation -- claims such as that Mr. Snowden took 1.5 million documents from the N.S.A. It has been widely reported that the N.S.A. cannot determine what data he copied, and that it based its estimate on the number of documents to which he gained access.

Calling the 1.5 million figure "wildly inflated," Mr. Wizner said that "if they are as loose as that with other facts in their report, there is nothing here of value."

While Mr. Snowden has said he did not take any of the classified files with him to Russia, the report quotes a lawmaker on a security committee in Russia's Parliament as saying that "Snowden did share intelligence." That allegation appears to come from an NPR interview, and Mr. Wizner rejected it as "totally uncorroborated," saying the lawmaker was "not in the loop."

The report's executive summary also accused Mr. Snowden of claiming that he had left Army basic training earlier in his career because of broken legs, as The Guardian reported when Mr. Snowden first came forward, "when in fact he washed out because of shin splints." Mr. Wizner said that Mr. Snowden has actually said the problem was "stress fractures."

And the report criticizes Mr. Snowden for sometimes citing as part of his motivation for the leaks testimony in March 2013 by James R. Clapper Jr., the director of national intelligence, in which Mr. Clapper falsely said that the N.S.A. did not collect records about millions of Americans. But Mr. Snowden had already begun copying classified files many months before that congressional hearing, it noted.

In June 2013, The Guardian and The Washington Post began publishing reports that revealed highly classified N.S.A. surveillance and data collection activities, starting with the existence of the bulk phone records program. Soon after, Mr. Snowden came forward and identified himself as the source of the leaks.

At the time, he was in Hong Kong. He later tried to travel to Latin America via Moscow and Cuba, but the State Department revoked his passport, stranding him in Russia.

In the ensuing debate over surveillance, leaders of intelligence oversight committees -- particularly in the House -- were some of the most outspoken defenders of the programs he had disclosed and some of his harshest critics.

In particular, the chairman of the House panel at the time that it opened the investigation, Representative Mike Rogers, Republican of Michigan, who is no longer in Congress, repeatedly insinuated that Mr. Snowden was a spy for Russia. But executive branch officials have said that they have never found evidence that he had been working with or for anyone else.

London Times
Fears over rise of Chinese CCTV
Friday, 16 September 2016
Byline: Alexi Mostrous, Billy Kember

London - China's investment in Britain came under fresh scrutiny last night after Beijing was revealed to be the country's biggest provider of surveillance equipment.
Hikvision, a company controlled by the Chinese government, has sold more than a million closed-circuit television cameras and recorders to British clients who have installed them at sites including airports, government buildings, sports stadiums and the London Underground.

Former MI6 officers and security ministers called for greater oversight of Chinese business after an investigation revealed that no national security assessment had been made of Hikvision's British operations. Some suggest that the cameras could be hacked from Beijing.

Senior figures at GCHQ are understood to be concerned that the government lacks a policy to assess the security risk of foreign investments. Nigel Inkster, former director of operations and intelligence at MI6, said: "There are questions to be asked [on Hikvision]. It's far from evident that they have been."

The disclosure comes after Theresa May yesterday approved the £18 billion Hinkley Point nuclear power plant, which will be part-financed by China. The deal paves the way for Beijing to build its own nuclear reactor in Bradwell on Sea, Essex. The Times revealed last month that China had become the largest crude oil operator in the North Sea in what one expert described as an exercise in "soft power".

The government said yesterday that it would introduce "significant new safeguards" on future foreign investment in nuclear power and critical infrastructure. Downing Street said that it would take a "special share" in future nuclear projects, enabling it to block changes of ownership on national security grounds. However, such reforms would be unlikely to apply to state-run companies such as Hikvision, which sell technology rather than invest in assets.

Many of Hikvision's cameras can automatically recognise car numberplates, track moving vehicles or use thermal imagery to see at night. Most are capable of being connected to the internet.

"If you've got cameras that are IP [internet-link] enabled, or potentially could covertly be so enabled . . . they could potentially be used for malign purposes," Mr Inkster said. "I can think of a hypothetical case of a Chinese [dissident] making his way to a police station seeking protection of asylum. It doesn't require a Nobel prize-winning intellect to work out what the possible implications of that could be. I think there are questions to be asked. It's far from evident that they have been."

Chinese companies have been accused of installing "back doors" in products, allowing them to spy on western companies. The United States has banned Huawei, the Chinese telecoms company, from entering the market on security grounds. Huawei has denied working for the Chinese government.

Hikvision grew out of China's military surveillance wing and several high-ranking executives continue to hold positions in the Communist Party. By offering significantly lower prices than its rivals it has captured 14 per cent of the British video surveillance market in only four years, according to the analysts IHS Markit.

By the end of the year 1.27 million Hikvision cameras will be in Britain, with nearly a quarter used to monitor public sector buildings. One distributor said that Hikvision was "aware that their cameras are in use by [the British] government" although this could not be confirmed.

Sir Malcolm Rifkind, the former foreign secretary, said that the government and western allies needed to carry out a "much more comprehensive assessment as to what is the line we will not cross with regard to giving China access to our infrastructure".

Sites with Hikvision cameras include Stanstead and Glasgow airports, the boroughs of Hammersmith & Fulham and Salford, Ely and Folkestone town centres, Burnley football club, Teesport sea port in Middlesbrough, Preston bus station and Legoland in Windsor. Public bodies do not normally disclose who makes their CCTV cameras.

Spokesmen for Salford council and London Underground said that their systems were not internet enabled and were installed on a secure network. A spokeswoman for Hammersmith & Fulham council said it had no concerns about security although its CCTV network could be connected to the internet to share information with the police. Experts said that disconnecting cameras lowered the risk although they warned that networks claiming to be "closed" often connected to the web through a weak point.

The Chinese state holds a controlling 42 per cent stake in Hikvision, with the remainder divided up between smaller private shareholders in Hong Kong and China. Hikvision says that the company is run independently. Hikvision declined to comment.

Council on Foreign Relations
Shouting at Americans: A Peek Into French Signals Intelligence
Friday, 16 September 2016
Byline: Alex Grigsby

Comment: Something remarkable happened a few months ago. Bernard Barbier, the former head of signals intelligence (SIGINT) between 2006 and 2014 at France's foreign intelligence agency (DGSE), gave a speech at one of France's top engineering schools in which he reflected on his career and imparted some of his wisdom to students. He also said some things that he probably shouldn't have, like confirming that France was behind the Animal Farm advanced persistent threat, commenting on the SIGINT capabilities of European allies, and reacting to the revelation that the U.S. National Security Agency (NSA) had compromised the networks of the French presidency.
Last week, Barbier's speech surfaced on YouTube but was quickly taken down (UPDATE: A new version of the video is up here. H/T Boing Boing). However, it was up long enough for French daily Le Monde to transcribe some of the highlights. Here they are, paraphrased and translated from the original French.

1. "I got the order from Mr. Sarkozy's successor [current President Hollande] to shout at the Americans ... it was a great moment in my professional career"

Barbier recalls that he was first informed of a possible compromise at the Élysée palace in 2012, when a former colleague working IT security at the palace reached out for analysis on a piece of malware. With the help of a new metadata capability the French obtained in 2012 and Edward Snowden's revelation of the NSA's QUANTUM capability in 2013, Barbier's staff concluded that the attack on the Élysée was the work of the United States. Barbier recalls:

I received the order from Mr. Sarkozy's successor to go to shout at the Americans. It was on April 12, 2013 and it was really a great moment in my professional career. We were convinced it was them. At the end of the meeting, Keith Alexander [director of the NSA from 2005 to 2014] was not happy. While we were in the bus, he told me he was disappointed because he never thought they would have been caught. He added: "You are pretty good." As allies, we didn't spy on them. The fact that the Americans broke this rule took us by surprise.

2. "And yes, it was a Frenchman"

In 2014, Le Monde published documents from the Snowden archive revealing that Canada's SIGINT agency, the Communications Security Establishment (CSE), suspected that Paris was behind a cyber espionage campaign that began in 2009 targeting Iran's nuclear program but also targeting computers in Canada. CSE was able to attribute the campaign to the French based on some reverse engineering revealing that the malware developer used references to a French children's cartoon character, Babar the Elephant. That reference also led Kaspersky to baptise the malware Animal Farm. Barbier recalls that CSE "concluded that he [the malware author] was French. And yes, it was a Frenchman."

3. The pipe dream of united European intelligence agency and the possibility of merging French and German intelligence.

In one of the more surprising aspects of Barbier's speech, he mused about the possibility of creating a European intelligence agency but quickly dismissed the notion, noting that only a fusion of French and German intelligence agencies would be feasible.

It is impossible to build a single European intelligence agency with twenty-eight countries that don't have the same capabilities or the same culture. The best, by population size, are the Swedes. The Italians are bad. The Spanish are a bit better, but don't have the capabilities. And the Brits, with 6,500 staff at GCHQ [Government Communications Headquarters, the UK SIGINT agency] are very good, but are they European? And France has the strongest technical capabilities for intelligence collection in continental Europe.

That leaves the Germans, who are solid partners. I've worked a lot with them, sometimes transmitting our knowhow and bringing them some technical capability. German and French engineers work very well together. In contrast, a British engineer with a French engineer is complicated.

To be more effective, I told French politicians that we had to merge the BND [the German foreign intelligence agency] and the DGSE. It's the only solution. It would be a an agency with 15,000 staff. The NSA has 60,000 people, and the SIGINT section of the DGSE is 3,000 agents. But the French politicians never followed up.

Merging the BND and the DGSE would have made for some awkward conversations given that last year, news reports revealed that the BND had been spying on France.

4. Snowden is a traitor that "rather helped us"

Finally, Barbier gives his opinion on Edward Snowden, presumably in response to a question from the audience.

For me, Snowden is a traitor to his country, but he has nothing to do with Julian Assange. The Americans made Snowden, who was an external contractor, a systems administrator. Those who do that job in the DGSE are bureaucrats that have between fifteen and twenty years of seniority. The possibility of having a Snowden in France is very low. Snowden showed that espionage between allies existed and that Americans compromised hardware, such as that sold by Cisco and poses a problem for technological independence. In that sense, Snowden rather helped us. (Note: Alex Grigsby is the assistant director for the Digital and Cyberspace Policy program at the Council on Foreign Relations.)

Washington Post
House Intelligence Committee urges no pardon for Edward Snowden
Friday, 16 September 2016
Byline: Ellen Nakashima

Washington - The House Intelligence Committee on Thursday sent a bipartisan letter to President Obama urging him not to pardon Edward Snowden, asserting that the former National Security Agency contractor carried out "the largest and most damaging" leak of classified information in U.S. history. The letter emerged on the same day that the panel unanimously voted to adopt a classified report on Snowden that, according to a three-page unclassified summary, portrays him as a disgruntled employee whose leak caused "tremendous damage to national security."

Snowden, 33, gave large numbers of sensitive files to journalists in 2013, an action he said he took out of concern that government surveillance programs were operating in violation of the U.S. Constitution. He said the public had a right to be informed of the programs so it could engage in debate about the proper scope of such surveillance.

On Wednesday, a coalition of human rights groups launched a campaign to urge Obama to pardon Snowden before he leaves office. Snowden was charged in June 2013 with espionage and felony theft of government property. And the letter comes on the eve of the release of an Oliver Stone movie that portrays Snowden sympathetically.

He is living in Russia under a grant of political asylum.

The intelligence panel rejected arguments that Snowden acted out of conscience and insisted that he should be held accountable for his actions. In their letter, the lawmakers reminded Obama that he had said in a news conference in 2013, "I don't think Mr. Snowden was a patriot."

"In short," they wrote, "we agree with you. Mr. Snowden is not a patriot. He is not a whistleblower. He is a criminal."

The lawmakers faulted Snowden for leaking material rather than reporting his concerns about surveillance overreach to oversight officials, such as the committee or inspector general. They said he began his massive download two weeks after a spat with a supervisor.

The vast majority of the documents he leaked had nothing to do with programs that affected privacy and civil liberties, they said, but pertained to military and intelligence programs "of great interest to America's enemies."

They said that Snowden failed basic annual training for NSA employees on a key provision of the Foreign Intelligence Surveillance Act, which included explanations of the privacy protections related to PRISM -- another program whose details were revealed as a result of Snowden's leaks.

Ben Wizner, an American Civil Liberties Union lawyer who represents Snowden, slammed the committee's letter and report summary. "There's no there there," Wizner said.

"They've been using the same rhetoric about damage to national security for three and a half years and have produced absolutely no evidence of concrete harm," he said. "If they had any evidence that any individual had come to harm, that would have been on the front pages of the newspapers."

The first document to emerge from the leaks revealed a secret program of bulk collection of data on Americans' phone calls. That program had been launched by President George W. Bush and retained by Obama. It had been operating with the approval of a federal court that oversees classified surveillance programs. And the intelligence committees, as well as some lawmakers on other committees, had been briefed on it.

"There is no oversight body that a whistleblower can go to when a program has been comprehensively approved by all three branches of government," Wizner said. "The only avenue is to find a way to bring the public into the conversation, which [Snowden] did by releasing information to journalists."

The committee asserted that Snowden "stole 1.5 million sensitive documents." But senior intelligence officials have couched it as "probably downloaded," cautioning that they do not know for sure how many he took.

The committee's classified report is 36 pages, with 230 footnotes, but must remain secret "to avoid causing further harm to national security," the summary stated.

Washington Times
Edward Snowden characterized as 'serial exaggerator' in House intelligence committee report
Friday, 16 September 2016
Byline: Andrea Noble

Washington - A House intelligence committee report on Edward Snowden characterizes the former National Security Agency contractor not as a whistleblower but as a "serial exaggerator" whose theft of 1.5 million classified government documents has done tremendous damage to national security.
A 4-page summary of the classified report released by the House committee on Thursday says the bulk of the documents taken "have nothing to do with programs impacting individual privacy interests" but rather pertain to military, defense and intelligence programs.

"A review of the materials Snowden compromised makes clear that he handed over secrets that protect American troops overseas and secrets that provide vital defenses against terrorists and nation-states," the report states. "Some of Snowden's disclosures exacerbated and accelerated existing trends that diminished the IC's capabilities to collect against legitimate foreign intelligence targets, while others resulted in the loss of intelligence streams that had saved American lives."

The report, two years in the making, was released a day after supporters of Mr. Snowden launched a formal campaign to request that President Obama grant him a pardon and just ahead of the release of Oliver Stone's theatrical film about Mr. Snowden.

The documents leaked by Mr. Snowden in 2013 revealed the U.S. government's global surveillance capabilities, which triggered public outcry and ultimately led to reform of the programs. The 33-year-old computer technician went into hiding as the reports about the telephone record surveillance programs were published. Prosecutors later charged him with theft of government property and espionage, but Mr. Snowden has avoided prosecution by taking asylum in Russia.

While Mr. Snowden has characterized himself as a whistleblower for revealing the surveillance programs, lawmakers on Thursday referred to him a disgruntled employee who argued with his supervisors and had been reprimanded just two weeks before he began illegally downloading classified documents.

"Edward Snowden is no hero - he's a traitor who willfully betrayed his colleagues and his country. He put our servicemembers and the American people at risk after perceived slights by his superiors," said Intelligence Committee Chairman Devin Nunes. "In light of his long list of exaggerations and outright fabrications detailed in this report, no one should take him at his word."

However, Mr. Snowden's supporters, including civil and privacy rights advocates, say his actions brought about awareness of secret government activities and should be applauded, not criminalized.

In addition to its conclusions about Mr. Snowden and the documents taken, the report summary also notes concern about the NSA's ability to prevent a breach of such magnitude in the future.

The report states that the NSA and the intelligence community "have not done enough to minimize the risk of another massive unauthorized disclosure. Although it is impossible to reduce the chance of

another Snowden to zero, more work can and should be done to improve the security of the people and computer networks that keep America's most closely held secrets."

The full report, which is 36 pages long, is classified. The summary report indicates that to write the report, the committee interviewed key individuals who had reviewed interviews with Mr. Snowden's coworkers and supervisors but that they did not speak with anyone directly who could be called as a witness in the criminal case against Mr. Snowden if he is eventually brought to trial.

Sputnik (Russia)
WikiLeaks' Assange Offers to Go to Prison in Exchange for Chelsea Manning Pardon
Thursday, 15 September 2016
Byline: Staff report

Washington - On Thursday morning WikiLeaks publisher Julian Assange tweeted that if US President Barack Obama would grant clemency to imprisoned whistleblower Chelsea Manning, Assange would turn himself over to the US government for imprisonment, "despite its clear unlawfulness."
In the tweet, WikiLeaks included a letter from their lawyer addressed to US Attorney General Loretta Lynch, detailing why the "Clinton precedent" requires closing the Department of Justice (DOJ) case against the publisher. "If Obama grants Manning clemency, Assange will agree to US prison in exchange -- despite its clear unlawfulness," the proposal read, linking to a previous tweet containing the letter.

The letter, from WikiLeaks attorney Barry Pollack, explained that on November 29, 2010, the DOJ announced an investigation into potential crimes committed by Assange and WikiLeaks, and that in March of this year it was confirmed that the investigation "continues to this day."

The investigation stems from the thousands of classified Army documents provided by Manning to the website, including diplomatic cables and airstrike videos, which later became known as the Afghan War Diaries. Manning is currently serving a 35-year prison sentence at Fort Leavenworth for revealing the extent of the US military's criminal actions.

"As Mr. Assange's criminal defense counsel in the United States, I have repeatedly sought information from the Department of Justice regarding this now nearly-six-year-old investigation," Pollack writes. "Despite the fact that the Department has continually publicly confirmed through court filings and statements to the press that it is conducting an on-going criminal investigation of Mr. Assange, the Department has provided me no substantive information whatsoever about the status of the investigation."

Pollack asserts that two developments during the pendency of the investigation led him to write and ask for a public announcement that the case is closed with no criminal charges filed.

The first development points to the Attorney General's revision of the DOJ regulations with respect to obtaining evidence from and charging members of the press in January 2015. "The Department's policy is intended to provide protection to members of the news media from certain law enforcement tools, whether criminal or civil, that might unreasonably impair newsgathering," the policy revision reads. "No member of the Department shall present information to a grand jury seeking a bill of indictment, or file an information, against a member of the news media for any offense which he or she is suspected of having committed in the course of, or arising out of, newsgathering activities without first providing notice to the Director of the Office of Public Affairs and obtaining express authorization of the Attorney General," it states. Pollack argues that the investigation against Assange is clearly based on his newsgathering activities, and that WikiLeaks had published the information because they believed it was newsworthy. The lawyer argues that the extensive coverage of the published documents by third party media outlets affirms the assertion of newsworthiness. The second development indicates that the investigation should be dropped due to a lack of charges against Democratic presidential nominee Hillary Clinton. He notes that FBI Director James Comey based his recommendation of no charges for Clinton on his belief that there was no criminal intent. "In his statement, and in subsequent testimony before Congress, Director Comey made it clear his conclusion was based on the necessity of proving criminal intent. Director Comey noted that responsible prosecutors consider the context of a person's actions," Pollack wrote. "Criminal prosecution is appropriate only when a person was knowingly violating the law and was intending to aid enemies of the United States or was attempting to obstruct justice."

Pollack argues that WikiLeaks' intent was lawful, as it was not intended to aid enemies of the United States or to obstruct justice; it was simply to publish material that was, and remains to this day, of urgent public interest.

"Manning disclosed the materials because, under the circumstances, she thought it was the right thing to do," Manning's attorneys state, in an appeal brief filed in May. "She believed the public had a right to know about the toll of the wars in Iraq and Afghanistan, the loss of life, and the extent to which the government sought to hide embarrassing information of its wrongdoing." Many have long believed that Manning's disclosures contributed significantly to bringing about an official end to the war in Iraq. Assange has been residing in the Ecuadorian Embassy in London out of fear of prosecution by the US government since 2012. In February, the UN Working Group on Arbitrary Detention (WGAD), ruled that Assange's four-year stay in the embassy was considered "arbitrary detention," as he had not been allowed to leave the building without the threat of arrest.

"For six years now, his rights have been severely violated, as have the rights of his children. WikiLeaks began its publication of US diplomatic cables on November 29, 2010, a week before Sweden and the UK arbitrarily imprisoned him," Assange's legal representatives said in a statement in August.

Assange has not been formally charged with any crime. In prison, Manning has just ended a hunger strike, after the Army finally agreed to allow her to receive gender- transition surgery. Following Manning's sentencing, it was announced that she would like to transition to a woman, but the prison

initially refused gender-affirming treatment. The lack of proper care culminated in a suicide attempt, after which she is now potentially facing further charges. If charged, she could be sentenced to finish her lengthy sentence in solitary confinement, or be reclassified to maximum security. "It is unnecessarily cruel to threaten Chelsea with additional punishment while in this very vulnerable state," a petition against the charges states. "The government is trying to silence her important voice--for good. Chelsea has been systematically mistreated by the US government since she was first taken into custody in 2010, including long stretches of extreme solitary confinement even before she had ever been convicted."

The Independent (UK)
Julian Assange: WikiLeaks founder could still be extradited as Swedish court upholds detention order
Friday, 16 September 2016
Byline: Samuel Osborne

London - A Swedish appeals court has upheld a detention order for WikiLeaks founder Julian Assange. Mr Assange is wanted by prosecutors in a rape investigation stemming from his visit to Sweden in 2010.

The decision made by the Svea Court of Appeal on Friday means the arrest warrant stands for the 45-year-old Australian, who has avoided extradition to Sweden by taking shelter in the Ecuadorian Embassy in London since 2012.

Mr Assange denies the rape allegation and has challenged the detention order several times.

It is unclear whether he will make an appeal against the decision to the Supreme Court.

Upholding a lower court ruling, the appeals court said Swedish prosecutors are actively trying to move the investigation forward and set up an interrogation of Mr Assange at the embassy.

Acting on behalf of Swedish investigators, an Ecuadorian prosecutor is set to question Mr Assange on 17 October.

"This means that there is at present no reason to set aside the detention order. Julian Assange's claim to that effect shall therefore be refused," the court said.

New York Times
Concern Over Hacked Emails Becomes a Fear of Being Next
Friday, 16 September 2016
Byline: Nicholas D. Shear, Nicholas Fandos

Washington - A panicked network anchor went home and deleted his entire personal Gmail account. A Democratic senator began rethinking the virtues of a flip phone. And a former national security official gave silent thanks that he is now living on the West Coast.
The digital queasiness has settled heavily on the nation's capital and its secretive political combatants this week as yet another victim, former Secretary of State Colin L. Powell, fell prey to the embarrassment of seeing his personal musings distributed on the internet and highlighted in news reports.

"There but for the grace of God go all of us," said Tommy Vietor, a former National Security Council spokesman for President Obama who now works in San Francisco. He said thinking about his own email exchanges in Washington made him cringe, even now.

"Sometimes we're snarky, sometimes we are rude," Mr. Vietor said, recalling a few such moments during his time at the White House. "The volume of hacking is a moment we all have to do a little soul searching."

The Powell hack, which may have been conducted by a group with ties to the Russian government, echoed the awkwardness of previous leaks of emails from Democratic National Committee officials and the C.I.A. director, John O. Brennan. The messages exposed this week revealed that Mr. Powell considered Donald J. Trump a "national disgrace," Hillary Clinton "greedy" and former Vice President Dick Cheney an "idiot."

The latest hack could well spur a new rash of email deletions across the country as millions of people scan their sent mail for anything compromising, humiliating or career-destroying. It adds to the sense that everyone is vulnerable.

The soul searching is happening with a special urgency in Washington, where email accounts burst with strategies, delicate political proposals, gossipy whispers and banal details of girlfriends, husbands, bank accounts and shopping lists.

A television news anchor said that producers and staff members at her network had jokingly agreed at a morning news meeting to issue blanket apologies to one another if their emails were ever made public.

She said Mr. Powell's emails had revealed him, a normally stoic public official, to be just as gossipy as everyone else, and added that the gossip, not classified information, was what people feared becoming public.

On Capitol Hill, Senator Richard J. Durbin of Illinois, the chamber's No. 2 Democrat, said the news of Mr. Powell's hacked emails had him thinking that Senator Chuck Schumer's never-ending use of an old-fashioned flip phone "makes more sense than ever."

"I think more and more people are realizing that there isn't a thing you can say in an email that isn't likely to be hackable or discoverable at some later point," Mr. Durbin said, lamenting his own complacency.

Senator Lindsey Graham, Republican of South Carolina, shrugged off the news. "I haven't worried about an email being hacked since I've never sent one," Mr. Graham said. "I'm, like, ahead of my time."

But for another network anchor in Washington, who declined to be named for fear of becoming an even more prominent hacking target, the Powell disclosures led to a long night Wednesday that involved saving a few personal emails and then deleting his entire account. Everyone, he said, has sent emails they would not want released, including innocent messages that could be misinterpreted.

Washington may be behind other big cities in learning that lesson. Bankers on Wall Street have favored very brief emails since their conversations were splashed across front pages because of lawsuits filed after the financial crisis. In 2010, Goldman Sachs executives used the acronym "LDL," for "let's discuss live," when a conversation turned at all sensitive.

Hank Paulson, a former Goldman Sachs chief executive, refuses to use email. Ben S. Bernanke, a former chairman of the Federal Reserve, once set up an email account under the pseudonym Edward Quince in the hopes of greater privacy.

Similar precautions have been common in Silicon Valley since a 2009 Chinese state cyberattack on servers at Google and other tech companies. In Hollywood, a breach at Sony Pictures in 2014 spilled out gossipy secrets and persuaded film crews, actors and executives alike to adopt security measures they once considered paranoid. Studios have turned to a new class of companies with names like WatchDox that wrap screenplays with encryption, passwords and monitoring systems that can track who has access to confidential files.

"It has, without question, affected what I say in writing," said Jordan Roberts, a writer and director whose credits include the coming comedic drama "Burn Your Maps." The Sony hack gave him "a personal pause button that hopefully spares me future potential embarrassment for the sake of a quick and pithy and frequently unfounded, and almost always unnecessary, insult," he said.

Joe Quenqua, who runs the entertainment practice at the DKC public relations firm, said by email that everyone thinks twice before shooting off an email. "Might it make for some more banal email exchanges? A bit less gossipy?" he wrote. "Sure, but it's so simple: Better safe than sorry."

Richard Gelfond, the chief executive of IMAX, said: "I used to be a little more tolerant of what others say in email. That ended."

In some countries outside the United States, there has long been a more cautious approach to electronic communications. In Pakistan, politicians often agree to speak to reporters in person only after removing

phone batteries or covering the microphones with a pillow. Many in the Middle East have migrated to more secure services like Telegram or Signal.

Many Americans have learned the hard way. Aaron E. Carroll, a pediatrician and research professor at Indiana University, discovered the dangers after writing a newspaper article defending artificial sweeteners that prompted health groups to demand his university emails. The groups hoped to prove links between Dr. Carroll and companies that make sugary drinks and snacks.

"It totally devastated me," Dr. Carroll said on Thursday. "I was freaking out, not because I did anything wrong -- all of a sudden, I was panicked about what have I said that was inappropriate or that could be taken out of context."

Dr. Carroll, who said he had no connection to any food companies, engaged in a "scorched earth" policy in the weeks after his emails were handed over to the health groups. He deleted just about everything off his university email account and now clears out the account regularly.

"I'm a little more careful now. I'll just walk down the hall instead of sending a long email," he said, though he added that he still sent personal and work messages on the same account for convenience. "It has not changed my daily habits of email as much as you might think."

That was also a sentiment on Capitol Hill, where some treated the prospect of a Powell-like hack lightly.

Senator Roy Blunt of Missouri said he was already a "late adopter" when it came to email because he never thought it was secure. He said he had been careful not to rely heavily on email when he was in charge of wrangling votes for Republicans in Congress.

"I think that a lot of people are now finding out why that should have been the case for lots of other people," Mr. Blunt said.

Mr. Durbin, asked if he was worried enough to scour through his sent mail, sighed and shook his head.

"Oh, no," he said. "The Russians will have to read it."

Globe and Mail
Bahrain using Canadian software to stifle dissent: report
Wednesday, 21 September 2016
Byline: Colin Freeze

Toronto - A new report from The Citizen Lab alleges that Canadian- made software is - once again - being used by a repressive Mideast state to keep its citizens from learning about news, religion and politics. The kingdom of Bahrain this summer starting using Web-filtering software from Netsweeper Inc. as a means of keeping a lid on dissent, the report said. It added that the Sunni-dominated monarchy is going so far as to use the software to deny Bahrain's majority Shia citizens access to basic information about their religion and religious leaders.

The Citizen Lab, a group of civil-minded technological researchers at the University of Toronto's Munk School of Global Affairs, last year released similar findings about Netsweeper software being used in Yemen, where religious strife has led to ongoing civil war. It has also previously documented the Ontario company's software being used in Pakistan and Somalia.

Typically Netsweeper sells its products to large firms which purchase it to keep computer viruses out of corporate networks or curb employees' access to porn and gambling sites.

Selling such software so that it can be used across an entire country can be controversial, however, especially if it ends up being tweaked to police morality and dissent. The Citizen Lab alleges this is what has happened in Bahrain, an island-nation monarchy strategically located between two much larger regional rivals, Iran and Saudi Arabia, which are now stoking sectarian tensions across the Middle East.

Ron Deibert, the director of The Citizen Lab, said that any Canadian company that sells information-scrubbing software in this backdrop risks raising the same kinds of questions as have surfaced in other ongoing corporate controversies. These include the question of whether Ottawa should be facilitating, or blocking, the Canadian armoured-vehicle companies that sell their wares to Saudi Arabia.

"I think the government has to develop some kind of guideline," said Mr. Deibert, adding that it could be simple enough for Canadian officials to put in place an array of measures, including export restrictions. "That would require Netsweeper, and other companies like them to apply for a licence to export their technology, that would have a checklist around due diligence for human rights. But, he added, "the rub of that would be they couldn't make a sale like this."

Bahrain had used Web- scrubbing software developed by an American company before it awarded Netsweeper a $1.2-million contract earlier this year.

The Citizen Lab report, financed with the help of the U.S.-based MacArthur Foundation, says its researchers confirmed the active use of Netsweeper software in Bahrain through Internet-scanning methods that looked for the company's telltale digital fingerprints.

"We confirm that Netsweeper technology is being used by at least one key [Internet service provider] ... to filter content, including critical political speech, news websites, human-rights content, websites of oppositional political groups and Shia-related content," the report reads.

In recent months, Bahrain has faced international condemnation for stripping a leading Shia cleric of his citizenship, for shutting down the country's largest political-opposition group and for arresting the founder of the Bahrain Centre for Human Rights. Access to websites relating to these groups and people have all recently been curbed in Bahrain, according to The Citizen Lab.

Ordinary Bahrainis have also had their access blocked to "websites on the Shia sect," "Iranian media outlets" and " content critical of Islam," according to the report.

The Globe and Mail called and e-mailed members of Netsweeper's management team on Tuesday but did not hear back.

New Straits Times
Kudos over setting up of cyber court
Wednesday, 21 September 2016
Byline: Ahmad Kushairi

Kuala Lumpur - The first cyber court in Malaysia officially began operations early this month. It's about time, too, as cybercrime has been growing at an unbelievable rate with each passing year as technology continues to evolve and play an important part in the lives of many.
Today, there are more than 13.5 million Internet users in the country, which is a staggering number of people who can be potentially exposed to cybercrime.

The CyberSecurity Malaysia agency had stated that there was no comprehensive definition of cybercrime, but for now, it could be categorised into three.

The first focuses on information and communications technology (ICT) systems and virtual properties that become the target of exploitation, infringement, and identity and information theft.

The second comprises ICT devices used to commit crimes in the virtual space, such as personal computers that are used to carry out acts of stealing money, information and identities in other computers.

The final category is where ICT devices are used as a medium to commit cybercrime. Using your personal ICT devices, such as computers and tablets, for slandering, sedition or instigating at a higher scale falls into this category.

CyberSecurity Malaysia reported that it received 3,752 cases of online fraud and intrusion this year, as well as a shocking 191,096 cases of botnet and malware viruses. Some 30 Malaysians have fallen prey to cybercrime daily, with fraud and intrusion cases taking the highest spot.

With that said, the setting up of the nation's first cyber court, located in the Duta Courts complex, is timely. The cyber court deals with cybercrime, such as hacking, bank fraud, spying, web defacement, identity and information theft, online gambling and online pornography.

Things are not like what they used to be after technology came into the picture. As technology continues to evolve, so does cybercrime. Many predators seek out the virtual world every day in the hopes of carrying out online crimes, thinking that there are no laws in the virtual space and they are free to do as they like.

There is no better time than now to take action, and the setting up of the cyber court is a positive move towards protecting Malaysians from the various forms of online menace.

Our cyberspace needs to be put in order. Regulating cybercrime would force online predators and those with bad intentions to think twice before carrying out their actions, as they now risk the possibility of getting caught and punished.

It was reported recently that more than 2,100 servers had been compromised. Precious and personal information is allegedly sold on an underground cybercrime shopping website called xDedic.

Imagine your banking details, those on properties and assets, and identification and passport details being made available to just about anyone. That's enough to send one into a frenzied state, as such information may be used by greedy cybercriminals. One stands to lose everything if his or her personal data is exposed.

One of the most common cases of cybercrime in the country, as reported by CyberSecurity Malaysia, is victims being targeted via social networking sites. Scammers hide behind an attractive female profile, lure potential lonely victims into chats and slowly gain their trust. Once this is achieved, they ask the victims to commit indecent acts via video chats and, then, proceed to blackmail the victims with the threat of exposing the videos online.

This is known as cyber blackmail, and it is growing exponentially across the globe. Of course, there are also other forms of cybercrime, such as extortion, bullying and shopping scams, which need to be addressed accordingly.

The setting up of the cyber court is, therefore, a positive move to enable the authorities to use cyberlaws in dealing with the increasing number of cybercrime cases more effectively. It sends out the message to criminals that they can no longer roam cyberspace as freely as before, as the long arm of the law is out to nab them. This, over time, will help Malaysians feel more secure and safe in cyberspace.

As Malaysia joins other countries, like the United States and those in Europe, in establishing its own cyber court and the subsequent use of cyberlaws, it is sending out positive vibes that it is keeping up with its duty as a responsible government to protect its people in cyberspace.

Just like the real world, the virtual world also needs law and order. It should be a safe haven where all can work, live and play.

Jakarta Post
Indonesia sees drastic increase in cyber crime
Wednesday, 21 September 2016
Byline: Ayomi Amindoni

Jakarta - President Joko "Jokowi" Widodo said on Tuesday that Indonesia had seen a drastic increase in cyber crime, with the number of cases growing by 389 per cent in 2014 to 2015. Most of the cases occurred in the e-commerce sector, he added.
Speaking during a limited Cabinet meeting at the State Palace, Jokowi said cyber threats posed new challenges regarding the readiness of government institutions.

"To deal with cybersecurity issues, we do not need to form a new institution, or start from zero. We can expand or consolidate units at ministries or institutions that have cyber security functions," he said.

The Office of the Coordinating Political, Legal and Security Affairs Minister revealed in July that cyberattacks in Indonesia rose by 33 per cent in 2015 from the previous year, of which 54.5 per cent were aimed at e-commerce-related websites. Most of the attacks caused systems to stop working.

In the meeting, the President also told his Cabinet members to improve the management of state officials amid an era of tighter competition. He said improved management could provide more professional, responsive and faster services.

"State official management reforms should be carried out thoroughly, from upstream to downstream," he said.

It World Canada
Prepare for threat of quantum computing to encrypted data, Canadian conference told
Wednesday, 21 September 2016
Byline: Howard Solomon

The race to create new cryptographic standards before super-fast quantum computers are built that can rip apart data protected by existing encryption methods isn't going fast enough, two senior Canadian officials have warned a security conference.
"I think we are already behind," Scott Jones, deputy chief of IT security at the Communications Security Establishment (CSE), responsible for securing federal information systems, told the fourth annual international workshop on quantum-safe cryptography in Toronto on Monday.

Quantum computing - or more accurately, computers that use quantum mechanics - is not a dream, Jones and others told the conference of business executives, crypto academics, IT companies and government officials. One prediction is there's a one in seven chance that by 2026 a quantum computer will exist that can break RSA-2048 encryption. It may take longer -- or, if there's an advance, shorter.

"Quantum represents a fundamental change and challenge to encryption for all of us," Jones said, noting that encrypted transactions are the backbone of security and trust on the Internet.

His comments were backed by David Sabourin, CSE's manager of cryptographic security, who said that if the 2026 prediction is right "we're in trouble." Speaking on a panel of government experts, Sabourin noted the U.S.-based National Institute of Standards and Technology (NIST) will close its call for proposed new and more quantum-secure public key encryption algorithms next year. Then it will take a couple of years of review, which means products that can use new crypto standards might be released in 2025 - and then start to be implemented around the world. So 2026 will be "messy," he concludes, with organizations rushing to install new solutions.

(For a more detailed look at post-quantum cryptography, see this NIST report)

However, Sabourin, Jones and others said chief information and risk officers can take steps today to start to mitigate the risk. That includes evaluating all organizational data to decide what could be at the greatest risk if encryption is broken and be ready to deploy what will hopefully be quantum-resistant solutions when they are approved. One possible interim solution is using symmetric key encryption rather than public key encryption solutions, Jones said. But it's expensive and likely could only be used for the most sensitive data.

There's no need to panic, Sabourin stressed, pointing out that the challenge of quantum computing has been known for some time and that governments, the computing industry and standards organizations (like NIST) have been working on it for some time. And, he noted, the first target of people who have quantum computers will probably be sensitive government information, not not go after corporate or banking data.

CSE is the lead federal agency working on quantum-safe computing solutions for the government.

Briefly, quantum computers take the theory of quantum mechanics to change the world of traditional computation of bits represented by zeros and ones. Instead, a bit can be a zero OR a one. Again, briefly, quantum computing means information could be stored and manipulated at the sub-atomic level.

Quantum offers the potential of huge speed gains in computing that could bring both benefits to science and medicine as well as threaten IT security. The problem quantum computing raises is to data secured with today's encryption that has to last years if not decades - for example, personal medical information, data required to be held for years by regulations or a any database held by a country's intelligence services. Merely using a solution with a longer encryption key won't defeat a quantum computer, at least for public key algorithms. The problem expands as organizations store more data in the cloud, where they may have to rely on the security of a provider. But quantum computers don't exist yet, so no one is sure products based on new crypto standards could withstand attack.

A number of countries and IT companies around the world are sponsoring research into building a quantum computer, including Canada. The European Union has set aside $1 billion.

Monday's session was aimed mainly at leaders of companies and government. Sessions today and Wednesday will see more technical proposals discussed on creating standards to meet the problem.

In an interview Jones said CSOs today have ask what information they have that is at risk. "If I take the worst case scenario] a quantum system that can break encryption in 10 years], is there information I am holding that I'm responsible for protecting? Then, what steps do I need to take to protect that. It's the same quesiton around general cyber security," he added.

Some governments are already taking action. For example, the conference heard, Germany requires satellites regulated by the country to be able to be reconfigured for quantum-secure solutions.

The conference is organized by the European Telecommunications Standards Institute (ETSI) and the University of Waterloo's Institute for Quantum Computing.

"This is not a just a nuisance for technical people or mathematicians," Michele Mosca, the IQC's co-founder and deputy director told the conference "This is going to seriously compromise the security and integrity of our information assets and core business functions. The business functions you and your customers rely on won't work - and its not a matter of patching it up in a couple of days."

There are two ways of mitigating the threat, he said: Deploying conventional quantum-safe cryptography (also called quantum resistant algorithms or post-quantum cryptography), which includes hash-based and lattice-based and symmetric key cryptography solutions; and the yet-t0-be built quantum cryptography, which uses the properties of quantum mechanics to establish keys that cannot be broken.

To help risk officers Mosca's reduced the problem to a mathematical equation, where x is the shelf life of current information, y is the number of years it would take to retool the organization's existing infrastructure with large scale quantum-safe solution, and z the number of years it will take for a large scale quantum computer to be built.

If x+y is greater that z, the organization has a problem and has to act, he said.

He also added that the threat is serious enough to predict that in the next six to 24 months organizations will be differentiated by whether they have a well-articulated quantum risk management strategy.

Governments and academics aren't working alone on the problem. So are companies as big as Cisco Systems, Microsoft and Intel, who had representatives on a panel. All said one reason is they need to ensure their companies are able to deliver secure software updates in the future.

It doesn't matter how far away a quantum computer is, said Brian LaMacchia, director of Microsoft Research's security and cryptography group - it's coming. Even if a quantum computer isn't built, he added, the solutions being worked on will help strengthen IT security.

David McGrew, a fellow in Cisco's advanced security research group, said one way CIO can be ready is ensuring it's organization has an agile infrastructure ready to adopt new encryption solutions.

ars Technica (UK)
Encrypted messaging apps need backdoors, says top Dutch spook
Wednesday, 21 September 2016
Byline: Jennifer Baker

London - Backdoor access to encrypted communications has been demanded by Netherlands' spy chief Rob Bertholee--a view that differs from the government's official position.
In an interview with local daily De Volkskrant at the weekend, Bertholee--head of the General Intelligence and Security Service of the Netherlands (AIVD)--said that terrorists are using encrypted chat applications such as Telegram, WhatsApp, and Signal, and argued that those services made it extremely difficult for authorities to prevent terrorist attacks.

At the beginning of the year, the Dutch government adopted a strong stance against "any restriction in the development, availability, or use of cryptography" in an official paper. It said that weakening encryption products with backdoors for law enforcement would leave systems vulnerable to criminals, terrorists, and foreign intelligence services.

However, Bertholee said he wants to have access to "the communications of those who pose a threat."

"Will people who value privacy over anything else continue to pursue their goal with the same enthusiasm after they have fallen victim to a terrorist attack? You should ask yourself how much security you are prepared to sacrifice for privacy," he said.

Dutch digital rights organisation Bits of Freedom said Bertholee was creating a "false dichotomy between privacy and security." It added:

Bertholee said that protection of privacy was "very important," added he wasn't interested in a "dragnet," then took a swipe at the current government position, and referenced Apple's refusal to unlock the San Bernardino shooter's iPhone for the FBI: "In that case the Dutch government should also accept the fact that we are no longer able to access communications of terrorists--and Apple. Should helping terrorists communicate securely be one of Apple's aims?"

Last month, France's interior minister, Bernard Cazeneuve, called for EU-level "action" on encrypted messaging apps.

The Daily Beast
Cellphone Bombs: The New American Terror
Tuesday, 20 September 2016
Byline: David Axe

Washington - Ahmad Khan Rahami the 28-year-old suspect in the twin bombings in New York City and New Jersey that injured dozens of people this weekend, apparently used cellphones to detonate his homemade bombs.
That should worry authorities. It's not hard to convert a cellphone into a remote trigger for an improvised explosive device. But it is hard--and illegal in most cases--to jam cell signals without inflicting extensive collateral damage that could be even worse than the harm a small IED might cause.

"Jamming technology generally does not discriminate between desirable and undesirable communications" is how the Federal Communications Commission put it in a fact sheet (PDF). "Use of cell phone jammers poses an unacceptable risk to public safety."

Cellphones are basically just small, sophisticated radios. They convert a radio signal into an electrical current and then process that current into sound. Incorporated into a bomb, a cellphone's electrical current is enough to jolt a small detonator charge, which in turn can set off the main explosive.

Modifying a cellphone into a trigger is so easy that some DIYers rig up old phones to set off fireworks. All it takes is a phone, five bucks worth of parts, and a few minutes of tinkering--plus, for first-timers, any one of scores of easy-to-follow internet tutorials.

Working the trigger is equally simple. Just get a safe distance away from your bomb and dial the number of the phone attached to the detonator. Boom.

In theory, it's a fairly straightforward process to jam a cell signal and thus prevent a bomb from exploding. Cellular jammers-- you can illegally buy them online for a few hundred dollars--work by flooding radio channels with jibberish signals, essentially crowding out the particular signal a cellphone is looking for.

But cellular jammers--any radio jammers, really--are fairly indiscriminate. Try to jam one phone or a few phones and, in practice, you'll end up wiping out communications across a wide area, potentially causing greater insecurity than you're preventing by blocking a bomb detonation.

To be sure, cellphone jamming in a small or fixed area can be useful. Many prisons jam incoming signals. The U.S. Secret Service reportedly possesses jammers that accompany presidential motorcades.

The U.S. military equips many of its armored vehicles with radio jammers, creating an electronic bubble in which many remotely triggered bombs won't detonate. More powerful airborne military jammers can sweep away signals underneath the emitting aircraft.

But jamming cellular signals across a wider area can be highly problematic. For starters, the most modern cellular services take advantage of what's called "frequency- hopping." That is, they can rapidly move signals across different frequencies more or less to avoid overcrowding. This complicates jamming. The more a signal hops, the more frequencies you'd have to jam.

Consider this scenario. Police get a credible tip that a terrorist is planning to detonate an IED by cellphone... somewhere. The cops set up jammers across a range of frequencies all over the city, perhaps for hours. Yes, authorities might stop the bomb from exploding. But they've also jammed 9-1-1 and many of their own communications.

Medical emergencies and crimes in progress could go unanswered. Thousands of crises of a personal nature might go unresolved. Business would suffer hugely. Unable to make plans and connections, untold throngs of commuters could find themselves lost or stranded.

The military certainly appreciates this problem. Ground convoys must turn off their jammers when they enter bases, lest they shut down the whole base's communications. Airborne jammers require careful coordination with other forces, as their powerful blocking signals could wipe out friendly troops' own radios and phones and potentially scuttle delicate battle plans.

The risk of collateral damage is one reason why the federal government bans most cellular jamming. It's illegal to sell a cell-jammer in the United States, so most buyers order theirs online from overseas retailers--and usually get away with it.

The jamming-ban isn't actually new. The Communications Act of 1934 states that "no person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under [the Communications] Act or operated by the United States government" (PDF).

"Jammers cannot be marketed or operated in the United States except in the very limited context of authorized, official use by the federal government," the FCC explained in its fact sheet. In May, the FCC fined a Florida man $48,000 for operating a cell-jammer during his commute to work, apparently in order to prevent other commuters from driving while on their phones and distracted.

And in March, Chicago cops arrested a man for jamming cellular calls on his daily train ride. "He was disturbed by people talking around him," his attorney said.

Legally speaking, the Department of Homeland Security or some other federal agency could authorize cell-jamming in support of local law enforcement. Some police departments have been caught jamming signals without federal approval. Devices called "stingrays" act as decoy cellular towers. Deployed by police eavesdroppers, stingrays can intercept cellular calls for purposes of gathering evidence.

But if a stingray is sucking up cell signals, that means calls--including, for example, 9-1-1 calls--aren't reaching actual cellular networks. On that basis and others, Georgetown University professor Laura Moy filed a complaint to the FCC over the Baltimore Police Department's use of stingrays.

"In a clear violation of law, BPD has no license whatsoever to operate its [cellular-site] simulator equipment on frequency bands that are exclusively licensed to cellular phone carriers in Baltimore," Moy wrote. "BPD further violates the Communications Act by willfully interfering with the cellular network through its use of [cell-site] simulator equipment."

To be clear, local authorities can skirt the 1934 law by simply asking telecoms to briefly shut down cellular service in a particular area, as city officials in San Francisco did in 2011 as they tried to disrupt a planned protest of a police shooting.

Voluntary cellular shutdowns aren't necessarily illegal, but like jamming, they do run the risk of interfering with emergency responders, business, and travel. So while cellphones have made it easier for terrorists to set off homemade bombs, cellphone-jamming probably isn't the best tactic for stopping them.

The Local (Germany)
Foreign state 'aims hack attack' against top politicians
Tuesday, 20 September 2016
Byline: Staff report

Berlin - Several German political parties were the target of hacker attacks over the summer, with a foreign government suspected to be behind them, the Süddeutsche Zeitung reports.
Security experts employed by the federal government believe that a foreign power initiated the attacks in order to gain sensitive information that could influence next year's national election, the Süddeutsche Zeitung (SZ) reports.

The security experts suggested to the SZ that the Russian government could be behind the latest attack on Germany's political establishment.

Politicians and employees of several parties received emails on August 15th and August 24th which appeared to come from NATO headquarters. Within the email was a link which, if clicked on, would enable spying software to be downloaded onto the computer.

The attack targeted high profile politicians such as opposition leader Sahra Wagenknecht (Die Linke), as well as the youth section of Angela Merkel's Christian Democratic Union (CDU). State offices of the CDU and Die Linke (Left Party) in Saarland, where elections will be held next spring, also received the email.

The emails came from a Heinrich Krammer, allegedly an employee at NATO headquarters, and offered information about the Turkish putsch attempt in July and the earthquake which hit central Italy in August.

In 2015, the German parliament was the target of a cyber attack. Following a similar pattern, the emails sent on that occasion appeared to come from the United Nations and claimed to offer information on the situation in Ukraine.

The hackers succeeded in stealing administrative passwords and accessing the entire internal network of the Bundestag (German parliament).

Bundestag IT experts said that the extensive damage from the virus attack meant that the whole parliamentary network would have to be replaced, at a cost of millions of euros.

Security experts voiced suspicions in May that Russia was behind the attack.

Washington Free Beacon
Snowden--Ultimate Insider Threat Missed by NSA Security
Tuesday, 20 September 2016
Byline: Bill Gertz

Column - Security officials today use the politically correct term "insider threat" to describe what were once called traitors, and no one was more aggressive in pursuing them than counterintelligence types at the National Security Agency.
Thus many intelligence officials saw more than a tinge of irony in NSA contractor Edward Snowden making off with 1.5 million highly classified NSA intelligence documents in May 2013 and handing them over to several anti-American journalists who seemed more interested in inflicting as much damage as possible on America's premier electronic spying and code-breaking agency than exposing alleged wrongdoing.

Until Snowden, the NSA had a reputation as one of the intelligence organizations most dedicated to protecting secrets. But the case exposed gaping holes at the agency, and a House intelligence report says gaps persist years after Snowden fled the country and holed up in Moscow.

Sure, the super-secret agency whose name itself was once classified had its share of Cold War spies, but nothing quite like Snowden.

One of my first reporting assignments 30 years ago was to cover the espionage trial in Baltimore of NSA analyst Ronald Pelton. Prior to the proceedings, NSA had argued within the government against prosecution in favor of a plea deal. The spooks were worried about the disclosure of secrets and spying methods during the high- profile case.

At trial, NSA technicians for the first time revealed how they secretly recorded Pelton's conversations using remote electronic equipment that turned slight vibrations on a windowpane in his house into a type of microphone for eavesdropping.

Also at trial, the federal government threatened this reporter and several others with unspecified action if we reported how Pelton had revealed to Moscow a secret underwater eavesdropping program that spied on Soviet military communications in the far east Sea of Okhotsk by tapping undersea cables. The operation, known as Ivy Bells, eventually became public despite the NSA's attempts to keep it secret.

Security at the NSA's large campus, visible from the Baltimore- Washington Parkway and inside the Army's Fort Meade, Maryland base, has always been tight. Anyone at the agency who runs afoul of feared security and counterintelligence police quickly can finds themself without a security clearance and assigned to the motor pool. Others have faced what critics describe as unfair scrutiny from NSA psychiatrists whose evaluations have spelled a quick end to intelligence careers. Employment at NSA is all about security clearances. Have one, and you work; lose one or have it suspended for a security infraction, and you might as well seek employment in another field.

Snowden had enough security clearances to get him access to a trove of secrets that he then leaked. For doing so, he has been lionized by many on the political left and a few on the libertarian right as a hero who allegedly exposed illegal electronic spying against Americans. The lionization reached new heights last week with a campaign seeking a presidential pardon and release of a new film by one the left's chief

conspiracy theorists, filmmaker Oliver Stone. The film traces Snowden's background as a washout from Army Ranger school to first the CIA and then to Booz Allen, an intelligence contractor who assigned him to NSA.

Stone held a Georgetown reception last week at a French restaurant where wine and cocktails were served and a number of officials rubbed shoulders with NSA critics after an exclusive screening of the film.

Once attached to NSA, Snowden worked as a computer administrator and hacked his way through electronic flaws in NSA's secret computer and information systems to siphon off the documents. The extremely secure networks used for classified information are not accessible from outside secure areas of NSA. But as with all computers, the systems have ports and entryways for loading software that Snowden was able to exploit in pilfering some of the crown jewels of the NSA.

An earlier documentary on Snowden, Citizenfour, featured the renegade contractor in Hong Kong claiming the NSA had engaged in a massive conspiracy to spy on Americans and violate their privacy--charges that were never proven.

What was revealed in NSA documents was not the agency portrayed by Snowden--a rogue elephant trampling the privacy rights of Americans. Instead, agency documents reveal remarkable capabilities for stealing secrets, some of them highly encrypted, and turning them into valuable intelligence for use in dealing with terrorists and enemies like China, Russia, North Korea, and Iran.

Those capabilities are now at risk. The reason is that one of the first rules of effective electronic eavesdropping is that the information gathered is only good as long as the method used to gather it remains a closely guarded secret.

NSA officials are unabashed about the agency's spying prowess, unlike the politicized CIA under current Director John Brennan. Brennan invoked scorn from agency veterans in February by making the dubious assertion that "we don't steal secrets." The comment reflected the CIA's shift away from its traditional role of conducting difficult cloak-and-dagger human spying abroad. According to former officials, the CIA today has lost much of its clandestine operations capabilities, instead embracing the much easier task of targeting and killing terrorists in remote-controlled drone strikes, which has become one of the agency's primary missions.

By comparison, the NSA's spying power is formidable, as revealed in documents showing that the agency not only breaks into foreign computers to steal secrets, but breaks into the computers of foreign intelligence services and steals secrets foreign intelligence services are gathering from their own targets. NSA wags code- named the practice "I drink your milkshake," after a quote in the 2007 film There Will Be Blood about oil drillers tapping wells of nearby competitors to secretly siphon off their crude.

Republicans in Congress last week sought to dispel the myth that Snowden is some kind of hero. On Friday, no doubt timed to the release of the Stone film, the House Permanent Select Committee on Intelligence released the damning executive summary of its still-secret 36-page review of the case. Its conclusions do not paint Snowden in a favorable light, to say the least.

"First, Snowden caused tremendous damage to national security, and the vast majority of the documents he stole have nothing to do with programs impacting individual privacy interests--they instead pertain to military, defense, and intelligence programs of great interest to America's adversaries," the report said.

The damage included compromised secrets that protect American troops overseas and bolster defenses against terrorists and states. Foreign states now know how the NSA targets their information and can take steps to counter the agency.

Snowden, who has been under Russian government protection since June 2013, has shared some of the stolen documents with Moscow. According to the House report, a Russian parliamentarian stated in June that Snowden shared intelligence with the Russians.

NSA reviewed all 1.5 million documents Snowden removed and will spend "hundreds of millions of dollars and will eventually spend billions, to attempt to mitigate the damage Snowden caused," the report said.

The House report also sought to counter the notion that Snowden was a whistleblower motivated to expose NSA wrongdoing.

Contrary to Snowden's claims that he sought to alert the NSA or other officials to his concerns about domestic spying, "the Committee found no evidence that Snowden took any official effort to express concerns about U.S. intelligence activities--legal, moral, or otherwise--to any oversight officials within the U.S. government, despite numerous avenues for him to do so."

The report reveals that Snowden, in the course of stealing documents, obtained login credentials from colleagues through unspecified misleading means. He then used administrator access to search coworkers' personal drives and removed personal information from thousands of intelligence officials and contractors.

Snowden has not disclosed the details surrounding his flight from Hawaii. The House report notes, however, that he engaged in "a fiery email argument" with an NSA supervisor about how to manage computer updates in June 2012.

"Two weeks later, Snowden began his mass downloads of classified information from NSA networks," the report said, describing Snowden as a "serial exaggerator and fabricator." One action was to doctor

his performance evaluations to obtain new positions at NSA. He notified his supervisor in May 2013 that he was taking time off for epilepsy treatment when in fact he was heading to Hong Kong.

Perhaps the most worrisome aspect of the House report was its conclusion that, three years after Snowden's actions, the NSA and intelligence community remain vulnerable to further document thefts.

"More work can and should be done to improve security of the people and computer networks that keep America's most closely held secrets," the report said, adding that the NSA has not initiated post-Snowden security enhancements.

The problem for NSA and other intelligence agencies is the imposition of liberal-left political correctness policies that prevent questioning the motives of renegade employees like Snowden.

The days of independent counterintelligence units within the intelligence community were ended in the 1970s. Since then, aggressive programs for the security of people and information systems remain off limits by policies that prevent questioning loyalties. Until that changes, expect further cases of betrayal.

China Daily
Three years after his revelations, Snowden in spotlight again
Wednesday, 21 September 2016
Byline: Chen Weihua

When President Xi Jinping and US President Barack Obama were about to meet in the California desert resort of Sunnylands in June 2013, the US government had worked hard to paint China as a villain in cyberspace.
The revelation made by former National Security Agency contractor Edward Snowden just days before the shirt-sleeves meeting, however, shocked the world. It showed that whatever other countries had done in cyber-surveillance and spying was really nothing compared to the massive scale of operations by the NSA, often labeled as No Such Agency.

To the rest of the world, Snowden is undoubtedly a whistleblower and a great hero because he revealed the US government secret scheme to spy on people all over the world, including foreign leaders who are US allies.

Such spying, which violates people's privacy and civil rights, often involves willing and unwilling collaboration with several major US tech companies.

In the US, debate about whether Snowden is a hero, patriot or traitor is still a divisive issue, despite that his revelation has resulted in the US government and Congress correcting many mistakes.

For example, the panel appointed by Obama to review NSA surveillance programs made dozens of reform recommendations. A federal appeals court has found NSA's call-tracking program revealed by Snowden illegal. The USA Freedom Act passed by the US Congress ended the bulk collection of phone data by the government.

In the past week, Snowden has again been in the spotlight. The German-American movie, Snowden, directed and written by Oliver Stone and Kieran Fitzgerald, hit US theaters on Sept 16.

Meanwhile, Snowden has pleaded for a pardon from Obama, arguing that his massive leak of NSA surveillance programs was "not only morally right" but also "left citizens better off".

On Sept 14, the American Civil Liberties Union (ACLU) Executive Director Anthony Romero called Obama to pardon Snowden by launching the Pardon Snowden campaign that will last untll the end of the Obama administration.

"Thanks to Edward Snowden's act of conscience, we've made historic strides in our fight for surveillance reform and improved cybersecurity," he said.

The ACLU campaign was joined by Amnesty International, Human Rights Watch and a list of more than 100 legal scholars, former national security officials, business leaders, human rights activists and artists.

Romero believes the Espionage Act, which the US government used to charge Snowden, is a World War I era law that doesn't distinguish between selling secrets to foreign governments and giving them to journalists in the public interest.

Most of the people who believe that Snowden is a traitor and should spend the rest of his life in prison argue, as I heard in the latest C-SPAN Journal on Sept 16, that he broke an oath and put the US national security in danger.

It is true that Snowden broke trust, but it occurred in a situation where he found serious wrongdoing by the US government, which is a much more serious crime that people should care about.

Even former US attorney general Eric Holder said that "we can certainly argue about the way in which Snowden did what he did, but I think that he actually performed a public service by raising the debate that we engaged in and by the changes that we made".

However, the US House Intelligence Committee unanimously signed a letter to Obama on Sept 15 not to pardon Snowden, describing his action as causing huge damage to the US intelligence community.

While Obama has commented that the debate triggered by Snowden "will make us stronger", it does not look likely that he will have the guts to pardon Snowden.

Both Republican and Democratic presidential candidates Donald Trump and Hillary Clinton are clearly against a pardon. Trump has repeatedly called for execution of Snowden although he said back in 2013 that he might become a major fan if he could reveal Obama's records.

Le Devoir
Médias - Snowden dans l'impasse
Wednesday, 21 September 2016
Byline: Brian Myles

Editorial - Le "Washington Post" a largué son plus célèbre lanceur d'alerte depuis "Deep Throat" en reprochant à Edward Snowden d'avoir compromis la sécurité nationale. Le quotidien fait reculer le journalisme d'enquête avec sa position, même si elle est nuancée.\r\nEn marge de la sortie du film d'Oliver Stone sur la vie d'Edward Snowden, ce spécialiste de la sécurité informatique qui a divulgué une avalanche de documents confidentiels de l'ultrasecrète National Security Agency (NSA), un mouvement international réclame qu'il soit gracié par le président Barack Obama. Trois médias qui ont collaboré avec le lanceur d'alerte, The New York Times, The Guardian et The Intercept, militent pour qu'il obtienne ce pardon. Le Washington Post, principal bénéficiaire des secrets de Snowden, fait figure d'exception en calquant désormais le discours des hauts gradés de la sécurité nationale à la Maison-Blanche.
" Pas de pardon pour Edward Snowden ", titrait le Post en éditorial, samedi dernier. Il n'est pas dans l'habitude d'un journal de critiquer l'éditorial d'un autre journal, mais la position défendue par le vénérable quotidien est à ce point dommageable pour le journalisme d'enquête et la protection des sources qu'elle mérite d'être condamnée.

Le Post ne reproche pas à Snowden d'avoir coulé des documents confidentiels sur le programme de collecte de métadonnées téléphoniques de la NSA, sur lesquels le quotidien s'est basé pour mener une série d'enquêtes lui ayant valu un prix Pulitzer pour service public (avec The Guardian). Les révélations de Snowden étaient à ce point dommageables que le gouvernement américain s'est résigné à circonscrire la collecte de métadonnées par la NSA, en juin 2015, avec l'adoption de l'" USA Freedom Act ".

Non, le Post reproche plutôt à Snowden d'avoir éventé le secret sur un autre programme de surveillance (Prism) " parfaitement légal ", sur les activités de renseignement visant la Russie, sur l'espionnage de l'épouse de feu Oussama ben Laden, et ainsi de suite. Il s'agit, à quelques nuances près, de la position défendue par un comité bipartisan du Congrès sur la sécurité nationale.

Selon cette logique, Edward Snowden a causé " des dommages énormes " à la sécurité nationale des États-Unis et ne mérite aucunement la grâce présidentielle. Qu'il revienne de la Russie, où il s'est réfugié en 2013, pour rentrer aux États-Unis et y subir un procès pour espionnage. Les détracteurs de Snowden ne lui laissent guère d'autre choix que de se cacher sous le manteau protecteur du président russe, Vladimir Poutine. Voilà qui n'est guère rassurant.

Le Washington Post passe un mauvais quart d'heure sur les réseaux sociaux, quoique sa position ne soit pas dépourvue de sympathie pour Snowden : celui-ci devrait accepter une responsabilité criminelle pour sa conduite, dans la plus pure tradition de la désobéissance civile, en échange d'une sentence clémente, écrit-on.

Cette position ne saurait faire oublier l'essentiel. Comme le souligne le journaliste d'enquête Glenn Greenwald, qui a mis l'affaire Snowden au monde dans The Guardian, le Washington Post est le premier quotidien à exiger des poursuites criminelles contre sa propre source.

Snowden n'a jamais rien publié de lui-même. Les médias, dont le Washington Post, portent le fardeau de ce " crime ". Les journalistes qui ont donné vie à l'affaire Snowden mériteraient-ils donc d'être poursuivis en justice ?

L'éditorial du Post est une trahison du rôle historique joué par les médias privilégiant le journalisme de qualité. Ils ont toujours protégé leurs sources et leur matériel contre les intrusions de l'État, même lorsque la sécurité nationale était en cause. Ce fut le cas du New York Times lors de la publication des " Pentagon Papers ", portant sur les insuccès de la guerre au Vietnam. Idem pour la décision de l'Ottawa Citizen de contester la perquisition abusive au domicile de la journaliste Juliet O'Neill, qui enquêtait sur le renvoi de Maher Arar en Syrie. Les exemples de résistance médiatique ne manquent pas.

Le fait qu'une source ait obtenu des documents de manière illégale ne change rien au fait que les médias ont le droit de colliger et de diffuser ce matériel, pourvu qu'il réponde à des critères de véracité et d'intérêt public.

Bien sûr, Edward Snowden a commis un geste illégal. Mais son geste en est un de " service public ", selon l'expression de l'ancien procureur général des États-Unis Eric Holder. Il est l'instigateur d'un débat national aux États-Unis et ailleurs dans le monde sur l'étendue démesurée des pouvoirs de surveillance des agences de sécurité nationale.

Si l'éditorial du Post choque autant, c'est qu'il est en rupture marquée avec les idéaux de défense des libertés civiles dont les médias traditionnels sont habituellement les gardiens.

Journal de Montréal
Les drones toujours plus populaires pour la livraison illégale en prison
Wednesday, 21 September 2016
Byline: Michaël Nguyen

Québec - Le nombre de vols observés au-dessus des prisons est passé de 4 à 27 en deux ans
L'utilisation des drones pour livrer des articles de contrebande en prison ne dérougit pas, surtout à Montréal où des détenus tentent d'obtenir de la drogue, des cellulaires, mais aussi des épices et des écouteurs.

Sur les 60 vols de drones observés autour des prisons du Québec en trois ans, 38 ont été recensés à l'Établissement de détention de Montréal.

«Le phénomène est en hausse, c'est une réalité depuis quelques années», déplore Mathieu Lavoie, président du Syndicat des agents de la paix en services correctionnels du Québec.

Selon des données obtenues auprès du ministère de la Sécurité publique, le nombre de vols de drones observés dans les prisons du Québec ne cesse d'augmenter.

En 2013-2014, le ministère avait recensé quatre vols de drones. L'année suivante, il y en a eu 18. Le nombre a encore augmenté en 20152016 pour atteindre 27.

Et depuis le mois d'avril, 11 vols de drones ont été observés, dont 10 à Montréal.

Sur les 60 événements au total, 49 concernaient les deux établissements de détention dans la métropole.

Selon les documents obtenus auprès du ministère de la Sécurité publique, les détenus tentent principalement d'obtenir des cellulaires, de la drogue et du tabac.

GROS PROFITS

«Compte tenu de la rareté, le prix du tabac peut être trois ou quatre fois plus élevé en prison», explique M. Lavoie, qui presse le gouvernement d'agir pour contrer le phénomène des drones autour des établissements de détention.

Mais les détenus peuvent aussi se faire livrer des articles plus insolites, comme des épices, une caméra GoPro ou une lampe de lecture.

Dans certains cas, l'interception de colis livrés par drone a permis de saisir des pics artisanaux et une lame pour scier le métal.

«Le trafic en prison est très lucratif, mais il représente un risque de sécurité. Il faut trouver des solutions», explique M. Lavoie, tout en ajoutant qu'un drone peut être capable de transporter jusqu'à 1 kg de matériel.

Il propose par exemple les brouilleurs d'ondes dans les prisons. Comme la plupart des drones sont souvent contrôlés avec un téléphone intelligent, dit-il, le problème serait ainsi réglé. De plus, cela empêcherait les détenus d'utiliser illégalement des cellulaires.

PEU DE MESURES

Le syndicat déplore toutefois le manque de mesures concrètes du gouvernement pour contrer le phénomène des drones, qui ne fait qu'augmenter.

«C'est préoccupant. Il y a des études, mais rien n'est mis en place, explique M. Lavoie. Soit les dirigeants n'ont pas d'argent, soit ils ne sont pas préoccupés par la problématique. Peut-être que c'est le prix de l'austérité.»

Lorsque nous l'avons contacté, le ministère de la Sécurité publique n'était pas en mesure d'indiquer quelles mesures étaient mises en place pour contrer le problème de livraison d'articles de contrebande par drone.

Notons qu'aux Pays-Bas, les autorités ont entraîné des aigles pour intercepter les drones qui survolent des zones interdites.

Philippine Star
NICA: 170 job vacancies up for grabs
Wednesday, 21 September 2016
Byline: Alexis Romero

Manila - The National Intelligence Coordinating Agency (NICA) is set to fill 170 job vacancies to perform its mandate and carry out its operations.
The agency is hiring analysts, researchers, information technology (IT) and technical personnel, lawyers and medical and dental staff, an advertisement published yesterday in The STAR showed.

The advertisement said those who would be hired would be "part of the change" and would "contribute to national development."

NICA is looking for 10 analysts, 10 junior analysts, and 20 senior analysts. Analysts will be tasked to process and analyze information on national security concerns as well as prepare, review and update reports for policy makers, according to a job description posted on the NICA website.

The agency is also hiring 10 field researchers, 10 junior field researchers and 10 senior field researchers.Researchers will gather information related to national security for policy makers and coordinate with state agencies and private institutions.

There are also job openings for 10 IT officers, 20 computer programmers and 10 computer maintenance technologists.

NICA is also looking for five engineers, 10 electronics and communications equipment technicians, 10 audio-visual technicians and 10 communication equipment operators.

Other vacancies are five chief accountants, five attorneys, five medical officers, five dentists and five nurses.

NICA, which is the principal adviser to the president on intelligence, is mandated "to be the focal point for the direction, coordination and integration of government activities involving national intelligence, and the preparation of intelligence estimates of local and foreign situations."

Asharq Al-Awsat
ISIS' Internet Communication Lessens after Sirte Battle
Wednesday, 21 September 2016
Byline: Abdul Sattar Hatita

Cairo - "Liberated Sirte", "Wilaya of Tripoli", "Soldiers of Caliphate in Libya" are samples of names that have disappeared from social media pages of ISIS in Libya.
Observers from Misrata say that the propaganda ISIS used to launch through social media and internet has remarkably declined after its defeat in Sirte.

During their capture of ISIS' strongholds in Sirte, Libyan forces of the Government of National Accord found laptops, smartphones and cameras, which were used by the extremist organization to spread its thoughts and to promote its intellect and achievements through internet not only in Libya, but also across the world in different languages.

A military investigator from Misrata said that after destroying ISIS' communication centers in Sirte and seizing all its equipment, the organization's propaganda on the internet has decreased, leaving the group with the option of using websites and pages in Syria and Iraq to cover its news.

Many forces supported by the United States and operating under the leadership of Fayez Al-Sarraj have broken into the city of Sirte and the sites ISIS used to control. They were able to confiscate more than 50 laptops and smartphones with several instant messaging programs uploaded on them.

According to investigations, ISIS used programs like Viber, WhatsApp Messenger, You Tube, and Telegram during its control of the city. One of the folders found after the break comprised religious lectures and speeches for the alleged Caliphate Abu Bakr al-Baghdadi and his spokesperson Mohammad Al-Adnani.

Investigations have also shown that many Libyan and foreign people were cooperating with the organization after its control of Sirte. The investigator from Misrata says that many merchants who used to transport relief and food aid among Libyan regions were obliged to pass by ISIS checkpoints and to give up shares of the provisions they were loading.

The government armed forces have recaptured the building of 'Sirte's radio" in the past month; national and foreign investigators (most of them from the United States and the United Kingdom) have participated in the post-liberation inquisitions.

Some of the videos feature leaders of ISIS ordering militants to kill people who refused to surrender in public squares.

A source from Tripoli has revealed to Asharq Al-Awsat that some ISIS-related documents concerning its links with sleeping cells and its communications in Libya and abroad have been moved out of the country during the past two weeks; however, many documents have been kept in Benghazi.

It is worth mentioning that following the liberation of Sirte, ISIS has admitted its defeat against the forces supported by the government in the city through its news outlets like Dabiq Agency and al-Naba newspaper.

ISIS has heavily attacked militias and factions which were supposed to back it in Libya. It has also threatened the leaders of factions that cooperated with the government, the parliament and the Presidential Council.

BDNews24

India urges SAARC states to counter cyber tactics of Islamic State militants

Friday, 23 September 2016

Byline: Staff Correspondent

Section: general

New Delhi - India has appealed the SAARC countries to adopt strong methodologies to counter all cyber threats from the Islamic State militants.
"The terrorist organisations use easily accessible technology to attack both soft and hard targets. Self-radicalisation over internet and social media, and spread of influence of Islamic State all over, including in our country, has added new dimensions to the threat," said Dineshwar Sharma, director of India's Intelligence Bureau, on Thursday.

He said IB has identified countering financing of terrorism as one of the most important tools to fight the terror menace.

"Cyberspace has become an important area for radicalisation and spread of jihadi materials. Besides, the problem of fake currency feeds into supporting terrorism and can create economic destabilisation in our region," he said.

He was speaking at the second meeting of the High Level Group of Eminent Experts to strengthen the SAARC Anti-Terrorism Mechanism.

Sharma called upon the eight member states to ratify and enable various conventions enacted by the South Asian Association for Regional Cooperation (SAARC) grouping, including the Convention on Suppression of Terrorism and Additional Protocols and the Mutual Assistance in Criminal Matters.

Sharma said terrorism has emerged as a big challenge for the entire world and no country today is in a position to tackle this problem on its own.

"Close cooperation and sharing of real-time intelligence are, therefore, imperative for all of us to secure our countries and our peoples," he stressed.

He lamented that not much progress has taken place on the operationalisation of the SAARC Terrorist Offences Monitoring Desk and SAARC Drug Offences Monitoring Desk.

The First meeting of the Anti-Terrorism Mechanism of SAARC in 2012 had stressed upon the need for immediate operationalisation of the desks.

Meeting of a High Level Group of Eminent Experts to strengthen the SAARC Anti-Terrorism Mechanism was recommended by the SAARC Ministerial Declaration on Cooperation in Combating Terrorism (adopted by the 31st Meeting of SAARC Council of Ministers in Colombo, February 2009).

India had hosted its first meeting in New Delhi from 9-10 February 2012.

Hosting the meeting for the second time, it is in line with the high priority India attaches for regional cooperation in Anti-Terrorism activities and given that terrorism remains the single biggest threat to peace, stability and progress in the region and beyond.

The meeting provides a platform for discussing and identifying measures to tackle this menace threatening our societies.

La Presse+

Deux drones observés, de la drogue et des armes trouvées

Friday, 23 September 2016

Byline: Daniel Renaud

Section: general

Montréal - C'était le jour des drones jeudi dernier au Centre de détention Rivière-des-Prairies à Montréal. Alors que deux de ces engins volants auraient été observés au-dessus des cours de la prison, les gardiens ont découvert dans un secteur abritant des membres de gangs de rue une quantité relativement importante de stupéfiants et d'inquiétants outils vraisemblablement arrivés par drone, a appris La Presse.
Drogue, cellulaires et lames de scie...

Après avoir reçu une information ou eu des doutes, les agents correctionnels ont effectué une fouille en soirée dans les 16 cellules d'un secteur où sont détenus majoritairement des individus d'allégeance bleue. Selon des sources, ils ont trouvé plus de 50 grammes de haschisch, une substance s'apparentant à de l'héroïne, six téléphones cellulaires, des lames de scie et un petit appareil électrique multifonctionnel. Quelques heures plus tôt, deux drones auraient été aperçus au-dessus de deux cours

de l'établissement, dont un autre secteur où les prévenus sont classés « général ». On ignore toutefois si des objets ont été saisis à la suite de l'observation de ces drones.

Grillages réclamés

Le président du Syndicat des agents en services correctionnels du Québec, Mathieu Lavoie, n'a pas voulu confirmer les informations recueillies par La Presse. Mais il implore le gouvernement d'agir pour mettre fin aux livraisons, de plus en plus nombreuses, par drones dans les 18 prisons du Québec. « On se rend compte que les projets-pilotes ou les mesures mis en place après les évasions de Québec et de Saint-Jérôme n'ont pas fait cesser ces intrusions », lance M. Lavoie.

Explosion des apparitions

Selon des chiffres obtenus du ministère de la Sécurité publique grâce à la Loi sur l'accès aux documents publics, les observations de drones au-dessus des terrains des prisons québécoises ont explosé depuis 2014. On en a dénombré 27 l'an dernier. Cette année, on en était à 11 au 16 juillet, un chiffre qui est déjà plus important qu'à la même période l'an dernier. Les statistiques de cette année ne comprennent pas les deux observations de jeudi dernier au- dessus du Centre de détention Rivière-des-Prairies.

Drones signalés à la sécurité dans les prisons du Québec

2013-2014 4

2014-2015 18

2015-2016 27

2016-2017 (au 16 juillet dernier) 11

Les plus livrés

Les objets apportés par drones les plus souvent saisis sont les stupéfiants, le tabac et le papier à rouler, en raison notamment du trafic institutionnel causé par la valeur très élevée de ces produits à l'intérieur des murs, où ils sont interdits. Les appareils cellulaires, qui peuvent permettre à un détenu de poursuivre ses activités criminelles depuis sa cellule, sont aussi très régulièrement saisis.

Saisies d'objets arrivés par drones (2013-2016)

Papier à cigarettes 9

Tabac 8

Stupéfiants 6

Briquets 5

Chargeurs de cellulaires 5

Cellulaires 4

Pic artisanal 2

Pots d'épices 2

Lame de scie à fer 1

Sphère de métal 1

Plaquette identificatrice 1

Bois 1

Draps 1

Caméra GoPro 1

Carte SIM 1

Écouteurs 1

Vis 1

Lampe 1

Ziploc 1

Timbres Nicoderm 1

Câble USB 1

Inconnu 1

*Le chiffre représente le nombre d'événements au cours desquels l'objet a été saisi et non pas le nombre d'objets de cette nature qui ont été saisis.

**Ces statistiques ne comprennent pas les objets de la saisie de jeudi dernier au Centre de détention Rivière-des-Prairies.

Jerusalem Post

New Israeli intelligence satellite 'sending back great images'

Friday, 23 September 2016

Byline: Yaakov Lappin

Section: general

Jerusalem - More than a week after it was launched and ran into serious technical difficulties, the Ofek-11 spy satellites began sending "great images" back to the ground control station, the Defense Ministry announced on Thursday evening.
Amnon Harari, head of the Space Administration in the Defense Ministry, and Ofer Doron, head of Israel Aerospace Industry's MBT Space Division, said the satellite's transponder and image broadcasting system began kicking in on Thursday, and that ground control officials were now seeing "operational results."

The IAI-made satellite was launched on September 13, and ran into unspecified difficulties after going into orbit.

Harari and Doron said the images they were now receiving "are what we hoped for," though they declined to provide further details on the overall health of the satellite.

Since the launch, engineers have been working to stabilize the satellite and its on board systems, the Defense Ministry and IAI said in a joint statement.

The teams systematically checked all of its systems from the moment of launch, and maintained continuous communication and control with it.

Ofek-11 launched from Palmahim Air Base south of Rishon Lezion near last week. Soon after its launch, officials said, "it's not yet clear if all on board systems are working," adding, "There are a number of things that are worrying us."

Ofek-11 is part of the Ofek series of satellites, and is Israel's sixth active spy satellite.

The troubled launch came after Amos- 6, an Israeli civilian communications satellite, was lost when its Falcon-9 launcher, made by SpaceX, blew up at the launch pad at Cape Canaveral in Florida on September 1.

Two years ago, the Defense Ministry and IAI launched Ofek-10 successfully into space on board a Shavi launch vehicle. Ofek -0 carries a SAR (Synthetic aperture radar), which has advanced day and night imaging capabilities.

Times of Israel

Despite initial woes, new Israeli spy satellite beams back first pictures

Friday, 23 September 2016

Byline: Judah Ari Gross

Section: general

Jerusalem - The Ofek-11 reconnaissance satellite launched earlier this month sent its first images down to Israeli engineers on Thursday, dispelling fears that the craft, which experienced issues after launch, would not be able to function at all, the Defense Ministry said.
At 5:10 p.m., engineers turned on the satellite's "payload" and downloaded the first images from the spacecraft, according to a ministry statement.

Shortly after the launch earlier this month, the team operating the satellite discovered it was "not functioning exactly the way we expected," Doron Ofer, CEO of the Israel Aerospace Industries' Space Division, said at the time.

Since then "dozens of engineers have been working to stabilize the satellite and its systems," the ministry said.

According to the ministry, that work paid off. "The Ofek-11 satellite will provide operational outputs," the ministry said.

The teams working on the satellite were made up of representatives from both the Defense Ministry's Space Department and the IAI Space Division, who ranged from "youngsters in their 20s to veteran engineers in their 70s," according to the statement.

The engineers have been in contact with the satellite since its launch, though the work was somewhat slowed due to the rotation of the Earth.

The satellite was shot into space at 5:40 p.m. on September 13 from the Palmachim Air Base, just outside the Tel Aviv suburb of Rishon Lezion.

The Ofek-11 is an upgrade from the Ofek-10 satellite launched in April 2014. However, Ofer would not discuss what exact improvements were made to the design of the satellite to make it superior to its predecessor.

The Ofek-11 was to join approximately 10 other satellites, including the Ofek-10, Ofek-9, Ofek-7 and Ofek-5, that feed intelligence to Israel's security forces.

Canadian Press

Feds warn of potentially crippling 'insider' cyberthreat to key sectors

Friday, 23 September 2016

Byline: Jim Bronskill

Section: general

Ottawa - Federal officials have quietly warned operators of electrical grids, transportation hubs and other key infrastructure of the cyberthreat from insiders who could unleash devastating viruses and cripple systems, internal government notes reveal.
Crucial networks that Canadians rely on for everyday needs face a ``substantial threat'' from rogue employees out to wreak digital havoc, warn the Public Safety Canada briefing notes.

``The insider threat is difficult to detect and can cause real damage.''

No special hacking skills are required, just a portable memory key loaded with a malicious code. As a result, it is important that organizations have the right security protocols and procedures, ``for example by limiting access to systems only to those who genuinely need it.''

A federal briefing on the insider threat was delivered last December to leaders of the 10 most crucial infrastructure sectors, the notes say.

They point out that over 90 per cent of critical infrastructure _ key to delivering everything from food and clean water to banking and health services _ is controlled by the private sector and all of it is dependent in one way or another on information technology to operate. Many critical infrastructure sectors are interdependent, meaning a problem in one could have a ``cascading impact'' in others.

The notes, prepared earlier this year for Monik Beauregard, a senior assistant deputy minister at Public Safety Canada, were obtained by The Canadian Press under the Access to Information Act.

Beauregard is chairing a panel today on the global implications of the challenges to cybersecurity at an intelligence conference in Ottawa.

In addition, Greta Bossenmaier, the head of Canada's electronic spy agency, the Communications Security Establishment, plans to discuss the various cyberchallenges the country faces.

The conference comes as the Liberal government undertakes a cybersecurity consultation that runs through mid-October. The overall aim is to identify gaps and opportunities, bring forward ideas to shape a renewed approach and capitalize on the advantages of new technology.

State-sponsored hackers, sophisticated criminals, cause-motivated hacktivists and people out to make mischief online all pose a threat, the government warns.

Public Safety is already working with critical infrastructure operators to prepare for the possibility of a major cyberattack on the Canadian electrical grid and telecommunications systems, the internal notes say.

Security officials call such an occurrence a ``black swan'' _ a rare but devastating event that requires special attention due to the potential for massive losses should it happen.

Washington Post

Yahoo hit in world's biggest data breach

Friday, 23 September 2016

Byline: Multiple reporters

Section: general

Washington - Yahoo on Thursday reported the largest data breach in history - affecting at least 500 million user accounts - months after first detecting signs of an intrusion that the company blamed on "state-sponsored" hackers.
The Web giant called on customers to change their passwords and institute other protective measures, but the largest fallout could be for Yahoo itself. The long-faltering company this summer agreed to sell its core business for $4.8 billion to telecommunications giant Verizon in a deal now clouded by news of the massive breach. Verizon said it learned of the incident only "within the last two days."

The timeline highlighted a predicament created by hacks: Companies often take months or even years to report suspicions of breaches - if they report them publicly at all - holding the information back from customers, business partners and even potential new owners of a company.

"The dark cloud this casts will be very long and will likely impact the merger agreement," Jeff Kagan, a Georgia- based telecommunications industry analyst, said in an email. "We'll just have to wait and see what happens next."

Yahoo learned of the incident in July, the same month it announced its deal with Verizon, a person familiar with the matter said, speaking on the condition of anonymity to freely discuss the issue.

When asked, Yahoo declined to say whether it learned of the hack before or after that deal was announced.

Yahoo revealed the breach after recode, a news site focusing on Silicon Valley, reported Thursday morning that the ailing tech giant would confirm a data breach affecting hundreds of millions of accounts.

Yahoo reported that the intrusion apparently began in 2014.

The number of affected accounts, by reaching 500 million, gave it the dubious distinction of being the largest breach on record, said Paul Stephens of the Privacy Rights Clearinghouse.

Stephens said that consumers must also take steps to take care of matters themselves, outside of their Yahoo accounts. "It's really important that individuals think long and hard about passwords as well as security questions and answers they used on Yahoo that they might have used somewhere else," Stephens said. "It's very important to remember that if that information is available to hackers, they are going to try and use it on other sites, as well."

Company Chief Information Security Officer Bob Lord wrote in a blog post that names, email addresses, telephone numbers, dates of birth and answers to security questions may have been stolen but that financial information such as credit card numbers apparently was not because that data was stored in a separate system.

"Yahoo is working closely with law enforcement on this matter," Lord wrote.

Sen. Mark R. Warner (D-Va.) chastised Yahoo for not reporting suspicions of a breach sooner and called on the federal government to impose stricter disclosure requirements for companies. Companies face a messy patchwork of state disclosure laws but no federal standard for reporting about breaches, including when, how and who was affected.

"While its scale puts it among the largest on record, I am perhaps most troubled by news that this breach occurred in 2014, and yet the public is only learning details of it today," Warner said in a statement. "Action from Congress to create a uniform data breach notification standard so that consumers are notified in a much more timely manner is long overdue."

Although President Obama proposed a federal law in 2015 that would give companies 30 days to notify the public about a discovered hack, lawmakers have yet to approve a national standard.

On Thursday, Sen. Richard Blumenthal (D-Conn.) called on investigators to determine whether Yahoo intentionally withheld information about the incident to "artificially bolster its valuation" by Verizon - a potentially serious act of deception.

The impact on Verizon's deal with Yahoo was not immediately clear. Major data breaches have become a routine event for corporate America and also for major government agencies and political groups. The Yahoo intrusion stands out for the sheer scale of the customers apparently affected, a legacy of the company's once-commanding position for Internet users who turned to the company for Web searches, email accounts, user groups and news reports.

The Verizon deal was seen as a relatively soft landing for Yahoo, a company overtaken by competitors in nearly every one of its major businesses.

Verizon, in a statement, said it was monitoring news of the breach. "We understand that Yahoo is conducting an active investigation of this matter, but we otherwise have limited information and understanding of the impact," the company said. "We will evaluate as the investigation continues through the lens of overall Verizon interests, including consumers, customers, shareholders and related communities. Until then, we are not in position to further comment."

The security breach is yet another bruise for the aging tech firm and chief executive Marissa Mayer, who joined Yahoo in 2012 to effect a turnaround and ended up having to sell the firm's core assets instead.

Microsoft's recent acquisition of LinkedIn, which came one month after the social network revealed that 167 million of its accounts had been breached, show a breach alone is not necessarily enough to derail a deal, said John Lovallo, senior vice president at the public relations and strategic communications firm Levick.

But he said the tech giant will be hard-pressed to rehabilitate its overall reputation in light of this breach.

"Focus on the consumer and not the deal," Lovallo said. "If I were in that boardroom at this moment in time, I would say, 'We understand there's a huge deal on the table right now.' But first address and resolve the issue for your consumers, and the transaction will take care of itself."

Yahoo has had a poor security reputation in the past, one of the many things that Mayer has focused on since becoming chief executive.

Vice's Motherboard blog in August reported that Yahoo was investigating an alleged breach after the news organization found that a cybercriminal known as "Peace" claimed to be offering 200 million Yahoo user credentials for sale online. The data was advertised on the "dark Web" - a part of the Internet accessible only through the use of special software such as the anonymous browsing tool Tor and often associated with illicit activities.

Tech City News

UK Government, Wayra and GCHQ partner to launch cybersecurity accelerator

Friday, 23 September 2016

Byline: Yessi Bello Perez

Section: general

London - The UK government has announced that it will be partnering with tech startups to develop new technologies aimed at protecting the country from cyber attacks.
According to a statement, the Department for Culture, Media and Sport (DCMS), Wayra UK and GCHQ - the UK's intelligence and cybersecurity agency - have come together to launch a new cybersecurity accelerator.

The partnership is considered to be the first step in the development of two world-leading innovation centres as part of the Government's £1.9bn National Cyber Security Programme.

Successful candidates will gain access to GCHQ's personnel and tech expertise to allow them to expand capability, improve their ideas and develop innovative products to counteract emerging threats.

Speaking about the announcement, Matt Hancock, Minister of State for Digital and Culture, said:

"We are making progress in our ambitious programme to support innovation in cyber security, grow the UK's thriving sector and protect Britain from cyber attacks and threats.

"Our two new Cyber Innovation Centres will bring together government, academic and business expertise, and will be invaluable in helping support start-up companies and develop world-class cyber technology," he concluded.

The accelerator will be based at a new Cheltenham Innovation Centre and is due to open around the turn of the year. A second innovation centre is expected to open in London in 2017.

The news comes after Hancock spoke at a Sharing Economy UK event yesterday, noting his desire to work collaboratively with industry to ensure the UK became the 'natural home' for firms operating in the sharing economy sector.

Ottawa Citizen

Hollywood gets it right on Snowden

Friday, 23 September 2016

Byline: David Lyon

Section: Opinion

Agency (NSA) leaker, distracted by a pre-dinner discussion with girlfriend Lindsay Mills, dashes to the stove where he has left the pasta. Testing the dangling fettuccine, he declares it as close to correctly cooked as he's managed.
Whatever the film critics make of the Snowden docudrama, it, too, may come as close to correctly rendered as Hollywood can manage. If you want to understand the serious computer geek who dared defy the NSA and, indeed, the entire U.S. government, Stone gets it about right.

This is no paranoid melodrama. The movie focuses persistently on the transformation of Snowden, from a loyal son of a military and government family, and who believes in patriotic obedience in service to his country, to the disabused but determined truth-telling NSA whistleblower whose controversial actions have ongoing global repercussions.

The film offers several players in that transformation. There's Snowden's dawning realization that his admired NSA seniors take the law into their own hands; the shocking discovery that his workmates

routinely conduct searches well beyond what is required for the task; and, most tellingly, his relationship with Lindsay Mills. Their early conversations contrast Snowden's conservative caution with Mills's open criticism of government as her democratic right and responsibility, and the film ends with his being entirely committed to her position - as a faithful citizen who "loves his country."

Though we might not express things in exactly the same way, many Canadians are also leery of some government activities. They're not being unpatriotic; it's an expression of the desire to see Canada flourish. Many, too, are concerned about the uncomfortably close relationship between the NSA and our own Communications Security Establishment (CSE), and about specific ways that the Anti-terrorism Act (Bill C-51) facilitates just such suspicionless surveillance (that is, placing under surveillance persons to whom are attached no already-existing suspicions) - based on "big data," as seen in the NSA. Films such as Snowden should be a spur to pressuring security agencies to more transparency and accountability. The current government's proposals for new oversight mechanisms are a solid start.

This does not mean governments should abandon all surveillance, as the movie also makes clear. It means querying the idea that metadata - details such as the times, places and duration of communication between identifiable persons - is merely "like a phone book," or that oldfashioned labour-intensive sleuthing can be abandoned in favour of flashy new solutions involving big data. Equally, the Snowden biopic may inspire efforts to demystify the arcane algorithms that guide the security surveillance systems to their persons of interest. The film hints helpfully at ways these algorithms are far from the neutral instruments they may be sold as - when in fact they're shaped politically.

Another way for Canadians to read this film is to consider its educational role in showing how once-secret NSA programs such as PRISM (which collects data from Internet companies) and XKeyscore (which searches and analyzes global Internet data) actually work. We have a long history of exploring the genesis, workings and impact of media and communication technologies - think Harold Innis or

Marshall McLuhan - and this can be put to good purpose right now. The Snowden Digital Surveillance Archive is based at Ryerson University, for instance, and is an ideal resource for making balanced judgments about contemporary surveillance practices. For director Oliver Stone, who spent many hours interviewing Snowden in Moscow, the quest is not merely to discover what made the truthteller tick, but how to do so in ways that resonate with regular filmgoers' lives. The issues, especially in Internet surveillance, are real, huge, complex and affect ordinary users' lives in often profound ways - without our knowing it. Learning to be digital citizens - as Snowden did - is a task for us all, not just in the land of the NSA.

At the very end of the film, Joseph Gordon-Levitt - the actor who plays Snowden - disappears symbolically behind his laptop lid and the person who reappears a moment later is not the actor, but the real Edward Snowden. He says nothing, but surely this image silently signals Snowden's approval of the film. It may not please the critics, but that message, at least, seems clear. Al dente. David Lyon directs

the Surveillance Studies Centre at Queen's University. His latest book is Surveillance After Snowden (Polity Press, 2015).

Washington Post

Report finds cyber-intrusions soaring, and slow progress on security measures

Friday, 23 September 2016

Byline: Joe Davidson

Section: column

Column - For the naive who still think cyberdata is safe with Uncle Sam, here is some information that demonstrates the harsh reality.
The number of cyber incidents reported by federal agencies jumped more than 1,300 percent, from 5,503 to 77,183, over the 10 years through fiscal 2015. Federal information security has been on the high-risk list of the Government Accountability Office (GAO) since 1997, and the situation has only grown worse.

These statistics, at once sobering and alarming, were included in a GAO report presented to the President's Commission on Enhancing National Cybersecurity this week. The report was in the form of a statement from Gregory C. Wilshusen, the GAO's director of information security issues.

"Over the last several years, we have made about 2,500 recommendations to agencies aimed at improving their implementation of information security controls," Wilshusen said. "These recommendations identify actions for agencies to take in protecting their information and systems. For example, we have made recommendations for agencies to correct weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources. ... However, many agencies continue to have weaknesses in implementing these controls, in part because many of these recommendations remain unimplemented. As of September 16, 2016, about 1,000 of our information security-related recommendations have not been implemented."

Ineffective cyberprotection "can result in significant risk to a broad array of government operations and assets," he added.

Jamal Brown, press secretary at the Office of Management and Budget (OMB), responded by saying that "cybersecurity is one of the most important challenges we face as a nation. Over the last nearly eight years, federal agencies have made significant progress in strengthening their overall cybersecurity

posture. Yet, as cyberthreats continue to evolve and grow, we must remain vigilant in our efforts to combat them."

Among those efforts was release of a first-ever cybersecurity workforce strategy and implementation of the Cybersecurity National Action Plan, which established the commission that heard Wilshusen's statement.

These examples from Wilshusen show how broad the array of threatened "government operations and assets" can be: "Sensitive information, such as intellectual property and national security data, and personally identifiable information, such as taxpayer data, Social Security records, and medical records, could be inappropriately added to, deleted, read, copied, disclosed, or modified for purposes such as espionage, identity theft, or other types of crime."

This is not just a theoretical warning. In June 2014, the Office of Personnel Management announced that personal information, including Social Security numbers, belonging to 22 million federal employees and others had been hacked. That is the largest announced cybertheft, but far from the only one. The private sector also has been repeatedly hit by cyberthieves.

"These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives," Wilshusen said. "For example, advanced persistent threats - where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives - pose increasing risks."

In a March report to Congress, the OMB linked the rising number of cybersecurity incidents to "an increase in total information security events and agencies' enhanced capabilities to identify, detect, manage, respond to, and recover from these incidents."

Although the report indicates that about 40 percent of the GAO's recommendations have not been implemented at any one time, Wilshusen said in an interview that the government's long-term record is significantly better. Within four years, 88 to 90 percent of the recommendations are followed, he said by phone. "Over time," he added, "the agencies do a pretty good job of implementing our recommendations."

The GAO offered several recommendations, including strengthening oversight of government contractors that provide information-technology services. That was a lesson learned the hard way through the OPM breach. In 2014, the GAO found that five of six selected agencies "were inconsistent" in their oversight of contractor cyber controls.

The GAO also recommended expanding the federal cyber workforce and training. That is not a new need. Said Wilshusen: "This has been a long-standing dilemma for the federal government."

Globe and Mail

Privacy watchdog concerned by 'smart' devices

Friday, 23 September 2016

Byline: Susan Krashinsky

Section: general

Ottawa - Canada's federal privacy watchdog is participating in a global initiative that's raising red flags about connected devices - everything from "smart" TVs to fitnesstracking wristbands and Internetconnected toys - and their failure to provide users with control over the personal information those gadgets collect.
The Office of the Privacy Commissioner of Canada (OPC) took part in the global "privacy sweep" in April, and is now releasing the results. The sweep involved 25 privacy authorities. It looked at 314 connected devices - often collectively referred to as the "Internet of Things" - and how they communicate their privacy practices.

Canada's focus was on 21 health and wellness devices that are popular among Canadians, including fitness trackers, smart watches, smart scales and bloodpressure monitors.

They found that connected devices "fail to inform users about exactly what personal information is being collected and how it will be used" - including sensitive data such as health and financial information.

The OPC says that the concept of "the body as information" is a major focus, as health, genetic and biometric information is being tracked more than ever.

During the sweep, staff used connected products and analyzed what information those devices asked for - and what privacy collection and protection information they provided to users.

Nearly half of Canadian "sweepers" - OPC staff who tested the devices - and more than three-quarters of international sweepers were unable to find basic instructions on how to delete their data once they had begun using the devices.

The Global Privacy Enforcement Network, now in its fourth year, is a joint effort among privacy organizations in many countries, including the United States, Britain , members of the European Union and China, and has conducted such privacy sweeps before. By acting in concert, the group is attempting to add global heft to major privacy concerns.

Last year, for example, the network conducted another sweep that showed how websites and mobile applications targeted to kids often do not do enough to protect children's privacy.

Among the devices that the OPC analyzed in this sweep, it highlighted concerns about a bloodpressure monitor and a thermometer that both asked to track users' locations, without giving adequate explanations about why that was necessary for the device's purposes.

Another concern was the Jawbone UP3, which tracks a user's activity, sleep and heart rate. The OPC noted that the device provided an easy online form to request that the company delete all personal information on its servers, including data shared with partners. But the "sweeper" found his account was still active, with personal information intact, two months later .

Both the Fitbit and Garmin Vivosmart HR fitness trackers were highlighted by the OPC for being too vague in their privacy policies about safeguards they put in place to protect users' data.

In another case, the iMazeFitness heart rate strap had a placeholder on its personal information page that said "[Insert customer data privacy clause here if applicable.]" "Many of the privacy communications were generic or vague, or had privacy policies that weren't specific to the devices being evaluated," said Brent Homan, the OPC's director-general of PIPEDA investigations. (PIPEDA stands for the Personal Information Protection and Electronic Documents Act, which is the law in Canada concerning privacy and personal data.)

"Providing information about what is being collected at key points - such as registration or purchase - is a best practice ... rather than having it buried in privacy policies," Mr. Homan said.

Not only should devices make clear what types of data are being collected and shared, Mr. Homan said, they should make it easier for users to exercise control over that information. Further, where information gathering is not essential to the device's purposes, user consent should be explicit - and the default setting should be not to gather that information, he said.

Washington Post

Key lawmakers accuse Russia of campaign to disrupt U.S. election

Friday, 23 September 2016

Byline: Greg Miller

Section: general

Washington - Two senior Democratic lawmakers with access to classified intelligence on Thursday accused Russia of "making a serious and concerted effort to influence the U.S. election," a charge that appeared aimed at putting pressure on the Obama administration to confront Moscow.
The jointly issued statement from Sen. Dianne Feinstein and Rep. Adam B. Schiff -- Californians who are the ranking Democrats on the Senate and House intelligence committees, respectively -- described recent cyber penetrations of the Democratic National Committee and other U.S. political entities as intrusions that were likely directed by Russian President Vladi-mir Putin.

"At the least, this effort is intended to sow doubt about the security of our election and may well be intended to influence the outcomes," the statement said. "We believe that orders for the Russian intelligence agencies to conduct such actions could come only from very senior levels of the Russian government."

Feinstein and Schiff said they reached their conclusion "based on briefings we have received" from U.S. intelligence agencies.

The blunt language goes far beyond the more equivocal characterizations issued by the White House and U.S. intelligence agencies, which have so far been unwilling to explicitly blame Moscow.

Speaking this week at a public event hosted by The Washington Post, Director of National Intelligence James R. Clapper Jr., cited a long history of Russian efforts to influence elections abroad, and said that "it shouldn't come as a big shock to people" that Moscow might seek to use cyber capabilities for that purpose.

But he stopped short of drawing aa direct link between the DNC hack and Russian intelligence services, amid an ongoing debate within the administration over whether to publicly blame Russia.

White House officials have repeatedly insisted that they are awaiting the outcome of a formal FBI investigation, even though U.S. intelligence are said to have concluded with "high confidence" that Russia was responsible for the DNC breach and other attacks.

The White House hesi-ta-tion has become a source of frustration to critics, including senior members of Congress.

The statement from Schiff and Feinstein did not critize President Obama's handling of the matter and called on Putin "to immediately order a halt to this activity." In an interview, Schiff said that he and Feinstein "think it's important to deter Russia from continuing this kind of conduct that they be called out on it. We've urged the administration to do that."

He said the timing of the statement was not driven by any new developments in the investigation of the hacks. "It's been in the works for longer than that," Schiff said, adding that "evidence is strong in terms of attribution."

Reuters

Probe of leaked U.S. NSA hacking tools examines operative's 'mistake'

Friday, 23 September 2016

Byline: Staff report

Section: general

San Francisco - A U.S. investigation into a leak of hacking tools used by the National Security Agency is focusing on a theory that one of its operatives carelessly left them available on a remote computer and Russian hackers found them, four people with direct knowledge of the probe told Reuters.
The tools, which enable hackers to exploit software flaws in computer and communications systems from vendors such as Cisco Systems and Fortinet Inc, were dumped onto public websites last month by a group calling itself Shadow Brokers.

The public release of the tools coincided with U.S. officials saying they had concluded that Russia or its proxies were responsible for hacking political party organizations in the run-up to the Nov. 8 presidential election. On Thursday, lawmakers accused Russia of being responsible.

Various explanations have been floated by officials in Washington as to how the tools were stolen. Some feared it was the work of a leaker similar to former agency contractor Edward Snowden, while others suspected the Russians might have hacked into NSA headquarters in Fort Meade, Maryland.

But officials heading the FBI-led investigation now discount both of those scenarios, the people said in separate interviews.

NSA officials have told investigators that an employee or contractor made the mistake about three years ago during an operation that used the tools, the people said.

That person acknowledged the error shortly afterward, they said. But the NSA did not inform the companies of the danger when it first discovered the exposure of the tools, the sources said. Since the public release of the tools, the companies involved have issued patches in the systems to protect them.

Investigators have not ruled out the possibility that the former NSA person, who has since departed the agency for other reasons, left the tools exposed deliberately. Another possibility, two of the sources said, is that more than one person at the headquarters or a remote location made similar mistakes or compounded each other's missteps.

Representatives of the NSA, the Federal Bureau of Investigation and the office of the Director of National Intelligence all declined to comment.

After the discovery, the NSA tuned its sensors to detect use of any of the tools by other parties, especially foreign adversaries with strong cyber espionage operations, such as China and Russia.

That could have helped identify rival powers' hacking targets, potentially leading them to be defended better. It might also have allowed U.S officials to see deeper into rival hacking operations while enabling the NSA itself to continue using the tools for its own operations.

Because the sensors did not detect foreign spies or criminals using the tools on U.S. or allied targets, the NSA did not feel obligated to immediately warn the U.S. manufacturers, an official and one other person familiar with the matter said.

In this case, as in more commonplace discoveries of security flaws, U.S. officials weigh what intelligence they could gather by keeping the flaws secret against the risk to U.S. companies and individuals if adversaries find the same flaws.

Critics of the Obama administration's policies for making those decisions have cited the Shadow Brokers dump as evidence that the balance has tipped too far toward intelligence gathering.

The investigators have not determined conclusively that the Shadow Brokers group is affiliated with the Russian government, but that is the presumption, said one of the people familiar with the probe and a fifth person.

One reason for suspecting government instead of criminal involvement, officials said, is that the hackers revealed the NSA tools rather than immediately selling them.

The publication of the code, on the heels of leaks of emails by Democratic Party officials and preceding leaks of emails by former U.S. Secretary of State Colin Powell, could be part of a pattern of spreading harmful and occasionally false information to further the Russian agenda, said Jim Lewis, a cybersecurity expert at the Center for Strategic and International Studies.

"The dumping is a tactic they've been developing for the last five years or so," Lewis said. "They try it, and if we don't respond they go a little further next time."

London Times

White House leak suspects linked to Kremlin

Friday, 23 September 2016

Byline: Rhys Blakely

Section: general

Washington - Hackers with suspected links to Russian intelligence boasted of infiltrating the White House yesterday.
Detailed travel plans for Michelle Obama, Hillary Clinton and Joe Biden, the US vice-president, were released, along with what appeared to be Mrs Obama's passport.

The documents, allegedly stolen from the personal Gmail account of a White house staff member, outlined the precise movements of three of the most protected people in the world. One set of plans included the exact number of steps Mr Biden had to climb as he entered a luxury hotel through a service entrance.

An email to The Times by DCLeaks, the website that shared the documents, said: "If terrorists hack emails of White House Office staff and get such sensitive information we will see the fall of our country."

Analysts have connected the website to Russia because of the techniques used to access other documents it has leaked. Its latest release came after one of America's top spy chiefs said Russia was suspected of attempting to meddle in the US presidential election.

The same website was behind a leak of hacked emails from Colin Powell, the former secretary of state, this month. In those messages Mr Powell shared candid assessments of Mrs Clinton and Donald Trump, calling the former sleazy and greedy and branding Mr Trump a "national disgrace and an international pariah".

DCLeaks yesterday claimed to release emails from the personal account of Ian Mellul, a White House employee responsible for planning travel. It is not clear why he was using a Gmail email address rather than an official account.

The documents included a copy of Mrs Obama's passport. One email detailed the itinerary for a visit that she made to a middle school in the state of Georgia in April, including details of how she would be waiting in a gymnasium locker room before the event began.

Another message contained a presentation, apparently prepared for Mr Biden before a visit to Cleveland in June. A series of photographs laid out the route he would take during an event in the Intercontinental hotel.

He would enter via a back loading entrance, the slides explained, adding: "1. YOU arrive in the loading dock and proceed up 4 stairs. 2. YOU proceed to HOLD via the staircase and walk up 26 steps to the 2nd floor." It showed which hotel room he would wait in until the event got under way and which adjacent hotel room his Secret Service detail would use.

A third message showed the route to be walked by Mrs Clinton at a fundraising event at a private home in Houston, including a plan of the house. Neither the White House nor Mr Mellul responded to requests for comment.

James Clapper, the US director of national intelligence, said this week that it would be no surprise if Russia was trying to influence the race for the White House. There was a well- established history of such attempts, dating back to the Cold War, he told a conference in Washington. An attempt to meddle in the presidential race "certainly should not come as a big shock to people", he said.

.Russia's increased willingness to flex its military muscle around the world dominated Theresa May's first in-depth security briefing with defence chiefs. The prime minister underlined Britain's decision to lead Nato's rapid reaction force in eastern Europe, Whitehall sources said. Mrs May was also updated on the RAF bombing campaigns in Syria and Iraq as well as Britain's operations in Afghanistan.

ABC (Australia)

Yahoo breach puts focus on Australian consumer hacking protections

Friday, 23 September 2016

Byline: Jake Sturmer

Section: general

Canberra - Yahoo's confirmation of a serious breach affecting 500 million users puts the spotlight on Australia's lack of regulation forcing businesses to tell victims their information has been stolen. Yahoo's confirmation of a serious hack has put the spotlight on Australia's lack of regulation forcing businesses to tell victims their information has been stolen.

The that occurred in 2014, with hackers accessing data from at least 500 million users.

Yahoo believes they may have been state sponsored attacks, capturing names, email address, birth dates, and scrambled passwords, along with encrypted or unencrypted security questions and answers that could help hackers break into victims' other online accounts.

In Australia, there are no laws that force companies that have been breached (or inadvertently disclosed information) to notify the affected customers.

The Government has released draft laws to force notification of personal information data breaches, known as mandatory data breach notification.

The legislation is proposed to be introduced in this year's Spring sittings of Parliament, as an amendment to the Privacy Act.

These laws have long been advocated for by privacy experts and were recommended as part of a Parliamentary Joint Committee on Intelligence and Security inquiry into Australia's data retention laws.

However, industry groups are pushing back against the changes fearing they could be difficult to implement and impose an unreasonable compliance burden on businesses.

Nick Abrahams, a partner at law firm Norton Rose Fulbright, advises companies on how to deal with data breaches.

He said "more often than not in Australia people aren't getting notified" and that the legislation was inevitable.

"We just need to get on with it - we're going to get it, we should have it," he said.

"Most other countries of our level of development have similar concepts.

"Particularly boards are having to deal with this issue because right now [breaches don't] get escalated to them because there's no obligation to notify.

"It's an important issue for boards to think about - 'are we risking serious harm to those people whose data we have compromised?'

"The reality is there's so much more of it happening now."

Dark web marketplace booming

Last month,

Other major companies including Jetstar and Suzuki had systems suspected to have been compromised, but both companies denied being breached.

Computers like these can be rented by cyber criminals and used to launch attacks against others for as little as $6.

And yesterday

H&L Australia, whose clients include Woolworths-owned Australian Leisure and Hospitality (ALH) Group, provide point-of-sale (POS) systems for more than 300 restaurants and liquor stores as well as pubs and clubs.

H&L confirmed to the ABC that a server containing marketing material and its client list, known as a Customer Relationship Management system, had been hacked but said no financial details had been stolen.

Several other Australian companies - and Kmart - have also been attacked by hackers, who then stole personal information.

The Australian

Attorney-General calls for more data sharing

Friday, 23 September 2016

Byline: Annabel Hepworth

Section: general

Canberra - The Attorney-General's Department has thrown its weight behind calls for more sharing of data across government in a fillip to some of the nation's most powerful regulators.
The department has pointed to NSW laws on data sharing as a model the government could look to. The move comes after the Australian Taxation Office has pushed for a review of decades-old confidentiality rules that restrict the sharing of personal data across government, while the Australian Securities & Investments Commission also wants to able to secure a wider scope of intelligence.

"The complexity of the current legislative regime can lead to a perception that the use and sharing of data within government is more restricted than it is in reality," the department says.

"Further, this complexity does give rise to genuine barriers to use of data across government including where secrecy provisions may operate ... If real or perceived barriers prove insurmountable to facilitate data sharing between agencies under current legislative settings, one option would be to introduce legislative changes to address cultural and systemic barriers to data use and sharing." The department also says that while public servants often point to concerns such as security or privacy, "the real issue can be a reluctance to make data available." The comments are contained in a new submission to an inquiry by the government's chief micro-economic adviser.

The Productivity Commission inquiry was called by the government after the Murray inquiry and the Harper inquiry both called for more reviews of the use of data.

The government is of a view that greater data sharing could use technology to drive efficiency. Last year, as part of the $1 billion innovation statement, the government released an open data policy.

However, critics have raised privacy concerns.

The Business Council of Australia has told the inquiry that governments should make their data more available. "When done appropriately, this can promote greater transparency, increased effectiveness of government services and broader innovation," the council told the review.Lateral Economics has estimated that greater open data could add $16bn a year to the economy, helping to deliver on the G20's target of boosting growth. Others groups such as the Actuaries Institute have told the inquiry that public access to information from bodies such as the ATO, Treasury and the Australian Prudential Regulation Authority would allow the financial services sector to develop products that meet the needs of consumers.

New York Times

Yahoo Hackers Plundered Data on 500 Million

Friday, 23 September 2016

Byline: Nicole Perlroth

Section: general

San Francisco - Yahoo announced on Thursday that the account information of at least 500 million users was stolen by hackers two years ago, in the biggest known intrusion of one company's computer network.

In a statement, Yahoo said user information -- including names, email addresses, telephone numbers, birth dates, encrypted passwords and, in some cases, security questions -- was compromised in 2014 by what it believed was a "state-sponsored actor."

While Yahoo did not name the country involved, how the company discovered the hack nearly two years after the fact offered a glimpse at the complicated and mysterious world of the underground web.

The hack of Yahoo, still one of the internet's busiest sites with one billion monthly users, also has far-reaching implications for both consumers and one of America's largest companies, Verizon Communications, which is in the process of acquiring Yahoo for $4.8 billion. Yahoo Mail is one of the oldest free email services, and many users have built their digital identities around it, from their bank accounts to photo albums and even medical information.

Changing Yahoo passwords will be just the start for many users. They'll also have to comb through other services to make sure passwords used on those sites aren't too similar to what they were using on Yahoo. And if they weren't doing so already, they'll have to treat everything they receive online with an abundance of suspicion, in case hackers are trying to trick them out of even more information.

The company said as much in an email to users that warned it was invalidating existing security questions -- things like your mother's maiden name or the name of the street you grew up on -- and asked users to change their passwords. Yahoo also said it was working with law enforcement in their investigation and encouraged people to change up the security on other online accounts and monitor those accounts for suspicious activity as well.

"The stolen Yahoo data is critical because it not only leads to a single system but to users' connections to their banks, social media profiles, other financial services and users' friends and family," said Alex Holden, the founder of Hold Security, which has been tracking the flow of stolen Yahoo credentials on the underground web. "This is one of the biggest breaches of people's privacy and very far-reaching."

The Yahoo hack also adds another miscue to what has been a troubled sale of a long-troubled company. In July, Verizon said it would acquire the internet pioneer, roughly a month before Yahoo security experts started looking into whether the site had been hacked. It is unclear what effect, if any, the breach will have on Yahoo's sale price.

In a statement on Thursday, a Verizon spokesman, Bob Varettoni, said his company learned of the breach of Yahoo's systems only two days ago and had "limited information and understanding of the impact."

It is unclear whether security testing -- such as a test to see if security experts could break into the Yahoo network -- was performed as part of Verizon's due diligence process before it agreed to the acquisition.

But such security is often overlooked by investors, even though breaches can result in stolen intellectual property, compromised user accounts and class-action lawsuits. To date, no law requires such security checks as part of due diligence.

"Cybersecurity can absolutely affect a valuation, and these are important questions that investors need to be asking," said Jacob Olcott, vice president of BitSight Technologies, a security company.

Yahoo said it learned of the data breach this summer after hackers posted to underground forums and online marketplaces what they claimed was stolen Yahoo data. A Yahoo security team was unable to verify those claims. But what they eventually found was worse: a breach by what they believe was a state- sponsored actor that dated back to 2014.

A potential breach of Yahoo's systems was first reported by the tech news site Recode early Thursday morning.

The first sign that something was amiss appeared in June, when a Russian hacker who goes by the user name Tessa88 started mentioning, in underground web forums, a new trove of stolen Yahoo data, Mr. Holden said. In July, Tessa88 supplied a sample of the stolen collection to people in the so-called underground web for authentication.

The sample contained valid Yahoo user accounts, but it was unclear whether the data was from a breach of a third-party service or Yahoo itself. And it was not clear whether it came from a recent Yahoo breach or a previous incident in 2012, when the internet service acknowledged that more than 450,000 user accounts were compromised.

Then, in August, a second hacker who goes by the alias Peace of Mind began offering a large collection of stolen Yahoo credentials -- including user names, easily cracked passwords, birth dates, ZIP codes and email addresses -- on a site called TheRealDeal, where hackers can buy and sell stolen data, Mr. Holden said.

TheRealDeal uses Tor, the anonymity software, and Bitcoin, the digital currency, to hide the identities of buyers, sellers and administrators who are trading attack methods and stolen data.

After looking into that data, Yahoo did not find evidence that the stolen credentials came from its own systems. But it did find evidence of a far more serious breach of its systems two years earlier.

Two years is an unusually long time to identify a hacking incident. According to the Ponemon Institute, which tracks data breaches, the average time it takes organizations to identify such an attack is 191 days, and the average time to contain a breach is 58 days after discovery.

Security experts say the breach could bring about class-action lawsuits, in addition to other costs. An annual report by the Ponemon Institute in July found that the costs to remediate a data breach is $221 per stolen record. Added up, that would top Yahoo's $4.8 billion sale price.

Thursday afternoon, Senator Mark R. Warner, a Democrat from Virginia and former technology executive, issued a statement that said the "seriousness of this breach at Yahoo is huge."

He weighed in with a call for a federal "breach notification standard" to replace data notification laws that vary by state. Senator Warner added that he was "most troubled" that the public was only learning of the incident two years after it happened.

New York Times

Email Hack Details Movements of Clinton, Biden and Michelle Obama

Friday, 23 September 2016

Byline: Michael D. Shear, Matthew Rosenberg

Section: general

Washington - Hackers on Thursday posted hundreds of emails from a young Democratic operative that contained documents detailing the minute-by- minute schedules and precise movements of the vice president, the first lady and Hillary Clinton during recent campaign fund-raisers and official political events.
The emails included names and cellphone numbers of numerous Secret Service agents, spreadsheets with the names and Social Security numbers of campaign donors, and PowerPoint presentations showing step-by-step directions for where officials like Vice President Joseph R. Biden Jr. should walk when they arrived at events.

The hackers who posted the emails also distributed what they claimed was a scanned image of the information page from Michelle Obama's passport, though the authenticity of the image could not be verified.

The emails were stolen from the personal Gmail account of the Democratic operative, Ian Mellul. They reveal how widely White House officials, Clinton campaign operatives and Secret Service agents have exchanged detailed and sensitive information with people using personal email accounts.

There is no indication that Mr. Mellul, 22, who was in effect working as a freelancer when the White House or the Clinton campaign needed help, did anything wrong, and government officials declined to talk about the use of the private account.

About a year and a half's worth of emails from Mr. Mellul's account were posted late Wednesday by the website DCLeaks.com, which earlier this month released a batch of emails from the personal account of Colin L. Powell, the former secretary of state, in which he voiced his scorn for Donald J. Trump, the Republican presidential nominee, and his personal peeves with Mrs. Clinton, his Democratic opponent.

The newly released emails do not provide specific security details, but they do reveal the types of movements that top political officials make at such events. If emails were hacked before an event, that could present a more serious security issue.

One document instructed Mr. Biden to walk up four steps at a loading dock in Cleveland before climbing 26 steps to a holding room. Another used blue arrows to show the route Mrs. Clinton should walk through a donor's house in Houston. Both documents included close-up pictures of the event locations.

Mr. Mellul, who volunteered to work as an advance staff member for the White House and the Clinton campaign as he finished his undergraduate education at George Washington University in Washington, declined to comment. "I've got to hang up," he said Thursday when reached on his cellphone.

Cathy L. Milhoan, the director of communications for the Secret Service, said the agency was "aware of the alleged email hacking of a White House staffer.

"Obviously the Secret Service is concerned any time unauthorized information that might pertain to one of the individuals we protect, or our operations, is allegedly disclosed," she added.

An F.B.I. spokesman said the bureau was looking into the hacking. Josh Earnest, the White House press secretary, said that officials took "any reports about a cyberbreach seriously" and that the episode was "something we are taking a close look at."

DCLeaks.com is a relatively new website that has posted documents taken from the accounts of prominent figures like Gen. Philip M. Breedlove, the former commander of NATO forces in Europe, and George Soros, a wealthy backer of liberal causes. On the site, its creators describe themselves as American "hacktivists" who aim to "publish a large amount of emails from top-ranking officials and their influence agents all over the world."

Mr. Mellul hardly fits either description. His low-level job ranks just above that of an intern.

The emails from his account document the often mundane process that White House or campaign staff members go through to prepare for an event, including setting up stages, organizing photo lines,

arranging for lecterns and coordinating with the Secret Service about getting clearances for all of the people the politician will encounter along the way.

One email contained a spreadsheet with the names and Social Security numbers of almost 100 people scheduled to attend a Houston fund-raiser for Mrs. Clinton. In another exchange, a Secret Service agent discussed how many official "pins" would be provided for hotel staff members to have access to an event. After Mr. Mellul said the hotel had requested 50 Secret Service pins, the agent wrote, "Yikes."

Several of the emails contain what is referred to as a "movement document" or a "site diagram" involving the vice president, the first lady or Mrs. Clinton. Those emails were often sent to a large number of people, including Mr. Mellul. In other cases, Mr. Mellul emailed copies of the documents to other campaign or government officials, including Secret Service officials.

"Good morning all," Mr. Mellul wrote on May 20, the day of a Hillary for America fund-raiser. "Please find the attached site diagram for Houston's H.F.A. finance event this evening. Please let us know if you have any questions or concerns. Ian."

The emails begin in February 2015, when Mr. Mellul was in the honors program and studying political science. In the messages, Mr. Mellul comes across as a conscientious and courteous young man whose friends would email him for help with their school essays and résumés.

After high school, he jumped into the intern circuit that feeds into entry-level jobs in Washington. In 2014, he received a coveted internship at the White House and later parlayed the connections he had made as an intern into low-level freelance work for the White House.

His tryout, it appears, was helping Mrs. Obama's team at a lunch for congressional spouses on April 15, 2015.

In an email two days before the event, Lindsay Drewel, a Washington public relations executive, wrote to Anthony R. Bernal, the deputy chief of staff for Jill Biden, the vice president's wife, that if Mr. Mellul "can survive that crazy event (which we know he will) he'll be ready to go! Haha."

After the event, Mr. Mellul even included a Secret Service agent in his round of emails thanking those with whom he had worked. And the day after the lunch, the first lady's office reached out again to see if he could help with an event in Virginia.

Mr. Mellul was excited, and in an email to a friend later that day, he noted that he had been told "it takes a few good trips/events before they really trust you."

On April 20, 2015, five days after his first job with Mrs. Obama's team at the congressional lunch, Mr. Mellul described himself as "on the advance team" for the first lady in an email to his professor saying he might miss class because of an event.

Radio-Canada - Nouvelles (site web) avec CBC

Ottawa a autorisé l'utilisation de dispositifs d'espionnage des communications

Friday, 23 September 2016

Byline: Journaliste maison

Section: general

Ottawa - Le ministère de la Sécurité publique du Canada a maintes fois autorisé l'utilisation par le Service canadien du renseignement de sécurité (SCRS) et la Gendarmerie royale du Canada (GRC) de dispositifs pour espionner les communications des Canadiens, révèlent des documents obtenus par CBC. Ceux-ci sont lourdement caviardés et ne permettent pas d'identifier les fabricants ou les dispositifs en question.

On y apprend ainsi que le ministère a approuvé des demandes de la GRC, du SCRS et du ministère de la Défense nationale pour qu'ils accordent plus d'une douzaine de licences à une société anonyme afin de posséder, fabriquer ou vendre des dispositifs « utilisés principalement pour l'interception des communications ».

Les licences, d'une durée d'un et deux ans, ont été émises à partir de 2015 et, dans certains cas, s'étendent jusqu'en 2018.

Elles ont été accordées en vertu de l'article 191 du Code criminel, qui interdit l'utilisation de technologie pour l'interception clandestine de communications privées, à moins que l'autorisation soit donnée par le ministère de la Sécurité publique.

La GRC a refusé de divulguer la nature de ces licences. Le SCRS n'a pas voulu commenter la nouvelle.

StingRay, un dispositif contesté

Il n'y a pas de politique claire sur la façon dont la police utilise la technologie à des fins de surveillance, ce que dénoncent des défenseurs de la vie privée.

Le mois dernier, la police de Vancouver a admis avoir utilisé le système de surveillance téléphonique StingRay, un appareil de la taille d'une petite valise dont se servent les agences de renseignement du monde entier.

Ce dispositif contesté dupe les téléphones cellulaires à proximité en envoyant des signaux semblables à ceux des tours cellulaires. Une fois connecté, un utilisateur de StingRay peut amasser de l'information transmise par le téléphone, comme son emplacement ou ses messages textes.

StingRay est utilisé également par la GRC pour ses enquêtes, ont révélé récemment des dossiers de tribunaux dans l'affaire Salvatore Montagna. Pour mener son enquête, la GRC avait intercepté des dizaines d'appels des accusés impliqués dans le meurtre de ce mafioso, près de Montréal.

Associated Press

Blazes at Iran petrochemical plants raise suspicions of cyberattack

Friday, 23 September 2016

Section: general

Dubai - A series of fires at Iranian petrochemical plants and facilities have raised suspicions about hacking potentially playing a role, with authorities saying that "viruses had contaminated" equipment at several of the affected complexes.
Iran officially insists the six known blazes over the span of three months weren't the result of a cyberattack. However, the government acknowledgment of supposedly protected facilities being infected points to the possibility of a concerted effort to target Iranian infrastructure in the years after the Stuxnet virus disrupted thousands of centrifuges at a uranium enrichment facility.

Among the worst of the fires was a massive, days-long inferno in July at the Bou Ali Sina Petrochemical Complex in Iran's southwestern province of Khuzestan. Insurance officials later estimated the damage at some $67 million. Authorities preliminarily blamed the blaze on a leak of paraxylene, a flammable hydrocarbon, without elaborating.

Initially, Brig. Gen. Gholam Reza Jalali, who heads an Iranian military unit in charge of combatting cybersabotage, dismissed any notion that the fires could have been caused by hacking. Iran's aging oil pipelines and plants, hit hard by years of Western sanctions, have seen a rapid push to increase production this year to take advantage of the nuclear deal with world powers. Iran also faces occasional separatist attacks on its pipelines.

But on Aug. 27, Jalali acknowledged Iran's petrochemical industry had been the target of cyberattacks. He put the blame on imported and installed components at the facilities.

"The viruses had contaminated petrochemical complexes," he said, according to a report by the state-run IRNA news agency. "Irregular commands by a virus may cause danger."

But despite the infections, Jalali said cyberattacks had no hand in the fires and explosions. He also said "defensive measures are underway," without elaborating. Beyond Jalali's vague comments, what actually infected the plants remains unclear.

It's unknown if Iran, which has boosted its own cyberwarfare and defense capabilities in recent years, has sought outside assistance in its investigation. The Russian antivirus firm Kaspersky Lab, whose analysts were among the first to investigate Stuxnet, said it wasn't involved in investigating this outbreak and declined to comment.

However, Jalali's comments that the viruses spread through imported parts suggests a concerted effort by a foreign power. Iran likely relied on black-market parts while the country faced international sanctions, said Robin Mills, a Dubai-based oil industry analyst and CEO of Qamar Energy.

"Maybe they couldn't always get the high-quality parts coming from countries who are sanctioning it and had to get second-hand parts or parts not of the right specifications and put these pieces together without a lot of international expertise," Mill said. "In that case, of course, accidents can happen." But the number of fires in row has raised suspicions of Iran being targeted.

Such an attack "requires a lot of resources" that individual hackers would not have, said Idan Udi Edry, a former Israeli air force captain who now is the CEO of Nation-E, a cybersecurity firm specializing in protecting industrial systems.

Asked if the Iranian blazes were the result of hacking, Edry said he was "100- percent" sure, based on his own company's experience and surveillance.

"No company, organization or nation in the world would like to admit they've been hacked," he said. "This specific attack was exact the same one (like Stuxnet), only on a different critical infrastructure area."

However, Ralph Langner, another industry expert who studied the Stuxnet virus, said it seemed "unlikely" the fires were caused by cyberattacks, though his firm hasn't investigated.

Stuxnet, widely believed to be an American and Israeli creation, infected thousands of centrifuges at the Natanz uranium enrichment plant at the height of Western fears over Iran's nuclear program. The virus targeted the machines through the industrial control systems that set their speeds, causing them to spin out of control and destroy themselves.

Such control devices, used for years in fields ranging from utility companies to the oil industry, are especially susceptible to hackers. That's because they weren't initially envisioned to be connected to the internet and that most security attention focuses on consumer products such as email and laptops.

While the Stuxnet virus was the most famous hack to exploit them, there have been others that caused real-world destruction. German authorities say a steel mill sustained massive damage to its blast furnace in 2014 after hackers took control of its industrial control systems, though details on the incident remain few.

Iranian hackers also allegedly penetrated the controls of a small dam less than 30 kilometers (20 miles) away from New York City. That dam's system, however, was connected directly to the internet, while the Iranian oil industry is believed to be "air-gapped" -- or not connected directly to the web.

Meanwhile, hackers of all kinds appear to be increasingly targeting industrial control systems. In the US alone, a Homeland Security center tasked with handling such attacks reported it responded to 295 incidents in 2015, up from 245 the year before.

"Cyberattacks are no longer how to steal information," Edry said. "These are attacks that are meant to shut down a country."

Le Temps (Suisse)

Réseau câblé: le futur mode opératoire des espions suisses

Friday, 23 September 2016

Byline: Mehdi Atmani

Section: general

Berne, Suisse - Surveillance L'exploration du réseau câblé prévue par la loi sur le renseignement cristallise les critiques car, aux yeux de certains, elle permettrait une surveillance de masse. Mais, techniquement, de quoi s'agit-il?
« Pêche au chalut » ou « pêche au harpon » ? Les nouveaux moyens d'action dont le Service de renseignement de la Confédération (SRC) devrait se doter avec la loi sur le renseignement (LRens) lui permettront-ils de mener une surveillance ciblée ou de masse? C'est principalement sur ce point que le projet de loi soumis en votation le 25 septembre divise la société civile et les partis. Car elle oppose l'impératif sécuritaire dans un contexte de lutte contre le terrorisme au respect des libertés fondamentales du citoyen.

Dans la future boîte à outils du SRC, la mesure de surveillance par l'exploration du réseau câblé cristallise toutes les critiques. La LRens autorisera en effet le SRC à intercepter en continu toutes les communications internationales qui transitent par la Suisse via le réseau câblé. Avec l'aval du Tribunal administratif fédéral et de la Délégation pour la sécurité du Conseil fédéral, le SRC pourra filtrer les courriers électroniques, procéder à des écoutes téléphoniques par Internet, et rechercher des informations par catégorie de mots clés. Au hasard: djihadisme, islam, finance...

« Menace pour la sécurité intérieure »

Avec l'exploration du réseau câblé, le mode opératoire du SRC rappelle celui du GCHQ - l'agence de renseignement britannique - et son programme Tempora. En juin 2013, Edward Snowden révélait que le GCHQ surveillait les câbles sous-marins reliant l'Amérique du Nord. L'agence interceptait les données pour les partager avec la NSA. En Suisse, la surveillance se fera sur les noeuds où convergent et transitent les données. Le SRC ne pourra rechercher que des informations sur des événements importants en matière de politique de sécurité se produisant à l'étranger. Les données qui ne correspondraient pas à ce critère devront être détruites. « En théorie », s'inquiètent les adversaires de la LRens, qui réunissent les Jeunes socialistes, les Verts et le Parti pirate.

L'habilitation du SRC est également valable dans le cas d'une « menace pour la sécurité intérieure » ainsi que pour « préserver les intérêts nationaux d'une grande importance » . En d'autres termes, seules les données transitant par le réseau câblé suisse vers des fournisseurs étrangers seront surveillées. L'utilisation des données collectées entre expéditeur et destinataire situés en Suisse sera interdite. Pour autant que leurs adresses e-mail soient enregistrées auprès d'un fournisseur d'accès à Internet (FAI) en Suisse.

Prenons l'exemple d'un e-mail envoyé de Lausanne à Saint-Gall. Si le destinataire utilise une adresse Gmail ou du service de messagerie allemand GMX, le courriel transitera par les serveurs de Google à l'étranger ou par l'Allemagne. Il traversera momentanément les frontières helvétiques et pourrait donc être intercepté. Le projet de loi précise que « les exploitants suisses de réseaux câblés ainsi que les fournisseurs suisses de prestations de télécommunication » fournissent « des renseignements sur les itinéraires des flux de données et, sur ordre, en détournant les flux de données en question » .

Pour les opposants à la LRens, l'exploration du réseau câblé par catégorie de mots clés est une méthode de collecte et d'analyse de l'information « archaïque » . Selon eux, toutes les agences internationales de renseignement n'utilisent plus seulement des mots clés, mais surtout des algorithmes. Ceux-ci viennent enrichir des bases de données dans lesquelles l'information interceptée est structurée, puis mise en relation et enrichie avec d'autres informations, dites secondaires: adresse postale, abonnement de téléphone mobile, profil LinkedIn, soit les données personnelles d'un citoyen.

Cette technique de « Deep Learning Management » permet aux agences d'affiner au maximum l'information et d'en tirer le plus de sens possible, comme un Google du renseignement. Si les services

suisses ont l'objectif de se mettre au niveau des techniques de collecte et d'analyse des agences internationales, ils devront employer les mêmes méthodes, préviennent les opposants à la LRens. « Les garde-fous prévus par la loi n'y changeront rien », insiste Guillaume Saouli, le président du Parti pirate.

Pour les opposants à la LRens, l'exploration du réseau câblé par mots clés est archaïque

Le Figaro

Sur les réseaux sociaux, Daech se fait plus discret

Friday, 23 September 2016

Byline: Fanny Lauzier

Section: general

Paris - La maîtrise des réseaux sociaux et des codes du divertissement permet à Daech de recruter des djihadistes de plus en plus jeunes.
Facebook, Twitter, Instagram ou encore Snapchat... Depuis deux ans, l'État islamique avait pignon sur rue sur les réseaux sociaux préférés des adolescents. Des forums d'initiés, la propagande de l'organisation terroriste s'était largement déplacée, en 2014, sur les canaux de transmission habituels de la webculture.

Pour recruter le plus largement possible, les partisans de Daech ont utilisé tous les codes d'Internet, étant eux-mêmes, pour beaucoup, des « digital natives » . « Ils ont autour de 25 ans et sont eux-mêmes usagers de ces réseaux » , explique David Thomson, journaliste spécialiste du djihadisme. Daech s'était largement approprié les symboles de la culture Web : ici, une photo de combattant armé d'une kalachnikov câlinant un chaton, là, des selfies de soldats s'immortalisent à bord de tanks ou autour de la piscine d'un hôtel abandonné en Syrie...

Mais l'âge d'or de la communication de l'EI touche peut-être à sa fin. « Depuis quelques mois, on note que Daech est de moins en moins présent sur Twitter. La phase d'euphorie est clairement passée » , constate David Thomson. Depuis la promulgation de la loi Urvoas, le 3 juin dernier, les sympathisants de Daech qui vivent en France sont plus vigilants. En effet, toute consultation « habituelle » de sites Internet ou réseaux sociaux faisant l'apologie d'actes terroristes est désormais punie par la loi. « Depuis, plus aucun partisan basé en France ne se revendique comme tel sur les réseaux sociaux » , observe David Thomson.

Même depuis la zone irako-syrienne, la communication marque le pas. « Des consignes de silence ont été données. Ils ne veulent plus voir circuler de contenus non officiels. La période des selfies est finie. » Les superproductions diffusées depuis le califat, qui reprenaient tous les codes hollywoodiens et des jeux vidéo ultraviolents, se sont aussi raréfiées. « Beaucoup de djihadistes des brigades médiatiques ont été tués. Ils ne sont plus en capacité de produire. »

Toutefois, l'EI pratique un « opportunisme digital » , rappelle Pascal Lardellier, professeur à l'université de Bourgogne et auteur de Génération 3.0, enfants et ados à l'ère des cultures numérisées . « Les partisans de Daech jouent à saute-mouton avec les technologies. Hier actifs sur Twitter et Facebook, ils sont aujourd'hui présents sur Telegram » , une application de communication chiffrée permettant d'échanger de façon sécurisée. C'est d'ailleurs sur cette plateforme que les deux terroristes de Saint-Étienne-du-Rouvray, âgés de 19 ans, se sont rencontrés. Mais sur Telegram, la propagande n'a pas le même impact : « C'est une sphère confidentielle. Il faut donc en faire partie pour avoir accès aux contenus » , nuance David Thomson.

Le Figaro

Sur les réseaux sociaux, Daech se fait plus discret

Friday, 23 September 2016

Byline: Fanny Lauzier

Section: general

Paris - La maîtrise des réseaux sociaux et des codes du divertissement permet à Daech de recruter des djihadistes de plus en plus jeunes.
Facebook, Twitter, Instagram ou encore Snapchat... Depuis deux ans, l'État islamique avait pignon sur rue sur les réseaux sociaux préférés des adolescents. Des forums d'initiés, la propagande de l'organisation terroriste s'était largement déplacée, en 2014, sur les canaux de transmission habituels de la webculture.

Pour recruter le plus largement possible, les partisans de Daech ont utilisé tous les codes d'Internet, étant eux-mêmes, pour beaucoup, des « digital natives » . « Ils ont autour de 25 ans et sont eux-mêmes usagers de ces réseaux » , explique David Thomson, journaliste spécialiste du djihadisme. Daech s'était largement approprié les symboles de la culture Web : ici, une photo de combattant armé d'une kalachnikov câlinant un chaton, là, des selfies de soldats s'immortalisent à bord de tanks ou autour de la piscine d'un hôtel abandonné en Syrie...

Mais l'âge d'or de la communication de l'EI touche peut-être à sa fin. « Depuis quelques mois, on note que Daech est de moins en moins présent sur Twitter. La phase d'euphorie est clairement passée » , constate David Thomson. Depuis la promulgation de la loi Urvoas, le 3 juin dernier, les sympathisants de Daech qui vivent en France sont plus vigilants. En effet, toute consultation « habituelle » de sites Internet ou réseaux sociaux faisant l'apologie d'actes terroristes est désormais punie par la loi. « Depuis, plus aucun partisan basé en France ne se revendique comme tel sur les réseaux sociaux » , observe David Thomson.

Même depuis la zone irako-syrienne, la communication marque le pas. « Des consignes de silence ont été données. Ils ne veulent plus voir circuler de contenus non officiels. La période des selfies est finie. » Les superproductions diffusées depuis le califat, qui reprenaient tous les codes hollywoodiens et des jeux vidéo ultraviolents, se sont aussi raréfiées. « Beaucoup de djihadistes des brigades médiatiques ont été tués. Ils ne sont plus en capacité de produire. »

Toutefois, l'EI pratique un « opportunisme digital » , rappelle Pascal Lardellier, professeur à l'université de Bourgogne et auteur de Génération 3.0, enfants et ados à l'ère des cultures numérisées . « Les partisans de Daech jouent à saute-mouton avec les technologies. Hier actifs sur Twitter et Facebook, ils sont aujourd'hui présents sur Telegram » , une application de communication chiffrée permettant d'échanger de façon sécurisée. C'est d'ailleurs sur cette plateforme que les deux terroristes de Saint-Étienne-du-Rouvray, âgés de 19 ans, se sont rencontrés. Mais sur Telegram, la propagande n'a pas le même impact : « C'est une sphère confidentielle. Il faut donc en faire partie pour avoir accès aux contenus » , nuance David Thomson.

Ottawa Citizen
Quantum computing will cripple encryption methods within decade, spy agency chief warns
Saturday, 24 September 2016
Byline: Ian MacLeod

Ottawa - The head of Canada's electronic spy agency warned Friday the advent of super-fast quantum computers will cripple current encryption methods for securing sensitive government and personal information within a decade.
In a rare public speech, Greta Bossenmaier, chief of the Communications Security Establishment, said cryptologists at the CSE and around the world are racing to find new cryptographic standards before Y2Q - years to quantum - predicted for 2026.

She is the third senior CSE official this week to warn publicly of the threat quantum computing poses to widely used public key cryptography (PKC), protecting sensitive data transmissions from hackers, hacktivists, foreign state spies and other malicious actors.

The CSE is best known as a spy agency -- it collects, decrypts and analyzes phone calls, faxes, emails, tweets, satellite and other electronic signals emanating from adversarial foreign nations and overseas threat actors. But it's also mandated to protect government computer systems and networks, and the information they carry.

Already, federal computer systems are "probed" more than 100 million time a day by suspected malicious actors searching for vulnerabilities.

Potentially every Canadian citizen could be vulnerable

Now, "the challenge of protecting systems is about to get a lot harder thanks to quantum computing," Bossenmaier told an Ottawa conference of the Canadian Association for Security and Intelligence Studies.

"Nearly every company, nearly every organization, nearly every government currently employs some form of encryption," she said. "It's also part of almost every Canadians' daily life, whether we know it or not. Our credit cards, debit cards, work and building passes, just to name a few examples, all work on some form of encryption.

"It's not really a question of if, it's a question of when. The clock has started to tick. So unless we collectively get ahead of the quantum challenge and rethink encryption, the systems and information of companies, of governments, of organizations, of citizens -- potentially every Canadian citizen -- could be vulnerable."

Her warnings follow remarks Monday by David Sabourin, CSE's manager of cryptographic security.

He told a Toronto conference on quantum-safe computing if the 2026 Y2Q prediction holds, "we're in trouble," according to an IT World Canada report.

Scott Jones, CSE's deputy chief of IT security, responsible for securing federal information systems, reportedly told the gathering, "I think we are already behind."

Quantum computing is based on quantum mechanics, the branch of physics that explores and explains the set of laws governing the atomic and subatomic world of atoms, electrons, photons and other particles. While traditional computers use long strings of bits to encode either a zero or a one, quantum computers use quantum bits, or qubits.

Two remarkable properties of qubits - the ability to be in multiple states at the same time (superposition) and the phenomenon in which pairs or groups of qubits can only be described in relation to one another even if they're on opposite sides of the universe (entanglement) - allow quantum computing to be exponentially faster and more capable at factoring very large numbers, which is the basis of current cryptology.

Today's computers simply can't solve what amounts to mathematical problems blocking unauthorized access to encrypted information. But the immense processing power of quantum computers will someday, rendering current PKC ineffective, if not useless.

Yet, as Bossenmaier noted, once the new class of technology becomes a commercial reality, it promises tremendous opportunities that could result in significant advances in science, medicine and engineering.

In April, the Toronto Star obtained a CSE memo discussing how to defend against the quantum threat. The document did not make it clear if the organization also is exploring quantum technology to decrypt intercepted computer communications, the newspaper said.

Toronto Star
National electronic intelligence agency executive calls for 'rational debate' on encryption
Monday, 26 September 2016
Byline: Alex Boutilier

OTTAWA-Canadians are being encouraged to ask more questions about the security of their electronic devices from an unlikely source: an executive at the country's electronic intelligence agency.
Scott Jones, the deputy director of IT security at the Communications Security Establishment, said Canadians need to start taking a greater interest in how their electronic devices protect personal information.

"We should be asking when we go and buy the stuff we have at home, OK, tell me how it's being protected," Jones said in an interview.

"If it's my cellphone, does it have encryption if I lose it? Can somebody just read the data off of it or not? We need to start asking questions like that ... We need to start helping each other, and helping citizens, helping businesses, helping the government when we're buying these products they need to be secure by default."

It may surprise some to hear an employee at CSE counselling Canadians to protect their private information. The agency, which has largely operated in secret since its creation at the end of the Second World War, was thrust into the spotlight after U.S. whistleblower Edward Snowden's disclosures.

CSE is part of the Five Eyes alliance, which includes security agencies in the United States, the United Kingdom, Australia and New Zealand. Snowden's disclosures drew back the curtain on mass surveillance programs used by those countries, including programs that scooped up their own citizens' communications.

Jones' comments also come as law enforcement agencies in the U.S. and Canada are forcefully arguing for limiting citizens' ability to secure their information through encryption programs -- calling for so-called "backdoors" that would let authorities decode the data.

When this is pointed out, Jones agreed the encryption debate is a difficult one to resolve.

"I don't take it personally, because I think it's a really important question," Jones said.

"(We need) a rational debate over the tools that law enforcement needs to do its job, right? I trust law enforcement to keep me safe, but I also trust the legal system to protect my privacy as well, and to find a balance. But we haven't been able to have those conversations in this country (yet)."

While police and intelligence agencies argue about whether citizens should have access to strong encryption, the federal government, on the other hand, is trying to improve its own electronic defences.

Known as "Part B" of CSE's mandate, cyber- defence operations require the agency to work with a host of other federal departments to try and protect government information -- including Canadians' personal information.

For serious cyberattacks, the response could include the RCMP, CSIS, Public Safety, Shared Services Canada, even Global Affairs and the Privy Council Office.

"Cyber is not a singular dimensional problem, it's not just a technical issue or the computer system, it's also about the objective of the compromise or what the threat actor was trying to obtain," Jones said.

"You can't have the master of cyber in a single department, because to do that you'd have to create the department of everything."

The Liberal government is in the middle of a wide-ranging review of Canada's approach to cyber security, and Jones expects the encryption debate to figure into that larger discussion.

The government has also pledged to review Ottawa's overall national security regime, beginning with increased oversight from a parliamentary committee, and to roll back some of the powers granted to intelligence agencies through the Conservatives' controversial terrorism law, Bill C-51

Hilal
Cyber World and Espionage
Monday, 26 September 2016
Byline: Mudassar Jehangir

Undisclosed placeline - The official statistics suggest that more than half of Pakistani population carries a mobile phone, and the craze is rising exponentially. From a small kid to a mature adult, everyone wants to get hold of the latest smart phone but out of all the people who believe they cannot live without a cell phone, merely a negligible percentage knows what actually a smart phone is. A dominant part of our mobile phone subscriber base does not want to think beyond selfies, cameras, and social media. Probably we just don't care, but a computer user is as vulnerable to a cyber criminal as a mobile phone user is. I assume we never have time to read the manual before installing any software. We never bother and believe in hit-and-trial methods. Mobile phone technology was boastfully introduced in Pakistan in the late 90s. However, it is still indigestible how all those strategists could never find few moments to sit together and chalk out some useful rules and regulations to regulate the use of this technology. In 2016, we finally have a document called Prevention of Electronic Crimes Bill 2015 which is also somewhat controversial and not comprehensive enough as the Pakistan Electronic Crimes Ordinance (PECO) in 2008.

We were all living a simple life. Therefore, the odds of technology have always been an alien concept to us but with the establishment of technology parks, centrally controlled metro train systems, several e-governance initiatives and a series of announcements of digitizing the entire society make us evenly exposed to the tyranny of cyberspace. If we don't equip ourselves with the arsenal, we would never be safe in this e- world. Only a set of clauses won't make a difference. Our society needs a change of mindset and the realization of the fact that we are not protected even inside our homes.

The smart phones have every necessary hardware and pre-built softwares that can even count the number of breaths we take. It keeps communicating with the nearest tower all the time and that tower to the entire system of telecommunication that has encapsulated the whole world like clouds. Whatever we do, is going into the safe repositories of large organizations. There is no way you can stop the auto-activation of any feature of your mobile phone. And what if you figure out such spying, where would you complain in Pakistan? We have no adequate forum....

Just to give you a little understanding, 97% of the smart phones in Pakistan are based on Android OS and for activating all the apps you need to log in through your Gmail ID. Now, how secure is your Gmail solely depends on your level of information and exposure to the technology. According to a survey, most of the users in Pakistan don't have sufficient knowledge of configuring proper security levels inside their smart phones. Ever wonder why a picture from past suddenly pops up on your screen even when you had deleted it long ago. It happens because Google, on its servers, keeps a record of every tiny thing you do through your mobile phone.

To breach the security of servers and steal the data, there exist a lot of ways. Or they (in the case of more individuals) just need to activate a virus inside our phone that you must have erroneously installed, unknowingly, because it was embedded into a free game app that you or your kid downloaded a few days ago. In this case, you will no more be the owner of your phone. I rarely believe in the claims of software and security companies because even the most secure systems are a piece of cake to crack by a smart hacker.

This is why even the most secure companies on earth keep paying white hackers for improving the security bugs. A recent example is the USD 200,000 offer from Apple for finding loopholes into its products. This measure is a part of SOPs for strengthening the systems that clearly shows there is always room for the smartest guy to get in. If these companies are unable to secure themselves, where does a poor technology user stand in Pakistan?

Just recently child abduction went viral on social media and many days after it was realized by the authorities that certain groups on social media are also taking benefit of the situation and circulating news of fake abduction cases through Facebook and other social networking sites for creating a panic situation in the public. Interestingly, a high-ranking police official in Karachi came up with a confession of helplessness that he did not have enough resources to track people behind the mess.

Since we are relatively new to this world, we therefore don't have a clue about what's going on around us. Producing proper statistics on the rate and pattern of cybercrime in Pakistan is a far-sighted wish. Let's take the example of the most developed country, the U.S. A latest research done by BTB Security based on the data from the FBI, FTC, U.S. Justice Department and other vendors confirm that cybercrime has risen exponentially in the U.S. and despite all the tech-based measures, it is surging like anything.

The findings reveal that business data of 190 million users was compromised in 2015. The identity theft had gone up by more than double from 8.3 million in 2005 to 17.6 million registered cases in 2014. Similarly, ransomware which was once a sub-million dollar business has swelled to $ 24 million in 2015. When I asked BTB Managing Director, Ron Schlecht about what cybercrime would be like in next ten years, he responded with concerns about the infrastructure that creates the digital world. According to him, "Hardware and software are aging, and it will create a vacuum of expense and time for those who were defending it."

Today, security experts believe that cyber wars are imminent, and terrorist organizations will exploit the digital realm to inflict real physical damage.

A widely accepted fact in the U.S. is its critical infrastructure which is vulnerable to collapse, and its electronic voting system is equally vulnerable to cyber attack. Huffington Post reports that what is considered a remote possibility in the U.S. - cyber attacks throughout the most sensitive parts of the U.S. government - are now becoming commonplace.

Just to refresh your mind, we are talking about a country considered technologically aware and that exports the most secure security solutions to the world. Where do we put Pakistan on the map where more than half of the population keeps a mobile phone, and most of the devices are housing multiple mobile SIMs which unfortunately are not backed by proper documentation. Most would argue with me in favor of biometric SIM verification system but how fool proof a verification would be when NADRA is in the process of verifying the CNICs of more than 25 million families.

Cybercrime happens because we step in the cyber world, and you can't protect a nation today by just making a law stringent than ever. The technology we use for our comfort also opens the window for an outsider to peep in. We have to shut that window, and it can only be done through mass education. There should be an extensive exercise and involvement of people from all walks of life for making a comprehensive policy to meet the challenges of the cyber world. The cyber world should be a proper subject and must be made a part of the curriculum in our education system.

Jerusalem Post
Spies in space: The story of Israel's Ofek satellite program
Monday, 26 September 2016
Byline: Barbara Opall-Rome

Jerusalem - If you're looking for a story that captures Israeli innovation, cunning and can-do chutzpa, think spy satellites. Look to Ofek, the Hebrew word for horizon. It's all there in Israel's military satellite program, the newest of which - Ofek 11 - is struggling to stabilize itself in space after its launch earlier last week.
Inserted successfully into orbit by the country's homemade Shavit launcher, the newest and most advanced satellite is likely to soldier on in space, but with limited lifespan and ability to perform its high-resolution spy duties. White- knuckled technicians and program managers toiling around the clock at Israel Aerospace Industries' (IAI) ground control station near Ben-Gurion Airport are still hoping for a favorable ending to the latest chapter still unfolding. But like the chapters that have gone before, Ofek 11 represents the highs and lows of a story driven by strategic need and enhanced by its share of diplomatic intrigue. Conceived in secret, it's a story of battling the laws of physics; and struggling on a shoestring budget to build rockets strong enough to loft satellites small enough into retrograde orbit against Earth's eastward spin.

It's also a story of fortitude. How the euphoria of reaching space in 1988 was followed by bitter back-to-back failures that saw two satellites swallowed by the sea. And how the heroes of our story finagled their way back from the brink with the 1995 launch of Ofek-3, Israel's first operational imaging satellite whose progeny continue to fuel the regional power status of the Jewish state.

"Small countries can be great only if they dream big," said former president Shimon Peres. "With Ofek, we penetrated space and skepticism." (Israel launches new spy satellite, but trouble reported)

Interviewed before the stroke that befell the pioneer of Israel's aerospace and defense industry, Peres said Israel's small size makes it uniquely positioned as a "center of excellence" for advanced research and development. "Our advantage is creative, out-of- the-box thinkers who push the boundaries of what was deemed impossible." But with all due respect to Israel's senior statesman, this is where our tale takes a cautionary turn.

Because the flip side of this story is one of untapped potential and failure to leverage billions of dollars invested in military space to assure commercial competitiveness on the global market.

The US Futron Corp. consistently ranks Israel eighth in an annual competitiveness survey based on myriad criteria, including government investment, national space policy, the ability to attract financing and annual sales. In its latest Space Competitive Index (SCI), we have dropped to number nine.

"Israel continues to be a leader in space technology, but has limited commercial sales," Futron reported in its first SCI survey from 2008. The same holds true today.

"Although Israeli technology is high quality and generally cost-competitive, Israeli manufacturers have less global scale than their counterparts," Futron senior analyst Jonathan Beland told the Jerusalem Post Magazine. But let's go back.

Our story begins in the late 1970s. US President Jimmy Carter was proving relentless in prodding Israel and Egypt toward peace. In the run-up to Camp David, the era of Israeli Air Force reconnaissance flights over Sinai was about to end.

Plan Treasure was a top-secret forum where US and Israeli officials hashed out compensation to come from the 1978 accord. Among Israel's requests: access to imagery from US spy satellites.

"The Americans didn't even answer us; they ignored the request," recalls David Ivry, a retired major general who commanded the Israel Air Force at the time. That's when the indigenous Israeli satellite program started to gain traction. Ivry said. "We knew after the treaty was signed, we would be obliged not to violate Egyptian sovereignty by overflying their airspace as we used to do," he added.

Even prior to the US slow-roll, Israel had been dabbling in military satellite research. Rafael Ltd., then an R&D arm of the Defense Ministry had the lead, but all three Israeli government-owned firms were involved in aspects of rocketry.

In any case, Israel did not start from scratch with continuously upgraded versions of the three-stage Shavit rocket that launches Ofek into space.

From here our story turns to the courageous few who fought for funding as fiercely as the technological hurdles blocking their way.

Chaim Eshed is a key protagonist. He's now a retired brigadier general, teacher and chairman of the national committee for space R&D, but then a young Air Force lieutenant colonel working technical issues for military intelligence. Eshed ran the Ofek satellite part of the program, subsequently serving for decades as Israel's military space czar.

Another key character in our story is Uzi Rubin. An aeronautical engineer hailing from the IAI, Rubin headed the Shavit launch effort for the Defense Ministry and went on to establish Israel's missile defense organization.

Together they toiled in secret - without the benefit of external assistance or outside consultants - on tenuous funds, working with guys named Moshe Bar- Lev, Aby Har-Even, Ilan Porat and a few dozens of others involved in the effort.

Success was achieved in September 1988, when the Israeli-built Shavit launched a test satellite named Oz into space. With Oz - Hebrew for courage - Israel joined only seven other nations at the time to launch satellites in space.

Confidence grew with a second success. Just 18 months after the first Oz entered orbit, another Shavit launched Oz number 2, another test satellite capable of communicating with its ground-based operators, but not yet endowed with a payload to capture images from space.

As testament to their confidence of the horizon ahead, they changed the name of the satellite program from Oz to Ofek. But that horizon proved elusive with two failures that followed.

Problems with the Shavit rocket sent two Ofeks fully equipped with imaging cameras plummeting into the sea.

To this day, Israel only acknowledges one failure - of Ofek 2 in September 1994 - prior to the successful April 1995 launch of Ofek 3. The name change offered a convenient cover for public consumption, but those back-to-back failures put the program on borrowed time.

No courage and conviction would save them from another failure. "After the first failure, there was tremendous pressure to cancel the project. But we managed to continue," recalls Ivry, who by this time was chief executive of the Defense Ministry.

"After the second failure, it was really a crisis. I managed to find a small amount of money to keep the team and continue the program... But I must say, if it failed yet again, we wouldn't have been able to proceed," Ivry said.

Eshed estimates the penalty of launching from Israel westward - over the Mediterranean rather than above its neighbors - at nearly 40 percent. To make up for it all, the launcher had to lift well above its weight class and Ofek satellites had to weigh a lot less and be more maneuverable than those that benefit from the initial velocity from Earth's rotation.

Every kilo counts, so much so that Israel had to develop new composite materials and super performing substructures. Even the screws holding it all together had to be hollow.

From his high-rise Tel Aviv sea-view flat, Eshed credited "the shadow of the guillotine" for the engineering feats.

"We had no choice. To do otherwise could be construed by our neighbors as an act of belligerence that could trigger a war... We had to struggle both ways with miniaturization of the satellite and added thrust to our launchers. Under the shadow of the guillotine, we can do wonders."

In an interview at a popular Tel Aviv café, Rubin remembered the intense pressure to perform. "We were out of money. We were desperate. And then the chief of my financial department figured out an aggressive accounting formula that basically allowed us to build the next launcher on credit, something that was not and is still not permitted."

As they struggled to identify and fix failures with the launcher, a separate team was racing to ready a replacement satellite.

"We were caught in a vise; pressed by both ends to come up with the launcher and satellite that would finally succeed," said Moshe Keret, former president and chief executive officer of IAI, the state-owned firm that still builds the Shavit launcher and all Israeli-made satellites.

With no more satellites on the shelf and no funds for new builds, they scavenged for the components that would transform a test satellite into an operationally capable vehicle.

"It was a qualification model; not flightworthy. But we had to make it work," recalls Uzi Eilam, a retired brigadier general who managed the entire effort as head of the Defense Ministry's research and development directorate.

After overcoming the breakdown of tracking radars, and other upsets too many to count, Israel managed to find a window between freak rainstorms and Russian satellites orbiting overhead for the ultimately successful April 1995 launch. Ofek 3, Israel's first orbital spy, finally made it to space.

Rubin said he would never forget the reaction of then-prime minister Yitzhak Rabin upon hearing the news.

"Uzi [Eilam] and I went to brief Rabin, and when we told him the satellite was going to take pictures, the first thing he blurted out was, 'What will Amr Moussa say?' ... Rabin hated his guts," Rubin said, referring to Egypt's foreign minister at the time.

Like earlier high points, success proved short- lived, when a January 1998 launch failure sent Ofek 4 plummeting into the Mediterranean. After that setback, the program was again in crisis; actually on the brink of bankruptcy.

But a big part of this story is refusing to go down for the count. Here's where Ilan Biran enters in a big way. A retired major general who hailed from Israel's can-do Golani infantry brigade, Biran succeeded Ivry as Ministry of Defense managing director.

When informed by his bosses that no more funds would be approved for the program, what did he do? He sold some 1000 MoD-owned apartments, from Safed in the Galilee down to Eilat on the Red Sea, netting some 400 million shekels ($115.69 million), enough, he maintained, to keep the program afloat for the coming years. "It doesn't sound like a lot of money, but for us, it was plenty enough to stabilize the program," Biran recalled.

"Instead of carrying on month-by-month or - in best cases - year-by-year, we finally had the multi-year funding that brought us additional electro-optic satellites and especially the all-weather/ day-night SAR [synthetic aperture radar] satellite, which at the time, was a kind of dream," he said.

Israel went on to deploy that first radar satellite, dubbed TecSAR, ahead of schedule in January 2008, thanks in large part to Biran's real estate sales and funding from India, according to publications. Now known as Ofek 8, TecSAR was the first MoD satellite to be launched abroad; part of a joint venture agreement whose details remain under wraps to this day. The satellite was launched in India from an Indian PSLV launcher.

At the same time, Biran threw Defense Ministry support into a new commercial venture that joined IAI, the nation's sole satellite producer; Elbit's Elop Electro-Optical Industries, producer of the high-resolution payload; and a commercial US firm then called Core Software Technology.

The resulting company, ImageSat International (ISI), would own and operate Ofek spinoff satellites for the commercial market under a new line called Eros (Earth Remote Observation System). Their first Eros reached orbit in December 2000 aboard a Russian Start-1 rocket.

And it's a good thing that it did, because at the time, Israel's defense establishment was still struggling to upgrade its Shavit launcher from the Ofek 4 failure while its sole pair of eyes in the sky - Ofek 3 - was running out of fuel. For nearly two years - from the eventual hero's death of Ofek 3 until the successful May 2002 deployment of Ofek 5 - that Eros satellite was Israel's prime source of space-based intelligence.

In the years that followed, Israel continued to put increasingly higher performance satellites into space, while suffering just one additional failure, that of Ofek 6 in 2004.

But instead of reaping the commercial benefits of the ImageSat venture - which aspired to a constellation of eight Eros satellites - turf battles and competing agendas led to the largest and most potentially damaging lawsuit in Israeli aerospace history.

IAI finally resolved the issue in 2014 by acquiring full control of ISI and settling claims out of court. Today, it has sole authority over the Eros satellite sector and is busy building a third Ofek-derived commercial satellite, dubbed Eros C.

Experts including Tal Inbar of the Fisher Institute for Strategic Air and Space Studies lament the lost time spent battling one another instead of growing Israel's observation satellite sector.

"This industry was built to support strategic needs, but we all knew it could never survive only on low volume orders from the MoD. In order to be truly self-sustaining, we needed to export," Inbar said.

But barring a few notable exceptions - which include an imaging payload to South Korea and joint scientific projects with the French, Italian and European Space Agencies - export and commercial orders failed to come. Industry titans at the time were in such distress they went public with heretofore closed-door appeals for state- level funding.

"We've had some successes, but on balance, it's been a failure," Haim Rousso, former president of Elbit Elop, a publicly traded firm that provides Israel's electro-optical imaging payloads, told an international conference here in early 2011.

"We Israelis, instead of relying on chutzpah and innovation to cover our share, must be able to tap into a significant, long-term, non-military budget, not crumbs," Rousso said.

For years, the Israel Space Agency had been subsisting on a joke of a budget; a mere $700,000 in 2000 that failed to breach the $1 million level until recently. After years of complaints and threats to close down key parts of Israel's satellite sector, the Treasury, in 2012, authorized 200 million shekels ($57.67 million) over two years.

Today, the Israel Space Agency's budget stands at 78 million shekels for 2017 and 86 million shekels for 2018.

Zvi Kaplan, a former Israel Space Agency director, welcomed the budget boosts, yet cautioned: "If you don't come out with a satellite every two or three years, the line goes cold. Your technology grows stale. And even if you manage to secure new collaborative projects every four or five years, if they are persistently plagued by funding flow, the market catches up."

But ours is a tale with an ending unknown. If you ask Joseph Weiss, IAI president and chief executive, it's already a feelgood story, and much like good wine, Weiss says the story only gets better with time.

"Look what we've done since the Camp David days, when less than a handful of countries could utter the word 'space.' We dived into an empty pool and slowly and surely, without budget, here we are: one of only eight or nine in the world who can really deliver a turnkey project to design, develop, manufacture, launch, operate and of course maintain the satellite throughout its life."

Weiss acknowledged numerous disappointments and missed opportunities. Among them, failure to translate the performance of the indigenous Shavit launcher into a business success; a failed joint venture with state-owned Rafael to develop micro-satellites weighing less than 120 kilograms; and competitions lost in Turkey.

The IAI chief insists the firm's earth imaging sector is not only surviving, but profitable, due to steady work from the Defense Ministry and occasional export orders. "Now I'm not saying its billions. That will take some time. Perhaps we'll need some partners."

Aside from Ofek 11, which was recently sent into space, two other IAI-built imaging satellites - one of the French Space Agency and another for the Italian Space Agency - are planned for launch in 2017. The firm is also building, as noted, the Eros C and at least two more successors to Ofek 11. As for new business, IAI is eyeing Brazil, Chile, Columbia and Mexico, among others.

Equally upbeat is Isaac Ben-Israel, a retired major general and former head of the Defense Ministry's Research and Development Directorate who now serves as chairman of the Israel Space Agency.

Ben- Israel led the effort to vector for commercial and civil space the approximately $80 million that the government invests annually in its military space program. He maintains that every dollar the government invests in space can yield fruit 15 times more than initial investment.

"I'm telling you that with $100 million investment, we can get to $1.5 billion, which is about 1 percent of the global space market. This year, the global space sector is about $200 billion all told - products and services - and all I want to get is one percent."

Meanwhile, Eshed, our protagonist from the beginning of this tale, refuses to stop dreaming big. He's now pushing to develop a world-leading sector for nano-satellites, each comprising several units weighing one-to-10 kilograms programmed to operate in small clusters or even huge swarms.

He's gathering inter-ministerial government support for a national program called "Israel 70," which aims to launch 70 such satellites built by 70 different local schools to mark Israel's 70th birthday in 2018.

"Imagine a swarm of 2000 nano-satellites working coherently together; you can get a huge aperture telescope far larger than the sum of their individual parts."

Eshed acknowledges that this vision is yet not widely shared by Weiss and other big players in Israeli industry.

But he insists Israeli industry salvation will not be achieved with more and better of the same, but by a whole new class of capabilities for government, commercial and scientific needs.

"Israel has all the means of becoming the world's fourth or fifth leading power in space... We have the manpower, we have the technology, we have 30 years of heritage, and that's the direction I'm trying to move us in," said Eshed.

"You can dream the dream as long as it does not contradict the laws of physics. You may need to be courageous; even a little crazy, but that's what happened with Oz and Ofek. It's the same story."

Al Jazeera
Facebook 'blocks accounts' of Palestinian journalists
Monday, 26 September 2016
Byline: Sophia Hyatt

Gaza - Editors from two Palestinian news publications based in the occupied West Bank say their Facebook accounts were suspended last week and that no reason was provided, alleging their pages may have been censored because of a recent agreement between the US social media giant and the Israeli government aimed at tackling "incitement".
Last week, four editors from the Shehab News Agency, which has more than 6.3 million likes on Facebook, and three executives from the Quds News Network, with about 5.1 million likes, reported they could not access their personal accounts. Both agencies cover daily news in the occupied Palestinian territories.

Nisreen al-Khatib, a translator and journalist at the Quds News Network, told Al Jazeera that the publication believes the account suspensions were triggered by an agreement between Facebook and Israel earlier this month, in which they agreed to jointly combat what Israeli claims is "incitement" by Palestinians on social media.

Al-Khatib said that even Quds News Network's non-political vertical that focuses on "entertainment" and "international news" had been suspended, although access was later restored.

"[Sharek-Quds News Agency] does not publish anything that violates Facebook standards or that could annoy governments. But still, we are targeted," she said.

Al-Khatib said the news agency asked Facebook for an explanation on why the accounts had been suspended "for no reason". Facebook replied on Saturday with an apology, saying the suspension had been "accidental".

The three suspended accounts of Quds News Newtork journalists were unblocked over the weekend by the networking site, she said.

Remah Mubarak, manager of Shehab News Agency, said one of four managers' accounts that had been suspended "with no warning" by the California-based tech company had still not been reactivated as of late Sunday.

"One manager's account is still suspended," he told Al Jazeera, adding the other three accounts were unblocked on Saturday.

Al Jazeera contacted Facebook for comment, but it did not respond by the time of publication.

Mubarak of Shehab News said the "agency covers news in the West Bank, Gaza Strip and also inside Israel".

"Maybe they don't want this covered, especially in the West Bank, where executions have happened in recent days. Maybe that effects them on social media and they want to stop these pages to hide the proof," he said.

Al-Khatib said the incident isn't the first time Palestinian news sites have had issues with Facebook.

"Many other Palestinian network agencies have been shut down by Facebook for no reason actually. There are at least five Palestinian pages that have been shut down. Gaza 24 was [one of them]," she said.

The Israeli military said on Sunday it has indicted more than 145 Palestinians so far this year for incitement over social media.

Sunday's announcement comes amid an Israeli campaign to put an end to online postings it says have fueled a near continuous wave of violence over the past year. Palestinians say the violence is the result of nearly 50 years of Israeli military occupation.

Since October, at least 230 Palestinians, 34 Israelis, two Americans, one Jordanian, an Eritrean and a Sudanese have been killed, according to a count by the AFP news agency.

Shortly after news broke earlier this month of the agreement between the Israeli government and Facebook, Israeli Justice Minister Ayelet Shaked said Tel Aviv had submitted 158 requests to the social media giant over the previous four months asking it to remove content it deemed "incitement". She said Facebook had granted 95 percent of the requests.

Over the summer, an Israeli legal advocacy group - connected to the Israeli army and intelligence agencies -filed a $1bn lawsuit against Facebook claiming the company was violating the US Anti-Terrorism Act by providing services that assist groups in "recruiting, radicalising and instructing terrorists".

But rights groups and monitors argue that activists and journalists, not "terrorists", are often the target of incitement charges.

USA Today
In breach's wake, Yahoo user lawsuits begin to pile up
Monday, 26 September 2016
Byline: Mike Snyder

Washington - The lawsuits filed against Yahoo in the wake of a massive data breach at the Net media company continue to come.
Two cases filed in U.S. District Court in San Francisco seek class action-status -- one Saturday on behalf of Edward McMahon of New York and another Friday for Maria Sventek of Little Rock, Ark. -- and charge Yahoo with failing to protect users' personal information in one of the largest data breaches of its kind.

Yahoo on Thursday said that it had been the victim of a breach in 2014 in which at least 500 million Yahoo accounts were stolen from the company in what it thought was a hack by a state-sponsored actor. Among the data possibly taken: names, email addresses, telephone numbers, dates of birth, and in some cases, encrypted or unencrypted security questions and answers.

In the McMahon case, his attorneys say that Yahoo "intentionally, willfully, recklessly, or negligently" failed to protect its computer systems and failed to tell users that their data "was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures."

Yahoo violated Federal Trade Commission Act provisions and California business laws by "failing to employ reasonable and appropriate security measures to protect subscribers' personal information," Sventek alleges in her suit.

These suits follow a similar one filed Friday by another Yahoo user Robert Schwartz of New York.

The investigation into the breach threatens to delay Verizon's acquisition of Yahoo. The telecom giant bet out multiple bidders for Yahoo's core business and assets and seeks to pay $4.8 billion to close the deal in the first quarter of next year.

Yahoo declined comment on the lawsuits.

The Australian
ASX told to step up cyber defences
Monday, 26 September 2016
Byline: Richard Gluyas

Canberra - The Australian Securities Exchange should upgrade its readiness for an extreme cyber attack, ensuring by the end of June next year that it can recover its critical clearing and settlement operations within two hours, says the Reserve Bank.
The RBA's recommendation is contained in its annual review of the ASX's clearing and settlement facilities. It came at the close of a torrid week for the ASX, which suffered an outage in its equities trading system, ASX Trade, last Monday, due to a hardware failure in the system's main database. The review was completed before the ASX's recent outage.

Equities trading is a separate function to clearing and settlement, and ASX chief executive Dominic Stevens said from the outset that the breakdown did not stem from a cyber attack.

Global regulators, however, are increasingly concerned about the resilience of financial market infrastructure to online threats.

The RBA said it had adopted a guidance note published in late June by IOSCO (the International Organisation of Securities Commissions) and CPMI (the Committee on Payments and Market Infrastructures), which recognised that it might take time to meet expectations of a full recovery of critical operations within two hours of a cyber attack.

"Consistent with the guidance, the assessment recommends that ASX develop concrete plans to improve its capabilities to meet this requirement by end June 2017," the RBA review said.

The review also stressed the importance of improving the resilience of the ASX's extended network, following the infiltration of the SWIFT global money-transfer system earlier this year.

Banks rely on the network, formally called the Society for Worldwide Interbank Financial Telecommunication, to guarantee the authenticity of orders to make payments from customers'

accounts. However, gaps in security standards and poor communication about breaches have raised questions about SWIFT's ability to deal with cyber attacks.

The RBA noted that the IOSCO and CPMI guidance required users of financial market infrastructure to adequately support cyber resilience frameworks.

"In light of these developments, the assessment recommends that ASX consider developing participant requirements in the area of cyber resilience, liaising as appropriate with (the RBA) and other relevant authorities," it said.

The ASX and Chi-X Australia got the thumbs up last March from an inaugural cyber resilience review of both exchanges by the Australian Securities & Investments Commission. The ASIC report concluded that the ASX and Chi-X had, up to that point, met their statutory obligations to have sufficient resources for the management of cyber resilience.

ASIC Commissioner Cathie Armour said a comprehensive and long- term commitment to cyber resilience was essential to assist all organisations and the Australian economy to manage the threat.

"ASIC encourages all financial services providers to consider and discuss the information in this report as they develop or enhance their cyber resilience frameworks," Ms Armour said.

"We also strongly encourage organisations to share threat intelligence and collaborate with industry peers to improve cyber resilience practices across the financial services industry." In its assessment, the RBA also said the ASX had completed a detailed review of the collapse and default of the stockbroking firm BBY, with a particular emphasis on default management actions.

The ASX, it said, had developed a plan to implement a number of enhancements to its risk management and default management arrangements, including an improvement in stress-testing models so they could better reflect liquidity, spread and concentration risk.

Implementation of the plan, which also features improvements to the close-out process and education and communication initiatives, will take place in 2016-17.

The RBA said the ASX had a well-established framework for managing the default of a participant, which it had continued to enhance in recent years.

The central bank, even so, had made a number of recommendations in line with the requirements of the financial stability standards.

The ASX's Mr Stevens last week apologised for the glitch, labelling the outage "unacceptable" to both market participants and the company.

Associated Press
Intelligence over riches in Yahoo breach
Sunday, 25 September 2016
Byline: Brandon Bailey

San Francisco - If a foreign government is behind the massive computer attack that compromised a half billion user accounts at Yahoo, as the company says, the breach could be part of a long-term strategy that's aimed at gathering intelligence rather than getting rich. Yahoo says the breach involved users' email addresses, passwords and other information - including birthdates - but not payment card or bank account numbers. Although the stolen data could still be used in financial crimes, such as identity theft, experts say a foreign intelligence agency might combine the Yahoo files with information from other sources to build extensive dossiers on U.S. government or corporate officials in sensitive positions. "With state-sponsored attacks, it's not just financial information that's of value," said Lance Hoffman, co-director of the Cyberspace Security and Privacy Institute at George Washington University. "In the long run, if the state accumulates a lot of information on you, and especially if it corroborates that with other sources, it can assemble a pretty good profile."

Governments have also been known to hack email accounts to keep tabs on their own citizens or dissidents. Experts believe that was one motive behind a 2010 hacking of Google Gmail accounts used by Chinese human rights activists.

Yahoo hasn't revealed the evidence that led it to blame a "state-sponsored actor" for the latest attack, which the Sunnyvale, California, company said occurred two years ago and was discovered only in recent weeks.

Some analysts warn that "state sponsored" can be a vague term. It might also be an easy excuse to deflect blame for a company's own security lapses, by suggesting it had no

See Breach, D2

From D1

hope of defeating hackers who had all the resources of a government intelligence agency behind them, warned Gunter Ollmann, chief security officer at Vectra Networks, a San Jose, California, security firm.

Yahoo declined comment, but its top security official, Bob Lord, has said the company would make that claim only "when we have a high degree of confidence." In a policy statement last year, Lord also said the company wouldn't release details about why it believes attacks are state-sponsored because it doesn't want to risk disclosing its methods of investigating breaches.

This wouldn't be the first time that governments were implicated in high-profile hacking attacks.

U.S. officials have hinted that China might be to blame for a 2015 breach at the U.S.

Office of Personnel Management, in which background files and even fingerprints of millions of federal employees were stolen.

China denied any official involvement.

More recently, news reports say U.S. intelligence officials have blamed Russian spies for the hack of Democratic National Committee files, although Russia's government has also denied this.

Some security experts believe the OPM attack was carried out by the same hackers who also stole data files from large U.S.

insurance and health-care companies in 2014 and 2015.

It may have been part of an effort to gather sensitive or compromising information to blackmail or coerce individuals working at a variety of federal agencies. Hackers could also use such personal information to concoct bogus emails and send them to a person's Yahoo account, in what might be a sophisticated "phishing" scheme aimed at getting the target to click on a link containing "spyware" or other malicious computer code.

"They'd have the ability to conduct targeted phishing attacks against individuals with potentially valuable information, without going through their government email accounts," said Tim Erlin, senior director of security and risk strategy at Tripwire, a cyber- security firm.

Similarly, governments might want to target executives at multi- national corporations, especially if they're competing with companies based in the country that sponsored the attacks. In such cases, intelligence officials might share useful commercial secrets with their home-grown industries, said Jeremiah Grossman, an official at SentinelOne, a Silicon Valley computer security firm. He noted that the 2010 attack on Google was blamed on Chinese hackers who also targeted U.S. companies outside the tech industry.

In any event, security experts warn that the Yahoo breach could still put ordinary users at risk, particularly if the hacked information finds its way to online marketplaces where stolen data are bought and sold.

Many people use the same email address and password for a variety of online services, where they might also have provided financial information such as credit card numbers.

TechMalak (Blog)
Is Quantum Computing A Risk For Canad'a Spy Agency
Sunday, 25 September 2016
Byline: Matthew Barnes

(Unidentified Placeline) - Quantum computing technologies are already here in various commercial application is select parts of the world. While a personal quantum computer is a reality that's several years away, that is not stopping the Communications Security Establishment(Canada's spy agency) from ringing the alarm bells.
On Friday, the head of the Communications Security Establishment warned that these highly advanced computers have the potential to bypass current encryption methods used all over the world.

According to the article in the National Post, many cryptologists around the world are in a race to find a viable solution to defend against hackers who want to use quantum computing techniques to hack into secure systems.

There are predicting this technology would be widely available sometimes in and around 2026.

Greta Bossenmaier, chief of the Communications Security Establishment:

It's not really a question of if, it's a question of when. The clock has started to tick. So unless we collectively get ahead of the quantum challenge and rethink encryption, the systems and information of companies, of governments, of organizations, of citizens -- potentially every Canadian citizen -- could be vulnerable.

Scientists are still working at harnessing the high potential of quantum computers. This technology can process colossal amounts of data extremely quickly and at the same time by using atoms as a computing platform.

What Is Quantum Computing

I have only just begun researching the technology in more detail, and already what could be achieved with this sort of computing power for artificial intelligence is absolutely astonishing. Major tech companies such as Google and Microsoft are already developing this technology for use in future products.

Moreover, it is this which security agencies around the world are worrying about. Using this technology, to hack into a secure server would not take too much time at all, if a quantum computer can analyze every possible combination at once to break into a system.

Deutsche Welle

Swiss hold referendum on state snooping
Sunday, 25 September 2016

Geneva - Swiss voters granted new powers Sunday to the country's intelligence services, allowing them to track internet activity, snoop on email and tap phones to better fight spies, criminal hackers and violent extremists.
A majority of 65.5 percent voted for the new law in the national referendum, Swiss media reported.

Under it, the Federal Intelligence Service and other authorities will be allowed to tap phones, infiltrate email and deploy hidden cameras and microphones to monitor suspects who are deemed a clear threat -- but only if authorized by the federal administrative tribunal and oversight counselors.

Until now, Swiss authorities had been barred from using anything more than publicly available information or tips from foreign officials when monitoring threats inside the country.

Proponents said the law was needed to help Switzerland catch up with other countries that have stronger legal arsenals to counter cyber- crime or extremist attacks. Opponents say it will deplete civil liberties, do little to truly impede terrorism and chip away at Switzerland's long- vaunted neutrality.

Associated Press
Swiss vote to grant new powers to intelligence services
Sunday, 25 September 2016
Byline: Jamey Keaten

Geneva - Swiss voters granted new powers Sunday to the country's intelligence services, allowing them to track internet activity, snoop on email and tap phones to better fight spies, criminal hackers and violent extremists.
A majority of 65.5 percent voted for the new law in the national referendum, Swiss media reported.

Under it, the Federal Intelligence Service and other authorities will be allowed to tap phones, infiltrate email and deploy hidden cameras and microphones to monitor suspects who are deemed a clear threat -- but only if authorized by the federal administrative tribunal and oversight counselors.

Until now, Swiss authorities had been barred from using anything more than publicly available information or tips from foreign officials when monitoring threats inside the country.

Proponents said the law was needed to help Switzerland catch up with other countries that have stronger legal arsenals to counter cyber- crime or extremist attacks. Opponents say it will deplete civil liberties, do little to truly impede terrorism and chip away at Switzerland's long- vaunted neutrality.

Associated Press

Hacker who aided Islamic State reveals complexity and challenges of terrorism in cyber age

Saturday, 24 September 2016

Washington - Ardit Ferizi wasn't your typical Islamic State soldier. He didn't travel to Syria or launch a "lone-wolf" style attack. He contributed in his own way - by hacking.
The teenage computer prodigy last year broke into a well-known US retailer's computers, swiped information on tens of thousands of its customers and provided a list to Islamic State of more than 1,300 names of those believed to be government and military personnel.

Within weeks of the June 2015 hack, the group published the identities as part of a "kill list", urging home-grown extremists to hunt and murder the military and government officials. The publication sent chills through those on the list and represented a propaganda coup that allowed Islamic State to boast of being able to reach directly into Americans' computers, "watching your every move".

In court papers and in interviews, US officials say the case highlights how fast the terror threat is evolving in the age of computers and social media, especially for a terror group urging its followers to carry out "lone-wolf" attacks when given the chance. It also revealed Islamic State's global reach - Ferizi, a citizen of Kosovo, used a computer in Malaysia to hack the US retailer and then forwarded the data to Islamic State operatives in Syria, who called on followers to strike the workers where they lived.

"This is the blended threat," said John Carlin, the Justice Department's top national security prosecutor. "Terrorism is now occurring at the speed of cyber, and they are exploiting Western-made technology and social media platforms."

Ferizi, who was arrested in Malaysia not long after the successful hack, was extradited to the United States. He was sentenced on Friday to 20 years in federal prison after having pleaded guilty to terrorism and hacking-related charges.

Standing before a US district judge in Alexandria, Virginia, on Friday, Ferizi wore a green jail jumpsuit and spoke in a quiet voice, saying he was "very sorry for what happened, making people scared".

His lawyer, Elizabeth Mullin, portrayed him as a troubled, misguided drug user who did not subscribe to Islamic State's radical ideology and didn't understand the consequences of his actions.

Federal prosecutors disagreed, pointing to excerpts of messages between Ferizi and well-known Islamic State recruiters that they said left little doubt he understood his work could be used in deadly ways.

"This was a hit list," said Special Assistant US Attorney Brandon L. Van Grack said. "This wasn't about stealing money from these people."

Ferizi, 20, was born in Gjakova, Kosovo, and raised in a middle- class family who endured ethnic cleansing at the hands of the Serbs in the late 1990s, his lawyer wrote in court papers. As a four-year-old, Ferizi and his family were forcibly removed from their uncle's home by Serbian police and watched helplessly as the uncle was executed, according to the papers.

After Nato intervened in the war and stopped the fighting, Ferizi returned to a somewhat normal life and got interested in computers. By the age of 10, he was a hacking prodigy and eventually assumed the online persona of "Th3Dir3ctorY", the leader of an Albanian hacking collective responsible for breaking into government databases in Israel, Serbia, Ukraine and elsewhere, court papers show.Ferizi, who struggled with undisclosed mental health problems. kept getting into trouble and was caught hacking into a Kosovo government database, court papers show. Hoping to turn his life around and improve his computer skills so he could earn a legitimate living, he moved to Malaysia to attend college.

While there, he communicated via Twitter's direct messaging system with two well-known members of Islamic State, Tariq Hamayun and Junaid Hussain, both British citizens who were fighting and acting as recruiters for the terror group in Syria. Both men had been in communication with jihadists linked to terror plots, federal officials say.

The FBI found Twitter records, for example, showing that Hamayun had been communicating with one of the two men who were fatally shot by police while trying to attack a "Draw Muhammad Contest" in Garland, Texas, in May 2015. Drawn to the Islamic State's rhetoric, Ferizi at first administered a website that published the group's violent videos and literature. He next passed along some stolen credit card data to Hamayun, who complimented the effort and said the credit card information was good enough to "do some damage".

"U sound like a good person," Hamayun messaged Ferizi in April 2015, according to excerpts of their Twitter direct messages included in court filings. "Plz brother come and join us in the Islamic State."

Two months later, Ferizi hacked into the US retailer, which is not identified in court papers, and began stealing the identities of tens of thousands of customers.

Proud of his work, he boldly emailed a representative of the company, demanding US$500 in Bitcoin, an online currency, to relinquish his access to the company's computers and to explain how he had broken into them.

The company's representatives reported the hack to the FBI, thinking they were the victims of an all-too-common cyberattack and extortion scheme. As the FBI traced the intrusion to Ferizi, the hacker was narrowing more than 100,000 identities down to 1,351 that had military and government email addresses.

He next sent the information to Hussain, who was a member of Islamic State's cyber unit. Two months after that, Hussain and the Islamic State unit published the identities, bragging, "We are extracting

confidential data and passing on your personal information to the soldiers ... who will strike at your necks in your own lands!"

Clearly proud of Ferizi's work, Hussain told the hacker he was helping Islamic State to "hit them hard".

"God willing", Ferizi replied in Arabic, punctuating the message with a smiley-face emoticon.

Hussain then urged the young man to come to Syria to join his elite group of cyberterrorists.

"We can work together here," the recruiter promised. "u will stay in the base. free food. free electric. free gas."

Ferizi never got the chance. Not long after that exchange, Hussain was killed in a US air strike, and the hacker was captured.

New York Times
What the hacking at Yahoo means for Verizon
Saturday, 24 September 2016
Byline: David Gelles

Washington - It was the kind of phone call no chief executive wants to make - or receive - in the middle of a multibillion-dollar deal.
On Tuesday, Lowell McAdam, head of Verizon Communications, was on the road. Marissa Mayer, chief executive of Yahoo, was at work in Silicon Valley. Executives at both companies were moving forward on Verizon's $4.8 billion acquisition of Yahoo's core business.

But Mayer had some unexpected bad news. She caught up with McAdam and Marni Walden, a rising star at Verizon who is expected to oversee the Yahoo business after the deal is complete, by phone, according to people briefed on the call, who spoke on the condition of anonymity.

Yahoo recently discovered that at least 500 million of its user accounts had been breached by hackers two years ago, well before the two companies began talks. Yahoo and law enforcement officials were scrambling to unwind the intrusion.

After calling McAdam and Walden, Mayer phoned Tim Armstrong, who leads the AOL business at Verizon, according to the people briefed on the conversation. Again, the news was not good.

The calls set off a flurry of questions at Verizon - How could this possibly have happened? Who was behind it? Why is it only becoming known now? Could this jeopardize the deal? - but also the sounding of an alarm and the deployment of a triage team to assist Yahoo.

The telecom giant directed its online security experts, including Chandra McMahon, Verizon's chief information security officer, to do their own investigation of the hack. And they enlisted the help of Verizon's security division, part of its enterprise solutions business, which helps companies defend against and manage hacks.

Now, just a few days after Verizon learned of the breach, it is contending with the ramifications of what is believed to be the largest hack of a single company. Even as Verizon tries to assess the damage at Yahoo and prevent further security intrusions, the scope of the hack and the potential fallout - including the possibility of a costly class-action lawsuit - is inevitably prompting renewed scrutiny of a deal that was intended to transform the telecom behemoth into a digital media powerhouse.

For now, Verizon has given no indication of whether the breach will affect its plans to acquire Yahoo. On Friday, the company declined to provide a comment beyond a statement it issued Thursday in which it said it would evaluate the situation "as the investigation continues through the lens of overall Verizon interests, including consumers, customers, shareholders and related communities."

Yahoo declined to provide further comment Friday.

The effort is complicated because the sales proceedings between Verizon and Yahoo are at an early stage. Though teams from the two companies were working together on integration plans, Verizon does not yet own Yahoo. As a result, Verizon does not have direct access to the Silicon Valley company's servers to conduct its own investigation.

In late July, after the Verizon deal was announced, Yahoo became aware of a claim that about 280 million of its user credentials had been hacked, according to a person briefed on the specifics, who spoke on the condition of anonymity. Yahoo started an investigation but could not substantiate the claim, this person said. It was not clear Friday whether Yahoo had made Verizon aware that it was looking into this claim in July.

During the course of that investigation, Yahoo learned of the more severe breach, which it has said it believes was state-sponsored. Yahoo has not yet said exactly when it realized how large the intrusion was, leaving open the question of whether Mayer and her team waited to notify Verizon of the hack. Yahoo is now working with outside security consultants on the matter and said its investigation was continuing.

Brian Quinn, an associate professor at Boston College Law School, said Verizon had two main options if it decided to use the hack as leverage in setting the terms of the deal.

"They could say, 'This thing is huge. We want to walk away from the transaction,' " he said. Were Verizon to try to claim that the breach was so severe it was grounds to terminate the deal, it would have to prove that the hack amounted to a material adverse effect on the value of Yahoo.

Such claims can be difficult to prove in court. According to Quinn's reading of the merger document for the deal, Verizon would most likely have to prove that certain high-level Yahoo employees were aware of the severity of the hack before the deal was agreed upon, and intentionally withheld that information.

In the merger agreement, Yahoo states that "there have not been any incidents of, or third-party claims alleging" security breaches or thefts of user data that might result in a major change to the value of the company.

More likely, Quinn said, Verizon could pressure Yahoo to renegotiate the terms of the deal.

"They go to court, or threaten to go to court, and renegotiate the price," he said. "That can be a very winning strategy."

Daily Telegraph (Australia)
Yahoo cyber attack affected 8m Britons
Saturday, 24 September 2016
Byline: Cara McGoogan

London - Eight million Britons have been urged to change their internet passwords after the information commissioner confirmed they were affected by the cyber attack against the US internet giant Yahoo, which involved the loss of at least half a billion users' information globally to "state-sponsored attackers".
The British watchdog said she will be asking "serious questions" after Yahoo revealed that it had suffered what is believed to be the worst cyber attack on record. The commissioner, who Continued on Page 2 Continued from Page 1 could levy fines of up to £500,000 against the company for not protecting its customers' information, described the data loss as "staggering" and warned companies that it is their responsibility to make theft "impossible" for cyber criminals.

"It is our job to ask serious questions of Yahoo on behalf of British citizens and I am doing that today," said Elizabeth Denham.

Yahoo advised any customer who had not changed their password since 2014 to do so. The company was under mounting pressure to provide more information about how attackers had got away with swathes of personal data, which included names, email addresses, telephone numbers, dates of birth, and encrypted passwords.

Yahoo claimed that the information was taken in a "state-sponsored attack" in 2014, but did not provide any further information, leading some to question the company's explanation.

Russia or China are the most likely candidates, according to cyber security experts.

But some analysts suggested that Yahoo could have overplayed the role of a nation state in the attacks to mitigate criticism about its security practices and defences.

New York Times
Hackers Trawl User Data in Hopes a Small Target Will Lead to a Big One
Saturday, 24 September 2016
Byline: Nicole Perlroth

San Francisco - In disclosing that at least 500 million of its user accounts had been hacked, Yahoo blamed an unnamed "state-sponsored actor" for the intrusion. While Yahoo customers were caught by surprise, officials in Washington were not.
For more than a year, they had been getting warnings from government technology managers that hackers were targeting their personal Yahoo email. Even the accounts of their friends and family were in the cross hairs.

These days, intelligence and security experts say, nearly anyone can be the target of government-sponsored hackers. By perusing the personal accounts of people with even the thinnest thread of a connection to power, hackers can unearth the occasional gold nugget, like the low-level Democratic operative whose private email correspondence, published online by hackers on Thursday, detailed the movements of Vice President Joseph R. Biden Jr. and Hillary Clinton and what appears to be Michelle Obama's passport.

This expanded hacking strategy presents a new challenge: While top-secret material is usually kept in more secure computer systems, it is hard -- if not impossible -- to predict what information people are exchanging in personal email accounts. And it is even harder to know if hacking into one person's account can set off a cascading chain of events that could lead foreign spies to more useful information.

In 2014, Yahoo also investigated attacks by Russian hackers that targeted dozens of private Yahoo accounts, one person with knowledge of Yahoo's investigation said, but it is not yet clear whether the same hackers were behind the larger hack.

"The Yahoo attack alone may not make sense, but when you combine the stolen data from Yahoo with other stolen data sets, it makes a lot more sense," said Sean Kanuck, the former national intelligence officer for online security issues at the Office of the Director of National Intelligence.

Hackers working on behalf of governments can match stolen Yahoo account data with their own material or information available on the criminal underground and published on the website WikiLeaks for a variety of purposes, Mr. Kanuck and other intelligence officials say.

At this point, they'd have a lot to work with. In the two years since Yahoo believes the hackers first penetrated its network, state-sponsored hackers have stolen tens of millions of records from the insurance companies Anthem and Premera Blue Cross, including Social Security numbers, health records, birth dates, addresses, emails, passwords and employment information -- basically, everything you'd need to know about a person.

Hackers amassed a vast collection of security clearance records, even fingerprints, in a yearlong hacking of the United States Office of Personnel Management. They have breached law firms and accounting firms, and last year they even made off with flight records for millions of United Airlines passengers.

It may sound like a crazy collection of unrelated information. But it is not that difficult to make connections among seemingly random bits of information using data-sifting technology.

Just as a corporation may use big data to figure out what a consumer might buy based on their past purchases, a spy agency can use big data to make connections to useful intelligence. A Palo Alto, Calif., company named Palantir sells this technology to American intelligence agencies, allowing them, for example, to match travel records and personal data to identify possible terrorists.

So while Yahoo's announcement on Thursday that state-sponsored hackers -- the company did not say what country it believes they are working for -- had made off with more than 500 million customers' personal records was stunning to many, intelligence officials say it can be seen as just the latest step in an escalating nation-state digital warfare campaign.

"A lot of people overlook why some of these seemingly purposeless breaches matter," said Mr. Kanuck.

Intelligence services could use this information for a range of things -- some trivial and some intrusive. They could match international flights taken by their own officials with those taken by American personnel to the same cities at the same time. They could, for example, comb the user names and emails released in a hacking of Ashley Madison, the online affairs site that was breached last year, with the personal Yahoo accounts of government officials and contractors or their spouses, and leak that information online or use it for blackmail.

And they can use the most intimate details of people's lives -- their medical records -- to undercut the reputations of prominent American athletes, as Russian hackers did in a release of medical records stolen from the World Anti-Doping Agency that belonged to the gymnast Simone Biles, the tennis stars Venus and Serena Williams and other Olympic athletes.

The biggest worry, Mr. Kanuck and other American intelligence officials say, is the impact these data thefts can have on global politics. James. R. Clapper, the director of National Intelligence, warned Senate officials earlier this year that Russia was escalating its espionage campaigns against United States targets.

"Russia continues to take information warfare to a new level, working to fan anti- U.S. and anti-Western sentiment both within Russia and globally," Mr. Clapper said in his annual worldwide threat briefing in February.

Intelligence officials and private security researchers say it's not just prominent United States government officials that Russian hackers are after. It's their spouses, staff members, lawyers, accountants and business partners, who may not have the same level of security awareness around their data and communications.

"In the past year, we've seen personal webmail accounts and social network accounts specifically being targeted by Russian, Chinese and Iranian espionage operators, on several occasions," said John Hultquist, an espionage analysis manager at FireEye, the security software company. "That's where some of the most sensitive conversations take place, and hacking private accounts leaves a much lighter footprint."

One of the most adept at this approach, Mr. Hultquist and other security researchers say, has been a Russian intelligence hacking group alternately known in the security and intelligence community as APT28, Fancy Bear or Pawn Storm. The group regularly uses the compromised personal webmail accounts of staff members, spouses and their colleagues as tools to glean more information on high-level government targets.

In just the last few months, the group has been blamed for attacks on the Democratic National Committee, the White House and the World Anti-Doping Agency.

Going back to last year, the Russian group also has been trying to break into the online accounts of 2,600 members of the Washington elite -- lobbyists, journalists, officials, contractors and even their spouses, according to private security researchers at Trend Micro, the global security company, who briefed intelligence agencies on the hacking.

Among the Russians' targets were Colin L. Powell, the former secretary of state, whose personal emails caused a sensation when they were leaked online last week, according to people with knowledge of the briefing who spoke on the condition of anonymity.

"This is the new normal," said Tom Kellermann, one of the security experts who briefed intelligence officials last year in his former role as chief security officer at Trend Micro. "It's not just the usual targets who are being hunted. It's their spouses."

Mr. Kanuck said no one should be shocked that this is going on. "Every prominent person in Washington, every publicly known intelligence official, congressman and significant staffer should presume they have been targeted," Mr. Kanuck said. "You'd be a fool not to think that's the case."

Wall Street Journal
FBI Gave Two Aides Of Clinton Immunity
Saturday, 24 September 2016
Byline: Byron Tau

Washington - Two of Hillary Clinton's attorneys were granted immunity as part of a now-closed Federal Bureau of Investigation probe into whether the former secretary of state or her aides mishandled classified information through her email practices, lawmakers said on Friday.
Meanwhile, a federal judge set a new timetable for the processing and release of Clinton emails recovered during the FBI probe, shifting the release of most of the material to after Election Day.

Judge James Boasberg ordered the State Department to finish processing 1,050 pages of material for release by Nov. 4 -- just a fraction of what could be as much as 10,000 pages of material -- in one of dozens of cases seeking access to Clinton materials.

Lawmakers who have reviewed documents turned over to Congress by the FBI said Cheryl Mills, a longtime Clinton aide, and aide Heather Samuelson were given limited immunity by the FBI in exchange for turning over their personal laptop computers as part of the investigation. A State Department staffer who at the time managed information resources was also granted immunity.

"The FBI was handing out immunity agreements like candy. I've lost confidence in this investigation," House Oversight and Government Reform Committee Chairman Jason Chaffetz (R., Utah) said.

The FBI declined to comment.

"The [Justice Department] and FBI considered my clients to be witnesses and nothing more," said Beth Wilkinson, an attorney for Mses. Mills and Samuelson. "At all points my clients cooperated with the government's investigation."

Brian Fallon, a spokesman for Mrs. Clinton, said "House Republicans are trying to make something out of nothing by rummaging through the files of a Justice Department investigation that was closed months ago."

London Times
Forged British documents being traded on dark web
Saturday, 24 September 2016
Byline: John Simpson

London - Forged British passports and documents including driving licences, utility bills and GCSE certificates are being sold on hidden websites, an undercover investigation has found.

Researchers who gained access to the sites -- known as the dark web -- saw the passports being offered by several sellers for as little as £800.

The investigation reveals for the first time the scale of the online trade in high-quality forged identity documents, which experts said yesterday were a goldmine for criminals.

Fraudsters can combine payslips, bank statements and gas and electricity bills with doctored photographic ID to open bank accounts and take out loans, or obtain genuine passports or driving licences in their victims' names.

The ready availability of forgeries vital to the activities of terrorists seeking to create fake identities will act as a warning to security services of the threat posed by the dark web. It is accessed only by invitation through secure internet browsers.

"It's scary that it's so easy for anyone to organise and buy stuff to be sent to their home," Sin Wee Lee, of the University of East London, which carried out the investigation, said. "It's so easy to get a user name and account and start buying."

Islamic State jihadists are known to be adept at using the kind of encoded technology that enables the use of the dark web, and have repeatedly shared guides on how to do it.

The sites also offer drugs and guns for sale, with the university team finding AK47s, cocaine and methamphetamine. The threat of the dark web was brought into sharp focus in Munich in July, when Ali David Sonboly, 18, murdered nine people with a Glock 9mm pistol bought through an illicit site before turning the gun on himself. MI6 said this week it would recruit almost a thousand spies to fight terrorism and exploit the potential of the digital age.

Dr Lee and Andres Baravalle, who led the research, spent three months trawling the Agora marketplace, known as "the king of the dark web".

They found eight sellers offering multiple British passports. These were mostly described as cloned or hacked, while two were offering only scanned copies. However, one of the passports was described as "custom", suggesting that it could be tailor made for the user.

False UK driving licences, templates for faking British Gas accounts and Barclays and HSBC bank statements, and forged GCSE results and university degrees were also on offer.

In three hours the academics intercepted several invitations to join Agora. They entered the site and unleashed custom-made "spider" software, which mimicked human behaviour while harvesting data. They found more than 30,000 illegal products on sale, largely fake or real identity documents and drugs worth at least £26 million. There were weapons and counterfeit goods.

They found a trade of nearly £2 million in identity documents, including EU identity cards for £142 and driving licences from EU countries for £419.

Dr Baravalle and Dr Lee worked undercover between July and September last year, when Agora was taken offline, but security experts warned that the marketplaces are quick to crop up in different guises. Silk Road was worth nearly £1 billion when it was shut down by the FBI in 2013. The site apparently resurfaced in March this year, in its third incarnation.

New questions have emerged over an £11 billion project to install smart energy meters in every British home, after experts warned that hackers could use the devices to shut down the nation's electricity supplies. A report on the meters from MPs on the Commons science and technology committee pointed to serious cyber- security concerns. About 3.6 million of the meters, which measure household electricity and gas consumption in real time, have already been installed. The report cited experts from the Royal Academy of Engineering who warned MPs that there was a "real and pressing threat of cyberattacks either to gain information, 'steal' electricity or disrupt supply".

Politico.com
Obama used a pseudonym in emails with Clinton, FBI documents reveal
Saturday, 24 September 2016
Byline: Josh Gerstein and Nolan D McCaskill

Washington - President Barack Obama used a pseudonym in email communications with Hillary Clinton and others, according to FBI records made public Friday.
The disclosure came as the FBI released its second batch of documents from its investigation into Clinton's private email server during her tenure as secretary of state.

The 189 pages the bureau released includes interviews with some of Clinton's closest aides, such as Huma Abedin and Cheryl Mills; senior State Department officials; and even Marcel Lazar, better known as the Romanian hacker "Guccifer."

In an April 5, 2016 interview with the FBI, Abedin was shown an email exchange between Clinton and Obama, but the longtime Clinton aide did not recognize the name of the sender.

"Once informed that the sender's name is believed to be pseudonym used by the president, Abedin exclaimed: 'How is this not classified?'" the report says. "Abedin then expressed her amazement at the president's use of a pseudonym and asked if she could have a copy of the email."

The State Department has refused to make public that and other emails Clinton exchanged with Obama. Lawyers have cited the "presidential communications privilege," a variation of executive privilege, in order to withhold the messages under the Freedom of Information Act.

The report doesn't provide more details on the contents of that particular email exchange, but says it took place on June 28, 2012, and had the subject line: "Re: Congratulations." It may refer to the Supreme Court's ruling that day upholding a key portion of the Obamacare law.

A report on the FBI's June 7, 2016 interview with "Guccifer" confirms FBI Director James Comey's claim that Lazar falsely asserted that he'd surreptitiously accessed Clinton's server.

"Lazar began by stating that he had never claimed to hack the Clinton server. [An FBI agent] then advised that Fox News had recently published an article which reported that Lazar had claimed to have to Clinton server. Lazar then stated that he recalled the interview with Fox News, and that he had lied to them about hacking the Clinton server."

Additional FBI interviewees whose reports were made public Friday included Jake Sullivan, Clinton's policy planning director; Bryan Pagliano, a former Clinton technology aide; Monica Hanley, a veteran Clinton aide who worked for her in the Senate and at State; and Sidney Blumenthal, Clinton's longtime confidant.

Hanley revealed in her FBI interview that she had no idea where a thumb drive she used to store an archive of Clinton's emails had gone. Hanley searched for the thumb drive, which the FBI described as "something she happened to have laying around the house," several times but was unable to find it.

The interviews provide more insight into Clinton's lack of technical acumen. According to the FBI's Abedin writeup, she "could not use a computer"; Hanley said Clinton had no idea what her own email password was, and had to rely on aides.

The so-called "302" reports also detail FBI interviews with former Secretary of State Colin Powell, former CIA acting director Mike Morell, State Department official Pat Kennedy, State Department Inspector General Steve Linick, Bill Clinton aide Justin Cooper, former diplomatic security chief Eric Boswell and longtime diplomat Lewis Lukens.

Some of the interview reports had the subject's name removed on privacy grounds before the records were released. Many of those people seem to be computer technicians or lower-level State Department officials.

The FBI published 58 pages of documents earlier this month that revealed Clinton had relied on others' judgment to not send her classified material during email correspondences.

"Clinton did not recall receiving any emails she thought should not be on an unclassified system," the FBI said in its Sept. 2 report. "She relied on State officials to use their judgment when emailing her and could not recall anyone raising concerns with her regarding the sensitivity of the information she received at her email address."

Sunday Times (UK)
China 'strips cloak' from US stealth bomber
Sunday, 25 September 2016
Byline: Damien McElroy

London - Chinese scientists claim to have developed a "stealthstripper" radar that could hand Beijing a decisive advantage in the military build-up in the South China Sea, just as America deploys more than half its navy to the Pacific.
The race to dominate the sea around China has drawn in military ships and planes from America, China, Japan and Taiwan, as well as the southeast Asian states.

A military-run research institute, China Electronics Technology Group, says it has developed a type of radar that can strip the cloak of invisibility used by the US B-2 stealth bomber. It detects the shadow the aircraft casts as it flies.

Capable of spotting planes at a 60-mile range, it is reported to be five times more powerful than anything produced for the Pentagon's rival Darpa programme.

"China has had a great leg-up over a short period of time since the 1990s by shopping for technology from the former Soviet Union and Israel," said Douglas Barrie, who is an expert in military aviation at the International Institute for Strategic Studies in London. "It has spent a lot of money and poured a lot of national resources into radar development."

The radar threatens to alter the military balance in the South China Sea, where Beijing asserts its territorial rights over scattered island chains.

The system was unveiled after America and Japan this month announced joint patrols of the islands claimed by China.

The Japanese said they were responding to Beijing's attempts to take over international waterways. The Chinese foreign ministry said that it was disappointed to the point of despair by the Japanese intervention.

China sets its southern maritime boundary within a disputed "nine-dash" line drawn on maps since the 1940s. But the islands and reefs, including Scarborough Shoal and the Spratly Islands, within the line are also claimed by the Philippines, Vietnam and Malaysia. China and its rival Taiwan rejected a UN tribunal ruling in July that the reefs were not their territory under the law of the sea. The two have continued a building spree and said they will ignore the ruling.

Concern over the military build-up on the islands grew last week when images emerged of Taiwanese fortifications, apparently designed for weapons emplacement, on Taiping, an island between Vietnam and the Philippines under Taiwanese control.

Taiwan asked Google Maps to blur the images, which show a cluster of reinforced concrete buildings. "Taiping is an important militarily jurisdiction. Some related infrastructure on the island is in a state of alertness," the request stated. Google was reported to be considering the request.

Military analysts regard the airstrips and other military facilities as substitutes for aircraft carriers.

While China has reconditioned a 1980s aircraft carrier in dry dock, it has not tried to build a vessel capable of going to sea. "Building a carrier strike capability doesn't happen overnight," said Barrie. "China can gain naval air power from putting an airstrip or bulldozing a runway out at sea." President Barack Obama's main foreign policy legacy is the pivot to Asia under which the Pentagon is deploying 60% of all its ships in the Pacific by 2020. The goal of the policy is to ensure freedom of navigation through a passageway for $5.3 trillion (£4 trillion) in trade, almost 30% of the global total.

With so much at stake, regional alliances are under strain. Diplomats have expressed concern for the longstanding US alliance with the Philippines after a spat between Obama and Rodrigo Duterte, the foul-mouthed new president.

Duterte signalled he could compromise with Beijing over the Spratlys when he visits China next month. "This piece of paper, the arbitral award, we don't go out of the four corners of this paper. Let's talk," Duterte declared.

In the long-run Washington's military superiority is not guaranteed. In one key area experts believe that China will have expanded its squadrons of fighter jets to match the numbers of US planes in the region by 2020.

Rand, the US military think tank, warns Washington could no longer count on a "decisive victory" in a war that would probably happen on the ocean.

"It would be waged mainly by ships on and beneath the sea, by aircraft and missiles of many sorts, and in space and cyber-space," it said.

"Sensors, weapon guidance, digital networking and other information technologies used to target opposing forces have advanced to the point where US and Chinese military forces seriously threaten each other."

Sunday Times (UK)
Fancy Bear hackers attack British TV

Sunday, 25 September 2016
Byline: Richard Kerbaj, Josh Boswell & Tom Harper

London - Chinese scientists claim to have developed a "stealthstripper" radar that could hand Beijing a decisive advantage in the military build-up in the South China Sea, just as America deploys more than half its navy to the Pacific.
The race to dominate the sea around China has drawn in military ships and planes from America, China, Japan and Taiwan, as well as the southeast Asian states.

A military-run research institute, China Electronics Technology Group, says it has developed a type of radar that can strip the cloak of invisibility used by the US B-2 stealth bomber. It detects the shadow the aircraft casts as it flies.

Capable of spotting planes at a 60-mile range, it is reported to be five times more powerful than anything produced for the Pentagon's rival Darpa programme.

"China has had a great leg-up over a short period of time since the 1990s by shopping for technology from the former Soviet Union and Israel," said Douglas Barrie, who is an expert in military aviation at the International Institute for Strategic Studies in London. "It has spent a lot of money and poured a lot of national resources into radar development."

The radar threatens to alter the military balance in the South China Sea, where Beijing asserts its territorial rights over scattered island chains.

The system was unveiled after America and Japan this month announced joint patrols of the islands claimed by China.

The Japanese said they were responding to Beijing's attempts to take over international waterways. The Chinese foreign ministry said that it was disappointed to the point of despair by the Japanese intervention.

China sets its southern maritime boundary within a disputed "nine-dash" line drawn on maps since the 1940s. But the islands and reefs, including Scarborough Shoal and the Spratly Islands, within the line are also claimed by the Philippines, Vietnam and Malaysia. China and its rival Taiwan rejected a UN tribunal ruling in July that the reefs were not their territory under the law of the sea. The two have continued a building spree and said they will ignore the ruling.

Concern over the military build-up on the islands grew last week when images emerged of Taiwanese fortifications, apparently designed for weapons emplacement, on Taiping, an island between Vietnam and the Philippines under Taiwanese control.

Taiwan asked Google Maps to blur the images, which show a cluster of reinforced concrete buildings. "Taiping is an important militarily jurisdiction. Some related infrastructure on the island is in a state of alertness," the request stated. Google was reported to be considering the request.

Military analysts regard the airstrips and other military facilities as substitutes for aircraft carriers.

While China has reconditioned a 1980s aircraft carrier in dry dock, it has not tried to build a vessel capable of going to sea. "Building a carrier strike capability doesn't happen overnight," said Barrie. "China can gain naval air power from putting an airstrip or bulldozing a runway out at sea." President Barack Obama's main foreign policy legacy is the pivot to Asia under which the Pentagon is deploying 60% of all its ships in the Pacific by 2020. The goal of the policy is to ensure freedom of navigation through a passageway for $5.3 trillion (£4 trillion) in trade, almost 30% of the global total.

With so much at stake, regional alliances are under strain. Diplomats have expressed concern for the longstanding US alliance with the Philippines after a spat between Obama and Rodrigo Duterte, the foul-mouthed new president.

Duterte signalled he could compromise with Beijing over the Spratlys when he visits China next month. "This piece of paper, the arbitral award, we don't go out of the four corners of this paper. Let's talk," Duterte declared.

In the long-run Washington's military superiority is not guaranteed. In one key area experts believe that China will have expanded its squadrons of fighter jets to match the numbers of US planes in the region by 2020.

Rand, the US military think tank, warns Washington could no longer count on a "decisive victory" in a war that would probably happen on the ocean.

"It would be waged mainly by ships on and beneath the sea, by aircraft and missiles of many sorts, and in space and cyber-space," it said.

"Sensors, weapon guidance, digital networking and other information technologies used to target opposing forces have advanced to the point where US and Chinese military forces seriously threaten each other."

Canadian Press
Dropping crime statistics not reflecting rise of cyber crime, Halifax police chief says
Saturday, 24 September 2016
Byline: Michael MacDonald

Halifax - Statistics suggesting crime rates in Canada have been falling for decades may not tell the whole story when it comes to criminal wrongdoing, the chief of Halifax Regional Police says.
Jean-Michel Blais says there are indications that the nature of crime is changing in a way that is not reflected in traditional crime data.

"And this crime is not being committed by your neighbour, and probably not someone here in Nova Scotia or even in Canada," he said in an interview.

"It's being committed by somebody in a different country."

Blais, who plans to explore the issue Friday in a speech to the Halifax Chamber of Commerce, says traditional crimes appear to be "morphing" and migrating to criminal acts perpetrated online.

As a result, he says, crime probably hasn't decreased as much as statistics might suggest.

In 2014, a study in the United Kingdom found just over half of those surveyed in Britain had been the victim of an online crime, including identity theft, hacking and illegally accessing and stealing from bank accounts.

The study found that much of this crime was never reported, which means it didn't show up in police statistics.

The Get Safe Online survey, conducted by market research firm Vision Critical, also showed that 53 per cent of those surveyed said they considered online crimes as serious as physical crimes.

"Crime really hasn't gone down as much as we think," Blais said in an interview. "It's ... migrated onto the internet."

To illustrate his point, he suggested it has become common for anyone using email to be routinely prodded by fake messages that seek access to bank accounts or offer rich rewards for participating in shady international transactions.

"Think about the number of passwords that you have in your life, and imagine if those were hacked," he said. "On average, it takes 400 hours of time to rehabilitate a person's identification."

Last year, a PwC study conducted for the British government found 90 per cent of large corporations surveyed in Britain had experienced a security breach last year, up from 81 per cent in 2014, reflecting a similar trend for small- and medium-sized businesses.

"So, if you're part of a large company, chances are that in the future you will have a data breach," Blais said. "It's a real challenge."

The chief also mentioned the rise of the so-called Dark Web, an off-limits layer of the Internet where special software and codes are needed to access illicit material.

Statistics Canada says that the overall police-reported crime rate in Canada has been falling for more than 20 years -- a reversal of the upward trend recorded between 1962 to 1991.

The trend applies to violent crime, including homicides, and many other Criminal Code offences, Statistics Canada reports.

The federal agency says experts have attributed the decline to a long list of factors, including an aging population, changing policing practices, shifts in unemployment and variations in alcohol consumption.

Similar downward trends have been observed in other countries.

Blais, a former Mountie who has served as Halifax police chief for almost four years, is also expected to speak about how traumatic events in other parts of the world -- such as the rise in gun violence in the United States -- can have ripple effect in Canada.

Washington Post
Tech law needs a reboot
Sunday, 25 September 2016
Byline: Garrett M. Graff

Washington - Last year, the FBI nearly destroyed the life of an innocent physicist. In May 2015, agents arrested Xi Xiaoxing, the chairman of Temple University's physics department, and charged that he was sneaking Chinese scientists details about a piece of restricted research equipment known as a "pocket heater." An illustrious career seemed suddenly to implode. A few months later, though, the Justice Department dropped all the charges and made an embarrassing admission: It hadn't actually understood Xi's work. After defense experts examined his supposed "leaks," they pointed out that what he'd shared with Chinese colleagues wasn't a restricted engineering design but in fact a schematic for an altogether different type of device. The case helped lead earlier this year to new Justice Department restrictions that took power away from prosecutors in the field and centralized certain investigations in Washington, where they could receive more oversight from a specially trained team of lawyers. Whether it's high- level physics research or the technology of our daily lives, the government's lawyers are struggling to grasp the increasingly technical cases that come before them. Both federal prosecutors and the attorneys who represent executive agencies in court are bungling lawsuits across the country because they don't understand what they're talking about. Too few lawyers have the skill set or the specialized knowledge to make sense of code, networks and the people who use them, and too few law schools are telling them what they need to know. "It would be enormously helpful to have a deeper bench of lawyers with technical backgrounds," says Susan Hennessey, a Brookings Institution fellow and former National Security Agency lawyer.

This situation is stymieing criminal investigations, upending innocents' lives and making it harder to set legal boundaries around mass- surveillance programs. The result is that, when it comes to technology, justice is increasingly out of reach.

Just this past week, a federal judge in Iowa threw out evidence collected by the FBI in a child porn investigation because the Justice Department's search warrant misstated the technical details of where and how it hoped to gather the evidence. As the judge concluded, either the FBI or the prosecutors hadn't understood exactly how their own "network investigative technique" worked, or they'd failed to explain it correctly in the courtroom. What's more, the judge who issued the original warrant didn't have the jurisdiction to do so, because the "network investigative technique," a piece of FBI-designed malware that sniffed out people trading illegal files, collected evidence far beyond the bounds of the Virginia district where the warrant was authorized.

Today, cyber, data and privacy questions lie at the core of numerous corporate and government cases, and there aren't anywhere near enough practicing lawyers who can adequately understand the complex issues involved, let alone who can sufficiently explain them in court or advise investigators on how to build a successful case. "This is a problem that pervades all of the national security apparatus," says Alvaro Bedoya, previously the chief counsel to the Senate Judiciary Committee's subcommittee on privacy, technology and the law, who now leads Georgetown Law's Center on Privacy & Technology. "You don't have a pipeline of lawyers right now who can read code."

The fallout from Edward Snowden's revelations exposed numerous instances in which agency lawyers miscommunicated to courts about what the government was doing. There are two possible explanations: Either they willfully exploited judges' lack of technical knowledge, or the lawyers themselves couldn't fathom the programs they were trying to explain. In a 2009 case that became public in 2013, NSA Director Keith Alexander admitted that none of the lawyers overseeing one surveillance program grasped what it was doing when it queried a particular agency database: "It appears there was never a complete understanding among the key personnel ... regarding what each individual meant by the terminology used." In a 2011 suit, Judge John Bates of the secret Foreign Intelligence Surveillance Court wrote an angry (and heavily redacted) 85-page decision saying he was "troubled" that the case marked "the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program." And in yet another case, Solicitor General Donald B. Verrilli Jr. found in 2013 that he'd misled the Supreme Court about how the Justice Department was using evidence derived from warrantless surveillance programs targeting foreigners, an error that led to a months-long internal debate as Verrilli questioned the department's interpretation of the law.

Such confusion is hardly confined to the NSA's most technical work. On a more mundane basis, government attorneys frequently confuse content and metadata, even though the two types of information face very different legal standards. One possible reason: The Justice Department's decade-old Electronic Surveillance Manual is incorrect about the basic mechanics of how email works, according

to a forthcoming article in the Harvard Journal of Law & Technology. Such problems are becoming more pervasive as lawyers misapply law designed for telephone surveillance to cases focused on the Internet, says Susan Landau, a computer scientist at Worcester Polytechnic Institute and one of the article's authors. They "don't know the right questions to ask." And it's not just them: "A judge may not even know what's wrong with the briefs. It's an extremely serious problem," she says.

Jurists have noticed how awkwardly analog-era laws govern modern digital life, and they've struggled over what to do with the disjunction, even at the Supreme Court. "It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," Justice Sonia Sotomayor wrote in a 2012 opinion. "... This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."

The Obama administration has made strides in incorporating technology into government, creating teams like the U.S. Digital Service that bring more of Silicon Valley to Washington. But the knowledge base of the government's lawyers is still badly lacking, particularly when it comes to marrying legal and technological tools, says Paul Ohm, a Georgetown law professor who used to work in the Justice Department's computer crime and intellectual property section. "Too much of [the focus] has been the import-export model - forgo your Silicon Valley salary for a couple years and help us be more savvy. And as awesome as that is, they're not going to solve the problem," Ohm says. The rotations through government are useful in the short term, but they don't help the bulk of the permanent workforce better understand the new digital landscape. "I've seen far less internal education at the agencies," Ohm says.

Some of today's technical legal befuddlement stems from the fact that the field is so new. "No one who is practicing today had a cybersecurity class in law school," explains Kristen Eichensehr, a UCLA law professor whose own cybersecurity course has doubled in the three years it's been offered. "Everyone who has been in practice has had to learn this on the job."

That problem won't go away soon: Even though student demand for such classes is growing, only a handful of mostly elite law schools - like Harvard, Yale, Cornell, Stanford, New York University, Georgetown and UCLA, as well as Indiana University's Maurer School of Law, which helped pioneer the field in the early 2000s - currently offer classes focused on cybersecurity. At Georgetown, Ohm is helping with what he thinks is the first law school class in the nation to teach students to code in the basic programming language Python. The course launched in January with spots for 20 students and a waitlist of more than 100. (For this school year, the class was expanded to 75 students but still had a long waitlist.) Among other projects, students learn to manipulate a 700-megabyte file of 200 years of Supreme Court opinions and code a search engine.

Yale, working with its first "cyber fellow," Ido Kilovaty, is offering its first mixed cybersecurity course this year, bringing together 10 law students and 10 computer science students in an attempt to bridge the jargon chasm between specialists in each field. "People who are trying to come up with solutions in this

area usually understand only one side - the law side or the technology side," Kilovaty says. "We want them to talk the same language when the class is done."

That's proving particularly essential in government, where few of the 93 U.S. attorney's offices around the nation have federal prosecutors who specialize in cyber-cases, even though cybercrime now touches every corner of the country. "Most lawyers are pretty deathly afraid of code. They don't even have a working knowledge - what an algorithm is, what a DDOS attack does, how a botnet operates," says Georgetown's Bedoya.

Kilovaty adds that too often he sees prosecutors limited by the complexity of the crimes confronting them. In one recent prosecution of a security researcher accused of illegal hacking, an assistant U.S. attorney summarized the case to the court by saying, "He had to download the entire iOS system on his computer, he had to decrypt it, he had to do all of these things I don't even understand." The government ultimately lost the case.

It is falling to law schools to educate attorneys who are already on the job. Georgetown hosts an annual conference on cyber- law. Stanford's Hoover Institution runs "cyber bootcamps" for congressional staffers who oversee the nation's technical and intelligence infrastructure, as well as for the judges who set precedent for how law will develop online. "Most of what they're getting is on-the-job learning. From a legal perspective, that's really troubling," says Amy Zegart, a Stanford intelligence expert who works on the cyber program.

Given the scope of the questions at hand - from digital eavesdropping to how the FBI should fight Russian ransomware attacks to how social-media sites can target user advertising and how Twitter should be blocking Islamic State recruitment online - the field will only grow more complicated and integral to daily life. "The number of people involved in cybersecurity [law] has to increase dramatically," says Harriet Pearson, who helps lead Hogan Lovells's cybersecurity and privacy practice, and who was IBM's first chief privacy officer. "There's going to need to be a huge amount of education."

The good news, at least, is that as the government scrambles to boost its cyber-law knowledge, students coming out of classes like Ohm's will have no shortage of job prospects.

garrett.graff@gmail.com

, an author and former editor of Politico Magazine, writes about national security, technology and politics.

Globe and Mail
Canada, China to discuss accord on cybersecurity
Tuesday, 27 September 2016
Byline: Colin Freeze

Prime Minister Justin Trudeau has directed his top security officials to discuss a cyber accord with China to help protect Canadian corporations from hackers.

The Prime Minister's national-security adviser, Daniel Jean, was sent to China earlier this month to co-chair the first in a series of meetings between the two countries' public-safety officials. These talks have become the focus of controversy because they include a possible extradition treaty.

Now The Globe and Mail has learned the discussions will also be a forum for Canada and China to iron out their differences on cybersecurity.

"The U.S. and U.K. recently concluded agreements with China not to engage in, or support, the theft of intellectual property and trade secrets to gain economic advantage," said Scott Bardsley, a spokesman for Public Safety Minister Ralph Goodale. "A similar agreement is a possible outcome."

Such a dialogue has profound implications for Canada's business community, given that Chinese government hackers are frequently seen as adversaries with a voracious appetite for corporate intellectual property as well as state secrets. Past victims of Chinese hacking campaigns include the federal government's National Research Council and, allegedly, the former telecom giant Nortel Networks.

The new security talks are a "forum for both countries to frankly discuss issues that need to be resolved," Mr. Bardsley said.

In September, 2015, U.S. President Barack Obama and Chinese President Xi Jinping announced a cyberaccord. Former British prime minister David Cameron unveiled a similar agreement when he met Mr. Xi one month later.

In April, a U.S. private-sector cybersecurity expert noted "a material downtick in what can be considered cyberespionage" after the U.S.-China accord. But U.S. government security officials have said they are unsure China is complying.

The president of the Business Council of Canada recently told The Globe that Canadian corporations are increasingly concerned about data theft of all kinds. "Many of the CEOs who are members of our council consider it their No. 1 risk factor," said John Manley, a former Liberal cabinet minister. "And they lose sleep over it."

Experts say diplomatic discussion of cybersecurity is a pressing need. Globally, recent months have shown that state-sponsored hackers and their proxies are becoming increasingly powerful in their bids to make mischief, steal secrets or engage in campaigns to sabotage utilities.

"If there is a general feeling, an assessment on the part of some hackers, there are no rules, that this is the law of the jungle, then that is a very destabilizing thing," Michael Walma, a senior Government Affairs Canada official, said during a conference last week.

Billed as Ottawa's "cyber foreign policy co-ordinator," he was one of several high-level civil servants who spoke at the Canadian Association of Security and Intelligence Studies (CASIS) symposium. Last Friday's discussion focused on cybersecurity and took place at Ottawa's War Museum.

Calling the discussion "timely," Mr. Walma told the gathering that Canadian diplomats are joining their counterparts in trying to iron out cybersecurity issues in bilateral and multilateral forums.

He specifically mentioned the U.S.-China accord as an example of what dialogue can achieve. But, he added, diplomatic agreements need to be backed up with deterrents, and pointed out that the United States is targeting state-sponsored hackers with criminal prosecutions, travel bans and financial sanctions.

"They are starting to equip themselves with a toolbox that allows them to respond with something between a diplomatic note and a nuclear strike," Mr. Walma quipped. "I think that kind of points to the way we should all be working."

In the summer of 2014, the U.S. government charged five officers of China's People's Liberation Army with hacking U.S. solar, steel and manufacturing companies. Shortly after, the United States launched a separate case against Vancouver-based Chinese national Su Bin, accusing him of helping PLA-affiliated hackers target aviation companies.

At that time, Canada's Conservative government publicly called out China for hacking into the computer networks of the National Research Council, the federal government's repository of secrets about emerging technology.

Whether "naming and shaming" foreign hackers accomplishes much was debated at the CASIS conference. "If you are going to call out an action by another country, there has to be actually something that's going to be a follow-up of some consequence," said Melissa Hathaway, a U.S. consultant who has advised two American presidents on cybersecurity.

She explained that any country that publicly accuses an autocratic country of hacking could expose its own expatriate citizens and corporate branch plants to countermeasures, given that such states react unpredictably when challenged.

Canada is not without some cybercapabilities. It is a member of the "signals intelligence" collective known as The Five Eyes, the world's most formidable electronic- spying alliance.

The Five Eyes' partners - agencies in Canada, the United States, Britain, Australia and New Zealand - are highly secretive, yet members publicly insist they do not spy on foreign corporations for the commercial gain of their countries' firms.

This was somewhat undercut in 2013, when Edward Snowden, a former U.S. government contractor, leaked documents that showed the Five Eyes frequently targeted the Chinese telecom giant Huawei Corp., among other foreign corporations.

The cyberaccords between the United States and Britain and China are primarily about stopping countries from spying on businesses. These accords sidestep state-on-state espionage - a prerogative governments have basically exercised since antiquity.

Yonhap News Agency
Prosecutors conduct 533 telecom-related monitoring since 2012: lawmaker
Tuesday, 27 September 2016
Byline: Staff reporter

Seoul - South Korean prosecutors conducted 533 individual cases of telecommunications-related monitoring through August from 2012, a lawmaker said Tuesday, urging the government to reorganize its privacy-related policies that can better protect the rights of its people.
Around 63 percent of the monitoring was made on request by South Korea's intelligence agency, the data compiled by Rep. Keum Tae-sup of the main opposition Minjoo Party of Korea showed.

Only 5.4 percent of the people involved, however, were notified of the monitoring, data showed.

"Nearly 95 percent of those monitored by investigators were not notified," Keum said. "There needs to be an improvement in policies to regulate abuse and protect the privacy of ordinary people."

ABC News
IBM 'unlikely to hit Customs and Immigration merger deadline' amid growing fears of system failure (Canada)
Tuesday, 27 September 2016
Byline: Matthew Doran and Chris Uhlmann

Canberra - Concerns are raised about IBM's ability to meet the demands of merging the Customs and Immigration computer systems. An IT failure could have serious national security implications as the mainframe will manage Australia's border controls, including red flagging terror suspects.

Serious concerns have been raised about IBM's ability to meet the demands of merging the Customs and Immigration computer systems by people familiar with the roll-out of the half-billion dollar contract.

The ABC has been told IBM looks increasingly unlikely to hit its October 31 deadline and there are growing fears in the Department of Immigration and Border Protection that the risk of a system failure is rising, as the busy Christmas holidays loom and a long-running industrial dispute remains unresolved.

An IT failure could have serious national security implications as the mainframe will manage Australia's border controls, including red flagging terror suspects attempting to enter or leave the country.

In response to a series of questions from the ABC, the department issued a statement saying: "This schedule remains under active review."

"This is common to all major system changes in which the protection of operational capability and security protections remains the overarching priority," the statement said.

The concerns about the enterprise-wide mainframe contract come in the wake of the high profile woes of another federal agency.

The Australian Bureau of Statistics was embarrassed by a census-night shutdown, .

The company is also currently embroiled in a Canadian payroll scandal, where .

And that echoes the billion-dollar health payroll debacle in Queensland, after which the .

Problems involving IBM would be 'deeply disturbing'

Labor's immigration spokesman Shayne Neumann said any problems involving IBM's contract with the department would be "deeply disturbing".

"You can't muck around with border protection and national security," Mr Neumann said.

"I have been to airports and seen the how the system works behind the scenes and any software problems will affect that."

He also pointed to a in the department when it came to procurement, and a between Immigration and Customs that said there was "an absence of a solid plan" for executing the integration.

"We can't have a department that's not up to the job and a tick-and-flick minister," Mr Neumann said.

Before Customs and Immigration merged in 2015, two companies had been delivering IT services -- IBM for Customs; and CSC, another US information technology giant, for Immigration.

CSC lost the bid for the combined tender and was told in February that its contract would be terminated 20 months early, with the new finish date set at October 31, this year.

That upped the ante on transferring enormous amounts of information between CSC-managed and IBM-managed data centres.

'Robust risk management framework in place'

As that deadline approaches, fears have grown within the department that IBM is not ready and that the system might fail.

There have been meetings between IBM and officials as they war game solutions, which might include IBM hiring CSC's workforce.

The total value through to 2019 of the mainframe contract is $509 million, and it is understood that the department does not have any more money to bolster the transition and is struggling to find the staff it needs within its own ranks to handle the change.

It is just one of many contracts IBM has with the Federal Government.

The department's statement in response to the ABC's questions also said it "has a robust risk management framework in place to address any potential risks that may arise from a large scale change to border systems".

"IBM has had a long relationship with the former Australian Customs and Border Protection Service and has maintained a stable computing environment for critical border systems," the statement said.

IBM said the department was also responding on its behalf.

Wall Street Journal
More Breaches Hit Swift System
Tuesday, 27 September 2016
Byline: Katy Burne

New York - Interbank message carrier Swift said customers had sustained three new cyber breaches over the summer and warned that attacks on banks in the network are continuing.
The company, whose systems are in the back offices of 11,000 financial institutions across more than 200 countries, issued the warnings as it rolled out new mandatory security requirements for customers.

Swift Chief Executive Gottfried Leibbrandt shared some anecdotal details of the fresh attacks in a speech at the company's annual conference in Geneva on Monday. He said a few months ago he got a series of calls from users with security breaches to report, although no money was stolen.

In the first, hackers had fraudulently sent payment instructions from the bank's Swift terminal to an unauthorized beneficiary and then altered payment records to cover their tracks. The next day, a second bank noticed the fraudulent messages being sent to the same rogue beneficiary. In the third instance, the same pattern of hacking was attempted but was thwarted with antivirus software that was part of a security patch.

The attacks follow a wave of cyberattacks on Swift bank customers in the past several months. Those attacks spanned the globe, including banks in Vietnam, Ecuador and one in Bangladesh where the thieves made off with $81 million from the country's central bank. The perpetrators remain unidentified and the money is yet to be returned.

In response, Swift, whose formal name is the Society for Worldwide Interbank Financial Telecommunication, has issued security patches and required customers to update their software, and encouraged banks that were attacked to share their findings on a restricted part of the network. Swift has also been under scrutiny from regulators.

"The attacks will continue and get more sophisticated. We are certainly not taking a break," Mr. Leibbrandt said. "I believe that in cyber, only the paranoid survive."

Swift has repeatedly said its core network, which processes the messages between senders and receivers, wasn't compromised.

Federal News Radio
Military intelligence cyber programs get boost from fund shift
Tuesday, 27 September 2016
Byline: Scott Maucione

Washington - The Defense Department is beefing up its cyber investments in the military intelligence arena by shifting some of its 2016 funds.
DoD moved nearly $20 million in funds from failing programs and contract savings early this summer to prioritize cyber, stated a reprogramming action released this week and signed by DoD Comptroller Michael McCord.

A large chunk of the funds will go to expanding the U.S. Army Intelligence and Security Command (INSCOM). The command, which conducts intelligence, security and information operations for military commanders, is set to receive about $6.2 million.

That money will go toward rapid research and development of low-density, non-standard technologies for cyberspace intelligence operations.

The funds will specifically go to upgrades for back-end enclaves, command and control device integration, integration of data storage capability supporting analytics and proxy and exit nodes.

"Without immediate funding, INSCOM will not be able to conduct the necessary system engineering changes to optimize the cyberspace platform, develop and modify cyberspace payloads, or conduct developmental and operational testing evaluation that enables the cyberspace mission," the reprogramming action stated.

DoD is also dropping money into the military services' IT, cyber and intelligence funds.

Nearly $3 million was programmed to the Air Force to build out and update tailored intelligence IT enterprise architectures for U.S. Strategic Command, U.S. Africa Command, U.S. European Command and U.S. Northern Command.

Those architectures are needed to create the Intelligence Community Information Technology Enterprise or ICITE. The ICITE network connects the intelligence agencies and military services all over the world to a common IT system.

Other services are also integrating in ICITE. The Army just restarted its ICITE initiative after a few years of delay. The service is slated to begin a small common desktop environment adoption pilot in 2017 that will create momentum for a larger movement in 2018 and 2019.

The Air Force is grabbing another $7.5 million for sensor and awareness systems. Funds will go to recapitalize Arc Storm system sites and upgrade system components. Those will be used to locate hostile electromagnetic interference of U.S. and allied satellites.

Other parts of the $7.5 million will go toward the Integrated Broadcast Service Enterprise, which provides near-real-time lethal warning and situational awareness to joint forces and coalition partners.

Finally, the reprogramming document gives $3 million to U.S. Cyber Command for classified purposes.

In the grand scheme of DoD's more than $600 billion budget, the recently released reprogramming seems tiny. But the direction of the funds does reiterate the Pentagon's increasing push toward cyber and space.

"Cyber operations and cyber security is a sustained area of focus for the Pentagon, and they will take advantage of the opportunity to add additional resources to that effort," Katherine Blakeley, a research fellow at the Center for Strategic and Budgetary Assessments told Federal News Radio.

This isn't the first time DoD has reprogrammed funds for cyber initiatives. In August, DoD requested to reprogram $100 million to uncover flaws in major weapons systems.

DoD already had $200 million set aside for the project, which it is required to inform Congress on in 2019.

SC Magazine
Presidential debate 2016: Candidates pledge cyber investment, differ on Russia
Tuesday, 27 September 2016
Byline: Teri Robinson

New York - In a brief exchange during the first of three presidential debates Monday night, former Secretary of State Hillary Clinton and Republican nominee Donald Trump agreed on the importance of investing in cybersecurity and briefly sparred over whether Russian hackers have a penchant for launching cyber attacks against U.S. targets.
Noting that the U.S. faces "two adversaries" - those hackers who engage in cyber espionage and nation-state actors, Clinton pledged that the country "will not sit idly by" as Russia, Iran, China and others ramp up their attacks. "We don't want to get into another kind of war," she said, but noted the U.S. will not back down. "Cyber warfare will be our biggest challenge."

Clinton specifically called out Russian President Vladmir Putin for "letting loose hackers allegedly behind hacks of the Democratic National Committee (DNC) and others.

But Trump contended that there was no proof that those hackers were Russian. "I don't think anyone knows whether Russia broke into the DNC," he said, adding that the hacks could be the work of another nation-state or group or even "someone 400 pounds sitting on a bed" with a laptop.

He also said that "ISIS is beating us at our own game" in cyberspace. "We have to do better," he said.

Clinton quickly noted that her plan for defeating ISIS includes a cyber component.

Slate
Donald Trump Defended Putin, Had No ISIS Plan, and Was Stunningly Ignorant on Iran
Tuesday, 27 September 2016
Byline: Fred Kaplan

Column - If anyone still thinks Donald Trump should be president after Monday night's debate, I'd like to know the reasons. In the segment dealing with foreign policy, he revealed himself--not for the first time, but more plainly than usual--to have little grasp of what power, diplomacy, and recent events are all

about. Hillary Clinton left a few gaps open as well, but the differences between the two could be measured in leagues, even light-years.
The first question was about cybersecurity and Russia's hacks of the Democratic National Committee. Hillary Clinton said we needed to make it clear that we're not going to let state actors go after our information, and that, while we don't want to unleash the full extent our far superior cyber powers, we will if this sort of "probing" continues. Trump came to the defense of Vladimir Putin, as he strangely has on many occasions, saying, "I don't think anybody knows it was Russia." The hacker, he added, could have been China, some other country, or "somebody sitting on their bed who weighs 400 pounds." (What is it with Trump and overweight people?) In fact, as his intelligence briefer could have told him (and perhaps did), there is no doubt that the hack came from Russia. Then Trump rambled, saying, "My 10- year-old son is so good with these computers, it's unbelievable. The security aspect of this cyber is very tough. We are not doing the job we should be doing." He also used the question as a chance to boast of his endorsement by lots of generals and admirals.

Neither candidate pointed out that the United States engages in a lot of cyberespionage as well, albeit not of the same type of espionage as Russia, China, and others. This is a contest that has been going on, though secretly, for decades.

Clinton spelled out her plan for defeating ISIS: recruiting Silicon Valley to block jihadist traffic online; intensifying air strikes; supporting Arab and Kurdish ground fighters; and launching an "intelligence surge" by promoting more cooperation among law-enforcement, intelligence agencies, and foreign intelligence. These are all good ideas, which the Obama administration has been pursuing very forcefully (if, in some cases, a little late). Trump put forth no plan, saying he didn't want to tell ISIS what he would do.

In a follow-up, Clinton pointed out that the fight against ISIS depends on our allies in the Middle East, who have Muslim-majority populations, which Trump has alienated with his rhetoric. Trump dismissed her premise, saying, "We've been working with them for many years, and we have the greatest mess anyone has ever seen." His alternative? He didn't say.

Trump said the biggest mistake happened when Obama pulled out of Iraq, even telling the jihadists the date of the withdrawal. After we left, ISIS erupted. Clinton noted, correctly, that the pullout date was specified in the 2008 Status of Forces Agreement signed during George W. Bush's presidency and that the Iraqi government would not allow any U.S. forces to remain after that date.

On NATO, Trump took credit, as he has in the past, for revitalizing the alliance. A while back, he said NATO was obsolete unless it helped us defeat terrorism--then, lo and behold, he read in the New York Times that NATO was creating a counterterrorism commission. "I think it's in large part because of what I said," he claimed. Clinton pointed out that, after the Sept. 11 attacks, all the NATO allies invoked Article 5--which says an attack on one member is an attack on all--and joined our war against al-Qaida and the Taliban in Afghanistan. She could also have pointed out that NATO issued specific "policy guidelines" on counterterrorism in 2012, well before Trump's off-hand remark.

And once again Trump prevaricated on the war in Iraq. He insisted that he always opposed the invasion, but then admitted that, in a 2002 interview, Howard Stern asked him about the war and, as he put it, "I said, 'I don't know, maybe.' " But, he insisted, he came out strongly against the war in an Esquire interview "shortly after the war started, I think in '04"--perhaps forgetting that the war started in March 2003.

Trump called the Iran nuclear deal "one of the worst deals ever made by any country in history," which, even if the deal's critics were right, betrays a stunning ignorance of history. Clinton pointed out that the deal puts a "cap" on Iran's nuclear program (that's an understatement, as it has actually forced Iran to dismantle almost the whole program) and added, "There's no doubt we have other problems with Iran, but I'd rather deal with those other problems having put that lid on their nuclear program."

Clinton didn't answer Trump's other claim about the deal--that it required us to pay Iran $150 billion--so I'll do it: That payment (and it hasn't been nearly that much) came from Iran's assets, which the United States and the European Union had frozen, as a sanction against its nuclear program. That was the deal: If Iran dismantles its nuclear program, the United States and the EU would unfreeze Iran's assets; that's what motivated Iran to make the deal.

The moderator, NBC anchor Lester Holt, asked whether the United States should adopt a "no-first-use" policy on nuclear weapons. This may have been the first time Trump had heard the phrase. First he said, "I certainly would not do first-strike; once the nuclear alternative happens, it's over"--an interesting comment that many doves might welcome--but then he said, in his next sentence, "At the same time, I can't take anything off the table." But that's what a no-first-use policy would do--explicitly take the nuclear option off the table. A quite detailed debate on this issue has been occupying the strategic community for decades, with legitimate points on both sides. It's not surprising that a real-estate tycoon is unfamiliar with the debate, but you'd think someone might have briefed him on it.

Clinton dealt with the question the way presidents generally do: "Words matter when you run for president, and they really matter when you are president. I want to assure our allies, in Japan and South Korea and elsewhere, that we have mutual defense treaties, and we will honor them." This, in response to Trump's point, famously made in a New York Times interview, that he might not come to the defense of an invaded ally if the ally hadn't paid its fair share--and that maybe it's not such a bad thing if such remarks compelled Japan and South Korea to build their own nuclear weapons.

Finally, Holt asked Trump what he meant when he said Clinton didn't have the "look" to be president. Trump replied, "She doesn't have the look, she doesn't have the stamina"--to which Clinton said, "As soon as he travels to 112 countries and negotiates a peace treaty, a cease-fire ... or even spends 11 hours testifying in front of a congressional committee, he can talk to me about stamina."

Game to Clinton.

Deutsche Presse-Agentur
Palestinian activists protest Facebook over incitement agreement
Tuesday, 27 September 2016

Palestinian social media activists said Monday that they have launched a campaign against Facebook, asking supporters to boycott the social media site for alleged bias towards Israel.
The campaign comes after several Palestinian journalists said Facebook blocked them from accessing their personal accounts last week and several news outlet pages were taken down.

All have since been reactivated, according to Husam al-Zayegh, a leader of the campaign and editor-in-chief at Gaza-based Shehab News Agency.

The Gaza-based activists are calling on supporters to avoid Facebook for two hours every night and to instead post on Twitter with the hashtag #FBCensorsPalestine.

"All we want is to see Facebook [act fairly] and implement its laws and regulations on all users," al-Zayegh told dpa.

The affected journalists say Facebook deactivated the pages in a bow to Israel following a September 12 agreement between the two to address concerns over material Israel says could incite terrorism.

Facebook said Monday the pages were mistakenly removed after being flagged, and that it restored them as soon as it learned of the error.

"Our team processes millions of reports each week, and we sometimes get things wrong. We're very sorry about this mistake," Facebook said in a statement.

Among other demands, the protesters want Facebook to withdraw from the Israeli agreement, arguing "it will contribute to further persecute Palestinians both on the ground and on the virtual space."

Facebook adheres to its own content removal policy, which has earned it criticism from Israeli politicians who have called for it to take down violence-inciting posts by Palestinians.

Press Trust of India
5th India-US cyber dialogue in New Delhi
Tuesday, 27 September 2016

A US delegation will participate in the fifth India-US cyber dialogue in New Delhi this week and interact with industry representatives to build strong regional partnerships with key stakeholders working on a range of cyber issues.

The US delegation is being led by Christopher Painter, US Department of State Coordinator for cyber issues, who along with the National Security Council Staff, will lead the American engagement on the broad set of cyber policy issues.

The fifth US-India Cyber Dialogue is part of an effort to build strong regional partnerships with key stakeholders working on a range of cyber issues, focusing on promoting an open, interoperable, reliable, and secure internet that benefits all users.

Daniel Sepulveda, Deputy Assistant Secretary of State and US Coordinator for International Communications and Information Policy, will lead the US-India Information and Communication Technology (ICT) Working Group which includes industry and government participation from both countries.

They will attend public events to engage with civil society and Indian youth on Internet and digital economy issues, a media release said.

At the ICT Working Group, it will be discussed how the US and India can work together to help expand the benefits of the digital economy to both of the countries and increase internet connectivity through programs like the Global Connect Initiative, which has a goal of bringing 1.5 billion new internet users online by 2020.

It World Canada
Ex-CSIS official backs Canada's attempt to get cyber promise from China
Wednesday, 28 September 2016
Byline: Howard Solomon

For several years Western governments have blamed official Chinese or Chinese-government backed groups for hacking into databases of public and private organizations. But a year ago the U.S. president Barack Obama and Chinese president president Xi Jinping signed an agreement not to direct or support cyberattacks that steal corporate data for economic benefit.
Now Canada wants to do the same.

A spokesman for Public Safety minister Ralph Goodale told the Globe and Mail that this country will try to get a similar agreement, which has also been negotiated between China and the United Kingdom.

The idea has the support of Ray Boisvert, a former assistant director for intelligence at the Canadian Security Intelligence Service (CSIS) who now has his own security consulting company.

"I do support this type of approach," he said in an email to ITWorldCanada.com. "As we collectively mature in this new networked, cyber-enabled world, be it governments, the private sector or citizens, we will have to apply all types of risk reduction strategies. And of course diplomacy should always be a first among strategic plays. It is no guarantee of success, especially without verification, but two previous agreements involving the U.S. and U.K. (and China) have recorded measurable reductions in cyber thefts of intellectual property and by extension breaches of individual privacy.

"We must do our utmost to get countries like China to enforce international laws and norms in regards to cyber security. Of course, I don't see that being possible with Russia at the moment as, unlike China, it has demonstrated total disregard for international agreements as it sees it's role as an unlawful, unregulated disruptor -- one that has pioneered new approaches in hybrid warfare (applying pressure on governments through stealth, including the enablement of proxies to attack Western organizations and institutions). "

Satyamoorthy Kabilan, director of national security and strategic foresight at the Conference Board of Canada, which represents CEOs was more cautious. "If such an agreement could be enforced, it could be a very worthwhile proposition. But we do need to look into the details - what does this cover, how will it be enforced, etc. I would be interested in finding out more about the exact terms before deciding on whether this would be a worthwhile effort."

Signing a deal and getting it implemented are two different things. In June the Wall Street Journal reported that nine months after a big ceremony at the White House the U.S. and China were still jousting over how to talk to each other. Apparently in the months all they could agree on were temporary email addresses for exchanging communications.

Early on there were signs that the agreement was limited to controlling the official intelligence agencies of each country. "With 1.3 billion people, (the premier) can't guarantee the behavior of every single person on Chinese soil," Obama was quoted as saying when the deal was signed.

One of the key problems of both sides in the Internet era is having absolute proof a government agency was behind an attack on a company.

In a paper earlier this year for the National Bureau of Asian Research, Adam Segal, a fellow at the U.S. Council on Foreign Relations, and Tang Lan, a deputy director at the China Institutes of Contemporary International Relations, wrote that the two countries have significant differences in their views on Internet governance, cyberattacks, cyber-espionage and the security of information and telecom equipment sold into each others' countries. Still they are both worried about threats to their critical infrastructure, stopping the proliferation of cyberattack capabilities of terrorist and criminal groups.

"While the two governments have vowed to clarify responsible behaviors through bilateral and multilateral discussions, identifying common ground and cooperative projects is necessary to reduce tensions in cyberspace," they wrote. But. they warned, failure to build on the agreement "could generate greater mistrust that spills over into other aspects of [their] relationship."

One thing both countries want to avoid, the report and other experts note, is cyber attacks -- particularly on critical infrastructure -- that lead to hostilities.

The academics noted that the U.S. and China have agreed on guidelines for requesting assistance on cybercrimes or other malicious cyber activities, as well as agreeing to conduct "tabletop exercises" and to define procedures for use of a hotline.

Globe and Mail
Privacy watchdog urges Ottawa to pass 'metadata' legislation
Wednesday, 28 September 2016
Byline: Colin Freeze

Canada's privacy czar is calling on the Liberals to fulfill a promise to pass laws constraining the federal spies who are allowed to capture records of Canadians' phone and Internet activities.
The Communications Security Establishment needs new legislation because it has not been careful enough in handling such material, says Daniel Therrien, the Privacy Commissioner of Canada. "The National Defence Act should be amended," he said in an interview. "I would want some clarity around the standards used to collect and share 'metadata.' Right now, the act is completely silent on this."

"Metadata" is the name federal officials give to phone logs, Internet exchanges and similar activity that spy agencies can electronically intercept in bulk. The substance of the underlying communications and the identities of communicators are not known.

CSE has been tasked with providing intelligence about foreigners to the Canadian cabinet since the 1940s. Mr. Therrien's call for new laws for CSE was formally made in his office's annual report on Tuesday. While the Liberals are not obliged to implement his findings, they promised new CSE laws on the campaign trail last year.

Canadian police officers who want access to an individual's phone records must get a judge to sign a warrant. CSE's technological analysts, which work with Canada's closest allies to capture and share communication trails of as many people as possible, operate without warrants and largely through secret edicts signed by the minister of national defence.

A once-classified "metadata ministerial directive" from the Liberal government of 2005 first told CSE it can capture and share as many phone and Internet logs as it can, so long as it does not go after Canadians specifically.

Should such metadata turn up in the wider trawl, the minster tells the spy agency to scrub out any known "Canadian identifying information" before sharing with allies.

During the 2015 campaign, the Liberals suggested they would like judges rather than ministers to make these decisions. The party has said almost nothing about constraining CSE since, but a spokeswoman for Defence Minister Harjit Sajjan told The Globe on Tuesday the government still hopes to introduce a law.

Problems with CSE metadata programs were revealed to the public earlier this year by the spy agency's watchdog, who reviews operations.

Jean-Pierre Plouffe, who is also calling for new laws for the spy agency, unveiled records showing the CSE bought privacy-protecting software that failed. Specifically, it did not remove identifiably Canadian phone logs and Internet Protocol exchanges.

So for years, potentially vast amounts of such material was shared in almost its raw form with allied agencies.

Mr. Sajjan played down the privacy implications, telling reporters the members of the intelligence partnership known as the Five Eyes - agencies in the United States, Britain, Australia, Canada and New Zealand -undertake to protect the privacy of one another's citizens, and not merely their own.

The privacy commissioner says such remarks cannot be taken at face value. "The privacy risk was minimized, downplayed."

Mr. Therrien said in the interview that the only reason spy agencies such as CSE collect metadata is that it is so very revealing.

And he added that no Five Eyes "gentlemen's agreement" overrides anyone's national interest.

When asked what kinds of worst-case scenarios could emerge from all this, Mr. Therrien cited the case of a Canadian software engineer once famously caught in the U.S. Central Intelligence Agency's crosshairs.

In 2001, Canadian officials wrongly red-flagged Maher Arar as a terrorist threat. He was arrested in a New York airport and flown on a CIA-leased jet to the Middle East and spent the next year jailed in his native Syria.

"We only need to think about Arar," Mr. Therrien said, adding that the Syrian-Canadian was tortured. "Arar is a real-life example of where information was shared to a third state. That is the worstcase scenario."

Sydney Morning Herald
Data delays thwart counter-terrorism
Wednesday, 28 September 2016
Byline: Rachel Olding

Sydney - Counter-terrorism police fear crucial information may slip through the cracks in major investigations because a national case- management system has not been rolled out, despite repeated requests for almost a decade.
The number of terrorism investigations in Australia is rising, yet officers say some are being jeopardised because each state police force uses a different system for managing investigations.

Fairfax Media understands that counter-terrorism police have picked up an increasing amount of communication between terror suspects in Sydney and Melbourne in recent months. Both cities remain the overwhelming focus of investigations.

But the country's eight police forces have 18 different systems and counter-terrorism police, who work in joint state and federal teams, are filing information twice into two systems.

Sam Mullins, professor of counter-terrorism at George C. Marshall European Center for Security Studies, interviewed 11 counter-terrorism officers from NSW, Victoria, Queensland and the AFP for a paper published in the latest Journal of Policing, Intelligence and Counter Terrorism.

While some officers viewed the issue as simply a hassle, others said it was jeopardising investigations.

"That would be the number one inhibitor that we've got today, because we miss out on so much intelligence," one Victorian officer said. "And missing [out] on something may well be that needle in a haystack."

An AFP officer said it needed fixing urgently because, if "a piece of information slips through the cracks, that may then have a ... significant implication".

A senior NSW officer said having to duplicate information is "a pain in the butt, it's costly, it's time-consuming".

The pace and frequency of terrorism investigations has rocketed since September 2014 when the national threat level was raised to probable. In some cases, police have been forced to move on rapidly radicalised individuals within hours.

There is "significantly more pressure" on information sharing, an AFP officer said.

Chief executive of the Police Federation of Australia Mark Burgess said police forces were getting an isolated picture of major incidents.

"One piece of information added to another piece added to another piece could become something vital," he said. "Sometimes the second, third or fourth piece is being missed."

The federation has been lobbying since 2007 for a $100 million national system, funded by criminals' confiscated assets.

In 2008, an inquiry into the bungled case of Queensland doctor Mohamed Haneef recommended a national system be adopted "as a matter of urgency".

Dr Haneef was detained, charged and had his visa cancelled on incorrect allegations of aiding a terrorist cousin in Britain. He was later awarded about $1 million compensation.

The inquiry found poor information sharing between Queensland police and the AFP meant evidence was not properly consolidated.

Justice Minister Michael Keenan said national security and counter terrorism legislation "is under constant review to ensure our law enforcement, security, and intelligence agencies have the tools and powers they need".

A feasibility study in 2009-10 highlighted a need to conduct further analysis on the economic and legal impacts associated with a national system.

The government spent $9.8 million last year on a two-year pilot of a national criminal intelligence database. Mr Burgess said a case-management system would be a logical extension but would require legislative change across all states.

The case-management system is the end-to-end process of managing a criminal case from the initial response to all aspects of the investigation, such as forensics and intelligence, to the prosecution.

Global Times
Security shortage
Wednesday, 28 September 2016
Byline: Cao Siqi

Beijing - Tech experts revealed that China is not training anywhere near enough IT workers to deal with digital threats issues at the country's largest cyber security event Tuesday.
"As of 2014, China has more than 700,000 cyber security talents working in key information system and infrastructure industries. By 2020, China will need about 1.4 million cyber security talents. In the last three years, we have recruited about 10,000 students pursuing cyber security, but we are hugely lagging behind demand," Feng Huamin, vice president of the Beijing Electronic Science and Technology Institute, said at a plenary session during China Cybersecurity Week held in Wuhan, capital of Central China's Hubei Province on Tuesday.

As China is launching a national push to train more cyber security talents, many top universities have started to offer cyberspace-related majors since 2015.

Vice Minister of Education Lin Huiqing said at a press conference in February that the number of new university majors involving cyber security, information countermeasures and confidential data management has surpassed 120 and other cyberspace-related majors have exceeded 4,800.

However, many cyber security experts at the Wuhan event pointed out that only a small proportion of China's schools offer such courses and there is a lack of qualified instructors, calling for the country to quickly establish a systematic discipline on cyber security education and promote more practical training.

No systematic method

At the session, Feng said that China now needs more cyber security talents working in several sectors, including those working in Party and government systems; in key infrastructure and information systems; and in combating cybercrimes and cyber terrorism.

Statistics show that China has 3,115 teachers involved in information security education but only 7 percent of them are classed as high-level talents.

Feng pointed out that only 10 percent of the 1,200 Chinese technology and science universities offer related majors while over 100 leading universities do not. Besides, only 15 Chinese universities have established cyber security schools and there is no systematic method for cyber security education.

In June 2015, China's State Council released a notice, demanding the quick establishment of a cyber security discipline and the cultivation of cyber security talents.

Moreover, Feng noted that a lack of practical training and high-quality instructors are also two highly important problems.

Ernest McDuffie, former director of the US National Initiative for Cybersecurity Education program, said at the Wuhan conference that he has not met many college students who have an interest in studying cyber security and the growth rate of global cyber security talents in 2015 was under their expectation.

Greater investment

Shen Changxiang, an academician at the Chinese Academy of Engineering, suggested China open classes to train minors and offer chances for special talents to study cyber security at college without taking the national college entrance examinations.

The Wuhan government has pledged to double the number of scholarships for cyber security majors and recruit top cyber security graduates from Chinese and overseas schools as well as the winners of cyber security contests. It will also open a class for minors and run special recruitment drives for "maverick geniuses."

Moreover, the city government will establish a new evaluation system. Instead of taking exams, cyber security majors will be evaluated based on their performance and priority will be given to those with practical and entrepreneurship experience.

As for cultivating first-class instructors, the Wuhan government vowed to offer twice the salary and research funds to the best cyber security experts compare to those working in similar positions.

Specifically, they will also receive 2 million yuan ($299,823) in subsidies and up to 100 million yuan in funding if they have innovative technologies that have a significant impact on the economy.

Mengchow Kang, board member of the Information Security Certification, called for the standardization of cyber security workforce development.

With such a system, cyber security talents, no matter where they are working, could get recognized with an international qualification, said Kang.

In February, China launched its first special fund for cyber security with initial capital of 300 million yuan to realize the nation's strategic goal of becoming a strong Internet power.

The fund, established by the China Internet Development Foundation, will be used to provide financial assistance to experts and teachers who specialize in cyber security.

Wall Street Journal
Facebook Told Not to Collect Data --- A German regulator ordered network to stop gathering WhatsApp user data
Wednesday, 28 September 2016
Byline: Friedrich Geiger

Berlin - A German privacy watchdog has ordered Facebook Inc. to stop collecting user data from its messenger subsidiary WhatsApp, the latest clash between European privacy authorities and the social network company.
Hamburg's commissioner for data protection, Johannes Caspar, said user-data exchange between the two services infringed on German data- protection law after WhatsApp changed its data-sharing terms last month. The Federation of German Consumer Organizations sent WhatsApp a similar warning.

A Facebook spokeswoman said, "We will appeal this order and we will work with the Hamburg [authority] in an effort to address their questions and resolve any concerns."

Facebook complied with EU data- protection law, she said. Mr. Caspar said Facebook reneged on a pledge it made on acquiring WhatsApp in 2014, when it said the services would keep user data separate. His office's order, Mr. Caspar said, protected the data of about 35 million WhatsApp users in Germany. WhatsApp has notified existing users of the change and given them the opportunity to opt out. In Mr. Caspar's view, however, Facebook is an independententity that also has to ask the permission of WhatsApp users.

"It has to be their decision whether they want to connect their accounts with Facebook," he said. "Facebook must ask their permission in advance (but) this did not happen."

In Germany, Mr. Caspar's office oversees Facebook's privacy practices because the company has its national office in Hamburg. His order forbids Facebook from collecting and storing data of German users of WhatsApp and requires the company to delete data it has received.

WhatsApp's plan to share user information with Facebook immediately raised concerns among privacy regulators in Europe when it was announced last month. The Article 29 Working Party, a body representing the European Union's 28 national data-protection authorities, at the time said its members were scrutinizing the WhatsApp change of terms "with great vigilance."

The change of terms is just one in a series of concerns about Facebook's data policies. France threatened the company with fines if it didn't change how it handled data, and Germany's Federal Cartel Office

earlier this year began an investigation into whether Facebook abused its dominance as a social network to harvest personal information.

According to Mr. Caspar, people who don't use WhatsApp or Facebook also were at risk of having their details collected should WhatsApp forward data that it collected from users' address books of external contacts.

"Facebook's answer that it hasn't done this yet nevertheless is a reason to worry that the magnitude of the data-protection breach will have a much more severe impact."

As part of its warning earlier this month, the Federation of German Consumer Organizations said it had given WhatsApp until Sept. 21 to agree to a cease-and-desist order regarding data transfer to Facebook. The federation's spokesman Timo Beyer said WhatsApp asked for a postponement of the deadline until Oct. 14, which was granted.

Al Jazeera
Opposing nuclear weapons in the era of millennials
Wednesday, 28 September 2016
Byline: James Reinl

New York - The mushroom clouds of nuclear explosions cast a long shadow over the 20th century. The fungal smoke stacks provoked fear of an atomic apocalypse and became a rallying symbol for anti-war activists.
Their fright factor may be waning. The Cold War arms race was over by the time millennials were born. For the Instagram generation, cyber-strikes and hijacked jets hitting skyscrapers weigh heavier on the mind.

"Nuclear weapons kind of faded down once, like, the issue of terrorism and 9/11 happened," New York high school pupil Lucy Li, 16, told Al Jazeera. World War II was a long time back, she said. "Terrorism is the main focus and worry right now."

This month, Li and other teens visited the United Nations headquarters to learn about the 1945 bombing of Hiroshima from survivor Setsuko Thurlow, 84, who relived harsh childhood memories of the blast, infernos and relatives dying from radiation sickness.

Thurlow worries that the strike, which claimed some 140,000 lives by the end of the year, was too-quickly forgotten. People "went back to sleep", she told Al Jazeera. "We gotta clean up this mess before we pass on the planet to the next generation."

Lecturing youngsters is only half the battle. Downstairs at the world body, diplomats were hatching plans to outlaw nuclear weapons, of which there are more than 15,000 globally, owned by nine countries.

Many nations abhor the weapons, saying any nuclear strike would kill masses of civilians and automatically constitute an atrocity. Like mustard gas and land mines, they are inhuman and should be banned, they say.

For several years, Austria, a landlocked European nation, has built support for a push against Russia and the United States - which have the lion's share of nuclear weapons - and other nuclear powers in a bid to declare the weapons illegal.

On September 21, Austria's Foreign Minister, Sebastian Kurz , told the UN General Assembly that Austria "will table a draft resolution to convene negotiations on a legally-binding comprehensive instrument to prohibit nuclear weapons".

Diplomats familiar with the talks told Al Jazeera that Austria, Mexico and others will shortly release a UN General Assembly resolution that already has the support of more than 120 of the UN's 193 members.

The document is still being drafted in Geneva, but is expected to arrange a confab aimed at creating a nuclear weapons treaty akin to legal prohibitions on chemical weapons, landmines and cluster bombs .

"We all agree that the humanitarian consequences of the explosion of nuclear weapons would be unacceptable," said Kurz. "Experience shows that the first step to eliminate weapons of mass destruction is to prohibit them through legally-binding norms."

In some ways, he is preaching to the converted. The five legally-recognised nuclear-armed states - the United States, Russia, France, China and Britain - known as the P5, have long vowed to ditch their doomsday arsenals under the Non-Proliferation Treaty.

In 2009, US President Barack Obama called for a world without nuclear weapons while in Prague. His New START deal with Russia, ratified the next year, cut the number of deployed strategic nuclear warheads to 1,550.

In his UN address this month, Obama spoke of his "unique responsibility" to scrap nuclear weapons and on September 23 the UN Security Council passed a resolution supporting a 20-year-old treaty against nuclear test blasts.

But progress is too slow for Austria and others. Despite talk of disarmament, the US will spend some $1 trillion over three decades to modernise its nuclear arsenal. Britain plans to renew its missile-launching submarines.

Prospects for more US-Russia deals are bleak, given the rows over Ukraine and Syria. Donald Trump, the Republican presidential nominee in this year's White House race, even suggested that Japan and South Korea acquire the weapons.

Meanwhile, the nuclear-toting states outside the NPT - Pakistan, India, North Korea and also Israel, which neither confirms nor denies its stockpiles - answer to nobody. Some fear that Iran will join them after its 10-year deal with the US and others expires.

North Korea came closer to being able to launch nuclear warheads at neighbours this month with its fifth test blast. Pakistan is deploying small, tactical nuclear weapons to deter India that could be stolen or misused.

The UN calls for a world free of nuclear weapons and marks September 26 as the International Day for the Total Elimination of Nuclear Weapons, but has largely shelved the issue to focus on more-likely gains against poverty and climate change.

Thomas Countryman, the US State Department's point man on nuclear arms, called Austria's effort "meaningless" and "dangerous". Pyongyang's recent test blast showed why the US should retain its deterrent advantage, he said.

"The international security environment needs to evolve in a way that gives the Russian Federation and the United States first, and later other nuclear weapon states, the confidence to negotiate further reductions in their nuclear arsenals," Countryman told Al Jazeera. "That is not something that can be accomplished by outside pressure from other states or from NGOs."

Opinions are mixed on whether Austria will achieve anything beyond a UN General Assembly resolution, which carry moral, not legal, force. Joseph Gerson, an anti-war activist, predicted an "intense fight" between the P5 and smaller UN members.

"It's the many against a few, but the few have considerable power," Gerson, from the American Friends Service Committee, a Quaker group, told Al Jazeera. "The US has sent out a demarche to quite a number of countries telling them not to push on this."

Kenneth Luongo, president of the Centre for a Secure Nuclear Future, a policy group, doubts that the US or Russia will yield to pressure. Their generals, however, may scrap some costly nuclear arms for weapons better suited against armed groups and other, more urgent, threats.

Global risk analyst Ian Bremmer, president of the Eurasia Group, says the threat of nuclear brinksmanship has subsided, while cyber-strikes are ever-more menacing and available to many more than the nine nuclear powers.

While envoys negotiate between governments, the activists continue campaigning, though without the frequent "Ban the Bomb" marches that once drew big crowds in western cities but dwindled from the 1980s onwards.

Hidenori Watanave, a Harvard University scholar, is building an online archive of survivors' testimonies from Hiroshima. Youngsters can use it to become "storytellers about the atomic bomb" via Facebook-style sharing, once Thurlow and others like her are gone, he told Al Jazeera.

His project and other efforts are having an impact, however limited. After the UN class, pupil Li grappled with a question that vexed even Robert Oppenheimer, the physicist behind America's nuclear project, seven decades ago.

"I feel like they were created in this race to show who is the No 1, like, most powerful country in the world," Li said. "What I don't get is why you would create a weapon that could destroy the world in a few seconds, just for the sake of power."

Associated Press
Across US, police officers abuse confidential databases
Wednesday, 28 September 2016
Byline: Staff report

Denver - Police officers across the country misuse confidential law enforcement databases to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work, an Associated Press investigation has found.
Criminal-history and driver databases give officers critical information about people they encounter on the job. But the AP's review shows how those systems also can be exploited by officers who, motivated by romantic quarrels, personal conflicts or voyeuristic curiosity, sidestep policies and sometimes the law by snooping. In the most egregious cases, officers have used information to stalk or harass, or have tampered with or sold records they obtained.

No single agency tracks how often the abuse happens nationwide, and record-keeping inconsistencies make it impossible to know how many violations occur.

But the AP, through records requests to state agencies and big-city police departments, found law enforcement officers and employees who misused databases were fired, suspended or resigned more than 325 times between 2013 and 2015. They received reprimands, counseling or lesser discipline in more than 250 instances, the review found.

Unspecified discipline was imposed in more than 90 instances reviewed by AP. In many other cases, it wasn't clear from the records if punishment was given at all. The number of violations was surely far higher since records provided were spotty at best, and many cases go unnoticed.

Among those punished: an Ohio officer who pleaded guilty to stalking an ex-girlfriend and who looked up information on her; a Michigan officer who looked up home addresses of women he found attractive; and two Miami-Dade officers who ran checks on a journalist after he aired unflattering stories about the department.

"It's personal. It's your address. It's all your information, it's your Social Security number, it's everything about you," said Alexis Dekany, the Ohio woman whose ex- boyfriend, a former Akron officer, pleaded guilty last year to stalking her. "And when they use it for ill purposes to commit crimes against you - to stalk you, to follow you, to harass you ... it just becomes so dangerous."

The misuse represents only a tiny fraction of the millions of daily database queries run legitimately during traffic stops, criminal investigations and routine police encounters. But the worst violations profoundly abuses systems that supply vital information on criminal suspects and law-abiding citizens alike. The unauthorized searches demonstrate how even old-fashioned policing tools are ripe for abuse, at a time when privacy concerns about law enforcement have focused mostly on more modern electronic technologies. And incomplete, inconsistent tracking of the problem frustrates efforts to document its pervasiveness.

The AP tally, based on records requested from 50 states and about three dozen of the nation's largest police departments, is unquestionably an undercount.

Some departments produced no records at all. Some states refused to disclose the information, said they don't comprehensively track misuse or produced records too incomplete or unclear to be counted. Florida reported hundreds of misuse cases of its driver database, but didn't say how often officers were disciplined.

And some cases go undetected, officials say, because there aren't clear red flags to automatically distinguish questionable searches from legitimate ones.

"If we know the officers in a particular agency have made 10,000 queries in a month, we just have no way to (know) they were for an inappropriate reason unless there's some consequence where someone might complain to us," said Carol Gibbs, database administrator with the Illinois State Police.

The AP's requests encompassed state and local databases and the FBI-administered National Crime and Information Center, a searchable clearinghouse that processes an average of 14 million daily transactions.

The NCIC catalogs information that officers enter on sex offenders, immigration violators, suspected gang members, people with outstanding warrants and individuals reported missing, among others. Police use the system to locate fugitives, identify missing people and determine if a motorist they've stopped is driving a stolen car or is wanted elsewhere.

Other statewide databases offer access to criminal histories and motor vehicle records, birth dates and photos.

Officers are instructed that those systems, which together contain data far more substantial than an internet search would yield, may be used only for legitimate law enforcement purposes. They're warned that their searches are subject to being audited and that unauthorized access could cost them their jobs or result in criminal charges.

Yet misuse persists.

'SENSE OF BEING VULNERABLE'

Violations frequently arise from romantic pursuits or domestic entanglements, including when a Denver officer became acquainted with a hospital employee during a sex-assault investigation, then searched out her phone number and called her at home. A Mancos, Colorado, marshal asked co- workers to run license plate checks for every white pickup truck they saw because his girlfriend was seeing a man who drove a white pickup, an investigative report shows.

In Florida, a Polk County sheriff's deputy investigating a battery complaint ran driver's license information of a woman he met and then messaged her unsolicited through Facebook.

Officers have sought information for purely personal purposes, including criminal records checks of co-workers at private businesses. A Phoenix officer ran searches on a neighbor during the course of a longstanding dispute. A North Olmsted, Ohio, officer pleaded guilty this year to searching for a female friend's landlord and showing up in the middle of the night to demand the return of money he said was owed her.

The officer, Brian Bielozer, told the AP he legitimately sought the landlord's information as a safety precaution to determine if she had outstanding warrants or a weapons permit. But he promised as part of a plea agreement never to seek a job again in law enforcement. He said he entered the plea to avoid mounting legal fees.

Some database misuse occurred in the course of other misbehavior, including a Phoenix officer who gave a woman involved in a drug and gun-trafficking investigation details about stolen cars in exchange for arranging sexual encounters for him. She told an undercover detective about a department source who could "get any information on anybody," a disciplinary report says.

Eric Paull, the Akron police sergeant who pleaded guilty last year to stalking Dekany, also ran searches on her mother, men she'd been close with and students from a course he taught, prosecutors said. A lawyer for Paull, who was sentenced to prison, said Paull has accepted responsibility for his actions.

"A lot of people have complicated personal lives and very strong passions," said Jay Stanley, an American Civil Liberties Union privacy expert. "There's greed, there's lust, there's all the deadly sins. And often, accessing information is a way for people to act on those human emotions."

Other police employees searched for family members, sometimes at relatives' requests, to check what information was stored or to see if they were the subjects of warrants.

Still other searchers were simply curious, including a Miami-Dade officer who admitted checking dozens of officers and celebrities including basketball star LeBron James.

Political motives occasionally surface.

Deb Roschen, a former county commissioner in Minnesota, alleged in a 2013 lawsuit that law enforcement and government employees inappropriately ran repeated queries on her and other politicians over 10 years. The searches were in retaliation for questioning county spending and sheriff's programs, she contended.

She filed an open-records request that revealed her husband and daughter were also researched, sometimes at odd hours. But an appeals court rejected her suit and several similar cases this month, saying the plaintiffs failed to demonstrate the searches were unpermitted.

"Now there are people who do not like me that have all my private information ... any information that could be used against me. They could steal my identity, they could sell it to someone," Roschen said.

"The sense of being vulnerable," she added, "there's no fix to that."

BETRAYAL OF TRUST

Violations are committed by patrol officers, dispatchers, civilian employees, court personnel and high-ranking police officials. Some made dozens of improper searches. Some were under investigation for multiple infractions when they were punished, making it unclear whether database misuse was always the sole reason for discipline.

Agencies uncover some violations during audits, or during investigations into other misconduct. Some emerge after a citizen, often the target of a search, finds out or grows suspicious. A Jacksonville, Florida,

sheriff's officer was found to have run queries on his ex-girlfriend and her new boyfriend after she raised concerns she was being harassed, an internal affairs report says.

The AP sought to focus on officers who improperly accessed information on others but also counted some cases in which officers divulged information to someone not authorized to receive it, or ran their own names for strictly personal purposes, including to check their car registrations.

The tally also includes some cases in which little is known about the offense because some agencies provided no details - only that they resulted in discipline.

The AP tried when possible to exclude benign violations, such as new employees who ran only their own names during training or system troubleshooting. But the variability in record-keeping made it impossible to weed out all such violations.

Agencies in California, for instance, reported more than 75 suspensions, resignations and terminations between 2013 and 2015 arising from misuse of the California Law Enforcement Telecommunications System, state records show. But because the records didn't identify officers or specify the allegations, it's unclear whether multiple violations were committed by the same person or how egregious the infractions were.

Colorado disclosed about 35 misuse violations without specifying punishment. Indiana listed 12 cases of abuse but revealed nothing about them. The Florida Department of Highway Safety and Motor Vehicles reported about 400 violations in 2014 and 2015 of its Driver and Vehicle Information Database, or DAVID, but didn't include the allegations or punishment.

The FBI's Criminal Justice Information Services Division offers training to state and local law enforcement agencies on NCIC use, and conducts audits every three years that include a sample of local departments, said spokesman Stephen Fischer.

But it doesn't track how often NCIC information is misused. Violations, which are not required to be reported directly to the FBI, are inconsistently disclosed to the federal government. The FBI relies on local agencies to address violations that are identified, Fischer said.

The AP requested records from large police departments and state agencies tasked with administering NCIC usage within their districts. The responses included cases where officers misused motor vehicle data, including driver's license and registration information, and also more sensitive criminal history records.

Officers are only occasionally prosecuted, and rarely at the federal level.

One recent exception is a former Cumming, Georgia, officer charged in June with accepting a bribe to search a woman's license plate number to see if she was an undercover officer. Another involved Ronald

Buell, a retired New York Police Department sergeant who received probation for selling NCIC information to a private investigator for defense attorneys.

At his July sentencing, Buell said he hoped other officers would learn "to never put themselves in the position I'm in."

It's unsettled whether improper database access is necessarily a federal crime and whether it violates a trespass statute that criminalizes using a computer for other than authorized purposes.

A federal appeals court last year reversed the computer-crime conviction of ex-NYPD officer Gilberto Valle, whom tabloids dubbed the "cannibal cop" for his online exchanges about kidnapping and eating women and who improperly used a police database to gather information. Valle argued that as an officer, he was legally authorized to access the database. The court deemed the statute ambiguous and said it risked criminalizing a broad array of computer use.

Misuse has occasionally prompted federal lawsuits under a statute meant to protect driver's license data.

A Florida Highway Trooper, Donna Watts, accused dozens of officers of searching her in the state's driver database after she stopped a Miami-Dade officer for speeding in 2011. She alleged in lawsuits that she was harassed with prank calls, threatening posts on law enforcement websites and unfamiliar cars that idled near her home.

Each unlawful access, she said in a court document, "has either caused or worsened anxiety, depression, insomnia, and other medical/physical/psychological conditions I suffer."

Law enforcement officials have taken steps to try to limit abuse, though they say they know of no foolproof safeguard given the volume of inquiries and the need for officers to have information at their fingertips.

"There's no system that could prohibit you from looking up your ex-wife's new boyfriend, because your ex-wife's new boyfriend could come in contact with the criminal justice system," said Peggy Bell, executive director of the Delaware Criminal Justice Information System.

The Minnesota Department of Public Safety said it changed the way officers access a state driver database after a 2013 legislative audit found over half of the 11,000 law enforcement personnel who use it made searches that appeared questionable. The audit was conducted after a former state employee was charged with illegally viewing thousands of driver's license records.

In Florida, a memorandum of understanding this year increased the amount of field audits law enforcement agencies must undergo regarding DAVID usage. Troopers in the Florida Highway Patrol sign

usage warnings when they access the DAVID system and a criminal sanctions acknowledgment. Users are audited and instructed to select a reason for a search before making inquiries.

Denver's independent monitor, Nicholas Mitchell, argued for strong policies and strict discipline as a safeguard, especially as increasing amounts of information are added to databases. His review found most of the 25 Denver officers punished for misusing databases over 10 years received at most reprimands.

Miami-Dade police cracked down after the Watts scandal and other high-profile cases. The department now does quarterly audits in which officers can be randomly asked to explain searches. A sergeant's duties have been expanded to include daily reviews of proper usage and troubleshooting, said Maj. Christopher Carothers of the professional compliance bureau.

Even if the public is unaware of the amount of available information, Carothers said, "The idea that police would betray that trust out of curious entertainment or truly bad intent, that's very disturbing and unsettling."

New York Times
Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say
Wednesday, 28 September 2016
Byline: Nicole Perlroth, Vindu Goel

San Francisco - Six years ago, Yahoo's computer systems and customer email accounts were penetrated by Chinese military hackers. Google and a number of other technology companies were also hit.
The Google co-founder Sergey Brin regarded the attack on his company's systems as a personal affront and responded by making security a top corporate priority. Google hired hundreds of security engineers with six-figure signing bonuses, invested hundreds of millions of dollars in security infrastructure and adopted a new internal motto, "Never again," to signal that it would never again allow anyone -- be they spies or criminals -- to hack into Google customers' accounts.

Yahoo, on the other hand, was slower to invest in the kinds of defenses necessary to thwart sophisticated hackers that are now considered standard in Silicon Valley, according to half a dozen current and former company employees who participated in security discussions but agreed to describe them only on the condition of anonymity.

When Marissa Mayer took over as chief executive of the flailing company in mid-2012, security was one of many problems she inherited. With so many competing priorities, she emphasized creating a cleaner look for services like Yahoo Mail and developing new products over making security improvements, the Yahoo employees said.

The "Paranoids," the internal name for Yahoo's security team, often clashed with other parts of the business over security costs. And their requests were often overridden because of concerns that the inconvenience of added protection would make people stop using the company's products.

But Yahoo's choices had consequences, resulting in a series of embarrassing security failures over the last four years. Last week, the company disclosed that hackers backed by what it believed was an unnamed foreign government stole the credentials of 500 million users in a breach that went undetected for two years. It was the biggest known intrusion into one company's network, and the episode is now under investigation by both Yahoo and the Federal Bureau of Investigation.

Certainly, many big companies have struggled with cyberattacks in recent years. But Yahoo's security efforts appear to have fallen short, in particular, when compared with those of banks and other big tech companies.

To make computer systems more secure, a company often has to make its products slower and more difficult to use. It was a trade-off Yahoo's leadership was often unwilling to make.

In defense of Yahoo's security, a company spokeswoman, Suzanne Philion, said the company spent $10 million on encryption technology in early 2014, and that its investment in security initiatives will have increased by 60 percent from 2015 to 2016.

"At Yahoo, we have a deep understanding of the threats facing our users and continuously strive to stay ahead of these threats to keep our users and our platforms secure," she said.

The breach disclosed last week is the latest black eye for Ms. Mayer, whose failed turnaround effort resulted in Yahoo's agreement in July to sell its core operations to Verizon for $4.8 billion. It is unclear whether the episode will affect the sale. Although Yahoo's email users are its most loyal and frequent customers, the company has been losing market share in email for years.

"Yahoo is already suffering. I don't think they'll suffer more because of this," said Avivah Litan, a security analyst with the research firm Gartner.

Ms. Mayer arrived at Yahoo about two years after the company was hit by the Chinese military hackers. While Google's response was public, Yahoo never publicly admitted that it had also been attacked.

A former Google executive credited with creating the search company's simple, colorful aesthetic, Ms. Mayer turned her attention at Yahoo to beating Google at search, creating new mobile apps, and turning Yahoo into a video powerhouse with television-style broadcasts featuring big-name talent like Katie Couric.

But in matters of security, Ms. Mayer, current and former employees said, was far more reactive. In 2010, Google announced it would start paying hackers "bug bounties" if they turned over security holes

and problems in its systems. Yahoo did not do the same until three years later, after it lost countless security engineers to competitors and experienced a breach of more than 450,000 Yahoo accounts in 2012 and a series of humiliating spam attacks in 2013. Yahoo said it had paid out $1.8 million to bug hunters.

In 2013, disclosures by Edward J. Snowden, the former National Security Agency contractor, showed that Yahoo was a frequent target for nation-state spies. Yet it took a full year after Mr. Snowden's initial disclosures for Yahoo to hire a new chief information security officer, Alex Stamos.

Jeff Bonforte, the Yahoo senior vice president who oversees its email and messaging services, said in an interview last December that Mr. Stamos and his team had pressed for Yahoo to adopt end-to-end encryption for everything. Such encryption would mean that only the parties in a conversation could see what was being said, with even Yahoo unable to read it.

Mr. Bonforte said he resisted the request because it would have hurt Yahoo's ability to index and search message data to provide new user services. "I'm not particularly thrilled with building an apartment building which has the biggest bars on every window," he said.

The 2014 hiring of Mr. Stamos -- who had a reputation for pushing for privacy and antisurveillance measures -- was widely hailed by the security community as a sign that Yahoo was prioritizing its users' privacy and security.

The current and former employees say he inspired a small team of young engineers to develop more secure code, improve the company's defenses -- including encrypting traffic between Yahoo's data centers -- hunt down criminal activity and successfully collaborate with other companies in sharing threat data.

He also dispatched "red teams" of employees to break into Yahoo's systems and report back what they found. At competitors like Apple and Google, the Yahoo Paranoids developed a reputation for their passion and contributions to collaborative security projects, like Threat Exchange, a platform created by Yahoo, Dropbox, Facebook, Pinterest and others to share information on cyberthreats.

But when it came time to commit meaningful dollars to improve Yahoo's security infrastructure, Ms. Mayer repeatedly clashed with Mr. Stamos, according to the current and former employees. She denied Yahoo's security team financial resources and put off proactive security defenses, including intrusion-detection mechanisms for Yahoo's production systems. Over the last few years, employees say, the Paranoids have been routinely hired away by competitors like Apple, Facebook and Google.

Mr. Stamos, who departed Yahoo for Facebook last year, declined to comment. But during his tenure, Ms. Mayer also rejected the most basic security measure of all: an automatic reset of all user passwords, a step security experts consider standard after a breach. Employees say the move was rejected by Ms.

Mayer's team for fear that even something as simple as a password change would drive Yahoo's shrinking email users to other services.

On Tuesday, six Democratic senators, led by Patrick Leahy of Vermont, sent a letter to Ms. Mayer demanding more details about the 2014 breach and what Yahoo was doing to prevent a recurrence. Another senator, Mark Warner, Democrat of Virginia, has asked the Securities and Exchange Commission to investigate Yahoo's disclosures to investors regarding the incident. And the company is already the subject of several class-action lawsuits from users over the intrusion.

Reuters
At your service: cyber criminals for hire to militants, EU says
Wednesday, 28 September 2016
Byline: Staff report

Brussels - Cybercriminals offering contract services for hire offer militant groups the means to attack Europe but such groups have yet to employ such techniques in major attacks, EU police agency Europol said on Wednesday.
"There is currently little evidence to suggest that their cyber- attack capability extends beyond common website defacement," it said in its annual cybercrime threat assessment in a year marked by Islamic State violence in Europe.

But the internet's criminal shadow the Darknet had potential to be exploited by militants taking advantage of computer experts offering "crime as a service", Europol added: "The availability of cybercrime tools and services, and illicit commodities (including firearms) on the Darknet, provide ample opportunities for this situation to change."

Overall, the report found, existing trends in cybercrime continued to grow, with some of the European Union's member states reporting more cyber crimes than the traditional variety.

"Europol is concerned about how an expanding cybercriminal community has been able to further exploit our increasing dependence on technology and the internet," its director, Rob Wainwright, said in a statement. "We have also seen a marked shift in cyber- facilitated activities relating to trafficking in human beings, terrorism and other threats."

"Ransomware" - programs which break into databases and demand payment for unlocking codes via virtual currencies such as Bitcoin - continued to expand as a problem, as did highly targeted "phishing" attacks to extract security data from senior figures - "CEO fraud" - and video streaming of child abuse.

Attacks on bank cash-machine networks were also increasing, the report found, as were frauds exploiting new contactless payment card transactions, while traditional scams involving the physical presence of a card had been successfully reduced.

Khaleej Times
Be cautious using social media, experts stress
Wednesday, 28 September 2016
Byline: Rohma Sadaqat

Dubai - The power of social media today for both consumers and businesses can't be ignored, however users have to be cautious about how they choose to consume it, experts at a panel discussion on media and technology have said.
The event brought together a number of industry experts including Sara Al Madani, board member of the Sharjah Chamber of Commerce and Industry; Shereen Ghabrial, general manager of Pyramedia Media Consultancy & Production; Vinay Kamat, editor of Khaleej Times; and Noor Shamma, founder of the Postcard Initiative.

"Technology has become part of our lives 24/7," said Saghir Ahmed Khan, senior vice president of finance and operations at Khaleej Times, in his opening address. "It needs to be embraced rather than adapted for us to reap its rewards. However, we have to be careful about the extent to which we use technology in our daily lives. We should be careful in that we don't allow it to affect they way that we interact with the people around us."

Al Madani highlighted how social media today is a platform for many users to share their culture with millions of people around the world. Through social media platforms such as facebook, twitter, and Instagaram, people can learn about different cultures, trends, and what is making news around the world. However, she also pointed out that with the many positives that come with using social media, there were also a few negatives such as inappropriate content, and being bombarded with information that has nothing to do with you.

"It is important to choose a social media platform that works best for you," she said. "Some people will of course misuse it, so it is up to you to determine how best to use it. If something offends you, then you can easily choose to ignore it or unfollow that person. Choose to follow what interests you, and you will have a whole world of opportunities open to you, whether it has to do with business, entertainment, or lifestyle."

Like Al Madani, Shamma cautioned attendees on using social media and technology to an extent where it is having a negative impact on your relationship with different people. "You must remember that some people, especially elders think it is offensive when you are on your phone constantly in front of them. For them it is a sign of respect when you give them your full attention. Also it is very important to monitor what children today are learning from social media, because everything, and I mean everything today is online. A lot of the content is inappropriate for young children and care should be taken to make sure that they aren't exposed to it."

Ghabrial pointed out how businesses that fail to have a social media presence in this day and age will not be very successful.

"Most businesses today have several different social media accounts that are linked to their website, and which they rely on to reach a wider audience," he said. "For example, a fashion house might have five shops in different locations that attract a certain number of customers. Now, with social media that same company can attract almost triple the number of their current clients. Their penetration online can reach millions of people. Also your reach isn't limited; for many businesses in the UAE today, social media is the tool with which they can expand their operations to the other GCC countries. E-trading is the name of the game now, and people are making millions through the use of social media."

Kamat also highlighted how social media has impacted journalism and mainstream media. "Journalism has had various transformational points throughout history. January 15, 2009 was one such date which sent out a signal that journalism as we knew it was about to change," he said.

It was the date that US Airways Flight 1549, on a routine flight from New York to North Carolina, ran into problems when a flock of birds flew directly into the plane's engines, rendering both useless. The aircraft was forced to make a controlled water landing on the Hudson River. The playing field was immediately changed when a single tweet, from one of the rescuers, headed for the floating aircraft reached millions of people, almost 15 minutes before any major news channel had even reached the site.

Fox News
Fewer than one in five State Dept employees with security clearance completed classified info training
Wednesday, 28 September 2016
Byline: Catherine Herridge

Washington - Fewer than one in five employees with a security clearance at the State Department has completed the mandated training for handling classified information as required by a 2009 Executive Order signed by President Obama, according to a new report from the government watchdog with oversight.
"Based on training records obtained from the Foreign Service Institute, the OIG (Office of the Inspector General) found that less than 14 percent of security-cleared employees had completed the required training within the timeframe considered in this review. Moreover, only 20 percent had completed the training even one time since the outset of the training program," the report said.

The report was commissioned after a 2013 review found severe deficiencies at the department when Hillary Clinton was secretary of state. "When Department employees and contractors are unaware of classification standards and no mechanism is in place to enforce training requirements, there is an increased risk that information could be incorrectly marked, misclassified, and/or improperly restricted or disseminated," it said.

The findings are notable because the recently released FBI files show how Clinton and her aides could not recall their classified information training, or if they did, still mishandled sensitive information.

In one case, the FBI documents show Clinton's "confidential" aide Monica Hanley received a high level clearance known as a Top Secret/SCI clearance. Despite acknowledging she received the training, during one trip to Russia, Hanley was specifically criticized for leaving a classified document in a hotel suite she shared with Clinton. "Hanley was informed by DS (Department of State) that the briefing book and document should have never been in the suite," the document said. Career government employees, who asked to speak off the record because they still hold clearances, said it was another example of a "double standard." In their experience, they said, in all other cases the individual would immediately lose his or her clearance pending a full investigation.

Two emails from Hanley to Clinton were marked classified with a c for "confidential," the lowest level of classification. Fox News first reported some of the emails contained classified markings despite Clinton's public claims.

Despite signing two non-disclosure agreements, known as NDA's, Clinton told the FBI she could not recall the training, and had trouble identifying classified information. Clinton told agents she could only speculate that the 'c' was part of an alphabetical listing such as A, B, C even though the other markings on the email were "SBU" for sensitive but unclassified.

Fox News has asked the State Department to respond to the findings.

New York Times
Voice in Russia Adds to Intrigue Over Computer Attacks in U.S.
Wednesday, 28 September 2016
Byline: Andrew E. Kramer

Biysk, Russia - Living anonymously, down a winding road in the wilderness of western Siberia, not far from the Mongolian border, the only person so far implicated in the flurry of Russian hacking of the Democratic National Committee and other political sites was obviously enjoying the moment.
"We have the information, but nobody contacted us," said Vladimir M. Fomenko, a tattooed 26-year-old who snowboards in his free time and runs a business out of a rented apartment.

"It's like nobody wants to sort this out," he added with a sly grin.

Mr. Fomenko was recently identified by an American cybersecurity company, ThreatConnect, as the manager of an "information nexus" that was used by hackers suspected of working for Russian state security in cyberattacks on democratic processes in several countries, including Germany, Turkey and Ukraine, as well as the United States.

Rather than issuing blanket denials, Mr. Fomenko is apparently eager to discuss his case, lending another, if still cryptic, dimension to the intrigue, restricted before now to digital codes and online fingerprints.

Mr. Fomenko is the owner of a server rental company called King Servers used by hackers in an incursion on computerized election systems in Arizona and Illinois this year. Its other principal clients, he said, have been pornographers.

His response has been a blend of sarcasm, vague denials and an invitation to cooperate with the F.B.I., offering potentially critical evidence in the Arizona and Illinois cases, should officials reach out to him here.

"If the F.B.I. asks, we are ready to supply the I.P. addresses, the logs," he said, referring to internet protocols, which identify a particular web page or device. "But nobody is asking. That is a big question."

Another is just how much Mr. Fomenko knows. Attribution in cases like these is a notoriously tricky business, especially when governments route their attacks through proxy servers like his or, in many cases, outsource espionage activities to criminal groups to maintain a measure of plausible deniability.

The investigation that led here began after the hacking of the state voting systems from June until August, what cyberanalysts say could be a bold bid by a resurgent Russia to undermine Americans' faith in their electoral process. The F.B.I. published eight internet addresses used in the attack. The bureau did not name the states, but officials in Arizona and Illinois acknowledged that their computers had been hacked.

ThreatConnect then identified six of the eight addresses as originating from servers owned by King Servers, Mr. Fomenko's company, in Dronten, the Netherlands, and possibly elsewhere. Mr. Fomenko also owns servers in Fremont, Calif.; Garden City, N.Y.; and Moscow.

The hackers, according to ThreatConnect, had used one of the eight internet addresses to send 113 precisely targeted, so-called spear phishing emails intended to dupe election officials and politicians in Turkey, Germany and Ukraine to click on links that downloaded malware. Some emails mimicked Gmail security warnings or notes from LinkedIn, the social networking site.

The emails were sent to members of the governing Justice and Development Party in Turkey, the German Freedom Party and Ukrainian members of Parliament, ThreatConnect said.

This spear phishing activity targeting the three countries was staged from one of the two addresses not originating from King Servers, while a King Servers address used Tor, the anonymity software, in the Illinois and Arizona electoral board hacks.

The security researchers said that the hackers who used Mr. Fomenko's server as part of this broader campaign were "looking to manipulate multiple countries' democratic processes" and that their modus operandi was "more suggestive of state-backed rather than criminally motivated activity."

Russian officials have denied any involvement in the hacking, but in an interview this month, President Vladimir V. Putin asked Bloomberg, "Does it even matter who hacked this data?" implying that the revelations were more important than the source. "The content was given to the public," he added.

The Democratic presidential nominee, Hillary Clinton, blamed the Russian security services for the hackings, and said that Mr. Putin "could barely muster the energy to deny" Russia's involvement. Donald J. Trump, the Republican nominee, has played down the prospect that Russia was involved.

Ambiguity has trailed the Russian hacking story all along. Mr. Fomenko, in an interview in a bar here called Rocks, flatly denied having any ties to the hacking. Yet he sports a collarbone-to-jaw tattoo of what he described as a version of the theatrical mask that is the symbol of the hacking group Anonymous.

He denied any connection to the group, saying he simply liked the symbolism of the mask. "A person can be evil, or a person can be good, or a person can hide who they are," he said.

The equivocation of responses by Mr. Putin and Mr. Fomenko is studied and deliberate, Kenneth Geers, a senior research scientist at Comodo, a cybersecurity firm, and a former cybersecurity officer with NATO, said in a telephone interview.

"You are not saying yes, you are not saying no, so it's frustrating for the victim, and it's intimidating," he said. "You are suggesting there is more to come."

The tattoo, though, "is something of a giveaway."

Mr. Fomenko, raised by a single mother, studied computer science at a technical college. He said he founded King Servers in 2008 when he was 18, buying computer servers and arranging for their installation remotely in Fremont, a city he said he had never visited.

He said he had about a thousand clients, 20 percent to 30 percent of whom are pornographers. Authorities in the Netherlands, he said, have notified him on several occasions that his servers had been used for spreading malware, advertising counterfeit designer handbags and distributing child pornography; in those cases, he said, he immediately revoked the rental agreements and closed the servers.

"If the person looks young, maybe 17 or 18, you cannot tell, we shut them down," he said. "Every company has their problems. You cannot control everything."

Mr. Fomenko said prospective renters using the nicknames Robin Good and Dick Robin had contacted him online in May and paid through WebMoney, an online payment system, not an uncommon profile for his clients.

On Sept. 15, Mr. Fomenko issued a statement saying that he had learned belatedly from news reports of the accusation that the hacking of the Arizona and Illinois voting systems were staged from two of his servers, and that he had shut them down. Mr. Fomenko does not deny that hackers used his servers, but does deny knowing that they did until Sept. 15. He says he does not know who they are, but that they are certainly not the Russian security agencies.

"The analysis of the internal data allows King Services to confidently refute any conclusions about the involvement of the Russian special services in this attack," he said in his statement. But then, apparently striking a sarcastic tone, he said he would send a bill to Mr. Trump and Mr. Putin for server rent left unpaid by the hackers.

He also says he has never been contacted by Russian or foreign law enforcement.

The clients, though, had left a trail through their contact with his billing page, he said. He added that he possessed the next step in the chain to bring investigators in the United States closer to the hackers, about 60 I.P. addresses used by his client -- the hacker of the state electoral systems -- to contact him. He said the addresses belonged to server companies in Britain, Finland, France, Italy, Norway and Sweden.

It was these addresses, he said, that he would be willing to share with the F.B.I., if "somebody wants to sort this out."

While ambiguous about the hacking on his servers, Mr. Fomenko minced no words about American presidential politics. "In Russia, we don't have this type of election," he said. "It looks like little children fighting."

Reuters
FBI probes hacks targeting phones of Democratic Party officials: sources
Wednesday, 28 September 2016
Byline: Mark Hosenball

Washington - The FBI is investigating suspected attempts to hack mobile phones used by Democratic Party officials as recently as the past month, four people with direct knowledge of the attack and the investigation told Reuters.
The revelation underscores the widening scope of the U.S. criminal inquiry into cyber attacks on Democratic Party organizations, including the presidential campaign of its candidate, former U.S. Secretary of State Hillary Clinton.

U.S. officials have said they believe those attacks were orchestrated by hackers backed by the Russian government, possibly to disrupt the Nov. 8 election in which Clinton faces Republican Party candidate Donald Trump. Russia has dismissed allegations it was involved in cyber attacks on the organizations.

The more recent attempted phone hacking also appears to have been conducted by Russian-backed hackers, two people with knowledge of the situation said.

Federal Bureau of Investigation representatives had no immediate comment, and a Clinton campaign spokesman said they were unaware of the suspected phone hacking.

The Democratic National Committee (DNC) did not respond to a request for comment. An official of the Democratic Congressional Campaign Committee (DCCC) said that nobody at the organization had been contacted by investigators about possible phone hacking.

Interim DNC Chairwoman Donna Brazile told CNN: "Our struggle with the Russian hackers that we announced in June is ongoing - as we knew it would be - and we are choosing not to provide general updates unless personal data or other sensitive information has been accessed or stolen."

FBI agents had approached a small number of Democratic Party officials to discuss concerns their mobile phones may have been compromised by hackers, people involved said. It was not clear how many people were targeted by the hack or whether they included members of Congress, a possibility that could raise additional security concerns for U.S. officials.

'OFFICE BRAIN'

If they were successful, hackers could have been able to acquire a wide range of data from targeted cellphones, including call data, text messages, emails, photos and contact lists, one person with knowledge of the situation said.

"In a sense, your phone is your office brain," said Bruce Schneier, a cyber security expert with Resilient, an IBM company, which is not involved in the investigation. "It's incredibly intimate."

"Anything that's on your phone, if your phone is hacked, the hacker can get it."

The FBI has asked some of those whose phones were believed to have hacked to turn over their phones so that investigators could "image" them, creating a copy of the device and related data.

U.S. investigators are looking into whether hackers used data stolen from servers run by Democratic organizations or the private emails of their employees to get access to cellphones, one person said.

Hackers previously targeted servers used by the DNC, the body that sets strategy for the party, and the DCCC, which raises money for Democrats running for seats in the House of Representatives, officials have said.

Clinton said during Monday's presidential debate there was "no doubt" Russia has sponsored hacks against "all kinds of organizations in our country" and mentioned Russian President Vladimir Putin by name.

"Putin is playing a really tough, long game here. And one of the things he's done is to let loose cyber attackers to hack into government files, to hack into personal files, hack into the Democratic National Committee," Clinton said.

Trump countered that there was no definitive proof that Russia had sponsored the hacks of Democratic organizations.

"I don't think anybody knows it was Russia that broke into the DNC," he said. "It could be Russia, but it could also be China. It could also be lots of other people."

USA Today
What a real cyber war would look like
Wednesday, 28 September 2016
Byline: Elizabeth Weise

San Francisco - Both U.S. presidential candidates have vowed to take on the world when it comes to cyber warfare. But full-scale cyber retaliation might be hard to spot and even harder to count as a win. "Unlike a traditional war, there is no end where there are clear winners and losers, no physical flag to capture," said Peter Tran, senior director at RSA Security in the company's worldwide advanced cyber defense practice.

If the U.S. were to ramp up its counterattacks on countries it thinks are sponsoring hackers that breach American accounts, don't expect a sci-fi digital armageddon. The target's electric grid might still work, and so may the ATMs. Think of it more as a creeping worry that simple things we rely on can't be trusted -- the machines that count our votes, the total on our bank balance, our personal digital files.

Democratic presidential nominee Hillary Clinton said the U.S. had the capability to stop the waves of attacks, which vaulted into the public consciousness again last week with Yahoo's disclosure that information from at least 500 million customer accounts was stolen in 2014. Yahoo said it believed the hacks came from a state-sponsored actor.

"We need to make it very clear -- whether it's Russia, China, Iran or anybody else -- the United States has much greater capacity. And we are not going to sit idly by and permit state actors to go after our

information, our private-sector information or our public-sector information," said Clinton when asked about attacks on U.S. institutions and theft of U.S. secrets.

In his reply, Republican nominee Donald Trump seemed to indicate the problems posed by cyber attacks were almost insurmountable.

"So we have to get very, very tough on cyber and cyber warfare. It is -- it is a huge problem. I have a son. He's 10 years old. He has computers. He is so good with these computers, it's unbelievable. The security aspect of cyber is very, very tough. And maybe it's hardly doable," he said.

N. Korea blackout

Many say we're already in the early stages of cyber war on multiple fronts. Nation-state hackers have targeted election databases in several states. U.S. officials believe China was behind a hack of the Office of Personnel Management in 2014, and that Iranians were behind an attack on the control system for a dam in New York state in 2013. Intelligence sources have fingered Russia as being behind the theft and release of embarrassing files from the Democratic National Committee.

So far the U.S. response has been mainly diplomatic. The most visible example was the sanctions on North Korea in 2014 and 2015 after it was tagged as the perpetrator of the hack that took down the Sony Pictures Entertainment computer network. That attack cost the company hundreds of millions of dollars and was purportedly the secretive nation's response to "The Interview," a comedy about the assassination of its leader by two bumbling Internet entertainment writers.

A month after the attack, the North Korean Internet was blacked out for about ten hours. The United States was coy about acknowledging whether it was behind the disruption.

Nor does cyber warfare have to stay in the digital realm. The U.S. Army Cyber Command is just one of multiple entities within the military focused on digital protection. And the United States has long reserved the right to retaliate with physical force against "significant cyber attacks directed against the U.S. economy, government or military."

Hot digital war

In a hot cyber war, the first line of attack would not be like on Star Trek, with spectacular bursts of sparks flying out of computers. Instead it would be a stealth attack on the enemy's military command and control infrastructure, to keep it from being able to strike, said Matt Devost, managing director of Accenture Security and a special government advisor to the U.S. Department of Defense.

The problem is that much like nuclear attacks, no one wants to let the genie officially out of the bottle. Certainly the United States and Europe benefit the most from a free and open Internet, so weaponizing it is not a step taken lightly.

"The United States is going to care a lot about not setting a precedent for that," said Christopher Porter, manager of iSIGHT Intelligence, which does strategic risk forecasting for the digital security company FireEye.

In many ways, digital fighting is a way for countries to engage in conflict when they don't want to escalate a dispute to the level of armed attack.

Russia excels at this, said Porter.

"They may not go after the government they're disagreeing with, they may go after citizens of the government, leaking documents on key political or military leaders" Porter said. "That's a very deliberate strategy and one they've been very effective at."

A higher level of escalation involves damaging critical infrastructure. This has already happened.

Russian launched a cyber attack against the Ukrainian power grid in 2015, according to U.S. officials. The attacks caused power outages in 103 cities and towns in the nation. Russia had been involved in military clashes with Ukraine over the Crimea.

A computer virus believed to be the work of Israel and the United States disabled a critical part of Iran's nuclear weapons program in 2010.

Multiple government websites in Estonia, one of the most wired nations on earth, were crashed in 2007. The country's foreign minister accuses Russia of being behind the attacks in retaliation over Estonia's move away from the Russian sphere of influence.

The United States has an advantage in this type of attack because so much of the technology that controls the networks today was either designed or built by the United States, said Srinivas Mukkamala, CEO of the computer security firm Risk Sense and one of the lead researchers for U.S. government research team that worked on CACTUS, the Computational Analysis of Cyber Terrorism against the U.S.

"Who designed the payment platforms? Who designed the chips? We did. So we can always find backdoors to get into whatever we've build," he said.

Cyber more humane

A final advantage of cyber warfare is that it's reversible, say experts. In a traditional war the only way to incapacitate an enemy's electric grid or transportation system is to physically destroy them. With cyber you can take them down but once the conflict is over they can be brought brought back online.

"It's potentially more humane," said Devost.

Reuters
Senior national security official to leave Justice Department
Tuesday, 27 September 2016
Byline: Staff report

Washington - A senior U.S. Justice Department official who oversaw efforts to prosecute Islamic State sympathizers and pursue cyber criminals is leaving the Obama administration next month, he told Reuters on Tuesday.
Assistant Attorney General John Carlin, chief of the national security division at the Justice Department, is departing on Oct. 15, less than a month before the U.S. presidential election.

Carlin, 43, confirmed his departure, expected to be announced later on Tuesday, in an interview with Reuters.

The departure comes as the Obama administration has struggled to develop clear guidelines on how to pursue hacking amid growing threats posed by foreign nation-states and criminal groups.

He declined to say where he was headed next. Carlin said he intended to spend time with his family before starting a new job, likely involved in cyber security.

Carlin, who has served in government for more than 15 years, oversaw a range of prominent cases in three and a half years since assuming an acting rank of the Justice Department's top national security lawyer in March 2013, including the prosecution of one of the 2013 Boston Marathon bombers.

He was confirmed full-time to the position in a 99-1 vote by the U.S. Senate in April 2014.

Carlin focused on pursuing cyber criminals during his two and a half years running the national security division.

His tenure included the unprecedented indictment of five Chinese military hackers in 2014 for alleged hacking into six U.S. companies in order to steal trade secrets, and the indictment of Iranian hackers earlier this year for alleged hacks on U.S. financial institutions and a New York dam.

Through a combination of legal cases, diplomatic sanctions and an effort to publicly name and shame hacking adversaries, Carlin sought to tame what he often called the wild west of cyberspace, where international norms for appropriate cyber activity are nascent or nonexistent.

"We've laid a strong foundation in cyber, but we've got to do more, faster, given the state of the threat," Carlin told Reuters. He said he hoped the next presidential administration could further "institutionalize" consequences from cyber crime.

Most recently Carlin announced this month the formation of a threat analysis team to study potential national security challenges posed by self-driving cars, medical devices and other Internet-connected tools.

Carlin's appointment in early 2014 coincided with territorial gains by Islamic State in Iraq and Syria that propelled the militant group to global notoriety. Since then, the department has prosecuted dozens of people on counts related to Islamic State: more than 100 people have been charged since 2014 in public federal cases.

Under Carlin, the national security division has also ramped up the Justice Department's efforts to combat what it sees as a rising threat from domestic anti-government extremists.

Press Association
Teenager appears in court over TalkTalk cyber-attack
Tuesday, 27 September 2016

London - A teenager has appeared in court accused of hacking the internet company TalkTalk to obtain customer data before asking for a six- figure blackmail payment in bitcoin.
Daniel Kelley, 19, appeared at Westminster magistrates court on Tuesday accused of demanding 465 bitcoins, worth about £216,000, from the company after allegedly carrying out a cyber- attack on its website in October last year.

He is also accused of carrying out similar attacks and making blackmail demands against other companies and their workers, including cigarette lighter manufacturer Zippo and an educational business in Queensland, Australia, in 2015.

Kelley, of Heol Dinbych in Llanelli, South Wales, faces 14 charges - eight of blackmail, four computer hacking offences and two fraud offences.

In total, he is accused of trying to obtain 593 bitcoins worth about £276,300.

The court heard he was arrested in November last year and charged by Scotland Yard detectives on Monday.

He did not enter a plea in court on Tuesday and was released on conditional bail to appear at the Old Bailey on 10 October.

Acadie Nouvelle
Le Darknet et les cyberprédateurs

Wednesday, 28 September 2016
Byline: Anthony Doiron

Non identifié - Il ne suffit pas de taper quelques mots clés dans un moteur de recherche pour trouver de la pornographie infantile. Les cyberprédateurs se tournent plutôt vers une facette sombre de l'internet - le Darknet -, accessible qu'à l'aide de certains logiciels disponibles gratuitement.
Cette expertise, autrefois réservée à quelques initiés, s'est démocratisée avec l'essor technologique des dernières années. Jonathan Nadeau, développeur web récemment diplômé, en témoigne.

«Prendre une année sabbatique dans le monde de la programmation informatique c'est une éternité. Il faut être à l'affût des nouvelles façons de faire dans ton domaine... et ça bouge vite.»

Le jeune programmeur est familier avec le Darknet. Il le décrit comme un système élaboré de relais entre ordinateurs, d'abord créé pour transférer des documents sensibles et assurer l'anonymat des délateurs politiques.

Des programmes disponibles gratuitement en ligne permettent d'y accéder, comme Tor et I2P. Ceux-ci masquent également l'adresse IP (Internet Protocol) d'un ordinateur, soit l'adresse internet accordée par un fournisseur internet. Les utilisateurs peuvent donc communiquer librement entre eux sans craindre d'être épiés par quiconque, dont les autorités policières. Même le fournisseur internet ne peut identifier les requêtes effectuées sur la connexion qu'il offre.

Par la force des choses, ce stratagème a attiré l'attention des criminels. Les réseaux du Darknet pullulent aujourd'hui de forums de services illégaux, comme l'embauche de tueurs à gages et la vente de drogues. Les pornographes pédophiles y ont également trouvé refuge.

Le Darknet est essentiellement un réseau à l'intérieur d'un réseau, explique Jonathan Nadeau.

«L'internet, c'est des ordinateurs connectés entre eux. Tu envoies une requête, mais tu ne sais pas par où ça va passer avant d'arriver à destination. Ça peut être intercepté par beaucoup de gens, incluant les services policiers. Le Darknet permet d'éviter ça.»

Le système n'est toutefois pas infaillible.

En février 2015, un forum d'échange de pornographie infantile nommé PlayPen a été la cible d'une vaste opération du FBI. L'agence fédérale a pris le contrôle du site et l'a hébergé sur ses propres serveurs pendant deux semaines, infectant les ordinateurs des présumés pédophiles de logiciels malveillants, pour permettre de les retracer. Le site comptait plus de 100 000 utilisateurs inscrits; seulement près de 200 d'entre eux ont été arrêtés.

«Tor n'est pas infaillible; l'opération du FBI l'a bien démontré. Mais avec Darknet, c'est impossible de faire de la surveillance de masse. Il faut identifier les cibles une par une», explique Jonathan Nadeau.

Ce sont souvent de petites erreurs qui vont permettre aux policiers de mettre la main au collet des cyberprédateurs: l'utilisation d'une même adresse courriel sur différents sites, le téléchargement d'un fichier contenant un logiciel d'espionnage de la police, ou carrément la publication de certaines informations personnelles sur les forums de discussion.

«Il peut y avoir des traces dans n'importe quel fichier transmis. L'information de l'appareil photo, la date, même la géolocalisation parfois.»

Jonathan Nadeau ne se surprend pas de voir cette montée fulgurante d'activité criminelle chez les cyberprédateurs. Le niveau de connaissance générale envers les outils technologiques a beaucoup augmenté au fil des ans. Le cyberespace a également pris de l'expansion.

«Avec l'internet, les pédophiles de toute la planète peuvent communiquer entre eux. Maintenant ils peuvent se rencontrer et s'organiser. C'est certain que ça risque de faire des sites inquiétants.»

La Presse+
Protection de la vie privée Les lois canadiennes jugées inadéquates
Wednesday, 28 September 2016
Byline: Joël-Denis Bellavance

Ottawa - Le gouvernement fédéral doit de toute urgence dépoussiérer et moderniser les lois canadiennes en matière de protection des renseignements personnels afin de tenir compte des changements technologiques fulgurants qui sont survenus au cours des dernières années, estime le commissaire à la protection de la vie privée du Canada, Daniel Therrien. Selon lui, reporter un tel exercice risque de compromettre la protection de la vie privée des Canadiens et miner la confiance des consommateurs dans l'économie numérique.
OTTAWA - DES OUTILS « INSUFFISANTS »

Dans son rapport, intitulé Le temps est venu de moderniser les outils du 20e siècle, le commissaire à la protection de la vie privée Daniel Therrien rappelle que l'internet n'existait pas quand le gouvernement fédéral a adopté la Loi sur la protection des renseignements personnels, en 1983. Et que des médias sociaux comme Facebook étaient des innovations qui n'avaient pas encore germé dans la tête de leurs inventeurs quand une deuxième loi en la matière, la Loi sur la protection des renseignements personnels et les documents électroniques, a été promulguée en 2001. « Le rythme incessant des changements technologiques exerce des pressions toujours croissantes sur la vie privée. Cet environnement exige une approche moderne de la protection des renseignements personnels. Nous essayons comme société de nous servir d'outils du XXe siècle pour résoudre des problèmes du XXIe siècle, et il est évident que ces outils sont de plus en plus insuffisants », a affirmé M. Therrien en conférence de presse.

DE GRAVES CONSÉQUENCES

Il y aura inévitablement de graves conséquences pour les Canadiens si le gouvernement fédéral tarde à moderniser les lois en matière de protection des renseignements personnels. Ces renseignements pourraient être mal protégés par le gouvernement ou le secteur privé et se retrouver inopinément entre les mains d'individus ou d'organismes qui ne devraient pas y avoir accès. Les Canadiens pourraient perdre confiance dans l'économie numérique. Des sondages indiquent que 90 % des Canadiens sont très préoccupés par leur incapacité à protéger leurs renseignements personnels. « Ultimement, si nous ne faisons rien, les conséquences seront réelles : risque d'atteinte à la protection des renseignements personnels, collecte et échange excessif de renseignements personnels par les entreprises et les gouvernements et diminution de la confiance dans l'économie numérique », a dit M. Therrien.

LES LACUNES DE LA LOI ANTITERRORISTE

Le commissaire Daniel Therrien se dit de nouveau inquiet que les ministères puissent partager plus facilement les renseignements qu'ils détiennent avec les agences de renseignement et les forces de l'ordre - des pouvoirs qui leur ont été accordés en vertu de la Loi antiterroriste (C-51). Le commissaire s'étonne d'ailleurs que la plupart des ministères n'aient pas fait d'évaluation de l'impact de la mise en oeuvre de cette loi sur la protection de la vie privée. Six mois après l'entrée en vigueur de C-51, les ministères et agences gouvernementales ont communiqué des renseignements personnels à 58 reprises et en ont reçu à 52 reprises. Ces renseignements concernaient des personnes soupçonnées de présenter une menace à la sécurité. Le gouvernement Trudeau a promis de modifier la Loi antiterroriste afin de mieux protéger les droits et libertés des individus.

MIEUX ENCADRER LE SECTEUR PRIVÉ

Grâce aux nouvelles technologies, les entreprises peuvent suivre à la trace des clients potentiels et analyser leur comportement comme jamais auparavant. Selon le commissaire Daniel Therrien, il faut mieux encadrer la notion de consentement à la collecte, à l'utilisation et à la communication de renseignements personnels pour éviter la multiplication de techniques de marketing « envahissantes ». Le commissaire a d'ailleurs lancé des consultations publiques afin de trouver des solutions possibles permettant de mieux encadrer la notion de consentement. « L'obtention du consentement sur la base de conditions d'utilisation que personne ne lit n'est pas un moyen efficace de protéger les renseignements personnels. On doit faire beaucoup mieux », a-t-il dit.

COMMUNICATION DE MÉTADONNÉES

Dans son rapport, le commissaire Daniel Therrien revient sur la controverse entourant la communication de métadonnées par le Centre de la sécurité des télécommunications (CST) à des partenaires internationaux du domaine de la sécurité en 2014. À l'époque, le CST avait soutenu que les risques d'atteinte à la vie privée étaient minimes parce que les métadonnées ne contenaient pas de renseignements personnels « sensibles » comme le nom d'individus, ni de détails contextuels qui les concernaient ou encore la teneur des communications. Mais Daniel Therrien demeure sceptique devant

ces explications. « Les métadonnées peuvent révéler des renseignements très sensibles concernant les activités, les relations, les champs d'intérêt et d'autres éléments de la vie d'un individu », écrit-il dans son rapport.

LE MODÈLE EUROPÉEN

Selon M. Therrien, le gouvernement canadien devrait s'inspirer de l'Union européenne en modernisant ses lois relatives à la protection des renseignements personnels. « Certains gouvernements ont déjà pris des mesures pour renforcer leur cadre de protection de la vie privée, en particulier l'Union européenne. Si l'Union juge que les lois canadiennes en matière de la protection de la vie privée ne sont plus équivalentes aux siennes, les relations commerciales entre le Canada et l'Europe risquent de devenir difficiles. C'est ce qui est arrivé aux États-Unis lorsque l'accord Safe Harbor a été invalidé par les tribunaux européens », a-t-il dit.

GOODALE RÉAGIT

Le ministre de la Sécurité publique, Ralph Goodale, a dit accueillir favorablement les critiques et les recommandations du commissaire à la protection de la vie privée Daniel Therrien, notamment en ce qui a trait aux changements qui devraient être apportés à la Loi antiterroriste. « Je porte un grand intérêt à l'examen, aux commentaires et aux recommandations du commissaire à la protection de la vie privée. Je vois en lui un acteur important pour assurer la reddition de comptes par le gouvernement. Il a fait l'examen de la première période de mise en vigueur de la Loi C-51 au sujet de l'échange d'informations. Il a des préoccupations importantes et je vais les traiter avec sérieux parce que ses opinions comptent », a dit le ministre Goodale.

Illustration(s) :

Photo Dado Ruvic, Reuters

Des sondages indiquent que 90 % des Canadiens sont très préoccupés par leur incapacité à protéger leurs renseignements personnels sur l'internet.

Photo Adrian Wyld, La Presse Canadienne

Dans son rapport, Le temps est venu de moderniser les outils du 20e siècle, le commissaire à la protection de la vie privée Daniel Therrien rappelle que l'internet n'existait pas quand le gouvernement fédéral a adopté la Loi sur la protection des renseignements personnels, en 1983.

Photo Stephanie Diani, archives The New York Times

Grâce aux nouvelles technologies, les entreprises peuvent suivre à la trace des clients potentiels et analyser leur comportement comme jamais auparavant.

Photo Graham Hughes, La Presse Canadienne

Le ministre de la Sécurité publique, Ralph Goodale, a dit accueillir favorablement les critiques et les recommandations du commissaire à la protection de la vie privée Daniel Therrien, notamment en ce qui a trait aux changements qui devraient être apportés à la Loi antiterroriste.

The National (UAE)
Jordan police make arrests over 'social media hate'
Wednesday, 28 September 2016
Byline: Suha Maayeh

Amman - Jordan's police arrested several people on Tuesday accused of circulating videos and posts on social media "promoting hate" days after a prominent Jordanian writer was shot dead.
Nahed Hattar, 56, an outspoken leftist and secular writer from a Christian family was killed on Sunday as he arrived at court to face charges for reposting on Facebook a cartoon deemed offensive to Islam.

Authorities are concerned his death would be exploited to sow discord in a country that is trying to avoid the violence that has engulfed the region.

The minister of justice Bassam Talhouni warned on Tuesday that those who misused social media to incite or spread hate speech would be prosecuted.

He told government news agency Petra that offenders would be referred to special courts where "deterrent legal action [would be taken] against them", particularly after a media gag order was issued by the state security court over the murder of Hattar. Mr Talhouni also said some acts of incitement could treated as terrorism offences.

The exact number of those arrested was not disclosed, but they included a relative of the shooter Riyad Ismaeel Abdullah. The family member created a Facebook page on social media called: "Yes to free the killer of Hattar". Police said several people who circulated such posts and videos were outside the country.

Jordanian authorities have been trying hard to reign in extremist ideology and have cracked down hard on extremists. But police described Abdullah, 49, as a lone wolf.

According to the police, Abdullah - who works as an electrical engineer at the ministry of education - planned his crime and bought a gun after Hattar shared the cartoon on August 13.

When Abdullah found out about the court session that Hattar was scheduled to attend, he waited for him in front of the court of justice and shot the writer several times before attempting to escape, a police report said.

A team of senior police officers searched Abdullah's house, car and electronic devices but did not find any evidence that proved he had accomplices. "He confessed to the crime and he carried out on his own and he did not inform anyone about his plans. It is an isolated crime," the statement said.

Abdullah will be detained for two weeks pending further investigation. He has been charged with crimes including premeditated murder, possessing a weapon illegally, and will face terrorism charges at the state security court.

La Tribune (France)
Surveillance spatiale : la France modernise le système Graves... a minima
Wednesday, 28 September 2016
Byline: Michel Cabirol

Paris - La notification du contrat de modernisation du système de surveillance de l'espace Graves est imminente. Un enjeu crucial pour la France qui peut ainsi suivre dans l'espace les satellites espions. C'est à la fois une bonne et une mauvaise nouvelle. La notification du contrat de modernisation du système de surveillance de l'espace Graves, par la direction générale de l'armement (DGA) au profit de l'ONERA est imminente, selon des sources concordantes. Ce n'est plus qu'une question désormais de quelques jours, le contrat étant actuellement dans les tuyaux administratifs. Cette notification est bien sûr très attendue tant ce système est stratégiquement clé pour la France, qui grâce à Graves (Grand Réseau Adapté à VEille Spatiale) peut suivre dans l'espace les satellites espions qui la survolent.

Contrairement aux préconisations de la DGA, cette opération de modernisation du système se fait malheureusement à minima. D'où un contrat relativement modeste évalué entre 20 et 30 millions d'euros dont une partie pourrait être financée par l'Europe. "Plus on avance dans le temps, plus on aura besoin de ces systèmes, explique-t-on au sein des armées. Mais ce qui nous manque aujourd'hui, c'est l'argent". Interrogé par La Tribune, le centre français de recherche aérospatiales, l'ONERA, "n'a pas de commentaire quant au périmètre de ce contrat dont le processus de notification n'est d'ailleurs pour l'heure pas encore finalisé".

Un manque de vision?

L'armée de l'air, qui a manqué de vision sur ce dossier, passe à côté d'un système beaucoup plus performant et surtout, d'un outil de puissance spatiale incroyable... alors même que l'espace va progressivement devenir un champ de bataille entre puissances spatiales ennemies et même alliées pour des raisons d'espionnage. Pourtant en 2012, 2013 et 2015, des engins spatiaux se sont approchés de satellites militaires français et sont restés à leur contact pendant une période relativement longue.

Avec un peu plus d'ambition, la France aurait pu disposer d'un système de veille spatiale plus puissant, notamment en augmentant les performances de son calculateur. Le système Graves aurait pu détecter

des objets plus petits. Mais l'opération de modernisation ne traitera finalement que les obsolescences du système pour qu'il puisse être opérationnel jusqu'en 2020- 2025.

« La France a été le troisième pays au monde, après les Américains et les Russes, à se doter d'un tel système, avait expliqué en juin 2015 dans une interview accordée à la Tribune le PDG de l'ONERA, Bruno Sainjon. L'Onera a conçu Graves, a piloté sa réalisation et l'a transféré à l'armée de l'air en 2005. Ce programme a notamment permis des échanges de données avec les États-Unis. Et, en avril 2015, cette coopération s'est renforcée, les deux ministères de la Défense voulant désormais échanger des informations classifiées. »

Un outil de puissance

Plus de 12.000 satellites artificiels et objets divers, dont la taille est supérieure à dix centimètres, orbitent autour de la Terre. Jusqu'en 2005, seuls Américains et Russes disposaient d'un système de veille spatiale opérationnel. En France, la mise en service du système Graves a permis de développer une mission de surveillance des satellites en orbite basse (d'altitude inférieure à 1.000 km). La France est ainsi entrée dans le club très fermé des puissances spatiales dotées de capacités autonomes de surveillance de l'espace.

Développé sous contrat de la DGA, le système Graves est constitué d'un radar spécifique associé à un système de traitement automatisé qui permet la création et le maintien à jour d'une base de données des paramètres orbitaux des satellites qu'il détecte. Fruit de la collaboration des spécialistes des départements Électromagnétisme et radar (DEMR) et Conception et évaluation des performances des systèmes (DCPS) de l'ONERA, le radar du système Graves a été spécifiquement conçu pour la surveillance de l'espace.

Le Monde
Trois prétendants demeurent en lice pour l'ex-Morpho (Canada)
Wednesday, 28 September 2016
Byline: Isabelle Chaperon

Paris - La décision sur le rachat de Safran Identity & Security, spécialiste de la biométrie et de la sécurité, devrait intervenir à la fin de la semaine
La bagarre pour le rachat de Safran Identity & Security (ex- Morpho), le spécialiste de la biométrie et de la sécurité mis en vente par Safran, bat son plein, sur fond de fortes tensions. Trois prétendants sont toujours en lice. Une décision est attendue en fin de semaine.

Advent, le fonds américain, également propriétaire d'Oberthur Technologies, et Gemalto, le leader mondial de la carte à puce, restent les favoris. Les offres d'Advent et de Gemalto seraient " très proches " , selon une source bien informée, pas loin de 2,4 milliards d'euros. Mais, selon plusieurs sources, Impala, le fonds de Jacques Veyrat, associé à KKR, n'a pas renoncé, même s'il est légèrement en retrait pour ce qui est du prix.

Parmi les cinq offres qui avaient été déposées, vendredi 16 septembre, auprès de Safran, deux auront donc été éliminées : celle de Bain Capital, avec le français Ardian et des investisseurs canadiens, et celle du fonds européen CVC Capital Partners associé à Astorg, sont arrivées loin derrière en matière de valorisation.

Safran a obtenu le prix qu'il désirait, et même bien au- delà. Le motoriste discute désormais, essentiellement avec Advent et Gemalto, pour les départager sur d'autres critères. En particulier, Safran demande aux deux candidats de renforcer leurs engagements sur le maintien de l'emploi chez Morpho et de prendre à leur charge le risque lié à la réglementation sur les concentrations.

Sujet sensible Il n'y a pas de miracle : si Gemalto et Advent sont capables de proposer des prix aussi élevés, c'est parce qu'ils estiment pouvoir tirer plus de synergies du rapprochement. Mais qui dit synergies, dit souvent aussi casse sociale. Au moment où le gouvernement doit gérer la crise liée à l'arrêt de la fabrication de locomotives chez Alstom à Belfort, il n'est pas question d'ouvrir un autre front.

Dans une lettre en date du 7 septembre adressée à Michel Sapin, le ministre de l'économie et des finances, Cédric Chateau, directeur associé d'Advent International, et Didier Lamouche, PDG d'Oberthur Technologies, ont assuré qu'ils envisageaient descréations d'emplois en France : " Cela nous permet de garantir un niveau global d'emplois permanents en France pendant une période d'au moins deux ans. " De son côté, Gemalto a promis qu'il n'y aurait pas de suppressions de postes en France, sans limitation de durée.

Le sujet est d'autant plus sensible que Patrick Drahi, le patron d'Altice, qui s'était engagé à ne pas licencier pendant trois ans après avoir racheté l'opérateur télécom SFR en 2014, vient d'annoncer un vaste plan social, une fois cette période expirée.

Cette négociation avec Safran se double d'une autre. Les prétendants discutent, en effet, en direct avec l'Etat. Compte tenu des activités exercées par Morpho en lien avec la sécurité et la défense, plus son poids dans une filière technologique majeure, les pouvoirs publics veulent s'assurer que les prétendants respecteront les intérêts français, de la localisation des centres de recherche à la propriété intellectuelle.

Pour s'assurer dans la durée du respect de ces engagements, l'Etat souhaite l'intervention de Bpifrance. La banque publique, qui détient déjà 8,4 % de Gemalto, pourrait ainsi accompagner le repreneur, quel qu'il soit, dans ce rachat.

Ottawa Citizen
Missing IDs won't alter military's policy
Thursday, 29 September 2016
Byline: David Pugliese

An incident involving hundreds of blank Canadian Forces identification cards that went missing just days after the 2014 attack on Parliament Hill has been meet with a shrug from the military.
The case involving the identity cards, which disappeared while being shipped from Ottawa to Toronto through Canada Post, resulted in a brief police investigation and no changes to the military's security policy.

Missing for 73 days, the cards were eventually discovered in a batch of mail that had been returned as undeliverable, according to the 2015 military police report obtained by the Ottawa Citizen using the Access to Information law.

They had been sent by mail during a tense period when the Canadian government and military were on edge and worried about domestic terrorist attacks. On Oct. 20 an Islamic extremist in Quebec deliberately struck Warrant Officer Patrice Vincent with his car, killing him. Two days later, Michael Zehaf- Bibeau gunned down Cpl. Nathan Cirillo at the National War Memorial in Ottawa before running into the Parliament Buildings, where he was shot dead. He had also espoused Islamist extremist views and was planning to leave for the Middle East.

The first inkling something had gone wrong with the shipment was after a military officer in Scarborough, a Toronto borough, received a package of 100 ID cards marked as "undeliverable mail." The cards were supposed to have been delivered to a Toronto armoury but instead appeared to have been misdirected to another address.

Military police wondered if they had been found by "an unknown person" who then dropped them into a Canada Post mailbox. Another 100 were successfully delivered, leaving the remaining 300 cards unaccounted for, the police report noted.

Initial attempts to find out the location of the cards were met with "negative results," the report added. One sailor who tried to alert Canadian Forces officials couldn't get through and instead had to leave phone messages at a number of locations.

On Jan. 9, 2015, the cards were discovered back in a military police unit in Ottawa, having been returned by Canada Post as undeliverable mail. Military police closed their investigation on March 26, 2015.

The incident has not prompted any changes, the Department of National Defence confirmed.

Military identification cards are still shipped using Canada Post, DND noted in an email to the Ottawa Citizen. "The Department of National Defence (DND) is confident this was an isolated incident," its

statement said. "The security implications were limited, as all of the identification cards were recovered and were not tampered with during shipping and recovery."

DND acknowledged in its email, "there is always a risk associated with lost ID (military and civilian) cards, and building access cards."

But it noted that since such temporary access cards had an expiry date, if such a card is misplaced or stolen, the risk it poses "is minimal."

DND statement also pointed out that the shipment was appropriately handled by all military and civilian staff.

CBC News
Conservatives took payroll training responsibilities away from Phoenix creator IBM
Thursday, 29 September 2016
Byline: Katie Simpson

Ottawa - As the federal government shaped its plan to modernize the public service payroll system, CBC News has learned that the former Conservative government took training duties away from IBM -- the company that created the Phoenix program.
The move raises new questions about what led to the payroll fiasco, as problems with training have been listed as a key cause of Phoenix's troubled rollout.

"Responsibility for training design and execution was transferred to the Crown in March 2014," said IBM spokeswoman Carrie Bendzsa.

The change was made at the request of the former government, Bendsza confirmed by email.

Conservative MP Diane Finley was the minister of Public Works at the time and responsible for overseeing the modernization project from 2013 to 2015. Her office refused multiple requests for an interview.

The current Liberal government is accusing the Conservatives of cutting corners on training to save money.

"There was a cost associated with training, and it was made clear to me that the Conservatives opted to go with the train-the-trainer model versus buying the IBM training approach. In this case, savings were prioritized before the project was fully implemented?," Judy Foote, the current minister of Public Services and Procurement Canada, said in a statement.

"It appears that when the previous government decided to go with Phoenix, the proper training wasn't done and they tried to implement a system without a sufficient number of employees," she added.

Liberals should have hit pause, MP says

While the Conservatives did not have an explanation as to why the decision was made, they blame the current government for not slowing down the rollout of Phoenix, which started this past February.

"If they weren't ready and they knew about it ... why would you go ahead and start the system if you're now saying that you knew the training was insufficient?" said Kelly McCauley, the Conservative critic of Public Services and Procurement.

"It goes back to, you knew it wasn't ready to implement, so why would you?"

Since the Phoenix system was fully implemented in April, more than 80,000 public servants have experienced problems with their pay. Most workers have been underpaid, while some have been over paid, or not paid at all.

The Department of Public Services and Procurement Canada has promised to clear the backlog of problems by the end of October. As of Sept. 21, there were still 57,500 public servants waiting for individual cases to be resolved.

The government estimates it will cost $50 million to fix the program, which was originally touted as a way to save the federal treasury $70 million annually.

Union 'not surprised'

The Public Service Alliance of Canada, the largest union representing federal public servants, expressed frustration over this latest development.

"I'm very disappointed but not surprised at all," said PSAC National Vice-President Chris Aylward. "[There's] no regard for the employees who have to perform those duties. No regard for the employees going on that new pay system."

At a labour board tribunal hearing earlier this month, a senior bureaucrat explained that training problems are at the root of the Phoenix issue.

"We underestimated the time it took people to adapt to the new technology. The learning curve just seemed to be much longer that we expected," said Rosanna Di Paola, the associate assistant deputy minister of Public Services and Procurement Canada.

Ottawa Citizen
Quantum computer has radical power
Thursday, 29 September 2016
Byline: Gordon Ball
Section: editorial

Re: Spy chief issues encryption warning, Sept. 24.
A Citizen article quoted the head of the Communications Security Establishment as saying that, in eight to 10 years, if people are able to build quantum computers they could break the security and encryption codes in use today.

Some years ago, I learned a bit about quantum computing. The experts said that formidable technological challenges would have to be overcome before anyone could actually build quantum computers. The experts were not sure it could be done at all. Perhaps the scientists and engineers have made advances since.

If it were actually possible to build working quantum computers, they would revolutionize computing as we know it.

Gordon Ball, P. Eng.

Ottawa

Le Soleil
La cyberattaque coûtera des centaines de milliers de dollars
Thursday, 29 September 2016
Byline: Ian Bussières

Thetford Mines - La commission scolaire devra remplacer plusieurs centaines d'ordinateurs
La cyberattaque dont a été victime il y a près d'un mois la commission scolaire des Appalaches (CSA) coûtera quelques centaines demilliers de dollars à cette commission scolaire de la région de Thetford Mines qui devra remplacer plusieurs centaines d'ordinateurs et en «nettoyer» plus de 2000.

-- PHOTO 123RF/ TYLER OLSON

Les classes iPad de la polyvalente de Black Lake et les cours de formation professionnelle nécessitant un ordinateur et l'accès à Internet ont pu reprendre mercredi.

Le président de la CSA, Denis Langlois, a confirmé au Soleil que son organisation était sur la bonne voie pour un retour à la normale. «Nous avons pu récupérer beaucoup de données grâce à une copie de

sauvegarde faite à la fin du mois de juin. Nous sommes présentement à rebâtir le reste, notamment le mois d'août », a-t-il expliqué.

Les classes iPad de la polyvalente de Black Lake et les cours de formation professionnelle nécessitant un ordinateur et l'accès à Internet ont également pu reprendre mercredi, mais M. Langlois a indiqué qu'il y aurait un peu de rattrapage à faire pour ces élèves.

« Nous avons payé nos employés, nous sommes en voie de compléter le paiement de tous nos fournisseurs, et le logiciel pour le transport scolaire est de nouveau en fonction. Il reste maintenant l e dossier des tableaux interactifs et l e "nettoyage" de tous les ordinateurs», a expliqué M. Langlois. Le parc informatique de la CSA compterait quelque 3000 appareils.

La commission scolaire profitera de l'occasion pour remplacer les ordinateurs qui arrivaient en fin de vie. «On parle de plusieurs centaines d'ordinateurs qui seront changés, l'é quivalent de deux années en une.»

PAS DE HAUSSE DE LA TAXE

Sans vouloir en dévoiler le chiffre précis, M. Langlois a laissé entendre que la gestion de l'attaque informatique allait coûter quelques centaines de milliers de dollars à l'établissement. «Je ne dirais pas "plusieurs" centaines de milliers de dollars, car en bout de ligne la récupération des données va mieux que prévu. Et il n'y aura pas de hausse de la taxe scolaire à cause de la cyberattaque», a-t-il ajouté pour rassurer les contribuables.

Denis Langlois affirme connaître le pourcentage des données perdues et récupérées ainsi que les sommes déjà dépensées et la facture totale qui sera déboursée pour faire face à la situation, mais préfère ne pas les dévoiler. Il a d'ailleurs défendu le mutisme dans lequel s'est emmuré le directeur général de la commission scolaire, Camil Turmel, depuis l'attaque. « La Sûreté du Québec nous a bien dit de ne pas commenter durant leur enquête. Nous avons fait une communication interne à nos employés et c'est tout.»

Le président de la CSA ajoute qu'il serait surprenant que les renseignements personnels des employés et des élèves aient été transmis aux pirates. « Les mesures prises sur le réseau privé ne démontrent pas un flot plus élevé que d'habitude, ce qui aurait été le cas si une grande quantité de données était sortie du serveur. De toute façon, il semblerait que ce n'est pas ce qui intéresse ces hackers. »

«UN SPAM»

Ce serait via le courrier électronique que les pirates auraient réussi à s'infiltrer dans le système informatique de la CSA. « C'est un spam qui est passé par là et il semblerait que c'est un spam nouveau et plus fort qui fait des dommages à plein. Ce qu'on nous a expliqué, c'est que c'est c o mme u n robot qui entre n'importe où et qui f ait des dommages » , a i ndiqué M. Langlois en soulignant qu'un plan

d'action était déjà en place pour éviter un autre épisode du genre. « Nos employés ont déjà reçu des directives à l'effet de faire certaines choses.»

Denis Langlois a dit toujours ignorer la provenance des pirates informatiques et a refusé de confirmer l'information corroborée par plusieurs employés de la commission scolaire voulant qu'ils aient réclamé une rançon que l'établissement a refusé de payer. «Ils pourraient venir de l'Inde, de l'Afrique, de la Chine ou du Québec. On ne le sait pas pour l'instant.»

Israel Defense
IntSights, Check Point to Deliver Threat Intelligence Capabilities for Thwarting Cyber Attacks
Thursday, 29 September 2016

Undisclosed placeline - IntSights, a leading intelligence-driven security provider for cyber threats from the dark, deep and open web, announced a partnership with Check Point Software Technologies Ltd. As part of this partnership, Check Point will integrate IntSights's cyber threat intelligence platform with its security suite. The combined offering will help customers leverage real-time threat intelligence to detect and remediate cyber threats.
Organizations consume endless amounts of information, but due to lack of context and automation they fail to create a cohesive view and act upon it. Often a crucial piece of intelligence is left unutilized due to an analyst's error or is simply lost in the siloed data stream.

"In the constant battle against cyberattacks, Check Point leverages threat intelligence and rapid response capabilities through our Next Generation Firewalls and SandBlast Zero-Day Protection," said Alon Kantor, vice president of business development, Check Point. "Our partnership with IntSights's intelligence adds additional capabilities and actionable intelligence that will help customers respond to attacks quicker."

IntSights provides extensive intelligence coverage that is easy to understand and act upon by a single analyst. This joint product offering will provide advanced warning and customized insight for customers, as well as continue to improve on and increase automated security and threat remediation.

"The IntSights platform is crucial in finding, detailing, reporting and understanding all of the potential Internet risks that face our business," said Rob Duchscher, Chief Information Officer, Starkey Hearing Technologies. "The IntSights platform is complementary to the Check Point security suite and helps provide end-to-end protection - from the external to the internal network."

This cooperation between IntSights and Check Point also extends the companies' existing research collaboration. Through intelligence cooperation, IntSights will complement Check Point's current research capabilities, collecting information from the many difficult-to-penetrate, closed communities and forums on the dark web.

"We are pleased to work alongside an industry leader like Check Point," said Guy Nizan, CEO, IntSights. "This newly formed partnership will provide long-term benefits for both parties and will provide added value to our customers. In addition, the opportunity for intelligence and research cooperation will be an advantage for both companies."

The two companies recently have produced joint research projects, including "An overview of the ransomware phenomenon" and "CerberRing: An In-Depth Exposé on Cerber Ransomware-as-a-Service." The latter, published last month, sheds new light on the Cerber ransomware, one of the most prominent ransomware variants.

Wall Street Journal
Yahoo Claim That Hack Was State Sponsored Is Disputed
Thursday, 29 September 2016
Byline: Robert McMillan

New York - An information-security firm says the hackers who stole at least 500 million records from Yahoo Inc. two years ago are criminals who are selling access to the database, and not a state-sponsored group as Yahoo contends.
The firm, InfoArmor Inc., appears to have access to portions of the Yahoo database. It successfully decrypted the passwords for eight Yahoo accounts provided by The Wall Street Journal, and provided the date of birth, phone number and ZIP Code information associated with the accounts.

InfoArmor said the hackers, whom it calls "Group E," have sold the entire Yahoo database at least three times, including one sale to a state-sponsored actor.

The hackers are engaged in a moneymaking enterprise and have "a significant criminal track record," selling data to other criminals for spam or to affiliate marketers who aren't acting on behalf of any government, said Andrew Komarov, chief intelligence officer with InfoArmor.

That is not the profile of a state-sponsored hacker, he said. "Their clients are state sponsored, but not the actual hackers."

Mr. Komarov's assessment conflicts with Yahoo's statement last week that its users' account information was stolen by "what it believes is a state- sponsored actor."

Yahoo didn't respond to requests for comment.

Mr. Komarov said InfoArmor has been tracking Group E for three years. It believes the hackers are Eastern European, but declined to specify why.

InfoArmor has linked the group to hacks that stole more than two billion records from about a dozen websites, including LinkedIn Corp., Dropbox Inc. and Myspace.

In a report published Wednesday, InfoArmor offered new details on the Yahoo breach and Group E.

The analysis still leaves many questions unanswered, including how InfoArmor obtained access to the database and why Yahoo didn't uncover the magnitude of the breach for nearly two years.

InfoArmor declined to say whether it has a copy of the database or accessed it through a third party.

Yahoo has said it began its investigation in July, around the time the company was completing plans to sell its core assets to Verizon Communications Inc. for $4.8 billion.

In a Sept. 9 securities filing, Yahoo said it wasn't aware of any "security breaches" or "loss, theft, unauthorized access or acquisition" of user data.

The Wall Street Journal reported last week that Yahoo in fall 2014 detected what it believed was a small breach involving 30 to 40 accounts, carried out by hackers working on behalf of the Russian government.

Yahoo reported the incident to the Federal Bureau of Investigation in late 2014 and notified affected users.

After selling the Yahoo database three times, starting in early 2015, the hackers have shifted tactics, Mr. Komarov said. They are no longer offering to sell the full database, but are seeking "to extract something from the dump for significant amounts of money," he said.

Prices vary based on the value of the target, Mr. Komarov added.

Meanwhile, six Democratic U.S. senators have written to Yahoo Chief Executive Marissa Mayer, seeking answers to questions about the company's 500 million-account data breach, thought to be the largest ever.

The letter, sent Tuesday, notes that Yahoo said the breach occurred in late 2014, yet was only disclosed last week. "That means millions of Americans' data may have been compromised for two years," the senators wrote. "This is unacceptable."

"We have received the letter and will work to respond in a timely and appropriate manner," a Yahoo spokesman said Tuesday in an email.

Wall Street Journal
U.S. Thinks Russia Shields Hackers
Thursday, 29 September 2016
Byline: Damian Paletta

Washington - U.S. officials are increasingly confident that the hacker Guccifer 2.0 is part of a network of individuals and groups kept at arm's length by Russia to mask its involvement in cyberintrusions such as the theft of thousands of Democratic Party documents, according to people familiar with the matter. While the hacker denies working on behalf of the Russian government, U.S. officials and independent security experts say the syndicate is one of the most striking elements of what looks like an intensifying Russian campaign to target prominent U.S. athletes, party officials and military leaders.

U.S. officials believe that at least two hacking groups with ties to the Russian government, known as Fancy Bear and Cozy Bear, are involved in the escalating data-theft efforts, according to people briefed on the Federal Bureau of Investigation's probe of the cyberattacks.

Following breaches, stolen material has been published by WikiLeaks, DCLeaks.com and a blog run by Guccifer 2.0. The websites have posted batches of stolen data at least 42 times from April to last week.

WikiLeaks has published U.S. secrets for years but has recently taken an overtly adversarial tone toward Democratic presidential nominee Hillary Clinton. Cybersecurity experts believe that DCLeaks.com and Guccifer 2.0 often work together and have direct ties to Russian hackers.

Guccifer 2.0 said in a Twitter direct message sent to The Wall Street Journal that he wants to expose corruption in politics and shine light on how companies influence policy. The hacker said he also hopes to expose "global electronization."

"I think I won't have a better opportunity to promote my ideas than this year," Guccifer 2.0 added in a long exchange with a Journal reporter.

The Journal couldn't verify the identity of the person sending messages on behalf of Guccifer 2.0, but the account is the same one that was used to publish personal information about Democrats. A posting on a blog run by Guccifer 2.0 says he is a man who was born in Eastern Europe, has been a hacker for years and fears for his safety.

"I think u've never felt that feeling when u r crazy eager to shout: look everyone, this is me, this is me who'd done it," the hacker wrote to the Journal. "but u can't."

WikiLeaks officials didn't respond to requests for comment on whether Russia fed them the stolen files it published in July. A DCLeaks.com representative asked the Journal to submit questions via email but hasn't responded to them.

Last week, U.S. intelligence chief James Clapper said it "shouldn't come as a big shock to people" that Russia is behind the hacking operation. While Russia has tried to interfere in U.S. elections since at least the 1960s by spying and funneling money to particular political groups, "I think it's more dramatic maybe because now they have the cyber tools," he said.

Earlier this month, leaked emails from former Secretary of State Colin Powell on DCLeaks.com revealed him calling Republican presidential nominee Donald Trump a "national disgrace" and accusing Mrs. Clinton of "unbridled ambition" and being "greedy, not transformational."

German officials said last week that hackers have sought to infiltrate computer systems of several German political parties. Two officials familiar with the investigation say there is evidence Fancy Bear was involved in the attempted German hack.

Longtime Russia analysts say its goal in the U.S. might be to attack the basic credibility and reputation of institutions such as the military, election system, political parties and the federal government more broadly.

Russian President Vladimir Putin has said disclosure of U.S. records is a public service. He has denied involvement in the hacks, and Russian officials have said they don't interfere in the democratic process in other countries.

In August, Russian Foreign Minister Sergei Lavrov said critics were falsely trying to pin offenses on Moscow. "We can hear and see Russophobia, which is off the charts in the U.S. media," he said.

Signs of an escalating strategy emerged in April when DCLeaks.com published batches of emails stolen from U.S. Air Force Gen. Philip Breedlove, then the top military commander of the North Atlantic Treaty Organization.

Gen. Breedlove was one of the U.S. government's biggest Russia critics, warning openly about the country's aggression toward Ukraine and the West while other U.S. leaders were taking a lower-key approach.

He realized his Facebook, LinkedIn and Gmail accounts had been hacked when friends received strange messages purporting to be from him. Then he found out that DCLeaks.com posted dozens of his emails.

From the start, Gen. Breedlove had little doubt that Russia was behind the intrusion. "A major world power has turned its cyber force onto private individuals and is now pouring out private accounts and emails to affect U.S. policy," he said in an interview with the Journal. He retired this summer.

In June, cybersecurity company CrowdStrike Inc. said Fancy Bear and Cozy Bear had penetrated the Democratic National Committee. The next day, Guccifer 2.0 published stolen records from the DNC. Three days later, the hacker disclosed DNC financial reports and donor data.

Washington Post
Russian hackers went after journalists investigating the downing of MH17
Thursday, 29 September 2016
Byline: Ellen Nakashima

Washington - Russian government hackers began targeting a British citizen journalist in February 2015, eight months after he began posting evidence documenting alleged Russian government involvement in the shoot- down of a Malaysian jetliner over Ukraine.
And then in February 2016, a group that researchers suspect is a propaganda mouthpiece of the Russian government - CyberBerkut - defaced the home page of Eliot Higgins's citizen journalism website, Bellingcat.com.

That same month, CyberBerkut hacked the email, iCloud and social-media account of a Bellingcat researcher in Moscow, then posted online personal pictures, a passport scan, his girlfriend's name and other private details.

Russia's information operations against Bellingcat are a taste of what may be in store for other media organizations whose reports anger the Kremlin, said a cyber-research firm that has extensively documented the effort.

"If Russia is willing to go these lengths to compromise a small journalist organization and its contributors, consider what they are willing to do to major news and media outlets that publish similar articles," said Rich Barger, chief intelligence officer at ThreatConnect, a Northern Virginia-based research firm that analyzed the campaign against Bellingcat in a report released Wednesday. ThreatConnect looked into the matter after being approached by Bellingcat.

The report comes on the same day that a Dutch-led, multinational joint investigative team announced the results of a criminal probe that corroborated Bellingcat's findings: The airplane was downed by a Russian surface-to-air missile fired from territory held by pro-Moscow separatists.

Russia has denied complicity in the downing.

Malaysia Airlines Flight 17 was destroyed on July 17, 2014, over eastern Ukraine. All 298passengers and crew members were killed.

Beginning that day and for the next 26 months, Bellingcat published no fewer than 92 posts focused on Russian involvement in the plane's downing, using open-source information and imagery to prove the presence of Russian military equipment that had been moved into eastern Ukraine despite the Kremlin's denials.

The Russian harassment and propaganda campaign against Bellingcat, and Higgins in particular, began in February 2015. Bellingcat had completed a report that documented Russian shelling of Ukrainian military positions in eastern Ukraine, which Moscow had denied. The state-run Sputnik website ran an article suggesting that Bellingcat was linked to the CIA.

Beginning that month through July 2016, three Bellingcat researchers, including Higgins, received "spearphishing" emails that were written in a way meant to dupe the recipient into clicking on a link containing malware. Higgins received 16 such emails, which consisted of false Gmail security notices urging the recipient to click a link to review recent suspicious activity.

That technique, Barger said, is consistent with a technique used by a Russian hacker group dubbed Fancy Bear by some security researchers. The group is run out of the GRU, the military intelligence service, analysts said.

Meanwhile, with every new Bellingcat revelation, Russian propaganda outlets such as Sputnik and RT, formerly Russia Today, produced pieces that called into question the citizen journalists' work.

In October, for instance, Bellingcat published reports based on the geolocation data of Russian defense ministry videos that showed that Russian airstrikes were destroying positions held by the Free Syrian Army and other rebel groups rather than the Islamic State, as Russia had indicated.

Nearly every day for a week, a new piece emerged on RT or Sputnik attacking Bellingcat. "After the fourth day, I said, 'This is out of control,'" Higgins said. "They've gone crazy."

RT even sent a satirist with a cameraman to find Higgins in his home town of Leicester, England.

The comic Nimrod Kamer wound up reaching Higgins's mother, who, Higgins said, was "in tears" after being questioned by Kamer about her son. "It was intimidating, given the circumstances," he said.

Then, in February, CyberBerkut, which describes itself as a group of pro-Russian Ukrainian hacktivists, defaced Bellingcat's website.

In a blog post, the group also said it had hacked Bellingcat researcher Ruslan Leviev. To gain access to his email inbox, the group hijacked a text message sent to his cellphone that contained a security code, Leviev said.

Barger said he thinks the group gained access to Bellingcat's website through Leviev's account.

In July, two days before the second anniversary of the crash, Russian bloggers "trolled" Higgins, publishing more than 30articles in Russian in 30 hours attacking his credibility and questioning his reporting.

Higgins is "bringing to light the truth behind the 298" people killed, Barger said. "There is an aggressive campaign to undermine those who are shining a light" on the tragedy.

"If you cross Russia, you become a target for Russia," said Higgins, 37.

But, he added, he thinks the campaign of harassment and hacking may backfire. "It just makes them look insane and makes us look far more credible because they are going at us so hard."

Bloomberg News
Pentagon's 5,000-Strong Cyber Force Passes Key Operational Step
Thursday, 29 September 2016
Byline: Nafeesa Syeed

Washington - A 5,000-person Pentagon force created to bolster military computer networks and initiate cyber attacks against terror groups should be ready to carry out its mission by the end of the week, a key step in improving the U.S.'s ability to respond to hacks by overseas adversaries.
The Cyber Mission Force will reach "initial operational capability" by Friday, said Colonel Daniel J.W. King, a Cyber Command spokesman, in an e-mail. The group's 133 teams have met basic criteria on personnel, training, resources and equipment, but all of them aren't necessarily ready to launch attacks, he said.

The force, which falls under the U.S. Cyber Command created in 2009, likely will focus on the highest priorities, such as risks from Russia, China, Iran and terrorist groups including Islamic State, according to Bob Stasio, a fellow at the Truman National Security Project and former chief of operations at the National Security Agency's Cyber Operations Center.

Until the force becomes fully operational, which is planned in 2018, the question officials directing it will ask first will be, "What's the minimum operation I need against the biggest threats that I have today -- the closest alligators to the boat," Stasio said.

Previously, cyber operations were scattered in silos across Cyber Command, the NSA and other military branches, according to Stasio. The new centralized force will help cut through the bureaucracy, he added. Officials plan to expand the force by another 1,200 people as part of the process of becoming fully combat ready.

"We continue to generate the mission force," Admiral Michael Rogers, who heads Cyber Command and the NSA, said in a Sept. 13 speech in Washington. "At the same time, we got to tell ourselves we are not where we need to be in this mission."

The operational capability designation means the Pentagon has better streamlined cyber activities across its bureaucracy, but analysts say it doesn't necessarily reflect greater security chops as defense officials try to keep up with fast-evolving technology and threats.

"What it means is we have the people, the tools, we've practiced and we're ready," said Mark Young, chief security officer and senior vice president at IronNet Cybersecurity Inc. and a former senior executive at Cyber Command.

Digital Labyrinth

As hacking attacks traced to countries such as Russia and China continue to make U.S. headlines, people "can feel more comfortable -- not completely comfortable - - but they can feel more comfortable, that we now have a military force that could respond if directed to these activities," Young said.

The mission force is tasked with defending the Defense Department's data and its labyrinth of thousands of digital networks across the world. It also has to defend the U.S. "against cyber attacks of significant consequence" as well as the nation's critical infrastructure, King said. Cyber war plans are also in place for the military's various regional commands.

Setting up the force is also a sign that cyber is more "baked into" the military's overall strategy, while providing defense officials a grasp of how much it needs to spend on cybersecurity, said Dave Aitel, chief executive officer of Immunity Inc. and a former NSA computer scientist. In its 2017 information technology budget, the Defense Department requested $6.8 billion for cyber operations.

Money Buckets

"You have to kind of look at it as if you're building a whole new Navy, that's a very expensive operation," Aitel said. "It gives them better buckets to throw money into and know where that money is going."

There's work ahead as the military builds out all of its cyber teams to full capability in the next two years.

Even when they reach that stage, officials will still have to keep pace with emerging tech tools and cyber-attack tactics, according to Ben FitzGerald, a senior fellow at the Center for a New American Security, who previously worked as an executive for technology companies with defense contracts.

"Cyber Comm is still going through a process of establishing the command and control arrangements between their teams, and the support they provide to rest of the Department of Defense, and that's going to take time to figure out," FitzGerald said. "The key challenge is will they be able to adapt and keep making changes as rapidly as they need to?"

Times of Israel
Poor cybersecurity habits persist worldwide
Thursday, 29 September 2016
Byline: Iacopo Luzi

Jerusalem - Israel's second-largest public security company, CyberArk, said a survey it published recently showed that heightened awareness of cybersecurity threats among information technology professionals has failed to translate into greater success in defending against those threats. "Despite increased cybersecurity awareness, nearly every IT security breach or cyberattack continues to be underpinned by the failure of organizations to enforce best practices or adequately protect against advanced threats," CyberArk's Global Advanced Threat Landscape Survey 2016 said.

Today, as never before, global enterprises are vulnerable to worldwide hackers. Last week, Yahoo announced that at least 500 million of its accounts were hacked in 2014, in the world's biggest known cyberattack by far.

CyberArk's report -- the result of surveys conducted with 750 IT and IT security decision makers from around the world -- shows rising confidence in cybersecurity strategies and, at the same time, poor IT security habits that continue across the industry in critical areas such as privileged account security, third-party vendor access and cloud.

According to the report, 79 percent of respondents said their organization has taken appropriate action to improve security while 55% of respondents said they have changed or evolved processes for managing privileged accounts. Yet, these changes do not always go hand in hand with best practices.

For example, 40% of interviewees store privileged and/or administrative passwords in Word documents or spreadsheets on a company computer, making this information easy for a hacker to discover.

The report also notes that nearly half of the organizations commonly allow third-party vendors (such as supply chain and IT management firms) remote access to their internal networks, making them an additional pathway for cyberattack.

With the threat landscape constantly shifting, it's hard to determine what type of cyberattacks will be the most dangerous in the next months, leading many organizations today to adopt a "post-breach" mindset, meaning they operate under the presumption of a breach and have developed response plans.

This attitude leads to positive steps in defensive post- breach planning, but it also reveals a risk of overconfidence - or maybe complacency - and may hamper the ability to efficiently respond when facing a sudden cyberattack.

"Many global organizations are taking positive steps toward better protecting against the damaging effects of a cyberattack, including implementing measurable security programs to benchmark progress.

However, there is still a gap between 'awareness' and 'preparedness' in protecting against attacks," the report said.

Washington Times
China cyber espionage continues
Thursday, 29 September 2016
Byline: Bill Gertz

Washington - U.S. Cyber Command recently reported within secret government channels that China is continuing aggressive cyber espionage against American companies.
An intelligence report disseminated earlier this month stated that one of China's biggest cyber spying operations involved the theft of 1.65 terabytes of sensitive proprietary data from a major U.S. software company, according to a defense official familiar with the report.

The U.S. company was not identified by name. But the hacker group behind the data theft is part of the Ministry of State Security, China's main police and intelligence service.

The hacking operation by the MSS was carried out from at least October 2015 and contradicts the U.S.-China agreement on cyber espionage reached between President Obama and Chinese President Xi Jinping in September 2015.

The agreement requires both sides to halt government-backed cyber espionage against private companies. Critics say the accord was skewed in Beijing's favor because U.S. intelligence agencies are barred from spying for American firms, while most Chinese companies are under government control or influence and regularly benefit from the state's intelligence-gathering.

American intelligence officials testified earlier this year that they have serious doubts about China halting cyber spying in the United States. Only FBI Director James B. Comey has said he believes the Chinese are abiding by the agreement. The Chinese have stolen massive amounts of American proprietary corporate and defense data over the past decade or more.

According to National Security Agency documents leaked by renegade contractor Edward Snowden, in 2010 the NSA assessed Chinese data theft totaled 50 terabytes -- or five times the holdings of the Library of Congress. Defense industrial espionage by China has compromised information on the B-2 bombers, the F-22 and F-35 jet fighters, space-based lasers and other high technology weapons.

Another NSA document revealed that most of Chinese cyber espionage is carried out by a military, with the MSS a close second.

A Cyber Command spokesman did not respond to email requests for comment.

CNN.com
Cyber warfare: Who is China hacking now?
Thursday, 29 September 2016
Byline: Kristie Lu Stout

Hong Kong - It's the nagging glitch in the US-China relationship that was inevitably mentioned during the first US presidential debate this week between Donald Trump and Hillary Clinton -- cyber warfare. During the debate, Trump questioned whether Russia was indeed behind a series of cyberattacks on the Democratic National Committee -- a conclusion that US officials and his election rival have reached.

"She says, 'Russia, Russia, Russia,'" said Trump. "It could be China."

In the dark world of cyber- espionage, the finger of blame has often been pointed at China.

Earlier this year, China's cyber spies were accused of hacking into dozens of workstations and servers at the Federal Deposit Insurance Corp.

Last year, Chinese hacking was blamed for the massive data breach at the US Office of Personnel Management which compromised the data of over 21 million people.

And in May 2014, US federal prosecutors indicted members of the People's Liberation Army (PLA) for cyber-espionage for economic gain.

China has all along denied the allegations of state-sponsored hacking. But analysts say China's cyber operations are an active threat.

"Military intelligence has rapidly moved from cloak-and-dagger to bits-and-bytes over the last fifteen years... and China's no exception to that," says Bryce Boland, Asia-Pacific CTO of FireEye, a cybersecurity firm.

"China has been developing its capabilities within the PLA for a number of years, going back at least a decade. And their capabilities have now also been brought together into a single, strategic organization that is essentially a new branch of the military."

China is of course not the only actor in this era of cyber warfare.

But it has taken a significant step forward with the United States to establish some ground rules in a new domain of conflict with no widely-held norms.

During President Xi Jinping's state visit to the US last year, the China and the US formally agreed not to conduct or knowingly support economic cyber-espionage.

"I think China, after that, has tried to comply with that agreement," says Tong Zhao of the Beijing-based Carnegie-Tsinghua Center for Global Policy.

"China increasingly realizes it is in China's interests to promote a rule-based system."

And since the agreement, FireEye has observed a significant change in Chinese cyber activity.

"We've seen a shift in behavior since the Obama-Xi agreement. And that shift in behavior has resulted in a decrease in attacks against US and Western organizations for the purposes of stealing their intellectual property," says Boland.

"We've almost seen a pivot towards Asia. We've seen more targeted attacks now focused on information gathering and intelligence collection from countries on the periphery of China -- anyone with a land boundary or involved in a maritime dispute. And that kind of activity is much more focused on intelligence."

China's cyber-spies are pivoting away from stealing US trade secrets as they move towards gathering intelligence in a region fraught with geopolitical tension.

Take Taiwan, for instance.

Relations with Taipei and Beijing have been tense since the landslide election of Tsai Ing-Wen, Taiwan's first female president. Her Democratic Progressive Party (DPP) has traditionally leaned in favor of formal independence from China.

After the DPP's election win, its website was compromised and replaced with a spoofed site to collect data on visitors.

And then, there's Hong Kong.

Two years after Hong Kong's pro- democracy "Umbrella Movement," the city's first legislative elections since the mass demonstrations provided a platform for a small but vocal independence movement -- much to the chagrin of Beijing.

Before the election, two Hong Kong government agencies were targeted by cyber-attackers using new malware tools.

According to FireEye, both incidents were the work of Chinese state-sponsored hackers.

"We know those that those attacks were originated from China... they were clearly politically motivated attacks," says Boland.

"The only logical consequence is that they are operated by a group of people who had a political activity to conduct, so we believe they were state-sponsored."

Not all attacks officially sanctioned

But not all hack attacks originating from China have the official red seal of approval.

After an international court ruled that China did not have a historic right to a disputed area in the South China Sea, flight information screens at Vietnam's two biggest airports were hacked to show messages criticizing the Philippines and Vietnam and their territorial claims in the region.

Analyst Tong Zhao is convinced that the Vietnam airport hack was not the work of Chinese state agents.

"We used to assume that China is a country having a very centralized political system -- the central government must be in control of everything. I think that assumption is inaccurate," Zhao says.

And he's right. As powerful as it may be, China is not a single monolith. It's a vast system of many different actors -- military or civilian, state-backed or for-hire.

But China's many cyber actors can come together for a common goal -- to advance China's security interests and its standing in the information age.

The Local (Norway)
Oslo court denies Snowden no-extradition pledge
Wednesday, 28 September 2016
Byline: Staff report

Oslo - A Norwegian court on Wednesday dismissed a fresh bid by fugitive whistleblower Edward Snowden to win assurances he would not be extradited to the US should he come to Norway to collect an award.
The Oslo appeals court said it was not competent to offer such a pre-emptive guarantee since Snowden had not set foot in Norway and Washington had not submitted a formal request for his extradition.

The former National Security Agency (NSA) contractor, who lives in exile in Russia, faces US charges of espionage and theft of state secrets that could land him up to 30 years in jail.

The charges followed his 2013 release to the media of the extent of the NSA's surveillance programmes.

The appeals court upheld the June ruling of a lower court to which Snowden had taken his challenge against the Norwegian justice ministry's position that no guarantees on extradition could be given before a request had been formally received.

The Norwegian branch of the PEN Club has invited Snowden to Oslo on November 18th to collect the Ossietzky prize, which celebrates "outstanding efforts for freedom of expression."

Norway's Pen Club said it would appeal the case at the Supreme Court.

Norway was one of the countries where Snowden had sought asylum when he fled the US in 2013, but Oslo's response was that asylum seekers had to be physically present in the country to apply.

Considered a whistleblower by some and a traitor by others, Snowden won a similar Norwegian award in 2015, but was unable to collect it in person for the same reason.

Snowden has also been nominated for the Nobel Peace Prize, also awarded in Norway, for a third straight year. This year's award will be announced on October 7th.

NBC News
Were the Russians Behind the Massive Yahoo Email Hack?
Wednesday, 28 September 2016
Byline: Chris Francescani

New York - The hack of more than a half billion Yahoo email accounts was motivated by espionage, not profit, according to an independent cybersecurity firm report released Wednesday, which contends that an Eastern European state-sponsored actor appears to have ordered the massive hack as part of a coordinated effort to infiltrate the email accounts of U.S. military, diplomatic and political figures.
The findings by the cyber security firm InfoArmor are consistent with Yahoo officials' claim last week that a state-sponsored actor was behind one of the largest corporate breaches in U.S. history.

Yet InfoArmor's version of events, if accurate, provides significant new details about how and why the company was hacked. Minor league hackers who were peddling Yahoo users' personal information for cash in "dark web" marketplaces were also part of a foreign government espionage campaign dating back to 2014. And the findings also suggest that hacks of LinkedIn, Dropbox, MySpace and other firms -- breaches affecting billions of customers worldwide -- might've been part of the same state- sponsored effort.

In an interview with NBC News prior to the release of his firm's findings, InfoArmor's chief intelligence officer Andrew Komarov described the Yahoo breach as part of a larger, ongoing campaign to break in to the email accounts of prominent officials from the U.S. and across the globe.

He said that his analysts have uncovered a previously unidentified collective of elite black hat hackers-for-hire from Eastern Europe -- a group that InfoArmor analysts now contend was also responsible for hacks of the other social media companies.

Komarov said that a state-sponsored actor from Eastern Europe commissioned and later paid the hacker collective $300,000 for the Yahoo data trove. He said he didn't know if the hacks of the other social media companies were also commissioned by a state-sponsored actor, but believed it was likely. He also said he didn't know if the state that directed the hacks was Russia, or if the state-sponsored actor that paid the hackers was a Russian intelligence agency or some other arm of the Russian government, but that Eastern European hackers often have links to the Russian government.

Eastern European operatives tied to Russia's intelligence agencies have been widely suspected by cybersecurity researchers of multiple efforts to hack U.S. government officials' email accounts and the accounts of Democratic party operatives.

Komarov said that InfoArmor's conclusions that the hackers who attacked Linkedin and other companies were also responsible for the Yahoo breach are based on an extensive intelligence analysis, underground contacts and information gleaned from multiple sources surrounding the Yahoo hack. His firm went into dark web chatrooms and made contact with hackers advertising Yahoo addresses for sale who said they were involved in the breach, and accessed and validated what Komarov described as a "large sample" of the stolen Yahoo data.

Yahoo's confirmation last week of the massive breach has placed the tech giant at the center of a storm of controversy and unanswered questions, and could jeopardize the company's imminent $4.8 billion sale of its core business to the telecom giant Verizon.

It remains unclear how long and how much Yahoo officials knew about the breach before publicly acknowledging it. Company officials have said that Yahoo became aware of the breach in August, and began to investigate. Experts have said that it's not uncommon for a company of Yahoo's size to withhold disclosure of a suspected breach until an internal forensic investigation has been complete.

Last week, Yahoo's chief information security officer, Bob Lord, said that an internal probe had determined that usernames, email addresses, telephone numbers, dates of birth, security questions and answers, and in some cases passwords were harvested from more than 500 million compromised Yahoo accounts.

Lord said in a blog post that the company does not believe that banking or payment information was stolen, and has found no evidence to indicate that the hackers remain inside Yahoo's systems.

Yahoo declined to comment.

"Island- Hopping" To Reach U.S. Officials

Komarov said that the apparently state- sponsored actor involved in the heist was using an indirect but increasingly common strategy known as "island-hopping" or "leap-frogging" to reach its ultimate targets. Rather than going after U.S. and other government officials directly, the aggressors used the data from the hired black-hat hackers to breach the Yahoo accounts of friends, family and associates of their ultimate targets.

Once inside compromised Yahoo accounts, hackers can email or respond to their targets directly with seemingly legitimate Yahoo emails that are virtually indistinguishable from real ones.

"The target will receive the exact same email from the Yahoo user and, for him, it will look legitimate," Komarov said.

He said that while it's extremely difficult to directly infiltrate a Google Gmail account, for instance, all you really need to get into it is a compromised account of a Yahoo email user who corresponds with the Gmail user.

"Then you simply hack the Yahoo account's contacts, and then analyze the [emails] sent from the real object of interest. At some point you replace [a legitimate Yahoo email sent to a target] and fill it with malware," he said. Once the end target clicks on a link or an attachment in the infected Yahoo email, hackers can get inside the target's account.

From Foreign Espionage to Dark Web Marketplaces

Komarov said that the state-sponsored actor appears to have been working with the black hat hacker collective -- which the InfoArmor team has dubbed "Group E" -- for at least several years.

He said that his analysts have determined that Group E was also responsible for earlier, high-profile hacks of LinkedIn, MySpace, Dropbox, the music-streaming service Last.fm, the microblogging site Tumblr and others -- likely for the same purpose of identifying trusted third parties surrounding their real targets. Tumblr was purchased by Yahoo in 2013.

"If you calculate all the victims for all these hacks by the same group, it will be several billion victims," Komarov said.

InfoArmor has determined that at least some of the hacks of the other tech firms "were requested of Group E...so we assume that the Yahoo breach was one of the tools used for successful attacks against U.S. government officials."

Komarov said that in recent years the state sponsored actor approached Group E and asked them to hack millions of Yahoo email users' accounts. They provided Group E with specific email addresses they

were seeking, and when they were turned over and verified, the foreign agent agreed to purchase the entire trove, he said.

The agent had initially sought exclusive access to the stolen Yahoo data set, but balked at Group E's $500,000 price. Instead, Group E brought the price for the Yahoo trove down to $300,000, and retained the right to peddle the hacked emails elsewhere.

Komarov told NBC News that the Yahoo trove was later sold off to two well-known spammers, who exploited it for profit.

After it had been sold off and mined for months, Group E appears to have provided a low-level but well-known hacker named Tessa88 with mostly useless leftovers from the Yahoo trove to further distance the foreign agent from the Yahoo hack, Komarov said.

Tessa88 began advertising Yahoo data for sale on a Russian- speaking dark web marketplace, and appears to have partnered with a hacker who goes by the handle "Peace," or "Peace of Mind," to do the same in an English-speaking online marketplace called The Real Deal, according to InfoArmor.

It was only when Peace began advertising the Yahoo trove for sale that the company apparently became aware that they had been breached.

InfoArmor's report describes the entire enterprise as "carefully orchestrated in order to mask the actual sources of the hacks."

"Hands in the Cookie Jar"

An independent cybersecurity expert, who was briefed by NBC News on the upcoming report -- with the permission of InfoArmor -- said the firm's conclusions are consistent with what the cybersecurity community has privately postulated about the Yahoo hack.

"The story overall has a legitimacy to it," said Ann Barron-DiCamillo, chief technology officer for Strategic Cyber Ventures, who recently retired as director of the U.S. Department of Homeland Security's Computer Emergency Readiness Team (U.S. CERT).

"If you look at when the data was stolen, because the data was stolen in 2014 and never [until recently] showed up for sale on these [dark web] markets, there's usually going to be a nation-state involved," Barron- DiCamillo said on Tuesday.

"Nation-state actors like to have a degree of separation, so their hands are not in the cookie jar if they get caught. You're seeing them more and more leveraging others. Plus there's the fact that the [Yahoo] data wasn't quickly monetized." She said that with large scale hacks like those of Yahoo email users, the attackers must move quickly to profit off the theft.

If the motive is pure profit, hackers "are going to want to monetize [the data] so quickly, because it has a short shelf-life in terms of its value."

Barron-DiCamillo said that she wouldn't be surprised to see a nation-state haggle over the price for a data dump it had commissioned.

"It's just like any other business transactions," she said. "It feels different because the outcome is a little unusual, but it's just like any other business transaction."

Washington Post
Hackers have attempted more intrusions into voter databases, FBI director says
Wednesday, 28 September 2016
Byline: Matt Zapotosky

Washington - Hackers have attempted more intrusions into voter registration databases since those reported this summer, the FBI director said Wednesday, and federal officials are urging state authorities to gird their systems against possible other attacks.
Testifying before the House Judiciary Committee, FBI director James B. Comey said that the bureau had detected scanning activities -- essentially hackers scoping out a potential attack -- as well as some actual attempted intrusions into voter registration databases.

He said those attempts were beyond what had been made public in July and August, likely referring to hacking efforts in Illinois and Arizona, though he offered no other specifics.

"We are urging the states just to make sure that their deadbolts are thrown and their locks are on, and to get the best information they can from" the Department of Homeland Security, he said.

Federal officials have been closely watching attempted hacking of the U.S. election system. Russia is believed to be behind the high-profile hack of Democratic National Committee computers, and the FBI told Arizona officials in June that Russians tried to access their system.

That hack shut down the voter registration system for a week, although it turned out that the hackers had not compromised the state system or even any county system. Illinois officials said they discovered a successful breach in which hackers were able to retrieve a small percentage of voter records, and they said the FBI told them agents were looking at foreign governments and criminal hackers as possible suspects.

Hacking that would actually affect an election would be difficult because of the localized, disparate and sometimes antiquated nature of the United States' voting systems, and because the balloting systems

are generally not connected to the Internet, officials have said. Such efforts, though, could spark doubts about the strength of the system and the legitimacy of the outcome it produces.

Homeland Security Secretary Jeh Johnson has said that 18 states have asked for help in improving their election-systems cybersecurity.

The National (UAE)
End of an era as BlackBerry bites the bullet and stops making phones (Canada).
Thursday, 29 September 2016
Byline: Staff Report

Abu Dhabi - BlackBerry, the Canadian firm that helped to pioneer the smartphone market, said on Wednesday it will stop making handsets, outsourcing production to an Indonesian partner, after it reported another loss and a steep decline in revenue.
Analysts had been holding their breath for the news after the chief executive John Chen said September was his deadline for making the chronically money-losing device business profitable. BlackBerry's device business, which it calls "Mobility Solutions", will focus on developing applications and an extra-secure version of Google's Android operating system that it can licence to other companies.

"Our new Mobility Solutions strategy is showing signs of momentum, including our first major device software licensing agreement with a telecom joint venture in Indonesia," Mr Chen said. "Under this strategy, we are focusing on software development, including security and applications. The company plans to end all internal hardware development and will outsource that function to partners. This allows us to reduce capital requirements and enhance return on invested capital."

Handsets with the BlackBerry name will be produced under licence by Tiphone Mobile Indonesia, allowing BlackBerry to concentrate on software and services, the firms said.

BlackBerry posted a 31.8 per cent fall in second-quarter revenue. The firm's net loss came to US$372 million, or 71 cents a share, on revenue of $334m, as it booked $147 million in charges from its reorganisation. A year ago, it reported a profit of $51m, or 24 cents a share, on revenue of $490m.

Excluding one-time items, the company said it said broke even. On that basis, analysts had on average expected an adjusted loss of 5 cents a share on revenue of $393.7m, according to Thomson Reuters I/B/E/S.

The company raised its adjusted earnings outlook for the year to a range of breakeven to a 5-cent loss, compared with an earlier forecast of a 15 cent loss, after refinancing its debt and as margins improved.

The company's shares rose 6.7 per cent to $8.35 in premarket trading. BlackBerry, which a decade ago was among the largest smartphone makers, has seen its global market share slip to less than one percent amid domination by Apple and Android devices.

As the market shifted, BlackBerry has sought to refocus on software, including security applications, and the latest announcement takes the company out of the handset market entirely. "We are reaching an inflection point with our strategy. Our financial foundation is strong, and our pivot to software is taking hold," said Mr Chen.

New Indian Express
Govt websites hot targets of foreign hackers
Thursday, 29 September 2016

New Delhi - Attacks on government computers are nothing new. But, unlike the past, when computers had not entirely permeated official works, more and more departments today are digitising information that affect the common man and storing them away in computers.
Ergo, this switch has exposed them to more sophisticated cyber attacks and bigger security risks. IT security experts believe so, too, when they warn that malware presence in systems of a crucial department such as Finance could affect salaries, pensions, contract payments and other related transactions.

According to them, computers and websites of government departments are favourite targets of foreign hackers. "Last year, 50 websites were defaced by pro- Pakistani hackers. This year, there have been 10 such incidents. Although we are yet to achieve complete digitisation, there are serious risks to data security," said Project Manager of Computer Emergency Response Team- Kerala, Renjith A.

Using unauthorised software, hosting websites sans proper security audit and the staff 's lack of awareness to cyber security threats are some major reasons that make them targets of hackers. Stepping up Now, there are plans to improve security of websites via SDCs.

Besides providing services for government's access, the SDCs would act as mediators and convergence point between open unsecured public domain and sensitive government environment. "We do not allow hosting of applications in SDC without mandatory security audit," said T Mohan Dhas, State Informatics Officer. The 'audit' he referred to was a half-yearly practice of National Informatics Centre (NIC) - which provides IT solutions to the state - on applications hosted in SDC to check for security loopholes.

Le Figaro
Le Bigh Daddy Show, la web série animée qui caricature Daech
Thursday, 29 September 2016
Byline: Journaliste maison

Non identifié - Vidéos - Des activistes arabes ont choisi l'humour comme arme pour combattre la propagande de l'État islamique. Morceaux choisis.
Un message clair. «Nous nous moquons de Daech pour ce qu'ils sont, des idiots», indique la page d'accueil You Tube de la web série animée The Big Daddy Show. Combattre la folie meurtrière de Daech par l'humour, telle est la devise du groupe d'activistes arabes qui se cache derrière ces petits clips facétieux.

Des djihadistes qui n'arrivent pas à manier leurs armes, un calife qui joue à «Pokémon Go» ou encore un âne qui demande l'asile politique en Turquie... «Tout est fait pour amuser le spectateur»,relate la journaliste Chloé Domat qui a déniché cette pépite pour Rue89.

Journalistes, écrivains, artistes ou avocats composent ce groupe de militants. Certains vivent dans les territoires occupés par l'État islamique en Irak, en Syrie et en Libye. Menacés de mort, c'est sous couvert d'anonymat que des membres du groupe se sont exprimé sur Skype auprès de Chloé Domat: «L'État islamique a mis la main sur les réseaux sociaux. Ils mènent une guerre psychologique qui vise à terroriser les gens à travers le monde.»

Et le porte-parole d'expliquer sa démarche: «Nous voulons contrer leur discours en occupant la Toile avec de l'humour.» Les vidéos sous- titrées en anglais, et parfois en français, mettent en scène sept personnages qui évoluent autour du calife Abu Bakr el BighDaddy, une évocation détournée d'Abou Bakr al-Baghdadi qui dirige actuellement l'État islamique d'Irak. À ses côtés, son épouse Chaïmaa et quelques djihadistes, parmi lesquels un play-boy australien converti. Cette galerie de personnages a été présentée, dans la première vidéo mise en ligne en février dernier. Retouvez ci-dessous notre sélection de quelques épisodes.

«THEY» Arrived in the Caliphate

The Caliphate meeting

In the Caliphate Radio Studio

À visionner: quand la télévision parodie le terrorisme islamique:

Canadian Press
CSIS halts bulk data searches after watchdog flagged concerns
Friday, 30 September 2016
Byline: Jim Bronskill

Ottawa - Canada's spy agency sifted through large troves of data for information of value until a federal watchdog raised questions about a lack of guidelines for such searches, a new report reveals.
The Canadian Security Intelligence Service agreed to halt its acquisition of bulk datasets until it had a framework in place to govern the process of mining so-called "big data."

In its annual report tabled Thursday, the Security Intelligence Review Committee said CSIS used datasets to identify previously unknown individuals of interest by linking together types of information that have indicated "threat behaviour."

"They can be used to conduct indices checks by taking information already connected to a potential threat -- such as an address, phone number or citizen identification number -- and using it to search for 'hits' in the data," the review committee report says.

Overall, the review committee was satisfied that CSIS acted in accordance with the law in 2015-16. But it issued several recommendations to make the spy service more accountable when examining data, tracking Canadian foreign fighters in Iraq and Syria, exchanging information with other agencies and using new powers to disrupt suspected terrorist plots.

CSIS argued that openly sourced and publicly available datasets were akin to the phone book, and therefore restrictions in the CSIS Act limiting collection to "strictly necessary" information did not apply.

However, the review committee looked at the full list of datasets held by CSIS and, in come cases, disagreed with the spy service's assessment that they were publicly available and therefore beyond the legal restriction.

As a result of the committee's intervention, CSIS finalized and implemented guidelines for acquiring bulk data and agreed to ensure it abides by the CSIS Act in collecting such information.

Pierre Blais, the review committee chairman, said in an interview that for many years CSIS essentially gathered information "piece by piece," making it easier to meet the threshold of "strictly necessary."

The advent of electronic databases containing hundreds of thousands of pieces of information has made things "more complicated," he said.

The committee also found CSIS failed to tell the public safety minister about a notable overseas incident during a probe into jihadi-inspired fighters.

The committee says CSIS should have informed the minister about the development -- one of several problems with the spy service's investigations of Canadian foreign fighters.

Neither Blais nor Public Safety Minister Ralph Goodale's office would disclose details of the incident. However, a spokesman for Goodale said the minister was eventually briefed on the matter.

CSIS needs to deal with lingering challenges associated with overseas operations, the review committee report says. The spy service can expect these challenges to increase as government demand for intelligence on threats to the security of Canada from conflict zones grows.

The committee found CSIS needed to emphasize strategic planning for foreign operations -- for instance, ensuring employees fully understand the legal risks of certain activities.

It also called on CSIS headquarters to take a more decisive leading role in some foreign activities.

In addition, the committee said CSIS should develop formal means of consulting with other government agencies about its efforts to derail threats using new powers introduced in the legislation known as Bill C-51.

Globe and Mail
Yes, please, to real metadata legislation
Friday, 30 September 2016
Section: editorial

Editorial: Metadata is not something metaphysical. As Daniel Therrien, the Privacy Commissioner of Canada, rightly says, "We generate metadata constantly." Like an envelope, this outer shell of any electronic communication - a phone log, a time stamp, an e-mail address or an IP address - can reveal a lot.
Mr. Therrien is particularly worried about the Communications Security Establishment, the Canadian member of the intelligence alliance called the Five Eyes; the other four eyes are the United States, Britain, Australia and New Zealand.

As long ago as 2008, the Five Eyes dealt well with metadata. But then something went wrong with the CSE's "filtering technique" - that is, separating the metadata attached to the private communications of Canadians from that of the foreigners the CSE is mandated to monitor. In 2013, the CSE realized that Canadians were getting scooped up in its metadata trawling.

The CSE maintains that the risk to privacy is minimal. If that is so, why did the Five Eyes design the the filtering technique in the first place? Was it really superfluous?

CSE officials themselves acknowledged to the Privacy Commissioner's office that the CSE had improperly shared large amounts of metadata. This could undermine the public's confidence, and the various governments' too, that the Five Eyes will never, ever spy on each others' citizens.

Mr. Therrien pointed to the work of three computer scientists at Stanford University that was published this year. They argue that people's supposedly innocuous metadata are often every bit as revealing as the types of evidence that police present when they apply for search warrants.

The scientists concluded that "telephone metadata is densely interconnected, can trivially be reidentified, and can be used to draw sensitive inferences."

Meanwhile, the Supreme Court's decision in R. v. Spencer in 2014 strongly reasserted the search-warrant requirement in cases of electronic communication.

Thus, Mr. Therrien is right to say that the National Defence Act should be amended to clarify the CSE's powers and to establish clear legal standards to protect the privacy of Canadians. In other words, metadata legislation.

Globe and Mail
CSIS suspends some bulk data mining programs pending new guidelines
Friday, 30 September 2016
Byline: Colin Freeze

Ottawa - Canada's domestic spy service has halted its "bulk collection" of data after criticisms were raised within government about the lawfulness of such techniques.
A watchdog agency's new report about the Canadian Security Intelligence Service speaks of littleknown CSIS data- mining programs, and of how some have recently been suspended because of a lack of clear rules and guidelines surrounding them.

CSIS is said to have wanted to leverage big pools of data "to identify previously unknown individuals of interest by linking together types of information that have mirrored threat behaviour," according to the report. But after concerns raised in the report, "CSIS agreed to halt ingesting bulk data sets pending" new rules.

These findings are from the Security Intelligence Review Committee (SIRC), the watchdog agency that tabled its annual report in Parliament on Thursday.

The cryptic discussion of CSIS's "data management and exploitation activities" is intriguing on several levels. Talk of spies "ingesting" data in "bulk" has had connotations of intelligence officials indiscriminately amassing citizens' telecommunications records. Yet CSIS officers, who work to track terrorists within Canada, are generally understood to handle cases one wiretapping warrant at a time.

This makes them more like conventional police detectives than the foreignfocused signals-intelligence - or "sigint" - spies who deal in volume.

On Thursday, a CSIS spokeswoman said the agency engages in a different kind of "bulk." "The collection referred to in the SIRC report is not the same collection that is sometimes done by sigint agencies," said Tahera Mufti.

She said what was at issue was CSIS collecting "data sets like maps, foreign telephone directories and airport codes." She did not explain how such data pools would help CSIS track terrorists.

The fundamental critique of SIRC, which won't speak to what kind of data it is referring to, is that CSIS has been amassing records at rates that may push past the parameters of federal law. Under its 1984 act, the spy agency can only collect information that is "strictly necessary" to preserve national security.

SIRC says the spy agency it watches keeps two kinds of records. "Referential" data sets are less inherently sensitive, and acquired through publicly available means. This probably means CSIS is buying material from "Big Data" brokers who routinely sell similar material to corporations.

But CSIS also independently acquires "non-referential" data.

SIRC regards such records as relatively intrusive "as they contain bulk information on a wide variety of individuals," the report says. "However, these can only be retained if they are assessed as being relevant to an ongoing, mandated investigation."

If CSIS wants to dredge up any data in bulk, SIRC says there needs to be compelling reasons.

"If there is no reasonable alternative to bulk collection, CSIS needs to provide an objective assessment of how closely connected the bulk information is to intelligence of value," reads the report.

This week, the federal Privacy Commissioner called for Parliament to pass new laws after finding Canada's other intelligence agency had been careless with records about the logged telecommunications of Canadians.

Communications Security Establishment (CSE), a foreignfocused "sigint" agency, says that whenever it collects Canadians' telecommunications trails, it does so only "incidentally." That's because it is pursuing foreign records in enormous volumes.

While CSIS and CSE have vastly different mandates, they also have adjacent headquarters. They can team up if a Federal Court judge endorses a joint operation.

In 2013, the former U.S. intelligence contractor Edward Snowden leaked documents to the media about the bulk collection of American citizens' telecommunications trails.

One revealing record showed CSE's and CSIS's U.S counterparts teamed up to acquire Americans' phone bills, thanks to sweeping warrants signed in secret courts.

The United States "targets the communications of everyone. It ingests them by default," Mr. Snowden said.

Washington Post
Cyber-experts: New Md. voting system is at risk
Friday, 30 September 2016
Byline: Josh Hicks

Washington - Cybersecurity experts are warning that Maryland's online absentee-ballot system is dangerously vulnerable to tampering and privacy invasions, both growing concerns in a year when hackers have breached the Democratic National Committee and attempted to access boards of elections in at least two states.
The system allows voters who request an absentee ballot to receive the form by email and send back a printed hard copy, with their votes marked by hand or with a new online tool that allows users to mark the document with the click of a mouse or the touch of a keyboard, then print it for mail delivery. Until this year, in large part because of security concerns, the latter option was available only to people with disabilities.

Critics say it is easy for impostors to use stolen credentials to request absentee ballots or for cyberthieves to hack in and retrieve data about who is requesting ballots or details of votes that were cast online.

All registered voters in Maryland are allowed to request an absentee ballot, regardless of whether they will be away from their polling station on Election Day.

With less than six weeks before Election Day, officials say they have taken steps to safeguard their online system, which was required as part of a 2013 law designed to increase voter participation and make voting more accessible. The board voted 4 to 1 on Sept. 14 to certify broad use of the online marking tool.

"The issue of electronic- ballot delivery is resolved," Nikki Charlson, deputy administrator of the Maryland State Board of Elections, said Thursday. "The General Assembly has made its policy decision, and without a repeal of the statute, it is what it is."

A group of computer scientists and cybersecurity experts wrote to the board two days before its vote and urged it not to certify the system, saying the setup would "make Maryland one of the most vulnerable states in the U.S. for major election tampering."

Save Our Votes, a voting-integrity group, says the state board shouldn't have certified the online marking tool, arguing that Maryland law prohibits the panel from greenlighting any voting program until it can ensure the secrecy of ballots.

"No information transmitted over the internet can be considered private or secure," the group said in an August letter to the board.

Charlson said the elections board has implemented numerous safeguards, including software that tries to identify and exploit potential vulnerabilities, regular monitoring for suspicious behavior and the use of best practices for information technology. She said the panel has no plans to take additional action.

During the board's meeting on Thursday, members met in a private session to discuss the security of the online system but did not share details of that conversation.

Chairman David J. McManus Jr. (R) and Vice Chairman Patrick J. Hogan (D) said that the state had adequately tested the system and that no online program could be completely secure.

"I felt comfortable, based on briefings that we had from our information-technology staff as well as the contractors," Hogan said. "Based on the continued work that is going on, it's as secure as it can be. The idea that any system is 100 percent secure - there is no such thing. If you took that attitude, you would never have any system."

Kelley A. Howells (R), the board member who voted against certification, said she was "worried by some of the writings of people at major universities saying 'stay away from the Internet.' " But she said she feels confident with the work of the board's information- technology team.

Charlson said that the state had sent out about 10,000 emails to voters who wanted to access absentee ballots as of Thursday and that 4,200 of those accounts had been logged into. Among those users, 2,500 had chosen to mark their ballots by hand, while 1,800 had chosen to use the online tool to mark their ballots.

The 2013 law requires online delivery of absentee ballots for all voters who request the service. It says the state board had to certify that the online ballot-marking system would ensure privacy before deploying it.

After a divided board refused to certify the tool in 2014, advocates won a federal court order that required the state to make the option available for the disabled anyway.

The 2016 presidential election will be the first time the state has offered the online ballot- marking system to all absentee voters.

More than 30 states use some form of electronic system for ballot delivery.

Alaska and Washington are the only other states that allow all voters to obtain absentee ballots from personal computers. Unlike Maryland, both of those states use a signature- verification process. Alaska also allows ballots to be submitted online.

"Very little information is required to impersonate a voter and request an online absentee ballot," Save Our Votes said in its letter.

North Dakota permits electronic ballots for overseas citizens and military members, while Missouri provides them only for members of the military serving abroad.

At least 20 other states and the District will allow certain voters living overseas to return their absentee ballots via email or fax in the upcoming election.

The threat of cyberattacks against electronic-voting systems has caused alarm within the Obama administration. Last month, U.S. Homeland Security Secretary Jeh Johnson said the federal government should consider designating electronic-ballot-casting systems as "critical infrastructure," meaning that, like the nation's power grid, they would require enhanced protections.

New York Times
It's No Cold War, but Putin Relishes His Role as Disrupter
Friday, 30 September 2016
Byline: David E. Sanger

Washington - Escalating airstrikes in Syria. Sophisticated cyberattacks, apparently intended to influence the American election. New evidence of complicity in shooting down a civilian airliner.
The behavior of Russia in the last few weeks has echoes of some of the uglier moments of the Cold War, an era of proxy battles that ended in 1991 with the collapse of the Soviet Union. President Obama, fresh from a meeting with President Vladimir V. Putin this month, wondered aloud whether the Russian leader was content living with a "constant, low-grade conflict." His reference was to Ukraine, but he could have been addressing any of the arenas where Mr. Putin has reveled in his new role as the great disrupter of American plans around the globe.

"It seems to me we have Mr. Putin's answer," said Richard Haass, the president of the Council on Foreign Relations and the author of a coming book, "A World in Disarray." "He's answered in the affirmative. Low-grade conflict is his thing. And the question is how directly or indirectly we introduce costs."

None of these conflicts have, in fact, cost Mr. Putin very much. Cyberpower in particular is tailor-made for a country in Russia's circumstances -- a declining economy with the gross domestic product of Italy. It

is dirt cheap, hard to trace to a specific aggressor and perfect for sowing confusion, which may be the limits of Mr. Putin's goals.

The bigger question confronting American intelligence officials, though, is whether the Russian president has a grander scheme at work. So far, their conclusion is probably not. Mr. Putin's moves, they argue in background conversations, are largely tactical, intended to bolster his international image at a moment he has plenty of troubles back home.

For a year now, the White House has argued that these escalating clashes, while worrisome, do not constitute a new Cold War. There is no great ideological struggle underway. No one is brandishing nuclear weapons, though after two decades of reducing their forces, each is now racing to modernize them. Syria is a humanitarian disaster of barely imaginable scope, but it is not a fundamental strategic threat to American interests.

Yet the few veterans of that era still in senior posts see similarities. "It shouldn't come as a big shock to people," James R. Clapper Jr., the director of national intelligence, said about the "information warfare" that has been put to sophisticated use from Kiev, Ukraine, to Washington. "I think it's more dramatic maybe because now they have the cybertools."

Mr. Clapper's colleagues go a step further in less public conversations. They argue that Mr. Putin has played his hand skillfully, stringing along Secretary of State John Kerry in a yearlong negotiation over cease-fires and political transitions in Syria, all the while bolstering their proxy, President Bashar al-Assad. Mr. Kerry's efforts in Syria all but collapsed this week in waves of Russian and Syrian government airstrikes.

The deal in Ukraine is hanging on, but just barely: Russia conveniently ignores many of the commitments it signed and has denied involvement in the downing two years ago of a Malaysia Airlines jet flying over Ukraine that killed 298 people.

The theft of voter rolls in Arizona and Illinois -- and "poking around" in the networks of other states, as James B. Comey, the F.B.I. director, described it to Congress this week without naming the Russians as perpetrators -- may be intended to rattle the United States, rather than change votes.

"It's probably not real, real clear whether there's influence in terms of an outcome," Mr. Clapper said. "What I worry about more -- frankly -- is just sowing the seeds of doubt, where doubt is cast on the whole process."

So far, the American response has been decidedly mixed. The West's sanctions against Russia for the annexation of Crimea have clearly stung; Russian officials make no effort to hide their desire to get them lifted. But the White House has not publicly blamed Russia for the hacking of the Democratic National Committee, the theft of the Arizona and Illinois voter registration rolls, or breaking into the cellphones of Democratic operatives.

Mr. Obama pulled Mr. Putin aside in China for a conversation that officials decline to recount, and Mr. Kerry has done the same with his counterpart during the long effort to find common ground in bringing peace to Syria.

The president's reluctance to publicly blame the Russians -- born of concern that taking on Mr. Putin head-on would only invite him to escalate -- has led to something of an uprising in parts of the White House and the State Department. A range of cyberstrategists and younger diplomats have complained over the past nine months that the failure to draw lines has encouraged Mr. Putin to see what else he can accomplish, especially at a time of political transition in the United States.

Few in the American intelligence community predicted much of this. Intelligence assets have been so focused for the past 15 years on counterterrorism that traditional targets have taken something of a back seat -- they have not been ignored, one senior intelligence official said recently, but only lately have they begun to receive new resources.

Perhaps that contributed to some misjudgments. It was more than a year ago that Mr. Obama said Russia would find itself in a "quagmire" in Syria; it may yet, but so far Mr. Putin's air war has propped up Mr. Assad, though at such a horrific human cost in the city of Aleppo that the United Nations' humanitarian chief, Stephen O'Brien, told the Security Council on Thursday that it had become a "merciless abyss of humanitarian catastrophe."

Mr. Kerry threatened earlier this week to cut off all negotiations with the Russians. The Russian Foreign Ministry responded that the United States was in an "emotional breakdown" and rejected the effort to restore a seven-day pause in hostilities, the first step in an agreement Mr. Kerry reached with his counterpart, Sergey V. Lavrov, on Sept. 9.

That was mild compared with what the spokesman for the Russian Ministry of Defense, Maj. Gen. Igor Konashenkov, said. He called the opposition leaders the United States has been not-so-covertly arming in Syria "a U.S.-controlled terrorist international," using a phrase that was a throwback to Soviet times.

And he warned that "should any attempt be made to carry out any threats against Russia or Russian servicemen in Syria, it is far from guaranteed" that the American-backed militias would have enough body bags.

So far, though, Mr. Putin has shown some caution. While he has tried to intimidate NATO nations with overflights of bombers, nuclear submarine runs along coasts and military exercises near the borders of Estonia and Latvia, he has been careful to stay on his side of the boundaries.

"These are all occurring in gray-zone locations with gray-zone tactics," said Robert Kagan, a historian at the Brookings Institution who has written on the return of geopolitical conflict. The question the United States will have to face, he added, is "Are we willing to operate in the gray area, too?"

New York Times
In Hacked Audio, Clinton Rethinks an Obama Plan
Friday, 30 September 2016
Byline: David E. Sanger, William J. Broad

Washington - Hillary Clinton expressed doubts about whether the United States should go forward with a trillion-dollar modernization of its nuclear forces at a fund-raiser in February, questioning an Obama administration plan that she has remained largely silent on in public.
Mrs. Clinton also suggested she would be far tougher against foreign nations that hack into American computer networks and would kill one of the Pentagon's pet projects, a nuclear-tipped cruise missile.

"The last thing we need," she told the audience, "are sophisticated cruise missiles that are nuclear armed."

Her comments were contained in an audio recording of the fund- raiser that appeared on the website of The Washington Free Beacon, a conservative publication, which said it was gleaned from the hack of a campaign staff member. But it said nothing about who did the hacking.

At a moment when Mrs. Clinton and the Obama administration have warned that Russia is trying to influence the American election, the mysterious release of the tape is also certain to raise new questions about the scope of attacks on the Democratic National Committee and the Clinton campaign.

A former Defense Department official present at the fund-raiser, Andrew C. Weber, who raised the question about nuclear modernization, verified the contents of the tape, but also suggested its release was part of the same hacking campaign that exposed D.N.C. emails.

Before she turned to nuclear matters, Mrs. Clinton used the fund-raiser to suggest that she would be much firmer against foreign nations that hack into American networks. Though the administration never formally accused China of stealing the security-review records of nearly 22 million federal employees and contractors, she called the theft "a gold mine for Chinese intelligence."

"They are at it all the time," she said of the Chinese state-sponsored hackers. But she also seemed to suggest -- more directly than she did in Monday night's debate -- that she thinks the best deterrent to the Russians, the Chinese, the Iranians and the North Koreans, all of whom she named, was a dose of American offensive cyberweaponry.

"They have physical assets that are also connected on the internet," she said. "So they have to know we would retaliate. So that provides a certain level of deterrence."

It may not: The Russian-backed hacks of the Democrats' infrastructure, so far without a visible American response, suggest that the deterrence Mrs. Clinton is relying on is not working.

The 50-minute recording was made in February during a fund-raising event at the home of Beatrice and Anthony Welters in McLean, Va. Mrs. Welters was ambassador to Trinidad and Tobago when Mrs. Clinton was secretary of state.

Mr. Weber was an assistant secretary of defense for nuclear programs from 2009 to 2014. Last year, after leaving office, he joined William J. Perry, a secretary of defense in the administration of President Bill Clinton and one of the Democratic Party's most influential nuclear advisers, to write an op-ed in The Washington Post strongly opposing White House approval of an upgraded nuclear cruise missile.

The missile is part of a sweeping modernization of the American nuclear arsenal that is estimated to cost up to $1 trillion over three decades. Undertaken by the Obama administration, it features new factories, refurbished nuclear arms, and a new generation of weapon carriers, including bombers, missiles and submarines. The new bombers are to carry the new cruise missile.

At the fund-raiser, Mr. Weber asked Mrs. Clinton about the modernization push and whether she, as president, would cancel the cruise missile, which he called a "particularly destabilizing, dangerous type of nuclear weapon."

"I certainly would be inclined to do that," she answered. "The last thing we need are sophisticated cruise missiles that are nuclear-armed."

Mrs. Clinton went beyond the question to warn of an emerging nuclear arms race, naming Russia and China as well as Pakistan and India. "This is one of the most dangerous developments imaginable," she told the audience.

"Pakistan is running full speed to develop tactical nukes in their continuing hostility with India." she said. "But we live in fear that they're going to have a coup, that jihadists are going to take over the government, they're going to get access to nuclear weapons, and you'll have suicide nuclear bombers. So, this could not be a more threatening scenario."

The United States, Mrs. Clinton said, needs to "do everything we can" to restrain the competitions, including exploring new treaties with Moscow that would go beyond the New Start treaty of 2010, which she helped negotiate.

Mrs. Clinton proceeded to praise Mr. Perry, saying the more he spoke out publicly and joined with Republican statesmen in trying to curb nuclear arms, "the better off we'll be in trying to really cut this off.'

"This is going to be a big issue," she added. "It's not just the nuclear-tipped cruise missile. There's a lot of other money we're taking about to go into refurbishing and modernization."

"Do we have to do any of it?" Mrs. Clinton asked. "If we have to do some of it, how much do we have to do? That's going to be a tough question, so I will look to people like you and Bill Perry to help me answer that question."

Mr. Obama has said he wants to reduce the role of nuclear weapons in American strategy, and his aides have hinted he may believe the modernization program needs reconsideration. But he seems to have left that to his successor, and the cruise missile Mrs. Clinton spoke about so disparagingly remains in the Pentagon budget.

NBC News
Hackers Target Election Systems in 20 States
Friday, 30 September 2016
Byline: Multiple reporters

New York - There have been hacking attempts on election systems in more than 20 states -- far more than had been previously acknowledged -- a senior Department of Homeland Security official told NBC News on Thursday.
The "attempted intrusions" targeted online systems like registration databases, and not the actual voting or tabulation machines that will be used on Election Day and are not tied to the Internet.

The DHS official described much of the activity as "people poking at the systems to see if they are vulnerable."

"We are absolutely concerned," the DHS official said. "The concern is the ability to cause confusion and chaos."

Only two successful breaches have been disclosed, both of online voter registration databases, in Illinois and Arizona over the summer.

While those two hacks were linked to hackers in Russia, the DHS official did not say who was responsible for the other failed attempts, noting that "we're still doing a lot of forensics."

Meanwhile, intelligence officials tell NBC News there is now "no doubt" the Russian government is trying to influence the election.

Classified material, prepared for briefings of Donald Trump and Hillary Clinton and examined by NBC News, reveals that officials have drawn "direct links" between Vladimir Putin's government and the recent series of hacks and leaks.

The secret material confirms what lawmakers on the Senate and House Intelligence Committees said they had concluded last week, based on briefings they received.

"At the least, this effort is intended to sow doubt about the security of our election and may well be intended to influence the outcomes of the election -- we can see no other rationale for the behavior of the Russians," Sen. Dianne Feinstein and Rep. Adam Schiff, both D-Calif., said in a statement.

For weeks, American officials have been saying that Russian intelligence agencies were behind hacks into the DNC, state election databases and other political entities, but they weren't definitive about the motive since nations routinely hack into their adversaries' political organizations to gather information for spying purposes.

In recent days, U.S. officials tell NBC News, American spy agencies have determined that the Russian government was behind the leaks of Democratic National Committee emails to Wikileaks and others -- and that the goal was to undermine confidence in the American presidential election.

Another possible aim: sending a geopolitical warning.

NBC News has learned that this summer, Adm. Michael Rogers, director of the National Security Agency, told congressional intelligence committees that Washington believes "potential adversaries might be leaving cyber fingerprints on our critical infrastructure partly to convey a message that our homeland is at risk if tensions ever escalate toward military conflict."

FBI Director James Comey told a congressional hearing this week that he is taking the threat to election systems "extraordinarily seriously."

"We are urging the states just to make sure that their deadbolts are thrown and their locks are on and to get the best information they can from DHS just to make sure their systems are secure," he told the House Judiciary Committee.

DHS has been pushing states to undergo free cyber-hygiene scans and other assessments before the Nov. 8 vote. Yet, as Homeland Security Secretary Jeh Johnson told a congressional committee this week, just 18 have signed up for the free help. The results of those scans are not available yet.

Washington Times
FBI partly blames Snowden for reduction in email, phone surveillance
Friday, 30 September 2016
Byline: Andrea Noble

Washington - The FBI's use of a surveillance statute to collect Americans' phone and email records has declined since details about the program were leaked by Edward Snowden in 2013, a watchdog report has found.

The FBI's use of Section 215 of the Patriot Act to obtain "business records" as part of national security investigations peaked in 2012, with the Foreign Intelligence Surveillance Court approving 212 orders seeking records, according to a report released Thursday by the Justice Department's inspector general's office.

The program was publicly disclosed in June 2013 after the former National Security Agency contractor leaked information to the press. That year, the number of orders authorized by the court dropped to 179. The number of orders approved by the court has continued to decrease annually, with 142 orders approved in 2015.

The program allowed authorities to collect information about clients from service providers, such as email or phone records -- including the numbers, times and durations of calls. Outcry over the program after Mr. Snowden's revelations led to reform the surveillance program. When Congress renewed the USA Freedom Act last year, it blocked bulk collection and storage of data.

A deputy chief within the FBI's National Security Division partly blamed Mr. Snowden's disclosures for the decrease in use of the provision.

"He attributed the decline in part to revelations by Edward Snowden about the U.S. government's use of Section 215 to collect bulk telephony metadata, both in terms of the stigma attached to use of Section 215 and increased resistance from providers," the inspector general's report said.

Responding to the report, FBI officials told the inspector general's office that the degree to which Mr. Snowden's disclosure led to the decrease was speculative and said agents had come to rely more on a different statute to obtain surveillance approvals -- specifically, Section 702 of the Foreign Intelligence Surveillance Act, which allows surveillance of foreigners.

Under the USA Freedom Act reforms enacted in 2015, authorities can't collect and keep bulk telephone data in government databases. Instead, spy agencies have to ask phone companies for data -- and they must submit a narrow search so it's clear that analysts are looking for a specific person, number or group, rather than bulk collection.

Frustration with oversight of the Section 215 program and the length of time it took to approve orders under it appear to have played a role in the decline of its use even before the law's reform.

"Agents also told the OIG that they increasingly were electing to use criminal legal process instead of FISA authority in counterterrorism and cyber investigations because of their frustrations with the lack of timeliness and the level of oversight in the business records process," the report states.

Some were opting to open parallel criminal cases and using grand juries "to obtain the same information more quickly and with less oversight than a business records order."

The increased reliance on other surveillance statutes or basic criminal processes raises questions from privacy rights advocates.

"We want the department to go through a process with a high level of oversight," said Neema Singh Guliani, legislative counsel with the American Civil Liberties Union.

If agents opt to use other surveillance statutes to obtain records because they are able to do so more easily, it raises concerns over the level of oversight of the alternative methods now favored, Ms. Singh Guliani said. If agents are falling back on basic criminal investigative practices to obtain information for national security investigations, "it raises real practical questions" about whether the specialized national security provisions are needed.

The report indicates that of the 561 records requests approved from 2012 through 2014, a median of 115 days passed from the time a field office made a records request to the FISA Court's order.

The inspector general's report recommends finding a way to make the process more efficient, particularly in cyberdata cases.

The FISA Court denied none of the 561 business records requests, though the report notes that some draft applications were withdrawn and not formally submitted for numerous reasons.

Large portions of the inspector general's 68-page report were redacted.

Overall, the report found that the business record orders were used "far more frequently in counterintelligence cases than as a counterterrorism or cyber tool." The exact figures for each type of case were redacted from the report.

CBS News
Cybersecurity expert: One battleground state most vulnerable to voting hacks
Thursday, 29 September 2016
Byline: Shanika Gunaratna

New York - The battleground state of Pennsylvania might as well have a target on its back as Election Day nears, the cybersecurity company Carbon Black warned in a new report released Thursday.
"If I was a 400-pound hacker, I would target Pennsylvania," Carbon Black chief security strategist Ben Johnson told CBS News, a reference to Donald Trump's comment in Monday's debate that the hacker behind the Democratic National Committee email leak could be someone "sitting on their bed that weighs 400 pounds."

U.S. intelligence officials actually believe Russia was behind that breach and a number of recent intrusions into state voter databases.

What makes Pennsylvania such a vulnerable target for hackers seeking to influence the election?

Across the state, most Pennsylvania counties use particularly high-risk electronic voting machines that leave behind zero paper trails, which could be useful to audit the integrity of votes cast. In addition, many of these machines -- called "direct-recording electronic" machines -- are running on severely outdated operating systems like Windows XP, which has not been patched by Microsoft since 2014, Carbon Black said in its report. In general, these complex machines are a headache compared to so-called fixed-function devices that perform just one task and are thus harder to hack.

Politically, Pennsylvania has extraordinary value with 20 electoral votes and polls showing a narrowing race between Hillary Clinton and Donald Trump.

According to Carbon Black, Pennsylvania is an easier target than other battleground states like Ohio and Florida. Ohio conducts post-election audits and has a manual recount provision that kicks in for tight races. Florida also has required audits.

The general lack of a paper trail throughout Pennsylvania is a recipe for disaster, Johnson said. Before he co-founded Carbon Black, Johnson was a National Security Agency (NSA) engineer and defense contractor during the Iraq and Afghanistan wars.

"If you buy something in the store with a credit card, you get a receipt. But if you cast your vote for president of the United States, you get nothing," Johnson said.

According to the Brennan Center for Justice, more than 40 states are using voting machines that are at least ten years old. Across the country, the disjointed patchwork of different ballots, different electronic voting machines, and different polling station standards creates a perfect storm for targeted hacking, particularly in battleground states.

With just over a month till Election Day, there's no time to redesign the voting process nationwide. But it's imperative to minimize risk in the system we already have, Johnson said.

At the very least, he suggested election officials should:

* Keep individuals from having prolonged access to the physical voting machines;

* Turn off any communications capacities, like Wi-Fi or Bluetooth, on the machines;

* Make sure no other devices are plugged into the machines;

* And train polling station workers, typically volunteers unfamiliar with cybersecurity, on the importance of enforcing these measures.

In the U.S., states select and operate their own voting systems, adhering to federal standards-- but beyond those standards, the federal government cannot dictate how states run their voting systems.

That oversight could conceivably change. Earlier this month, Rep. Hank Johnson, D-Ga., introduced legislation that would designate voting systems as "critical infrastructure" -- a move that would heighten the federal government's security obligations towards voting systems nationwide. It would also limit the purchase of new voting systems that do not provide adequate paper trails for verification.

But for now, the federal government's power is limited to pushing individual states to "wake up" to the imminent threat of voting system hacks, Johnson said.

"You kind of need a federal, Congressional discussion. You need that kind of energy and influence. But it's really up to the states to opt into something like that," he said of the possibility of an overhaul.

Fears of hackers tampering with Election Day have mounted for months, especially during a campaign season in which the Democratic National Committee's internal email communications were leaked to the public and Donald Trump invited a foreign actor, Russia, to hack into his rival's emails (jokingly, he later said).

In August, the FBI found evidence that hackers broke into Arizona and Illinois' state election databases. And this week, law enforcement officials told CBS News the intrusions may have been more widespread, with about 10 states' systems probed or breached.

Experts said the ultimate goal of these hackers is not necessarily to change the outcome of the election, but to de- legitimize it by sowing doubt, uncertainty and suspicion through a series of cyberattacks.

Last month, Senate Minority Leader Harry Reid asked the FBI to be more aggressive in examining the possibility that Russia could try to "falsify official election results."

There is no indication that any previous U.S. election has been tampered with.

But the fear of Election Day hacks this time around has already had a chilling effect on the electorate. More than half of U.S. voters (56 percent) are concerned that this year's election will be affected by a cyberattack, and more than one-third of U.S. voters (36 percent) feel their voting information is insecure, according to the survey by Carbon Black, which polled 700 registered voters ranging in age from 18-54.

Among the voters who believed their voting information is not secure, one in five said they would consider not voting in this year's election given their concerns -- a "surprising and depressing" reality that America must grapple with, Johnson said.

"We fundamentally say, 'Go vote. Don't let this get you down.' But we need to understand the risk," Johnson said.

He likened this moment in U.S. politics to an addict's first Alcoholics Anonymous meeting: the first step in a long process is acknowledging that a problem exists, he said. The next is probing the weaknesses in the system with the same vigor that, chances are, America's adversaries are doing at this very moment.

What's Johnson's personal plan for Nov. 8? The former NSA engineer said he's somewhat comforted by the state he's registered in.

"I'm in Illinois, and most of Illinois gets a paper receipt," he said.

The Intecept
The FBI Wanted to Target Yemenis Through Student Groups and Mosques
Thursday, 29 September 2016
Byline: Cora Currier

Washington - The FBI envisioned infiltrating mosques and Muslim student associations to look for young Yemenis to serve as informants, according to an internal presentation obtained by The Intercept. The document suggests that agents scour Facebook "to find individuals who are dramatically increasing their levels of piety -- that's the demographic you want."

"Since we're looking for young people re-engaging with their Islamic faith," it continues, "the local MSA [Muslim Student Association] is a great place to start."

The 24-slide presentation, prepared for a Source Development Unit in the FBI's Directorate of Intelligence, is titled "Responding to the Yemeni Threat: Scenarios for CHS Development," using the bureau's lingo for informants, which it calls "confidential human sources."

It's not clear if the presentation describes a specific program that was put into action or whether it was meant to offer general tips for cultivation of sources who could provide information related to al Qaeda in the Arabian Peninsula, al Qaeda's Yemen affiliate. The document appears to suggest identifying potential informants solely on the basis of their religious affiliation or national origin, which could violate FBI rules meant to curb profiling and discrimination.

The document is undated, but from references in the text, it appears to have been prepared around 2010 or 2011 by Centra Technology Inc., a company selling intelligence services. Centra Technology has

had regular contracts with the FBI since 2008, including for training courses vaguely described in contract records as "analytic tools and techniques." Centra did not respond to a request for comment.

According to FBI operating guidelines originally promulgated in 2008, agents are allowed to use a variety of tactics when it comes to seeking information to identify potential informants or recruiting particular individuals, including database searches, physical surveillance, and even combing through someone's trash. Still, the current version of the guidelines state that someone should not be targeted as an informant "based solely on race, ethnicity, national origin, religion or activities protected by the First Amendment, or a combination of only such factors."

It's not clear how looking at expressions of piety and attendance at a Muslim student group would not run afoul of that guidance. An FBI spokesman declined to answer specific questions about the document, instead providing a statement saying that the FBI conducts investigations under guidelines that are "intended to ensure that FBI employees act in accordance with the law and the Constitution." He added that "all Confidential Human Source relationships with the FBI are voluntary."

According to the FBI's guidelines, investigations involving academic or religious groups are considered "sensitive investigative matters" and require extra supervision and particular rules for deploying undercover officers or informants, as do investigations of mosques. The presentation does not mention any such sensitivities.

"The FBI's focus on Muslim student groups does not make anyone safer," said Ramzi Kassem, a law professor at the City University of New York who directs CLEAR, an initiative that works with communities affected by counterterrorism policies. "It also comes at the expense of students whose college experience is no longer a time for intellectual exploration and the building of lasting friendships but a paranoid nightmare where certain thoughts are taboo and your classmate might be an informant."

FBI surveillance of mosques and Muslim communities in the past has generated controversy, as has the bureau's aggressive use of its army of informants -- which grew to over 15,000 in the years after the 9/11 attacks. In 2012, the American Civil Liberties Union obtained documents showing that the FBI had used "mosque outreach" programs ostensibly meant to build relationships with Islamic communities in order to collect intelligence. There is a long-running lawsuit over an FBI informant who was sent into mosques in Southern California in 2006 and 2007.

Federal authorities investigating the influence of the Islamic State in the United States have increased their use of informants and sting operations. In the past two years there have been 101 Islamic State-related cases in U.S. courts, and 59 percent of them involved the use of informants or undercover agents, according to a report released in July by the Center on National Security at Fordham Law School.

Many of the individuals who actually carried out attacks motivated by violent Islamic ideologies in recent years were known to authorities, illustrating the difficulty in predicting who may become violent. Omar Mateen, who killed 49 people in an Orlando nightclub this year, had been the subject of an FBI

investigation involving informants; the suspect in recent bombings in Manhattan and New Jersey, Ahmad Khan Rahami, was reported to the FBI by his own father.

"Younger, More Devout Sources"

The Centra Technology presentation obtained by The Intercept is undated but the figures mentioned in it suggest that it was prepared around 2010 or 2011. It focuses on the threat to the United States posed by al Qaeda in the Arabian Peninsula, al Qaeda's affiliate in Yemen, and mentions the radical Yemeni-American cleric Anwar al-Awlaki, and Samir Khan, who published the jihadist magazine Inspire. Both were killed in a drone strike in 2011; the presentation references their influence on would-be terrorists in the United States, but in such a way that it remains unclear if they were still alive when it was written. It also mentions Sharif Mobley, an American citizen who has been in prison in Yemen since 2010. (The FBI interviewed Mobley in 2010 after he was arrested by Yemeni authorities on terror charges, which were later dropped; Mobley's family denies that he has any ties to extremism.)

The presentation's authors were especially interested in Salafism, a conservative form of Sunni Islam, and the influence of particular schools in Yemen, including al-Iman University, in Sanaa, and schools they call "DAHN," perhaps a reference to Dar Al Hadith, a group of Salafist schools where foreign converts studied and in which Western intelligence agencies have long been interested. (The Intercept spoke to one Yemeni-American who was questioned by the FBI in 2011 about both institutions.)

Yet the presentation admits that "institution of study is of limited predictive value" and there is "no systematic way of identifying who has become radicalized." The only commonalities between the individuals they had identified -- presumably referring to people who had left the United States to join AQAP -- were that they were all between the ages of 20 and 40, and "'born again' Muslims -- either converts to Islam or people who had rediscovered their faith in mid-life."

"Our 'threat pool' consists of born- again muslims who have traveled to Yemen or who intend to do so. However, there are thousands of such people, and very few of them become AQ groupies," the presentation asks. "How do we weed out the true threats?"

The FBI thought it could get to them by looking for "younger, more devout sources" -- specifically, "young Salafists." They wanted people who had been or were thinking of going to Yemen, or were "in the social circles where travel for overseas study is discussed." It also suggests that agents "focus on recruiting young Salafists of any ethnic background," who could serve as "human tripwires -- they're the ones who can tell you when people they know begin to move in the takfir/jihad direction."

Under headings like "Finding Your Salafis" and "Seducing the Salafis," the presentation suggests that "existing sources in local mosques should be able to tell you about groups of young Salafis in the community," and advises that agents take advantage of undercover operations "that capture discussions between Salafis," study Facebook profiles for signs of increasing "levels of piety," and target "the local MSA," or Muslim Student Association.

The goal was "to look for people at the edges who are in the same circles, but not radical enough" to warrant opening an investigation into. The presentation suggests exploiting doctrinal disputes and making appeals to potential sources who may "hold views that strike us as extreme," but who are not "jihadists of the AQ stripe."

A Broad-Brush Approach

The focus in the document on young, pious Muslim students echoes a now- discredited effort by the New York City Police Department to monitor Muslim student groups as part of widespread surveillance of Muslim communities and businesses in and around New York. The NYPD sent undercover police officers onto college campuses in the city and across the Northeast, and monitored students' online interactions. Internal records showed that the NYPD was especially interested in Muslim student associations, which they defined as "a university-based student group, with an Islamic focus, involved with religious and political activities." Some groups drew NYPD interest because they had invited "salafist speakers," according to the AP, while another had "students who are politically active and radicalizing." The program was exposed in 2011 and the department eventually disbanded the unit in charge, admitting that it had never generated a lead.

In 2011, when the Associated Press first reported on the NYPD surveillance, the FBI insisted that its agents were bound by stricter rules, and in fact, that the NYPD's clumsiness was interfering with the bureau's investigations. Given that the presentation says the FBI was looking for informants with specific insights into Al Qaeda, it's possible that the approach would have been more tailored and required more supervision than the kind of blanket surveillance of entire neighborhoods and establishments that the NYPD engaged in. Yet the presentation does suggest broad scrutiny of Yemeni populations, and does not mention rules governing that type of surveillance. The presentation notes that the "FBI has access to thousands of Yemeni immigrants residing in the U.S." and was "developing strategies for identifying people in the U.S. with familial connections to specific tribes." The presentation encourages agents to "know where the Yemenis in your [Area of Responsibility] are from," and to ask their existing sources "to find individuals from the relevant regions."

"I don't think there is much difference between this approach and what the NYPD was doing, in that it is identifying religious practice or ethnicity as an indicator of association with terrorism," said Mike German, a former FBI agent and fellow at the Brennan Center for Justice at New York University School of Law.

The fixation on Salafism was common in both agencies, German said. He pointed to other FBI materials that include references to Salafism "as the foundation from which terrorism arises, which is an inaccurate and simplistic idea."

The NYPD had produced a heavily criticized report that drew a direct link between commonplace religious activity and terrorism; FBI materials from the same time period also described a simple theory

of a line from conversion to jihad, and identified mosques and other associations as places where radicalism might grow. German says that the FBI's current radicalization theory "tends to be more vague about what indicators they should look for, I think because we know there aren't reliable indicators" of propensity to violence.

Yet, he said, the FBI is still "looking at the general population and trying to predict where someone will go bad -- a broad-brush approach that amounts to profiling -- as opposed to looking at where there's actual evidence."

The National (UAE)
GCC gains from French high-tech experience
Friday, 30 September 2016
Byline: Colin Randall

Toulon - On the quayside at Saint-Mandrier-sur-Mer, opposite the French naval port of Toulon, state-of-the-art drones and robots capable of performing the most intricate of tasks on land, in the air and at sea stand gleaming in the Mediterranean sunshine.
Behind them rest two elderly and decommissioned warships. The frigates' remaining function is to serve as breakwater for the combat diving school run by DCI, the French defence ministry's commercial arm for exporting know-how.

The expertise taught by DCI centre instructors travels successfully and 60 per cent of the divers trained there in the past 14 years have been from the Arabian Gulf.

DCI sales in the fields of consulting, training and technical assistance reached 227.5 million (Dh904m) in 2015m, reflecting a 35 per cent increase in five years. It brings employment for almost 1,000 people and there are permanent offices in the UAE, Saudi Arabia, Qatar and Kuwait and Saudi Arabia as well as South East Asia and India.

The juxtaposition of old and new on the Saint-Mandrier quayside presents a striking contrast. The old frigates have done their active service and been replaced by much more modern vessels; the robotic equipment to which they provide a backdrop has a wide range of military and civil applications in a more technological age.

The most eye-catching device on display is a yellow drone from the Toulon-based defence manufacturer ECA's IT180 range. Valentin Hanns, ECA's export sales director, says it would cost a buyer up to 300,000 for the basic model, adding: "What you pay above that depends on what kind of payload you want fitted."

Beyond their value in conflict zones - a camera system with powerful zoom can identify enemy troops at a range of 600 metres - IT180s can be used in survey missions in mining and on pipelines and power lines and are proving an effective tool in firefighting.

At the naval air base of Hyeres, a short drive east of Toulon, Lt Bernard Bastien is happy to talk about the Panther Standard 2 helicopter he flies.

The aircraft is classically used for naval missions, either in conflict or in combating drug trafficking and piracy at sea. Gulf Armed Forces deploy several of the aircraft.

A reliable workhorse with a history stretching back more than 20 years, the Airbus-built helicopter has undergone significant upgrades to give it, in the words of the makers, a second youth. "We do not carry arms but act as the eyes of the frigate in any operation," says Lt Bastien, 31, who serves with the French navy's 36 Squadron or Flottille 36F.

"Previously, it could be like flying blind at night, with just radar, so we were able to detect what was there but not identify it. Infrared night visibility has made a huge difference; it's as if we are flying in daylight."

The Euronaval exhibition will also showcase developments in systems to counter cyber threats.

As Jean-Michel Orosco, senior vice- president in charge of cyber security for DCNS, puts it, "it comes down to trying to stay a step ahead of the bad guys".

At the company's new site in Ollioules, just outside Toulon, Mr Orosco says cyber attacks can be mounted for reasons of espionage or for use as a weapon or in organised crime.

"Just think about any major country in the world being without electricity supply for several weeks, as a result of state, terrorist or criminal cyber attacks," he says. "It would be a nightmare."

DCNS, which employs 13,000 people in 10 countries including Saudi Arabia, Malaysia and India, is currently building six Fremm-class frigates for the French navy, all to be delivered by 2019. It prides itself on its "cyber resilient" ships.

But as if to demonstrate the need for constant vigilance - that need to outsmart the assorted enemies mentioned by Mr Orosco - DCNS is currently embarrassed by a huge data breach concerning six Scorpene-class submarines it is due to supply to the Indian navy later this year.

The technical information targeted by hackers was handed to an Australian newspaper, which published extracts from the 22,000 pages reportedly leaked.

The technewsworld.com website says the episode raised questions about an Australian deal to buy 12 submarines from DCNS.

It echoes previous cyber attack on contractors who were in the running for the Australian deal.

No DCNS official was willing to comment beyond confirming that the leak was being investigated - and that the Australian contract was still considered on.

Times of India
First major use of Cartosat images for Army
Friday, 30 September 2016
Byline: Chethan Kumar

Bengaluru - In what's being described as the first major use of the Cartosat family of satellites, the last one (2c) launched in June this year, sources in Isro said that the armed forces were aided by high-resolution images for the surgical strikes+ conducted across the line of control+ (LoC) in the small hours of Thursday.
A source in Isro said: "We've been providing images to the armed forces, the army in particular. While I cannot comment if any specific image was sent on a particular day in the previous week, I can say that Cartosat images are meant for this purpose and the army has used this."

Both Isro and the Ministry of Defence (MoD) have largely remained tight-lipped about the uses of the Cartosat family of satellites-- which experts call India's 'eye in the sky'--built for dual use.

The Cartosat-2C in particular added more teeth to India's military surveillance and reconnaissance capabilities, and has been providing high resolution images of 0.65 metres, an improvement over the 0.8m resolution of the earlier missions.

"Cartosat also provided Area of Interest (AOI) based images for the armed forces," the source said. Another explained that based on requests, one or more scenes/images covering the AOI as specified is provided in as a single polygon (all the areas in one circle) in the form of a shapefile (non-topological geometry and attribute information for the spatial features).

According to the National Remote Sensing Centre (NRSC) in Hyderabad, AOI products are of two types--standard and precision-based ortho (where images taken from space are corrected to have an uniform scale- -both of which are useful for the armed forces. Ortho rectified products are corrected for terrain distortions and camera tilt effects.

While the first Cartosat was launched in 2005, Cartosat-2A launched in 2007 was the first dual-use satellite with capabilities of monitoring missile launches in India's neighbourhood.

And, the Cartosat-2C is the best in the class that India boasts of although countries like the US and Israel boast of better ones. This satellite can not only click pictures of areas of interest, but also record videos of sensitive targets from space, compress it, and relay it back to earth.

Gulf News
Why IT spending is top priority for organisations?
Friday, 30 September 2016
Byline: Naushad K. Cherrayil

Dubai - With a wide array of new cyber threats constantly pushing IT organisations, it is no wonder that IT security is the top spending priority for most organisations worldwide.
IT security spending is only a small part of the total IT budget, but it has been steadily growing and will continue to do so.

Statistics show that the average share of IT budgets has been growing every year. According to Ponemon Institute, it was 7.5 per cent of their overall IT budgets in 2005 and 10 per cent in last year.

In Europe, Middle East and Africa, it is between 8 and 12 per cent of the IT budget on security. Why is it growing? Many high-profile companies have been subject to hacker attacks recently and they probably won't be the last.

"Organisations are struggling to keep up against cyber threats as cyberattacks are growing in complexity," said Alain Kallas, Middle East managing principal for security and risk consulting at Dell Technologies subsidiary SecureWorks, a provider of intelligence-driven information security solutions.

He said that 66 per cent of the cyberattacks on organisations are discovered by third parties and 33 per cent of attacks are discovered only within two years.

For example, Yahoo revealed last week that personal information accounts belonging to at least 500 million accounts, biggest data breach so far, was stolen from its network in late 2014.

"50 per cent of the cyberattacks use evasive techniques to bypass existing controls to steal information. $3.7 million is the average cost of a breach involving records in one organisation," Kallas said.

Kaspersky Lab estimated that every day a security breach goes undetected costs large businesses $100,000 on average, while an average cost of recovery from a breach detected within hours is less than $400,000.

Kallas said that organisations are not only finding it difficult to hire the right security professionals but also struggling to retain the talents. "75 per cent of security professionals have been approached by a

hiring organisation or headhunter about IT job opportunities in the past year. 17 per cent premium paid to senior and middle level managers with security in their titles," he said.

With security risks becoming more pervasive and difficult to prevent, he urged companies in the Middle East to be more vigilant and invest in cyber defence to protect their infrastructures.

The cyber groups are well financed because of the amount of money generated out of each transaction.

"The Darknet eCommerce, which is an environment within the internet which a common cannot access and cannot be monitored, is an illegal marketplace where criminals buy and sell stolen information," he said.

One of the website, Evolution, makes roughly between $20 million and $25 million revenue a month. There are other sites like Tor, i2P, The Freenet Project, etc.

"It is difficult to trace them and needs huge amount of sophisticated technologies, even Cyber Threat Intelligence Units around the world find it difficult to catch them. These guys have huge salaries and life insurance, among other benefits. It is an organised cybercrime and it is a big business," he said.

SecureWorks collects billions of events on a daily basis from over 4,300 clients across 59 countries and multiple industries worldwide.

He said that SecureWorks' Counter Threat Platform (CTP) processes as many as 190 billion events a day, and the platform quickly determines which of these events are cyberattacks and blocks them, while providing important clues as to the hackers behind the attacks and their ultimate intent.

"It will take two to three months to detect a signature and once detected, we inform the industries to be aware that a new attack is detected and this is what you can do to protect it till further action is taken. Based on that, we can tell our clients who are the threat actors and how they operate," he said.

Cyber security experts said that ransomware, which has been growing in leaps and bounds globally, is a lucrative and safe method of making money for criminals.

Kallas said that 55 per cent growth in quarter-on-quarter in ransomware in the second quarter of this year.

Ransomware is software that infects a computer and prevents users from accessing their data unless the user pays a ransom.

Kaspersky Lab said that the total number of users encountering any type of ransomware increased from 1.97 million in 2014 to 2.31 million users in 2015 around the world.

The cost of decryption varies -- from as little as $30 to thousands of dollars. The average ransom demanded by cybercriminals is $300, and according to various sources, at least 40 per cent of the victims pay their ransom.

The victims were asked to pay between $50 and $500, depending on the data.

Symantec said that 40 per cent of global consumers have admitted to paying a ransom to attackers to unlock their computers and smartphones.

Businesses in the UAE were a victim of 2.7 per cent of global targeted attacks, with an organisation facing an average of 2.2 attacks through the year.

Over the last five years, the Middle Eastern organisations surveyed have incurred a total financial loss of approximately $1.49 million due to system perimeter breaches. Subsequently, the average cost of detecting and fixing these breaches was approximately $35.23 million.

Yahoo News
Russia steps up trolling attacks on the West, U.S. intel report finds
Thursday, 29 September 2016
Byline: Michael Isikoff

New York - A new U.S. intelligence report says the Russian government is conducting a wide-ranging and "opportunistic" campaign to expand its political influence in Europe by deploying Internet "trolls and other cyber actors" to challenge pro-Western journalists and spread pro- Kremlin messages in social media forums.
Yahoo News obtained a declassified summary of the report, which also describes the role of two state-owned media outlets, RT and Sputnik, in what some experts say is an increasingly aggressive "information warfare" campaign. According to the report, the outlets promote Russia's political aims with programming targeted to "activist" audiences including "far-right and far-left elements of European society." It adds that the RT channel gives "disproportionate coverage and airtime to the European Parliament's more extreme factions."

The report, by the office of Director of National Intelligence James Clapper, was originally requested by congressional intelligence committees late last year. The panels also asked for a separate report on Russia's use of political assassination. Classified versions of both documents were delivered by Clapper's office to Capitol Hill in July.

The decision to declassify brief excerpts from the first report coincides with recent disclosures about suspected Russian cyberattacks on the Democratic National Committee and other political groups. Many in the U.S. intelligence community believe that indicates Russia has expanded its cyberwar and disinformation efforts to the United States. "This is the 21st century version of 'active measures,'" said

Heather Conley, director of the Russia program at the Center for Strategic and International Studies (CSIS), a reference to the Cold War term for the Soviet Union's efforts to manipulate Western opinion by spreading false information, such as the claim that U.S. scientists had manufactured the AIDS virus as part of a biological weapons project at Fort Detrick, Md.

Conley added that the use of "information warfare" techniques to pursue political goals has now been incorporated into official Russian military doctrine. The goal, she said, is not "the annihilation" of the country's enemies, but to "weaken them from within" by "keeping everybody off balance" and "sowing doubt" about their political leaders and institutions. A report by Conley describing this effort is due to be released by CSIS next month.

Russia's use of trolls on social media would appear to fit that pattern. A report in the Guardian last year identified a St. Petersburg office building where "hundreds of paid bloggers work around the clock" to flood Internet sites and Western social media forums with posts praising Russian President Vladimir Putin and denouncing the "depravity and injustice" of the West.

Michael Weiss, editor of the Interpreter, an online publication that tracks the Russian media (and that is funded by Radio Free Europe/Radio Liberty), said he was personally targeted by Russian trolls after he published an article exposing a frequent RT commentator on Germany as the editor of a neo-Nazi magazine. "They've been on a campaign to destroy my career," said Weiss. He's found himself attacked on social media forums as a "neocon Zionist propagandist," he said. A pro-Russian troll even dug into his wife's Facebook account to retrieve old photos, he said.

Another tactic of the trolls is to inject blatantly false stories into the media, forcing public officials in Europe and the U.S. to respond, according to Weiss and other experts. A New York Times Sunday Magazine piece last year documented how Russian trolls based in the St. Petersburg office had swamped Twitter with hundreds of messages about an explosion at a Louisiana chemical plant that never took place, setting up dozens of fake accounts and doctoring screenshots from CNN and Louisiana TV stations to make the pseudo-event seem real. (The trolls even created a fake Wikipedia page about the supposed explosion, which in turn linked to a phony YouTube video.) Similar methods were used to spread false stories about an outbreak of Ebola in Atlanta, the Times account reported.

The author of the Times article, Adrian Chen, now a writer for the New Yorker, recently said many of the Russian trolls he was tracking have begun tweeting favorably about Donald Trump.

Although the activities of the Russian trolls have been aired in a handful of media accounts in recent years, the decision to include references to them in the declassified DNI summary appears to be part of a stepped-up effort by Washington to publicly combat Russian Internet efforts and cyberattacks. The full report covers a much broader subject: the scope of Russian influence operations throughout Europe and Central Asia, including the covert funding of political parties and nongovernmental organizations.

"Moscow has been opportunistic in its efforts to strengthen Russian influence in Europe and Eurasia by developing affiliations with and deepening financial or political connections to like- minded political parties and Non-governmental Organizations," according to a letter containing the declassified excerpts that was sent this week by Clapper's office to House Intelligence Committee Chair Rep. Devin Nunes and ranking minority member Rep. Adam Schiff.

"Moscow appears to use monetary support in combination with other tools of Russian statecraft, including propaganda in local media, direct lobbying by the Russian Government, economic pressure, and military intimidation," the letter states.

The declassified excerpts don't include specific examples. But a separate report on the same subject earlier this year by the Congressional Research Service, prepared at the request of Rep. Chris Stewart, a Republican from Utah, cited as evidence Russian financial and political support for far-right, anti-immigrant European political parties, including the National Front in France and Jobbik in Hungary. The French National Front, which is headed by Marine Le Pen and which backed Russia's annexation of Crimea, has received a loan of 9 million euros from a Russian bank with close ties to Putin, the CRS report notes, and Jobbik's finances have been under investigation by the Hungarian Parliament amid allegations that it had received funding from Moscow.

Time Magazine
How Russia Wants to Undermine the U.S. Election (Canada)
Thursday, 29 September 2016
Byline: Massimo Calabresi

New York - The leaders of the U.S. government, including the President and his top national-security advisers, face an unprecedented dilemma. Since the spring, U.S. intelligence and law-enforcement agencies have seen mounting evidence of an active Russian influence operation targeting the 2016 presidential election. It is very unlikely the Russians could sway the actual vote count, because our election infrastructure is decentralized and voting machines are not accessible from the Internet. But they can sow disruption and instability up to, and on, Election Day, more than a dozen senior U.S. officials tell TIME, undermining faith in the result and in democracy itself.
The question, debated at multiple meetings at the White House, is how aggressively to respond to the Russian operation. Publicly naming and shaming the Russians and describing what the intelligence community knows about their activities would help Americans understand and respond prudently to any disruptions that might take place between now and the close of the polls. Senior Justice Department officials have argued in favor of calling out the Russians, and that position has been echoed forcefully outside of government by lawmakers and former top national-security officials from both political parties.

Unfortunately, it's not that simple. The President and several of his closest national- security advisers are concerned about the danger of a confrontation in the new and ungoverned world of cyberspace,

and they argue that while the U.S. has powerful offensive and defensive capabilities there, an escalating confrontation carries significant risks. National Security Council officials warn that our critical infrastructure-including the electricity grid, transportation sector and energy networks-is vulnerable to first strikes; others say attacks on private companies, stock exchanges and the media could affect the economy. Senior intelligence officials even worry about Russia exposing U.S. espionage operations in retaliation. And while U.S. officials have "high confidence" that Russia is behind what they describe as a major influence operation, senior U.S. officials tell TIME, their evidence would not yet stand up in court.

And so with five weeks to go, the White House is, for now, letting events unfold. On one side, U.S. law-enforcement agencies are scrambling to uncover the extent of the Russian operation, counter it and harden the country's election infrastructure. On the other, a murky network of Russian hackers and their associates is stepping up the pace of leaks of stolen documents designed to affect public opinion and give the impression that the election is vulnerable, including emails from the computers of the Democratic National Committee (DNC). Meanwhile, the FBI alerted all 50 states to the danger in mid-August, and the states have delivered evidence of a "significant" number of new intrusions into their election systems that the bureau and their colleagues at the Department of Homeland Security "are still trying to understand," a department official tells TIME.

All of which makes Donald Trump's repeated insertion of himself into the U.S.-Russia story all the more startling. Trump has praised Putin during the campaign, and at the first presidential debate, on Sept. 26, he said it wasn't clear the Russians were behind the DNC hack. But the U.S. intelligence community has "high confidence" that Russian intelligence services were in fact responsible, multiple intelligence and national security officials tell TIME. Trump was informed of that assessment during a recent classified intelligence briefing, a U.S. official familiar with the matter tells TIME. "I do not comment on information I receive in intelligence briefings, however, nobody knows with definitive certainty that this was in fact Russia," Trump told TIME in a statement. "It may be, but it may also be China, another country or individual."

Russia's interference in the U.S. election is an extraordinary escalation of an already worrying trend. Over the past 2½ years, Russia has executed a westward march of election meddling through cyberspace, starting in the states of the former Soviet Union and moving toward the North Atlantic. "On a regular basis they try to influence elections in Europe," President Obama told NBC News on July 26. With Russia establishing beachheads in the U.S. at least since April, officials worry that in the final weeks of the campaign the Russian cybercapability could be used to fiddle with voter rolls, election-reporting systems and the media, resulting in confusion that could cast a shadow over both the next President and the democratic process.

Obama's decision not to call out the Russian espionage operation has so far left the effort to educate Americans about it to lawmakers and national-security experts. On Sept. 22, the ranking Democrats on the Senate and House Intelligence Committees, California's Senator Dianne Feinstein and Representative Adam Schiff, released an unusually blunt statement. "Based on briefings we have received, we have concluded that the Russian intelligence agencies are making a serious and concerted

effort to influence the U.S. election," they said. "At the least, this effort is intended to sow doubt about the security of our election." Orders for Russian intelligence agencies to conduct electoral-influence operations, they added, could come only from very senior levels of government. "We call on [Russian] President [Vladimir] Putin to immediately order a halt to this activity." The statement, though not endorsed publicly by the Administration, was cleared with the CIA.

To understand why Putin would want to undercut the legitimacy of the U.S. election, it helps to step back from the long and ugly presidential campaign and remember why we're voting in the first place. Elections are the ultimate source of authority in our democracy. Because Republicans and Democrats have agreed for decades that spreading democracy is good for everyone, America has pushed for free and fair elections around the world. And many nations have embraced them: peasants in the Balkans put on their Sunday best to go to the polls, and burqa-clad women in Afghanistan brave terrorist attacks to stand in line for hours to cast their ballots.

Not surprisingly, quasi- authoritarian rulers in the former Soviet Union, latter-day communists in China and medieval theocrats in the Middle East, among many others, see America's sometimes aggressive evangelism about the benefits of liberal democracy as a direct threat to their own claims to authority. Putin has taken particular umbrage, accusing the U.S.-and former Secretary of State Hillary Clinton in particular-of meddling in Russia's presidential election in 2012. He has publicly questioned the validity of past U.S. presidential elections, saying, on June 17, of the Electoral College, "You call that democracy?" Now, experts say, Putin is expanding his anti-American campaign into cyberspace. "More than any attempt to get one candidate or another elected, this [Russian influence operation] is about discrediting the entire idea of a free and fair election," says Dmitri Alperovitch, co-founder and chief technology officer of CrowdStrike, the cybersecurity company that did the analysis of the DNC hack.

No one knows that better than Arizona secretary of state Michele Reagan. One day in June she was in her backyard in Phoenix when she got a call from her chief of staff. "Are you sitting down?" he asked. The FBI had been monitoring a corner of the so-called dark web, the network of hidden sites used by criminals to buy and sell drugs, pedophilic pornography and stolen identities. A group of hackers known collectively as Fancy Bear, which the U.S. government believes is controlled by Russian military intelligence, was trying to sell a user name and password that belonged to someone in an Arizona county election official's office, which holds the personal data of almost 4 million people. "My first reaction was, Well, this is like the worst thing that you want to hear," Reagan recalls.

Reagan and the FBI scrambled to figure out how the Russians had gotten into Arizona's system and what needed to be done to secure it. It turned out that an election official in rural Gila County, pop. 54,000, had opened a Word document on her desktop computer that contained malicious software. Fortunately, while Fancy Bear had penetrated a local computer system, it hadn't accessed the statewide registration database. Others weren't so lucky. Fancy Bear's electronic fingerprints were found on the hack into the DNC computers. In Illinois, the feds found that Fancy Bear had stolen 85,000 voter records from that state's registration systems in mid- July. Later that month, the Democratic Congressional Campaign Committee (DCCC) revealed that it, too, had been hacked by Fancy Bear.

With other states now reporting intrusions of unknown origin, the government wants to reassure the public that the vote count itself is safe. "We have confidence in the overall integrity of our electoral systems," Homeland Security chief Jeh Johnson said on Sept. 16. "It is diverse, subject to local control, and has many checks and balances built in." Each of the U.S.'s more than 9,000 polling places uses machines not connected to the Internet, precincts count and report their results independently, and most have paper or electronic backups in case a recount is needed.

The Administration has a message for Russia too. The U.S. has privately warned that any effort to sway the election would be unacceptable, intelligence and other Administration officials tell TIME. Secretary of State John Kerry delivered the message to his counterpart, Russian Foreign Minister Sergei Lavrov, in Laos on July 27. During a 90-minute meeting with Putin on the sidelines of the G-20 meeting on Sept. 6, Obama pulled Putin aside and discussed the cyberconcerns one-on- one, with no aides present, a White House official tells TIME. In a press conference later, the President called for restraint on all sides in the use of cyberweapons and issued a veiled threat about America's cyberpowers. "Frankly, we've got more capacity than anybody both offensively and defensively," Obama said.

Putin's history of using influence operations against opponents begins, appropriately enough, with himself. As he was rising quickly through the Kremlin ranks in 1999, one of his main opponents, Prosecutor General Yuri Skuratov, was caught on tape having sex with two women in a hotel room in what Skuratov later claimed was a Putin-run espionage operation traditionally known as a "honey trap." Putin, who had risen from a Soviet-era KGB operative to head the country's intelligence services, denied he was behind it but said on TV that his agents had confirmed that the man in the grainy video was Skuratov. Putin went on to win the presidency the next year. Skuratov, who ran against him, got less than 1% of the popular vote.

With the expansion of the Internet in the decade that followed, the Russians adopted cyberweapons as a standard tool of political meddling. Nowhere has their tactic of spreading chaos around a vote been clearer than in Ukraine, where three days before the presidential election on May 25, 2014, the computer systems of the Central Electoral Commission went dark. "The servers wouldn't turn on. The links to the local election authorities were cut off," says Victor Zhora, director of the cybersecurity firm Infosafe, which had been hired to defend the system. "Literally, nothing worked."

As Zhora and his team worked successfully to restore the system in time for the vote, they became convinced that the collective behind the hack, known as CyberBerkut, was a front for Russian security services. The malware that crashed the system was not available on the market and had been built from scratch. And the effect of the attack supported Russia's strategic goal of undermining the validity of the election. The hackers could have manipulated the outcome of the vote, Zhora says, but "their main goal was to take out the system itself, to destroy the data, to wipe out the hard drives before the elections started." Moreover, the CyberBerkut efforts appeared to be coordinated with Russian state propaganda. Zhora and his team stopped a subsequent effort by CyberBerkut to post false voting results on the election commission's website that would have showed a far-right militant ahead in the polls. But a

screenshot of the fake web page appeared anyway on Russia's main state-run news network as the vote was still going on.

Russia has also meddled in the elections of major U.S. allies that have imposed sanctions on Russia for its invasion of Ukraine, and many of the Russian cyberoperations have benefited populist, anti-immigrant parties that oppose Western European unity in the face of rising Russian aggression. In August, a spear-phishing e-mail attack targeted German party officials, including some members of Chancellor Angela Merkel's Christian Democrats. The emails contained malware that bore the signatures of Fancy Bear, according to Germany's top cyberdefense official, Arne Schönbohm, who warned on Sept. 9 that the attack could be an attempt to manipulate parliamentary elections next year. Merkel had previously ordered German intelligence agencies to look into Russia's peddling of a false story about a Russian girl raped by migrants in Germany-a story that has helped fuel the rise of the right-wing opposition party AfD. That party beat Merkel's Christian Democrats in a regional ballot in the Chancellor's home district in September.

Farther west, in France, a Russian bank with close ties to the Kremlin lent the far-right party of Marine Le Pen some 9 million euros in November 2014, helping it prepare for regional elections a year later, when it received its best results ever. Russia also tried a more subtle information operation designed to fuel the anti-immigrant and national-security fears that have contributed to Le Pen's rise. In April 2015, the programming of the French broadcaster TV5Monde was blocked by unknown hackers, and for 18 hours the channel's websites transmitted only the image of the signature black flag of ISIS. French intelligence officials and the British signals-intelligence agency, the GCHQ, found it was not ISIS but in fact Fancy Bear that was behind the hack, according to a Sept. 25 article by the London Sunday Times and U.S. officials.

Britain, too, has been targeted. The Times article quoted David Anderson, an independent watchdog appointed under British law, as saying the GCHQ had blocked a Russian attempt to disrupt the May 7, 2015, general election there. The Times said Fancy Bear planned to target government servers and major TV broadcasters. But not all stations were to be hit. In the fall of 2014, the pro-Moscow RT network, which is funded by the Kremlin, launched a 24-hour news network in the U.K. aimed at British viewers. The message, Russia experts say, is that Western democracy is not so hot. "It's a cynical message: No one is democratic," says Peter Kreko, an expert on the European right and a visiting professor at Indiana University.

The most pessimistic Kremlin watchers worry how far Putin will go with the combination of psychological manipulation and cyberwarfare. They view the pattern of Russia's electoral meddling in the context of Putin's recent embrace of what is known as the Gerasimov doctrine, a nontraditional approach to military conflict named after the chief of the Russian general staff, Valery Gerasimov, that relies heavily on cyberwar and influence operations. "A perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict," Gerasimov posited in a now famous 2013 manifesto, through "political, economic, informational, humanitarian and other nonmilitary measures applied in coordination with the protest potential of the population."

That is how Putin stoked a separatist rebellion in eastern Ukraine in 2014. But the current and former senior intelligence and national-security officials interviewed for this story agree that the principal benefit Putin gains from his Western European and U.S. meddling is the leg up it gives him with his own political and diplomatic challenges at home. "In the long run, if people start to question the integrity of our election system," says one senior U.S. intelligence official, "potentially to Russia that's a plus. But I would argue more strongly that this is as much about domestic constituents and his public," the official says. The more chaos in Europe and the U.S., the better.

Putin has shown little sign of stopping, even when meddling is discovered. In April, the DNC suspected it had been hacked and called in the cyberforensics firm CrowdStrike, which was co-founded in 2011 by Alperovitch and employs a number of former government cybersecurity experts. CrowdStrike was familiar with Fancy Bear: it had previously found the group's hacks in Canada, Japan and the former Soviet republic of Georgia. It identifies the group based on the Russians' unique cybertradecraft, including nonpublic code in its malware, its infrastructure of servers around the world and the techniques that it uses to move and hide within the systems it penetrates. After inspecting the DNC computers, Alperovitch concluded that the hack was indeed executed by the Russians. And while CrowdStrike usually keeps its findings secret, the DNC told the company it was outraged that the Russians were trying to interfere with our political system, and "they wanted us to come forward," Alperovitch says.

Twelve hours after the DNC break-in was revealed in June, a hacker who insisted he was Romanian and who called himself Guccifer 2.0 popped up online and tried to discredit CrowdStrike's attribution to Russian military intelligence. Guccifer 2.0 started leaking information from the DNC hack in blog posts and on Twitter, but his professed identity wasn't very convincing. When reporters reached out to him online, for example, the responses he sent in Romanian were riddled with errors. U.S. government officials privately confirm that they believe Fancy Bear and Russian military intelligence are behind the DNC and DCCC hacks.

The pace of leaks has accelerated as the election approaches, revealing a murky network of actors. Around the time of the DNC hack, a website called DCleaks.net was established by a group identifying themselves as "hacktivists." By June the group began posting hacked documents, including emails from retired General Philip Breedlove, the former commander of NATO and U.S. forces in Europe, asking former Secretary of State Colin Powell how to persuade Obama to more forcefully oppose Russian meddling in Ukraine.

Initially, there was no evidence of a connection between DCleaks and Russian hackers, and even now it is not clear who is behind the site. In late June, however, Guccifer 2.0 contacted the website the Smoking Gun and provided it with a link to material from the DNC hack that DCleaks was preparing to publish. In recent weeks, DCleaks has published new emails belonging to Powell, which included damaging remarks about Clinton, even though the overall gist of his emails was supportive. And recently, the site published what purported to be a copy of Michelle Obama's passport.

The leaks tend to favor isolationist policies over ones aimed at confronting Russia. The Breedlove leaks showed an embarrassing and unsuccessful effort to build U.S.-led pushback against Russia in Ukraine. The DNC documents, which made their way to WikiLeaks through unknown channels, weakened Putin's old foe, Clinton, on the eve of the Democratic National Convention. And DCleaks claimed that its ability to obtain the First Lady's passport demonstrated U.S. vulnerability to terrorism.

Putin has done what he can to maintain deniability. Asked by Bloomberg TV on Sept. 2 whether Russia was behind the DNC hack, he said, "I don't know anything about that." But he seemed admiring, if not proud, of Fancy Bear's work. "They work so much like fine jewelers, so delicately, that they can leave their tracks, or someone else's tracks, at just the right place and just the right time in order to camouflage their work and make it look like the work of some other hackers from somewhere else, some other country."

In fact, it might take a real jewel thief-or an army of them-to rig the U.S. presidential election. Because they are not connected to the Internet and are controlled by thousands of independent precincts, U.S. voting machines are largely safe from meddling, says Merle King, executive director of Kennesaw State University's Center for Elections Systems. The feds have pushed out patches for known vulnerabilities in state computers and offered security scans. America's cyber and counterespionage forces will be looking "to see if there's anything coming from overseas or even domestically that looks like an effort to target election offices," says George W. Bush's Homeland Security chief, Michael Chertoff. The FBI has opened a formal investigation into the DNC, DCCC, Arizona and Illinois hacks

But with the election fast approaching, some experts in and out of government say the Administration is moving too slowly to publicize the Russian influence operation and explain it to Americans. A bipartisan group of former national-security officials that included Chertoff and others called on Obama in July to name the perpetrators of the DNC hack. Alperovitch says the U.S. is misreading the battlefield in cyberspace. "The U.S. government for the last 20 years was so focused on how to achieve kinetic effects in cyberspace, how to produce what they call cyberbombs, because that's what we're used to," he says. "But the Russians understand that the real power of this domain is in influence operations, psychological warfare, changing people's perceptions of what's truly going on."

For much of the summer, Trump made casting doubt on the validity of the U.S. electoral system a prominent feature of his campaign. "I'm afraid the election's gonna be rigged," Trump said in Ohio on Aug. 1. " I have to be honest." Trump backers who sign up to be "Trump Election Observers" are told the campaign will "stop crooked Hillary from rigging this election."

Asked at the first debate whether they would support the outcome of the vote, both candidates said they would. But Trump has a record of doing the opposite. As results came in on election night in 2012, he falsely tweeted that the Republican had won the popular vote and urged an uprising. "The phoney Electoral College made a laughingstock out of our nation," Trump tweeted. "The world is laughing at us.

More votes equals a loss ... revolution! This election is a total sham and a travesty. We are not a democracy!"

Clinton has said Putin is trying to get Trump elected; there is no evidence of that. Trump does have some ties to Russia. Trump's former campaign manager worked for Putin's proxy in Ukraine until the pro-Western uprising there, and Trump, his family and a foreign policy adviser have done tens of millions of dollars of business in Russia. The exact amount is unclear, and Trump has declined to disclose details of his Russian business partners.

The links worry even rock-ribbed Republicans. Chertoff led the Senate Whitewater investigation of Bill and Hillary Clinton's obscure Arkansas land deal in the mid-'90s and has been critical of the Democratic presidential candidate. But he is alarmed by Trump's talk of a rigged election. "This business about talking about rigged elections is very dangerous," Chertoff says.

On the ground in Arizona, Michele Reagan, a Republican, has been working to make the vote safe. She took the entire state voter database offline for 10 days after learning of the Fancy Bear hack to ensure the system was secure. In conversations with the FBI and her own cybersecurity team she has learned phrases like SQL injection and dual- factor authentication. "Yes, we believe we're safe," she now says.

That doesn't mean she isn't worried about Russian attempts to undermine the credibility of the vote. "We know there's these bad actors out there that are coming in from other countries and they're trying to scare us," she says. "This isn't about stealing information or altering information. The entire conversation I believe needs to be shifted to what this is really doing to the confidence of the American electorate." Does she have a message for Americans on how to respond to Putin's effort? "Our job is to try to encourage people to get involved and to be connected in government, to go out and vote."

New Zealand Herald
NZME alerts contest entrants after cyber attack on server
Friday, 30 September 2016

Wallington - Media company NZME has warned some details of competition entrants may have been accessed by a cyber attack on a third- party cloud server used by the company.
Initial investigations show information relating to about 76,000 people was held on the overseas cloud server.

They were primarily email addresses, names and phone numbers, and some travel information for a small group.

NZME said that when it was alerted to the breach by a competition partner earlier this week, access to the server was immediately locked down.

Chief executive Michael Boggs said there was no evidence any of the information hacked had been used.

It did not contain any financial information or credit card data.

Competition partners and those contest entrants in the database were being contacted.

"The priority for us is firstly security and secondly then making sure that they're not open to spam or phishing that could come from this," he said.

"We're continuing our investigations - we believe it would be an offshore person or persons involved."

An external forensics team is working on the breach.

NZME, publisher of the New Zealand Herald and other newspapers and websites, and owner of radio stations including Newstalk ZB and ZM, had briefed the Privacy Commission and would work to ensure all appropriate steps were taken.

"Our priority now is working with competition partners and customers to [help them] make sure their information stays secure," said Boggs.

Chief executives responding to the Herald's Mood of the Boardroom identified cyber security as one of their main concerns.

"This highlights these threats are ever-present and we have to ... evolve and keep on top of them to protect the customers," Boggs said.

Ottawa Citizen
'Critical' for DND staff to do mandatory Phoenix training
Saturday, 01 October 2016
Byline: David Pugliese

Ottawa - Thousands of civilian employees at the Defence Department have until next week to complete mandatory training on the controversial Phoenix pay system.
The training is critical to minimize errors affecting the problemplagued federal government system, noted a message sent to all department workers and obtained by the Ottawa Citizen.

Phoenix pay system foul-ups have left thousands of Canada's public servants unpaid. But senior federal officials have countered that many of the issues with the pay system are not technical, but linked to employees failing to properly fill out workrelated information.

"It is critical that you complete the mandatory training to minimize errors that will lead to pay issues," the Department of National Defence message pointed out. "Training can help both employees and managers overcome the challenges associated with the transition to the new system."

The training must be completed by Oct. 7 and involves a one-hour course that can be completed online.

"The majority of employees who have taken the self-paced course have indicated that the training was beneficial to ensuring that their information was entered correctly," the message said.

Once training is completed, the employee must provide a training co- ordinator with a copy of a certificate of completion. There was no indication what the consequences of failing to complete the course are.

DND employees have been taking the training voluntarily, but as many as 30 per cent of the 24,900 workers have yet to complete the course. "The October 7th deadline reflects the fact that resolving pay issues is a top priority for the department,"

DND spokeswoman Jessica Lamirande said in an email response to the Citizen.

Lamirande said the training is offered by the Canada School of the Public Service to all federal employees. "DND chose to make the training mandatory for those who had not yet taken it," she said.

Several weeks ago, the senior bureaucrat who oversaw the Phoenix project suggested problems could have been avoided if all federal employees were forced to take training on how the system worked.

Rosanna Di Paola, Public Services and Procurement Canada's associate assistant deputy minister of accounting, banking and compensation, told a labour board hearing that when she looks back at what went wrong she now believes she should have pressed for mandatory training.